В.А. Конявский, С.В. Лопаткин

КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ

1

Москва 2004

Конявский В.А., Лопаткин С.В.

Компьютерная преступность. В 3-х томах. Т. 1. М.: . — 2004.

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. В первом томе даётся общая характеристика преступлений в сфере компьютерной информации, излагаются истоки, история и тенденции развития этого явления, рассматриваются методы и способы совершения, а также классификация компьютерных преступлений. Кроме того, в нём рассказывается о вредоносных компьютерных программах и их авторах, а также последствиях проникновения указанных программ в компьютер пользователя, информационную систему или сеть. Второй том представляет собой изложение хронологии возникновения и совершенствования вредоносных компьютерных программ, известных под названием «компьютерные вирусы». В этом томе читателю предлагается также достаточно подробное изложение истории возникновения и «развития» компьютерного андеграунда. В третьем томе рассматриваются конкретные случаи электронного мошенничества и способствующие их совершению условия. Материал третьего тома содержит и описание попыток борьбы с компьютерной преступностью с помощью законодательных методов, а также подходов, обеспечивающих безопасность компьютерных систем. Приводятся доводы в пользу необходимости применения различных средств в целях обеспечения защиты информации, в том числе внедрения современных аппаратно-программных комплексов.

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 высоких информационных технологий и языков программирования. Материал книги опирается на обширную фактографическую основу, статистические данные и, в необходимых случаях, проиллюстрирован соответствующими схемами и таблицами, а отдельные тома дополнены приложениями.

Конявский Валерий Аркадьевич, доктор технических наук, директор Всероссийского научно-исследовательского института проблем вычислительной техники и информатизации (ВНИИПВТИ), член научного совета при Совете Безопасности РФ, заведующий кафедрой защиты информации Московского физико-технического института (государственного университета – МФТИ).

Автор более 150 работ, включая изобретения и монографии.

Лопаткин Сергей Владимирович, начальник отдела Федерального агентства по информационным технологиям («Росинформтехнологии»), автор более 70 работ, включая научно-технические отчеты, статьи, брошюры и книги.

СОДЕРЖАНИЕ

От авторов

ЧАСТЬ I. КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ:
ВОЗНИКНОВЕНИЕ, ИСТОРИЯ, ТЕНДЕНЦИИ

Глава I. Угроза нового типа

§1. Предмет преступного посягательства,
уголовно-правовой аспект компьютерной преступности
и источник угрозы

§2. Методы совершения компьютерных преступлений и их
классификация, основанная на кодификаторе Интерпола

§3. Основные подходы, развивающие и дополняющие
классификацию Интерпола

§4. Великое противостояние: зарождение и динамика,
победы и поражения

§5. Борьба с компьютерной преступностью
и государственная политика

Глава 2. Вредоносные компьютерные программы и их авторы

§1. Основы вирусологии

§2. Глазами аналитика: общепринятая классификация вредоносных компьютерных программ

2.1. Среда обитания

2.2. Заражаемые операционные системы

2.3. Особенности алгоритма работы

2.4. Деструктивные возможности

2.5. Использование Интернет-технологий

2.6. Проникновение в систему и автономность

2.7. Программы конструкторы и генераторы вирусов

§3. Глазами пользователя: говорим «компьютерные вирусы» — подразумеваем «потери»

3.1. Масштабы ущерба

3.2. Действие и противодействие

3.3. Невзирая на громкие имена и авторитеты

3.4. Терроризм и кибертерроризм

3.5. Жертвы и разрушения

§4. Работа над ошибками: причины живучести вредоносных программ и их успешного распространения

ЧАСТЬ II. ЛЕТОПИСЬ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ – XX ВЕК

§1. Повторение – мать учения

§2. Оценка серьёзности угрозы со стороны вредоносных компьютерных программ

2.1. Методологический подход, принятый компанией Symantec

2.2.Методологический подход, принятый фирмой Panda Software

§3. Моделирование процессов распространения вредоносных компьютерных программ

§4. Когда деревья были большими

4.1. 40-е — 50-е годы: доисторический период – курьёз и теория

4.2. 60-е — 70-е годы: у истоков вирусописания – Рубикон перейдён

§5. 1980-1985 гг.: детство и отрочество

5.1. 1980 год – первые «радости»

5.2. 1981 год – первая масштабная эпидемия и диагноз

5.3. 1982 год – вирус-антивирус, эксперименты и программы «черви»

5.4. 1983 год – рождение компьютерной вирусологии

5.5. 1984 год – мы уже умеем читать прерывания и считать циклы

5.6. 1985 год – осваиваем конструкцию «троянского» коня

§6. 1986 год – пандемия первого компьютерного вируса для IBM PC

§7. 1987 год – наступила эра загрузочных вирусов

§8. 1988 год – отсроченные эпидемии, первые компьютерные мистификации и великий «червь» Морриса-младшего

§9. 1989 год – болгарский «завод» по производству вредоносных программ, вирусы-разрушители, технология «стелс», рождение журнала «Virus Bulletin»

§10. 1990 год – полиморфизм, бронирование, многоуровневое шифрование, сегментация, многокомпонентность и многое, многое другое

§11. 1991 год – первые программы-генераторы и конструкторы вирусов, «противо-противо-вирусный» компьютерный вирус

§12. 1992 год — новые приёмы маскировки, вирусы для платформы «Macintosh», первый «пермутативный» вирус, первый компьютерный вирус, разработанный специально для операционной системы MS Windows 3.xx, а также польза и вред от около вирусной шумихи

§13. 1993 год — «бомбы замедленного действия», усовершенствованный полиморфизм, вирусы «компаньоны», издание первого официального перечня «WildList», творения «Чёрного барона», усложнённый алгоритм шифрования, конвейер на основе конструкторов вирусов и полиморфик-

генераторов

§14. 1994 год — освоение вирусами новых «ниш» продолжается, и они становятся всё быстрее и опаснее: первая в России эпидемия полиморфного вируса, деструктивный вирус для платформы Macintosh, «великий и ужасный шифровальщик жёсткого диска» по имени «One_Half», отечественная «Зараза», продолжение компьютерных мистификаций

§15. 1995 год — начало заката эры загрузочных вирусов, новые приёмы маскировки от антивирусных средств и пользователя, «двуполый» вирус, пандемии «Byway» и «DieHard2», триумфатор года макровирус «Concept»

§ 16. 1996 год — деструктивность, сложность и скорость распространения вредоносных кодов неуклонно растут. Они были первыми: вирусы под операционные системы Windows 95 и OS/2, «Zhengxi», межплатформенный «Laroux» для MS Excel. Первая эпидемия вируса для Windows 3.x

§17. 1997 год — макровирусы множатся, совершенствуются, мигрируют в MS Office 97 и превращаются в проблему номер один. Они были первыми: вирус под операционную систему Linux, использующий протокол FTP сетевой вирус-червь, самостоятельно шифрующийся вирус для Windows 95, черви mIRC и PIRCH

§18. 1998 год – совершенствование вирусов для 32-разрядных Windows, а также «троянских» программ и утилит скрытого администрирования продолжается. Они были первыми: макровирусы для СУБД Access, для Access и Word одновременно, для PowerPoint, вирус-червь для платформ *Power Macintosh,* вирус-паразит на Java-файлах, HTML-вирус и Его Величество «Chernobyl»

§19. 1999 год – они были первыми: использующий MS Outlook современный Интернет-червь под Windows, похищающий ключи системы шифрования PGP макровирус, макровирус для Access, Word и PowerPoint одновременно, записывающий свой код в файлы помощи Windows вирус, вирус для Corel DRAW! и приложений Corel PHOTO-PAINT, Corel VENTURA. А также Её Величество «Melissa» и многое другое

ПРИЛОЖЕНИЯ

Приложение 1. Компьютерные мистификации и вредоносная мимикрия

Приложение 2. Портрет вирусописателя

Приложение 3. Что это такое — «дикий» вирус?

Приложение 4. Перечень Международной организации «The Wild List»

Список литературы

От авторов

Написать эту книгу хотелось давно. Начиная с тех лет, когда абсолютно безвредные резидентные программы, например, время от времени печатающие «жуткое» сообщение: «Сашка — козел», вызывали у упомянутого Сашки вовсе не раздражение (типа «за козла ответишь»), а искренний испуг и призывы о помощи в борьбе со страшным «вирусом». Сашка тогда не мог даже предположить, что этот «вирус» не послан свыше, а представляет собой простенькую программу, написанную приятелем в соседнем кабинете.

Время было романтическое, и вирусы воспринимались как наказание за «нечистоплотность» — стал использовать нелицензионную программу — получи, фашист, гранату!

Потом была первая попытка создать систему страхования информационных рисков, ставшая неудачной преимущественно из-за того, что на вопрос страховых компаний: «А статистика есть?» — не нашлось положительного ответа.

Дальше стало не до книг — все силы были брошены на борьбу с вирусами и вирусописателями (которые нет-нет да и оказывались в одном лице с лицами, предлагающими антивирусные программы).

С широким распространением «Интернет» расширился и канал распространения вирусов, упомянутые лица одержали недвусмысленную победу, и в необходимости оплаты антивирусных программ сомневаются уже гораздо меньше, чем в необходимости налога на добавленную стоимость. Само по себе это довольно удивительно, ведь за последние годы не появилось ни одного принципиально нового канала распространения вирусов — а справиться с ними не удается.

Действительно, 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. Так значит, схватка не вечна, и мы ее уже проиграли? Тоже «Нет». Не проиграли и даже можем победить. Несмотря на то что «вирусология» — скорее искусство, чем наука, тем не менее, победа возможна. Необходимое условие для этого — знать

врага «в лицо». И не только в его сегодняшнем обличии, но и понимать, каким он может стать завтра.

Переломный момент в развитии вирусов, на наш взгляд, уже наступил. Наиболее ярко отражает это появление вируса «I love you». Используется традиционный канал доставки, но активизация обеспечивается ментальными причинами — как не посмотреть, что тебе пишут в письме с такой темой! Вирусы, построенные по такой схеме, показались нам не менее циничными, чем мины, замаскированные под детские игрушки. Это еще одна из причин появления этой книги.

Книга, которую мы предлагаем Вашему вниманию, представляет собой попытку целенаправленного обсуждения широкого круга вопросов, связанных с компьютерной преступностью, и её основной целью является предоставление Вам набора базовых знаний и фактов, которые позволят принимать аргументированные решения для защиты собственных компьютерных систем, а также ответить на такие вопросы, как, например: «Что представляет собой компьютерная преступность?», «Каковы основные тенденции ее развития?», «От кого, откуда и когда может исходить угроза защищенности компьютерной системы?», «Как бороться с различными проявлениями компьютерной преступности?»; и им подобные.

Книга состоит из двух томов, каждый из которых, в свою очередь, содержит две части, которые иногда делятся на главы. Вот как выглядит структура книги:

Компьютерные преступления. Т. I.

Часть 1. Компьютерная преступность: возникновение, история, тенденции

Глава 1. Угроза нового типа

Глава 2. Вредоносные компьютерные программы и их типы

Часть 2. Летопись компьютерных преступлений — XX век

Приложения

Литература

Компьютерные преступления. Т. II.

Часть 1. Летопись компьютерных преступлений — XXI век

Часть 2. Компьютерный андерграунд — действия и противодействие

Глава 1. Компьютерный андерграунд и используемые им упущения в системе обеспечения информационной безопасности

Глава 2. Электронное мошенничество и его результаты

Глава 3. Основные направления и меры по обеспечению информационной безопасности компьютерных систем

Заключение

Приложения
Литература

В первом томе книги даётся общая характеристика преступлений в сфере компьютерной информации, излагаются истоки, история и тенденции развития этого явления, рассматриваются методы и способы совершения компьютерных преступлений, а также их классификация, задаются основные области, в которых необходимо безотлагательно усилить противодействие компьютерной преступности. Кроме того, в этом томе ведётся серьёзный разговор о вредоносных компьютерных программах и их авторах, а также о последствиях проникновения указанных программ в компьютер пользователя, информационную систему или сеть.

Во второй части первого тома книги излагается история возникновения и развития вредоносных компьютерных программ — «компьютерных вирусов». Эта история охватывает несколько основных этапов вирусописания, которые выделены нами в первой части тома, и повествует о возникновении новых разновидностей компьютерных вирусов, а также технологий инфицирования компьютерных систем, способов распространения и т. п. Здесь же достаточно подробно рассмотрены такие знаменитости, как сетевой «червь Морриса», и другие наиболее известные компьютерные вирусы, проявившие себя в XX веке и нанесшие большой моральный и материальный ущерб всему компьютерному и бизнес сообществу.

Во втором томе летопись компьютерных преступлений продолжается — она охватывает период от начала XXI века до наших дней. Во второй части иного тома книги читатель «близко» познакомится с так называемым «компьютерным андеграундом». Его вниманию предлагается достаточно подробное изложение истории зарождения и роста этого явления, и, в первую очередь, деятельности хакеров: кто они, каковы их цели, способы и технологии проникновения в компьютерные системы и пр.

Далее рассматриваются конкретные случаи электронного мошенничества и условия, которые создают соответствующую благоприятную среду для их совершения. Характеризуется так называемый «человеческий фактор», благодаря которому в защите компьютерных систем остаются бреши для злоумышленников, приводятся примеры спама как одного из видов наносящей всё больший ущерб деятельности, связанной с мошенничеством в информационных сетях, и в последнее время получившего высокие темпы развития во всём мире в качестве достаточно «самостоятельного» явления. Материал этого раздела излагается в виде двух, с одной стороны, различных, а с другой стороны, переплетающихся генеральных направлений. К пер-

вому направлению авторами отнесены попытки (удачные и не очень) борьбы с компьютерной преступностью с помощью нормативной правовой составляющей или, иными словами, борьбы с компьютерной преступностью законодательными методами. Здесь дан краткий анализ зарубежной и российской практики, приведены конкретные примеры по различным видам компьютерного мошенничества и уголовным делам. Ко второму направлению отнесены основные методы и средства, обеспечивающие безопасность компьютерных систем, в частности банковских. Приводятся доводы в пользу необходимости применения различных подходов в целях обеспечения защиты информации: от принятия мер предупреждения компьютерных преступлений до широкого внедрения современных аппаратно-программных комплексов.

Книга завершается заключением, которое обобщает весь материал, резюмируя исследование феномена компьютерной преступности.

В целом книга ориентирована как на специалистов, область деятельности которых непосредственно связана с разработками в области информационных технологий и средств защиты информации, так и на более широкую аудиторию читателей, включающую в себя руководителей организаций и их структурных подразделений в различных областях профессиональной деятельности (служащих государственных учреждений, менеджеров в коммерческих структурах и пр.), научных работников, сотрудников средств массовой информации, электронных изданий и правоохранительных органов, учащихся школ, колледжей и лицеев, студентов высших учебных заведений, аспирантов и слушателей курсов повышения квалификации, а также она адресована всем, кто интересуется современными информационными технологиями.

Материал книги содержит в себе обширную фактографическую основу, статистические данные и в необходимых случаях проиллюстрирован соответствующими схемами и таблицами. В приложениях изложены материалы, к вторые носят либо справочный характер, либо важны для понимания всей книги или её отдельного раздела, главы, а также познавательны и интересны для значительной части читателей, но основной текст они бы «отягощали», например, разрывая его в виде непомерно длинной врезки.

И последнее. Настоящая книга преднамеренно составлена авторами таким образом, чтобы освоение её содержания практически не требовало специальных углублённых знаний и профессиональных навыков в области высоких информационных технологий и языков программирования.

Когда книга уже была написана и находилась в редакции, среди груды

спама и вирусов, ежедневно осаждающих почтовые ящики, обратило на себя внимание письмо следующего содержания: «Здравствуйте, я белорусский вирус. По причине ужасной бедности моего создателя и низкого уровня развития технологий в нашей стране я не способен причинить какой либо вред Вашему компьютеру. Поэтому очень прошу Вас, пожалуйста, сами сотрите какой-нибудь важный для Вас файл, а потом разошлите меня по почте другим адресатам. Заранее благодарю за понимание и сотрудничество».

Нужны ли комментарии?

В. А. Конявский, С. В. Лопаткин

Часть 1

Компьютерная преступность: возникновение, история, тенденции

Глава 1. Угроза нового типа

Какие явления можно отнести к компьютерной преступности? Какие действия следует расценивать как компьютерные преступления? В чём они заключаются и чем характерны? Насколько широкие масштабы приобрела компьютерная преступность в мире? Как с ней эффективно бороться? Исчерпывающе и однозначно ответить на эти и некоторые другие вопросы крайне сложно, хотя такие попытки у нас в стране и за рубежом предпринимались и предпринимаются достаточно регулярно.

В частности, это связано с тем, что «демаркационная линия», точно и недвусмысленно отделяющая подобную деятельность от деятельности законопослушной, пока ещё однозначно не проведена. Нет и общепризнанной в мире унифицированной системы, включающей в себя формулировки конкретных условий, принципов, требований, стандартов и критериев для обозначения и подробного описания феномена компьютерной преступности, а также однозначно характеризующей, фиксирующей и регистрирующей все совершённые компьютерные преступления, процесс их подготовки и попытки осуществления. Однако можно сказать с полной уверенностью, что новые информационные технологии дали толчок не только в плане прогресса общества, но и стимулировали возникновение и развитие абсолютно новых проявлений преступности во всём мире. Более того, буквально до последнего времени считалось, что компьютерная преступность присуща лишь наиболее развитым странам, а в других государствах, в силу их слабой компьютеризации, она не может существовать и, тем более, быстро развиваться. Но, возникновение компьютерной преступности в странах с фактически полярным уровнем компьютеризации приводит нас к закономерному выводу о том, что

это явление носит поистине глобальный характер и свойственно всем государствам, даже тем, которые только вступили на путь широкой информатизации своего общества.

Хотя, безусловно, разница проявляется, например, в масштабах и изощрённости совершаемых компьютерных преступлений.

Шогди Нагиб, имеющий двойное гражданство, египетское и российское, был арестован в ноябре 2001 года в Египте за публикацию в Интернет поэмы «Кусс Уммият». Поэма, которая была написана отцом Шогди, Нагибом Шуруром, изобилует нецензурными фразами и содержит крайне жёсткую критику в адрес тех политических деятелей, которых Шурур считал виновными в поражении в шестидневной арабо-израильской войне 1967 года. В результате целых 30 лет стихи передавались из рук в руки в виде звукозаписей и рукописей, но так и не были опубликованы ни в одной из арабских стран. Размещение Шогди Нагибом такого рода материалов в Интернет никоим образом не нарушало египетские законы по той простой причине, … что в Египте на тот момент вообще отсутствовали даже зачатки законодательства, регулирующего использование Интернет. Тем не менее, представители египетских спецслужб произвели обыск в доме Нагиба, конфисковали компьютер и отправили его в полицейский участок. В конечном итоге следствие по делу было поручено службе «Адаб» – местной полиции нравов, занимающейся проститутками и им подобным контингентом.

В марте 2002 года Canal Plus обвинил NDS Group в электронном взломе систем кодирования сигналов цифрового телевидения. Принадлежащая Vivendi Universal компания коммерческого телевидения Canal Plus подала судебный иск в размере 1 млрд. долл. против подразделения News Corporation британской компании NDS Group, которая обвинялась в незаконном использовании информационных технологий конкурента и поощрении деятельности электронных взломщиков для подрыва репутации и коммерческого благополучия Canal Plus. Как утверждалось в иске, NDS выделила специальные средства и персонал для взлома программного кода, используемого при трансля-

ции цифрового канала телекомпании. Представители NDS, естественно, полностью отвергли все выдвинутые против их компании обвинения.

Как говорится в известном слогане: «Почувствуйте разницу!» Два коротких факта, которые хронологически разделяет всего лишь четыре месяца, вместе с тем, на наш взгляд, красноречиво отражают собой различие в мировоззрении, повседневных заботах и задачах двух во многом «перпендикулярных миров» нашей общей планеты Земля.

Итак, научно-техническая революция в области компьютерной техники предоставила преступникам широкие возможности в плане доступа к новым техническим средствам и технологиям, да, к тому же, в современных условиях, криминальные элементы обычно не испытывают недостатка в квалифицированных кадрах, способных эффективно использовать новейшие электронные разработки, технологические инновации, профессиональные знания и опыт для подготовки, совершения и последующей маскировки преступлений, а также активного противодействия работе правоохранительных органов. Иными словами, можно сказать, что компьютерная преступность это специфичная область деятельности криминальных структур и индивидуумов, которые жёстко противостоят законопослушной части общества, а также системам защиты любой без всякого исключения организации, использующей в своей профессиональной деятельности современные средства вычислительной техники и телекоммуникаций. Сами же компьютерные или «электронные» преступления являются, пожалуй, самым новым видом преступной деятельности среди криминальных проявлений, порождённых научно-техническим прогрессом в области инновационных технологий. В наше время компьютерная преступность вторглась даже в такую интимную сферу человеческих взаимоотношений, как личные знакомства.

Японская национальная полиция, например, была вынуждена опубликовать на эту тему специальное предупреждение под заголовком: «Знакомства через Интернет-агентства зачастую опасны для вашей жизни». Согласно приведённой в этом заявлении статистике, число преступлений, так или ина-

че связанных со знакомством через Интернет, в 2001 году увеличилось в восемь раз по сравнению с 2000 годом. Так в 2001 году в стране восходящего солнца было зафиксировано 888 преступлений подобного рода, в числе которых 6 убийств и 44 изнасилования (для сравнения в 2000 году – одно убийство и 8 изнасилований). Только за два месяца 2002 года в Японии произошло 104 преступления, относящихся к категории личных знакомств посредством использования Глобальной сети. Характерно, что около 80% жертв были несовершеннолетними, а 90% женщины. Преступления, подпадающие под статью «детская проституция и порнография», составили почти 40% от общего числа преступлений. В итоге японское правительство, учитывая очевидный рост связанных с Интернет преступлений, внесло поправки в соответствующий закон, который вступил в силу в апреле 2002 года. В новой редакции закона ужесточён контроль над различными и многочисленными «службами знакомств» по Интернет, а также по телефону и, во избежание участия несовершеннолетних, в качестве обязательной процедуры введена возрастная идентификация клиентов.

Законодательные и исполнительные, а также правоохранительные и правоприменительные органы государственной власти во всех развитых странах мира стараются адаптироваться к новым реалиям и своевременно принимать соответствующие меры по профилактике и пресечению роста компьютерной преступности[1]. Но, в целом, как отмечают специалисты в данной области знаний, процесс выработки законодательных инициатив и принятия необходимых нормативных правовых актов, судебная практика, а также теоретическая подготовка и техническая оснащённость специальных служб, призванных пресекать проявления компьютерной преступности, не успевают за темпом роста и видоизменением последней.

Вместе с тем имеют место и положительные прецеденты. Например, в июне 2000 года впервые в южнокорейской судебной практике было возбуж-

[1] Панов В. П. Сотрудничество государств в борьбе с международными уголовными преступлениями. М., 1993.

дено уголовное дело, которое опиралось лишь на электронные письма потерпевшего. Представители районной прокуратуры столицы Южной Кореи г. Сеула заявили, что они арестовали 32-летнего Ким Санг Хуна, сотрудника фирмы по производству программного обеспечения, по обвинению в нарушении закона об управлении информацией и телекоммуникациями. Сотрудники прокураторы подчеркнули, что информация, полученная по электронной почте, была хотя и не единственной по этому делу, но объективно определяющей. Свидетелем, который посылал информацию суду через Интернет, был хозяин Web-сервера, пострадавшего от действий Ким Санг Хуна. Это дело получило большой резонанс в обществе и юридических кругах Южной Кореи. Дело в том, что по имевшемуся на то время в стране уголовному законодательству в качестве показания свидетеля мог служить документ либо написанный рукой свидетеля, либо с поставленной под текстом собственноручной подписью или печатью. Понятно, что в электронном письме эти условия не были выполнены и, следовательно, не должны были расцениваться как свидетельство. Но представители прокуратуры заявили, что воспринимали показания не как юридические документы, а как «информацию в чистом виде, которая помогла проводившемуся следствию».

В марте того же 2000 года британский Интернет-провайдер понёс ответственность за размещённый в телеконференции материал. Согласно решению суда, Интернет-провайдер Demon Internet признан виновным за появление клеветнического материала в одной из телеконференций и родительскую компанию Thus обязали выплатить 24 тыс. долл. в качестве компенсации физику Лоуренсу Годфри, который содержал эту телеконференцию, а также оплатить все судебные издержки, которые превысили 300 тыс. долл. Помимо всего прочего, это судебное решение создало прецедент, так как теперь Интернет-провайдеры могут нести ответственность за материалы, публикуемые в телеконференциях, над которыми, собственно говоря, они не имеют прямого контроля. Правда компания Thus заявила, что будет добиваться изменения решения суда в пользу Интернет-провайдеров, так как они

не могут отвечать за весь огромный материал, который ежедневно появляется в Глобальной сети.

В июне 2001 года Верховный уголовный суд Германии увеличил меру пресечения за распространение детской порнографии через Интернет. Постановление федерального суда подняло максимальную меру наказания до 15 лет, так же как и меру наказания за распространение печатных материалов. Этот шаг создал прецедент для Германии, у которой ранее не было устойчивой юридической политики и практики по отношению к Глобальной сети. Заседание Верховного суда прошло после того, как государственный суд в Вюрцбурге приговорил подсудимого, признанного виновным в жестоком обращении с детьми и публикации порнографических фотографий 13-летней девочки на Web-сайте, к 4 годам тюрьмы. При этом государственный суд Вюрцбурга заявил, что действия подсудимого не подпадают под определения статей о сексуальных преступлениях, по которым обычно выносится суровое обвинение за распространение печатной детской порнографии, поскольку фотографии, технически, являются электронными данными. Верховный суд отменил это решение, отметив, что распространение данных в режиме «онлайн» ничем не отличается от распространения печатной порнографии традиционным способом.

Итак, проблема компьютерной преступности в различных её проявлениях растёт и обостряется параллельно с процессом проникновения средств вычислительной техники практически во все сферы жизнедеятельности государства и общества, и об её актуальности свидетельствует постоянно расширяющийся список всевозможных видов, способов и методов совершения компьютерных преступлений, о которых подробно мы будем говорить ниже. Причём, в роли объекта преступных посягательств может выступать как сама техника (аппаратные средства[2], периферийное оборудование[3], средства обес-

[2] Аппаратные средства – технические средства, используемые для автоматической обработки информации в процессе решения вычислительных и информационных задач.

[3] Периферийное оборудование – комплекс внешних устройств электронно-вычислительной машины не находящихся под непосредственным управлением центрального процессора.

печения связи), так и программные средства[4], банки и базы данных, для которых технические средства являются окружением, а квалификация правонарушения зависит от того, является ли компьютер только объектом посягательства или он выступает и в роли инструмента. В этих условиях, естественно, предлагаются различные меры противодействия компьютерной преступности, в том числе и довольно радикальные.

В июле 2000 года корпорация The Cyber Group Network (CGN) объявила о разработке программного обеспечения, фактически уничтожающего компьютер в случае его кражи. Суть состоит в том, что в некоторых случаях кражи жёсткого диска, содержащего некие коммерческие тайны, предпочтительней было бы дистанционно уничтожить его, чтобы не дать сделать копии конфиденциальных материалов. Корпорация CGN решила пойти именно по этому пути и разработала программно-управляемое устройство, которое может быть установлено в любой компьютер, что позволит определить его местоположение и уничтожить в случае, если он будет потерян или украден. Задача распространения продукта возложена на филиал CGN – Cyber Crime Corporation и, по словам представителей CGN, программно-аппаратная комбинация под названием «C-4 Chip», способна с точностью до полутора метров установить местоположение пропавшего системного блока или любого другого электронного устройства. Независимо от времени суток пропавший компьютер можно обнаружить более чем в 20 странах мира и хозяин компьютера, в случае необходимости, имеет возможность отследить его перемещение и уничтожить содержащуюся на дисках информацию, жёсткий диск или

[4] Программные средства – объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определённого результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения. К ним относится программное обеспечение как совокупность управляющих и обрабатывающих программ, включающих в свой состав: системные программы – операционные системы и программы технического обслуживания; прикладные программы – компьютерные программы, которые предназначены для решения задач определённого типа, например текстовые процессоры, антивирусные программы, СУБД и т. п.; инструментальные программы – системы программирования, состоящие из языков программирования и трансляторов, то есть комплексов программ, обеспечивающих автоматический перевод с алгоритмических и символических языков в машинные коды.

материнскую плату по беспроводной связи, а также может уведомить о происшествии правоохранительные органы.

В сентябре 2000 года компания Content Technologies, специализирующаяся в области защиты передаваемых данных, представила программный продукт PORNsweeper. Это программное обеспечение предназначено для корпоративного использования, и его задачей является отслеживание всей корпоративной электронной переписки для выявления прикреплённых графических файлов порнографического характера. В основе PORNsweeper лежит разработанная Content Technologies технология анализа и распознавания изображений, которая позволяет выявить порнографическое содержание в 90% случаев. Программный продукт Content Technologies получил поддержку у руководства многих корпораций, так как проведённые незадолго до его представления исследования IDC показали, что в среднем 79% служащих используют электронную почту для получения порнографических фотографий и применение PORNsweeper должно снизить корпоративный трафик за счёт пресечения использования электронной почты не по назначению, в том числе и в преступных целях.

Таким образом, в наше время, когда наступила эпоха информационных технологий и глобальных информационных сетей, компьютерная преступность стала «суровой» реальностью и, несмотря на свою весьма краткую по сравнению с «традиционной» преступностью историю, компьютерная преступность, которую зачастую относят к прибыльному и трудно наказуемому занятию, сейчас уже широко известна, распространена и вызывает серьёзную озабоченность специалистов, общественности, коммерческих структур и органов государственной власти.

Компьютерная преступность стала одним из наиболее опасных видов преступных посягательств и, в соответствии с оценками экспертов, она способна нанести ущерб, превышающий объём хищений произведений искусства во всём мире. В марте 2001 года Рональд Дик, директор Центра защиты национальной инфраструктуры (США), заявил, что онлайновый терроризм и

другие виды киберпреступности могут оказать сильное негативное воздействие на экономику США, если федеральные агентства и корпорации не будут работать более тесно в этом направлении. Он подчеркнул, что многие районы страны с «критической инфраструктурой», в которую входят электростанции, офисы федеральных организаций и жизненно важные центры компьютерных систем, могут подвергаться нападениям со стороны кого угодно – от представителей наций изгоев до обиженных работников компаний[5]. В своей речи к коллегам, многие из которых раннее служили в Федеральном бюро расследований США (ФБР США) и Министерстве обороны США, Дик также отметил, что только на текущий момент расследуется уже около 1400 дел о компьютерных преступлениях в Интернет, и их число постоянно растёт. Причём, каждую неделю появляется в среднем до 50 вредоносных компьютерных программ, каждая из которых «несёт в себе потенциальную опасность».

Подкомитет Организации объединённых наций по преступности не случайно приравнял компьютерную преступность по степени опасности к «торговле наркотиками и терроризму». Более того, ситуация, сложившаяся с темпами роста компьютерной преступности, крайне неблагоприятна во всём мире, будь то Северная (Канада, США, Мексика) или Южная Америка, Западная или Восточная Европа, Азия или Австралия, что подтверждают данные многочисленных аналитических исследований последних лет[6]. Однако

[5] В качестве подтверждения правоты Рональда Дика приведём следующий пример.

В ноябре 2001 года гражданин Австралии Витек Боден был приговорён судом г. Маручи Шайр (Квинсленд) к 2 годам тюремного заключения за взлом муниципальной компьютерной сети и ещё 29 нарушений закона. В феврале-апреле 2000 года Бодену удалось 46 раз проникнуть в городскую компьютерную систему контроля канализации, в результате чего коллекторы, собирающие фекалии, оказались до отказа переполненными, и несколько миллионов литров нечистот вылились в окружающие водоёмы. Местные реки, озёра, леса и поля оказались залиты фекалиями, и их расчистка обошлась городу в 176 тысяч австралийских долларов. Как выяснилось в ходе следствия, поступками пятидесятилетнего Бодена двигало чувство обиды на власти города за то, что его не приняли на работу в городской совет. Мстительный Боден в прошлом сам принимал участие в установке программного обеспечения для контроля над городской канализацией, так что ему не составило труда взломать муниципальную компьютерную сеть и совершить своё воистину грязное дело. Полиция арестовала Бодена, когда он в очередной раз пытался залить город фекалиями, не выходя из собственного автомобиля, где были найдены передающее устройство и компьютерное оборудование. Исследовав компьютер, эксперты обнаружили на его жёстком диске компьютерную программу, позволяющую получать доступ и полностью контролировать систему управления городской канализацией.

[6] Вместе с тем есть и определённые нюансы. Например, в феврале 2000 года в электронных изданиях появились тревожные сообщения, посвящённые безопасности Web-сайтов стран Латинской Америки, в которых говорилось о том, что компьютерные преступники оттачивают своё мастерство как раз на этих

эти исследования и содержащиеся в них статистические выкладки, как подчёркивают специалисты по борьбе с компьютерной преступностью, хотя и задают вполне определённый ориентир с точки зрения вектора развития этой проблемы, всё-таки отражают собой лишь небольшую часть от истинного количества подобных преступлений, несущих угрозу компьютерным системам и современному мировому сообществу в целом.

Тем не менее, не требует доказательств тот факт, что специалисты в любой из областей современных знаний при проведении научных исследований и постановке экспериментов не обходятся без широкого и целенаправленного использования такого инструментария, как упорядочивание наблюдаемых ими явлений и (или) событий, а также накопления и статистической обработки имеющегося в их распоряжении фактического материала. Ведь эти хорошо известные и научно обоснованные методы позволяют проникнуть в самую суть изучаемого явления и способны оказать существенную помощь в исследовании какой-либо конкретной субстанции. Именно поэтому, мы будем здесь, и далее по тексту книги, широко использовать и анализировать доступный фактографический материал, отдавая предпочтение не отдельным – не слишком характерным случаям, хотя и их постараемся не оставить без должного внимания, но систематизированному материалу, как можно более полно используя все преимущества классифицированных в соответствии с определёнными критериями понятий, данных, явлений и событий.

Искажение, утеря или хищение информации в подавляющем большинстве случаев связаны с прямой потерей материальных ценностей и финансовых средств, а любой достаточно серьёзный сбой или отказ компьютерной системы наносит ещё и моральный ущерб руководству и персоналу, про-

---

Web-сайтах. Они облюбовали серверы стран Латинской Америки для совершенствования технологий электронного взлома и их атакам подвергаются Web-сайты любого рода, от газетного портала в Колумбии до государственного сервера, посвящённого выборам в Перу. Как правило, на Web-сайтах своих жертв нарушители оставляют сообщения, содержащие ругательства, неприличные картинки, а иногда и политические заявления. Как с ними бороться, представители атакованных серверов не знали, так как Интернет в странах Латинской Америки стал развиваться сравнительно недавно и дорогие, качественные системы защиты пока не получили должного распространения. Со стороны же местных спецслужб серьёзной помощи не ожидается, так как эти органы, созданные по аналогии с отделом по борьбе с электронными преступлениями ФБР США, заняты, в основном, борьбой с отмыванием денег в Интернет.

граммистам и системным администраторам, а также урон деловой репутации фирмы в целом.

В результате широкого применения современных технологий электронных платежей и электронного документооборота, а также им подобных, нарушение компьютерными преступниками нормального режима функционирования локальных сетей может привести к отказу связанных с ними систем и сетей, что, в свою очередь, остановит работу крупных корпораций и банковских структур и, скорее всего, повлечёт за собой крайне неприятные последствия и невосполнимые потери[7]. Действующие же системы защиты информации коммерческих структур и государственных учреждений во многих случаях оказываются несостоятельными или малоэффективными в противоборстве с компьютерной преступностью из-за наличия в них многочисленных уязвимых мест.

В июне 2000 года в Австралии правительственный Web-сайт GTS, принадлежащий федеральному казначейству, оказался в центре внимания всей страны. Неизвестный, назвавшийся Келли, позвонил на радиостанцию ABC и сообщил, что на Web-сайте GTS собрал банковскую информацию о примерно 17 тысячах бизнесменов. При этом, как заявил Келли, он не взламывал защитные системы сервера GTS, так как информация лежала практически на поверхности и была доступна любому посетителю сервера. Кроме объявления о своей находке на радиостанции, Келли разослал предупреждающие письма всем тем, чью информацию он нашёл на Web-сайте GTS. В самом письме, помимо личного телефона и факса сотрудника компании, Келли поместил и всю банковскую информацию, принадлежащую тому, кому предназначалось письмо. Все эти события не на шутку встревожили получателей писем. Правда, Келли поспешил заверить, что информацию он разослал только владельцам и только в целях предупреждения. Казначейство отказалось давать какие-либо комментарии до окончания расследования по этому

[7] Шаваев А. Г. Безопасность корпораций: криминологические, уголовно-правовые и организационные проблемы. М., 1998.

делу, но некоторые эксперты поделились своим мнением по поводу защитных систем правительственного Web-сайта, назвав их «по меньшей мере, архаичными и дырявыми как решето».

В октябре 2000 года Джерри Мансур, один из лидеров голландской группы электронных взломщиков «Hit2000», заявил, что нашёл ошибку в системе безопасности Nasdaq.com и ещё трёх крупных финансовых Web-сайтов, поддержкой которых занимается MarketWatch.com. В отличие от многих своих менее сознательных коллег, он никак не использовал обнаруженную информацию, а напротив, сообщил об ошибке в системе безопасности администраторам ресурсов. В частности, электронное письмо от него получил директор технической службы CBSMarketWatch.com Дэн Шиндлер, который в ответном письме поблагодарил Мансура за честность и сообщил, что упомянутый недочёт в системе безопасности устранён. В распоряжение Джерри Мансура попал файл global.asa, содержащий пароли для доступа к центральной базе данных сервера. В результате под потенциальный удар попали серверы Nasdaq.com, CBSMarketWatch.com, BigCharts.com, и FTMarketWatch.com. Кроме того, Мансур сказал, что воспользовался написанной им самим специальной компьютерной программой и не собирается разглашать её исходные коды, чтобы она не попала в руки менее законопослушных личностей.

Итак, отдельные сферы деятельности, такие как банковские и финансовые институты, вычислительные сети и системы государственного управления требуют специальных мер безопасности данных и предъявляют повышенные, соответствующие важности решаемых задач требования к надёжности функционирования информационных систем[8].

О существовании уязвимых мест в системе обеспечения информационной безопасности могут свидетельствовать выделяемые специалистами признаки, приведённые в табл.В.1.

Таблица 1

[8] Курушин В. Д. Компьютерные преступления и информационная безопасность: Справочник. М., 1998.

Признаки
наличия уязвимых мест в системе обеспечения информационной безопасности

Формулировка признака
Не разработаны положения о защите информации или они не соблюдаются и не назначен ответственный за информационную безопасность
Пароли пишутся на компьютерных терминалах, помещаются в общедоступные места, ими делятся с другими или они появляются на дисплее во время ввода
Удалённые терминалы и компьютеры оставляются без присмотра в рабочие и нерабочие часы, данные отображаются на дисплеях, оставленных без присмотра
Не существует ограничений на доступ к информации, или на характер её использования, все пользователи имеют доступ ко всей информации и могут использовать все функции системы
Не ведутся системные журналы и не хранится информация о том, кто, когда, как и в каких целях использует компьютер
Отсутствует документация или она не позволяет понимать получаемые отчёты и формулы, по которым рассчитываются результаты, модифицировать программы, готовить данные для ввода, исправлять ошибки, производить оценку мер защиты, и понимать сами данные – их источники, формат хранения, взаимосвязи между ними
Делаются многочисленные попытки войти в систему с неправильными паролями
Вводимые данные не проверяются на корректность и точность, или при их проверке много данных отвергается из-за ошибок в них, требуется делать много исправлений в данных, не ведутся записи в журналах об отвергнутых транзакциях
Имеют место приносящие большие убытки случаи выхода системы из строя
Не производится анализ информации, обрабатываемой в компьютере, с целью определения необходимого для неё уровня безопасности
Мало внимания уделяется информационной безопасности и, хотя политика безопасности существует, большинство пользователей считает, что на самом деле она не нужна
Изменения в компьютерные программы вносятся без предварительного уведомления и утверждения руководством
Изменения в аппаратные средства вносятся без предварительного уведомления и утверждения руководством
Не применяются, неправильно подобраны и установлены (или установлены устаревшие) программные средства защиты
Не применяются, неправильно выбраны и установлены (или установлены устаревшие) аппаратные средства защиты

Несмотря на то что многие из совершаемых компьютерных преступлений осуществляются по известным «сценариям», процесс совершенствования информационных технологий в целом и развитие компьютерных сетей в частности, постоянно даёт в руки электронным правонарушителям новые и всё более широкие технико-технологические возможности и аппаратно-

программные средства для их совершения[9]. Преступные группировки в настоящее время используют такие технические средства как, например, электронные стетоскопы, которые позволяют прослушивать даже армированные бетонные и кирпичные стены около метра толщиной. Специальная техника может снимать информацию на значительном расстоянии от объекта, улавливая акустические, электромагнитные и другие излучения, передаваемые в окружающую среду строительными конструкциями зданий и сооружений, с помощью лазерных устройств можно без особых проблем получить необходимые данные через стёкла окон. Существуют специальные устройства, способные давать точное изображение людей и отчётливую запись конфиденциальных переговоров, ведущихся за закрытыми окнами с металлическими решётками на них и плотно задёрнутыми шторами[10]. Практически во всём мире в поте лица трудятся целые артели «Кулибиных», способных поставить и ставящих на поток производство фальшивых CD-ROM и электронных карточек, качество которых если и не выше, то и не ниже настоящих[11].

В силу указанных причин становится понятно, почему в рамках мероприятий соответствующих структур Организации объединённых наций регулярно проводятся семинары и конференции по профилактике и пресечению компьютерной преступности, главной задачей которых декларируется целенаправленный поиск путей противодействия данному явлению – как на международном, так и на региональном, национальном, а также корпоративном уровнях. В ходе работы указанных семинаров и конференций, прежде всего, вырабатываются меры жёсткого противодействия «электронному» виду криминальных деяний, а также уделяется должное внимание разработке универ-

[9] Возьмите, к примеру, «электронный взлом» банковской системы, который при наличии профессиональных навыков и определённой информации осуществить намного безопаснее, прибыльнее и комфортнее, чем орудовать при помощи газовой горелки, фомки, набора отмычек, когорты не всегда надёжных подручных и информаторов, да к тому же в кожаных перчатках, в темноте и в условиях жёстких ограничений по времени.

[10] Современный промышленный шпионаж // Борьба с преступностью за рубежом. М., 1995. № 11. Как хранят секреты в Америке // Новости разведки и контрразведки. 1994. № 13.

[11] Ривкин К. Преступления с кредитными карточками //Экономика и жизнь. 1997. № 2.

сально применимых стандартов и нормативов, гарантирующих надёжное использование компьютерных систем и средств телекоммуникаций.

Кроме того, эксперты Организации объединённых наций считают общепризнанным фактом, что для выработки всесторонней стратегии по профилактике и борьбе с компьютерной преступностью необходим согласованный план действий, который должен включать в себя взаимоувязанный комплекс мер на различных уровнях их дальнейшей реализации, табл. В. 2.

Таблица 2

Комплекс мер
в целях осуществления профилактики и ведения борьбы с компьютерной преступностью

Уровень реализации	Краткая характеристика
Международное сотрудничество	Международное сотрудничество, направленное на унификацию законодательных актов, развитие международных стандартов и координацию действий органов уголовной юстиции.
Правительственные меры	Действия правительства на государственном уровне, направленные на совершенствование национального уголовного законодательства, а там, где это необходимо, и промышленного производства средств противодействия компьютерным преступлениям.
Неправительственные меры	Выработка программы инициатив по внедрению принципов ответственности в экономике и промышленности, стандартов профессиональной квалификации, технических и процедурных норм, а также этических установок и кодексов поведения.

Примером озабоченности крупного бизнеса ростом компьютерной преступности может служить тот факт, что в августе 2000 года главы высокотехнологичных компаний, в частности, IBM, Microsoft и Oracle, встретились с представителями государственных структур в Белом доме (Вашингтон, США), чтобы обсудить вопросы, касающиеся необходимости внедрения определённых стандартов безопасности для ведения электронной коммерции по модели B2B[12]. Дело в том, что компаниям, участвующим в торгах на элек-

[12] Обозначение модели ведения электронной коммерции составляется из наименований продавца и покупателя. В данном случае, по-английски, «Business to Business» или, по-русски, «Предприятие–Предприятие». Сокращённое обозначение модели строится из начальных букв английских названий покупателя и продавца, между которыми стоит цифра 2. В данном случае: B2B. Наибольшее распространение в

тронных торговых площадках, приходится открывать часть своих внутренних ресурсов для онлайновых площадок, при этом они часто подключают свои сети к этим площадкам так, что их конкуренты или сторонние компании получают возможность добывать конфиденциальную информацию напрямую из компьютеров этих компаний. Так, например, поставщик, узнав, что какая-то компания в настоящее время испытывает дефицит в каком-либо сырье, может резко повысить цены на него даже до того момента, когда заказ будет реально размещён на электронной торговой площадке, что может негативным образом сказываться на отношении к ведению электронной коммерции в целом.

По итогам указанной встречи был организован комитет, который должен заниматься исключительно проблемой внедрения стандартов безопасности для ведения электронной коммерции по модели B2B. И, несмотря на то, что компании не изъявили особого желания поддерживать контроль государства в этой сфере деятельности, необходимость её регулирования они признали.

Кроме того, была высказана необходимость подключения иностранных государственных и частных структур к процессу становления хотя бы минимальных стандартов безопасности. Первые шаги было намечено сделать по примеру Visa International, потребовавшей от двадцати одной тысячи своих партнёров использования минимальных средств безопасности: шифрования хранимых и передаваемых данных, модернизации операционных систем и приложений, а также широкого использования современных аппаратных средств защиты вычислительной техники от компьютерных преступников.

странах Северной Америки, Западной Европы и у нас в России в настоящее время получили следующие модели ведения электронной коммерции: B2B – «Предприятие–Предприятие», B2C – «Предприятие-Потребитель», C2C – «Потребитель–Потребитель», C2B – «Потребитель–Предприятие».

Модель B2B появилась за рубежом более тридцати лет тому назад и успешно развивается коммерческими структурами. В «идеальном» случае ведение электронной коммерции по модели B2B предполагает полностью автоматизированное взаимодействие предприятий или организаций в ходе осуществления ими предпринимательской деятельности.

Подробно об электронной коммерции и моделях её ведения можно прочитать в книге: Волокитин А. В., Лопаткин С. В. Электронная коммерция. Учебное пособие для служащих государственных организаций и коммерческих фирм // Под общей редакцией Л. Д. Реймана М., 2002.

Естественно, что повышение показателя результативности борьбы с компьютерной преступностью является предметом пристального внимания и такой известной международной организации, как Интерпол, на ассамблеях которой регулярно рассматриваются важнейшие вопросы борьбы с компьютерными преступлениями, осуществляется координация деятельности национальных правоохранительных органов, а также принимаются соответствующие резолюции, подобные тем, что приведены в табл. В. 3.

Таблица 3

Пример
резолюций, принимаемых Генеральной Ассамблеей Интерпола в целях усиления борьбы с компьютерной преступностью

№ резолюции	Вопрос	Принятая формулировка
AGN/64/P.RES/17	Универсальная система классификации фальшивых платёжных документов	64-я сессия Генеральной Ассамблеи Интерпола рекомендует Рабочей группе продолжить работу по универсальной системе классификации фальшивых платёжных документов путём: 1. Совершенствования индикативной системы фальшивых платёжных документов. 2. Создания международной базы данных платёжных документов и изучения возможности создания центральной международной информационной базы и центральной справочной библиотеки фальшивых платёжных документов.
AGN/64/P.RES/18	Мошенничество с платёжными документами	64-я сессия Генеральной Ассамблеи Интерпола рекомендует странам-членам Интерпола, где платёжные документы используются в качестве расчётного средства, пересмотреть свою законодательную базу и убедиться, что в ней содержатся соответствующие положения для всех видов мошенничества с платёжными документами. В частности, Генеральный секретариат должен убедить правительственные органы указанных стран-членов Интерпола сделать всё возможное для введения в свою законодательную базу в качестве уголовного преступления подделку или использование фальшивых платёжных документов, неправомочное использование информации, полученной обманным путём о банковских и других счетах, а также участие в мошеннических сделках.
AGN/64/P.RES/19	Компьютерно-ориентированная преступность	64-я сессия Генеральной Ассамблеи Интерпола рекомендует: 1. Решать проблему борьбы с преступностью, связанной с незаконным использованием компьютеров, с одинаковой интенсивностью в африканском, американском, европейском и азиатском регионах и в каждой стране-члене Интерпола в этих регионах, – с оказанием возможной помощи Генеральным секретариатом на региональном уровне.

№ резолюции	Вопрос	Принятая формулировка
		2. Создать Координационный комитет в составе группы экспертов из различных регионов для координации и реализации всех региональных инициатив, стимулирования единообразия в методах расследования международных компьютерных преступлений. 3. Поручить Генеральному секретариату подготовку в кратчайшие сроки соответствующих предложений по достижению поставленных задач.

Кстати сказать, уже на первой Международной конференции Интерпола по вопросам компьютерной преступности (апрель 1995 года), в работе которой приняли участие представители правоохранительных органов и специальных служб, служб безопасности банков, а также специалисты в сфере информатизации из сорока девяти стран, отмечалось, что факты совершения международных компьютерных преступлений получают всё большее распространение и особую озабоченность вызывает резкий рост мошенничества с использованием средств вычислительной техники. Более того, так как во многих странах мира преступниками в криминальных целях всё чаще применяются самые современные информационные технологии, давно назрела настоятельная необходимость постоянного и углублённого изучения этого негативного явления. Ведь в результате использования этих технологий совершаемые с их помощью компьютерные преступления всё труднее поддаются расследованию и раскрытию.

Кроме того, на конференции было отмечено, что всё в больших масштабах средства вычислительной техники используются компьютерными преступниками для несанкционированного доступа в международные информационные системы и сети в целях кражи информации, отмывания преступно нажитых средств и распространения вредоносных компьютерных программ. В связи с этим было рекомендовано интенсифицировать процесс разработки международных процедур по оказанию помощи при расследовании таких преступлений и создать соответствующий координирующий орган в рамках Интерпола. В итоговых документах конференции также подчёрки-

валось, что для правоохранительных органов многих стран проблема компьютерной преступности является новым видом проявления международной криминальной деятельности, и их борьба с ней далеко не всегда оказывается эффективной, в том числе и по той причине, что сообщения об этих преступлениях крайне фрагментарны.

§1. Предмет преступного посягательства, уголовно-правовой аспект компьютерной преступности и источник угрозы

В настоящее время, в качестве общего знаменателя бытует мнение, что полную картину компьютерной преступности в мире получить невозможно, и эту позицию вполне разделяет, к примеру, ФБР США, по оценке которого только около 30% от общего числа обнаруженных компьютерных преступлений доводится до сведения официальных органов, призванных бороться с этим видом преступности.

В 1996 году ФБР США в целях оценки масштабности компьютерных преступлений и принимаемых для их предотвращения мер был проведён опрос более четырёхсот компаний, итоговые материалы которого достаточно широко известны в профессиональных кругах специалистов по борьбе с компьютерной преступностью, в том числе и у нас в России. Среди других сведений, которые содержались в достаточно объёмном итоговом отчёте, приводились данные, подтверждающие, что информационные системы отвечавших на вопрос находятся под угрозой электронных нападений со стороны компьютерных преступников, так как в течение года 42% от общего числа компаний испытали на себе ту или иную форму несанкционированного вмешательства в штатную работу или другое несанкционированное использование их компьютерных систем.

Причём, более 50% из тех компаний, которые испытали электронные нападения или проводили анализ работы собственных систем, указали на то обстоятельство, что ими были вскрыты факты несанкционированных действий со стороны собственного персонала. Столько же респондентов рассматривают конкурентов как вероятный источник нападений (от подслуши-

вания до проникновения в информационные и телекоммуникационные системы) и считают, что похищенная информация может использоваться конкурентами. Кроме того, свыше 50% из числа ответивших компаний не имели плана действий на случай электронного нападения на их компьютерные сети; свыше 60% не имели стратегии сохранения доказательств для дальнейшего судебного рассмотрения уголовных или гражданских дел; свыше 70% респондентов не имели устройств, предупреждающих о вторжении в их компьютерные системы; свыше 70% назвали в качестве основной причины отказа от обращения в правоохранительные органы опасение антирекламы и лишь 17% указали, что они уведомят правоохранительные органы в случаях нападения на их компьютерные системы.

В ходе последующего исследования ФБР США «Computer Crime and Security Survey» в 2002 году эксперты пришли к выводу, что число киберпреступлений, совершаемых на территории США, продолжает неуклонно расти, однако их учёт и меры противодействия сильно затруднены тем, что многие жертвы сетевых преступников предпочитают не обращаться в правоохранительные органы. По данным отчёта 90% респондентов признали, что в течение последних 12 месяцев им приходилось сталкиваться с фактами правонарушений, осуществляемых в онлайн. При этом заявление в полицию подали лишь 34% из них. Несмотря на то, что это очень мало, как признают сотрудники ФБР США, динамика положительная. Ведь в 2000 году этот показатель составлял не более 25%, а в 1996 году, как мы указывали выше, тот же показатель был на уровне 17%. «В Сети совершается гораздо большее число преступлений, чем в этом готовы признаться своим клиентам и инвесторам ведущие корпорации», – полагает Патрис Рапалуш, глава подразделения ФБР США, специализирующегося на предотвращении вторжений в компьютерные системы.

По данным недавно проведённого университетом штата Мичиган исследования 98,6% фирм США становятся жертвами компьютерных преступлений, причём более 43,3% из 200 опрошенных в ходе исследования компа-

ний страдали от подобных правонарушений более 25 раз. Наиболее распространёнными формами компьютерных преступлений признаны непристойности и компьютерное хулиганство, а также преднамеренное распространение вредоносных компьютерных программ и электронное мошенничество[13].

Например, в январе 2001 года в Париже был арестован очередной сетевой извращенец 21-летний француз Гийом М., которого подозревали в распространении посредством Интернет 10 тысяч детских порнографических фотографий. В период с июня по июль 2000 года он занимался снабжением специализированных Web-сайтов незаконными изображениями, сообщала французская полиция. Подозреваемый делал это в рабочее время, со своего рабочего места в компьютерной компании, расположенной в пригороде Парижа, а на его домашнем компьютере полиция обнаружила 30 тысяч порнографических фотографий, собранных им в Интернет.

Многие согласны с тем, что родители должны в какой-то мере отслеживать и контролировать деятельность своих детей в Интернет, но судебные власти штата Иллинойс (США) решили пойти дальше. Теперь по решению суда родители могут подвергаться судебному преследованию за деятельность своих «отпрысков» в Глобальной сети. Судья Вард С. Арнольд в декабре 2000 года вынес решение о возможности возбуждения судебного дела против отца подростка, поместившего на порнографическом Web-сайте сгенерированную на компьютере фотографию своей одноклассницы. Отца шутника ждал иск о возмещении морального ущерба, и его сумма составила 50 тысяч долларов.

В апреле 2000 года китайская полиция в очередной раз проявила суровость в отношении нарушителей правил поведения в киберпространстве. На этот раз в немилость попали «шутники» с Web-сайта www.21f.net, которые разослали около двух тысяч писем, где утверждалось, что вместе с письмом адресаты получили неустранимый компьютерный вирус, и помочь им может

[13] Fraud protection and detection series: Counterfeit Securities. Check Fraud, Letters of Credit Fraud, Account-Opening Fraud, Cheque Kiting, Advanced Fee Fraud, Money Transfer; Bank Administration Institute, Rolling Meadows, Illinois, 2002.

только регулярное посещение упомянутого Web-сайта. Вируса в письме не было и из текста было ясно, что это розыгрыш, однако полиция заявила, что в киберпространстве таким шуткам и электронным хулиганам не место и закрыла Web-сайт на неопределённое время.

14 сентября 2001 года 35-летний сотрудник IBM из Новой Зеландии был направлен на психиатрическое освидетельствование после обвинения в «почтовом терроризме». Он был арестован вечером 12 сентября в сингапурском аэропорту Чанжи, где находился в ожидании рейса авиакомпании Singapore Airlines в г. Йоханнесбург (ЮАР). Утром 12 сентября сотрудник IBM сообщил по электронной почте о бомбе, якобы заложенной на борту самолета Boeing 747-400, вылетающего рейсом SQ 422, которым и должен был отправиться сам. В результате ложного сообщения рейс был отложен на шесть часов (с 4:20 дня на 10:30 вечера), а повысившая бдительность полиция вскоре арестовала электронного хулигана. IBM подтвердила, что неудавшийся «шутник» действительно является её сотрудником, осудила его действия и пообещала всячески содействовать полиции в расследовании. В частности, сингапурское отделение корпорации помогло отследить, откуда было отправлено сообщение. Наказание за данное компьютерное преступление предусматривает до 7 лет тюремного заключения и (или) штраф до 29 тысяч долларов.

В феврале 2000 года компания Adobe Systems Co., Ltd. сделала заявление, что демонстрационный CD-ROM, который распространялся на выставке MacWorld Expo/Tokyo 2000, содержит записанные на него неизвестным злоумышленником компьютерные вирусы MBDF.a и MBDF.b. Заражённым оказался программный продукт Premiere 5.0 с диска Adobe Dynamic Media Solutions & Product Sampler vol.1. Каждый участник семинара Adobe и каждый, кто правильно отвечал на вопросы викторины, получал такой диск в подарок. 18 февраля компания прекратила распространение диска и начала мероприятия по оповещению всех обладателей CD-ROM и выявлению компьютерного преступника.

Только за первые шесть месяцев 2000 года в Австралии в рамках политики в области цензуры было закрыто 93 Web-сайта (из 201 Web-сайта на которые поступили жалобы). Специальная организация, целью которой является рассмотрение жалоб населения, начала функционировать 1 января 2000 года, а уже 5 сентября Ричард Алстон, министр информационных технологий и связи Австралии, обнародовал доклад о результатах её деятельности в первом полугодии. В докладе указывалось, что большинство Web-сайтов, на которые поступили жалобы, действительно содержали оскорбительную и нелегальную информацию. «Около 80% случаев закрытия Web-сайтов в Австралии были связаны с непристойным изображением детей и несовершеннолетних, включая извращения по отношению к детям, – заявил Алстон, – австралийские органы власти расследовали 197 из 201 поступивших жалоб, но доведено до конца только 160 дел. Из них в 93 случаях содержание Web-сайта было признано запрещённым, ещё 44 дела было передано в общегосударственную и местную полицию. Кроме того, австралийская полиция получила 51 заявление на расследование работы Web-сайтов в других странах».

В результате своей деятельности компьютерные преступники присваивают деньги с кредитных карточек и информацию, которая циркулирует в сетях, различные сведения, хранящиеся на не принадлежащих им компьютерах, посягая на информацию, имеющую сугубо конфиденциальный характер[14]. Например, в сентябре 2000 года Web-сайт Western Union[15] оставался неработоспособным в течение пяти дней после того, как компьютерным преступникам удалось взломать защиту и похитить конфиденциальную кредитную и дебетовую информацию о 15,7 тысячи клиентов – держателей кредитных карт этой компании, пользующихся услугами Western Union для перевода своих средств через Интернет. Причём задачу компьютерным преступникам облегчили сами сотрудники компании Western Union, оставив незащищённой

[14] Electronic fund transfer systems fraud, Paladin Press, Boulder, Colorado, 1989.

[15] Western Union представляет собой часть базирующейся в г. Атланта (США) корпорации First Data – гиганта среди фирм, осуществляющих электронные платежи. Среди прочих услуг, Western Union предоставляет, например, платёжный Интернет-сервис «person-to-person» – MoneyZap. Эта услуга позволяет клиентам отправлять и получать платежи, делать запросы о переводах через Интернет, и предназначена для всех, кто имеет адрес электронной почты, а также текущий счёт или кредитную карту.

компьютерную систему во время проведения рутинных профилактических работ, что официально подтвердили представители самой компании. Во избежание мошенничества Western Union уведомила Visa и MasterCard о номерах украденных кредитных карт, а также фирмы, принимающие эти кредитки и самих держателей карт. Представитель Western Union Питер Зиверц, утверждал, что после восстановления Web-сайта компания полностью уверена в его безопасности, так как для этого предприняты «все необходимые действия, какие только можно».

В августе 2000 года, человек, который по сообщению официальных лиц, был конфиденциальным консультантом ФБР США по вопросам компьютерной преступности (!), обвинён в незаконном проникновении в правительственные компьютеры с целью хищения конфиденциальной информации. Во время предварительного слушания 27-летний Макс Рей Батлер, также известный как Макс Вижен, был обвинён в незаконном доступе в защищённые компьютеры и нанесении им ущерба. В марте Батлер уже обвинялся в электронном взломе и нанесении вреда сотням компьютеров, а также в попытке выманить персональные пароли у 477 пользователей калифорнийского Интернет-провайдера Aimnet. В совокупности совершённые Максом Вижеком компьютерные преступления квалифицируются как уголовные и предполагают отбытие пятилетнего заключения, а также уплату штрафа в размере 250 тыс. долл.

По материалам уже упоминавшегося отчёта Мичиганского университета средняя сумма, похищаемая в каждом отдельно взятом случае электронного мошенничества, составляет более 500 тысяч долларов, тогда как «обычный» профессиональный преступник присваивает в среднем лишь около 24 тысяч долларов. Заметим, что, в соответствии со статистическими данными этого исследования, большинство случаев электронных хищений и неправомерного использования служебной информации в электронной форме приходится не на сторонних злоумышленников, а на штатных, контрактных, а также бывших сотрудников фирм. Тем не менее, огульное обвинение бывших

сотрудников в преступных намерениях не допустимо, что и подтвердило в августе 2000 года судебное разбирательство, в ходе которого суд не удовлетворил требование Lucent Technologies о запрете бывшим сотрудникам работать на конкурентов. Таким образом, Lucent Technologies потерпела неудачу в попытке запрета десяти своим бывшим сотрудникам работать на компанию Cisco Systems. В Lucent Technologies они занимались созданием оптических сетевых DWDM систем и, перейдя в Cisco Systems, они начали работу над аналогичной технологией, что не могло не вызвать недовольства у руководства Lucent Technologies. Однако суд посчитал, что одного предположения о возможном использовании в интересах конкурента служебной информации в электронной форме явно недостаточно для того, чтобы запретить им работу в конкурирующей фирме.

Но, оказывается, слишком честным сотрудником быть не всегда безопасно. В августе 2000 года жюри суда г. Сан-Франциско (США) постановило выплатить 2,66 млн. долларов бывшему вице-президенту Oracle Corporation. По словам Сэнди Баррата, причиной её увольнения с поста вице-президента послужило решение об информировании своего непосредственного руководства о возможном нелегальном использовании Oracle Corporation модулей программного обеспечения R/3, принадлежащего немецкой компании SAP. Она была уволена уже на следующий день после того, как сообщила об этом своему руководителю, но суд высшей инстанции признал увольнение г-жи Баррата незаконным.

Впрочем, в отчёте отмечен и рост доли «вольных электронных взломщиков», а также организованных преступных групп[16]. В качестве общего вывода специалисты предсказывают дальнейший рост компьютерных преступлений, что увязывается ими с бумом распространения домашних персональных компьютеров, а также компьютеров для сферы малого бизнеса. В связи с

[16] Интересно отметить, что уже в самом начале процесса срастания традиционной организованной уголовной преступности с компьютерной преступностью, – зарождение которой в западных странах приходится на шестидесятые годы прошлого столетия, изначально объектом пристального внимания этого «союза» стала не наличность банков, например, а информация, содержащаяся в электронно-вычислительных машинах.

этим эксперты по информационной безопасности призывают целенаправленно заняться обучением сотрудников фирм[17], усилить персональную ответственность, развернуть систему пропускного контроля, установить в офисах телекамеры, дублировать и шифровать важную информацию, чаще менять пароли и т. п. Необходимо также обращать внимание на неавторизованное использование компьютерного времени и несанкционированные попытки доступа к файлам данных, кражи частей компьютеров и программ, физическое разрушение оборудования, уничтожение данных или программ, неавторизованное владение дискетами, магнитными лентами, листингами компьютерных программ или распечатками, содержащими персональные данные, разглашение которых представляет собой угрозу нарушения гражданских прав.

Кстати, выступая в январе 2000 года на дискуссионной панели Washington DC Chapter, ассистент общего совещания ФБР США Стивен Чабински заявил, что угрозу нарушения гражданских прав представляет не его ведомство, а частные компании и системные администраторы, имеющие доступ ко всей частной информации, проходящей по сетям. Чабински заявил также, что развитие технологий делает необходимым наделение ФБР США особыми полномочиями, подобно принятому в 1994 году Digital Telephony Law, предписывающему телефонным компаниям открыть специальные возможности для прослушивания телефонов в случае судебных решений по этому поводу. Он также заявил, что особую угрозу конфиденциальности информации представляют собой так называемый «кибертерроризм» и электронные взломщики, способные проникнуть в частные компьютерные системы.

Продолжая тему, отметим, что в феврале того же года Федеральный апелляционный суд США оставил за Центральным разведывательным управлением (ЦРУ) США право контролировать то, как используют Интернет его

[17] В США студенты, изучающие и работающие над системами информационной безопасности, получают специальные стипендии. Например, Национальный научный фонд США в 2000 году опубликовал документ, в котором говорится о поддержке Federal Cyber Services Program, программы правительства, посвящённой информационной безопасности. С 2001 года фонд поддерживает программу выдачей специальных субсидий колледжам и университетам, которые, в свою очередь, выплачивают из этих денег стипендии самым способным студентам. По программе научного фонда также возможно трудоустройство студентов в федеральных агентствах после окончания вузов.

служащие[18]. Тем более что такой контроль дал результаты: было установлено, что один из сотрудников ЦРУ США в рабочее время занимается перекачиванием детской порнографии. Затем, в течение 2000 года, руководство ЦРУ провело внутреннее расследование по поводу деятельности некоторых сотрудников управления, которые создали в его внутренней сети секретный чат, который использовался для неформального общения и содержал шутки и комментарии сексуального характера. В общение в чате было вовлечено около 160 сотрудников, впрочем, представители самого ЦРУ США заявили, что данная цифра несколько завышена, и многие из них появлялись в чате только один раз и больше туда не возвращались. По словам представителя ЦРУ США Билла Хэрлоу, данный инцидент является типичным случаем злоупотребления компьютерным оборудованием, но секретная информация при этом не подвергалась опасности. Тем не менее, представители управления не исключали, что в результате расследования некоторые сотрудники могут лишиться работы. И, действительно, через несколько дней после этого заявления за участие в секретном эротическом чате четыре сотрудника было уволено, восемнадцати объявили выговор, двоих офицеров понизили в звании, а 79 сотрудников получили предупреждение. Секретный чат существовал на компьютерах ЦРУ США достаточно долго, и доступ к нему получали только те, кого пригласили другие участники, причём вопрос о приёме нового члена решался при помощи процедуры общего голосования.

Согласно отчёту Группы по исследованию проблем компьютерной безопасности университета Carnegie Mellon, выпущенному в июне 2000 года, основной угрозой компьютерной безопасности корпораций являются сотрудники этих корпораций, пользующиеся различными приложениями, позволяющими мгновенно обмениваться сообщениями в Интернет (IRC-клиенты, ISQ, Instant Messenger и т. д.). Как советуют компьютерные эксперты, компаниям лучше ограничить использование таких приложений, или запретить со-

[18] Контроль над работой сотрудников осуществляет один из отделов (Foreign Bureau of Information Services) ЦРУ США и подобного рода работой он начал заниматься ещё в 1998 году, когда ему был поручен «электронный аудит» компьютеров служащих. Аудит заключается в просмотре электронной почты служащих ЦРУ и слежении за тем, какие Web-сайты посещают сотрудники в рабочее время.

трудникам пользоваться ими вообще, если нет настоятельной служебной необходимости в подобных программах. «Пользователи должны помнить, что программное обеспечение для чата не предназначено для безопасного обмена информацией» и вся информация, проходящая по IRC-каналам, может быть относительно легко отслежена и перехвачена компьютерными преступниками. Тем более что существуют специальные утилиты, с помощью которых даже подросток может полностью отследить трафик обмена информацией. Кроме того, недостатки в программном обеспечении чатов могут использоваться и успешно используются для запуска в Интернет разрушительных вредоносных компьютерных программ.

Например, в марте 2002 года американские военные были вынуждены провести срочное внутреннее расследование, а также проверку всех собственных Windows систем на предмет наличия нелегально установленных программ слежения. Согласно предупреждению, распространённому 6 марта специальной группой ВМФ США по контролю над компьютерными происшествиями (Navy's Computer Incident Response Team – NAVCIRT), все сетевые администраторы должны проверить Windows системы на предмет наличия популярной коммерческой программы слежения и удалённого администрирования RemotelyAnywhere. Подобное предупреждение, копия которого попала в сетевой журнал Newsbytes, через неделю было распространено также и во всех частях сухопутных войск. Свои комментарии происшествию дал представитель компании Binary Research International, которая разрабатывает и распространяет программу RemotelyAnywhere. «Мы тесно сотрудничаем с Министерством обороны США и делаем всё возможное для того, чтобы найти компьютерных злоумышленников», – заявил пресс-секретарь компании Джим Сзопински. По всей видимости, злоумышленники использовали незаконно зарегистрированную или «взломанную» версию RemotelyAnywhere, выбрав эту коммерчески распространяемую программу, а не одну из похожих по функциям свободно доступных утилит, вследствие того, что её наличие в системе не отслеживалось имеющимися на тот момент

антивирусными пакетами. Отметим, что RemotelyAnywhere позволяет удалённым пользователям получить через Интернет доступ ко всем файлам на компьютере, используя при этом только Web-браузер.

Особый акцент можно сделать на угрозе, исходящей от внутренних пользователей: по ряду оценок 83% случаев несанкционированного доступа связано с действиями сотрудников компаний. Нужно отметить, что в США компании тратят огромные средства на безопасность корпоративных сетей, корпорация «Боинг», например, ассигнует на эти цели до 500 млн. долларов в год.

По данным насчитывающей порядка 10 тысяч членов AMA (Американская ассоциация менеджмента) на июль 2000 года: 45% компаний в США отслеживали поведение своих сотрудников в Интернет; 55% из обследованных компаний использовали различные фильтры для предотвращения несанкционированного использования электронных коммуникаций; 29% блокировали доступ к Web-сайтам, которые, по мнению руководства компании, не имеют отношения к работе сотрудников. Согласно исследованиям компании Vault.com, проведённому в тоже время, что и исследование AMA, 90% работников посещали не относящиеся к работе Web-сайты и 54% работодателей принимали меры противодействия этому. Только 10% работников не получали в рабочее время личные электронные сообщения.

В августе 2000 года компания Dow Chemical объявила об увольнении 24 служащих, которые были уличены в хранении порнографических фотографий и картинок, а также обмене ими по электронной почте. Менее жёсткие административные санкции были применены ещё к 235 служащим Dow Chemical (причём, месяцем раньше компания уже уволила 50 и наказала 200 служащих по этой же причине). Инцидент произошел на одном из заводов компании в Техасе. Системные администраторы начали мониторинг электронной почты сотрудников после того, как серверы компании начали испытывать перегрузки. Некоторые из пострадавших служащих заявили, что ме-

ры, подобные принятым руководством Dow Chemical, являются незаконными.

В апреле 2001 года был опубликован специальный обзор, озаглавленный «The Web@Work Survey 2001», который был составлен Taylor Nelson Sofres по заказу компании Websense, занимающейся разработкой программного обеспечения, призванного покончить с проблемой нецелевого использования Интернет в рабочее время. Главный вывод обзора можно кратко сформулировать следующим образом: «кибербездельник – угроза для благополучия компании». В соответствии с его данными более половины менеджеров европейских компаний не предпринимают ровно никаких попыток ограничить нецелевое использование их сотрудниками доступа в Глобальную сеть, в то время как две трети сотрудников компаний не видят в подобном использовании Интернет ничего предосудительного. Исследование показало, что из всех европейцев, британские работодатели наиболее склонны принимать административные меры для поддержания трудовой дисциплины. И неудивительно, согласно данным «The Web@Work Survey 2001» потери небольшой компании, предоставляющей своим сотрудникам неограниченный доступ по коммутируемым линиям, могут составить около 50 тысяч фунтов стерлингов в год, учитывая и снижение производительности труда. Более крупные компании могут потерять десятки миллионов фунтов стерлингов только на неправильном расходе рабочего времени.

Интересно, что мэрия Челябинска в январе 2003 года приняла специальное постановление, запрещающее сотрудникам задерживаться на рабочем месте дольше положенного времени. Об этом сообщил руководитель аппарата администрации. Такое необычное для России решение объясняется вполне закономерным желанием администрации сэкономить деньги налогоплательщиков, уходящие на оплату Интернет. По словам Главы администрации Челябинска, внеурочное присутствие на рабочем месте сотрудников вызвано отнюдь не повышенным рвением к работе, а лишь желанием «на дармовщинку» воспользоваться Интернет в личных целях. Теперь челябинские чинов-

ники могут оставаться на работе дольше положенного только по специальному разрешению руководства, а за невыполнение предписания могут быть уволены.

Топ менеджеры IT-компаний, уделяющие серьёзное внимание обеспечению сетевой безопасности своих систем, очень часто недооценивают того ущерба, который может быть нанесён их бизнесу собственными же сотрудниками. К такому выводу пришла консалтинговая компания KPMG, в рамках исследования которой в ноябре 2001 года было изучено мнение 1200 руководителей крупнейших компаний, работающих в сфере информационных технологий. 79% опрошенных выразили уверенность в том, что единственной функцией системы безопасности является защита сервисов электронной коммерции от несанкционированного вмешательства извне. При этом регулярный аудит систем безопасности проводят только 35% компаний, а сотрудники, способные выступить в роли экспертов по организации юридического процесса в случае причинения ущерба, работают только в 22% компаний. 62% руководителей заявили, что они проводят серьёзные проверки сотрудников, которых они нанимают на должности, связанные с обеспечением безопасности, тем не менее, как свидетельствует статистика, большинство взломов информационных систем происходит именно «изнутри» организаций. При этом 83% пострадавших компаний, как правило, не предпринимают никаких юридических действий с целью компенсации ущерба.

Рассерженные сотрудники, а также бывшие сотрудники компаний, имеющие авторизованный доступ к корпоративной информации, гораздо опаснее «чужих» компьютерных преступников – к такому выводу пришли аналитики из Digital Research Inc., проводившие в июне 2001 года анонимное исследование по заказу разработчика систем компьютерной безопасности фирмы Camelot и журнала «eWeek». Из 548 опрошенных пользователей 57% заявили, что утечка информации дело рук корпоративных пользователей. Вторая по значимости причина это несвоевременная деактивация электронных счетов сотрудников, более в компаниях не работающих. И только 21%

респондентов сослался на внешние «вторжения» в компьютерные системы с целью получения информации. В ходе исследования также выяснилось, что компании тратят большие деньги на совершенствование защиты корпоративных сетей от «собственных» нарушителей уже по следам реальных происшествий, причём эти траты имеют тенденцию к росту, хотя своевременное принятие превентивных мер защиты обошлось бы намного дешевле. Кстати, по мнению Моти Долгина, вице-президента Camelot, компании стараются не афишировать в средствах массовой информации электронные атаки со стороны своих бывших сотрудников, но, тем не менее, такие случаи постоянно становятся предметом общественного внимания, что говорит о масштабности этого проявления компьютерной преступности.

Рассмотрим несколько интересных и, вместе с тем, поучительных примеров.

17 марта 2000 года по подозрению в проведении электронной атаки на Web-сайт собственной компании был арестован некий Абделькадер Смайрс, бывший служащий нью-йоркской корпорации Internet Trading Technologies Corp. (ITTI). Система ITTI позволяет фирмам осуществлять онлайновые операции с акциями, а сама компания является активным участником торгов Nasdaq. Атака была начата 9 марта и продолжалась целых три дня, пока 12 марта специальное подразделение секретной службы США Electronic Crimes Task Force не отследило компьютер, с которого производились электронные атаки. Им оказался компьютер одного из технических колледжей, где Смайрс работал в это время инструктором.

В январе 2001 года бывший системный администратор окружного суда штата Аляска Скотт Деннис был признан виновным в серии электронных атак, предпринятых им против Web-сайта окружного суда Нью-Йорка. Обвинители утверждали, что Деннис осуществил их в целях доказательства того, что система не в состоянии обслуживать большое число пользователей. Скотт Деннис был приговорён к трём месяцам тюремного заключения, трём месяцам домашнего ареста и штрафу в размере 5,3 тысячи долларов, который

он обязан выплатить суду Нью-Йорка, а также двум провайдерским службам, услуги которых он использовал без их ведома для прикрытия своих преступных действий. Кроме того, в течение отбытия наказания власти будут следить за компьютерной активностью Денниса, а после освобождения из тюрьмы он должен отработать 240 часов на общественных работах.

В мае 2001 года 28-летнего жителя Сан-Хосе Макса Рэя Батлера, известного в Интернет под именем «Max Vision», приговорили к тюремному заключению сроком на 18 месяцев и штрафу в 60 тысяч долларов за взлом нескольких сотен компьютерных сетей Министерства обороны США и двенадцати федеральных агентств. С 1998 года, будучи информатором подразделения по кибербезопасности (!) ФБР США, Батлер успешно внедрялся в сети нескольких военно-воздушных баз, в сеть центра НАСА в Алабаме и в компьютеры канцелярии Министерства транспорта США. От его действий пострадали также компьютеры лаборатории Калифорнийского университета, Министерства торговли США и Министерства внутренних дел США. Согласно документально подтверждённым данным, всякий раз, получая приоритетные права при внедрении в систему, Батлер использовал одну и ту же программную ошибку в популярной компьютерной программе BIND (Berkley Internet Name Domain), которая позволяет переводить IP-адреса в доменные имена и наоборот. Помимо этого, Батлер взломал сети Интернет-провайдера Aimnet и получил доступ к паролям 477 его пользователей.

Два бывших бухгалтера компании Cisco Systems – 30-летний Джеффри Осовски и 35-летний Уилсон Танг – отбывают по решению окружного суда, приговорившего их в ноябре 2001 года к этому наказанию, 34-месячное тюремное заключение. Помимо тюремного заключения суд постановил Осовскому и Тангу выплатить разницу между стоимостью украденных акций и растраченными ими 5 млн. долларов, полученных в обмен на акции Cisco Systems. Причиной столь сурового решения стала деятельность бывших бухгалтеров на «ниве» электронной преступности. Осовски и Танг взломали компьютерную сеть компании и похитили акции стоимостью почти в 8 млн.

долларов. Согласно протоколам суда, в течение шести месяцев компьютерные преступники подделывали документы, санкционирующие выпуск около 275 тысяч фальшивых акций компании Cisco Systems.

В феврале 2002 года в результате полицейского рейда в Кингсфорде (пригород г. Сидней) был задержан 21-летний бывший служащий телекоммуникационной компании Optus, занимающей одну из ведущих позиций на рынке телекоммуникаций Австралии. Полицией конфискованы компьютер и документация, которые послужили уликами, и арестованный компьютерный преступник обвиняется в «несанкционированном вторжении и внесении изменений в базы данных компании». По словам управляющего корпоративными делами Optus Стивена Вудхилла, подтвердившего факт электронной атаки на компьютерные системы, обвинения были предъявлены согласно новому закону, вступившему в силу в 2001 году.

В августе 2002 года 28-летний гражданин Великобритании Стивен Кэри был признан виновным во взломе компьютерной сети компании RP Duct Work и приговорён к полутора годам тюрьмы. Кэри работал в компании техническим консультантом, и в его обязанности входила поддержка компьютерной базы данных. В скором времени после начала работы, когда действия Кэри привели к сбою в работе базы данных и прекращению доступа к корпоративной информации, он предложил руководству оплатить восстановление системы по тарифу 80 фунтов стерлингов за час работы. Руководство RP Duct Work не согласилось с такими расценками, и Кэри был уволен. Прежде чем покинуть компанию, он обеспечил себе возможность проникновения в компьютерную сеть RP Duct Work и из дома удалил базу данных с большим количеством важной информации. Нанесённый действиями компьютерного преступника ущерб был оценён в 50 тысяч фунтов стерлингов. Позже Кэри был арестован полицией, и расследование подтвердило факт проникновения в компьютерную систему RP Duct Work перед тем, как была стёрта база данных, что и послужило основным доказательством вины.

Выше, в таблице В.1, мы указали только самые очевидные признаки, на которые следует обращать внимание при выявлении компьютерных преступлений. Иногда эти признаки говорят о том, что преступление готовится или уже совершено, или о том, что не выполняются необходимые меры защиты. Они также могут свидетельствовать о наличии так называемых уязвимых мест компьютерной системы, то есть указать, где конкретно находится незащищённое место и помочь наметить или реализовать соответствующий план действий по его устранению. Подчеркнём, что эти признаки могут помочь *выявить* преступление или злоупотребление, и только меры защиты могут помочь предотвратить его[19].

Кроме всего прочего, до сих пор отсутствуют даже чёткое определение компьютерной преступности и единое понимание сути этого явления, что значительно затрудняет постановку конкретных задач правоохранительным органам, а также выработку единой стратегии борьбы с компьютерными злоумышленниками.

Вместе с тем, в результате интенсивных исследований в области компьютерной преступности был предложен ряд различных подходов к определению понятия этого феномена. В 1983 году в Париже группой экспертов было дано криминологическое определение компьютерного преступления, под которым понималось «…любое незаконное, неэтичное или неразрешённое поведение, затрагивающее автоматизированную обработку данных и (или) передачу данных». Тем не менее, в настоящее время в криминалистической науке все ещё не существует единого понятия компьютерного преступления. В марте 1993 года на заседании межведомственного семинара «Криминалистика и компьютерная преступность» была сделана попытка формулировки одного из первых отечественных определений понятия «компьютерное преступление». Согласно этому определению, под компьютерным преступлением следует понимать «…предусмотренные уголовным законом

[19] Меры защиты – меры, вводимые руководством для обеспечения безопасности информации: административные руководящие документы (приказы, положения, инструкции), аппаратные устройства или дополнительные программы, основной целью которых является предотвращение преступления и злоупотребления. Меры защиты могут выполнять функцию ограничения, уменьшая размер ущерба от преступления.

общественно опасные действия, в которых машинная информация является либо средством, либо объектом преступного посягательства».

В контексте уголовно-правового понятия компьютерное преступление трактуется отечественными специалистами также и как «предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершённое во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства»[20]. По определению А. П. Полежаева, понятие «компьютерная преступность» охватывает «преступления, совершаемые с помощью компьютеров, информационно-вычислительных систем и средств телекоммуникаций, или направленные против них с корыстными либо некоторыми другими целями». Ю. М. Батурин считает, что в юридическом смысле компьютерные преступления как особая группа преступлений не существуют, но при этом подчёркивает, что многие традиционные виды преступлений усовершенствовались в результате привлечения средств вычислительной техники и, следовательно, можно говорить только о компьютерных аспектах преступлений без выделения их в отдельную группу[21]. Несколько иного мнения придерживается А. Н. Караханьян, который понимает под компьютерными преступлениями «противозаконные действия, объектом или орудием совершения которых являются электронно-вычислительные машины».

Приведённые разночтения в определении компьютерного преступления существуют, скорее всего, по причине как множественности предметов преступных посягательств с точки зрения их уголовно-правовой сути, так и невозможности выделения единого объекта преступного посягательства[22]. Одна часть специалистов относит к компьютерным преступлениям только противозаконные действия в сфере автоматизированной обработки информации, а

[20] Уголовное право России. Особенная часть: Учебник // Отв. ред. Б. В. Здравомыслов. М., 1996.

[21] Батурин Ю. М., Жодзинский Н. Л. Компьютерная преступность и компьютерная безопасность. М., 1991.

[22] Криминология. Учебник для юридических вузов // Под ред. В. Н. Кудрявцева, В. Е. Эминова. М., 1995.

другая – все действия, в которых компьютер является либо объектом, либо орудием посягательств.

В целом в уголовно-правовой литературе последних лет при характеристике интересующей нас области противоправной деятельности используется целый ряд терминологических понятий, среди которых: «информационное преступление», «компьютерное преступление», «преступление в сфере компьютерной информации»[23]. Первые два из них, говоря строгим математическим языком, представляют собой два взаимно пересекающихся множества, и при этом оба термина включают в себя третий термин в качестве собственной части – как более узкий по смыслу. В то время как предметом информационного преступления может являться любая без каких-либо изъятий информация, в том числе и в электронной форме, под компьютерным преступлением в специальной литературе обычно понимается действие, в котором машинная информация и компьютер являются либо предметом, либо средством, – например, мошенничество с помощью компьютера. Поэтому сейчас законодательства многих стран сходятся в том, что «…компьютерное преступление, в самой его общей формулировке, есть любое противозаконное действие, объектом посягательства которого является информация, обрабатываемая в компьютерной системе, а орудием посягательства служит компьютер»[24]. Другими словами, отталкиваясь от приведённого определения, можно сказать, что в большинстве случаев компьютерные преступления представляют собой разновидность давно известных, традиционных видов преступлений, которые совершаются при помощи нового инструментария в абсолютно несвойственной традиционной преступности среде[25].

---

[23] Мелик Э. Компьютерные преступления. Информационно-аналитический обзор. М., 1999.

Сорокин А. В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия и расследования. Курган, 1999.

Наумов В. Отечественное законодательство в борьбе с компьютерными преступлениями. М., 1997.

Родионов А. Компьютерные преступления и организация борьбы с ними // Научно-правовой альманах МВД России «Профессионал». 5 (31). 1999.

[24] Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // «Российская юстиция». 1999. № 1.

[25] Крылов В. В. Информационные компьютерные преступления. М., 1997.

Кстати, законодательство России фактически пошло именно по этому пути, что и нашло своё отражение и в Уголовном кодексе Российской Федерации при определении общественно опасных деяний в отношении средств компьютерной техники, но об этом мы будем говорить ниже.

Американский эксперт в области компьютерной преступности Марк Экенвайлер отводит компьютеру различное место в процессе совершения преступлений и, в соответствии с этим подходом, формирует три основные категории – в зависимости от способа использования компьютера при совершении преступлений[26].

В первой категории компьютер выступает в качестве объекта нападения, когда целью преступника является хищение информации или нанесение какого-либо урона интересующей его компьютерной системе.

В этом случае эксперт указывает на две разновидности преступлений, где компьютер является объектом посягательства: изъятие средств компьютерной техники (к этой группе относятся традиционные способы совершения преступлений, в которых преступные действия сосредоточены на изъятии чужого имущества) и электронное нападение на компьютер с целью несанкционированного доступа для получения хранящейся в нём информации (хищение данных), бесплатного пользования данной компьютерной системой (кража услуг) или повреждения самого объекта нападения – компьютерной системы.

Основная доля второй разновидности преступлений осуществляется с помощью несанкционированного доступа к системе или, иными словами, «электронного взлома». Если компьютерный преступник обладает возможностями физического доступа к средствам управления системой, которые открывают доступ к конфиденциальной информации, и определённым временем для реализации своих целей, то речь должна идти о так называемом «электронном взломе изнутри». Если компьютерный преступник не имеет

[26] Причём, Экенвайлер указывает, что при совершении ряда преступлений может использоваться комбинация способов использования компьютера изо всех категорий.

прямого физического доступа к компьютерной системе, но может каким-либо путём проникнуть в неё для совершения противоправных действий, речь идёт об «электронном взломе снаружи». К этой же разновидности «электронных» преступлений Экенвайлером отнесены также деяния, совершаемые в отношении информации, находящейся в компьютерных сетях и электронно-вычислительных машинах, не являющихся компьютером в классическом понимании этого слова: сотовые телефоны, кассовые аппараты, пейджеры и т. п.[27]

Эксперт особо подчёркивает, что преступления, связанные с хищением информации, могут принимать различные формы в зависимости от характера системы, в отношении которой осуществляется несанкционированный доступ, а информация, являющаяся объектом преступного посягательства, может быть отнесена к одному из четырёх типов: персональные данные; корпоративная информация, составляющая коммерческую тайну; объекты интеллектуальной собственности и материалы, защищённые авторским правом; а также общая информация, имеющая значение для развития отраслей промышленности, экономики отдельных регионов и государства. Например, получение несанкционированного доступа к компьютерной системе с целью бесплатного пользования предоставляемыми услугами может квалифицироваться как кража услуг, и одним из самых распространённых компьютерных преступлений данного вида является так называемый «уивинг», который применяется компьютерным преступником с целью собственной маскировки. Он выбирает сложный маршрут прохождения через различные компьютерные системы и сети, чтобы скрыть свои «истинные координаты» и другие, идентифицирующие его признаки.

Преступления под общим названием «повреждение системы» совершаются против компьютерной системы с целью уничтожения или искажения данных, которые представляют собой ценность для её владельца или пользо-

[27] Отмечается тенденция к переходу от разовых преступлений по проникновению в системы со своих или соседних рабочих мест к совершению сетевых компьютерных преступлений путём «электронного взлома» защитных систем организаций.

вателей. Они осуществляются при помощи массированной передачи электронных сигналов на серверы для вывода их из рабочего режима, внедрения в компьютеры вредоносных компьютерных программ, которые в заданный момент изменяют или уничтожают файлы и программы, а также манипуляции данными.

Во второй категории компьютер используется в качестве орудия совершения традиционных преступлений и электронной атаки на другой компьютер. Значительная часть преступлений данной категории: мошенничество с предоплатой, распространение порнографии, виртуальные финансовые пирамиды и пр.[28], – совершается с использованием Глобальной сети.

В некоторых случаях компьютер является как объектом несанкционированного доступа, так и орудием атаки, но в подавляющем большинстве случаев электронные атаки на компьютеры совершаются с других компьютеров. Эксперт отмечает существование двух основных видов компьютерных преступлений, совершаемых на удалении: несанкционированный доступ и отказ в обслуживании.

В первом случае компьютерный преступник может использовать недочёты в системе обеспечения безопасности для получения доступа к компьютерной системе с целью хищения или уничтожения информации, а также нападения на другие компьютерные системы. Во втором – целью преступника является нарушение нормального функционирования атакуемой им системы, а доступ к информации этой системы может его и не интересовать.

В третьей категории Экенвайлер отводит компьютеру роль запоминающего устройства, которое представляет собой в совершаемом преступлении объект несанкционированного доступа. Например, в результате электронного взлома на жёстком диске системы под уникальными именами образуются дополнительные каталоги или каталог, где электронный взломщик может прятать свой программный инструментарий, файлы с данными, и пр.

[28] У. Альбрехт, Дж. Венц, Т. Уильямс. Мошенничество. Луч света на темные стороны бизнеса. СПб., 1996.

На настоящий момент в результате расширяющегося из года в год международного сотрудничества, обмена передовым опытом и конструктивными идеями, практически все ведущие в политическом, экономическом, научном, индустриальном и социальном аспектах державы уже накопили вполне определённый опыт в области систематизации преступлений, касающихся компьютерной информации и аппаратно-программных средств. По завершении соответствующих исследований специалистами классифицированы многие распространённые способы, виды, методы совершения и последующего сокрытия компьютерных преступлений.

Экспертами в данной области знаний обычно выделяются различные, весьма обширные криминологические группы компьютерных преступлений, рис. В. 1.

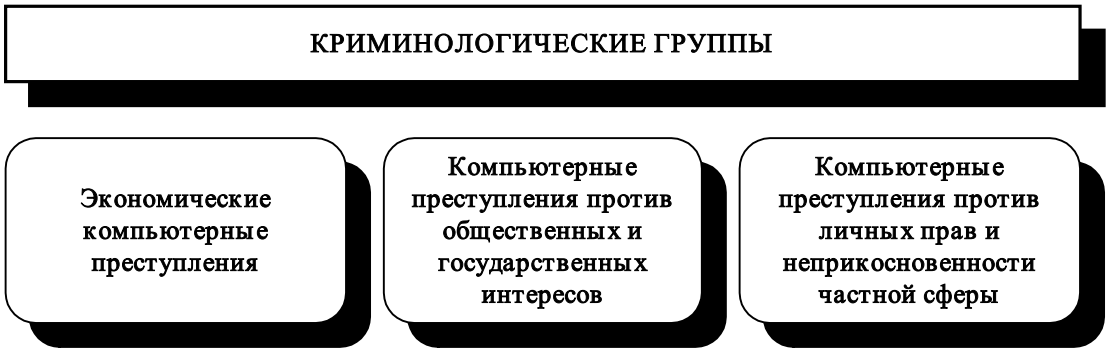

Рис. В.1. Криминологические группы компьютерных преступлений

Причём, среди указанных на рис. В. 1 групп компьютерных преступлений наибольшей масштабностью и широким распространением отличаются экономические компьютерные преступления[29].

Как известно каждый конкретный метод совершения компьютерного преступления представляет собой набор специфичных действий правонарушителя по проведению необходимой подготовки к преступлению, совершению самого преступления с использованием электронно-вычислительных средств и дальнейшей маскировки преступления. Компьютерные правонарушители до, в момент и после совершения своих деяний оставляют хотя бы

[29] Свенссон Б. Экономическая преступность. М., 1987.

минимальные улики, которые затем предоставляют соответствующим специальным службам возможность восстановления обстановки и обстоятельств произошедшего, а также дают представление об отличительных чертах преступного поведения правонарушителя и данные относительно его личности.

Метод совершения преступления всегда является результатом совокупного действия значительного числа факторов и, чем больше будут они проявляться в действиях, тем больше следов будет оставлять компьютерный преступник, тем большей информацией будет располагать следователь при выдвижении следственных версий и проведении розыскных мероприятий. Очевидно, что применительно к рассматриваемой нами проблеме наибольшую ценность будут представлять конкретные следы, указывающие на то, каким образом преступник проник в компьютерную систему (то есть преодолел систему защиты), использовал ли он при этом своё служебное положение и выполнил ли намеченную преступную цель, какие навыки и знания применил, как пытался скрыть следы совершённого преступления. Очень существенными являются следы, свидетельствующие о характере связи преступника с предметом преступного посягательства.

С криминалистической точки зрения, метод совершения преступления всегда конкретен и обладает характерными чертами, которые имеют важное следственно-оперативное значение. Среди них можно выделить распространённость данного метода, конкретные приёмы его применения и источники знаний об этих приёмах, используемые программно-аппаратные средства и их технические параметры, сведения о том, как и где проходит подготовка самого преступления и прочее. При выборе конкретного метода совершения компьютерного преступления немаловажны мотивы и цели, с которыми оно готовится и совершается.

Анализ зарубежных и отечественных отчётов о выявленных компьютерных преступлениях позволяет сделать вывод о том, что лишь немногие из них включают в свой состав целенаправленное разрушение компьютеров или данных. Только в 3% мошенничеств и 8% злоупотреблений происходило

специальное разрушение оборудования и уничтожение компьютерных программ. В значимой части случаев целью мошенничеств и злоупотреблений является критическая информация[30].

Например, в октябре 2003 года компьютерная система корпорации ViewSonic была атакована её бывшим сотрудником. В окружном суде г. Лос-Анджелес 38-летний Эндрю Гарсия, работавший в офисе корпорации ViewSonic в г. Валнут (штат Калифорния, США), признал себя виновным в получении несанкционированного доступа к защищённому компьютеру, взломе компьютерной системы и преднамеренном удалении критической информации, повлекшей за собой закрытие сервера, который являлся основным для зарубежных операций.

Гарсия был сетевым администратором в Валнутском офисе корпорации, где отвечал за несколько компьютерных серверов и имел доступ к паролям системы для служащих. Как следует из документов суда, 14 апреля 2002 года – спустя всего лишь две недели после своего увольнения из корпорации – Гарсия получил доступ к компьютерной системе и удалил несколько критически важных файлов на одном из серверов, которые он поддерживал, работая в ViewSonic. Потеря этих файлов вывела сервер из строя, и на протяжении нескольких дней офис корпорации не мог принимать важную служебную информацию. Приговор Гарсия будет вынесен в течение 2004 года и ему грозит 5 лет тюрьмы, а также штраф в 250 тысяч долларов.

Основные мотивы и наиболее распространённые цели совершения компьютерных преступлений, обычно выделяемые специалистами, представлены на рис. В. 2а и рис. В. 2б, соответственно.

---

[30] Под термином «критическая информация» обычно подразумеваются данные, которые требуют защиты из-за возможности или риска нанесения ущерба в том случае, если произойдёт их случайное или умышленное раскрытие, изменение или разрушение.

Этот термин включает в себя данные, неправильное использование или раскрытие которых может негативно отразиться на способности организации или учреждения выполнять свои производственные функции, персональные и другие данные, защита которых требуется в соответствии с законами Российской Федерации, указами Президента Российской Федерации и другими нормативными актами.

Технические средства по защите критической информации могут быть встроены непосредственно в компьютер или программное обеспечение. Некоторые меры по защите критической информации выполняются людьми и являются реализацией указаний руководства, содержащихся в соответствующих инструкциях. Принятие окончательного решения о выборе уровня защиты требует установления критичности информации и последующего определения необходимого уровня безопасности.

Рис. В.2.а. Основные мотивы совершения компьютерных преступлений

Кстати говоря, в последнее время психологи всерьёз заинтересовались проявлениями раздражительности и нервозности, присущими некоторым пользователям, часто работающим или развлекающимся в Интернет. У психологов такое поведение получило название «Web-агрессия» и ими доказано, что оно может приводить к абсолютно немотивированному совершению компьютерных преступлений.

Приводящее к крупным авариям бесконтрольная агрессия водителей автомобилей в экстремальных ситуациях явление давно известное. Как оказалось подобное поведение свойственно и некоторым пользователям Интернет, которые ежедневно подвергают собственную психику испытаниям не намного меньшим, чем усреднённый автолюбитель. Во всяком случае, согласно исследованию специалистов, больше половины пользователей как минимум раз в неделю претерпевают приступы гнева, связанные с функционированием Глобальной сети. Раздражающими факторами становятся выска-

кивающие окошки с навязчивыми просьбами ввести личную информацию, пароль и т.п., которые оттягивают желанный момент открытия нужной Web-страницы. «Я действительно испытываю чувство ненависти тогда, когда трачу кучу времени на то, чтобы открыть нужную мне Web-страницу, и, в конце концов, обнаруживаю, что в данный момент она недоступна или же находиться в стадии разработки», – вот типичное заявление пользователя.

Рис. В.2.б. Наиболее типичные цели совершения компьютерных преступлений

Более того, согласно статистике, только 2% пользователей могут самостоятельно справиться с приступами необузданной Web-агрессии. Что тут можно посоветовать? Как это ни «дико» звучит («… они не могут сами справится, а он им советует успокоиться»), но изначально, ведь вы в подавляющем большинстве случаев наедине с собой, мера здесь может быть всего лишь одна – самоконтроль. Поэтому, психологи предлагают «взять себя в руки» и успокоиться (2%), а затем, если это не помогает (те самые 98%), обратиться к ним за квалифицированной помощью. И ни в коем случае не совер-

шайте непродуманные поступки, которые потом могут быть расценены как преступное деяние с использованием средств вычислительной техники. Лучше сразу выключить компьютер!

В целом совершающие компьютерные преступления физические лица, обычно подразделяются на четыре агрегированные совокупности, рис. В. 3.

Рис.В.3. Основные группы физических лиц, совершающих компьютерные преступления

Кроме приведённой на рис. В. 3 группировки, с точки зрения возможностей совершения компьютерных преступлений, специалисты подразделяют представляющий опасность персонал в соответствии со сферами его деятельности на пять категорий или групп риска, рис. В. 4.

Таким образом, особую опасность могут представлять собой специалисты в случае их сговора с руководителями подразделений и служб организации или связанных с ней систем, а также с организованными преступными

группировками, поскольку в этих случаях причиняемый ущерб от совершённых преступлений и тяжесть последствий значительно увеличиваются.

Например, около 90% злоупотреблений в финансовой сфере, связанных с нарушениями в области информационной безопасности, происходит при прямом или косвенном участии действующих или бывших работников банков. При этом на преступный путь часто становятся самые квалифицированные, обладающие максимальными правами в автоматизированных системах категории служащих: системные администраторы и другие сотрудники служб автоматизации и информатизации.

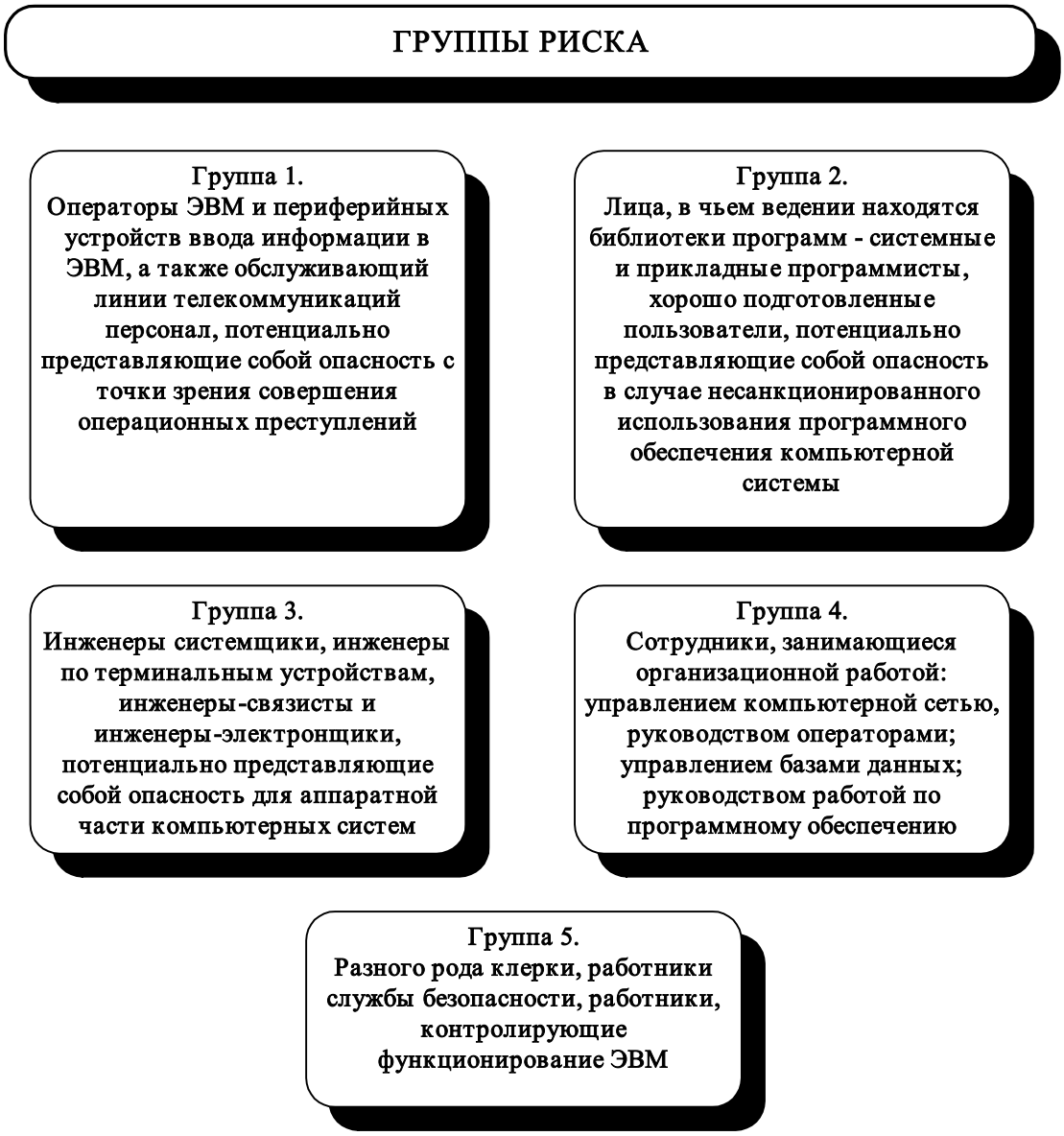

Рис.В.4. Категорирование персонала в зависимости от возможностей совершения компьютерных преступлений

Между прочим, банальная халатность или технические ошибки персонала без заведомо преступного умысла тоже далеко не подарок! Чтобы не быть голословными, приведём конкретные примеры.

В январе 2000 года юристы America Online всеми силами и доступными им средствами пытались остановить распространение нелегальных копий новейшей версии программного обеспечения AOL 6.0, находившейся на тот момент в разработке. Начало тестирования было запланировано только на май, но, благодаря стараниям администратора Web-сайта Kenton.org, эту версию можно было получить уже в январе. В ходе последовавшего разбирательства по поводу того, как ему удалось заполучить копию, администратор утверждал, что просто скачал её из библиотеки America Online.

В итоге библиотеку закрыли для всех пользователей с целью проведения тщательной проверки системы безопасности.

В том же январе компания Microsoft бросила весьма солидные силы на расследование утечки, в результате которой в Глобальной сети появилась бета-версия Internet Explorer 6.

Копии этой программы были разосланы бета-тестёрам, которые подписали соглашение, по условиям которого обязались не разглашать подробности, связанные с новым программным обеспечением. Тем не менее, благодаря небрежности некоторых из них копии Internet Explorer 6 появились на Web-сайтах The-Ctrl-Alt-Del.com и FileClicks. Microsoft отреагировала достаточно быстро. На Web-сайте FileClicks вообще не осталось никаких следов данного программного обеспечения, а на Web-сайте The-Ctrl-Alt-Del.com осталась лишь надпись «самые отважные из вас могут загрузить Internet Explorer 6 уже сейчас», однако все соответствующие ссылки были приведены в нерабочее состояние.

В мае 2000 года сотрудниками Microsoft на Web-сайте Mactopia по ошибке была выложена избыточная информация о предстоящей версии Macintosh Office.

Представители компании подтвердили тот факт, что произошла ошибка, и указанные данные были изъяты. Однако утечка уже случилась, и стали известны закрытые характеристики нового программного продукта.

Буквально через пару недель из-за технической ошибки свыше 16 тысяч пользователей компании мобильной связи Verizon Wireless, созданной компаниями Vodafone и Bell Atlantic, остались без голосовой почты. Инцидент произошел при попытке обновления аппаратно-программного обеспечения, в ходе которой был потерян месячный архив сообщений голосовой почты клиентов, а резервных копий этого архива тоже не осталось[31].

Месяцем позже с очередной проблемой столкнулись пользователи почтовой службы Hotmail. На протяжении нескольких дней некоторые из них не могли получить доступ к своим почтовым ящикам. Когда доступ был восстановлен, их ждал неприятный сюрприз. Вся старая почта, персональные папки и записи в адресной книге были удалены. Представители Microsoft не смогли дать внятного ответа о причинах ошибки. Они сказали только, что компания ведёт работу, направленную на восстановление информации пользователей.

В августе попытки America Online повысить эффективность систем безопасности службы ICQ обернулись для некоторых пользователей «отказом в обслуживании». В результате поступило множество жалоб со стороны пользователей, которые не могли получить доступ к своим счетам. Их старые пароли просто-напросто не распознавались системой, и пользователи получали отказ. При этом America Online полностью игнорировала жалобы, заявив, что работа по корректировке системы безопасности идёт в рамках намеченного плана и никаких отклонений или ошибок не наблюдается.

В начале октября представители Yahoo! подтвердили сообщение о том, что имели место нарушения в работе e-Mail службы компании. К услугам электронной почты Yahoo! прибегают миллионы пользователей со всей планеты и, по словам представителя компании, она является одним из крупней-

[31] В дополнение к указанным неприятностям немедленно начали распространяться слухи о том, что услуги беспроводной связи вообще далеко не так надёжны, как об этом говорят операторы Verizon Wireless.

ших провайдеров e-Mail. В конце сентября многие клиенты не могли получить доступ к своим почтовым ящикам, и это продолжалось в течение нескольких часов. Подобные сбои в системе, продолжавшиеся на протяжении двух недель, представители Yahoo! объяснили ведущимися работами по усовершенствованию архитектуры почтового сервера.

6 декабря в очередной раз произошёл серьёзный сбой на Web-сайте Интернет-магазина Amazon.com Inc. По словам представителей компании, причиной сбоя стала ошибка в использовании программного обеспечения. «Мы одновременно запустили две программы, которые оказались несовместимыми. Именно поэтому и произошёл сбой», – сообщила представитель компании Кристин Шаефер. Во время неполадок на Web-сайте Amazon.com было вывешено сообщение о том, что Интернет-магазин временно закрыт, а затем было объявлено о технических проблемах.

В январе 2001 года в течение трёх дней несколько Web-сайтов компании Microsoft, включая её главный Web-сайт, а также Интернет-портал MSN, были недоступны для многих пользователей.

По официальному сообщению, проблемы начались после того, как во вторник была проведена реконфигурация основных DNS на маршрутизаторах компании. Как выяснилось позже, в этом процессе был допущен ряд ошибок, приведших к тому, что DNS-серверы сети Microsoft оказались «отрезанными» от публичных DNS-серверов. В результате несколько Web-сайтов компании стали недоступны для пользователей Интернет. Среди них оказались главный Web-сайт компании microsoft.com, порталы msn.com, msnbc.com и ряд других. Следует отметить, что сами Web-серверы Microsoft не прекращали работать, и в принципе доступ к ним можно было получить, набрав в строке браузера не имя Web-сайта, а его IP-адрес. Представитель компании г-н Сон заявил также о том, что данные проблемы не коснулись почтового сервера Hotmail.com, который обеспечивает бесплатную электронную почту для 74 млн. пользователей во всём мире.

Отметим, что все эти неприятности происходили в тот момент, когда Microsoft вела широкомасштабную рекламную кампанию стоимостью в 150 млн. долларов для того, чтобы заявить о себе как о крупнейшем Интернет-портале, и опередить по этому показателю America Online и Yahoo!

В мае группа пользователей Интернет получила возможность перекачать бета-версию новой операционной системы компании Microsoft – Windows XP, официальный выход которой был намечен на 25 октября.

Дело в том, что один из бета-тестеров без ведома компании выложил в Интернет свои логин и пароль. Компания Microsoft подтвердила произошедшую утечку, назвав появление данной информации в открытом доступе «случайным». Логин и пароль для откачивания операционной системы Windows XP появились в Интернет в пятницу, и к моменту обнаружения этого факта представителями Microsoft доступ к Windows XP, по данным самой компании, получили «несколько человек». Как заявил один из ведущих менеджеров Microsoft Грег Салливан, бета-версию операционной системы пытались скачать несколько тысяч человек, однако, это удалось «немногим из них», поскольку в неё встроены специальные средства защиты. Однако точное число получивших доступ к Windows XP г-н Салливан назвать отказался.

В октябре компания Microsoft была вынуждена в срочном порядке «латать» дыры во внутренней службе поддержки пользователей после того, как её проинформировали о возможности поиска по базе данных клиентов компании. Данные по кредитным карточкам не были доступны, однако поиск по именам и личным данным, таким как номера телефонов, адреса и покупательская активность, вполне можно было осуществить. И, что интересно, сообщил об этом не кто-нибудь из персонала компании, а уже успевший прославиться своей деятельностью по поиску «брешей» в безопасности систем Адриан Ламо.

Далеко не законопослушный двадцатилетний Ламо, который сам незадолго до того занимался изменением новостей на сервере Yahoo!, сообщил, что ему удалось получить доступ к Web-сайту для внутреннего пользования.

Эта «находка» позволила ему, как при желании и любому другому загружать личные данные о любом пользователе, который оформлял бланк заказа продуктов компании Microsoft через e-Mail. Web-сайт даже не надо было взламывать – фактически, о его безопасности никто и не задумывался, полагаясь на то, что адрес Web-сайта никогда и нигде не афишировался! Microsoft удалила этот Web-сайт сразу же после того, как была проинформирована о наличии проблемы.

Ламо удалось найти его простым перебором комбинаций известных IP-адресов Microsoft, и неизвестно, как долго данные клиентов компании находились в таком открытом доступе. Ламо уверял, что база данных была весьма и весьма обширной.

В марте 2002 года несколько дней бездействовал Web-сайт электронной газеты Silicon Times Report.

По словам главного редактора газеты Ральфа Мариано, это произошло из-за сбоев в работе компании VeriSign, осуществляющей обслуживание Web-сайта. И Silicon Times Report была не единственной жертвой – по той же причине, как сообщается, пострадали ещё 46 Web-сайтов, восстановить работу которых было достаточно трудно, поскольку многие из них обслуживаются в автоматическом режиме. Мариано полагает, что сбой произошёл из-за отключения домена Visioncommerce.com и внесения изменений в его базу данных. Не имея возможности быстро вернуться к нормальной работе Web-сайта газеты, Мариано создал ещё один Web-сайт, где и разместил специальный список допущенных VeriSign ошибок.

По опубликованному в онлайновом издании Risks Digest сообщению, которое было посвящено опасностям, связанным с применением компьютерных систем, в феврале 2003 года компьютерная система медицинского центра Св. Мэри в городе Гранд Рэпидс (штат Мичиган, США) объявила восемь с половиной тысяч пациентов мёртвыми, в то время как все они были живы.

Массовый переход живых пациентов медицинского центра «в мир иной» случился после обновления программы для управления данными о па-

циентах больницы. В процессе переноса записей в новую версию программы, была допущена ошибка в подстановке полей и код «20», который означал смерть больного, получили все пациенты, у которых ранее стоял код «01», означавший выписку из больницы. Ошибочные данные были разосланы не только самим пациентам, но также отправлены в страховые компании и местные офисы системы социального обеспечения, которые определяют право на получение денежных пособий пожилыми пациентами и инвалидами.

Таким образом, халатность, невнимательность и ошибочные решения могут являться источником больших неприятностей, а в отдельных случаях – даже провоцировать на совершение противозаконных действий. Давайте теперь вернёмся к нашей главной теме – преднамеренной компьютерной преступности.

Так кто же он, типичный компьютерный преступник?

В России, как показывают статистика и проведённые отечественными специалистами исследования, до 20% от общего числа компьютерных преступников олицетворяют собой некий стереотип. В соответствии с ним компьютерный преступник это гражданин страны примерно 18–20 лет, выросший в российской семье со средним достатком, обладающий неряшливой причёской, в очках, молчаливый, замкнутый и рассеянный, увлечённый компьютерной техникой и игнорирующий события в окружающем мире.

Остальные 80% компьютерных преступников либо полностью, либо частично отличаются от приведённого описания, и их можно подразделить на группы следующим образом. Около 20% технократов, то есть людей, буквально «молящихся» на компьютер и электронную технику в целом, о которых иногда говорят «не от мира сего». Порядка 40% «крепкого середняка», знающего своё дело, но «звёзд с неба не хватающего». И примерно 20% «компьютерной элиты», представляющей собой законченный продукт рыночных отношений, знающей себе и своим знаниям истинную цену.

Последняя и, частично, вторая группа превратили увлечение в доходное дело, обладают не только общими знаниями в области информационных

технологий, но и специальными навыками и наработками в плане обращения со средствами вычислительной техники, программным обеспечением, компьютерными системами и сетями, которые позволяют им преодолевать защиту компьютерных систем.

Именно «компьютерная элита» является движущей силой как в законопослушной деятельности в сфере высоких информационных технологий, так и в области компьютерной преступности.

Интересно, а к какой группе следует отнести такую незаурядную личность как индус Анкит Фадиа? Так же, как и миллионы его сверстников во всём мире, индийский подросток Анкит любит слушать музыку, смотреть сериал «Секретные материалы» и собирать фотографии знаменитых актёров, звёзд Голливуда. Как и миллионы подростков непосредственно в современной Индии, он целиком захвачен всем тем, что связано с вычислительной техникой.

Исключительно ради забавы он регулярно взламывает различные Web-сайты. Кроме того, 16-летний подросток стал автором довольно незаурядного справочника по всемирному киберпространству. На то чтобы написать этот 600 страничный опус «Неофициальное руководство этичного электронного взлома» (The Unofficial Guide to Ethical Hacking), Анкит Фадиа потратил часть своих летних каникул. Наряду с описанием различных методов информационного пиратства и вредоносных компьютерных программ, в руководстве приводятся способы защиты от действий электронных злоумышленников.

У Анкита прослеживается даже собственная философия или, если хотите, выработана несколько противоречивая, но, безусловно, своя жизненная позиция. Как считает юный автор книги, чтобы защититься от электронного взлома, нужно знать, как действуют компьютерные преступники, и в наш век высоких технологий быть одним из них просто необходимо. Однако своё будущее Анкит Фадиа видит связанным с работой в IT-секторе и собирается,

получив соответствующее образование, создать собственную фирму, занимающуюся разработкой систем компьютерной безопасности.

Ещё один «писатель» Кевин Митник[32] (о котором мы ещё будем упоминать по тексту книги), отбывший почти пять лет тюремного заключения по обвинению в краже программного обеспечения и изменение информации в компьютерных системах, принадлежащих ряду известных компаний, в том числе Motorola, Novell, Nokia, Sun Microsystems, и освобождённый в январе 2000 года, в своём выступлении перед менеджерами корпораций на тему борьбы с компьютерной преступностью и защиты корпоративных сетей заявил, что самым уязвимым звеном для электронных нападений является человек.

Особое внимание присутствующих на человеческий фактор и метод внедрения, известный как «социальная инженерия», 37-летний Митник обратил на конференции «Инфраструктура электронного бизнеса», проведённой компанией Giga Research.

Сам Митник, с 16-летнего возраста начавший свой путь в качестве «фрикера» (индивидуума, внедряющегося в телефонные сети и использующего их без уведомления владельцев), достигал наибольшего успеха именно благодаря этому методу. «Люди являются самым слабым звеном. Вы можете иметь наилучшие технологии, отлично настроенные межсетевые экраны, системы обнаружения вторжения, биометрические приборы... а некто обратится к ничего не подозревающему сотруднику компании, который выдаст что-нибудь лишнее», – заявил Митник.

В конце выступления он дал ряд рекомендаций по защите систем, которые мы представляем вниманию читателя в виде табл. В4.

---

[32] Лишённый по решению суда права пользования Интернет до января 2003 года Митник в июле 2002 года объявил о завершении работы над романом, название которого переводится на русский язык как «Искусство обмана» («The Art of Deception»).

В книге рассказывается о человеке, считающем себя супер электронным взломщиком. По ходу сюжета смышлёный компьютерный злоумышленник несколько раз обманывает сетевых администраторов и получает доступ к паролям и шифровальным ключам. Интересно, что хотя роман не относится к документальной прозе, и по жанру это чистая беллетристика, издатели тщательно исследовали текст, чтобы исключить из него любые намёки на особенности реальных систем безопасности.

Книга была опубликована в конце 2000 года.

Таблица 4

Рекомендации
от Кевина Митника по защите систем от компьютерных преступлений

Формулировка рекомендации
Всегда
перед тем как выдать какую-либо информацию, удостоверяйтесь в том, что ваш собеседник не выдает себя за кого-то другого
безвозвратно ликвидируйте ненужные дискеты и компакт диски физически во избежание восстановления информации
уничтожайте бумажные документы без следов, предпочтительно – шредером
как можно чаще и регулярно меняйте пароли доступа к системе
Никогда
не выбирайте пароли, состоящие из одного слова и тем более, как-то связанные с вашей личностью
не храните написанные пароли в легко доступном месте – под клавиатурой, наклеенные на монитор и т. д.
не используйте один и тот же пароль в разных системах

§3. Методы совершения компьютерных преступлений и их классификация, основанная на кодификаторе Интерпола

Теперь можно более подробно рассмотреть такой важный предмет, как методы совершения компьютерных преступлений[33].

Зарубежные исследования в этой области начались примерно на 15–20 лет раньше, чем в нашей стране – с конца 70-х годов, и поэтому в США, Канаде, Австралии, Западной Европе и Японии к тому времени, когда аналогичные исследования стали практиковаться в России, были накоплены достаточно обширный фактический материал и практический опыт.

Вместе с тем, как мы уже упоминали, даже в настоящее время в отечественной и зарубежной криминалистической науке не существует единых понятий в вопросах характеристики субъектов компьютерных преступлений, методов совершения компьютерных преступлений, их единых названий и классификации. Эта проблема настолько нова, что во многом находится пока

[33] Вехов В. Б. Компьютерные преступления: способы совершения, методики расследования. М., 1996.

лишь на стадии осмысления и теоретических разработок. Особенно это касается российской криминалистики, которая как наука, столкнулась и вплотную занялась проблемой характеристики методов подготовки и совершения компьютерных преступлений только на рубеже 80-х и 90-х годов прошлого столетия.

За рубежом имеется целый ряд ценных с научной и практической точек зрения разработок и статистических данных, которые необходимо всемерно использовать при изучении компьютерной преступности в целом и осуществлении борьбы с отечественной компьютерной преступностью[34], конечно с учётом определённых объективных и субъективных поправок, отражающих российскую действительность.

Американский национальный институт компьютерной безопасности и ФБР США, например, опросили представителей 269 компаний о наиболее распространённых компьютерных преступлениях, причём в отчёте по результатам опроса были учтены ответы только тех респондентов, компании которых проводили оценку своих финансовых потерь. Итоги таковы: финансовое мошенничество – средний ущерб 957 тысяч долларов в год, кража конфиденциальной информации – средний ущерб 955 тысяч долларов в год, мошенничество со средствами связи – средний ущерб 647 тысяч доллар в год, несанкционированный доступ – средний ущерб 181 тысяч долларов в год, проникновение в систему – средний ущерб 132 тысяч долларов в год.

Основными методами несанкционированного получения информации, сформулированными по данным зарубежной печати, являются: применение подслушивающих устройств (закладок); дистанционное фотографирование; перехват электронных излучений; мистификация (маскировка под запросы системы); перехват акустических излучений и восстановление текста принтера; хищение носителей информации и производственных отходов (сбор мусора); считывание данных из массивов других пользователей; копирование

[34] Проблемы борьбы с компьютерной преступностью // Борьба с преступностью за рубежом. М., 1992. № 4.

носителей информации с преодолением мер защиты; маскировка под зарегистрированного пользователя; использование программных ловушек; незаконное подключение к аппаратуре и линиям связи; вывод из строя механизмов защиты[35].

Сейчас специалистами выделяется около трёх десятков основных методов совершения компьютерных преступлений и порядка пятидесяти вариаций этих методов[36], причём, их количество постоянно пополняется за счёт всё более «свежих инноваций», которые незамедлительно выносятся компьютерными преступниками «на суд широкой общественности».

Таким образом, методов совершения компьютерных преступлений становится всё больше по причине использования преступниками различных их комбинаций, модификации применяемых алгоритмов, и происходит это по мере совершенствования средств вычислительной техники. Естественно, что эта проблема привлекает к себе пристальное внимание отечественной криминалистики.

В настоящий момент одной из наиболее распространённых, из числа существующих классификаций преступлений в сфере компьютерной информации, признана классификация кодификатора Генерального секретариата Интерпола. На основе этого классификатора создана и, с 1991 года, продуктивно функционирует специализированная автоматизированная информационно-поисковая система. В настоящее время её услугами пользуются более чем в 100 странах мира.

Классификация соответствующих кодификатору Генерального секретариата Интерпола методов совершения компьютерных преступлений приведена на рис. В5.

Можно дать следующую краткую характеристику соответствующим кодификатору Интерпола методам компьютерных преступлений.

---

[35] Мелик Э. Компьютерные преступления. Информационно-аналитический обзор. М., 1999.

[36] Вместе с тем, в соответствии с данными проведённых в последнее время исследований о существовании тех или иных методов совершения компьютерных преступлений осведомлены всего лишь около 10–12% респондентов от общего числа отвечавших на соответствующий вопрос в ходе анкетирования.

Во-первых, следует отметить что, как видно из рис. В5, все коды, характеризующие компьютерные преступления, имеют собственный идентификатор, начинающийся с латинской буквы «Q» и, во-вторых, при необходимости для характеристики преступления могут использоваться до пяти кодов, расположенных в порядке убывания значимости совершённого деяния.

Итак, в соответствии с названным кодификатором, компьютерные преступления классифицированы следующим образом.

QA – несанкционированный доступ и перехват;

QAH – компьютерный абордаж (несанкционированный доступ);

QAI – перехват с помощью специальных технических средств;

QAT – кража времени (уклонение от оплаты за пользование автоматизированной информационной системой);

QAZ – прочие методы несанкционированного доступа и перехвата.

К этой группе относятся методы совершения компьютерных преступлений, основанные на действиях преступника, направленных на получение данных и машинной информации посредством использования технических средств, в том числе, например, аудиовизуального и электромагнитного перехвата, широко практикуемых в оперативно-розыскной деятельности правоохранительных органов.

Необходимо подчеркнуть, что в этой и последующих группах средства вычислительной техники выступают как в качестве предмета, так и в качестве орудия совершения преступного посягательства. Кроме того, как указывалось выше, несанкционированный доступ в компьютерные системы финансовых учреждений с целью хищения финансовых средств представляет собой особую опасность.

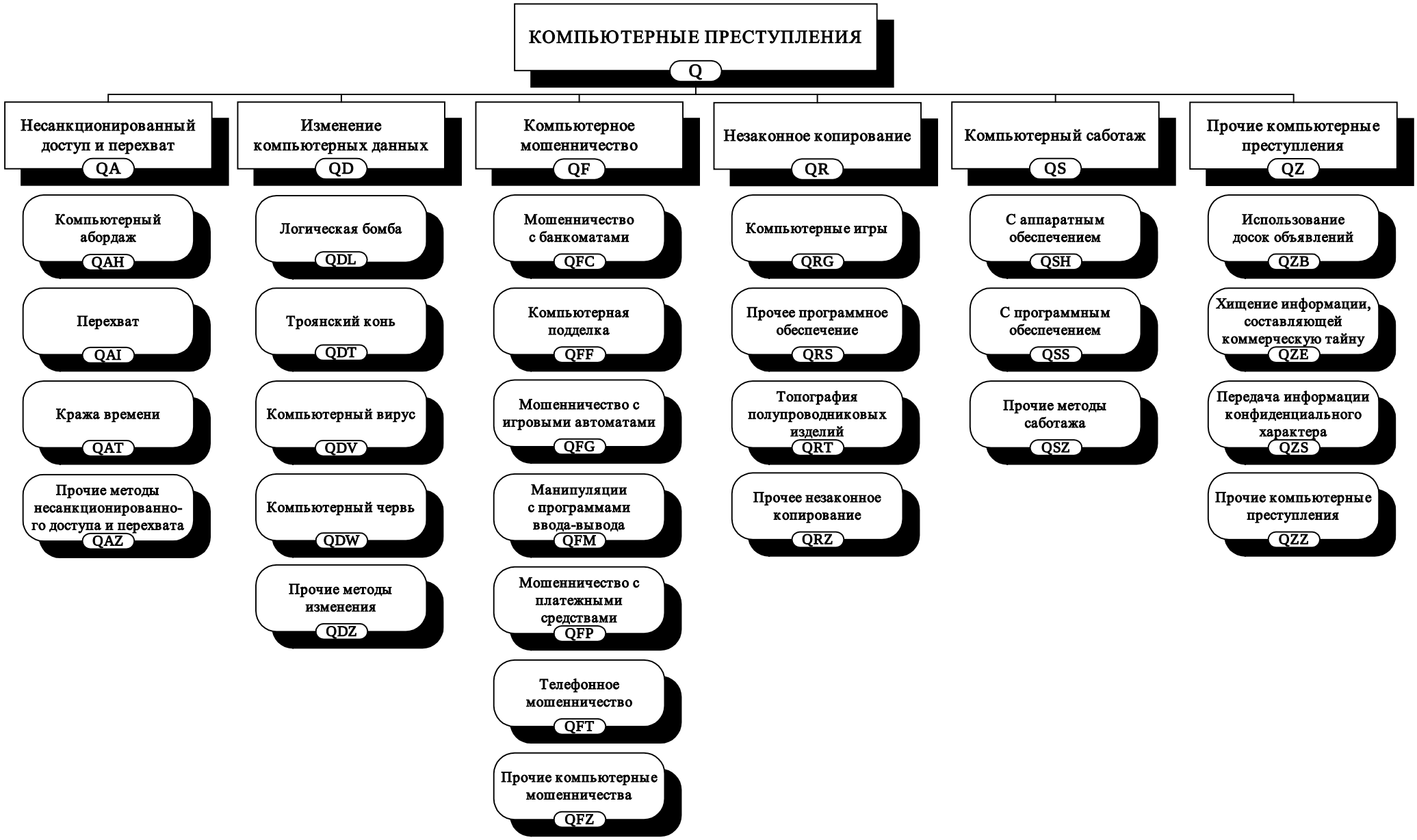

Рис.В.5. Классификация методов совершения компьютерных преступлений в соответствии с кодификатором Генерального секретариата Интерпола

По оценкам отечественных специалистов уже сейчас хищения с применением компьютерной техники и средств электронного платежа несут серьёзную угрозу для национальной и информационной безопасности России и, к тому же, в ближайшем будущем прогнозируется значительный рост компьютерной преступности в данной сфере и увеличение её доли в общем количестве компьютерных преступлений.

Несанкционированный доступ и перехват информации (QA) включают в себя следующие виды компьютерных преступлений.

«Компьютерный абордаж» (несанкционированный доступ) (хакинг – hacking) – доступ к компьютеру или компьютерной сети без права на осуществление такой деятельности.

Этот метод компьютерного преступления обычно используется посторонними лицами для проникновения в информационные сети, владельцами которых они не являются. Компьютерное преступление осуществляется при помощи специального подбора (или заранее добытого) абонентного номера компьютерной системы потерпевшей стороны с использованием, например, обычного телефонного аппарата. Делается это до тех пор, пока на другом конце линии не отзовётся другой компьютер. После этого достаточно подключить собственный компьютер и, определив код, можно внедриться в чужую информационную систему.

Обычно, когда компьютерный преступник получает доступ к компьютеру, он не может сразу получить нужные ему данные, так как полезную информацию закрывают паролем доступа. Поэтому, применяя данный метод, компьютерный преступник производит подбор кода. Для этих целей используются специальные программы (называемые на профессиональном языке «hack tools» – инструментарий взлома), которые с помощью высокого быстродействия компьютера автоматически перебирают все возможные варианты (комбинации букв, цифр и специальных символов, имеющихся на стандартной клавиатуре персонального компьютера) пароля законного пользователя и, в случае совпадения набора символов с оригиналом, производят автомати-

ческое соединение указанных абонентов. В том случае, если компьютерный преступник знает пароль доступа или код отсутствует, доступ в систему открывается практически незамедлительно.

Характеризуя данный метод совершения компьютерных преступлений, необходимо подчеркнуть, что по существу «компьютерный абордаж» является как бы подготовительной стадией перед совершением компьютерного преступления. Кроме того, с одной стороны существует множество программ, которые взламывают пароль доступа, но, с другой стороны, есть также и программы «сторожа» компьютерных портов, которые отключают пользователя от системы в случае многократных некорректных попыток доступа. По этой причине в последнее время компьютерными преступниками всё чаще стал использоваться метод *«интеллектуального подбора»*.

«Интеллектуальный подбор» (intellectual matching) – программе «взломщику» передаются некоторые данные о личности составителя пароля (имя, фамилия, номер телефона и т. д.), добытые компьютерным преступником. Так как пароли пользователей в подавляющем большинстве случаев составляются именно из такого рода данных, действенность этого метода совершения компьютерных преступлений достаточно высока. По оценкам специалистов, использовавших данные экспериментов, поставленных в целях проверки эффективности рассматриваемого метода «интеллектуального подбора», даже при его применении вручную вскрывается более 40% от общего числа паролей пользователей.

Результаты указанных экспериментов приведены в табл. В5[37].

Таблица 5

Результаты
экспериментов в целях проверки эффективности метода интеллектуального подбора

№ п.п.	Тематические группы паролей	Частоты выбора пароля человеком, %	Раскрываемость пароля, %
1.	Имена, фамилии и производные	22,2	54,5
2.	Интересы (хобби, спорт, музыка)	9,5	29,2

[37] Лучин И. Н., Желдаков А. А., Кузнецов Н. А. Взламывание парольной защиты методом интеллектуального перебора // Информатизация правоохранительных систем. М., 1996.

№ п.п.	Тематические группы паролей	Частоты выбора пароля человеком, %	Раскрываемость пароля, %
3.	Даты рождения, знаки зодиака свои и близких; их комбинации	11,8	54,5
4.	Адрес жительства; место рождения	4,7	55,0
5.	Номера телефонов	3,5	66,6
6.	Последовательность клавиш персонального компьютера, повтор символа	14,1	72,3
7.	Номер документов (паспорт, удостоверение) и т.д.	3,5	100,0
8.	Прочие	30,7	5,7

«Перехват» (interception), *«умышленный перехват»* (willful interception) – перехват информации осуществляется с применением специальных технических средств без законного права на осуществление такой деятельности.

Методы перехвата основаны на целенаправленных действиях компьютерного преступника, ориентированных на получение интересующих его данных.

«Непосредственный перехват» (direct interception), *«активный перехват»* (active interception) – перехват информации осуществляется либо напрямую, через телекоммуникационное оборудование компьютера, компьютерной системы или сети (внешние коммуникационные каналы), либо путём непосредственного подключения к линиям периферийных устройств, например, к линии принтера или телефонному проводу канала связи, используемому для передачи данных и управляющих сигналов компьютерной техники, либо непосредственно через соответствующий порт персонального компьютера.

Подключение может осуществляться с помощью использования бытовых средств и оборудования – обычного телефонного аппарата, телефонного кабеля, компьютерного шлейфа, специальных щупов игл от контрольно-измерительной аппаратуры, зажимов типа «крокодил», набора радиомонтажных инструментов, кассетного портативного магнитофона, принтера, модема,

персонального компьютера типа «Laptop» в блокнотном и субблокнотном исполнении и пр.

Средствами компьютерной техники перехваченная информация записывается на какой-либо физический носитель и переводится в удобную для чтения человеком форму посредством бытовой или специальной электронной аппаратуры, в качестве которой компьютерным преступником могут использоваться компьютеризированные анализаторы проводных линий связи, многофункциональные цифровые регистраторы сигналов и т. п.

При этом объектами непосредственного перехвата могут быть системы правительственной связи, системы спутниковой связи, проводные и кабельные системы, а также наземные микроволновые системы. В связи с этим различают:

«форсированный перехват» – перехват сообщений, направляемых рабочим станциям, имеющим неполадки в оборудовании или каналах связи;

«перехват символов» – выделение из набираемого пользователем на клавиатуре терминала текста знаков, не предусмотренных стандартным кодом данного компьютера;

«перехват сообщений» – несанкционированное подключение специального терминала к линии связи, приём и использование сообщений, циркулирующих между абонентскими пунктами и компьютером пользователя.

«Электромагнитный перехват» (electromagnetic pickup), *«пассивный перехват»* (passive interception) – перехват осуществляется за счёт электромагнитных излучений от центрального процессора, коммуникационных каналов, дисплея, принтера, других периферийных устройств и т. д.[38], так как современные технические средства позволяют получать информацию без непосредственного подключения к компьютерной системе.

Данные и информация могут быть перехвачены не только в канале связи, но и в помещениях, в которых находятся средства коммуникации. При-

[38] Гасанов Р. М. Шпионаж особого рода. М., 1989.

чём, указанные действия можно осуществлять, находясь на достаточно большом удалении от объекта, который является целью перехвата[39].

Без прямого контакта можно записать на физический носитель электромагнитное излучение, возникающее при функционировании средств компьютерной техники, включая и средства телекоммуникаций. Следовательно, «электромагнитный перехват» можно охарактеризовать как перехват на расстоянии, основанный на установке специального принимающего устройства, которое получает электромагнитные волны на заданной частоте. Если эти волны приняты аппаратурой и переданы на компьютер преступника, он может получить «образ», эквивалентный изображению, возникающему на мониторе «передающего» компьютера, для чего достаточно настроиться на его индивидуальную частоту[40].

При совершении компьютерного преступления с помощью этого метода может использоваться специальная техника, например, сканирующие устройства.

«Кража времени» – незаконное использование компьютерной системы или сети с целью неуплаты или частичной уплаты за их эксплуатацию для удовлетворения собственных потребностей.

Для описания прочих методов несанкционированного доступа и перехвата информации используется следующая специфическая терминология:

«склад без стен» – доступ осуществляется в результате системной поломки, когда нарушается система защиты, например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям базы данных;

«жучок», «клоп», «таблетка» (bugging) – доступ осуществляется при помощи подслушивающего устройства, реализующего один из самых опас-

[39] На Международном конгрессе по вопросам безопасности ЭВМ в Каннах (март 1985 года) впервые был публично продемонстрирован дистанционный перехват информации с дисплея персонального компьютера. Вим-Ван-Эк, являвшийся сотрудником голландской телекоммуникационной компании PTT, продемонстрировал процесс считывания данных с экрана персонального компьютера, установленного на восьмом этаже здания и расположенного в 100 метрах от автомобиля, в котором находилось разработанное им специальное устройство.

[40] Каждый компьютер можно идентифицировать по конкретным параметрам: рабочей частоте, интенсивности электромагнитного излучения и т. д.

ных методов перехвата информации при помощи установки специального прослушивающего устройства с целью фиксирования и записи аудиоинформации, исходящей от целевого объекта – «*аудиоперехват»*. Эти устройства очень трудно обнаружить, так как их маскируют под обычные бытовые приборы и вещи[41];

«аудиоперехват», «снятие информации по виброакустическому каналу» – фиксирование и запись аудиоинформации, исходящей от целевого объекта. Защита от утечки информации по этому каналу очень сложна, и аудиоперехват может проводиться с помощью дорогостоящих лазерных установок, которые способны снимать звуковые вибрации, к примеру, с обычного оконного стекла. Этот метод съёма информации признан одним из наиболее опасных, широко используется профессиональными преступниками, спецслужбами и имеет две разновидности: *заходовую* (заносную) и *беззаходовую.*

Заходовая разновидность заключается в установке подслушивающего устройства в аппаратуру средств обработки информации и различные технические устройства, на проводные коммуникационные линии (радио, телефон, телевизионный кабель, охранно-пожарную сигнализацию, электросеть и т. п.), а также в различные конструкции инженерно-технических сооружений и бытовых предметов, находящихся на объекте, с целью перехвата разговоров работающего персонала и звуковых сигналов технических устройств (определение номера вызываемого абонента АТС и т. п.). Установка аппаратуры на объект возможна тремя способами: скрытное или легендированное проникновение в помещение; внедрение во время постройки или ремонта поме-

[41] Успех в совершении любого преступления зависит от многих факторов, и не последним из них является наличие у преступника современных профессиональных технических средств. Раньше такие средства различными путями ввозили в Россию из-за рубежа, а в настоящее время и этот поток расширился, и доморощенные умельцы без дела не сидят. В первую очередь это касается «жучков», «клопов» и «таблеток» – миниатюрных электронных устройств, способных передавать информацию своему хозяину и активизироваться или замирать по его приказу. Некоторые из этих устройств способны, в случае их обнаружения, даже на совершение «суицида», то есть могут в автономном режиме запускать процедуру немедленного самоуничтожения. Обычно такие устройства тщательно прячутся в различных бытовых предметах, электронной технике, предметах интерьера, подаренных во время переговоров сувенирах, зажигалках, пудреницах, сумках, каблуках, пуговицах, дипломатах и пр. Часто их вмонтируют в системы сигнализации и пожаротушения, линии связи, электропроводку. Дистанционно управляемые и получающие питание от внешних источников, расположенных в служебных или жилых помещениях, они почти не подвержены риску обнаружения и последующей ликвидации, поэтому найти их может лишь квалифицированный специалист, к тому же оснащённый необходимыми техническими средствами.

щения; монтаж в приобретаемые потерпевшей стороной предметы. Обнаружить аппаратуру съёма информации крайне трудно, так как она хорошо маскируется, например, под обычную микросхему.

Беззаходовая разновидность наиболее опасна и заключается в том, что акустические и вибрационные датчики съёма информации устанавливают на инженерно-технические конструкции, находящиеся за пределами охраняемого помещения, из которого принимаются речевые сигналы. При этом необязательно проникать в помещение, так как датчик может устанавливаться на достаточном расстоянии от объекта преступного посягательства[42];

«видеоперехват» – данный метод совершения преступления заключается в действиях, направленных на получение информации путём использования различной видеооптической техники, и имеет две разновидности: *«физический видеоперехват»* и *«электронный видеоперехват».*

Физический видеоперехват, заключается в применении различных видеооптических приборов (подзорные трубы, бинокли, приборы ночного видения и т. п.) с возможностью сохранения добытой информации на физическом носителе. Преступником проводится наблюдение за целевым объектом с расстояния для получения необходимой информации.

Электронный видеоперехват предполагает использование специальных электронных устройств, которые располагают различными каналами связи. Эти устройства состоят из передающих и принимающих устройств. Передающее устройство находится в помещении и передаёт получаемые сигналы на принимающее устройство, которое находится у компьютерного преступника. Этот метод видеоперехвата называется электронным видеоперехватом и предполагает использование преступником цифровых электронных видеока-

[42] Вехов В. Б. Компьютерные преступления: способы совершения, методики расследования. М., 1996.

Кащеев В. И. Специальная техника контроля и защиты информации // Системы безопасности. М., 1995. № 1.

мер, видеомагнитофонов с возможностями длительной записи, оборудования для скрытой видеосъёмки, приборов ночного видения и пр. [43];

«уборка мусора» (scavening) – поиск компьютерным преступником технологических отходов информационного процесса (носителей информации), оставленных пользователем после работы на электронно-вычислительной технике.

Этот метод имеет две разновидности деятельности: *«физическую»* и *«электронную»*.

В физическом варианте он может сводиться к банальному осмотру столов, мусорных корзин, ёмкостей для технологических отходов и сбору оставленных или выброшенных физических носителей информации: дискет с файлами, листингов (распечаток), деловой и служебной документации, переписки и т. д.

Электронный вариант предполагает тщательное исследование оставленных пользователем в памяти компьютера данных в целях получения необходимой информации. Таким образом, могут обследоваться рабочие места программистов с целью поиска каких-либо записей, а также проводиться просмотр стёртых компьютерных программ и данных с целью их восстановления. Служащие, читающие чужие файлы, могут обнаружить там персональную информацию о своих коллегах. Квалифицированный компьютерный преступник может просматривать остаточную информацию, оставшуюся в памяти компьютера или на носителе информации после выполнения сотрудником задания и удаления своих файлов. Кроме того, существуют специальные программы, которые могут частично или полностью восстанавливать данные на компьютере. Компьютерный преступник, используя такую программу, может получить доступ к уничтоженной с точки зрения пользователя необходимой информации. Нужно отметить, что такое происходит из-за ха-

[43] Кащеев В. И. Специальная техника контроля и защиты информации // Системы безопасности. М., 1995. № 1.

латности пользователя, который выполнил не все действия для полного уничтожения данных.

Этот метод широко используется, например, при осуществлении промышленного шпионажа, а также службами противодействия иностранным техническим разведкам с целью установления факта проникновения в информационную систему и уязвимых с точки зрения информационной безопасности мест в информационной системе.

«откачивание данных» (data leakage) – имеет своей целью оценку возможности и сбор информации, необходимой для получения основных данных, в частности, о технологии её прохождения в компьютерной системе;

«следование «за дураком» (pigg backing) – представляет собой несанкционированное проникновение в закрытые, режимные, категорированные зоны – как пространственные, так и электронные – с целью получения противоправного доступа к средствам компьютерной техники. Этот метод рассчитан на низкую бдительность сотрудников организации, а также охраняющих её лиц, и его суть состоит в следующем: если «экипироваться» различными предметами, которые явно связаны с работой на вычислительной технике, и энергично прохаживаться с деловым видом возле запертой двери, где находится компьютерное оборудование, то, дождавшись, например, появления имеющего санкционированный доступ законного пользователя, можно пройти в дверь помещения, за которой находится предмет посягательства, вместе или следом за ним. Правонарушителями чаще всего, в данном случае, являются внутренние пользователи определённой системы. Используя этот способ, компьютерный преступник получает несанкционированный доступ к средствам вычислительной техники путём прямого подключения к ним. Преступление обычно совершается в тот момент, когда отвечающий за работу средств вычислительной техники сотрудник ненадолго покидает рабочее место, оставляя технику в активном режиме работы без соответствующего надзора;

«за хвост» (between the lines entry) – при использовании этого метода компьютерный преступник подключается к линии связи законного пользователя, дожидается сигнала, обозначающего конец работы, перехватывает его «на себя», и, дождавшись, когда последний закончит активный режим работы, осуществляет несанкционированный доступ к компьютерной системе. Технологически этот метод обычно сравнивают с работой двух и более неблокированных телефонных аппаратов, соединённых параллельно и работающих на одном абонентном номере: когда телефон «А» находится в активном режиме, на другом телефоне «В» поднимается трубка, когда разговор по телефону «А» закончен и трубка положена – продолжается разговор с телефона «В»;

«неспешный выбор» (browsing) – целенаправленный поиск и анализ компьютерным преступником слабого места в защите компьютерной системы с целью дальнейшего осуществления многократного несанкционированного доступа к базам данных и файлам законного пользователя. Когда такое место найдено, компьютерный преступник копирует нужную ему информацию на физический носитель. Однажды обнаружив слабое место, постороннее лицо может беспрепятственно считывать и анализировать хранящиеся в системе данные, а также копировать их и возвращаться к ним по мере собственной необходимости. Обычно такой метод используется компьютерным преступником в отношении тех пользователей средств вычислительной техники, которые не уделяют должного внимания регламенту проверки своей системы, предусмотренному методикой защиты компьютерной системы, а назван он так потому, что поиск слабого места проводится долго и очень тщательно;

«поиск бреши» (trapdoor entry) – в отличие от «неспешного выбора» при данном способе компьютерный преступник осуществляет поиск слабых мест в защите компьютерной системы, то есть в компьютерных программах определяются конкретные участки, имеющие ошибки или недочёты в логике, алгоритме построения и т. п., то есть любые ошибки, а затем проводится кон-

курентизация или, иными словами, сравнительный анализ всех обнаруженных слабых мест этой системы с целью осуществления наиболее лёгкого доступа. Обнаруженные однажды «бреши» могут затем многократно использоваться посторонними лицами до тех пор, пока они не будут выявлены и устранены.

Дело в том, что программисты допускают ошибки при разработке программного обеспечения, которые не всегда удаётся обнаружить в процессе отладки программного продукта и такие ошибки впоследствии может обнаружить только высококвалифицированный специалист. Иногда программисты намеренно делают такие «бреши» с целью подготовки совершения преступления. Например, в середине апреля 2000 года корпорация Microsoft официально подтвердила наличие секретного пароля («чёрного хода») на полный доступ к программному обеспечению Microsoft Internet Server, работающему совместно с расширениями из пакета Frontpage 98. Это стало возможным по вине программиста, который заменил определённое имя файла в модуле «dvssr.dll» на фразу «Netscape engineers are weenies», что в мягком переводе означает «Инженеры Netscape – нехорошие люди». При помощи этого кода электронные взломщики могли получать несанкционированный доступ к Web-сайтам, использующим расширения Frontpage 98. Стив Липнер, руководитель центра безопасности Microsoft, заявил, что наличие такого пароля полностью противоречит политике компании, и проводятся мероприятия по выявлению компьютерного злоумышленника. Microsoft также разослала по e-Mail и разместила на своём Web-сайте бюллетень с предупреждением о проблеме. Кроме того, пользователям было рекомендовано незамедлительно удалить из системы файл «dvssr.dll»;

Кстати, об ошибках программистов, которые они допускают при разработке программного обеспечения, создавая, тем самым, компьютерному преступнику условия для несанкционированного проникновения в систему. Эти ошибки (называемые *компьютерными багами* или просто *багами*), обычно представляют собой биты ошибочного компьютерного кода, которые при-

вносят серьёзные проблемы даже в самые известные программные продукты и, несмотря на попытки производителей программного обеспечения искоренить их, они очень распространены.

В своём известном заявлении в начале 2002 года Билл Гейтс (глава компании Microsoft) сделал упор на борьбу с компьютерными багами, и 7 тысяч разработчиков компании в рамках программы улучшения надёжности программного обеспечения получили возможность пройти специальный месячный курс по технологии избавления от багов. Но проблема багов относится не только к Microsoft, она присуща программным продуктам многих фирм-разработчиков, в том числе и таких гигантов программной компьютерной индустрии как Oracle Corporation или производители видеоигр. Фактически каждый пользователь наверняка не раз сталкивался с проблемами, которые могут принести имеющиеся в компьютерных программах ошибки.

Почему же возникают баги? Причины коренятся в природе компьютерного кода и определённых условиях, влияющих на его создание. По словам вице-президента Gartner Group Джона Пескатора программирование – это наука, которая всё ещё развивается. Он сравнивает её с химией: «прошёл не один век, прежде чем люди научились создавать искусственные химические соединения, а ведь они долгое время просто смешивали и взрывали какие-то вещества, методом проб и ошибок». Многие компьютерные программы пишутся, когда нужно быстро решить какую-то конкретную проблему, это, как правило, небольшие программы, в них не так много строк и если и попадаются баги, то они не имеют разрушительного воздействия. Но если это касается серьёзных и больших программ, таких как операционные системы, наподобие Windows XP, состоящей из миллионов строк кода, возможность возникновения багов и сила их возможного отрицательного воздействия многократно возрастают.

Есть примеры таких багов, которые программистам часто просто не под силу устранить, несмотря на то, что у них есть достаточно времени, чтобы проанализировать и проверить код. Например, баг, связанный с перепол-

нением буфера данных, обнаруженный в операционной системе Windows XP и America Online Instant Messenger. Переполнение буфера, как известно, происходит тогда, когда программа пытается разместить в буфере больший объём информации, чем для этого выделено место на жёстком диске компьютера. Правильно написанная программа игнорирует информацию, выходящую за пределы буфера или попытается задействовать дополнительный участок памяти. Но в большинстве случаев программы будут записывать выходящую за пределы буфера информацию на другие участки жёсткого диска компьютера, даже поверх уже имеющихся данных и электронные взломщики используют этот недочёт, чтобы привести атакуемый компьютер к сбою или запустить на нём вредоносную компьютерную программу. Кроме того, причиной неисправленных ошибок в коде служит обычное для программистов желание быстрее дописать программу и выпустить её, а также давление со стороны руководства и устанавливаемые им жёсткие временные рамки. Так, например, происходило в Microsoft, когда приоритетом для программистов было написание большого количества новых дополнительных программ и подпрограмм или создание новых возможностей для уже существующих, тогда как чистоте и надёжности кода не уделялось должного внимания. Теперь же, как мы упоминали выше, усилия руководства компании направлены на изменение этих приоритетов в сторону обеспечения надёжности.

Уоттс Хапри из Carnegie Mellon Software Engineering Institute предложил взять за основу при создании надёжного кода следующий принцип: «лучше с самого начала, с базы писать чистый код, проверять «костяк» программы, чем выискивать и исправлять баги в уже созданной программе». В качестве контраргумента, иногда, говорят, что существуют инструментальные средства для отлавливания программных ошибок, которые могут в считанные секунды проверить миллионы строк компьютерного кода и заметить баги. Однако даже современные специальные тестирующие программы не способны найти многие из программных ошибок, которые может обнаружить

только человек. Следовательно, можно констатировать, что Уоттс Хапри действительно прав.

В прошлом покупатели программного обеспечения не отдавали предпочтения какой-то из программ только потому, что она была известна как «Bug Free» (свободна от ошибок в коде). Но теперь компании-производители программного обеспечения, такие как Oracle Corporation и Microsoft, используют самые разные маркетинговые стратегии, чтобы привлечь внимание клиентов к своим технологиям «очистки» программ от багов; в том числе в рамках этих стратегий осуществляется участие компаний в High-Dependability Computing Consortium, организованного NASA и Carnegie Mellon University. Бывший администратор NASA Дэн Голдин отметил, что надёжность программного обеспечения становится непременным фактором и необходимость обеспечения надёжности программного обеспечения для NASA очевидна, потому что правительство не может допускать провалов космических экспедиций, а частные компании не могут отставать в своих разработках, чтобы обеспечить должный уровень конкурентоспособности, в том числе и с точки зрения повышения эффективности борьбы с компьютерной преступностью за счёт искоренения багов в своих продуктах;

«люк» (trapdoor) – этот метод является как бы продолжением и развитием предыдущего. В найденной «бреши» компьютерная программа искусственно «разрывается», то есть осуществляется так называемый преднамеренный «разрыв программных команд», в него вставляется определённое число команд, которые и направляют деятельность всей системы в нужное для компьютерного преступника русло. По мере необходимости «люк» как бы приоткрывается, и встроенные команды выполняют свою задачу в автоматическом режиме. Таким образом, этот метод основан на использовании скрытого программного или аппаратного механизма, позволяющего обойти методы защиты в системе. Этот механизм активируется некоторым неочевидным образом. Иногда программа пишется таким образом, что специфич-

ное событие, например, число транзакций, обработанных в заранее определённый день, вызовет запуск неавторизованного механизма.

«Люк» часто применяется, например, при совершении хищений денег с электронных банковских счетов;

«маскарад» (masquerading) – в этом случае постороннее лицо, используя различные средства и уловки, проникает внутрь информационной системы, выдавая себя за её легального пользователя. Самый простой путь к проникновению в информационные системы это получение кодов и других идентифицирующих шифров её законных пользователей с помощью подкупа, вымогательства и т. д., либо используя рассмотренный выше метод «компьютерный абордаж». Преступник проникает в компьютерную систему, выдавая себя за законного пользователя, а системы защиты средств компьютерной техники, которые не обладают функциями аутентичной идентификации (по отпечаткам пальцев, рисунку сетчатки глаза, голосу и т. п.), оказываются незащищёнными от этого метода компьютерного преступления;

«мистификация» (spoofing) – используется при случайном подключении «чужой» системы. Компьютерный преступник, периодически формируя правдоподобные отклики, может держать в заблуждении ошибочно подключившегося пользователя в течение какого-то промежутка времени и получать некую полезную для него информацию, например, индивидуальные данные о легальном пользователе этой системы (коды доступа, отклик на пароль и т. д.). Таким образом, этот метод использует знание человеческой психологии, так как пользователь, который подключился к чьей-то системе, обычно уверен, что общается с нужным ему абонентом. Этим и пользуется компьютерный преступник, который старается правильно отвечать на вопросы обманутого им пользователя;

«аварийная ситуация» (emergency situation) – метод, основанный на использовании того обстоятельства, что в любом компьютерном центре имеется особая программа или пакет программ, применяемых как системный ин-

струмент в случае возникновения сбоев или других отклонений в работе эксплуатируемой электронно-вычислительной техники.

Этот метод совершения компьютерных преступлений крайне опасен тем, что для получения несанкционированного доступа в систему компьютерный преступник использует служебные программы, которые находятся на «жёстком» диске компьютера, причём, это такие программы, которым для успешной работы необходим и разрешён непосредственный доступ к наиболее критичным данным.

В силу указанных причин подобные программы при попадании под контроль компьютерного преступника являются очень мощным и опасным инструментом в случае их применения в криминальных целях.

QD – Изменение компьютерных данных:

QDL – логическая бомба;

QDT – троянский конь;

QDV – компьютерный вирус;

QDW – компьютерный червь;

QDZ – прочие методы изменения данных.

Эта группа представляет собой, пожалуй, наиболее «популярные» и распространённые методы совершения компьютерных преступлений. Сюда относятся компьютерные преступления, связанные с использованием методов манипуляции данными и управляющими командами средств вычислительной техники.

Действия компьютерного преступника при этом обычно направлены на изменение или получение данных и достаточно хорошо известны сотрудникам подразделений правоохранительных органов, специализирующихся на борьбе с экономическими преступлениями. Хотя и здесь без курьёзов не обходится. Например, в январе 2001 года выяснилось, что компьютер вполне способен сам по себе успешно выступать в роли компьютерного преступника и решать, как поступать клиентам онлайнового аукциона eBay. Ошибка в системе регистрации пользователей этого аукциона автоматически изменяла

регистрационные данные клиентов компании. Всего с этой проблемой столкнулось около шести миллионов человек! В частности, система самостоятельно отвечала «да» на вопрос «хотите ли вы получать звонки от фирм, занимающихся телефонным маркетингом?». Многие клиенты компании были крайне недовольны создавшейся ситуацией, с критикой eBay выступили и представители Privacy Foundation, обвинившие компанию в «злоупотреблении доверием» своих клиентов.

Изменение компьютерных данных (QD) включает в себя следующие методы компьютерных преступлений.

«Логическая бомба» (logic bomb) – компьютерный вирус, настроенный на изменение компьютерных данных без соответствующей санкции, которое заключается в скрытном встраивании в программное обеспечение набора специальных команд, который должен заработать (или срабатывать каждый раз) при наступлении определённых условий через какой-либо промежуток времени. Далее включается алгоритм программы *«троянского коня»*. Этот метод компьютерные преступники используют, когда уверены, что сложится вполне определённая ситуация. «Логическая бомба» применяется, как правило, из хулиганских побуждений и в целях затруднения поиска компьютерного преступника, кроме того, иногда из тактических соображений хищение удобнее всего совершать при стечении каких-либо обстоятельств, которые обязательно должны наступить. Разновидностью этого метода является *«временная бомба»*.

«Временная бомба», «бомба замедленного действия» (time bomb) – компьютерный вирус, настроенный на срабатывание в определённый, заранее заданный момент времени. Другими словами, это логическая бомба, условием срабатывания которой является наступление определённого времени. Далее включается алгоритм программы *«троянского коня»*.

«Троянский конь» (Trojan horse) – весьма популярный метод совершения компьютерных преступлений, который заключается в изменении компьютерных данных без соответствующей санкции и осуществляется при помо-

щи скрытого введении в чужое программное обеспечение команд (специально созданных компьютерных программ), добавляющих в это программное обеспечение недокументированные свойства, которые позволяют ему выполнять не планировавшиеся владельцем программы функции, вместе с тем, сохраняющие работоспособность оригинального программного обеспечения.

Иными словами, этот метод предполагает, что пользователь не заметит, что компьютерная программа была изменена таким образом, что теперь включает в себя дополнительные функции.

С целью облегчения внедрения «троянского коня» в компьютерные системы преступники, обычно, предусматривают средства его маскировки, например, под известные сервисные программы, утилиты.

«Троянские кони» очень часто применяются в целях хищения денег с электронных банковских счетов. Обычно они используются компьютерными преступниками для отчисления на заранее открытый счёт определённой суммы с каждой операции. Возможен здесь и вариант увеличения преступниками избыточных сумм на счетах при автоматическом перерасчёте рублевых остатков, связанных с переходом к коммерческому курсу соответствующей валюты. Действия такого рода часто совершаются также и сотрудниками, которые стремятся отомстить за несправедливое, по их мнению, отношение к себе, либо оказать воздействие на администрацию организации в корыстных целях[44].

Идентификация в компьютерной системе «троянского коня» представляет собой неординарную задачу, требующую больших затрат различных ресурсов и может успешно проводиться только силами квалифицированных специалистов.

[44] «Из зарубежной следственной практики интересен факт использования “троянского коня” одним американским программистом. Он вставил в программное обеспечение персонального компьютера по месту своей работы команды, которые не выводили на печать для отчёта определённые поступления денежных средств. Эти суммы особым образом шифровались и циркулировали только в информационной среде компьютера. Похитив бланки выдачи денег, преступник заполнял их с указанием своего шифра, а затем проставлял в них определённые суммы денег. Соответствующие операции по их выдаче также не выводились на печать и, следовательно, не могли подвергнуться документальной ревизии». (Мелик Э. Компьютерные преступления. Информационно-аналитический обзор. М., 1999).

В соответствии со статьёй 273 Уголовного кодекса Российской Федерации «троянский конь» подпадает под определение «программы для ЭВМ, приводящей к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети».

Отметим также, что «троянский конь» по своей сути напоминает «люк», но их различие состоит в том, что он не требует непосредственного участия самого компьютерного преступника, программа способна выполнять все зловредные действия в автономном режиме.

«Компьютерный вирус» (computer virus) – это специально написанная компьютерная программа, которая может самопроизвольно «присоединять» себя к другим программам, то есть «заражать» их и при запуске последних выполнять нежелательные действия, размножаться и порождать новые программы для выполнения нежелательных действий на компьютере. Например, вносить изменения и искажения в компьютерные данные или программы, портить файлы и каталоги, уничтожать информацию без соответствующей санкции, переполнять память и создавать помехи во время работы компьютера и т. п.

Существуют и другие определения компьютерного вируса, о которых мы будем говорить ниже. Этот метод совершения компьютерных преступлений без преувеличения не знает себе равных по масштабности и в настоящее время в мире существуют десятки тысяч компьютерных вирусов и их модификаций, которые, тем не менее, можно классифицировать, разбив их на группы, а по задуманному и реализованному компьютерным преступником алгоритму работы вируса можно судить о том, насколько он профессионален. Более того, «троянских коней», также как и «компьютерных червей» (см. ниже) в определённом смысле можно считать логической модернизацией компьютерных вирусов, а всех их вместе взятых правомерно отнести к единой категории «вредоносных компьютерных программ».

Между прочим, нетерпеливый читатель может заглянуть в соответствующую главу этой книги, чтобы поближе познакомиться с указанной классификацией вредоносных компьютерных программ.

Нужно иметь в виду, что метод совершения компьютерного преступления посредством инфицирования компьютерным вирусом может применяться как самостоятельно, так и в сочетании с иными методами. В этом случае данный метод используется в качестве камуфлирующего фактора с целью сокрытия следов преступления.

Между прочим, инфицирование электронно-вычислительной техники компьютерным вирусом и последующая ликвидация или лечение от этого вируса (кстати, должно быть абсолютно ясно, что избавиться от компьютерного вируса гораздо сложнее, чем своевременно применить действенные профилактические меры), имеют ряд черт, свойственных медицинской практике. По крайней мере, используемая терминология весьма близка медицинской, и об этом мы ещё будем говорить более подробно. Здесь же отметим, что весьма полезной процедурой является резервирование, которое представляет собой одно из основных средств защиты от компьютерных вирусов: копирование FAT (File Allocation Table – Таблица размещения файлов), ежедневное ведение архивов изменённых файлов и пр. Программные методы защиты при помощи антивирусного программного обеспечения, например, не могут заменить ежедневное резервирование, хотя и повышают общий уровень защиты;

В общем случае компьютерные вирусы представляют собой крайне неприятное явление и могут использоваться в различных целях.

Например, в апреле 2001 года британский бизнесмен чтобы нанести ущерб своему конкуренту преднамеренно отправил по электронной почте компьютерный вирус своему конкуренту. За что и был, впоследствии, приговорён судом к 175 часам общественных работ и конфискации компьютерного оборудования.

Пол Брогден, 27-летний владелец компьютерной фирмы «Sure Computers» после продолжительной войны цен со своим основным конкурентом Колином Бэглоу, которому принадлежит фирма «Complete Computers», не нашёл ничего лучшего, как послать своему злейшему врагу по электронной почте компьютерный вирус. Брогден отправил ему письмо с вложенным файлом и заголовок этого сообщения гласил: «Наши последние цены – во вложении, взгляните, пожалуйста». Но персонал «Complete Computers» оказался бдительным, при проверке компьютерный вирус в письме был обнаружен, и фирма обратилась с заявлением в полицию. На суде Брогден в своё оправдание заявил, что конкурент обеспечивал себе выгодные цены, используя нелицензионное программное обеспечение. Судья, однако, посчитал поступок Брогдена «единичной ребяческой выходкой» и назначил упомянутое выше наказание. «Если бы я думал, что имелись более серьёзные намерения, то наложил бы более жёсткое наказание в виде лишения свободы», – добавил судья при объявлении приговора.

Компьютерные вирусы могут распространяться также и по причине «недоразумений».

В конце апреля 2001 года Microsoft призналась в заражении Win32-вирусом «FunLove»[45] Web-сайтов своих основных партнёров, имеющих статус «Premier Support» и «Microsoft Gold Certified Partners». Microsoft выпустила предупреждение о вирусной опасности, которая угрожала её главным партнёрам и, по своей сути, это предупреждение явилось признанием своей вины в том, что различные файлы «заплатки», размещённые на Web-сайтах главных партнёров корпорации, могли быть инфицированы Win32-вирусом «FunLove». В этом заявлении также говорилось, что примерно на две недели «в порядке защиты клиентов» всем партнёрам будет приостановлен доступ на Web-сайты Microsoft для перекачивания определённых файлов.

[45] Win32-вирус «FunLove» впервые был обнаружен в «диком виде» в ноябре 1999 года. Он представляет собой резидентный паразитический Win32-вирус, который работоспособен под операционными системами Windows 95/98/NT. Вирус заражает PE exe-файлы (выполняемые файлы Windows) на локальных и сетевых дисках. Благодаря своей способности размножаться по локальной сети, вирус может инфицировать всю корпоративную сеть с одной рабочей станции, если ей предоставлены права записи на сетевые диски.

В декабре 2001 года сотрудник компании Cisco Systems Энди Ли принес свои извинения за массовую рассылку писем, инфицированных Интернет-червём «Goner», тысячам системных администраторов.

Заражённые сообщения были отосланы подписчикам, внесённым в список рассылки Североамериканской группы сетевых операторов (North American Network Operators Group – NANOG). Подписчики мгновенно отреагировали на попытку заразить их компьютеры вредоносной программой. Так один из них в письме, адресованном Cisco Systems, написал: «Это чрезвычайно грустный день, когда служащий Cisco пытается заразить подписчиков NANOG опасным вирусом». «Хотелось бы надеяться, что любой сотрудник любой компании (а тем более Cisco), будет заботиться о защите от нового вируса в течение 24 часов после его появления, а не неделю спустя», – заявил другой участник рассылки. Сам же Ли прокомментировал ситуацию следующим образом: «Я не понимал, что система была инфицирована компьютерным вирусом до тех пор, пока не заметил в своём MS Outlook тысячи сообщений о заражении». «Чрезвычайно сожалею о приключившемся хаосе...», – добавил ответственный сотрудник Cisco Systems.

Интересно, что в качестве антивирусной защиты Cisco Systems использовалось антивирусное программное обеспечение McAfee VirusScan и, более того, базы данных этого продукта своевременно обновлялись!

В январе 2002 года подписчики новостей SiliconValley.com получили опасный вирус «Magistr», который был по ошибке разослан с Web-сайта компании вместе с ежедневной почтовой рассылкой «Good Morning Silicon Valley». В тот же день вечером SiliconValley.com принесла извинения подписчикам, объяснив подобную ошибку злым умыслом компьютерного преступника, атаковавшего один из серверов компании. Заражённые письма с темой «If the hyperlinks in your documents» рекомендовалось уничтожить. В тоже время, независимые эксперты предположили, что, возможно, причиной рассылки компьютерного вируса «Magistr» стал не целенаправленный взлом Web-сайта, а случайное заражение.

В июне 2002 года, как сообщалось на Web-сайте The Inquirer, британский дистрибьютор West Coast в массовом порядке рассылал собственным клиентам сообщения, содержащие компьютерный вирус. Одна из жертв массовой рассылки обратилась в The Inquirer, полагая, что «может быть, публикация в средствах массовой информации остановит вирусный поток, непрекращающийся уже в течение двух дней подряд». В сообщениях, рассылаемых West Coast, содержался давно известный компьютерный вирус «Gokar», который рассылает себя по контактам в адресной книге MS Outlook, используя различные варианты имён приложенных файлов, тем сообщения и содержимого письма. Заражённый вирусом файл, как правило, имеет расширение «*.pif», «*.scr», «*.com», «*.bat» или «*.exe».

Буквально через пару недель аналогичному бедствию подверглась компания Microsoft. Сотрудники софтверного гиганта сообщили об обнаружении компьютерного вируса «Nimda» в составе дистрибутива среды разработки Visual Studio.Net. В итоге было срочно выпущено специальное обновление для корейской версии VS.Net, в которой и была обнаружена вредоносная программа.

Компьютерные вирусы могут стать и причиной возникновения поистине скандальных ситуаций.

В ноябре 2000 года произошёл скандал из-за несовместимости новой версии антивирусной программы McAfee со старым сканирующим программным обеспечением, используемым при проверке компьютера. Указанная несовместимость вызывала сбой работы операционной системы MS Windows.

Принято считать, что программы, сканирующие компьютер в поисках вируса одно из наиболее эффективных средств в борьбе с компьютерными вирусами, однако Network Associates подтвердила, что в последней версии файла VirusScan компании McAfee (подразделение Network Associates) содержится программная ошибка, которая вызывает зависание операционной системы MS Windows при её запуске пользователем. Проблема заключалась

в несовместимости обновлённого программного обеспечения, предназначенного для лечения заражённых компьютерным вирусом ресурсов, со сканирующим «движком» VirusScan. Тем из пользователей кто столкнулся с этой проблемой, рекомендовалось перезагрузить MS Windows в режиме «Защиты от сбоев» и убрать функцию автозапуска системы VirusScan. Приятная перспектива для неопытного пользователя, который заплатил за обновление свои «кровные» и знать не желает, где у компьютера системный блок, не говоря о функции автозапуска программного приложения.

В мае 2001 года крепко поссорились две антивирусные компании: английская – Sophos и американская – McAfee.

Как сообщала Sophos, ранним утром девятого мая компания выпустила предупреждение о вирусной опасности, касающееся Интернет-червя «Homepage» (также известного под именем VBS/VBSWG-X). Но, вскоре начались загадочные вещи: служба технической поддержки Sophos оказалась завалена множеством запросов от пользователей другой антивирусной компании – McAfee с претензиями, что e-Mail предупреждения о вирусе от Sophos сами были заражены вирусом «VBS/VBSWG.gen@mm» (так McAfee называет «Homepage»). В пресс-релизе Sophos заверила своих клиентов, что не рассылала им никаких компьютерных вирусов, а также дополнительно сообщила, что компания McAfee официально подтвердила – их продукт иногда ошибочно определяет вирус там, где его нет и в помине. В заключение Sophos рекомендовала пользователям, пострадавшим вследствие возникшей неразберихи, связываться со службой поддержки компании McAfee и просить помощи у них.

В январе 2003 года в буквальном смысле слова оскандалилась скандинавская компания по компьютерной безопасности Norway's Data Inspectorate, которая признала, что в её сообщениях с рекомендациями по обеспечению компьютерной безопасности (!) содержался Win32-вирус «FunLove». Как оказалось, компьютерный вирус проник во внешний почтовый сервер и, воспользовавшись данными контактного листа, начал немедленно распростра-

нять себя по адресатам, в результате чего был разослан более чем 1700 подписчиков Norway's Data Inspectorate. После того как стало известно о произошедшем, специалисты службы безопасности Norway's Data Inspectorate сразу же выключили систему рассылки сообщений. Однако было уже поздно – вирус разослал себя по всем адресам.

«Компьютерный червь» – вредоносная компьютерная программа, которая нацелена на проникновение в компьютерные системы без законного на это права путём передачи, внедрения и самостоятельного распространения своих копий по компьютерной сети. Чтобы были более понятны специфика данного определения и, соответственно, различие компьютерных вирусов, «троянских» программ и «червей», приведём их основные свойства в виде табл. В6.

Таблица 6

Характерные черты
компьютерных вирусов, «троянских» программ и «червей»

	Вирус	**Троянская программа**	**«Червь»**
Инфицирование файлов	Да	Нет	Нет
Самостоятельное распространение	Нет	Нет	Да
Вредоносная «начинка»	Может быть	Всегда	Может быть

Обычно, когда нет необходимости в точном разграничении, все три вида вредоносных компьютерных программ, указанных в табл. В6, обозначают одним термином – «компьютерный вирус». Это общепринятая в мире практика.

На самом деле «черви» и «троянские» программы не являются компьютерными вирусами, и не относятся к какому-либо их типу. «Троянские» программы, например, всегда содержат вредоносную «начинку», но не могут распространяться, за исключением того случая, когда пользователи выполняют операцию копирования файла с «троянской» программой. «Черви» самостоятельно распространяются среди электронно-вычислительной техники без уведомления пользователя и могут содержать вредоносную «начинку».

«Черви» и «троянские» программы не инфицируют файлы. В последнее время именно «черви» и «троянские» программы становятся всё более «популярными», например, в качестве средства открывающего «чёрный ход» («люк») внутрь компьютера-жертвы через сеть, включая и Интернет.

Таким образом, компьютерные вирусы, «троянские» программы и «черви» это близкие родственники, но не братья близнецы. Причём, старшим поколением среди вредоносных компьютерных программ следует признать компьютерный вирус, а «черви» и «троянские» программы могут претендовать на роль сводных братьев.

Впрочем, более подробно об этих вредоносных компьютерных программах и их разновидностях мы поговорим несколько позже, а здесь давайте приведём пример «червя».

Второго марта 2001 года знаменитая и весьма уважаемая во всём мире японская компания Pioneer Corporation продемонстрировала в «редчайшую заботу» о своих многочисленных клиентах, разослав более чем 10 тысячам из них знаменитого, но чрезвычайно противного Интернет-червя «Hybris». Инцидент произошел средь бела дня – ровно в 16:00, когда компания Pioneer Corporation по электронной почте запустила рассылку новостных писем своим подписчикам. В результате 10758 подопытных кроликов… извините, пользователей, получили сообщение, инфицированное вышеупомянутым Интернет-червём «Hybris».

Как сказал по ещё не остывшим следам событий представитель Pioneer Corporation, только через час после проведения рассылки компания поняла, что произошло, так как несколько возмущённых пользователей без излишних слов благодарности незамедлительно вернули полученный ими «подарок», на полную катушку использовав при этом возможности своих компьютеров, современных информационных технологий и хорошо известный принцип «бумеранга».

Надо отдать должное, но уже на следующее утро и повторно 12 марта, Pioneer Corporation принесла официальные извинения своим клиентам и пре-

дупредила тех из них, кто ещё не понял, что их компьютеры, возможно, заражены Интернет-червём «Hybris». По сообщениям самой компании, несмотря на массовый характер рассылки, по настоящему пострадало только несколько десятков подписчиков.

QF – Компьютерное мошенничество:

QFC – мошенничество с банкоматами;

QFF – компьютерная подделка;

QFG – мошенничество с игровыми автоматами;

QFM – манипуляции с программами ввода-вывода;

QFP – мошенничества с платёжными средствами;

QFT – телефонное мошенничество;

QFZ – прочие компьютерные мошенничества.

Компьютерные мошенничества (QF) объединяют в своем составе разнообразные методы совершения компьютерных преступлений.

«Мошенничество с банкоматами» – компьютерные преступления, связанные с хищением наличных денег из устройств их выдачи в автоматическом режиме.

«Компьютерная подделка» – все разновидности мошенничества и хищения из компьютерных систем, осуществляемые при помощи создания поддельных устройств и носителей специальной информации (карточек и пр.).

«Мошенничество с игровыми автоматами» – мошенничества и хищения, связанные с использованием в качестве объекта преступления игровых автоматов различной конструкции. Они могут осуществляться и самими владельцами игровых автоматов с целью обналичивания денег или «отмывания» криминальных доходов.

«Манипуляции с программами ввода-вывода» – мошенничества и хищения посредством неверного ввода или вывода в компьютерные системы или из них при помощи манипуляции программами.

В этот метод компьютерных преступлений включается метод *подмены данных,* который является простым и, поэтому, часто применяемым способом

совершения компьютерных преступлений. В частности, данный метод применяется для приписывания счёту «чужой» истории, то есть производится модификация данных в автоматизированной системе банковских операций, приводящая к появлению в системе сумм, которые реально на данный счёт не зачислялись. Например, оператор, используя удалённый терминал, вводит фиктивный запрос в компьютер на получение 10 тысяч долларов по процентам и затем удаляет все записи об этой транзакции.

В метод *«манипуляции с программами ввода-вывода»* включается также и метод *подмены данных кода* (data diddling code change), который обычно осуществляется при вводе-выводе данных. При применении данного метода при вводе, например, документы могут быть заменены на фальшивые, вместо рабочих дискет подложены посторонние, и данные, таким образом, будут сфальсифицированы. Это простейший, не требующий технических знаний и относительно безопасный метод. И именно поэтому он очень часто применяется для совершения компьютерных преступлений.

«Мошенничества с платёжными средствами» – все компьютерные мошенничества, связанные с платёжными средствами. Большой ущерб может быть нанесён, например, при доставке заказа на оборудование от федерального правительства. В этом случае готовятся фиктивные реквизиты для счёта, направленного в центр автоматизированной обработки данных. В этих реквизитах указывается адрес реальной организации, которая в действительности выполняет государственные заказы, но перед самой доставкой, один из компьютерных преступников звонит в эту организацию и предупреждает о якобы произошедшей «ошибке», а потом доставляет оборудование своим соучастникам.

«Телефонное мошенничество» (telephone fraud, wire fraud) – доступ к телекоммуникационным услугам путём посягательства на протоколы и процедуры компьютеров, обслуживающих телефонные системы.

«Воздушный змей» – для реализации этого метода в простейшем случае необходимо открыть в двух банках по небольшому счёту. Далее деньги пере-

водятся из одного банка в другой и обратно с постепенно повышающимися суммами.

Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк, так, чтобы общая сумма покрывала требование о первом переводе. Этот цикл повторяется большое число раз до тех пор, пока на счёте не оказывается приличная сумма (фактически, она постоянно «перескакивает» с одного счёта на другой, увеличивая свои размеры), после чего деньги снимаются, и владелец счетов скрывается.

Этот метод совершения преступления требует очень точного расчёта и без компьютера его можно осуществить только для двух банков. На практике, в такую игру включают большое число банков – так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты, но управлять этим процессом можно только с помощью современной вычислительной техники.

«Салями» (salami) – метод, при котором компьютерное преступление совершается понемногу, небольшими частями, настолько маленькими, что они фактически незаметны.

Этот метод совершения преступления стал возможным лишь благодаря использованию компьютерной технологии в бухгалтерских операциях, основан на быстродействии средств компьютерной техники и, обычно, сопровождается внесением изменений в компьютерные программы. К примеру, платежи могут округляться до нескольких рублей или центов, и разница между реальной и округлённой суммой поступать на специально открытый подставной счёт – результат округления на профессиональном бухгалтерском языке называется «салями».

С точки зрения преступников, это один из простейших способов совершения преступления. Он используется, как правило, при хищении денежных средств в тех бухгалтерских операциях, где перечисляются дробные (меньше, чем одна минимальная денежная единица) сумма денег с каждой

операции, так как в этих случаях всегда делается округление сумм до установленных целых значений. Ставка компьютерных преступников делается на то, что при каждой проверке потерпевший теряет очень мало и это практически не фиксируется документально. Или, к примеру, узнав о смерти вкладчика, оператор информационной системы по приёму платежей открывает счёт в банке, используя имя клиента, другие его персональные данные и реквизиты. Вкладчик не удаляется из списка клиентов, на счета которых начисляются проценты, с помощью компьютерной системы заменяется его адрес и запрашивается прямой перевод процентов на счёт, открытый самим оператором.

Ну, что же, как говорится: «Курочка по зёрнышку клюёт…»

В завершение приведём два случая компьютерного мошенничества, в которых были замешаны сотрудники корпорации Microsoft.

Один из служащих корпорации Microsoft нанёс ей ущерб в размере более 9 млн. долларов. Инженер среднего уровня Даниэл Фосснер, участвующий в разработке систем распознавания речи, был арестован в декабре 2002 года по обвинению в компьютерном мошенничестве. Согласно судебным документам, Фосснер заказывал на своё имя серверные продукты Microsoft, после чего сбывал их на стороне по более высокой цене.

Проворовавшийся программист проходил по статье, в результате применения которой может назначаться наказание в виде лишения свободы минимум на 5 лет и выплаты штрафа в размере 250 тыс. долларов за каждый факт обмана компании, а таковых эпизодов накопилось целых пятнадцать. Однако правосудию не суждено было свершиться, так как Фосснер умер в 2003 году – до суда – в тюремной больнице.

23 июня 2003 года бывший сотрудник Microsoft был арестован по подозрению в том, что он заказал по льготной внутренней цене корпорации программные продукты более чем на 17 млн. долларов, а затем продавал их, присваивая себе разницу. Дело сорокатрёхлетнего Ричарда Грэга также включает еще 62 эпизода мошенничества, связанного с компьютерами и Интернет. Как утверждает обвинение, Грэг заказал с января по декабрь 2002 го-

да 5436 программных продуктов по оптовой цене и затем спекулировал ими. Следствие вели ФБР США и прокуратура Западного округа Вашингтона. Грэг, отказавшийся признать себя виновным, был уволен из Microsoft в декабре 2002 года, где был координатором проекта по разработке операционной системы Windows XP, и именно это стало причиной введения в конце 2002 года более строгой системы предотвращения краж в компании. «Когда в конце декабря мы узнали о том, что происходит, то немедленно предприняли меры для предотвращения повторения этого и сообщили о Грэге правоохранительным органам, – сказал финансовый директор Microsoft Джон Коннорс, который также осуществляет надзор за состоянием внутри корпорации, – С этого времени мы очень тесно сотрудничали с ФБР США и прокуратурой и ввели изменения в нашу систему внутренних заказов».

Компания Microsoft провела следствие и ввела новую систему борьбы с нарушениями внутренней политики компании после увольнения и ареста в 2002 году упоминавшегося нами выше менеджера Фойснера.

QR – Незаконное копирование:

QRG – компьютерные игры;

QRS – прочее программное обеспечение;

QRT – топография полупроводниковых изделий;

QRZ – прочее незаконное копирование.

Компьютерный преступник незаконно копирует информацию на свой физический носитель, а затем использует её в своих корыстных целях. Этот метод достаточно распространён из-за своей сравнительной простоты, например, для того чтобы выполнить контракт на разработку какой-либо компьютерной программы, исполнитель копирует нужную ему программу из постороннего источника и выдаёт её за свою собственную разработку, требуя с заказчика оговорённый в договоре гонорар за фактически не проделанную работу.

Незаконное копирование информации (QR) включает следующие методы компьютерных преступлений.

«Копирование компьютерных игр» – незаконное копирование, распространение или опубликование защищённых законом программных кодов компьютерных игр.

«Прочее программное обеспечение» – незаконное копирование, распространение или опубликование защищённого законом программного обеспечения за исключением программных кодов компьютерных игр.

«Топография полупроводниковых изделий» — незаконное копирование топографии полупроводниковых изделий: копирование защищённой законом топографии полупроводниковых изделий, коммерческая эксплуатация или импорт с этой целью топографии или самого полупроводникового изделия, произведённого с использованием данной топографии без законного права на указанную деятельность.

В конце ноября 2000 года федеральные власти США арестовали Питера Морча, бывшего инженера Cisco Systems, по обвинению в краже при помощи незаконного копирования находящихся в разработке документации и чертежей продукции компании.

Морч уволился из Cisco Systems в октябре 2000 года и устроился на работу в конкурирующую компанию – Calix Networks. Он не обвиняется в попытке злонамеренного использования похищенной информации, часть данных является его собственными разработками и, по мнению адвоката Дэна Бэртона, ведущего аналогичное дело другого бывшего сотрудника Cisco Systems, компания таким образом расправляется с теми, кто ушёл работать в конкурирующие фирмы, а факт копирования собственных разработок при увольнении довольно распространён в среде программистов Силиконовой долины. Обвиняемый Морч был отпущен под залог в 100 тысяч долларов, и ему грозило до 10 лет тюремного заключения и 250 тысяч долларов штрафа.

<u>QS – Компьютерный саботаж:</u>

QSH – саботаж с аппаратным обеспечением;

QSS – саботаж с программным обеспечением;

QSZ – прочие методы саботажа.

Компьютерный саботаж (QS) составляют следующие виды преступлений.

«Саботаж с аппаратным обеспечением» – нарушение работы вычислительной техники с использованием аппаратного обеспечения: ввод, изменение, стирание, подавление компьютерных данных или программ; вмешательство в работу компьютерных систем с намерением помешать функционированию компьютерной или телекоммуникационной системы.

«Саботаж с программным обеспечением» – нарушение работы вычислительной техники с использованием программного обеспечения: стирание, повреждение, блокирование информации, ухудшение или подавление компьютерных данных или программ без законного права на осуществление этого вида деятельности.

В июле 2000 года 19-летний студент Фрэнк де Граф стал участником «культурного саботажа» в Интернет. Он решил инвестировать деньги в Интернет, но заработанные за лето 200 долларов вложил в совершенно необычный ресурс под названием RTMark.com. В обмен на вложенные деньги его пригласили стать участником организации, которая занимается «культурным саботажем». На счету RTMark.com масса довольно экстравагантных проектов: продажа «антисувениров» – игрушек для туристов, намекающих на различные социальные проблемы, отключение голосовых чипов в куклах «Барби», создание Web-сайта Gatt.org, являющегося пародией на деятельность Всемирной торговой организации (WTO). RTMark также выступила в защиту маленького швейцарского арт проекта www.etoy.com, у которого Интернет-магазин eToys пытался отсудить домен.

Десять тысяч членов организации провели электронную атаку под названием «отказ в обслуживании» на сервер eToys. Они одновременно начали посылать запросы в указанный Интернет-магазин, вызвав тем самым резкое повышение трафика и, соответственно, нагрузку на Web-сервер этого магазина. В результате потенциальные покупатели Интернет-магазина eToys получали, например, уведомления о невозможности оформления их заказа,

что, естественно, наносило финансовый и моральный ущерб владельцам электронного магазина. Действие явно противоправное, но, как ни странно, в конечном счёте, домен всё-таки остался у арт проекта, а eToys пришлось даже выплатить 40 тысяч долларов, чтобы покрыть судебные издержки по собственному же иску.

Сам же де Граф признался, что очень рад найти в RTMark столько единомышленников. Что движет членами столь необычной организации не совсем понятно, хотя в Интернет действительно есть много людей, которых не устраивает существующий порядок вещей, и которые хотели бы его полностью изменить.

«Суперотключение» – название метода присвоено по имени компьютерной программы, использовавшейся в ряде вычислительных центров, обходившей системные меры защиты и использовавшейся при аварийных ситуациях.

Владение таким «мастер ключом» даёт возможность в любое время получить доступ к компьютеру и находящейся в нём информации.

QZ – Прочие компьютерные преступления:

QZB – использование компьютерных досок объявлений;

QZE – хищение информации, составляющей коммерческую тайну;

QZS – передача информации конфиденциального характера;

QZZ – прочие компьютерные преступления.

К прочим методам (QZ) в классификаторе отнесены следующие компьютерные преступления.

«Использование компьютерных досок объявлений» – использование электронных досок объявлений (BBS) для хранения, обмена и распространения материалов, имеющих отношение к преступной деятельности.

«Хищение информации, составляющей коммерческую тайну» – приобретение незаконными средствами или передача информации, представляющей собой коммерческую тайну, без права на то или другого законного обос-

нования, с намерением причинить экономический ущерб или получить незаконные экономические преимущества.

Обычно продаётся персональная информация, информация об условиях контракта, и конфиденциальная информация о деятельности компании (например, технология создания продукции или конкретного продукта) посторонним лицам, либо копируются и используются программы для личной выгоды. Этот вид компьютерных преступлений до последнего времени был достаточно редким для России.

Интересно, что сюда можно отнести и «традиционные» методы совершения преступлений, в которых действия преступника направлены на изъятие чужого имущества в виде средств вычислительной техники или носителей информации. Поэтому, с уголовно-правовой точки зрения подобные преступления квалифицируются соответствующими статьями Уголовного кодекса Российской Федерации как обычное хищение ценного имущества. Характерной отличительной чертой данного метода совершения преступлений является то обстоятельство, что в них средства компьютерной техники всегда выступают только в качестве предмета преступного посягательства, а в качестве орудия совершения преступления используются иные инструменты, технические устройства и приспособления, не являющиеся средствами компьютерной техники[46]. Противоправное изъятие различных физических носителей информации (магнитных лент и дисков, оптических и магнитооптических дисков, электронных кредитных карточек, электронных акций, услуг и т. п.) также всегда выступает только в качестве предмета преступного посягательства.

В апреле 2000 года 29-летний Сэй Лай Оу из Малайзии, бывший сотрудник Intel, был обвинён в хищении коммерческих секретов этой компании. Кража коммерческих секретов Intel касалась её будущего процессора Itanium, как говорилось в обвинении, Сэй Лай Оу похитил документы и компьютерные файлы, посвящённые устройству и процедурам испытаний про-

[46] Гасанов Р. М. Шпионаж и бизнес. М., 1992.

цессора. По законам США за это деяние предполагается тюремное заключение до 30 лет и штраф до 1,5 млн. долларов.

В мае 2000 года бывший служащий компании Cisco Systems был осуждён жюри присяжных в Верховном суде г. Санта Клара (США) по обвинению в хищении информации, представляющей коммерческую тайну, которая оценивается в миллиарды долларов.

Дэвид Хоукинс был признан виновным в краже перед своим увольнением исходного кода продукта Cisco Systems под названием Private Internet eXchange (PIX). Хоукинс устроился на работу в Cisco Systems примерно за год до того, как она приобрела Translation Network Inc. (TNI), после чего работал в TNI после слияния компаний. По словам поверенного представителя района Хоукинс никогда лично не участвовал в разработке PIX и после увольнения открыл собственное дело. От своего имени он продвигал на рынок аналогичный PIX товар, под названием «Aegis», который представил на крупнейшей торговой выставке в Лас-Вегасе. На его беду одним из посетителей выставки оказался основатель TNI Джон Мэйс. Демонстрация Хоукинса вызвала подозрение из-за необычного подобия «Aegis» и программного обеспечения, принадлежащего Cisco Systems. Компания оценила свой продукт в 2 млрд. долларов, начала внутреннее расследование и обнаружила достаточно фактов, чтобы обратиться к районному прокурору. Двумя месяцами позже полиция провела санкционированный обыск на квартире Хоукинса и обнаружила две версии оригинала исходного кода PIX на жёстком диске его компьютера. По законам США это деяние предполагает до 3-х лет тюремного заключения.

«Передача информации конфиденциального характера» – использование компьютерных систем или сетей для несанкционированного хранения, обмена, распространения или перемещения информации конфиденциального характера.

В августе 2000 года компания Apple Computer подала в суд на неизвестное лицо[47], опубликовавшее на Web-сайте в Интернет её коммерческие секреты, которое обвинялось в разглашении коммерческой тайны посредством Глобальной сети. Суть дела заключалась в том, что некий компьютерный злоумышленник опубликовал на Web-сайте фотографии двухпроцессорного компьютера PowerMac, а также новой мыши. Помимо этого им была опубликована информация и о других продуктах компании, которые не были анонсированы. В своём иске компания Apple Computer потребовала как запрета дальнейшей публикации подобных материалов, так и компенсации за причинённый материальный и моральный ущерб.

В том же августе 2000 года Федеральные агенты арестовали во Флориде сотрудника компьютерной фирмы Майкла Пителиса. Он был арестован за попытку вымогательства и разглашения информации конфиденциального характера, так как посылал в софтверную компанию Parametric Technology письма с угрозами опубликовать в Интернет пароль, позволяющий пользоваться программным обеспечением этой фирмы бесплатно. За неразглашение этих данных Пителис требовал миллион долларов. Федеральные агенты проследили Пителиса до публичной библиотеки, откуда он выходил в Интернет, и арестовали его. Компьютерный шантажист подпадает под наказание в виде 20 лет тюрьмы и штраф в размере 250 тысяч долларов. Как отметил федеральный прокурор Доналд К. Стерн, «Интернет представляет множество новых возможностей для преступных действий, и данный случай показывает, что некоторые законы требуют серьёзного пересмотра».

В дополнение к уже приведённым методам некоторые специалисты по компьютерной преступности в особую группу выделяют методы, которые имеют следующие специфические названия.

[47] На момент подачи иска Apple Computer не смогла установить личность человека, который был виновен в утечке коммерческих секретов компании, и воспользовалась своим правом обращения в суд с обвинением «неизвестного лица». Однако в дальнейшем, в результате проведённого служебного расследования, злоумышленник был найден – им оказался один из сотрудников компании Apple Computer, недовольных своим руководством.

«Асинхронная атака» (asynchronous attack) – состоит в смешивании и одновременном выполнении компьютерной системой команд двух или нескольких пользователей. Этот способ основан на совмещении команд двух или нескольких пользователей, чьи программы компьютер выполняет одновременно. Для правильного понимания этого метода совершения компьютерных преступлений необходимо знать, что такое операционная система[48]. Компьютерный преступник-профессионал в своём «деле» может внести соответствующие изменения и дополнения в операционную систему, чтобы заставить работать её в своих целях. Причём заметить такие изменения и дополнения достаточно сложно, а привнесённый извне в операционную систему программный код будет выполняться параллельно с командами пользователя.

«Моделирование» (modeling) – этот метод совершения компьютерных преступлений всё чаще используется компьютерными преступниками и представляет собой копирование поведения какого-либо устройства или системы с помощью специального программного обеспечения. Например, ведение так называемой двойной бухгалтерии, когда в одно и тоже время функционируют две бухгалтерские программы, одна из которых работает в легальном режиме, а другая – в незаконном для проведения «теневых» операций. Обычно компьютерными преступниками моделируется либо среда, область деятельности в которую они собираются вторгнуться, либо конкретный метод совершения преступления, который затем может быть использован для проникновения в систему.

«Имитационное моделирование» (simulation modeling) – является разновидностью моделирования и используется как для анализа процессов, в которые компьютерные преступники хотят вмешаться, так и для отбора мето-

[48] Операционная система – это комплекс программных средств, обеспечивающих управление информационными процессами во время функционирования компьютерной системы. Основной задачей операционной системы является обеспечение максимальной производительности компьютера, а функциями – управление, коммуникация, планирование и т. д. Поэтому, этот комплекс программ имеет сложную структуру и состав, а также большие размеры. Разработкой операционных систем занимаются профессиональные группы программистов иногда в течение нескольких лет и, следовательно, операционную систему практически невозможно проверить на полную работоспособность.

дов совершения преступления при помощи компьютера. Таким образом, осуществляется «оптимизация» самого метода совершения преступления.

«Реверсивная модель» (reverse model) – является разновидностью моделирования, и существо метода заключается в том, что создаётся модель конкретной системы, которая намечена в качестве «жертвы» электронной атаки. В эту модель вводятся реальные исходные данные и учитываются планируемые действия. Исходя из полученных данных, подбираются желаемые результаты, а потом модель совершения компьютерного преступления прогоняется обратно к исходной точке, и становится ясно, какие действия нужно проводить с входными и выходными данными, чтобы достичь желаемого результата. В принципе, прокручивание модели «вперёд-назад» может проходить не один раз, чтобы посредством нескольких итераций добиться желаемого результата и, в итоге, остаётся только осуществить задуманное.

«Манипулирование с пультом управления» (manipulation with console) – относится к злоупотреблениям механическими элементами управления компьютера, краткое описание которых заключается в том, что в результате механического воздействия на технические средства электронно-вычислительной машины создаются необходимые условия для манипуляции данными.

Иногда, специалисты выделяют также группу методов совершения компьютерных преступлений, которые позиционируются ими в качестве вспомогательных по отношению к основным, приведённым выше.

«Преодоление программных средств защиты» – представляет собой умышленное преодоление компьютерным преступником системы защиты программными средствами и имеет несколько разновидностей:

«создание копии ключевой дискеты» – для запуска некоторых систем необходима ключевая дискета, на которой записаны системные файлы и компьютерный преступник, получая возможность незаконного создания копии такой дискеты, затем, с её помощью проникает в нужную компьютерную систему;

«модификация кода системы защиты» – внося изменения в этот код, компьютерный преступник обходит систему защиты компьютерной системы. Этот метод может быть реализован на практике только квалифицированными программистами, которые обладают достаточным опытом в указанной области деятельности, а время, необходимое для выполнения успешного обхода системы защиты, может составлять несколько недель[49];

«использование механизма установки (снятия) программных средств защиты информации» – некоторые программные средства защиты устанавливаются на физический носитель и закрепляются на нём вместе с другими данными так, что с такого носителя невозможно произвести копирование. В этом случае компьютерный преступник выполняет некую заданную последовательность действий, снимая с носителя защищённые программы. По оценке специалистов, данный метод требует от правонарушителя немалых профессиональных знаний и соответствующего опыта;

«снятие системы защиты из памяти» – система защиты периодически загружает защищаемое программное средство в оперативную память для передачи управления от этой программы коду защиты и, в тот момент пока код не взял управление на себя, в оперативной памяти компьютера находится абсолютно незащищённая программа. В результате компьютерному преступнику остаётся сохранить её в каком-нибудь файле.

Рассмотренная нами классификация применяется при отправлении запросов или сообщений о компьютерных преступлениях по телекоммуникационной сети Интерпола и её общепризнанным достоинством является введение литеры «Z», отражающей прочие методы преступлений, что позволяет развивать и дополнять используемую классификацию.

Однако, как отмечают некоторые отечественные и зарубежные эксперты, «…приведённая выше система классификации, как и ряд других, напри-

[49] Совершенно понятно, что систему защиты необходимо строить так, чтобы код защиты был неизменяемым.

мер, «минимальный» и «необязательный» списки нарушений «Руководства Интерпола по компьютерной преступности», страдают одним общим недостатком – в них происходит смешение уголовно-правовых начал и технических особенностей автоматизированной обработки информации, что приводит к неоднозначности толкования и ещё большей неопределённости понятия «компьютерное преступление». Кроме того, как правило, современные компьютерные преступления не ограничиваются использованием лишь одного известного метода и совершаются либо с помощью всевозможных сочетаний вышеописанных методов, либо с применением вновь изобретённых компьютерными преступниками методов, а также их комбинаций с уже апробированными методами.

§4. Основные подходы, развивающие и дополняющие классификацию Интерпола

Некоторые отечественные специалисты классифицируют компьютерные преступления в зависимости от других признаков, например, применённого способа совершения и, по их мнению, все преступления такого рода можно объединить в три (перехват, несанкционированный доступ и манипуляции) или пять (изъятие средств компьютерной техники, перехват информации, несанкционированный доступ к средствам компьютерной техники, манипуляция данными и управляющими командами, комплексные методы) основных групп[50]. При этом в качестве главного классифицирующего признака выступает способ действий компьютерного преступника, направленный на получение доступа к средствам компьютерной техники с различными намерениями. Кроме того, в зависимости от характера воздействия на компьютерную систему иногда выделяют четыре основных вида компьютерных преступлений, рис. В6.

[50] Батурин Ю. М. Проблемы компьютерного права. М., 1991.

Рис. В.6. Классификация компьютерных преступлений в зависимости от способа воздействия на компьютерную систему

Указанные на рис. В6 виды компьютерных преступлений можно охарактеризовать при помощи следующих определений:

физические преступления – включают в себя разрушение оборудования, уничтожение данных или программ, ввод ложных данных, кражу сведений, записанных на различных носителях информации;

операционные преступления – представляют собой мошенничество (выдача себя за другое лицо или использование прав другого лица), несанкционированное использование различных технических устройств;

программные преступления – включают в себя различные способы изменения системы математического обеспечения, например, «логическая бомба» – введение в программу команды компьютеру проделать в определённый момент какое-либо несанкционированное действие, «троянский конь» – включение в обычную программу своего задания, см. выше;

электронные преступления – включают в себя схемные и аппаратные изменения, приводящие к тому же результату, что и изменение компьютерных программ.

Некоторые западные специалисты по борьбе с компьютерной преступностью классифицируют компьютерные преступления исходя из других под-

ходов. В этом случае различают девять основных видов преступлений, рис. В7.

Рис. В.7. Классификация компьютерных преступлений в зависимости от их вида

Приведённые на рис. В7 виды компьютерной преступности обычно кратко характеризуются специалистами следующим образом.

Нелегальное получение товаров и услуг

Весьма распространённый вид преступления, который состоит в получении товара или услуги либо бесплатно, либо за счёт другого лица. Наиболее часто встречающейся его разновидностью является бесплатное пользование услугами связи, предоставляемыми за плату различными телефонными компаниями. Такие преступления начали отмечаться с 1961 года. В 60-х годах был создан «синий ящик» – устройство для генерации тональных сигналов готовности, – который позволял преступнику бесплатно использовать телекоммуникационную систему, выдавая себя за её технического работника. Благодаря мерам противодействия, предпринятым телефонными компаниями, этот способ сейчас практически не применяется. Основным способом мошенничества в настоящее время стали манипуляции, позволяющие вести бесплатные разговоры за счёт других абонентов. Воровство телекоммуника-

ционных услуг в последние годы превратилось в массовый и очень доходный вид компьютерной преступности. С конца 80-х годов похищенные телекоммуникационные услуги стали продаваться третьим лицам.

Другая разновидность незаконного пользования услугами состоит в изменении сведений о предоставлении таких услуг в базах данных компаний, их оказывающих. Например, информация о предоставлении какой-либо услуги в кредит может изменяться таким образом, чтобы потребителем уже оплаченной кем-то услуги стал сам компьютерный преступник.

Незаконный доступ к информации, её подделка или хищение

Объектом этого распространённого компьютерного преступления является интеллектуальная собственность. Несанкционированный доступ к информации, хранящейся в компьютере, осуществляется обычно путём использования чужого имени, изменения физических адресов технических устройств, использования информации, оставшейся после решения тех или иных задач, модификации программного и информационного обеспечения, хищения носителя информации, установки аппаратуры перехвата в каналах передачи данных. Для несанкционированного доступа к данным законного пользователя могут также использоваться уязвимые места в защите компьютерной системы, вызванные ошибками в программах и т. п. В данном контексте подделка и хищение компьютерной информации представляют собой несанкционированное копирование данных с целью их присвоения и последующей продажи.

Мошенничество в сфере электронной торговли и инвестирования

Данный вид компьютерных преступлений основан на возможностях, которые предоставляет электронным мошенникам Глобальная сеть, где информация распространяется анонимно, с минимальными затратами, в режиме реального времени и на весь мир. Можно назвать следующие сферы мошенничества при ведении электронной коммерции и инвестирования: продажа несуществующих товаров, предложение мифических услуг, привлечение

средств на ложную благотворительность, азартные игры, финансовые пирамиды и пр.

Электронный вандализм и терроризм

Основными мотивами такого рода компьютерных преступлений являются месть и конкурентная борьба. Повреждение компьютерных систем или вмешательство в их работу могут приводить к очень серьёзным последствиям, так как даже простая угроза уничтожения компьютерной информации может стать действенным инструментом вымогательства или шантажа. Электронный вандализм и терроризм осуществляются путём внедрения в компьютерные системы и сети таких вредоносных компьютерных программ, которые способны повредить или уничтожить данные и программное обеспечение, хранящиеся на жёстком диске компьютера.

Электронное отмывание денег и уклонение от налогов

Развитие компьютерных и телекоммуникационных систем привело к появлению электронной наличности и возникновению глобальной системы электронных денежных расчётов, вокруг которой сформировалась «теневая» банковская система с сетью полулегальных финансовых учреждений. Она позволяет переводить денежные средства в любую географическую точку мира быстро, анонимно, по чрезвычайно запутанным маршрутам и в обход государственных систем финансового контроля. Поэтому электронные переводы стали использоваться компьютерными преступниками для сокрытия источников поступления денежных средств, «отмывания» денег и ухода от выплаты налогов.

Мошенничество с переводом электронной наличности

Этот вид преступлений заключается в изменении информации, отображающей электронную наличность на счетах в системе электронных банковских расчётов. Известно несколько способов такого мошенничества: информация о наличности, имеющейся на счетах клиентов, переписывается на счета, которыми распоряжаются компьютерные преступники или модифицируется алгоритм, по которому функционирует система обработки информации

об электронных банковских расчётах или десятичные доли, образующиеся в результате финансовых расчётов, автоматически переводятся на счёт компьютерного преступника. Также известны способы мошенничества с переводом электронной наличности, в которых компьютер используется в совокупности с другими устройствами, например, банкоматами.

Нелегальное прослушивание телекоммуникационных линий связи

Этот вид преступлений представляет собой особую угрозу, так как компьютерные системы хранят большие массивы данных, располагающихся на компактных носителях информации, а современные информационные технологии, как известно, позволяют очень быстро осуществить копирование этих данных, в том числе и при помощи технических средств удалённого доступа. Применяемые при совершении нелегального прослушивания телекоммуникационных линий связи технические средства и методы совершения таких компьютерных преступлений описаны нами выше.

Распространение нелегальных материалов

Этот вид компьютерных преступлений стал особенно актуален в связи с развитием Глобальной сети и взрывным увеличением общего количества её пользователей во всём мире. Используя возможности Интернет, а также других информационных сетей, компьютерные преступники в невиданных ранее масштабах распространяют порнографические и другие незаконные материалы.

Прочие преступления

Специалисты относят к этой группе компьютерных преступлений те случаи, в которых компьютер выступает в качестве помощника при планировании, совершении или сокрытии следов традиционного преступления. Сегодня широкие возможности современной компьютерной техники и инновационных информационных технологий интенсивно используются организованной преступностью. Компьютерные системы и телекоммуникационные сети помогают компьютерным преступникам оперативно устанавливать и под-

держивать устойчивую связь между собой, а также координировать свои противоправные действия.

Иногда в целях классификации и характеристики компьютерных преступлений используют также термин «технология». Например, изначально все компьютерные преступления делят на две генеральные совокупности: мошенничества и злоупотребления; а затем формулируют методы (или способы) их совершения, которые называют технологиями, табл. В7.

Таблица 7

Основные технологии, использующиеся при совершении компьютерных преступлений

Мошенничества		Злоупотребления	
1.	Ввод неавторизованной информации	**1.**	Ввод неавторизованной информации
2.	Создание неавторизованных файлов с информацией	**2.**	Создание неавторизованных файлов с информацией
3.	Манипуляции разрешенной для ввода информацией	**3.**	Кража компьютерного времени, программ, информации и оборудования
4.	Манипуляции или неправильное использование файлов с информацией	**4.**	Разработка компьютерных программ для неслужебного использования
5.	Обход внутренних мер защиты	**5.**	Манипулирование или неправильное использование возможностей по проведению работ на компьютерах

На наш взгляд такая классификация не даёт полного представления обо всём многообразии методов и способов, применяемых современной компьютерной преступностью, так как в данном случае используются излишне агрегированные показатели. Кстати, это замечание справедливо и по отношению к некоторым другим подходам в области классификации компьютерных преступлений из числа рассмотренных.

В связи с приведёнными выше системами классификации компьютерных преступлений вполне очевидный интерес представляет классификация, предложенная В.А. Мещеряковым,[51] рис. В8.

Приведём краткую характеристику компьютерных преступлений соответствующих классификации В.А. Мещерякова и указанных на рис. В8.

[51] Мещеряков В.А. Криминалистическая классификация преступлений в сфере компьютерной информации // Конфидент. № 4–5, 1999.

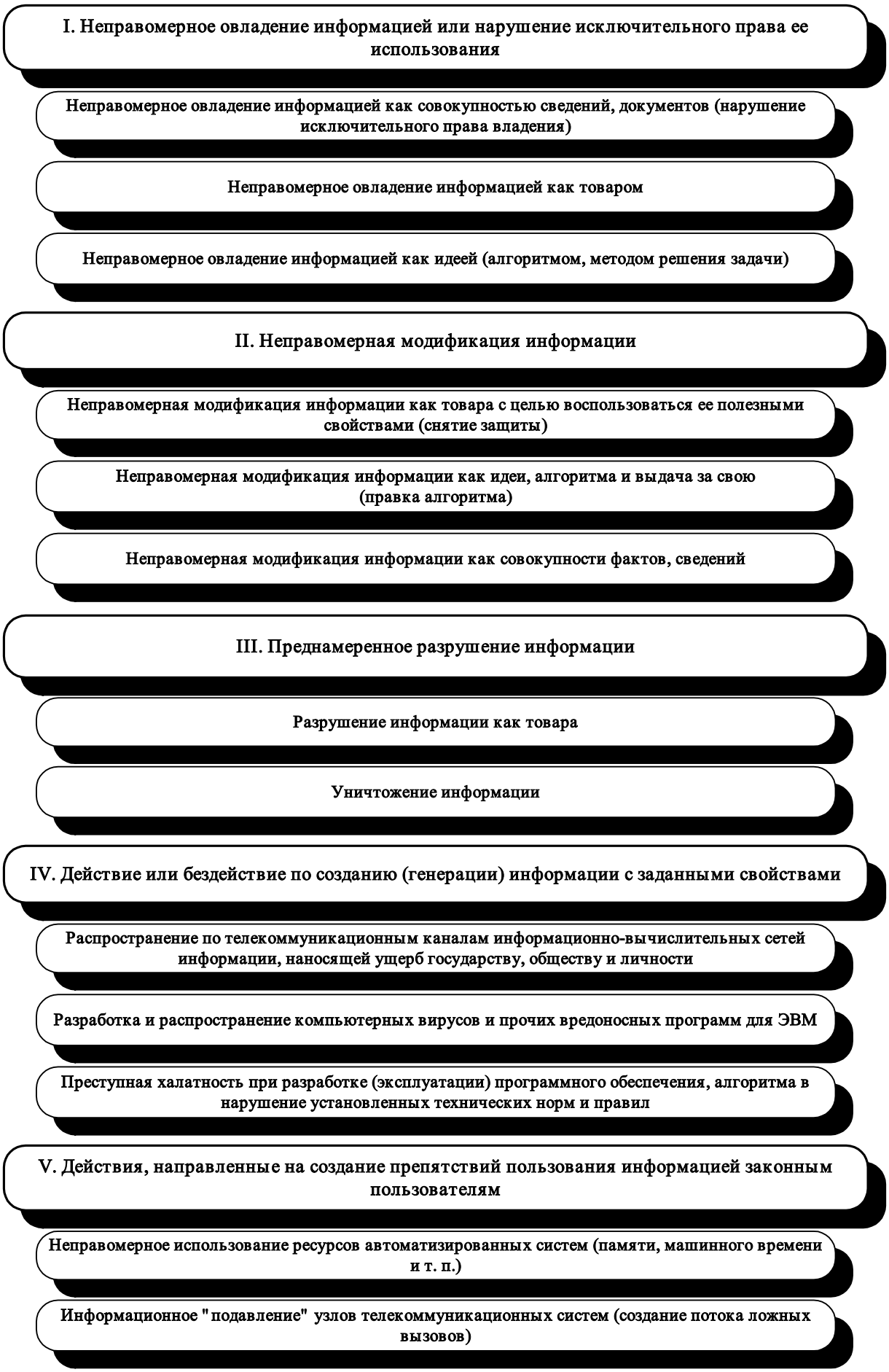

Рис.В.8. Классификация компьютерных преступлений, предложенная В.А. Мещеряковым

Неправомерное овладение информацией как совокупностью сведений, фактов (нарушение исключительного права владения) представляет собой часто встречающийся на практике класс компьютерных преступлений. С точки зрения криминалистики этот класс включает наиболее простые компьютерные преступления для подготовки и совершения которых не обязательны длительная специальная подготовка, высокая квалификация и разработка специальных технических приспособлений. Следовательно, в этом случае компьютерный преступник может ограничиться обычными средствами программно-аппаратного обеспечения компьютерной системы. Результаты неправомерного овладения информацией могут записываться на любой носитель информации.

Неправомерное овладение информацией как товаром (незаконное копирование информации как товара) заключается в копировании компьютерных программ или целого упорядоченного массива информации (например, базы данных) без разрешения владельца или собственника. Данный вид деяний очень широко распространён в нашей стране как практически единственная форма получения новых версий программного обеспечения. При этом в качестве конечного итога преступления выступают извлечение личной выгоды из незаконно полученной информации и (или) использование её нужных свойств в собственных целях.

Компьютерные преступления в части неправомерного овладения информацией как идеей представляют собой несанкционированное ознакомление с использующейся методологией проведения каких-либо вычислений и (или) алгоритмами принятия решений какой-либо автоматизированной системой. Криминалистический аспект таких компьютерных преступлений должен рассматриваться как достаточно сложное и комплексное деяние, так как оно предусматривает получение доступа к некоему множеству структурированных данных и проведение специальных процедур, связанных со специфичным анализом используемой в системе информации, а также опреде-

лением её смыслового содержания и процедур реализации в целях получения необходимого результата.

Компьютерные преступления, которые в классификации В. А. Мещерякова принято обозначать как «неправомерную модификацию информации как товара», получили на сегодняшний день в нашей стране широкое распространение и организации-разработчики программного обеспечения вынуждены применять различные меры для защиты своих программных продуктов от так называемого «пиратского копирования». Недостаточность нормативного правового обеспечения и правоприменительной практики, а также невозможность создания и применения абсолютно надёжных средств защиты создают такие условия, при которых в любой легально приобретённый программный продукт затем могут вноситься недокументированные изменения, позволяющие незаконно его тиражировать и использовать в качестве высокодоходного товара без каких-либо ограничений на число инсталляций или времени пользования. В силу указанных причин неправомерная модификация в подавляющем большинстве случаев является к тому же и «гарантией» последующего нарушения авторских и смежных прав.

Неправомерная модификация информации как идеи в качестве ещё одного вида компьютерных преступлений пока получила значительно меньшее распространение и заключается не только в получении какого-либо программного обеспечения, но и его обязательном предварительном анализе. Практически все известные на сегодняшний день компьютерные преступления этого вида совершены самими разработчиками программного обеспечения и, чаще всего, теми же лицами, которые его и эксплуатируют.

Вид компьютерных преступлений, именуемый «неправомерной модификацией информации как совокупности фактов, сведений», получил достаточно широкое распространение в банковских системах, так как в них записи в полях баз данных отражают определённые денежные суммы или другие сведения, которые имеют конкретное денежное или иное экономическое выражение.

Разрушение информации как товара в качестве вида компьютерных преступлений характеризуется тем, что легальный владелец информации не может воспользоваться программным обеспечением или базой данных как товаром, его полезным свойствами. Известный интерес представляют случаи, когда значительный ущерб, вследствие невозможности использования информации, владельцу наносится при совершении умышленных действий, не связанных с влиянием на информацию посредством ЭВМ.

По мнению некоторых отечественных специалистов, распространение по телекоммуникационным каналам информационных сетей информации, наносящей ущерб государству, обществу и личности с уголовно-правовой точки зрения может быть полностью охарактеризовано с помощью других (не компьютерных) составов преступлений, но совершённых с использованием компьютера. В качестве примера этого вида компьютерных преступлений иногда приводят создание и распространение компьютерных игр порнографического характера с известными персонажами, использование компьютерных сетей для передачи и распространения материалов, содержащих призывы к насильственному изменению конституционного строя и т. п.

Разработка и распространение компьютерных вирусов и прочих вредоносных компьютерных программ представляет собой, пожалуй, самый распространённый вид компьютерных преступлений. По оценке экспертов он может соперничать по количеству зарегистрированных фактов только с таким видом компьютерных преступлений как неправомерное овладение информацией как товаром.

Под преступной халатностью при разработке программного обеспечения и математических алгоритмов понимаются нарушения установленных стандартов, технических норм и правил, которые повлекли за собой тяжкие последствия, то есть нанесли непоправимый ущерб. Обычно такие последствия могут иметь место в случае нарушения стандартов, инструкций и рекомендаций, определяющих порядок разработки, испытания, эксплуатации и сопровождения программных средств в составе компьютерных систем, об-

служивающих критические отрасли экономики: объекты атомной энергетики, непрерывные химические производства, системы управления воздушным движением и т. п.

Под составом преступного деяния, в случае неправомерного использования ресурсов автоматизированных систем, следует понимать скрытный несанкционированный захват вычислительного ресурса коллективного пользования (внешняя и оперативная память, центральный процессор и пр.) каким-либо субъектом с намерениями минимизации либо полного исключения своих затрат за его использование.

Осуществление компьютерных преступлений, получивших в классификации В. А. Мещерякова название «информационное подавление узлов телекоммуникационных систем», возможно, например, при использовании стандартных телефонных коммутируемых каналов, когда по заданному телефонному номеру осуществляется постоянный автоматический вызов с нескольких источников. В этом случае создаётся поток ложных вызовов, при котором настоящий абонент не может установить желаемое соединение.

По нашему мнению к достоинствам предложенной В. А. Мещеряковым классификации компьютерных преступлений можно отнести достаточно удачную попытку применения проявлений реальной компьютерной преступности к российским условиям. Вместе с тем, классификация В. А. Мещерякова в первую очередь отражает не сами компьютерные преступления, а комплекс вероятных действий, нацеленных на противоправное использование информации.

В завершение подчеркнём, что подходы, реализованные в классификации В. А. Мещерякова с целью описания отечественной компьютерной преступности, могут учитываться при совершенствовании действующего в нашей стране законодательства.

§ 4. Великое противостояние: зарождение и динамика, победы и поражения

Как известно, самый первый зарегистрированный случай злоупотребления с использованием компьютера относится к теперь уже очень далёкому от нас 1958 году[52]. Но, только после выявления и раскрытия в начале 60-х годов ряда громких преступлений, совершённых с использованием электронно-вычислительной техники, термин «компьютерная преступность» был введён американскими средствами массовой информации в широкое употребление. Затем, несколько позднее, стараниями печатных изданий, телевидения и радио он появился в употреблении и быстро вошёл в повседневный обиход большинства стран Западной Европы. Пристальное внимание криминалистов ведущих зарубежных стран проблема компьютерной преступности привлекла к себе в 70–80-х годах прошлого столетия, когда началось бурное развитие компьютерной техники, повлекшее за собой целый комплекс негативных последствий и обострившее ситуацию с защитой ценной информации, содержащейся в базах и банках данных компьютерных систем. Ведь уже в 1979 году некий Рифкин нанёс ущерб Security Pacific Bank на сумму 10 млн. долларов. Совершение этого компьютерного преступления стало возможным исключительно благодаря слабой системе безопасности банка. Рифкину удалось перевести 10 млн. долларов из Калифорнии в Швейцарию и снять деньги со счёта до того, как кто-либо обнаружил хищение.

В начале 90-х годов произошло одно из крупнейших электронных хищений денежных средств – со счетов знаменитой немецкой фирмы BMW было снято 700 млн. долларов. В США ежегодные убытки от компьютерной преступности только в области банковского и делового электронного документооборота перевалили за 100 млрд. долларов, в Великобритании превысили 5 млрд. долларов, а в Западной Европе 30 млрд. долларов. Поэтому уже на состоявшемся в конце 1993 года международном форуме по защите информации отмечалось, что в западных странах примерно половина финансо-

[52] Андрианов Б. Ч., Бородин В. А. «Шпионские штучки» и устройства защиты объектов и информации. СПб., 1996.

вых и экономических преступлений происходит с использованием компьютерных сетей.

Однако вопрос о компьютерной преступности был поставлен «ребром» только около пятнадцати лет тому назад, когда в результате проникновения студента Корнельского университета в компьютерные системы разведки и Министерства обороны США произошло отключение в них нескольких тысяч компьютеров. В связи с этим беспрецедентным на то время случаем были предприняты первые масштабные меры противодействия. На средства Пентагона была создана компьютерная группа быстрого реагирования – CERT (Computer Emergency Response Team), основными задачами которой были определены регистрация и документирование информации[53] о крупных «взломах» компьютерных сетей, а также оказание помощи в ликвидации проделанных компьютерными преступниками «дыр» в программном обеспечении[54].

С тех пор в США, в связи с продолжающимся ухудшением ситуации, количество организаций по борьбе с компьютерной преступностью постоян-

---

[53] Документированная информация – это любые данные, сведения, зафиксированные на носителе информации и обладающие реквизитами, позволяющими их идентифицировать.

Носитель информации – материальный объект, предназначенный для хранения, обработки и передачи каких-либо сведений, данных.

Идентификация – присвоение идентификаторов субъектам и объектам системы, а также процесс распознавания определённых компонентов системы, обычно с помощью уникальных имён (идентификаторов), воспринимаемых системой.

Идентификатор – персональное обозначение (имя, код и т. п.), позволяющее однозначно выделить идентифицируемый субъект (объект) среди всех других в полном множестве субъектов (объектов).

[54] Краткая справка. Координационный центр CERT/CC находится в Питсбурге (штат Пенсильвания, США) при Университете разработки программного обеспечения Карнеги (Carnegie Mellon University's Software Engineering Institute, SEI). SEI, спонсируемый Министерством обороны США, занимается улучшением методов разработки программного обеспечения. Координационный центр CERT/CC является частью программы, которая разрабатывается в SEI – Networked Systems Survivability (NSS). Основная цель данной программы – обеспечить построение соответствующей технологии и методов управления системой таким образом, чтобы максимально эффективно противодействовать электронным атакам, минимизировать ущерб и обеспечить непрерывность работы системы даже в случае успешного осуществления атаки. Координационный центр CERT/CC предназначен для решения следующих задач: обеспечить постоянную и надёжную связь для реагирования на сообщения об атаках; обеспечить взаимодействие между экспертами, работающими в области обеспечения информационной безопасности; служить центром для идентификации и коррекции уязвимостей в компьютерных системах; проводить научные исследования для повышения уровня безопасности существующих систем. Для периодического ознакомления с обнаруженными в исследовательских лабораториях CERT/CC уязвимостями программного и аппаратного обеспечения на WWW-сервере (http://www.cert.org), FTP-сервере (ftp://ftp.cert.org/pub/cert_advisories), в телеконференции USENET (comp.security.announce) и через список рассылки публикуются так называемые «Advisories» – описания уязвимостей и способов их устранения. Информация, полученная от фирм-производителей о проблемах безопасности и их решении, публикуется в специальных информационных бюллетенях от поставщиков (Vendor-Initiated Bulletins, VIB), распространяемых по тем же каналам, что и «Advisories».

но увеличивается. Министерство обороны США, в дополнение к выше указанной группе, создало группу (Automated Systems Security Incident Support Team, ASSIST) для поддержки программы по обеспечению безопасности информационных сетей и защиты информационных систем Пентагона (Defense Information Infrastructure, DII) – INFOSEC. Открыты центры для информационной защиты крупных энергетических, нефтяных, железнодорожных, авиационных и телекоммуникационных компаний. При Министерстве энергетики США в 1989 году был организован специальный центр (Computer Incident Advisory Capability, CIAC) основной целью которого является обеспечение компьютерной безопасности служащих и подрядчиков Министерства энергетики США. В настоящее время CIAC выполняет множество функций, включая обработку сообщений об инцидентах; обеспечение компьютерной безопасности служащих и подрядчиков Министерства энергетики США; проведение симпозиумов по вопросам информационной безопасности; консультации по вопросам защиты информации. Группа CIAC входит в состав Центра безопасных компьютерных технологий (Computer Security Technology Center, CSTC) и расположена в Лоуренс-Ливерморской национальной лаборатории (Lawrence Livermore National Laboratory). Кроме того, центр CIAC является одним из участников форума FIRST[55] и для периодического ознакомления Интернет-сообщества с «дырами» в программном обеспечении, по аналогии с координационным центром CERT/CC, публикует информационные бюлле-

[55] Краткая справка. После создания CERT/CC, CIAC и других групп, каждой со своим финансированием, своими целями и требованиями, стало ясно, что без единого координирующего центра не обойтись. При взаимодействии между группами, зачастую находящимися в разных часовых поясах, возникали языковые и иные проблемы. Поэтому в 1990 году при содействии 11 участников (CERT, CIAC и т. п.) был создан FIRST (Forum of Incident Response and Security Teams) – международный форум, объединяющий практически все группы реагирования на инциденты. К середине 1997 года состав FIRST (http://www.first.org) уже насчитывал более 60 команд и групп реагирования на инциденты из различных стран мира. Цели FIRST: обеспечение сотрудничества между участниками форума для эффективного предотвращения, обнаружения и восстановления информационных систем после компьютерных инцидентов; обеспечение связи между участниками форума для аварийной и консультативной информации о потенциальных угрозах и атаках; облегчение взаимодействия участников FIRST, проводящих исследования в области информационной безопасности; облегчение распределения информации, инструментов и механизмов, обеспечивающих информационную безопасность. FIRST – организатор ежегодного симпозиума Computer Security Incident Handling Workshop, на котором собираются все команды и группы реагирования на инциденты и на котором они обсуждают свои проблемы. На этом симпозиуме собираются не только участники FIRST, но и все желающие. Два-три раза в год FIRST организует закрытые коллоквиумы только для своих участников. Являясь координатором групп реагирования на инциденты, сам форум FIRST не публикует информацию об уязвимостях и атаках на компьютерные системы.

тени «Advisories» на своем WWW-сайте (http://llnl.ciac.gov), а также через список рассылки. Министерство финансов США открыло в г. Рестон (штат Виржиния) Центр по обмену и оценке информации (Information Sharing and Assessment Center, ISAC), который объединил, информационные системы частных банков, финансовых и страховых компаний. ФБР США организовало Центр защиты национальной инфраструктуры (National Infrastructure Protection Center, NIPC). Активно действует и Национальный центр компьютерной безопасности (National Computer Security Center, NCSC) – организация, поддерживающая и стимулирующая распространение защищённых систем в учреждениях федеральной Администрации США. NCSC, являясь подразделением Агентства национальной безопасности (АНБ) США, осуществляет также координацию в области анализа и разработки систем с гарантированной защитой, повышающих общую эффективность защиты информации[56].

Американским аэрокосмическим агентством (NASA) для выполнения инструкции OMB A-130, закона Computer Security Act от 1987 года и других федеральных законов, нормативных документов и правил, имеющих отношение к защите информационных технологий, был создан Центр NASA Automated Systems Incident Response Capability (NASIRC). Центр NASIRC (http://www-nasirc.nasa.gov) координирует, управляет и обеспечивает технической поддержкой по вопросам информационной безопасности, включая реагирование на электронные атаки, все подразделения NASA. NASIRC решает следующие задачи: анализ, координация деятельности и реагирование на широкий диапазон атак и угроз компьютерам и сетям. Исследование и выработка способов и рекомендаций, уменьшающих риск информационным системам; анализ имеющихся на рынке средств защиты и распределение их среди подразделений NASA; обучение служащих NASA; выпуск брошюр и информационных бюллетеней, повышающих осведомлённость пользователей в области защиты информации. Аналогично многим другим командам

[56] Эффективность защиты информации это степень соответствия достигнутых результатов выполненных действий по защите информации поставленной цели защиты.

реагирования на атаки, NASIRC входит в FIRST и выполняет свои функции путём сотрудничества и координации внутренних подгрупп реагирования на инциденты, а также взаимодействуя с внешними организациями, такими, как указанная FIRST.

В целях проведения научно-исследовательских и опытно-конструкторских работ (НИОКР) в области информационной безопасности, разработки защитных программных и аппаратных средств и обучения вопросам обеспечения информационной безопасности по имени соответствующего проекта была учреждена лаборатория Computer Operations Audit and Security Technology (COAST) (о создании COAST официально объявлено в 1992 году). В рамках НИОКР, проведённых её сотрудниками, было опубликовано большое число статей и книг, разработаны такие известные системы, как система анализа защищённости Unix-систем COPS; система контроля целостности файлов Tripwire; система обнаружения атак IDIOT и пр. Проект COAST поддерживается такими крупными компаниями и организациями как Microsoft, Sun, Cisco, DARPA, AT&T, Internet Security Systems, NSA и многими другими.

В 1994 году один из организаторов CERT/CC – Кристофер Клаус основал компанию Internet Security Systems Inc., которая является одним из лидеров в области разработки средств анализа защищённости и обнаружения электронных атак. В компании ISS действует научно-исследовательская группа X-Force, объединяющая экспертов в области обеспечения информационной безопасности. Эта группа не только постоянно отслеживает все публикуемые другими группами реагирования сообщения об обнаруженных уязвимостях, но и сама проводит тестирование программных и аппаратных средств. Результаты этих исследований помещаются в базу данных уязвимостей и угроз (ISS X-Force Threat and Vulnerability Database).

В Великобритании при Министерстве торговли и промышленности (Department of Trade and Industry) был создан Центр по защите коммерческой информации (Commercial Computer Security Centre), который является разра-

ботчиком «Технических критериев для оценки коммерческих изделий обеспечения безопасности информации» (Technical Criteria for Evaluation of Commercial Security Products), основные положения которых соответствуют «Оранжевой книге» (Orange Book)[57]. В 1990 году, в противовес «Оранжевой книге», Германией была предложена и одобрена представителями Великобритании, Германии, Франции и Голландии «Зелёная книга» (Green Book), задуманная в качестве основы для «Белой книги» (White Book), которая адресована всей Европе. В отличие от «Оранжевой книги», «Зелёная книга» рассматривает кроме конфиденциальности информации также её целостность и доступность и предназначена не только для военной сферы, но и для коммерческого сектора экономики.

Разработанные впоследствии Information Technology Security Evaluation Criteria (ITSEC, называемые «Белой книгой») являются документом, который стал общеевропейским стандартом, определяющим требования и процедуры для создания систем повышенной надёжности. «Белая книга» одобрена Германией, Францией, Великобританией, Нидерландами и основана на немецком стандарте – «Зелёной книге». В соответствии с ней все системы могут

[57] Trusted Computer Security Evaluation Criteria (TCSEC, называемые по цвету обложки «Оранжевой книгой») разработаны Центром компьютерной безопасности Министерства обороны США (DoD Computer Security Center) в соответствии с директивой 525, и утверждены 15 августа 1983 года. Документ, является руководством по безопасности, предназначенным как для покупателей, так и для разработчиков. В документе описываются критерии, в соответствии с которыми оцениваются операционные системы и аппаратно-программные средства, изменяющие функции операционных систем. Оценка безопасности СУБД и вычислительных сетей производится по другим нормативным документам. В TCSEC изложены единые для Министерства обороны США требования к обеспечению безопасности компьютерных систем и порядок определения классов защищённости компьютерных систем, выделены общие требования по обеспечению безопасности обрабатываемой информации, определён перечень показателей защищённости, характеризующих реализацию этих требований. Совокупность показателей определяет класс безопасности рассматриваемой системы. Выделяются семь классов с различными механизмами обеспечения информационной безопасности. Самый нижний класс D присваивается системам, которые не соответствуют ни одному уровню безопасности. Остальные шесть классов образуют 4 группы. Класс А означает гарантированную защиту и предназначен для систем, к которым предъявляются достаточно высокие требования по безопасности. Класс В характеризуется полномочным управлением доступом и делится на три подкласса B1, B2 и B3 (от более низкого к более высокому подклассу). Класс С характеризуется избирательным управлением доступом, применяется к оценке большинства коммерческих систем и делится на два подкласса C1 и C2. Класс безопасности присваивается системе при прохождении процесса сертификации в NCSC. Описанному в TCSEC подходу присущ ряд недостатков: данный документ не применим к персональным компьютерам, и игнорирует проблемы целостности информации – упор делается на её конфиденциальности; основной акцент делается на «безопасность при приобретении», а не на «безопасность при эксплуатации». В целом TCSEC ориентирован на применение в военных организациях и не учитывает специфики коммерческих структур.

оцениваться по эффективности (для наиболее защищённых систем) и по функциональности.

Данный документ является наиболее развитым по сравнению с «Оранжевой книгой» и «Зелёной книгой».

В США также образован консорциум из крупных компаний «high-tech», которые обмениваются между собой информацией о нарушениях их систем безопасности. «Мы собираемся отложить в сторону проблему конкуренции и будем работать вместе, чтобы убедиться, что мы сверх активно заботимся о повышении безопасности информации[58]», – было сказано в совместном заявлении.

Кроме всего прочего, руководители компаний, вошедших в указанную корпорацию, высказались за тесное сотрудничество между профессионалами служб безопасности своих компаний и федеральными служащими правопорядка, в рамках которого корпоративные следователи могут контактировать со своими коллегами по обеспечению правопорядка и оперативно принимать необходимые решения. Ведь не является откровением тот факт, что часто компании, которые страдают от атак компьютерных правонарушителей, тем не менее, предпочитают не прибегать к помощи государственных правоохранительных органов, поскольку боятся возможных корпоративных затруднений, которые могут возникнуть у них впоследствии. Коммерческие, а иногда и государственные структуры, которые подверглись нападениям, не склонны афишировать причинённый им ущерб и, соответственно, «эффективность»

[58] Безопасность информации – защищённость информации от нежелательного (для соответствующих субъектов информационных отношений) её разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного её тиражирования.

Субъекты информационных отношений – государство, государственные органы, государственные, общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельные граждане (физические лица) и иные субъекты, взаимодействующие с целью совместной обработки информации. По отношению к данным, обрабатываемым в автоматизированной системе различные субъекты – участники информационных отношений, могут выступать (возможно, одновременно) в качестве источников, пользователей (потребителей) и собственников (владельцев, распорядителей) информации; физических и юридических лиц, в отношении которых собираются и обрабатываются какие-либо сведения; владельцев компьютерных систем и участников процессов обработки и передачи данных.

Безопасность субъектов информационных отношений – это их защищённость от нанесения материального, морального или иного ущерба при помощи воздействия на информацию и (или) средства её обработки и передачи.

своих систем защиты, поэтому случаи компьютерных преступлений становятся достоянием гласности далеко не всегда.

Более того, иногда боязнь сотрудничества с официальными органами заходит слишком далеко и переходит все разумные границы. Например, в начале февраля 2000 года в США многие пользователи Интернет начали паниковать, так как в Глобальной сети появились предположения о том, что такие сайты, как Yahoo!, eBay, Buy.com, CNN и некоторые другие пали жертвами электронных атак ЦРУ США!

Это произошло сразу после ряда успешных электронных нападений на указанные Web-сайты, и покупателей крупнейших электронных магазинов невольно начали волновать вопросы типа: «если этот Web-сайт не может противостоять атаке, то где гарантии, что информация, хранящаяся в моём досье на их сервере, в котором содержится номер кредитной карты, а также другие конфиденциальные сведения, не станет достоянием электронных взломщиков?» Тем более что специалисты не отвергали возможность повторения атак, а слухи о том, что истинным источником атак на самом деле было ЦРУ США, которое таким образом надеется «выколотить» из федерального бюджета повышенные субсидии на свои нужды, нашли благодатную почву в лице мало осведомлённых налогоплательщиков.

Правда, такие высказывания крайнего толка в дальнейшем не получили широкого распространения, но, зато, указали на очевидный факт: поиск общественностью «альтернативного» источника атак на компьютеры, такого, как спецслужбы, со временем может набрать силы.

Естественно, что подобные настроения в обществе не могли остаться незамеченными, и в ходе проведённого ФБР США расследования по поводу электронных нападений на крупнейшие Web-сайты Америки было доказано, что задолго до того, как был выведен из строя Web-сайт Yahoo! – первая жертва компьютерных преступников, возможности такого рода нападений с использованием тех же технологий электронного взлома обсуждались в ча-

тах, в которых общались представители компьютерной преступности[59]. К такому выводу пришли федеральные агенты после проведения соответствующих бесед с представителями The Internet Relay Chat Networks, так как именно в этом объединении чат серверов предоставляется возможность самому создать свой собственный чат, некоторые из них создавались компьютерными преступниками для обмена «передовым опытом» электронного взлома и т. п. Кроме того, именно на этих серверах была впервые опробована методика электронной атаки, впоследствии получившая название «Denial of Service» («отказ в обслуживании») или «DoS»[60], о которой мы поговорим более подробно в соответствующем разделе настоящей книги, но руководство The Internet Relay Chat Networks, в отличие от Yahoo!, eBay и др., не стало обращаться в ФБР США, сделав это только после уже произошедших электронных атак на крупнейшие Web-серверы Америки.

Таким образом, ЦРУ США было «оправдано», но сомнения у части пользователей, наверняка остались.

Интересно, что как минимум, восемь раз банки и другие финансовые учреждения США получали по закрытой сети предупреждения о готовящихся электронных атаках на крупнейшие Web-сайты. Однако, их руководство, получившее соответствующие электронные письма, не стало обращаться ни в ФБР США, ни в какие-либо ещё официальные органы даже после того, как эти атаки начались. И это несмотря на то, что первые предупреждения стали поступать по e-Mail и посредством пейджинговой связи за четыре дня до «потопа» на Web-сайте Yahoo! Более того, помимо информации о готовящихся электронных атаках на Web-сайты, передавалась и информация об ад-

[59] Интересно, что на конференции «Компьютерная преступность 2001» (Cybercrime 2001), которая прошла в Коннектикуте, было принято следующее решение: если компьютерные преступники всех мастей могут обмениваться информацией в секретных чатах и проводить обучающие конференции, то тоже самое могут и должны делать и полицейские.

[60] DoS (Denial of Service) атаки – класс атак, приводящих к отказу в обслуживании. Во время таких атак происходит повышенный расход ресурсов процессора, и уменьшение пропускной возможности канала связи, что может привести либо к критическому замедлению работы отдельных прикладных задач, всей компьютерной системы, либо к полной остановке выполняющихся задач пользователя.

Отказ в обслуживании – любое действие или последовательность действий, которая приводит какую-то часть системы к выходу из строя, при котором она перестаёт выполнять свои функции. Причиной может быть несанкционированный доступ, задержка в обслуживании и т. д.

ресах, с которых они будут осуществляться. Вместе с тем банки и не имели права (!) предупреждать представителей официальных органов власти согласно правилам частной сети, созданной за 1,5 млн. долларов всего лишь за несколько месяцев до развернувшихся событий для финансовой индустрии с целью обмена информацией по безопасности и другим важным вопросам. Уильям Марлоу, вице-президент компании Global Integrity Corporation, создавшей сеть, сказал, что «…каждый чувствует себя уверенно, будучи заранее информированным. …Правительство не вмешивается в эту сеть, являющуюся анонимной, а в частном секторе могут помогать друг другу и без чьего-либо регулирующего воздействия».

Насколько прав мистер Марлоу, судить Вам, уважаемый читатель, а мы, со своей стороны, отметим, что пользоваться закрытой сетью имеют право только лицензированные финансовые организации, а также некоторые правительственные финансовые учреждения, выплачивая за её использование от 13 до 125 тысяч долларов в зависимости от количества штатных сотрудников. Между прочим, в отличие от Марлоу, который абсолютно невозмутим и спокоен, даже уже упоминавшийся нами Кевин Митник, вошедший в легенды и отбывший 59 месяцев в тюрьме за взломы компьютерных систем крупнейших компаний, которые привели к потере миллионов долларов, дал эмоциональное интервью по поводу нападений на Web-сайты Yahoo!, eBay, Buy.com и др. Приведём одно из его высказываний: «Если бы я мог поговорить с теми людьми, которые устроили эти перебои в работе Web-сайтов, то я бы им сказал, что их действия просто не та вещь, которую стоит делать. Их атаки совершенно не впечатляют, так как они не представляют собой ничего сложного. Это все равно, что поцарапать машину – ничего страшного, но очень злит». В общем, он осуждает совершивших атаки электронных вандалов, но вот что интересно – разделяют ли они его мнение?

Общую картину дополняет и озвученная в Сенате США мысль о том, что прошедшие электронные атаки не просто хулиганство, и причины атак на крупнейшие Web-сайты Америки лежат более глубоко, вопреки сложивше-

муся мнению, что напавшие на Web-сайты Yahoo!, eBay, CNN и др. – просто подростки, которые каким-то образом заполучили в свои руки страшное оружие и сейчас просто развлекаются. Напротив, существует убеждённость в том, что электронные атаки на Web-сайты, которые получили название «отказ в обслуживании» всего лишь маскировка настоящей цели – электронного взлома серверов для хищения интеллектуальной собственности, а истинные объекты атаки не разглашаются самими компаниями, так как признание о неспособности сохранения в безопасности конфиденциальной информации клиентов испортит их репутацию.

Не прошло и нескольких недель после всех этих пертурбаций, как представители ФБР США подтвердили тот факт, что их собственный Web-сайт подвергся электронной атаке, аналогичной атакам на коммерческие Web-сайты в начале февраля. В результате Web-сайт ФБР США был недоступен в течение нескольких часов, но никто так и не взял на себя ответственность за эту акцию. Как указывали специалисты, это преступное деяние, скорее всего, стало своеобразным ответом на заявление ФБР США о готовности найти и наказать компьютерных преступников, ответственных за атаки на Web-сайты Yahoo, eBay, E*Trade, Amazon.com и др.

Ещё через три недели, в день 50-й годовщины опубликования списка «Десяти наиболее разыскиваемых преступников», Web-сайт ФБР США вновь был успешно атакован и выведен из строя на несколько часов. Причём, метод атаки был абсолютно тем же, что и в прошлый раз! Неизвестным компьютерным преступникам удалось за короткий срок уже вторично успешно применить DoS атаку на сервер этого ведомства, самого активного члена «поисковой группы», занимающейся розыском электронных преступников, применяющих технологию DoS нападения. Кроме официального подтверждения, никаких комментариев от ФБР США не поступило, а война между официальными властями и компьютерной преступностью продолжилась на новом, очередном витке противостояния «гигантов».

Конечно, подобные, мало сказать «курьёзные», случаи становятся объектом пристального внимания всей общественности, не добавляют уверенности гражданам разных стран. В итоге не только частные организации, но и граждане опасаются сотрудничать с официальными органами, так как не видят в этом никакой пользы.

Например, в марте 2000 года (обратите, пожалуйста, внимание на хронологию событий в связи с изложенным выше) у Бюро по переписи населения США появилась новая проблема. Если ранее его представителям приходилось сталкиваться с упрёками по поводу слишком большого любопытства официальных властей (в соответствующей анкете, называемой «Long Form», содержится целых 53 вопроса, которые касаются практически всех важнейших сторон жизни гражданина США), то теперь добавилась и ничем не прикрытая боязнь перед электронной преступностью. Подавляющее число населения США опасается того, что Web-сервер бюро будет взломан и конфиденциальная информация попадёт в руки компьютерных преступников, которые будут использовать полученные сведения в своих собственных, в том числе и корыстных целях.

Представители Бюро по переписи населения США всячески старались успокоить людей, утверждая, что их Web-сервер ещё никогда не подвергался электронному взлому, приводили мнение уважаемых экспертов о его сверхнадёжной защите. Но, неприятный симптом налицо: население начало проявлять недоверие к официальным властям по поводу их способности не то что искоренить, но и удержать компьютерную преступность в каких-либо разумных рамках. Беспокойство граждан США имело вполне реальную причину, что не замедлило проявиться в сообщениях из других стран.

Из Бразилии поступила и была официально подтверждена лабораторией криминалистики г. Сан Пауло информация, суть которой заключалась в том, что в середине апреля 2000 года был обнародован факт хищения информации из базы данных о налогоплательщиках Налоговой службы Бразилии – 11,5 млн. записей о гражданах страны и информация об уплате налогов. В

ходе последовавшего расследования было выдвинуто предположение, что база данных была сразу же продана компаниям, занимающимся прямым маркетингом по e-Mail. Причём, несмотря на то, что утечка информации из базы данных состоялась ещё в ноябре 1999 года, полиция хранила полное молчание, а граждан даже не поставили в известность о том, что их личные данные могут использоваться в нечистоплотных или даже криминальных целях. Из последующих, вялых объяснений полиции можно было сделать вывод о том, что после того, как компания Telefonica сообщила полицейским о подозрительных объявлениях, в которых предлагалось приобрести указанную базу данных, были арестованы четыре человека.

Такой способ действий официальных властей, естественно, не укрепил доверие к ним со стороны собственных граждан.

В мае 2000 года электронные взломщики завладели всей информацией о клиентах индийского банка. Группой нарушителей, единственной целью которых (правда лишь по их собственным словам) была проверка защитных систем различных Web-сайтов, был взломан сервер индийского банка Saraswat. Как заявили представители этой группы, им было совсем не сложно обойти защитные системы Web-сайта банка и получить доступ ко всей информации самого банка. В итоге проведённой электронной атаки в их распоряжении оказалась вся личная информация клиентов этого банка. Причём, установить контроль над онлайновой системой платежей банка электронным взломщикам не удалось лишь по одной причине – такой системы просто не существовало.

Официальные лица банка распространили заявление о том, что все прорехи в защитных системах Web-сайта устранены. Неужели все и навсегда? Верится, но с большим трудом.

31 июля 2000 года списки успешно сдавших экзамены абитуриентов кипрского университета должны были публиковаться на официальном Web-сайте Министерства образования Кипра. Несколько часов подряд об этом знаменательном для страны событии сообщали все местные радиостанции,

но списки так и не появились. Компьютерные преступники залепили увесистую пощёчину Министерству образования Кипра, исхитрившись получить доступ ко всем «строго конфиденциальным данным», касавшимся результатов экзаменов в университет и… без долгих размышлений удалили их ещё до момента размещения на официальном Web-сайте.

Разгневанный Министр образования Кипра заявил на своей пресс-конференции, что будет проведено официальное расследование этого инцидента, но уровень доверия у граждан Кипра по отношению к официальным органам, – в плане их способности сохранять в неприкосновенности конфиденциальную информацию о частных лицах, – естественно, резко понизился.

20 ноября 2000 года был «взломан» официальный Web-сайт Министерства финансов Марокко. Потенциальные инвесторы, посещавшие этот Web-сайт, могли увидеть сделанное на ломаном французском языке заявление, информирующее о том, что: «Данный Web-сайт был вскрыт группой «Net-Operat», при этом ущерб ему не причинён». В своём сообщении неизвестные электронные злоумышленники призывали власти Марокко обратить внимание на защиту Web-сайта и оставили ссылку, позволяющую получить доступ к нему. Официальные представители марокканских властей подтвердили, что информация, хранящаяся на Web-сайте, не была повреждена и, как заявил советник генерального секретаря Министерства финансов Марокко, Web-сайт был атакован впервые со времени его открытия четыре года назад.

Неплохая статистика, не правда ли!? Первый раз атакован и сразу «взломан»? Как в том анекдоте: «А почему Джо зовут неуловимым? Он, что, так хитёр? – Да, нет. Просто, он никому не нужен». Шутки шутками, а пример весьма показателен и, для тех же инвесторов, ещё и поучителен.

В декабре 2000 года представители Медицинского центра Вашингтонского университета официально признали, что их Web-сервер был взломан злоумышленником, которому удалось скопировать на свой компьютер около 5 тысяч историй болезни пациентов. Как заявил представитель Медицинского центра Том Мартин, компьютерный преступник по кличке «Кейн», по его

словам проживающий в Нидерландах, проник во внутреннюю сеть Центра, используя один из компьютеров, стоящих в отделении. Кейн сообщил о взломе редакции Web-сайта SecurityFocus.com, посвящённого проблемам безопасности, и передал в качестве доказательства несколько украденных файлов с историями болезней. Как утверждает сам электронный взломщик, его целью было указание администрации Медицинского центра на ошибки в системе безопасности, и причинять кому-либо вред он не собирался.

Тем не менее, администрация Центра сообщила о факте взлома в ФБР США, а владельцы украденных медицинских карт пребывают в шоковом состоянии от того, в какие руки могли бы и ещё могут попасть их истории болезни.

«Заявление об электронном взломе Web-сайта малазийского парламента привело к возрастанию в стране беспокойства общественности по поводу того, что правительство не уделяет должного внимания вопросам Интернет-безопасности и обеспечения конфиденциальности личных данных граждан», – сообщало в первых числах января 2001 года малазийское агентство новостей Bernama. Парламентский Web-сайт был взломан 29 декабря 2000 года, и всё это время малазийская полиция занималась поисками электронного взломщика, о котором известно лишь то, что он заявлял о себе, используя кличку «Топейра».

Как объявили официальные представители малазийского правительства: «…данный инцидент подрывает доверие к использованию Интернет в стране, а также отрицательно сказывается на репутации её властей, так как на этот момент уже взломано 50 из 700 действующих правительственных сайтов».

Примерно в тоже время на другом континенте американская компания Health Net, занимающаяся страхованием здоровья, разослала по электронной почте список, содержащий 12 тысяч имён пациентов. Казалось ничего особенного, однако этот список был отправлен не лечащим врачам, а врачам, которые не имели к этим пациентам никакого отношения. Тем самым компани-

ей Health Net была нарушена конфиденциальность личных данных о заболеваниях пациентов. Лишь после того, как примерно 5 тысяч врачей получили электронное письмо со злополучным списком пациентов, застрахованных в Health Net, компания разослала по тем же адресам просьбу уничтожить полученные данные и затем сообщить им об этом.

Скорее всего, большинство врачей так и поступило, но кто знает... а Health Net необходимо принять срочные дополнительные меры, обеспечивающие конфиденциальность информации своих клиентов, число которых в Калифорнии составляет ни много, ни мало 2,2 миллиона человек.

В феврале 2001 года из Швейцарии пришло сообщение о том, что компьютерным злоумышленникам удалось внедриться в информационную систему Всемирного экономического форума (WEF), традиционно проходившего в Давосе. Об этом вторжении WEF предупредила швейцарская ежедневная газета Sonntags Zeitung, которому была передана часть украденной информации. В результате нападения злоумышленники получили доступ к конфиденциальной информации, а организаторы форума не знают имён электронных взломщиков и не могут объяснить, каким образом преступникам удалось получить информацию о номерах кредитных карточек некоторых весьма солидных участников форума. Представитель WEF Чарльз МакЛин заявил, что «форум добьётся расследования этого дела, – и добавил, – если уж преступники смогли атаковать компьютерные сети Пентагона и Госдепартамента США, то неудивительно, что они смогли проникнуть в нашу сеть».

Конечно, странное оправдание, но хотя бы такое, а не полное молчание, как это бывает в некоторых случаях.

В том же феврале был взломан Web-сайт Центрального банка Египта и стёрта вся содержащаяся на нём информация. Указанный Web-сайт, на котором обычно представлен развивающийся флаг Египта, а также присутствует изображение самого банка, предстал перед клиентами абсолютно чёрной страницей с красным текстом, написанном на португальском языке, а также

несколькими бразильскими адресами в Интернет. Надпись, оставленная электронным взломщиком, гласила: «Ха-ха-ха, и вы до сих пор говорите, что бразильцы тупые?»

Для того чтобы избежать подобного в будущем и успокоить своих клиентов руководство банка предприняло дополнительные меры компьютерной безопасности.

В мае 2001 года 28-летнего жителя Сан-Хосе Макса Рэя Батлера, известного в Интернет под именем «Max Vision», приговорили к тюремному заключению сроком на 18 месяцев и штрафу в 60 тысяч долларов за взлом нескольких сотен компьютерных сетей Министерства обороны США и ещё двенадцати федеральных агентств. С 1998 года, будучи информатором подразделения по кибербезопасности ФБР США (!), Батлер успешно внедрялся в сети нескольких военно-воздушных баз, в сеть центра НАСА в Алабаме и в компьютеры канцелярии Министерства транспорта США. От его действий пострадали также компьютеры лаборатории Калифорнийского университета, Министерства торговли США и Министерства внутренних дел США. Согласно документально подтверждённым данным, всякий раз, получая приоритетные права при внедрении в систему, Батлер использовал одну и ту же программную ошибку в популярной компьютерной программе BIND (Berkley Internet Name Domain), которая позволяет переводить IP-адреса в доменные имена и наоборот. Помимо этого, Батлер взломал сети Интернет-провайдера Aimnet и получил доступ к паролям 477 его пользователей.

24 июля 2001 года швейцарские компьютерные злоумышленники смогли проникнуть в почтовый сервер компании SwissOnline и получить доступ к 250 тысячам электронных адресов, паролям и счетам, включая принадлежащие посольствам Франции, Израиля, Монако, Швеции и Уругвая, известным политикам, телевизионным звёздам, артистам и спортсменам, а также Ассоциации иностранных банков (Association of Foreign Banks), Центру кредитных карт банка UBS, Церкви сайентологов в Цюрихе и швейцарской федерации полицейских. Представитель SwissOnline подтвердил факт

взлома защиты Web-сервера, о котором сообщил воскресный выпуск газеты. В газете была рассказана история о том, как в её офис по почте был прислан CD-ROM, содержащий 185 тысяч паролей к счетам SwissOnline и 250 тысяч электронных адресов. Диск был отправлен «молодым человеком, который представил себя, как хорошо информированного в делах швейцарского компьютерного андеграунда», – сообщала газета. По предположению специалистов, компьютерные злоумышленники имели доступ к почтовому серверу SwissOnline в течение нескольких месяцев, что позволяло им читать, удалять, изменять и пересылать чужие письма. Только через сутки специалисты закрыли «дыры» в безопасности сервера, а пользователи получили предупреждение о происшествии и совет сменить свои пароли.

Профессор Питер Хейзман, глава Института Интернет-технологий при Техническом институте в своём интервью газете Sonntags Zeitung сказал, что SwissOnline пренебрегал элементарными правилами защиты, которые его студенты изучают во время первого семестра. Он также добавил, что при таком отношении к защите любой начинающий компьютерный преступник мог проникнуть в почтовый сервер SwissOnline. Однако представители SwissOnline отрицали справедливость этого утверждения: «Мы знаем, что это был не просто любитель, а профессионал. Не просто было войти в нашу систему, и это была тяжёлая работа».

26 июля 2001 года неизвестные взломали несколько Web-сайтов местных правительств Уэльса и заменили официальное приветствие, содержащееся на главной странице, своим собственным сообщением. Причём, за первое полугодие 2001 года были предприняты три неудачные попытки преодолеть защиту Web-сайтов и только четвёртая увенчалась «победой» компьютерных преступников. Интересно, что успешная попытка была осуществлена после того, как местные органы самоуправления, напуганные тремя предыдущими атаками, приняли меры по повышению уровня информационной безопасности Web-сайтов.

В результате представителям правительства Уэльса пришлось убеждать общественность в том, что никакой важной информации похищено не было, а Web-сайты восстановлены и работают в нормальном режиме.

В августе 2002 года была опубликована информация о том, что за последние два месяца был взломан целый ряд компьютеров, входящих в правительственные сети США. Электронный взлом был осуществлён, якобы, с исследовательской целью, сотрудниками американской фирмы ForensicTec, специализирующейся на проблемах компьютерной безопасности. Данная акция была предпринята специалистами ForensicTec из-за серьёзной обеспокоенности состоянием безопасности компьютерных сетей американского правительства. По итогам эксперимента, сотрудники ForensicTec заявили, что данные правительства США являются недостаточно защищёнными и легко могут стать жертвой компьютерных преступников. В качестве подтверждения представители ForensicTec привели тот факт, что для проникновения в сети оказалось достаточным использовать исключительно бесплатно распространяющиеся в Интернет компьютерные программы. В результате, в руках ForensicTec оказалась такая конфиденциальная информация, как электронные письма, радио шифры и данные о работниках государственных учреждений.

Пентагон в свою очередь достаточно болезненно отреагировал на попытку дискредитации компьютерных сетей правительства и обвинил сотрудников ForensicTec в совершении преступления и кражи ценных данных. Круг замкнулся.

Приведённые нами выше примеры с одной стороны преднамеренно отражают собой широкую географию, а с другой всего лишь небольшую часть широкого спектра компьютерных преступлений, который затрагивает взаимоотношения общественности, пользователей и владельцев информационных ресурсов между собой и с официальными органами власти, которые при-

званы предпринимать все меры для подавления компьютерной преступности как национального и наднационального, глобального явления[61].

Без рассмотрения на конкретных примерах этого важнейшего аспекта жизнедеятельности мирового компьютерного сообщества нам было бы трудно продвигаться далее в понимании такого сложного и комплексного явления как компьютерная преступность. Мы, конечно, не собираемся «тыкать пальцем» в кого бы то ни было и, если акцент в приведённых примерах несколько смещён в сторону США, то это объясняется тем, что именно эта страна добилась наибольших успехов в области использования современных информационных технологий и компьютерной техники.

Ведь хорошо известно, что лидеру достаются не только награды и титулы победителя, но и всевозможные «шишки» и сопутствующие им экономические потери, а также неизбежные ошибочные технические и социально-политические решения и инициативы. С этой точки зрения компьютерная преступность отнюдь не является исключением из правил и лидерство США в сфере высоких технологий предполагает пристальное внимание к пройденному ими пути, заставляет исследовать как негативный, так и позитивный опыт этой сверхдержавы в осуществлении деятельности по защите своих компьютерных систем от нарушителей, принятии необходимых мер по обеспечению стабильного функционирования аппаратных средств и программного обеспечения.

Нравится это или нет, но остальные страны мира идут как бы «в кильватере» США, используя уже апробированную ими методологию и специфические подходы к борьбе с компьютерной преступностью, изучая сделанные ими ошибки и, соответственно, во многих случаях обходя стороной ложные ориентиры, а также избегая невосполнимых потерь всех видов ресурсов, в том числе и информационных[62].

А как складываются дела на этом поприще в нашей отчизне?

---

[61] Батурин Ю. М., Жодзинский Н. Л. Компьютерная преступность и компьютерная безопасность. М., 1991.

[62] Крылов В. В. Информационные компьютерные преступления. М., 1997.

Россия известна во всём мире не только балетом, ракетной техникой и вооружением, но и своими программистами, в том числе и компьютерными правонарушителями. Согласно данным опроса, проведённого в Интернет в начале 2001 года, 82% от общего числа опрошенных считают, что лучшие в мире «электронные взломщики» – русские, и только 5% настаивают на превосходстве американцев. «Российское высшее образование всегда славилось высоким уровнем преподавания технических наук, которые и лежат в основе «электронного взлома», однако, на российском рынке существует недостаточное число рабочих мест для подобных специалистов», – считает менеджер антивирусных исследований финской компании F-Secure Микко Хиппонен. По его мнению, именно россияне стоят за большинством известных, но не раскрытых и порой очень эффектных и прибыльных электронных нападений на компьютерные системы различных стран.

Со своей стороны подливает керосина в огонь и британская компания Information Risk Management (IRM), специализирующаяся на исследованиях в области компьютерной безопасности.

По данным, представленным в конце декабря 2001 года одним из ведущих экспертов IRM в области компьютерной безопасности, её техническим директором Нейлом Барреттом, российские криминальные круги взяли на прицел Web-сайты компаний, специализирующихся на рынке онлайновых азартных игр. Компьютерные преступники, работающие на мафию, занимаются вымогательством, шантажируя эти Web-сайты DoS атаками, и пока компании не могут принять действенных мер по обеспечению защиты. По его словам, механизм таков: сначала Web-сайт подвергается кратковременной DoS атаке, длящейся минут пятнадцать, а затем вымогатели списываются с компанией, владеющей Web-сайтом, и следом за ещё одной атакой поступает требование выкупа.

По мнению г-на Барретта, всё это сильно напоминает версию предложения «защиты», обкатанную мафией за долгие годы применения, только на новом технологическом уровне. Он говорит также, что не удивился бы,

узнав, что, по крайней мере, некоторые из компаний предоставили запрошенные суммы. Определяя объёмы «отступного», преступники рассчитывают стоимость минуты простоя сайта во время DoS атаки и затем просят отчислять получившуюся в результате сумму ежемесячно за «консультационные услуги по безопасности». Что указывает на криминальность всей схемы, так это реалистичность запросов. Они, как правило, основываются на малой доле действительных убытков, понесённых компанией за время простоя Web-сайта, а малый процент от десятков тысяч недополученных фунтов стерлингов за консультационные услуги – это уже бизнес-план. Пока электронные атаки направляются только против работающих на рынке игорного бизнеса Web-сайтов, однако жертвой может оказаться любая онлайновая компания, предупреждает г-н Барретт. Он считает, что остановить вымогательство можно только усилив защиту от DoS атак, что представляет немалую трудность, поскольку они могут исходить откуда угодно. Это не является невозможным, однако почти невыполнимо, объясняет он. В качестве хоть сколько-нибудь действенной меры компаниям предлагается обращаться в полицию, с тем, чтобы компьютерных преступников можно было отследить по передвижению выплаченных денег. Пока всё, вроде бы, логично и вдруг! Г-н Барретт, оказывается, убеждён, что ниточки тянутся к русской мафии, поскольку деньги и сообщения часто направляются через Санкт-Петербург, однако пока неясно, служит ли он центром криминальной цепочки, или только перевалочной базой.

Пока не ясно, однако картина уже практически завершена, цепочка выстроена, приоритеты расставлены, выводы сделаны, и указующий перст направлен в нужную сторону. Это уже было, было, ещё раз было… и нас этим не особенно-то удивишь.

Новые информационные процессы сформировали и новые общественные отношения, появилась необходимость их упорядочения. Традиционно функции социального регулятора выполняло право, однако в связи с бурным развитием информационных технологий обнаружилось его отставание –

юристы оказались «позади» инженеров, и поэтому им в спешном порядке приходится разрабатывать новые нормы, приспосабливать действующее законодательство к складывающимся условиям. Не явилось исключением и уголовное право. С развитием информационного общества появилась потребность в защите его главного движущего фактора – информации, а теперь и особого её вида – компьютерной информации. Пресечь наиболее опасные проявления человеческого поведения в информационной сфере – это задача уголовного законодательства.

По мере компьютеризации хозяйственной, управленческой, финансовой и коммерческой деятельности у нас в стране появились новые виды преступлений, которые стали называться компьютерными, исходя из терминологии зарубежной юридической практики. Первое преступление с использованием компьютера в Советском Союзе было официально зарегистрировано в 1979 году в г. Вильнюсе, столице Республики Литва. Тогда, по оценке правоохранительных органов, нанесённый государству ущерб составил 78,5 тысяч рублей, что, при существовавшем курсе доллара США по отношению к рублю, вылилось в достаточно крупную сумму и в этой валюте, приближающуюся к 90 тысячам долларов. Данное происшествие было зафиксировано в международном реестре правонарушений в области компьютерной преступности и явилось как бы вехой или, если хотите, точкой отсчёта зарождения и дальнейшего развития этого вида преступлений в нашей стране.

В течение 80-х годов прошлого века компьютерные преступления в СССР носили спорадический характер и не доставляли больших хлопот правоохранительных органам. Например, экономист Брестского областного производственного объединения совершила хищения денежных средств. Из материалов уголовного дела видно, что, будучи экономистом по учёту заработной платы и отвечая за достоверность документов, а также сдачу их в отраслевую автоматизированную систему управления, она, начиная с 1981 года, на протяжении нескольких лет вносила в документы на начисление заработной платы подложные данные. В результате чего заработная плата начислялась

на счета вымышленных лиц и переводилась в сберкассы г. Бреста на специально открытые счета. Всего, таким образом, было похищено 22960 рублей, и в 1988 году она была осуждена Брестским областным судом по ч. 1 ст. 91 УК БССР.

Для сравнения, в Италии, в 1983 году с помощью компьютеров было украдено из банков более 20 млрд. лир. Во Франции в 80-е годы количество подобных преступлений увеличивалось на 30–40% ежегодно, а в Германии компьютерная преступность похищала каждый год несколько миллиардов марок. По данным американского Национального центра информации по компьютерной преступности за 1988 год компьютерная преступность нанесла американским фирмам убытки в размере 500 млн. долларов, а всего ежегодные потери от неё в Европе и Америке составляли несколько десятков миллиардов долларов.

Впервые о проблемах борьбы с компьютерной преступностью в России отечественная криминалистическая наука официально заявила в июле 1992 года, когда научно-исследовательским институтом проблем укрепления законности и правопорядка Генеральной прокуратуры Российской Федерации и Экспертно-криминалистическим центром Министерства внутренних дел Российской Федерации был организован межведомственный семинар «Криминалистика и компьютерная преступность». Первое же подразделение «по борьбе с хищениями, совершаемыми с использованием электронных средств доступа» было создано в Главном управлении по экономическим преступлениям Министерства внутренних дел Российской Федерации лишь в январе 1997 года, и входило в эту группу всего четыре сотрудника[63].

Статистика крупных компьютерных преступлений с участием российских граждан, расследованных в 90-е годы и официально зарегистрирован-

[63] В США и странах Европейского Союза составы компьютерных преступлений присутствовали в законе уже с конца 80-х годов, а в России глава «Преступления в сфере компьютерной информации», включающая три статьи (неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации компьютеров и компьютерных сетей), появилась в Уголовном кодексе Российской Федерации только в 1997 году. Для сравнения: в Швеции несанкционированное получение компьютерных данных было объявлено преступлением ещё в 1973 году.

ных Главным информационным центром Министерства внутренних дел Российской Федерации (ГИЦ МВД России) свидетельствует в пользу, казалось бы, достаточно «спокойного» развития событий по сравнению, например, с положением дел в США.

Однако общая динамика совершения этих преступлений, по оценке ГИЦ МВД России, выглядит достаточно угрожающе. Тем более что по оценкам отечественных и зарубежных специалистов при 90% уровне латентности компьютерных преступлений из выявленных 10% раскрывается только 1%. И это плюс к тому, что защищённость компьютерных систем в нашей стране находится на весьма низком уровне.

Известный российский специалист А. Агеев (Научно-исследовательский центр компьютерной безопасности) в порядке эксперимента проник в вычислительную сеть Главного управления Центрального банка России по г. С.-Петербургу и получил доступ к счетам более чем 44 тысяч вкладчиков «Промстройбанка». Нетрудно представить себе последствия такого деяния, если бы на месте уважаемого эксперта оказался компьютерный преступник, так как подобное несанкционированное проникновение в сеть дало бы ему широкие возможности искажения, кражи и уничтожения важной информации, что, в свою очередь, могло привести к значительным финансовым и временным потерям.

Итак, получение информации о счетах банков не представляет собой неразрешимую для компьютерного преступника проблему. Ну, а затем, можно использовать добытые сведения в целях собственного обогащения, например, переводя суммы с разных счетов на подставные. Достаточно проделать несколько рутинных операций и ищите ветра в поле. Ведь если не «зарываться», то владельцы миллиардных счетов вряд ли обнаружат, что у них исчезло со счетов несколько десятков или сотен тысяч рублей.

Итак, начиная с 90-х годов и до настоящего времени направленность компьютерных преступлений можно кратко охарактеризовать с помощью следующих примеров:

в 1991 году преступники, являвшиеся сотрудниками вычислительного центра Внешэкономбанка, похитили у своего же банка 125,5 тысяч долларов, переводя их на свои личные счета, открытые по поддельным паспортам;

в 1992 году один из штатных сотрудников Игналинской атомной электростанции, исходя из корыстных мотивов, задействовал в автоматизированной системе управления этой электростанцией прикладное программное обеспечение, которое не было разрешено к применению. В результате этой деятельности произошло искажение данных, отображаемых на пульте оператора атомного реактора, повлекшее за собой возникновение непредвиденной ситуации, последствия которой могли стать катастрофическими. Летом этого же года представитель зарубежного алмазного концерна скопировал на свои дискеты оценённую впоследствии как служебная тайна информацию из компьютеров сети алмазодобывающего объединения России;

в 1993 году в одном из коммерческих банков России было похищено программное обеспечение системы электронных платежей с использованием кредитных карт. В сентябре того же года была пресечена попытка «электронного мошенничества» в особо крупных размерах на сумму более 68,3 млрд. рублей из Главного расчётно-кассового центра Центрального банка России;

в 1994 году житель Санкт-Петербурга Владимир Лёвин «взломал» компьютерную сеть отдела денежных переводов американского Citibank и перевёл на счета своих сообщников в банках США, Нидерландов, Финляндии, Германии и Израиля более 10 млн. долларов;

в 1995 году было пресечено более ста попыток незаконного проникновения в компьютерную сеть Центрального банка России для хищения денежных средств, а всего за 1993–1995 годы выявлено и пресечено более 300 попыток незаконного проникновения в компьютерную сеть Центрального банка России с целью незаконного получения денежных средств;

в 1996 году со счетов крупных компаний преступники пытались внедрить в банковскую компьютерную систему Москвы поддельные векселя с

реквизитами Московского сберегательного банка. Эта операция проводилась с целью хищения 375 млрд. рублей и 80 млн. долларов. В этом же году было пресечено мошенничество одного из сотрудников банка «Российский кредит», который ввёл в банковский компьютер информацию, позволявшую ему переводить деньги банка на личный счёт. В феврале 1996 года один из инженеров подотдела ГАИ за определённую плату внёс в компьютерную базу данных РЭО ГАИ УВД г. Кургана заведомо ложные сведения о регистрации автомобилей[64]. В сентябре 1996 года пользователи информационной системы ИнфоАрт, распространяющей котировки ценных бумаг по системе Интернет, получили на экраны вместо экономической информации картинки эротического содержания;

в 1997 году было зарегистрировано примерно сто серьёзных компьютерных преступлений в кредитно-финансовой сфере (0,02% от общего числа преступных посягательств в этой области), а размер понесённого ущерба составил 20 млрд. рублей. Вместе с тем, согласно результатам независимых опросов, проведённых в то время социологическими службами, каждый второй респондент прогнозировал рост банковских убытков из-за возрастания вероятности электронного мошенничества. Для сравнения, по данным совместного отчёта Института компьютерной безопасности и ФБР США, в котором приняли участие представители 250 компаний этой страны, убытки от компьютерных преступлений в 1997 году составили в общей сложности 137 млн. долларов, что на 37% превысило уровень 1996 года. Наибольшую опасность в США представляла собой компьютерная преступность в финансовой сфере и отмечалась тенденция к быстрому росту компьютерных преступлений в банковской сфере;

в 1998 году тенденция к росту компьютерных преступлений не изменилась, и только в кредитно-финансовой сфере было зарегистрировано более ста подобных преступлений и попыток преступлений. Пойман и приговорён

[64] Сорокин А. В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия и расследования. Курган, 1999.

к тюремному заключению сроком на 5 лет математик Владимир Лёвин. Ему было предъявлено обвинение в нападении на систему Citibank и в краже 12 млн. долларов с банковских счетов. Многие специалисты придерживались мнения, что и в мошенничестве с программным обеспечением Global Positioning System также виноваты наши соотечественники;

в 1999 году, по словам официальных представителей Газпрома – крупнейшего российского монополиста и самого большого поставщика и добытчика газа в Восточной Европе, Газпром подвергался постоянным электронным атакам со стороны компьютерных преступников. Причём, со временем их активность по отношению к компьютерной системе Газпрома постоянно возрастала. Некоторые атаки были достаточно удачны, к примеру, в течение какого-то времени распределительный щит корпорации, управляющий потоком газа, был в руках электронных взломщиков, обошедших его защиту. Представители Газпрома оставили без комментариев сумму ущерба, которую понесла корпорация из-за этой, а также всех остальных атак. Вообще, в России, включая атаки на Газпром, за 1999 год было зафиксировано 852 электронных нападения, что в несколько раз больше, чем годом раньше;

в 2000 году по данным ГИЦ МВД России было зарегистрировано уже 1463 преступления в сфере высоких технологий. Компьютерный злоумышленник, известный под кличкой «Maxus», украл номера кредитных карт из Интернет-магазина CD Universe и потребовал выкуп в 100 тысяч долларов. Когда ему было отказано, он разместил 25 тысяч номеров кредитных карточек на Web-сайте. Интернет вора так и не нашли, но, по мнению западных экспертов, его родиной следует считать Россию. 8 июня 2000 года примерно в 11:15 по московскому времени неизвестными злоумышленниками был взломан Web-сайт Российской торговой системы (РТС) www.rtsnet.ru. На главной странице была помещена надпись: «Hacked by NIXSO ... Best regards». Однако в течение буквально нескольких минут Web-сайт был восстановлен силами программистов самой компании. В октябре ещё раз подтвердилась репутация России как родины наиболее одарённых программи-

стов, так как стало известно, что украденные пароли компании Microsoft для доступа к исходным кодам были отправлены из её сети по адресу электронной почты в Санкт-Петербурге. Конечно, это не являлось прямым доказательством причастности представителей нашей компьютерной преступности к этому деянию, но многие зарубежные специалисты, «пользуясь случаем», на все лады расхваливали искусность русских в связи с этим делом;

в 2001 году по данным того же центра общий ущерб от преступлений только в сфере электронных платежей в России составил около 6 млрд. долларов. По сообщению представителя компании «Изософт» 5 декабря был произведён взлом Интернет-сайта компании. Злоумышленник разместил хулиганскую надпись на домашней странице, а также произвёл другие изменения внутри Web-сайта, и, в целом, «работал», как минимум, в течение полутора часов. В результате Web-сайт был отключён от Интернет, что привело к прекращению приёма заказов и других операций. Затем для обеспечения безопасности посетителей Web-сайт был полностью восстановлен с резервной копии. Вероятной причиной электронного взлома представители компании называют «засылку» почтового сообщения с новым компьютерным вирусом на компьютер администратора Web-сайта компании. Как сообщали представители «Изософт», в изучении происшествия и выработке мер по предотвращению подобных происшествий в дальнейшем принимали участие специалисты по компьютерной безопасности таких известных российских компаний как разработчика антивирусного программного обеспечения «ДиалогНаука» и Интернет-провайдера «Зенон Н.С.П.». В конце года в г. Самара сотрудниками ГУВД Самарской области было установлено, что трое нигде не работающих молодых человека 1980–1982 года рождения в течение нескольких месяцев осуществляли «неправомерный доступ к ресурсам Интернет путём использования чужих реквизитов». По словам представителя ГУВД Алексея Саломатина, их деятельность привела к модификации базы данных провайдера ЗАО «Крафт-С», а ущерб составил 5000 рублей. Во всех трёх случаях

были возбуждены уголовные дела по ст. 272–1 УК РФ. Мера пресечения – подписка о невыезде;

в 2002 году, как сообщал представитель Министерства внутренних дел Российской Федерации (МВД России) Константин Мачабели на проведённом этим министерством специальном брифинге, в стране было совершено 6251 преступление в сфере высоких технологий, причём, по данным указанного управления 90% этих преступлений, в том числе и компьютерных преступлений, по-прежнему остаются латентными. В ходе всероссийской конференции «Информационная безопасность России» официальную информацию огласил начальник Главного управления специальных технических мероприятий МВД России Борис Мирошников. По его словам, в стране за 2002 год зарегистрировано 3371 преступление в области компьютерной информации, из числа зарегистрированных правонарушений свыше 90% составляют преступления, связанные с незаконным доступом к информационным ресурсам.

23 января 2002 года в Самаре прошёл суд над 20-летним администратором локальной сети одного из самарских техникумов Е. Меретиным. По данным информационного портала «Самара сегодня», он неоднократно с домашнего и рабочего телефонов выходил в Сеть, используя чужие реквизиты (в частности, клиентов компаний «Самара-Интернет» и «Крафт-С»). Ущерб от его деятельности составил 10 тысяч рублей, а обвинение было вынесено по двум статьям УК РФ: за неправомерный доступ (ст. 272) и за нанесение материального ущерба (ст.161 ч.1), наказание по которым предусматривает 5 лет лишения свободы. Впрочем, судьи учли «активное сотрудничество обвиняемого со следствием, его деятельное раскаяние, а также полное возмещение им материального ущерба» и ограничились наложением штрафа в размере трёх месячных окладов.

В конце мая 2002 года была реализована массовая электронная атака на Интернет представительства МВД России, включая и различные подведомственные ему организации. По имеющимся данным от рук компьютерных преступников пострадали серверы www.mvdinform.ru (собственный Web-

сайт МВД России), www.ma-mvd.ru (Web-сайт Московской академии МВД России), www.crime.ru и www.policeacademy.ru. На главных страницах указанных Web-сайтов появились сообщения о взломе, подписанные группой электронных взломщиков под названием «NERF». Эти Web-сайты объединены не только своей принадлежностью к структуре МВД России, но и тем, что все они разработаны (как хостинг, так и дизайн) одним предприятием. Использование одного разработчика привело к тому, что все серверы функционировали под управлением единого программного обеспечения: Apache (версия 1.3.23) и операционной системы Linux (версия ядра предположительно 2.2.13, 2.2.14 или 2.2.19). Именно эти два факта, вероятнее всего, и позволили компьютерным преступникам взломать одновременно несколько Web-сайтов МВД России.

В июне 2002 года представители Администрации Президента Российской Федерации подтвердили, что за первые три часа работы нового президентского Web-сайта было совершено несколько десятков попыток взломать этот Интернет-ресурс главы российского государства, но все попытки были успешно пресечены соответствующими службами. Открывшийся обновлённый сайт Президента Российской Федерации оказался очень популярным, о чём свидетельствует число его посетителей: за первые три часа работы Web-сайт посетило более 10 тысяч пользователей Интернет.

Ровно в 0:00 16 декабря 2002 резко возросло количество запросов с различных IP-адресов на титульную страницу Web-сайта afisha.ru. Анализ показал, что, по всей видимости, в Интернет активизировался компьютерный «червь», написанный неизвестными вирусописателями. При наличии соединения пользователя с Интернет-червь выкачивал титульную страницу afisha.ru со средней частотой 10 запросов в секунду. Симптомы проявились в виде увеличения количества запросов на передачу HTML-кода страниц до 200 запросов в секунду. При этом на Web-сайте одновременно было около ста посетителей. За сутки количество загрузок титульной страницы достигло нескольких миллионов, то есть нагрузки на серверы afisha.ru были сопоста-

вимы с нагрузками на серверы широко известного портала Яndex. Глубокой ночью количество запросов уменьшалось, но сохранялось нереальное для этого времени суток количество запросов (до пятнадцати в секунду). При этом серверы afisha.ru выдержали нагрузку и продолжали работать в штатном режиме. При исследовании логов доступа выяснилось, что с большого количества различных IP-адресов в различное время происходит всплеск активности с различной продолжительностью от нескольких десятков минут до нескольких часов. Например, с одного IP-адреса в первый день электронной атаки было скачано около гигабайта. Проведённое исследование свидетельствовало, что в электронной атаке участвовало не меньше нескольких тысяч компьютеров. К сожалению, у afisha.ru не было доступа хотя бы к одному заражённому компьютеру, однако высококвалифицированные технические специалисты afisha.ru и РосБизнесКонсалтинга идентифицировали несколько сотен инфицированных компьютеров, и эта информация была немедленно направлена российским разработчикам антивирусного программного обеспечения.

В конце декабря 2002 года сотрудники подразделения милиции г. Тула задержали 17-летнего подростка, которому было предъявлено обвинение во взломе компьютерной базы МВД России. Используя откачанную им из Интернет вредоносную компьютерную программу, Сергей Сироткин сумел получить доступ к конфиденциальным данным МВД России. Получив секретную информацию, он разместил в Глобальной сети объявление о её продаже. Прокуратура Центрального района г. Тула возбудила против Сироткина уголовное дело, и за создание, использование и распространение вредоносных компьютерных программ ему грозило три года лишения свободы. Сам Сироткин признался, что взломал базу МВД России, но никому не нанёс вреда, а просто пошутил.

Ну и шуточки у вас, г-н Сироткин …

18 марта 2003 года примерно с 11 до 14 часов доступ к некоторым российским и зарубежным Web-сайтам был затруднён. Проблема возникла из-за

«наводнения» на внешних каналах Интернет-провайдера «МТУ-Интел». Как сообщили в пресс-службе компании затруднения с трафиком возникли лишь у части абонентов и были в оперативном порядке ликвидированы. По информации из неофициальных источников, провайдер подвергся сильнейшей атаке из-за рубежа.

В связи с приведёнными примерами необходимо отметить, что одним из современных инструментов, призванных хотя бы частично компенсировать владельцу компьютерной системы понесённый им ущерб следует признать страхование от электронных компьютерных преступлений. Уже в 1976 году компанией Ллойдс был разработан полис LPO 218 для неамериканских банков, который, однако, не предусматривал покрытие рисков при переводе денежных средств. Но банкирам и страховым компаниям хорошо известно, что основной риск приходится как раз на автоматизированную систему перевода денежных средств[65], и поэтому в настоящее время любой полис страхования банковских рисков, оформленный солидной страховой компанией, предусматривает эту операцию. Первый полис, предоставляющий страховое покрытие от рисков, связанных с компьютерными преступлениями и преступлениями в сфере современных систем телекоммуникаций, используемых финансовыми институтами, был разработан в 1981 году той же компанией Ллойдс в результате проведённых исследований и консультаций со своими клиентами.

С тех пор в первоначальный вариант этого полиса был внесён целый ряд изменений и сейчас используется полис Ллойдс по страхованию от электронных и компьютерных преступлений LSW 238 (Electronic and Computer

[65] Вследствие стремительного роста объёмов межбанковских расчётов в начале 70-х годов прошлого столетия появились системы межбанковского перевода денежных средств, к наиболее известным из которых можно отнести, например, систему SWIFT. Обычно, если два банка планируют заключение межбанковской сделки, в ходе которой один из банков продаёт акции другому банку, то подготовка к ней, чаще всего, начинается с телефонных переговоров представителей этих банков. Они заключают сделку, а последующий расчёт производится техническим персоналом с использованием системы перевода денежных средств, которая является межбанковской системой коммутации сообщений и, следовательно, при её помощи банк может передавать необходимые сообщения другому банку. Сообщения обычно имеют форму долговой расписки и служат либо подобием чека, либо содержат инструкции для банка-получателя о переводе средств со счёта на счёт. Банк-получатель немедленно исполняет поручение, так как считается, что оно пришло к нему по закрытым телекоммуникационным каналам, которые защищены от электронного взлома.

Crime policy – ECC), который предусматривает покрытие двух главных областей риска. К этим областям относятся финансовый убыток в результате мошеннического ввода, изменения или удаления электронных данных или мошеннического изменения или создания программ в компьютерной системе, используемой Страхователем, а также исполнения Страхователем определённых инструкций по переводу денежных средств, которые были изменены в процессе передачи, либо должны были поступить от определённого финансового института, но в действительности поступили от другого отправителя. При этом большинство банкиров и экспертов по безопасности считают, что наибольшая угроза в сфере компьютерных преступлений исходит от всевозможных нарушений или мошенничества со стороны персонала, поэтому они пренебрегают полисом ECC.

Однако при этом следует учитывать, что обычный полис страхования от преступлений требует от Страхователя доказательства того, что сотрудник совершил действие, приведшее к убытку. Во многих случаях это оказывается невозможным, и Страхователь сможет получить возмещение только по полису ECC, так как этот полис исключает лишь мошеннические действия, совершённые сотрудником, личность которого установлена. Именно поэтому любому банку, использующему в своей работе электронные системы перевода платежей или хранящему ценную электронную информацию в компьютерной системе, рекомендуется приобрести полис по страхованию от электронных и компьютерных преступлений.

Полис страхования от преступлений, совершаемых против банков и других финансовых институтов с использованием их компьютерных сетей и систем электронных расчётов, обычно является дополнительным к полису комплексного страхования финансовых институтов (BBB), который предусматривает широкую страховую защиту от целого набора разнообразных рисков. Таким образом, данный вид страхования не обеспечивает покрытия по убыткам, связанным с мошенническими действиями сотрудников Страхователя и эти убытки страхуются по полису BBB, но покрытие от электрон-

ных преступлений возможно, если убыток связан с компьютерными и электронными сетями Страхователя и, скорее всего, вызван преднамеренными действиями сотрудника Страхователя, однако этот сотрудник не может быть идентифицирован.

Риски, которые могут быть застрахованы в соответствии с полисом по страхованию от электронных и компьютерных преступлений, приведены на рис. В9.

§5. Борьба с компьютерной преступностью и государственная политика

Итак, в России компьютерная преступность в качестве нарастающей проблемы, а не отдельных, достаточно разрозненных эпизодов, начала заявлять о себе где-то с середины 90-х годов XX века, когда высказывания типа: « … перед Россией из-за её технической отсталости проблема обеспечения информационной безопасности не будет остро стоять в обозримом будущем, а компьютерные преступления не смогут как-либо повлиять на общую картину преступности в стране», – поросли мхом и потеряли актуальность.

Рис. В.9. Страхование рисков в соответствии с полисом по страхованию от компьютерных преступлений

Следовательно, мы вряд ли ошибёмся, если сделаем следующее предположение: именно к этому времени уже полностью сложилась весьма благоприятная среда для совершения компьютерных преступлений и, в частности, правонарушители новой формации кроме неуёмного желания лёгких денег, которое существовало «испокон веков», получили необходимый и очень

мощный инструмент в виде современного аппаратно-программного обеспечения, в сочетании с недостаточностью оказываемого им противодействия.

Сам по себе рубеж середины 90-х годов далеко не случаен, так как именно в этот период наша страна начала реально включаться в построение единого глобального информационного пространства. Причём, процесс был двухсторонний, как со стороны США, Западной Европы и Японии, так и России как полноправного партнёра международного сообщества.

В это время с одной стороны были инициированы мероприятия по участию России в новых масштабных международных проектах, а с другой стороны, снижены или вообще сняты существовавшие до того неоправданные барьеры и ограничения на импорт и эксплуатацию электронно-вычислительной техники. В результате в страну стали осуществляться широкомасштабные поставки западной компьютерной техники[66] и комплектующих, что резко снизило цены, как на сами компьютеры, так и на соответствующую периферию. В стране стало развиваться пусть и «отвёрточное», но собственное производство компьютеров, собранных из импортных комплектующих. Современные компьютеры и соответствующая периферия стали обыденностью не только для крупных учреждений и организаций, но и вполне доступным для приобретения отдельными гражданами повседневным предметом.

Информация в машиночитаемом виде постепенно стала всё больше заменять бумажный документооборот и в частных организациях, и в государственных учреждениях, традиционные машинописные бюро (кто-то о них сейчас помнит?) и, даже, средства массовой информации. В базах данных таких государственных, акционированных и коммерческих структур как МВД

[66] Под компьютерной техникой здесь понимается совокупность носителей, предназначенных для хранения информации в числовом представлении, вычислительных машин, преобразующих информацию в ходе своего функционирования в числовую форму, а также периферийного оборудования, компьютерных сетей. Оперирование информацией в них в виде двоичного кода, предопределяет её легкую пересылку, модификацию, размножение, возможность неограниченного копирования без потерь и искажений.

К носителям компьютерной информации относятся различного рода магнитные, магнитооптические, оптические накопители, запоминающие устройства в виде интегральных схем (например, оперативная память персонального компьютера) и иные материальные объекты и устройства, способные хранить информацию в числовом машиночитаемом виде.

России, Министерство по налогам и сборам Российской Федерации и Государственный таможенный комитет Российской Федерации, Сберегательный банк Российской Федерации, Пенсионный фонд России, Центральная избирательная комиссия Российской Федерации, крупные операторы сотовой связи и банковско-финансовый сектор национальной экономики, электронные магазины – накоплены сведения персонального характера о большей части активного (работники, сотрудники, служащие), да и пассивного (пенсионеры, дети, инвалиды) населения страны.

Таким образом, компьютерная информация вошла во все сферы жизни нашего общества и, как следствие, отсутствие должного внимания к этому явлению породило опасность стремительного развития компьютерной преступности со всеми вытекающими последствиями нарушения процедур сбора, хранения, обработки и передачи данных, что, естественно, влечёт за собой неизбежные присвоение, хищение или искажение личной, служебной, конфиденциальной информации[67].

Параллельно с указанным процессом полным ходом шло комплексное внедрение новых информационных технологий и готовых системных технико-технологических решений, результатом чего стало возможным формирование и последующее совершенствование глобальных компьютерных сетей, а также современных ведомственных сетей и сетей общего пользования[68]. Объединение компьютеров в сети позволило существенно облегчить процесс обмена информацией на национальном и международном уровнях, так как предназначенные для решения конкретных задач компьютеры, объединённые в сеть, в совокупности с программным обеспечением и информационными ресурсами, обрабатываемыми в них, составляют автоматизированную ин-

[67] Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных».

[68] Компьютерная сеть – это два или более двух компьютеров, связанных каналом передачи данных, то есть физической средой (радиолиния, кабель) по которой передаётся информация от одного устройства на другое устройство. При помощи сетей пользователь может иметь доступ к информационным и вычислительным ресурсам других компьютеров, сетям связи различного уровня (локальным, национальным, международным, глобальным).

формационную систему, интегрирующую возможности отдельно взятых компьютеров.

В наши дни, используя электронную систему перевода платежей, банк практически мгновенно может перевести денежные средства в любую точку планеты. Сотрудники финансовых отделов компаний имеют возможность незамедлительного перевода денежных средств с одного континента на другой или же оплаты корпоративных счетов, не выходя из своих офисов и не имея дела с наличными деньгами. Сегодня практически каждый человек может стать причастным к этому процессу: каждый раз, когда вы пользуетесь пластиковыми картами VISA или MasterCard за рубежом, вы используете сложную электронную систему перевода денежных средств, осуществляющую переводы при помощи компьютеров и телекоммуникационных систем, каналы передачи информации которой ведут в США и другие страны.

Но, палка, как известно, имеет два конца.

Интенсификация процесса обмена данными, использования информационных ресурсов, привнесла с собой и новые проблемы. Ведь, если законопослушный пользователь получает всё новые и новые возможности, связанные с его выходом и эксплуатацией внешних информационных сетей, то и компьютерная преступность, естественно, не спит, широко используя в своих целях те же самые информационные сети[69]. А цели эти хорошо известны: использование подключения пользователя к внешним сетям для того, чтобы «исследовать» его компьютер, а также соответствующую локальную сеть, если компьютер пользователя имеет с ней соединение.

Таким образом, благому делу, как водится, сопутствует зло, и информационные ресурсы независимо от того, представляют они собой отдельные документы и массивы документов, находящиеся в индивидуальном пользовании, или документы и массивы документов в информационных системах (архивах, банках и базах данных и пр.), становятся объектом всё большего числа попыток преступного посягательства.

[69] Беляев В.С. Безопасность в распределительных системах. М., 1995.

Существует целый ряд особенностей, которые отличают информационные ресурсы от других видов ресурсов: они не потребляемы и не подвержены ни физическому, ни моральному износу, они по своей сути нематериальны и несводимы к физическому носителю, на котором размещены. Их использование позволяет резко сократить потребление остальных видов ресурсов, что в конечном итоге приводит к экономии средств, а процесс их создания и использования осуществляется с помощью компьютерной техники. То есть, информация стала продуктом общественных отношений, приобрела черты товара. Следовательно, возросла и вероятность преднамеренного хищения, уничтожения или искажения информации, которую Федеральный закон «Об информации, информатизации и защите информации» (утверждён Президентом Российской Федерации 20 февраля 1995 года №24–ФЗ) [70] определяет как «сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления». В данном случае, мы, естественно, имеем в виду информацию в её электронной форме, зафиксированную на машиночитаемом носителе или передаваемую по каналам связи. Кстати, под термином «компьютерная информация», приводимым в Уголовном кодексе Российской Федерации, понимается именно информация, хранящаяся или передаваемая в электронной форме, то есть информационные ресурсы, в процессе создания которых используются возможности компьютерной техники[71].

Российское законодательство определяет безопасность как состояние защищённости жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, а информационной безопасности, наряду с подсистемами экономической, военной, социальной, внутриполитической, международной, экологической и других видов безопасности, отводит важнейшую роль в общей системе обеспечения интересов общества и госу-

[70] Статья 2. Термины, используемые в настоящем Федеральном законе, их определения.

[71] Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. М., 1998.

Уголовный кодекс Российской Федерации. Глава 28: Преступления в сфере компьютерной информации.

дарства. Исходя из этих предпосылок национальные интересы Российской Федерации в области информатизации, ускоренного внедрения инновационных информационных технологий заключаются в соблюдении конституционных прав и свобод граждан в части, касающейся свободного получения, обмена и пользования информацией, а также в защите государственных информационных ресурсов от несанкционированного доступа, в том числе и в преступных целях.

Следовательно, под информационной безопасностью понимается состояние защищённости информационной инфраструктуры всего общества, то есть национальных информационных ресурсов, а также всех без исключения компьютерных систем, которые участвуют как в формировании и использовании единого информационного пространства страны, так и единого глобального информационного пространства.

Доктрина национальной безопасности, например, указывает на усиление внешних угроз в информационной сфере, а также на то обстоятельство, что серьёзную опасность представляют претензии отдельных стран на господство в глобальном информационном пространстве. Причём, подобные устремления сопровождаются как открытыми, так и закрытыми разработками концепций информационных войн, предусматривающих создание средств прямого вмешательства в процесс функционирования информационных инфраструктур и компьютерных систем отдельно взятых стран мира и нацеленных на нарушение штатных режимов работы информационных систем и систем связи, а также на сохранность национальных информационных ресурсов и получение несанкционированного доступа к ним.

Таким образом, в итоге реализации со стороны внешней и внутренней компьютерной преступности угроз информационной безопасности государства и общества, посягательств на национальные информационные ресурсы и компьютерные системы может произойти нарушение режима секретности (конфиденциальности) информации (разглашение, утрата, хищение, утечка и перехват), целостности информации (уничтожение, искажение, подделка),

доступности информации и работоспособности информационных систем (блокирование данных и информационных систем, разрушение элементов информационных систем, компрометация систем защиты информации).

В силу указанных причин «Доктрина информационной безопасности Российской Федерации»[72] – один из основополагающих нормативных документов в области обеспечения информационной безопасности, в частности, и от посягательств компьютерных преступников, – указывает на необходимость обеспечения национальных интересов Российской Федерации в информационной сфере всеми имеющимися в распоряжении государства средствами.

В первом разделе документа недвусмысленно говорится о том, что национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и что в ходе технического прогресса эта зависимость будет постоянно возрастать. Интересы личности в информационной сфере заключаются в реализации конституционных прав человека в защите информации, обеспечивающей личную безопасность, а интересы общества заключаются в обеспечении интересов личности в этой сфере, упрочении демократии и духовном обновлении России. Здесь же выделяются основные составляющие национальных интересов Российской Федерации в информационной сфере, к которым относится соблюдение конституционных прав и свобод человека и гражданина в области получения и использования информации[73]. Для достижения этого требуется обеспечить: личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, защиту своей чести и доброго имени; развитие современных информационных технологий, отечественной индустрии информации; защиту информационных ресурсов от несанкционированного доступа.

В указанных целях необходимо:

[72] «Доктрина информационной безопасности Российской Федерации», утверждена Президентом Российской Федерации 9 сентября 2000 года № Пр–1895.

[73] Федеральный закон «Об информации, информатизации и защите информации».

повысить безопасность информационных систем федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, финансово-кредитной и банковской сфер, сферы хозяйственной деятельности;

повысить безопасность систем и средств информатизации вооружения и военной техники, систем управления войсками и оружием, экологически опасными и экономически важными производствами;

интенсифицировать развитие отечественного производства аппаратных средств защиты информации;

обеспечить защиту сведений, составляющих государственную тайну.

По своей общей направленности угрозы информационной безопасности Российской Федерации доктрина подразделяет на следующие виды:

угрозы развитию отечественной индустрии информации, обеспечению потребностей внутреннего рынка в её продукции и выходу этой продукции на мировой рынок. При этом угрозой развитию отечественной индустрии информации может являться закупка органами государственной власти импортных средств информатизации при наличии отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

угрозы обеспечению сохранности отечественных информационных ресурсов[74];

угрозы безопасности информационных систем, как уже развёрнутых, так и создаваемых на территории России.

Во втором разделе документа приводятся основные методы обеспечения информационной безопасности Российской Федерации и к ним отнесены такие организационно-технические мероприятия как разработка, использование и совершенствование средств защиты информации; создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничто-

[74] Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных».

жение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи; сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны. Далее в документе говорится, что информационная безопасность Российской Федерации является одной из составляющих национальной безопасности Российской Федерации в важнейших сферах жизнедеятельности общества и государства.

Например, в сфере экономики обеспечение информационной безопасности играет ключевую роль в обеспечении национальной безопасности Российской Федерации в целом. Причём, неблагоприятному воздействию в сфере экономики, в том числе и со стороны компьютерной преступности, наиболее подвержены системы бухгалтерского учёта, а также системы хранения финансовой, биржевой, налоговой, таможенной информации предприятий, учреждений и организаций независимо от формы собственности.

Иными словами, бесконтрольная деятельность по созданию и защите систем хранения статистической, финансовой, биржевой, налоговой, таможенной информации создаёт реальную угрозу безопасности России в экономической сфере. Аналогичные угрозы возникают и при бесконтрольном привлечении иностранных фирм к созданию подобных систем, поскольку при этом складываются благоприятные условия для несанкционированного доступа к конфиденциальной экономической информации и для контроля над процессами её передачи и обработки со стороны иностранных спецслужб. В тоже время критическое состояние предприятий разрабатывающих и производящих средства защиты информации, приводит к широкому использованию соответствующих импортных средств, что создаёт угрозу возникновения технологической зависимости России от иностранных государств.

Существенный экономический ущерб хозяйствующим субъектам может быть нанесён также вследствие разглашения информации, содержащей коммерческую тайну. Кроме того, в системах сбора, обработки, хранения и передачи финансовой, биржевой, налоговой, таможенной информации

наиболее опасным противоправным деянием признаётся несанкционированное копирование информации. Это касается и федеральных органов исполнительной власти, занятых формированием и распространением информации о внешнеэкономической деятельности Российской Федерации.

В соответствии с вышеизложенным, основной мерой по обеспечению информационной безопасности в сфере экономики признаётся разработка национальных сертифицированных средств защиты информации и внедрение их в системах и средствах сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации.

В сфере внутренней политики наиболее важными объектами обозначены конституционные права и свободы человека и гражданина, а наибольшую опасность представляет нарушение конституционных прав и свобод граждан, реализуемых в информационной сфере. В сфере внешней политики к наиболее важным объектам относятся информационные ресурсы:

федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях;

представительств федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, на территориях субъектов Российской Федерации;

российских предприятий, учреждений и организаций, подведомственных федеральным органам исполнительной власти, реализующим внешнюю политику Российской Федерации;

Кроме того, к наиболее важным объектам в сфере внешней политики относятся и блокирование деятельности российских средств массовой информации по разъяснению зарубежной аудитории целей и основных направлений государственной политики Российской Федерации, её мнения по социально значимым событиям российской и международной жизни.

Из внешних угроз наибольшую опасность представляют попытки несанкционированного доступа к информации федеральных органов исполнительной власти, реализующих внешнюю политику Российской Федерации, российских представительств и организаций за рубежом, представительств Российской Федерации при международных организациях.

В области науки и техники наиболее важными объектами являются открытия, не запатентованные технологии, промышленные образцы, полезные модели и экспериментальное оборудование, а к числу основных внутренних угроз следует отнести сложности реализации мероприятий по защите информации, особенно на акционированных предприятиях, в научно-технических учреждениях и организациях[75].

В сфере духовной жизни к числу основных объектов относятся неприкосновенность частной жизни, личная и семейная тайна, а также объекты интеллектуальной собственности.

В общегосударственных информационных и телекоммуникационных системах основными направлениями обеспечения информационной безопасности являются: исключение несанкционированного доступа к обрабатываемой или хранящейся в технических средствах информации; обеспечение информационной безопасности при подключении общегосударственных информационных и телекоммуникационных систем к внешним информационным сетям, включая международные; обеспечение безопасности конфиденциальной информации при взаимодействии информационных и телекоммуникационных систем различных классов защищённости. Основными организационно-техническими мероприятиями по защите информации признаётся создание и применение информационных и автоматизированных систем управления в защищённом исполнении.

В сфере обороны к объектам обеспечения информационной безопасности отнесены:

[75] Закон Российской Федерации «Об авторском и смежных правах».

информационная инфраструктура центральных органов военного управления и органов военного управления видов Вооруженных Сил Российской Федерации и родов войск, объединений, соединений, воинских частей и организаций, входящих в Вооруженные Силы Российской Федерации, научно-исследовательских учреждений Министерства обороны Российской Федерации;

информационные ресурсы предприятий оборонного комплекса и научно-исследовательских учреждений, выполняющих государственные оборонные заказы либо занимающихся оборонной проблематикой;

программно-технические средства автоматизированных и автоматических систем управления войсками и оружием, вооружения и военной техники, оснащённых средствами информатизации;

информационные ресурсы, системы связи и информационная инфраструктура других войск, воинских формирований и органов.

В этой сфере внутренними угрозами являются нарушение установленного регламента хранения информации, находящейся в штабах и учреждениях Министерства обороны Российской Федерации, а также на предприятиях оборонного комплекса страны. Главными специфическими направлениями совершенствования системы обеспечения информационной безопасности признаются постоянное совершенствование средств защиты информации от несанкционированного доступа и развитие защищённых систем связи и управления войсками и оружием.

В правоохранительной и судебной сферах в качестве наиболее важных объектов выделены:

информационные ресурсы федеральных органов исполнительной власти, реализующих правоохранительные функции, судебных органов, их информационно-вычислительных центров, научно-исследовательских учреждений и учебных заведений, содержащие специальные сведения и оперативные данные служебного характера;

информационно-вычислительные центры, их информационное, техническое, программное и нормативное обеспечение;

информационная инфраструктура (информационно-вычислительные сети, пункты управления, узлы и линии связи).

Внутренними угрозами, представляющими наибольшую опасность для указанных объектов, являются нарушения установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных базах данных и использующейся для расследования преступлений[76]. Наряду с широко используемыми общими методами и средствами защиты информации в правоохранительной и судебной сферах могут применяться также специфические методы и средства обеспечения информационной безопасности. Главным из них является создание защищённой многоуровневой системы интегрированных банков данных оперативно-розыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем.

В условиях чрезвычайных ситуаций к специфическим для данных условий направлениям обеспечения информационной безопасности относится разработка специальных мер по защите информационных систем, обеспечивающих управление экологически опасными и экономически важными производствами.

Основным направлением международного сотрудничества Российской Федерации в области обеспечения информационной безопасности признано предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной, в том числе и компьютерной преступностью,

[76] Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных».

международным, в том числе и электронным, терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

Таким образом, среди основных подходов, на которых основывается государственная политика обеспечения информационной безопасности страны, в которую составной и неотъемлемой частью входит борьба с компьютерной преступностью, можно выделить приведённые на рис. В10.

В сжатые сроки и коренным образом были перестроены процедуры поиска, сбора, обработки, хранения и передачи данных, которые обусловили ускоренное формирование и развитие так называемой информатизации, пронизавшей за последние 15–20 лет все сферы человеческой деятельности от предоставления бытовых услуг до международного бизнеса, представляющего собой современный банковский сектор экономики, промышленность и т. д.

Эти без преувеличения тектонические сдвиги затронули представителей практически всех слоёв мирового сообщества и во многом задают генеральное направление дальнейшего развития общественных, социальных, политических и экономических отношений во всём мире, а темпы развития человечества сейчас определяются количеством и качеством доступной информации. Сейчас, в силу всё возрастающей роли информации в обеспечении нормальной жизнедеятельности мирового сообщества, компьютерные преступления с использованием инновационных информационных технологий, современных аппаратно-программных средств и существующих подходов к их подготовке и совершению признаны во всём мире, как уже говорилось, крайне опасным и стремительно набирающим силу явлением, и изложенные выше факты свидетельствует о всё возрастающей необходимости борьбы с ним.

В настоящее время меры противодействия компьютерным преступлениям принято подразделять на программно-технические, организационные и правовые.

К программно-техническим мерам можно отнести, например, защиту от несанкционированного доступа к системе, профилактику от вредоносных компьютерных программ, разработку и использование специальных аппаратных и программных комплексов для обеспечения информационной безопасности, резервирование и дублирование особо важных компьютерных подсистем и систем, применение конструктивных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещении кодовыми замками, установку сигнализации и пр.

Рис.В.10. Основные подходы государственной политики по обеспечению информационной безопасности

К организационным мерам обычно относят охрану компьютерных систем и вычислительных центров, тщательный подбор кадров, исключение случаев ведения особо важных работ только одним человеком, наличие плана на случай непредвиденных и чрезвычайных обстоятельств, а также плана восстановления работоспособности компьютерной системы после произошедшего сбоя или отказа и т. п.

К правовым мерам относится разработка нормативных правовых документов, устанавливающих ответственность за компьютерные правонарушения и защищающих интеллектуальную собственность, авторские права и права владения, устанавливающих правила лицензирования и сертификации в области защиты информации, правовые основы деятельности органов государственной и местной власти, а также совершенствование административного, уголовного гражданского законодательства, международного права, принятие соответствующих международных актов, ведение судебных разбирательств.

Однако, по мнению некоторых известных отечественных специалистов[77], меры, применяемые в России в целях борьбы с компьютерной преступностью, выполняются в условиях действия ряда факторов, резко снижающих их эффективность, табл. В8.

Таблица 8

Факторы
снижающие эффективность мер противодействия компьютерным преступлениям

№ п.п.	Формулировка фактора
1.	Отсутствие отлаженной системы правового и организационно-технического обеспечения законных интересов граждан, государства и общества в области информационной безопасности
2.	Недостаточное осознание органами государственной власти на федеральном и, особенно, региональном уровне возможных политических, экономических, моральных и юридических последствий компьютерных преступлений

[77] Курушин В. Д., Минаев В. А. Компьютерный преступления и информационная безопасность. М., 1998.

№ п.п.	Формулировка фактора
3.	Слабая координация действий правоохранительных органов, суда и прокуратуры в борьбе с компьютерными преступлениями, неподготовленность их кадрового состава к эффективному предупреждению, выявлению и расследованию таких деяний
4.	Несовершенство системы единого учёта правонарушений, совершаемых с использованием средств информатизации
5.	Существенное отставание отечественной индустрии средств и технологий информатизации и информационной безопасности от мирового уровня
6.	Ограниченные возможности бюджетного финансирования научно-исследовательских и опытно-конструкторских работ по созданию правовой, организационной и технической базы информационной безопасности

Таким образом, чтобы успешно противодействовать приведённым в табл. В8 негативным факторам, борьба с компьютерными преступлениями обязательно должна быть изменена в своей основе и носить всеобъемлющий характер, что связано с целым комплексом взаимосвязанных причин.

1. Компьютерные преступления недостаточно хорошо изучены – появившись в 60-х годах в качестве быстро нарастающей проблемы, они обратили на себя серьёзное внимание лишь в начале 90-х годов прошлого столетия и, в подавляющем большинстве случаев, борьба с ними носила фрагментарный характер.

2. Наказать даже «вычисленного» правоохранительными органами компьютерного преступника не всегда представляется возможным ввиду того, что при отсутствии соответствующих национальных правовых актов, правовых мер защиты информации в целом[78] он, зачастую, не может быть под-

[78] Правовые меры защиты информации – действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения, препятствующие, тем самым, неправомерному её использованию и являющиеся, совместно с организационными, техническими и физическими мерами защиты информации, сдерживающим фактором для потенциальных нарушителей.

Организационные меры защиты информации – это меры, регламентирующие процессы функционирования системы обработки данных, использование её ресурсов, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности циркулирующей в ней информации.

Технические меры защиты информации – всевозможные электронные устройства и специальные программы, входящие в состав автоматизированной системы, которые выполняют – самостоятельно или в комплексе с другими средствами – функции защиты информации: идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т. п.

вергнут ни административному взысканию, ни уголовному преследованию в своей собственной стране. Более того, используя лакуны и разноголосицу в законодательных системах различных государств, компьютерный преступник, являясь гражданином другого государства, может осуществлять свои атаки против информационных систем с территории страны, где подобные деяния не являются противозаконными.

3. Компьютерная преступность, изначально имевшая черты некоторой хаотичности, в последнее время приобретает всё более упорядоченный характер и проявляет отчётливую тенденцию к смыканию с традиционной организованной уголовной преступностью. Интернет предоставил преступникам огромные возможности в некоторых сферах. Делли-Колли, руководитель Центра по борьбе с компьютерной контрабандой в США, считает, что электронная торговля, например, является совершенным инструментом для распространения нелегальной торговли наркотиками. Более того, Интернет поставил таможенные органы перед дилеммой в плане того, кого следует подвергать такой серьёзной мере как арест. «Мы всегда ориентировались на посредника, контрабандиста, который привозил товар в страну, – говорит Делли-Колли, – Теперь посредников не существует. Они больше не гонят набитые наркотиками трейлеры по автотрассам». При помощи Интернет покупатели наркотиков заключают сделки напрямую за границей, а поставка осуществляется с использованием возможностей наиболее солидных в этой сфере бизнеса и легальных систем доставки, естественно без уведомления о действительном содержимом груза. Кроме наркотиков, которые могут быть заказаны через Интернет, есть также и лекарства, продающиеся только по рецепту.

4. Компьютерные преступления очень сложно предотвратить, так как современные методы их предупреждения далеко не всегда достаточно эф-

---

Физические меры защиты информации – это разного рода механические, электрические или электронные устройства, а также сооружения, специально предназначенные для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к модулям, подсистемам автоматизированной системы и компонентам защищаемой информации, включая технические средства визуального наблюдения, связи и охранной сигнализации.

фективны, поскольку разрабатываемые и применяемые средства защиты информационных систем перманентно отстают от средств и методов нападения. Ситуация усугубляется ещё и тем, что описания современных методов и технические характеристики средств нападения на компьютерные системы, а также программные коды вредоносных компьютерных программ, предназначенных для их реализации, регулярно публикуются как в традиционных изданиях, так и в их электронных аналогах. Особенно негативным явлением, по нашему мнению, следует признать бесконтрольное распространение подобной информации в Глобальной сети, так как оно неимоверно расширяет круг потенциальных потребителей, одновременно снижая требования к уровню специальных знаний и, соответственно, подталкивая психологически неустойчивых индивидуумов к совершению компьютерных преступлений.

5. Для успешной борьбы с компьютерной преступностью, которая в настоящее время располагает такими современными средствами обработки и передачи информации как Интернет, персонал специальных подразделений правоохранительных органов, компаний и корпораций необходимо оснастить не менее «продвинутыми» аппаратно-программными средствами, чем имеются в наличии у компьютерных преступников и он должен обладать не меньшими профессиональными знаниями по сравнению с ними. Например, надо уметь вовлекать потенциальных преступников в чаты, завязывать с ними необходимые для раскрытия преступлений отношения и учиться распознавать их возможные планы в отношении электронных нападений на компьютеры и сети пользователей;

6. Применение «точечных», узконаправленных мероприятий для нейтрализации или, по крайней мере, минимизации негативных последствий от совершённых компьютерных преступлений чрезвычайно затруднено на практике благодаря высокой степени их латентности[79]. Именно высокая степень латентности компьютерных преступлений является отличительной чертой данного вида преступлений. Отсюда сложность сбора доказательств от-

[79] Корчагин А. Г. Экономическая преступность. Владивосток, 1998.

носительно, например, транснациональных преступлений с использованием информационно-телекоммуникационных систем, значительность материального ущерба, а также специфичность личности самих компьютерных преступников, которыми, зачастую, становятся высококвалифицированные программисты, руководители и технический персонал солидных организаций и государственных учреждений. Высокая же латентность компьютерных преступлений во многом обусловлена тем, что большинство коммерческих структур разрешает проблему своими силами, поскольку убытки от проведения расследования официальными органами власти могут оказаться намного выше суммы причинённого ущерба (изъятие документации и компьютерной техники на неопределённое время приведёт к остановке деятельности, что недопустимая роскошь для любой компании). Кроме того, как уже отмечалось ранее, руководство каждой фирмы опасается подрыва её репутации и, в итоге, ухода клиентов к конкурентам, раскрытия в ходе судебного разбирательства системы безопасности организации, выявления собственной незаконной деятельности и пр.

7. Неудовлетворительное состояние дел в плане правильного использования даже имеющихся в распоряжении персонала средств обнаружения попыток атак на информационные системы. Например, проведённый в США одним из правительственных учреждений эксперимент по проникновению в свою собственную компьютерную сеть показал, что удалось выявить лишь менее 5% от общего числа успешных атак, то есть на практике регистрировалась лишь каждая двадцатая успешно реализованная атака на сеть, а остальные проникновения в сеть так и остались незамеченными;

8. В борьбе с компьютерными преступлениями негативным фактором, снижающим результативность проводимых мероприятий, является запоздалая реакция администрации информационных систем и технического персонала даже на вполне очевидные попытки компьютерных преступников совершить противоправные действия. К таким деяниям можно отнести, например, попытки хищения носителей информации с записанными на них про-

граммами и данными, а также необоснованного перевода денег с одного счёта на другой (особенно при использовании поддельных кредитных карточек); разрушение программ и «заражение» их компьютерными вирусами; потерю значительных массивов данных; попытки проникновения в компьютер в обход показания программных «локаторов» о несанкционированном доступе;

9. Большинство наиболее опасных компьютерных преступлений осуществляется с использованием различных ухищрений с целью «заметания следов», и компьютерные преступники действуют на большом удалении из любой точки мира. При этом компьютерному преступнику совсем не обязательно физически присутствовать и в стране, откуда последовала реальная атака на компьютерную систему, кроме того, чаще всего в ход идут фальшивые или чужие имена, а также клички.

В указанных условиях основной целью государственной политики по выявлению и пресечению компьютерных преступлений является устранение перечисленных негативных факторов и причин и, соответственно, последующее создание эффективной национальной системы борьбы с правонарушениями в сфере компьютерной информации, к базовым элементам которой специалисты обычно относят:

- формирование целостной системы непрерывного отслеживания обстановки в сфере обеспечения информационной безопасности различных систем в стране и упреждающего принятия решений по выявлению и пресечению компьютерных преступлений;

- организацию взаимодействия и координацию усилий правоохранительных органов, спецслужб, судебной системы, обеспечение их необходимой материально-технической базой;

- организацию эффективного взаимодействия правоохранительной системы России с правоохранительными органами зарубежных стран, осуществляющими борьбу с компьютерными преступлениями;

- координацию действий с общественными и частными организационными структурами – фондами, ассоциациями, фирмами, службами безопас-

ности банковских и коммерческих структур, на своём уровне осуществляющими практические мероприятия по обеспечению информационной безопасности.

И несколько слов в заключение этого раздела книги.

На протяжении многих лет преступления в рассматриваемой нами области являлись прекрасной возможностью для компьютерных преступников совершать свои криминальные деяния практически безнаказанно в подавляющем большинстве случаев, так как доказательство этих преступлений чрезвычайно трудоёмко и специфично. Чаще всего мировой общественности становились известны только наиболее громкие дела, связанные с компьютерными преступлениями, а у нас в стране, до последнего времени, даже законодательной базы для привлечения к уголовной ответственности за написание и распространение вредоносных компьютерных программ, хищение компьютерной информации, электронный взлом компьютеров и тому подобную деятельность фактически не существовало.

Как показывает хронология компьютерной преступности, правоохранительные органы во всём мире изначально пытались вести борьбу с компьютерными преступлениями с помощью традиционных правовых норм, касающихся преступлений против собственности – кража, присвоение чужой собственности, мошенничество и т. п. Однако сама практика расследования реальных уголовных дел показала, что такой подход, чаще всего, абсолютно не приемлем, поскольку многие компьютерные преступления не подпадают под состав традиционных преступлений и общеуголовную юрисдикцию. Например, у правонарушений, связанных с компьютерной преступностью, может полностью отсутствовать материальная составляющая, так как средство нападения или предмет преступного посягательства виртуален по своей сущности, и попросту отсутствует в качестве физической материи. Зачастую отсутствует и факт уничтожения имущества как такового, что тоже не подходит под определение традиционного уголовного преступления.

В силу указанных причин компьютерные преступления обладают как бы свойством двойственности, и поэтому жизнь потребовала введения в Уголовный кодекс Российской Федерации специальных статей и, в результате в последней его редакции появилась отдельная глава, включающая в себя три статьи.

Законодательный аспект борьбы с компьютерной преступностью будет подробно рассмотрен в соответствующем разделе настоящей книги, а здесь без пространных комментариев приведём текст упомянутых статей Главы 28 («Преступления в сфере компьютерной информации») Уголовного кодекса Российской Федерации.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осуждённого за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершённое группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осуждённого за период от пяти до восьми месяцев, либо исправительными работами на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – наказываются лишением свободы на срок до трёх лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осуждённого за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказываются лишением свободы на срок от трёх до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определённые должности или заниматься определённой деятельностью на срок до пяти лет, либо обязательными работами на срок от ста восьмидесяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырёх лет.

Пусть нас это не касается, но давайте запомним эти скупые строки, и дальше по жизни будем держаться подальше от всего, что связано с «преступлением и наказанием» в целом, а также деяниями, подходящими под определение «компьютерное преступление», в частности.

Глава 2

Вредоносные компьютерные программы и их авторы

§1. Основы вирусологии

Прогресс человечества породил множество масштабных проблем и надо сказать, что проблема антивирусной безопасности занимает в ней достойное место. Вполне очевидно, что вредоносные компьютерные программы – компьютерные вирусы[80], «троянские» программы[81], «черви»[82], равно как и их разновидности и модификации, которые обычно объединяются, если нет особой необходимости в жёстком разграничении, одним понятием «компьютерный вирус» или просто «вирус», – требуют мониторинга и исследования основных направлений, тенденций их развития, а также ведения перманентной, желательно упреждающей борьбы с ними и их негативными проявлениями.

Но отчего же все-таки проблема компьютерных вирусов, в основном, в плане борьбы с ними, приобрела в последнее время такое значение? Насколько и чем оправданы усилия всего компьютерного сообщества от пользователей до профессионалов, затрачиваемые на изучение и борьбу с

[80] Компьютерный вирус – вредоносная компьютерная программа, способная «размножаться», «заражать» иные компьютерные программы и файлы, модифицируя их так, чтобы они включали в себя копию этой программы или её разновидности.

[81] «Троянская» программа («троянский» конь) – вредоносная компьютерная программа, выполняющая в дополнение к основным функциям, неописанные в документации, несанкционированные действия. Данные действия могут использовать полномочия законного субъекта компьютерной системы или сети для осуществления несанкционированного доступа к информации.

Несанкционированное действие – действие субъекта в нарушение установленных в системе правил обработки, хранения и передачи информации.

Несанкционированный доступ к информации – доступ субъекта к данным, сведениям в нарушение установленных в системе правил разграничения доступа, которые представляют собой совокупность требований, регламентирующих порядок и условия доступа к защищаемой информации, а также к её носителям.

Полномочия – право субъекта (объекта) системы осуществлять доступ к защищаемым данным.

[82] Червь – вредоносная компьютерная программа, которая отличается повышенной степенью автономности, размещается практически в любом месте автоматизированной системы, нацелена не на конкретные программы или файлы, а на архитектуру инфицируемых систем и может использоваться как для санкционированных, так и для несанкционированных действий, см. выше.

компьютерной заразой? Причин такого положения дел достаточно много, но начнём с начала.

Первые исследования саморазмножающихся искусственных объектов проводились в середине нынешнего столетия. В работах фон Неймана, Винера и других авторов дано определение и проведён математический анализ конечных автоматов, в том числе и самовоспроизводящихся. По мнению некоторых специалистов, теоретическое обоснование возможности появления компьютерных вирусов следует искать именно в работах Джона фон Неймана, который ещё в 1949 году интересовался проблемами роста интеллектуальной мощности и развития вычислительной техники. В том числе и возможностью саморазмножения компьютеров или отдельных команд. Скажем, из-за какой-то невероятной ошибки, сбоя программы компьютер в процессе работы формирует некую команду, способную уничтожать другие программы, оставаясь при этом невредимой, а потом, из-за другой системной ошибки, команда приобретает способность к саморазмножению. Хотя вероятность возникновения такой цепочки событий отлична от нуля, особенно с усложнением компьютеров, но на современном уровне развития вычислительной техники практически невозможна. Для Неймана теоретическое построение «вирусы – продукт работы самого компьютера» было всего лишь игрой ума, а у реального компьютерного вируса есть вполне человеческие родители – вирусописатели, которые представляют собой людей определённого, с позволения сказать, склада ума. Но, одно совпадение налицо, первый компьютерный вирус действительно появился на свет в результате безобидных развлечений программистов-профессионалов.

Специалисты из McAfee AntiVirus Technology и учёные Национального института медицинских исследований (NIMR) из Великобритании попытались выяснить, насколько компьютерные вирусы похожи на своих биологических родственников, и как это можно использовать для борьбы с ними. В отчёте за 2002 год об исследовании «Виртуальная вирусология» (Virtual Virology) проведены некоторые параллели в их строении и действиях. И ком-

пьютерные и биологические вирусы имеют схожее устройство: они состоят из большого числа простых блоков, объединённых в последовательности, то есть в строки программы или в цепочки ДНК. Широкому распространению компьютерных вирусов способствуют глобальные информационные сети, а широкому распространению болезней – мобильные носители инфекции, и чем быстрее и доступнее средство передвижения, тем скорее вирус добирается до новых жертв, при этом и те, и другие эпидемии распространяются обычно с востока на запад. Примерно совпадают экономический ущерб от простоя компьютерного оборудования и потери от бездействия болеющих сотрудников. И не случайно выше названный отчёт был передан для изучения, как медикам, так и программистам.

Таким образом, если заменить организм компьютером, а клетки – программами, то можно провести аналогию между биологией и информатикой, а компьютерный вирус не привнёс ничего радикально нового. Попадая вместе с заражённой программой в организм-компьютер, вирус перехватывает контроль над его управлением и, используя его же материальные ресурсы (память и энергию), начинает размножаться, уничтожая «хозяина» и угрожая другим «клеткам». Эта аналогия, проводимая специалистами в области «компьютерной вирусологии», настолько прочно вошла в информатику, что в настоящее время компьютерная терминология органично включила в себя такие медицинские термины, как «инфицирование», «инкубационный период», «вакцина», «вакцинация» и т. п. Это обстоятельство иногда приводило и к нелепым ситуациям – когда у нас в стране началось массовое внедрение вычислительной техники, ходили «достоверные» слухи о распространении вирусной инфекции посредством закупаемой за рубежом вычислительной техники. Причём, говорилось об этом в прямом смысле слова и вполне серьёзно.

Приведём описание некоторых широко используемых терминов:

● *профилактика* – раздельное хранение вновь полученных и уже эксплуатируемых программ, разбиение жёстких дисков на отдельные логиче-

ские диски, зоны с установленным режимом «только для чтения», хранение неиспользуемых программ и файлов в заархивированном виде, использование специальной «карантинной» области для записи новых программ с носителей информации, регулярная проверка загрузочного сектора используемых дискет и т. п.;

● *анализ* – ревизия любых полученных «из внешнего мира» программ специальными средствами и их запуск в контролируемой среде, систематическое использование контрольных сумм при хранении и передаче программ. Каждая новая программа, полученная без контрольных сумм, должна тщательно проверяться компетентными специалистами, по крайней мере, на наличие известных на тот момент компьютерных вирусов и, в течение определённого времени, за её «поведением» должно быть организовано соответствующее наблюдение;

● *фильтрация* – использование специальных резидентных компьютерных программ, утилит для своевременного обнаружения и последующего пресечения попыток выполнения несанкционированных действий;

● *вакцинирование* – специальная электронная обработка жёстких дисков, логических дисков, директориев (каталогов), файлов, запуск специальных резидентных программ-вакцин, имитирующих сочетание условий, которые используются данным типом компьютерного вируса в целях инфицирования программы или всего жёсткого диска;

● *терапия* – деактивация конкретного компьютерного вируса в заражённых программах с помощью специальной антивирусной программы или восстановление первоначального состояния компьютерных программ при помощи уничтожения всех экземпляров вируса в каждом из инфицированных файлов или жёстких дисков с помощью специальной программы-фага.

Итак, своим названием компьютерные вирусы обязаны вполне определённому сходству с вирусами «от медицины»: своей способностью к саморазмножению и инфицированию ещё незаражённых систем, скоростью распространения и избирательностью поражаемых систем или определённых

групп однородных систем, сложностями в ведении борьбы с эпидемиями, нарастающим темпом в плане появления всё более вредоносных модификаций, версий старых и целых поколений новых вирусов и т. д.

Медики сегодня имеют хорошо отлаженную систему предупреждения международного уровня, которая помогает в случае опасности своевременно оповещать население и объединять усилия для борьбы с распространением инфекции – во всех странах используется стандартный порядок описания нового вируса и его действий.

Вместе с тем компании-разработчики антивирусных аппаратно-программных средств и соответствующие специалисты (исследователи, аналитики в данной области профессиональной деятельности) не имеют в наличии такой международной системы, но их преимущество заключается в оперативности поступления и обработки информации для последующего её анализа, изучения и разработки новых технологий, методов борьбы и соответствующего современного инструментария.

За последние годы компьютерные вирусы приобрели широкую известность: специалисты изучают эту проблему, разработчики создают всё более сложные средства защиты, системные администраторы и программисты выявляют вирусы и борются с ними при помощи имеющихся в их распоряжении аппаратных и программных средств, а владельцы информационных систем и пользователи терпят то больший, то меньший ущерб от атак вирусов[83] и масштабных эпидемий ими вызываемых.

---

[83] Атака вируса – действие любой из разновидностей вредоносных компьютерных программ (компьютерных вирусов, троянских программ, червей и т. п.), которое приводит к реализации угрозы путём использования уязвимостей автоматизированной системы.

Атака на компьютерную систему – это действие, предпринимаемое нарушителем (злоумышленником), которое заключается в поиске и использовании той или иной уязвимости. Таким образом, атака – это реализация какой-либо угрозы.

Нарушитель – лицо (субъект), которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещённых ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или с целью самоутверждения и т. п.) и использовавшее для этого различные возможности, методы и средства (чисто агентурные методы получения сведений, технические средства перехвата без модификации компонентов системы, штатные средства и недостатки систем защиты, подключение к каналам передачи данных, внедрение программных закладок, использование специальных инструментальных и технологических программ и т. п.).

Злоумышленник – нарушитель, преднамеренно действующий из корыстных побуждений.

В отдельных случаях борьбу с компьютерными вирусами пытаются перевести на национальный и международный уровни и вести её в масштабах всей страны или группы стран. Например, в мае 2000 года министерство государственной безопасности Китая ввело регулирование, направленное на предотвращение распространения компьютерных вирусов. Регулирование заключается в обязательном антивирусном контроле всей информации, публикуемой в Интернет. Компьютеры, используемые для распространения массовой информации, в соответствии с новыми правилами, должны обязательно иметь установленные антивирусные средства. Одновременно с этим была выпущена директива, регламентирующая цены на антивирусное программное обеспечение и содержащая рекомендации по использованию конкретных антивирусных продуктов.

В июле 2000 года Министерство науки и техники Испании совместно с компанией-разработчиком антивирусного программного обеспечения Panda Software, и в сотрудничестве с Ассоциацией пользователей Интернет, инициировало национальную кампанию против вредоносных компьютерных программ. Официально провозглашённая цель этой акции – «Максимальная очистка Испании от компьютерных вирусов». Любой пользователь Интернет с 17 по 31 июля мог бесплатно загрузить с правительственного сайта программу Panda-антивирус для анализа и «лечения» своего компьютера. На Web-сайте также была размещена информация об основных способах распространения компьютерных вирусов, и пользователям давалось 15 простых советов о том, как защитить от компьютерных вирусов свой компьютер. Более того, ровно через год, в июле 2001 года, правительство Испании создало Центр информации по компьютерным вирусам, который должен бесплатно информировать население о появлении новых вирусов. Государственный секретарь Испании по телекоммуникациям Баудилио Томе заявил, что этот Центр будет работать без выходных, информировать население о новых компьютерных вирусах, а также давать советы о том, каким образом от них можно избавиться. На сайте Центра можно подписаться на бесплатную рассылку

с последней информацией о вирусах. «Вирусы несут угрозу информационному обществу не только потому, что они наносят вред компьютерам, но ещё и потому, что они сеют неуверенность среди граждан, – сделал заявление г-н Томе, и добавил, – Ведь только на прошлой неделе восемь тысяч испанских предприятий было успешно атаковано вирусом «SirCam».

В сентябре 2001 года министрами информационных технологий Сингапура и Бельгии Йео Чоу Тонгом и Риком Демсом был подписан договор, в рамках которого эти государства обязались сотрудничать в сфере предупреждения атак вирусов на национальные компьютерные системы. Согласно подписанному договору государственные органы обеих стран, ответственные за распространение предупреждений о вирусах, обязались оповещать друг друга о появлении новых вредоносных программ, а также о потенциальной опасности их появления. Данный шаг призван снизить экономический урон, наносимый вирусами, особенно их самостоятельно распространяющимися по сетям разновидностями, то есть «червями». Во время видеоконференции, на которой проходило подписание соглашения, сингапурский министр назвал вирусы «опасными паразитами, от которых трудно избавиться» и добавил следующее: «Предоставив людям всего мира уникальные возможности общения, Интернет, в то же время, существенно повысил опасность распространения компьютерных вирусов и лучшее, что мы можем сделать для предотвращения этой опасности – оставаться бдительными и внимательными».

В феврале 2002 года Министерство информации и коммуникаций Южной Кореи приняло решение о создании в первой половине этого же года системы раннего предупреждения для обнаружения попыток атак компьютерных вирусов, которая должна способствовать снижению ущерба от их эпидемий. Причём было подчёркнуто, что к сотрудничеству привлекаются не только Интернет-провайдеры, но и ведущие разработчики антивирусных аппаратно-программных средств.

И ещё один интересный пример проекта, выходящего за национальные рамки борьбы с компьютерными вирусами. В феврале 2001 года компания-разработчик антивирусного программного обеспечения McAfee анонсировала свою новую разработку, так называемую «вирусную карту», которая затем была интегрирована в принадлежащий ей Web-сайт. Карта отображает информацию обо всех случаях вирусных инфекций в мире: регионы, в которых произошли заражения, типы вирусов, которые их вызвали, количество инфицированных компьютеров и т. п. По утверждениям представителей компании эта карта обновляется в режиме реального времени и позволяет отслеживать тенденции распространения компьютерных вирусов в мире, предсказывать вспышки вирусных инфекций, а также предупреждать компьютерных пользователей о грядущих эпидемиях компьютерных вирусов. Данные для карты собираются отовсюду, где установлены онлайновые службы антивирусного сканирования McAfee, а это, по утверждению компании – тысячи и тысячи компьютеров во всём мире. Всякое появление вируса в «диком»[84] виде автоматически отмечается на карте. Специалисты McAfee подчеркнули, что они просмотрели 39 миллиардов файлов в компьютерах 780 тысяч подписчиков своих онлайновых служб антивирусного сканирования во всём мире, и среди них было найдено 18 миллионов инфицированных файлов. Двадцать процентов от просмотренных компьютеров были инфицированы каким-либо вирусом. На тот момент возглавлял этот список вирусов Интернет-червь «I Love You» (другие названия «LoveLetter», «LoveBug»): 1423777 случаев заражения за январь 2001 года; за ним следовала троянская программа «ASPtrojan.qa», ворующая пароли входа в Интернет у пользователей известного провайдера America Online, на её счету 292794 заражений; вирус-червь «MTX», инфицирующий системы под управлением Win32, обосновался на третьем месте – за

[84] В настоящее время введён в употребление и получил широкое распространение термин «дикий» компьютерный вирус, который служит для идентификации вредоносных компьютерных программ, которые реально могут инфицировать современные компьютеры и сети. И, в первую очередь, именно на эти программы следует обращать внимание, как профессионалам, так и пользователям с целью принятия необходимых и своевременных мер предупреждения против реальных атак компьютерных вирусов.

Подробно о возникновении и употреблении понятия «дикий» компьютерный вирус, зачем оно введено, что означает, мы поговорим во втором томе настоящей книги, так как это тема отдельного и достаточно серьёзного разговора.

тот же период он поразил 134227 компьютеров. Карта также позволяет отслеживать тенденции вирусных заражений внутри конкретного региона. Например, в соответствии с этой картой на тот момент в США самыми «инфицированными» штатами были Калифорния и Вашингтон, а в Европе наибольшее число инфицированных компьютеров находилось в Великобритании и Германии.

Не подвергая сомнению неординарность, и пользу подобных проектов в плане повышения информированности компьютерного сообщества, отметим, что данная «карта» носит оттенок субъективности, так как McAfee собирает данные о заражениях тем или иным вирусом только с тех компьютеров, на которых установлено антивирусное программное обеспечение этой компании. Подобная карта существует, к примеру, и на сайте компании-разработчика антивирусного программного обеспечения Trend Micro и, если сравнить первые места, которые занимают наиболее активные вирусы в «горячих десятках» этих компаний, можно заметить отличия. Таким образом, более объективный характер «вирусная карта» может приобрести в том случае, если в ней будут задействованы данные всех компаний-разработчиков антивирусных аппаратно-программных средств во всём мире (хотя довольно трудно представить себе подобное альтруистическое сотрудничество между фирмами-конкурентами). В противном случае подобные карты можно называть не «карта мира компьютерных вирусов», а, например, «карта компьютерных вирусов, атакующих пользователей Trend Micro» или «карта компьютерных вирусов, атакующих пользователей McAfee» и т. п.

Чтобы вы нас правильно поняли и не обвинили в тенденциозности, ещё раз подчеркнём – повышение информированности компьютерного сообщества очень важный фактор, и мы этого ни в коем случае не отрицаем. В знак подтверждения приведём следующее утверждение тогдашнего министра иностранных дел Соединённого Королевства Великобритании и Северной Ирландии Робина Кука. В своей речи от 4 апреля 2001 года он заявил буквально следующее: «Компьютерное хулиганство наносит сегодня больший

урон, чем могли бы нанести военные действия. С увеличением роли электроники в контроле над водоснабжением, электроэнергией и транспортом инфраструктура Соединённого Королевства становится всё более незащищённой перед лицом атаки компьютеров. Такая атака может навредить экономике страны больше, чем обычная война. В мае прошлого года вирусом «Love-Bug» было повреждено множество компьютеров во всём мире, причём британский парламентский комитет по вопросам безопасности подвергся критике за очень медленную реакцию в ответ на случившееся. И реакция на критику последовала – предупреждение о вирусе «Анна Курникова», появившееся в феврале этого года, было разослано в течение часа. Ведь в современном мире разницей между стабильностью и хаосом может быть просто своевременное предупреждение».

§2. Глазами аналитика: общепринятая классификация вредоносных компьютерных программ

Вообще-то говоря, компьютерные вирусы заявили о себе достаточно давно. Во всяком случае, первое официальное сообщение о них как о новом виде компьютерных программ, основывавшееся на высказываниях из среды профессиональных программистов, относят к 1978 году, хотя эту дату трактуют по разному, и её нельзя считать окончательной с точки зрения зарождения феномена вирусов в качестве проблемы. Собственно же термин «компьютерный вирус» по отношению к определённому виду компьютерных программ первым в 1984 году употребил сотрудник Лехайского университета (США) Фред Кохен в своём докладе о проведённых им исследованиях, который был представлен компьютерному сообществу на проходившей в США 7-ой международной конференции по вопросам безопасности информации.

Иногда проблему широкого распространения компьютерных вирусов связывают с… появлением операционной системы UNIX.

Операционная система UNIX, разработанная программистами Д. Ричи и К. Томпсоном в Bell Laboratories (США) – филиале American Telephon & Telegraph (AT&T) и появившаяся в 1969 году, изначально замышлялась толь-

ко как средство для удовлетворения внутренних нужд. Она была достаточно проста в использовании, дружественна по отношению к пользователям и мало зависела от типа машин, на которых работала. UNIX разрабатывалась как многопользовательская система и потому имела систему разделения доступа, базирующуюся на парольной защите. В итоге успех системы превзошёл все самые смелые ожидания, и она завоевала весь компьютерный мир. Появилось множество усовершенствованных версий этой операционной системы: 1975 год – UNIX V6, 1976 год – UNIX V7 (первая «базовая» версия), 1982 год – UNIX System III, 1984–1985 годы – UNIX System V и т. д. Появились и клоны UNIX: GENIX, XENIX, Ultrics, VENIX, PC-IX. Университет Беркли (штат Калифорния, США) разработал UNIX 4.0, 4.1, 4.2 и т. д.

Большие системы тех лет имели не так много проблем с вирусами в силу своей уникальности, которая обеспечивалась тем, что каждая система проходила стадию генерации, во время которой многочисленные системные параметры образовывали уникальное сочетание, и имела развитые подсистемы разделения доступа и защиты, что является серьёзным препятствием для компьютерных вирусов и позволяет обнаруживать источник заражения. Но, стремление к глобализации коммуникаций привело к появлению современных многомашинных систем – распределённых компьютерных сетей. Во всём мире программисты и пользователи стали работать примерно с одним и тем же программным обеспечением, например, операционной системой UNIX (а также её клонами) и компиляторами языков программирования C, Pascal и т. п. Таким образом, тенденция к объединению уникальных систем в сочетании с появлением на рынке и широким распространением операционной системы UNIX и однотипных компиляторов языков программирования высокого уровня, усложнили ситуацию с обеспечением антивирусной безопасности в мире и создали необходимую среду для появления различных компьютерных вирусов и их модификаций.

Вместе с тем, очевидно, что во весь рост проблема компьютерных вирусов встала только с момента массового внедрения персональных компью-

теров (в России примерно в 1988–1990 г.). Ведь легко заметить, что малые системы, как правило, лишены уникальности и сильно унифицированы, но именно их стандартность и является, с одной стороны, неоспоримым преимуществом, которое предопределило их широчайшее распространение во всём мире, а с другой стороны, существенным недостатком. Компьютерный вирус, появившийся в какой-либо системе, без особых проблем поражает аналогичную систему, затем следующую и так до бесконечности (конечно, в условиях отсутствия противодействия этому процессу), так как по архитектуре эти системы идентичны. В этом ракурсе становится понятным значение для усугубления проблемы распространения компьютерных вирусов и их многочисленных модификаций развёртывание в 1981 году фирмой IBM серийного производства персональных компьютеров. Экономическая эффективность серийного производства персональных компьютеров является следствием стандартности их аппаратной архитектуры и архитектуры математического обеспечения, что и послужило толчком для развития массового вирусописательства.

Как обычно, всю опасность сложившегося положения сознавала незначительная часть специалистов, которые тщётно предупреждали, что пренебрежение вопросами обеспечения хотя бы собственной безопасности даром не пройдет. С тех пор прошло достаточно времени, и острота проблемы вирусов многократно возросла, однако заслуживающего внимания и серьёзного отношения к себе компьютерные вирусы «добились» относительно недавно.

Даже единого формального определения того, чем же является компьютерный вирус, так и не дано, несмотря на то, что попытки сформулировать такое определение предпринимались многократно. Основная трудность, возникающая при попытках дать строгое определение вируса, заключается в том, что практически все отличительные черты вируса или свойственны и другим программам, которые ни в коем случае не являются компьютерными вирусами, или напротив, существуют вирусы, которые за исключением возможности распространения не содержат вовсе или большей части общих от-

личительных черт этих вредоносных программ. Например, если в качестве главной отличительной черты вируса принять его латентность, то можно привести примеры вирусов, особенно и не скрывающих процесс своего распространения. Такие вирусы перед заражением какого-либо файла выводят на средства отображения ЭВМ специальное сообщение, которое говорит о том, что в компьютере находится вирус и этот вирус «собирается» заразить очередной файл, а потом выводят имя этого файла и спрашивают разрешение у пользователя на его инфицирование. Если в качестве отличительной черты вируса приводится возможность уничтожения им программ и данных на носителях информации компьютера, то в качестве обратного примера к данной отличительной характеристике можно указать на абсолютно безвредные вирусы, которые кроме своего распространения больше ничем особым не отличаются. Основная же особенность компьютерных вирусов – возможность их самопроизвольного внедрения в различные объекты операционной системы – присуща многим программам, которые заведомо не являются компьютерными вирусами. Таким образом, первая причина, которая не позволяет сформулировать точное определение вируса это невозможность однозначного выделения отличительных признаков, которые соответствовали бы вирусам, и только им. Второй причиной является тот факт, что определение компьютерного вируса, по идее, должно быть привязано к конкретной операционной системе или операционным системам, в которых он действует и распространяется. Теоретически же могут существовать операционные системы, в которых наличие вируса невозможно ни при каких условиях. Например, операционные системы, где запрещено создавать и изменять области выполняемого кода, то есть, запрещено изменять объекты, которые либо уже выполняются, либо могут выполняться системой при каких-либо условиях.

Однако, бесспорно, что, заражая тем или иным способом компьютерную систему, вирус в большинстве случаев, проникает в различные модули этой системы. Параллельно этому процессу компьютерный вирус вносит в инфицируемую систему изменения, тяжесть последствий которых может

оцениваться от неприятных, но не приводящих к её краху, до полного разрушения, в случае осуществления вирусом деструктивных действий. В связи с изложенным, целесообразно согласиться со сформулированным специалистами-разработчиками антивирусных средств обязательным условием того, что некоторая последовательность исполняемого кода является компьютерным вирусом: «обязательным (необходимым) свойством компьютерного вируса является возможность создавать свои дубликаты (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению»[85].

Таким образом, единого и точного определения компьютерного вируса до сих пор не удалось выработать, и вряд ли оно будет сформулировано в скором времени. Поэтому, естественно, нет и однозначно принятых стандартов, по которым «полезные» программы можно отделить от вредоносных программ и, в конечном счёте, некоторые программы и файлы довольно сложно вывести за рамки подозрения в их идентичности с той или иной разновидностью компьютерных вирусов. В результате специалисты вынуждены классифицировать компьютерные вирусы по самым различным признакам, что вносит достаточно большую неразбериху. По опасности производимых действий, способу проникновения в системы, местам размещения в системе, степени «самостоятельности» (автономности) и т. д.

Давайте вкратце рассмотрим общепринятую классификацию компьютерных вирусов, так как это необходимо для понимания дальнейшего материала настоящей книги.

Подобно живым внутриклеточным паразитам, компьютерные вирусы способны размножаться только в действующих компьютерных системах и, чем интенсивнее жизнь конкретного компьютера (обмен файлами, установка программного обеспечения, взаимодействие в сети и пр.), тем выше риск его

[85] Вслед за авторами данной формулировки отметим, что это условие не является необходимым и достаточным, так как операционная система MS-DOS, например, соответствует данному свойству, но вирусом не является.

инфицирования. Итак, компьютерные вирусы в целом обычно делят на классы в соответствии с основными признаками, которые приведены на рис.1.

2.1. Среда обитания

По признаку среды обитания компьютерные вирусы можно разделить на файловые, загрузочные, макро и сетевые, которые, в свою очередь, делятся на соответствующие подгруппы (Рис. 1а).

Файловые вирусы – либо различными способами внедряются в выполняемые файлы (распространённый тип вирусов), либо создают файлы-двойники (см. ниже компаньон вирусы), либо используют особенности организации файловой системы (link-вирусы). Таким образом, к данной группе относятся компьютерные вирусы, которые при своём размножении тем или иным способом используют файловую систему какой-либо операционной системы или каких-либо операционных систем. Внедрение файлового вируса возможно практически во все исполняемые файлы всех действующих операционных систем. На сегодняшний день известны вирусы, поражающие все типы выполняемых объектов стандартной MS-DOS: командные файлы («.bat»), загружаемые драйверы («.sys», в том числе специальные файлы («io.sys», «msdos.sys») и исполняемые двоичные файлы («.exe», «.com»). Существуют вирусы, поражающие исполняемые файлы других операционных систем: Windows 3.x/9.x/ME/2000/NT/XP, OS/2, Macintosh, UNIX, включая VxD-драйверы Windows. Существуют вирусы, заражающие файлы, которые содержат исходные тексты программ, библиотечные или объектные модули. Возможна запись вируса и в файлы данных, но это случается либо в результате ошибки вируса, либо при проявлении его агрессивных свойств. Макровирусы также записывают свой код в файлы данных – документы или электронные таблицы, однако эти вирусы настолько специфичны, что обычно выделяются в отдельную группу.

Большинство файловых стелс-вирусов (см. ниже стелс-вирусы) либо перехватывают DOS-вызовы обращения к файлам (INT 21h) либо временно «лечат» файл при его открытии и заражают при закрытии. Также как и для

загрузочных вирусов, существуют файловые вирусы, использующие для своих стелс-функций прерывания более низкого уровня: вызовы драйверов DOS, INT 25h и даже INT 13h. Полноценные файловые стелс-вирусы, использующие первый способ сокрытия своего кода, в большинстве своем достаточно громоздки, поскольку им приходиться перехватывать большое количество DOS-функций работы с файлами: открытие/закрытие, чтение/запись, поиск, запуск, переименование и т. д. Некоторые файловые вирусы используют часть функций полноценного стелс-вируса. Чаще всего они перехватывают функции DOS FindFirst и FindNext (INT 21h, AH=11h, 12h, 4Eh, 4Fh) и «сжимают» заражённые файлы. Такой вирус невозможно определить по изменению размеров файлов, если, он резидентно находится в памяти.

Загрузочные вирусы – записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик жёсткого диска – MBR (Master Boot Record), либо меняют указатель на активный boot-сектор. Загрузочные вирусы ориентированы на конкретные форматы расположения системных данных в загрузочных секторах дисков. Существующая во многих версиях BIOS функция Anti Virus Protection запрещает запись в boot-сектор жёсткого диска, однако со временем загрузочные вирусы научились обходить такую защиту. Загрузочные стелс-вирусы для сокрытия своего кода используют два основных способа.

Первый из них заключается в том, что вирус перехватывает команды чтения заражённого сектора (INT 13h) и подставляет вместо него незаражённый оригинал. Этот способ делает вирус невидимым для любой DOS-программы, включая антивирусы, неспособные «лечить» оперативную память компьютера. Возможен перехват команд чтения секторов на уровне более низком, чем INT 13h.

Рис. 1. Классификация компьютерных вирусов по основным признакам

Рис. 1.а. Классификация компьютерных вирусов по признаку среды обитания

Второй способ направлен против антивирусов, поддерживающих команды прямого чтения секторов через порты контроллера диска. Такие вирусы при запуске любой программы (включая антивирус) восстанавливают заражённые сектора, а после окончания её работы заново инфицируют диск. Поскольку для этого вирусу приходится перехватывать пуск и окончание работы компьютерных программ, он должен перехватывать также DOS-

прерывание INT 21h. С некоторыми оговорками загрузочными вирусами можно назвать вирусы, которые вносят изменения в заражаемый сектор (например, при заражении MBR правят только активный адрес загрузочного сектора – изменению подлежат лишь 3 байта), либо маскируются под код стандартного загрузчика.

Макро-вирусы – заражают файлы-документы, электронные таблицы и некоторые другие типы прикладных программ. Наибольшее распространение получили макро-вирусы для MS Word и MS Excel, а доля макро-вирусов для других продуктов (например, MS Access, MS Visio, MS PowerPoint, AmiPro) крайне незначительна. Макро-вирусы одновременно являются и резидентными, так как остаются в оперативной памяти всё время пока работает, например, инфицированный ими текстовый процессор. Таким образом, макро-вирусы, это компьютерные программы, написанные на макро языках программирования встроенных в некоторые системы обработки данных (текстовые процессоры, электронные таблицы и т. д.). Для своего размножения такие вирусы используют возможности указанных языков и при их помощи переносят себя из одного заражённого файла в другие. Для существования макро-вирусов в конкретной компьютерной программе необходимо наличие встроенного в неё макро языка с возможностями: привязки программы на макро языке к конкретному файлу; копирования макропрограмм из одного файла в другой; получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы).

Сетевые вирусы – активно используют для своего распространения протоколы и возможности локальных и глобальных сетей, команды компьютерных сетей и электронную почту, то есть сетевые вирусы распространяются по локальной или любой другой сети. Многие сетевые вирусы не портят данные и не заражают программы, но размножаются с катастрофической скоростью, парализуя остальные сетевые транзакции. Основным принципом работы сетевого вируса является возможность самостоятельной передачи своего кода на удалённый сервер или рабочую станцию. «Настоящие» сете-

вые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удалённом компьютере или спровоцировать пользователя к запуску инфицированного файла. Существует неверное мнение, что сетевым является любой вирус, распространяющийся в компьютерной сети, но, в таком случае, фактически все вирусы были бы сетевыми, в частности, наиболее примитивные из них – даже обычные нерезидентные вирусы при заражении файлов не делают различия между сетевыми (удалёнными) и локальными жёсткими дисками. В итоге специалисты такие вирусы к сетевым вирусам не относят, хотя они и могут инфицировать файлы в пределах какой-либо сети. Известность сетевые вирусы обрели в конце 1980-х годов, во многом благодаря знаменитому сетевому вирусу Морриса о котором мы подробно поговорим ниже в этой книге. Здесь же скажем, что эпидемия, связанная с вирусом Морриса, охватила несколько глобальных сетей в США, и для своего распространения он использовал ошибки и недокументированные функции глобальных сетей, передавая свои копии с сервера на сервер и запуская их на выполнение. Таким образом, ранние версии сетевых вирусов распространялись в компьютерной сети и, как правило, так же как и компаньон вирусы (см. ниже), не изменяли файлы или сектора на дисках. Они проникали в память компьютера из сети, вычисляли сетевые адреса других компьютеров и рассылали по этим адресам свои копии. Эти вирусы иногда создавали рабочие файлы на дисках системы, но могли вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

После нескольких эпидемий сетевых вирусов ошибки в сетевых протоколах и программном обеспечении были исправлены. В результате примерно десять лет случаи заражения «настоящим» сетевым вирусом не отмечались, собственно говоря, как и сами вирусы этого типа. Вновь проблема сетевых вирусов проявила себя только в 1997 году, когда появились вирусы «Macro.Word.ShareFun» и «Win.Homer». «Macro.Word.ShareFun» использовал возможности электронной почты MS Mail, создавая новое письмо, содержащее заражённый файл-документ («ShareFun» в этой точке своей деятельности

выступает как бы в роли макро-вируса) и, затем, отбирая из списка адресов электронной почты три случайных адреса и рассылая по ним инфицированное письмо. В результате, если пользователь устанавливал параметры электронной почты таким образом, что при получении письма автоматически запускался MS Word, вирус немедленно заражал компьютер адресата инфицированного письма. То есть «Macro.Word.ShareFun» представляет собой тип современного сетевого вируса, который объединяет в себе возможности встроенного в MS Word или MS Excel языка программирования Basic, а также протоколы и особенности электронной почты и функции автозапуска, необходимые для его распространения. Вирус «Win.Homer» использовал для своего распространения протокол FTP (File Trabsfer Protocol) и посылал копию на удалённый FTP-сервер в каталог Incoming, представляя собой пример возможностей вирусов по использованию современных сетевых протоколов и поражению глобальных сетей. Так как сетевой протокол FTP исключает возможность запуска файла на удалённом сервере, этот и подобные ему компьютерные вирусы характеризуется специалистами как *«полусетевые»*.

Заканчивая описание компьютерных вирусов по признаку сферы их обитания подчеркнём, что эти сферы могут пересекаться, вирусы в состоянии скрещиваться, мутировать и умело маскироваться. И вы это видели из приведённых примеров. Следовательно, кроме «чисто» файловых, загрузочных, макро и сетевых вирусов существует большое количество *вирусов со смешанной средой обитания*, например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков; сетевые макро-вирусы, которые не только поражают редактируемые документы, но и рассылают свои копии по электронной почте; загрузочно-сетевые вирусы, которые инфицируют и сети, и загрузочные сектора диска.

Вирусы со смешанной средой обитания, как правило, имеют сложный алгоритм работы, часто применяют оригинальные методы проникновения в компьютерную систему, используют «стелс» и «полиморфик» технологии и, поэтому, их не всегда просто нейтрализовать.

2.2. Заражаемые операционные системы

По признаку заражаемых операционных систем, то есть операционных систем, объекты которых подвержены инфицированию, деление вирусов на классы является как бы вторым уровнем. Очевидно, что вирусы, заражающие системные объекты, должны ориентироваться на форматы данных конкретной операционной системы, вследствие чего каждый файловый или сетевой вирус заражает файлы одной или нескольких операционных систем. Каждый файловый или сетевой вирус заражает файлы в какой-либо одной или нескольких операционных системах: MS DOS, Windows 3x/9x/ME/2000/NT/XP, Netware, OS/2, Macintosh, UNIX, Linux и т. п.; а также их многочисленных версиях, клонах или модификациях. Обнаружение резидентного Windows-вируса, например, является сложной задачей. Вирус, находясь в среде Windows как приложение или VxD-двайвер, практически невидим, поскольку одновременно активны несколько десятков приложений и VxD, и вирус по внешним признакам от них ничем не отличается. Следовательно, чтобы идентифицировать программу-вирус в списках активных приложений и VxD, необходимо досконально разбираться в самой операционной системе и, плюс к тому, иметь полное представление о драйверах и приложениях, установленных на данном компьютере. Итак, для того чтобы оставить исполняемый код вируса, например, в памяти Windows, существует три способа, причём все три способа уже применялись различными вирусами. Самый простой способ – регистрация программы как одного из приложений, работающих в настоящий момент. Для этого программа регистрирует свою задачу, окно которой может быть и скрытым, затем регистрирует свой обработчик системных событий и т. д. Второй способ – выделить блок системной памяти при помощи DPMI-вызовов и скопировать в него свой код; третий способ – остаться резидентно как VxD-драйвер (например, Wnidows 3.xx, Windows95) или как драйвер Windows NT. Перехват обращений к файлам производится одним из двух способов: перехватываются вызовы INT 21h (Hook_V86_Int_Chain, Get/Set_V86_Int_Vector, Get/Set_PM_Int_Vector) или

системный вызов API. Затем резидентные Windows-вирусы перехватывают обращения к файлам и заражают их.

2.3. Особенности алгоритма работы

По признаку особенностей алгоритма работы вирусы делятся на нерезидентные, резидентные, компаньоны, черви, паразитические, невидимые, полиморфные, студенческие и нестандартные (Рис. 1б).

Рис. 1.б. Классификация компьютерных вирусов по признаку особенностей алгоритма работы

Нерезидентные вирусы – не заражают память компьютера и сохраняют активность ограниченное время, лишь некоторые из этой группы компьютерных вирусов оставляют в оперативной памяти компьютера небольшие резидентные программы, которые, тем не менее, не занимаются дальнейшим распространением вируса.

Резидентные вирусы (TSR, Terminate and Stay Resident) – при проникновении в компьютер копируют в оперативную память резидентную часть своего тела, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и сохраняют активность до тех пор, пока есть питание, то есть вплоть до выключения компьютера или перезагрузки операционной системы. Резидентными можно считать и макро-вирусы, поскольку они постоянно присутствуют на всё время работы в памяти инфицированного компьютера. При

этом роль операционной системы берёт на себя конкретная программа (например, текстовый процессор), а понятие «перезагрузка операционной системы» трактуется как выход из этой программы. В многозадачных операционных системах время «жизни» резидентного вируса может быть ограничено моментом закрытия заражённого модуля.

Компаньон вирусы (companion viruses) – это вирусы, не вносящие изменения в файлы. Алгоритм этих вирусов действует так, что они создают свою копию для exe-файлов, то есть файлы-спутники, у которых тоже имя, но с расширением «.com»), например, для файла «point.exe» они создают файл «point.com». Этот вирус пристраивается к com-файлу не изменяя exe-файл. При запуске файла, операционная система первым выполняет com-файл, в котором вирус, а затем com-файл запускает exe-файл.

Вирусы-черви (worms) – вредоносные компьютерные программы, которые отличаются повышенной степенью автономности, размещаются практически в любом месте системы, обычно нацелены не на конкретные программы или файлы, а на архитектуру инфицируемых систем и могут использоваться как для санкционированных, так и для несанкционированных действий. Вирусы-черви, так же как и компаньон вирусы, обычно не изменяют файлы или сектора дисков. Они проникают в память компьютера из компьютерной сети, вычисляют и захватывают разными способами сетевые адреса других компьютеров и рассылают по этим адресам свои многочисленные копии. Такие вирусы далеко не всегда создают рабочие файлы на жёстких дисках системы и могут не обращаться к ресурсам компьютера за исключением его оперативной памяти. Существуют вирусы-черви, использующие своеобразные приёмы внедрения в систему и дальнейшего распространения, например, упаковывающие свои копии в архивы (ZIP, ARJ и т. п.). Файловые черви[86] являются, в определённом смысле, разновидностью компаньон вирусов (см. выше), но при этом никак не связывают своё существование с каким-

[86] Не следует путать файловые вирусы-черви с сетевыми червями, так как файловые вирусы-черви используют только файловые функции какой-либо операционной системы, а сетевые черви при своём размножении используют сетевые протоколы и т. п.

либо выполняемым файлом. При размножении они всего лишь копируют свой код в каталоги жёстких дисков и «ожидают», когда копии их кода будут запущены ничего не подозревающим пользователем. Файловые черви могут присваивать своим копиям определённые имена, которые эксплуатируют психологию человека в целях провоцирования пользователя на запуск этих копий, например, «setup.exe». Некоторые вирусы записывают команду запуска инфицированного файла в bat-файлы.

«Паразитические» вирусы (parasitic viruses) – все вирусы, которые при распространении своих копий обязательно изменяют содержимое дисковых секторов или файлов. Их действие вредит вдвойне. Фактически к этой группе относятся все вирусы, которые не являются «червями» или «компаньонами».

Невидимые или стелс-вирусы (stealth viruses) – представляют собой весьма совершенные программы и стремятся стать незаметными. Они перехватывают обращения операционной системы к заражённым файлам или секторам дисков и «подставляют» вместо себя незаражённые участки. Кроме того, такие вирусы при обращении к файлам используют альтернативные алгоритмы, позволяющие «обманывать» резидентные антивирусные мониторы. Использование стелс-алгоритмов позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространённым стелс-алгоритмом является перехват запросов операционной системы на «чтение-запись» заражённых объектов. Стелс-вирусы при этом либо временно «лечат» их, либо «подставляют» вместо себя незаражённые участки. В случае макро-вирусов наиболее популярный способ это запрет вызовов меню просмотра макросов. Одним из первых файловых стелс-вирусов признан вирус «Frodo», а первым загрузочным стелс-вирусом – «Brain».

Полиморфик-вирусы (polymorphic viruses) или *вирусы-призраки* – вирусы, которые довольно трудно обнаружить. Они не имеют сигнатур, то есть не содержат ни одного постоянного участка кода и осуществляют шифрование тела вируса и модификацию программы расшифровщика. В большинстве случаев два образца одного и того же полиморфик-вируса не имеют ни одно-

го совпадения. Шифрование основного тела вируса и модификация программы-расшифровщика делает это возможным. Процедуры самостоятельного шифрования и полиморфизм используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуры их детектирования, блокировки и уничтожения. Полиморфные вирусы зачастую пытаются уничтожить CMOS-память, Flash BIOS компьютера и, по возможности, удалить все файлы на всех имеющихся в системе дисках.

«Студенческие» вирусы – примитивные вирусы, почти всегда нерезидентные, содержащие большое количество ошибок и неспособные причинить какой-либо ощутимый вред. В настоящее время эта разновидность компьютерных вирусов встречается довольно редко.

Нестандартные вирусы – это вирусы, использующие различные нестандартные приёмы. Зачастую используются в компьютерных вирусах для того, чтобы как можно глубже спрятать себя в ядре операционной системы, защитить от обнаружения свою резидентную копию или затруднить лечение от вируса (например, поместив свою копию во Flash BIOS) и т. п.

2.4. Деструктивные возможности

По признаку деструктивных возможностей вирусы делятся на четыре группы, показанные на рис. 1в.

Безвредные вирусы – никак не влияют на работу компьютера, кроме уменьшения объёма свободной памяти на жёстком диске в результате своего размножения. Такие вирусы лишь распространяют свои копии в ресурсах компьютера, но не причиняют никакого вреда ни рабочим файлам, ни загрузочным.

Но даже если в алгоритме вируса не найдено ветвей, наносящих ущерб системе, этот вирус нельзя с полной уверенностью назвать безвредным, так как проникновение его в систему может вызвать непредсказуемые и даже катастрофические последствия. Ведь, как и другие компьютерные программы, вирусы содержат разнообразные ошибки, в результате которых могут быть испорчены как файлы, так и сектора дисков.

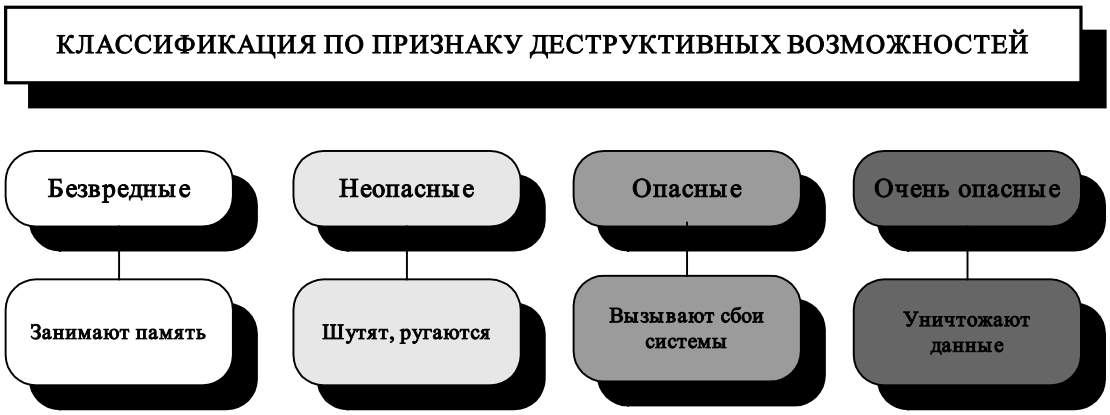

Рис. 1.в. Классификация компьютерных вирусов по признаку деструктивных возможностей

Неопасные вирусы – влияние этих вирусов ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами: на экране, сопровождаемые звуковыми эффектами, появляются физиономии, которые показывают язык, выпучивают глаза и т. д. Эти зрительные и звуковые эффекты не приводят к потере данных. К категории таких вирусов можно отнести, например, вирус «Joke_JS.Spawn.b». После запуска Java-скрипта, который содержится внутри HTML-документа, у пользователя начинает произвольно передвигаться по экрану окно MS Internet Explorer. Кроме этого, происходит самопроизвольное открытие в фоновом режиме ещё нескольких окон Internet Explorer.

Между прочим вроде бы неопасные шуточки в Интернет могут приносить вполне осязаемый ущерб. Так в феврале 2001 года американская компания Go Online Networks Corp., занимающаяся онлайновым маркетингом и рекламой, стала жертвой слухов, распространившихся в Интернет. На одном из финансовых Интернет-форумов некий «Microcap_Matty» объявил о том, что Go Online занимается, в частности, модификацией генома человека. После этого курс акций компании упал на 20%. Go Online обратилась к организаторам форума с просьбой снять с него указанное сообщение, которое в самом лучшем случае можно охарактеризовать как глупую шутку. Однако «Microcap_Matty» вновь проявил себя, опубликовав на этом же форуме заяв-

ление о том, что «все это принесёт ему дополнительную рекламу, и он попадет даже в программу 60 минут (популярная в США телепередача)».

В связи с участившимися случаями насилия среди детей и подростков в США, школьные власти стали очень серьёзно относиться к любым проявлениям агрессии со стороны детей, даже если дело так и ограничилось лишь шутками-угрозами, распространяемыми в Интернет. Ученик одной из школ в Нью-Йорке открыл сайт, на котором назвал своих учителей «извращенцами», а также заметил, что не против «заглянуть в школу с автоматом». Ученика лишили права пользования Интернет и исключили из школы на два дня. Некоторые учителя также настаивали, на его переводе в другую школу. Ученица другой школы, находящейся в штате Нью-Джерси, поместила список своих одноклассников на сайте People2kill («Люди, которых нужно убить»). Девушка не отделалась простым отлучением от Интернет, её исключили из школы и обязали пройти психологическое освидетельствование. Полиция даже обыскала дом ученицы, чтобы обнаружить оружие, с помощью которого она могла бы претворить свои виртуальные угрозы в жизнь.

Среди неопасных вирусов следует особо отметить «компьютерные мистификации» (computer hoaxes). К ним относятся компьютерные программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят заведомо ложные сообщения о новых ранее неизвестных компьютерных вирусах сообщения о том, что такой вред уже причинён, либо будет причинён при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. К ним относятся, например, программы, которые запугивают пользователя ложными сообщениями о форматировании диска, обнаруживают вирусы в незаражённых файлах или выводят вирусоподобные сообщения. В таких сообщениях пользователей «информируют» о том, что в Интернет появился новый вирус, распространяющийся в письмах и/или через WWW-сайты, и уничтожающий всю информацию на заражаемых им компьютерах и т. п.

Например, в мае 2000 года фирма IBM уведомила компьютерных пользователей о вирусной мистификации, которая состоит в распространяемом от лица компании IBM ложном предупреждении о вирусе, который, как говорится в этой мистификации, является ещё более разрушительным, чем «Melissa». В заявлении также говорилось, что «ложное сообщение, адресованное пользователям PC и Mac, впервые появилось в конце марта под заголовком «Let's watch TV» (давай смотреть ТВ) и не получило широкого распространения, но его появление отмечено вновь вскоре после вирусной эпидемии с «любовными письмами». Мистификация циркулировала достаточно широко, возможно как следствие обеспокоенности компьютерных пользователей в связи с вирусами, подобными вирусу «I Love You» и встречается также под именами: «Wobbler», «California» и «Kali». IBM предупреждала, что сообщение является обманом и настоятельно советовала получателям игнорировать его, а также удалить это письмо и не пересылать его другим.

В мае того же года финская антивирусная компания F-Secure предупредила компьютерных пользователей о распространяемой по e-Mail фальшивке под названием «Win the holiday» («Выиграй отдых»). Ложное сообщение e-Mail содержало предупреждение о несуществующем вирусе, который будто стирает информацию на диске, а также предложение разослать это сообщение другим. F-Secure посоветовала проигнорировать само послание, но ни в коем случае не пересылать его своим знакомым во избежание распространения ложной информации.

В начале сентября 2000 года в Интернет появился вирус «Joke.Win32.Errore», который представлял собой программу-шутку, имитирующую форматирование жёсткого диска. При запуске он выводил несколько сообщений о якобы случившейся в Windows ошибке: «Errore interno di Windows 345 all'indirizzo 4E6F:942A; Errore interno di Windows 591 all'indirizzo 93C0:6210; Errore interno di Windows 712 all'indirizzo 7ED5:89C2; Errore interno di Windows 128 all'indirizzo 6542:EF21; Errore interno di Windows 591 all'indirizzo 63F0:81B2; ERRORE FATALE 14». Затем выводил запрос на

форматирование логического диска C: Sei veramente sicuro di voler formattare l'hard disk? [Yes] [No] [Cancel]. И, вне зависимости от полученного ответа (Yes/No/Cancel) симулировал форматирование диска. Пользователю при этом не предоставлялось возможности прекратить выполнение этой операции, но на самом деле никакого форматирования не происходило, и все данные на жёстком диске оставались в целости и сохранности. По окончании «форматирования» программа выводила на экран «мусор», ещё несколько сообщений и завершала свою работу.

Аналогичная «Joke.Win32.Errore» программа-шутка «Joke_FakeFormat» также имитирует форматирование жёсткого диска – после запуска программы нажатие на любую кнопку вызывает запуск ложного форматирования. Пользователь, как и в первом случае, не может самостоятельно прекратить его выполнение, а после окончании «форматирования» программа закрывается кнопкой «Close». Стоит ли говорить, что и в этом случае, разрушается нервная система пользователя, а все данные на жёстком диске остаются в целости и сохранности.

Более подробно об этих и других компьютерных мистификациях вы можете прочитать в Приложении 1.

Опасные вирусы – вредоносные программы, деятельность которых может привести к серьёзным сбоям в работе системы. Эти вирусы портят, уничтожают файлы или осуществляют их подмену другими.

Очень опасные вирусы – вредоносные программы, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожению данных, стиранию необходимой для работы компьютера информации, записанной в системных областях памяти (BIOS, загрузочные сектора диска). Таким вирусом, без всякого сомнения, является знаменитый «CIN» (другое название: «Чернобыль»), который, например, разрушает, стирает FAT (File Allocation Table – Таблица размещения файлов).

В дополнение к рассмотренным выше основным признакам компьютерные вирусы можно также делить в соответствии с критериями, которые приведены на рис. 2 и 3.

2.5. Использование Интернет-технологий

По признаку использования Интернет-технологий специалисты обычно выделяют несколько разновидностей вирусов, показанных на рис. 2.

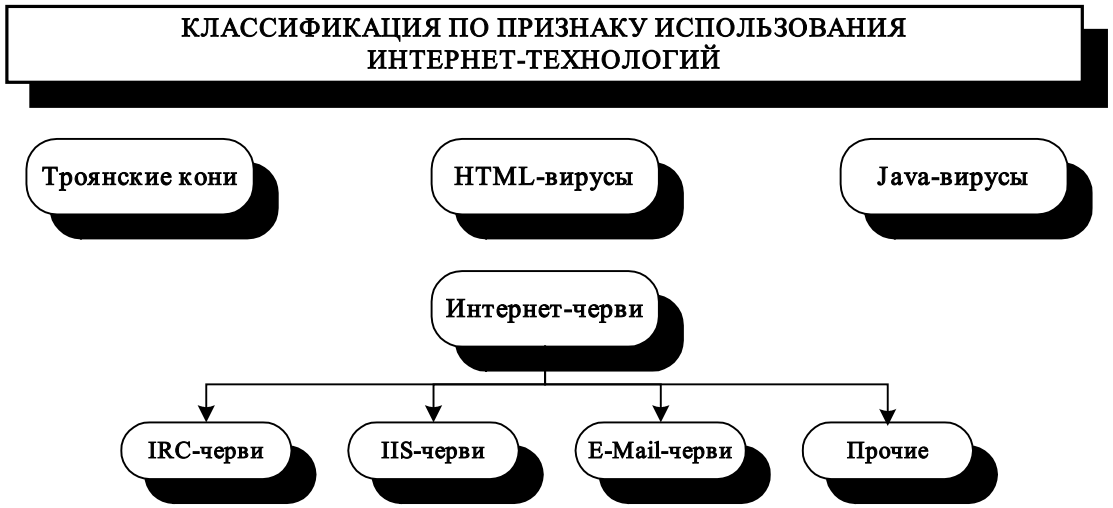

Рис. 2. Классификация компьютерных вирусов по признаку использования Интернет-технологий

Троянские программы (троянские кони, логические бомбы) – вычисляют или, можно сказать, «подсматривают» на компьютере имена и пароли пользователей, а затем используют их по своему усмотрению в широком диапазоне несанкционированных действий от снятия средств с кредитной карточки пользователя до осуществления иных криминальных акций под подставными именами. Троянские программы могут действовать в различных операционных системах MS DOS, MS Windows (например, «Trojan.Win32.Malantern», «Trojan.Win32.DiskAdmin», «Trojan.IRC-Hack») и пр. Классические троянские кони служат для осуществления скрытого управления удалённым компьютером, выполняются по стандартной технологии «клиент-сервер» и, соответственно, состоят из двух частей – клиентской и серверной. Серверная часть устанавливается на «компьютер-жертву» и управляется с удалённого компьютера при помощи клиентской части. Таков,

например, троянский конь «Backdoor.Nethief». Существуют и троянские кони, которые отличаются довольно «узкой специализацией», к примеру, воруют системные пароли PSW (Password-Stealing-Ware): «Trojan.PSW.CrazyBilets», «Trojan.PSW.Hooker», «Trojan.PSW.Gip». Присутствуют в наличии и так называемые «троянские макро-вирусы», сочетающие в себе свойства как тех, так и других типов вирусов, например: «Trojan.WordMacro.Format», Trojan.Macro.Excel.Taiwanes», «Macro.Word97.Trojan.Tvangeste», «Macro.Word97.Trojan.Tvangeste». Кроме того, к троянским программам относят вредоносные компьютерные программы, оказывающие какое-либо разрушительное воздействие на систему, то есть в зависимости от сочетания заданных условий или при каждом запуске уничтожающие информацию на жёстких дисках, «подвешивающие» операционную систему и т. п. Многие из известных троянских коней являются программами, которые маскируются под полезные компьютерные программы, новые версии широко известных утилит или их модификации. Очень часто они рассылаются по BBS-станциям или электронным конференциям и по сравнению с некоторыми другими типами компьютерных вирусов троянские кони обычно не получают более широкого распространения по достаточно банальным причинам: они уничтожают себя вместе с остальными данными на жёстком диске пользователя или непроизвольно демаскируют своё присутствие и уничтожаются пострадавшим пользователем.

Иногда, в качестве разновидностей троянских программ выделяют так называемую *«троянскую матрёшку»* и *«троянского червя»*.

«Троянская матрёшка» (Trojan nested doll) – эта разновидность троянских программ предполагает запуск процедуры самоуничтожения после выполнения своей задачи, которая заключается в том, что программные модули-фрагменты создают «троянского коня» и самоликвидируются на программном уровне по окончании этой деятельности. Отметим, что найти указанные команды-модули в программном коде крайне трудно и такая работа может быть выполнена только квалифицированным программистом.

«Троянский червь» (Trojan worm) – особенностью этой разновидности троянских программ является то обстоятельство, что в алгоритм работы компьютерной программы наряду с основными функциями закладывается алгоритм действий, осуществляющих саморазмножение, программное автоматическое воспроизводство «троянского коня». «Троянские черви» автоматически копируют себя независимо от других программ в памяти одного или нескольких компьютеров при наличии компьютерной сети.

Существуют также вредоносные программные коды, которые сами по себе не предназначены для выполнения функций троянских программ и создаются с вполне конкретной целью доставки последних на «компьютер-жертву», например: «TrojanDownloader.Win32.Ultimx», «Backdoor.Death», «TrojanDownloader.Win32.WebDown». Они содержат в себе информацию об именах и расположении вредоносных программ, которые, впоследствии, загружаются ими в компьютер и запускаются без уведомления пользователя. Указанная информация обычно находится в зашифрованном блоке в конце тела троянца. Она может проявлять себя ложным уведомлением о якобы случившейся ошибке в архиве или неверной версии операционной системы.

К троянским коням можно отнести так называемые «*дропперы вирусов»*, которые представляют собой заражённые файлы, код которых представлен таким образом, что известные версии антивирусного программного обеспечения не определяют наличие в файле компьютерного вируса. Например, файл упаковывается «экзотическим» или мало известным архиватором, или шифруется с использованием какого-либо специального математического алгоритма, что не позволяет антивирусному программному средству идентифицировать и ликвидировать инфекцию.

Таким образом, в результате использования «неполноценных троянцев» вирусописатели обычно достигают сразу две основные цели: скрытая инсталляция троянских или других вредоносных компьютерных программ и защита от антивирусного программного обеспечения.

HTML-вирусы – встречаются достаточно редко и вопреки своему названию не используют собственно язык разметки гипертекстовых страниц. HTML-вирусы используют программные вставки – скрипты, написанные на языке программирования Visual Basic. С помощью этих скриптов вирусы находят HTM-файлы на локальной машине и записываются в них. Однако при стандартных настройках браузера запрещено выполнение скриптов, в которых происходит обращение к файлам локального компьютера, и это обстоятельство резко ограничивает вредоносную деятельность данного вида компьютерных вирусов. Фактически заражение файлов HTML-вирусами возможно только при стечении обстоятельств («человеческий фактор») и, безусловно, неверных действиях или злом умысле администратора системы.

Java-вирусы – это вирусы, которые, как и следует из самого их названия, написаны на языке программирования Java. Как известно, у Java-программ существует два типа исполняемых модулей: приложения и апплеты. Java-апплеты не имеют доступа к файловой системе локального компьютера, а Java-приложения хотя и могут выполняться под управлением браузеров, но, для обеспечения безопасности на них накладываются весьма серьёзные ограничения. Java-вирусы могут быть оформлены как приложения, но для подавляющего большинства пользователей практической опасности не представляют. Фактически, так же как и в случае с HTML-вирусами, заражение файлов Java-вирусами возможно только при стечении обстоятельств («человеческий фактор»), а также неверных действиях или злом умысле администратора системы.

19 августа 2000 года компания Sun Microsystems и ряд её партнёров объявили о завершении разработки стандарта MID (Mobile Information Device) на базе языка программирования Java для использования в мобильных телефонах. Одновременно с этим один из крупнейших мировых разработчиков технологий беспроводной связи компания Motorola выпустила интерфейс прикладного программирования (API), позволяющий разрабатывать для этих устройств дополнительные программы. Таким образом было поло-

жено начало нового этапа в развитии функциональности мобильных телефонов, так как интеграция языка программирования Java предоставляет пользователям возможности запуска на телефонах программ третьих компаний и создания своих собственных программ, а также обмена ими. Однако новые функциональные возможности мобильных телефонов открывают путь для создания как полезных, так и вредоносных программ. Если до того компьютерные вирусы атаковали мобильные телефоны опосредованно, например, через посылку навязчивых SMS-сообщений, то могут появиться целые семейства вирусов, «живущих» непосредственно в мобильных телефонах. Насколько вероятна такая перспектива, спросите Вы? Технология Java на деле доказала свои надёжность и защищённость. За годы её существования на персональных компьютерах были обнаружены всего лишь несколько Java-вирусов. Их, в свою очередь, скорее можно назвать концептуальными, нежели представляющими реальную угрозу. Принцип работы Java-программ, основанный на выделении виртуального защищённого пространства, практически полностью исключает возможность появления «диких» вирусов для этой платформы. «Пока что у нас нет оснований полагать, что J2ME менее защищена, чем другие версии Java. Однако для того, чтобы сделать окончательный вывод, необходимо время для проведения многочисленных тестов, – сказал Евгений Касперский, руководитель антивирусной «Лаборатории Касперского», – Даже если J2ME окажется абсолютно защищённой платформой, остаётся самое уязвимое место в системе безопасности – человеческий фактор. Это, в свою очередь, может быть исправлено исключительно целенаправленным просвещением».

IRC-черви – эти вирусы занимают отдельную «нишу» в классификации. Internet Relay Chat – это специальный протокол, разработанный для взаимодействия пользователей Интернет в реальном времени, и для поддержки IRC-конференций созданы различные IRC-серверы, которых в мире насчитывается огромное множество. IRC-серверы объединены в так называемые сети и самой большой из них является сеть EFnet, серверы которой каждый день

одновременно посещают десятки тысяч пользователей. В целом IRC-разговор похож на обычную телефонную беседу за исключением того, что в IRC-разговоре могут участвовать более двух собеседников, объединяющихся по интересам в различные группы IRC-конференций. Для подключения к IRC-серверу и общения участников конференции разработаны специальные программы – IRC-клиенты. Подключившись к IRC-серверу при помощи программы-клиента, пользователь выбирает тему IRC-конференции, при помощи команды «join» входит в одну или несколько конференций (в IRC приняты термины – «канал», «каналы») и начинает общение с другими участниками конференций. Помимо посещения общих (public) конференций любой пользователь имеет возможность общаться с другим пользователем в режиме диалога (private), причём они могут находиться в различных каналах. Кроме того, существует достаточно много IRC-команд, позволяющих пользователю получать информацию о других пользователях и каналах, изменять некоторые установки IRC-клиента, передавать и принимать файлы. Именно на возможности передавать и принимать файлы основываются IRC-черви, создание двух первых представителей которых относят к 1997 году. Оба первых вируса получили свои названия («mIRC.Acoragil» и «mIRC.Simpsalapim») по используемым кодовым словам, так как сразу после ввода пользователем «Acoragil» или «Simpsalapim» они немедленно отключали их от канала. Среди других вредоносных программ, которые относят к IRC-червям, укажем на такие «экземпляры» как: «I-Worm.Goner», «I-Worm.Jer», «IRC-Worm.Lara», и «IRC-Worm.Lucky». Пока достаточно.

IIS-черви – это вирусы-черви пытающиеся распространяться через Web-серверы, поражая установленное на них управляющее программное обеспечение – Internet Information Servers (IIS). Классические IIS-черви реализуют метод распространения от Web-сервера к другим Web-серверам, передавая на них свой exe-файл и запуская его там. Эти черви поражают серверы при условии установленной на них системы IIS и при наличии стандартных файлов Web-сервера. При запуске на заражённом сервере вирус-червь

ищет на ней ссылки на другие Web-серверы, пересылает на них свою копию и при помощи программного трюка запускает её на выполнение на заражаемом сервере. В результате червь заражает все серверы, на которые есть ссылки с текущего сервера; вновь зараженные серверы передают копию червя дальше и т. д. Среди вредоносных программ, которые относят к IIS-червям вполне достаточно указать на два «великих и ужасных» Интернет-червя нового столетия «IIS-Worm.CodeRed» (другие названия: «CodeRed», «Baby») и «SQL.Slammer» (другие названия: «Worm.SQL.Helkern», «Sapphire»). Но о них будет подробный разговор в других главах этой книги.

E-Mail-черви (почтовые черви) – обычно это вирусы-черви, распространяющиеся по почте в виде электронного письма с прикреплённым файлом небольшого размера, упакованным одним из архиваторов и заголовком письма, который выбирается случайным образом. Черви этого типа используют брешь в системе безопасности почтового клиента, запуская прикреплённый файл без ведома пользователя. После запуска программы вирус считывает адреса получателей заражённых писем из адресной книги Windows, отсылает заражённые письма и на этом может заканчивать свою работу, а может и устанавливать троянскую программу, ворующую пароли с заражённой машины. В этом случае червь имеет двухкомпонентную структуру – состоит из двух независимых частей, которые выполняются независимо друг от друга. Этими компонентами являются: червь, рассылающий электронные письма, и троян, ворующий пароли. Если червь не инсталлирует себя в систему, то он может вновь запуститься только в случае повторного открытия заражённого письма.

Среди наиболее известных представителей «почтовых червей» можно назвать: «Worm.Aliz», «Worm.Badtrans» и «Worm.BadtransII», «Worm.Blebla», «Worm.Bridex», «Worm.Zoher».

Прочие Интернет-черви – вирусы, относящиеся к этому типу, могут как сочетать в себе характерные черты различных компьютерных вирусов,

так и применять достаточно оригинальные приёмы, чтобы в полной мере использовать современные Интернет-технологии.

2.6. Проникновение в систему и автономность

По признаку проникновения в систему вирусы обычно делятся на пять основных источников, показанных на рис. 3.

Рис. 3. Классификация компьютерных вирусов по признаку проникновения в систему

На этом можно бы и закончить анализ классификации современных компьютерных вирусов, однако мы предлагаем вам рассмотреть ещё один, на наш взгляд интересный признак, который иногда выделяется специалистами-вирусологами и связан как раз и с классификацией по признаку проникновения в систему.

Это так называемый критерий автономности компьютерного вируса, который позволяет разбить множество вирусов на две неравные по численности группы.

В этом случае правомочен следующий подход.

Как уже говорилось выше, большинство компьютерных вирусов паразитирует на «известных» им конкретных программах или файлах, присоединяя свой код к телу программы или заранее определённым файлам, обязательно присутствующим в поражаемой системе. Также большинство вирусов имеет собственные «излюбленные» места в инфицируемой системе, в которых они помещаются непосредственно после проникновения в неё. Выявление этих характерных черт, специфичных для каждого отдельно взятого се-

мейства вирусов, облегчает обнаружение вирусов и проведение мероприятий, необходимых для их блокирования и уничтожения. Как раз это «большинство» компьютерных вирусов обычно и называют собственно вирусами, когда необходимо выделить их из общей группы вредоносных компьютерных программ. Очевидно, что отсутствие в системе пользователя нужных вирусу программ гарантирует, что система не будет инфицирована вирусом, который предназначен для того, чтобы паразитировать на этих программах. Иная ситуация с компьютерными вирусами, нацеленными на системные программы и файлы, однако именно эта нацеленность облегчает борьбу с инфекцией.

Рассмотренная нами ранее группа вредоносных программ, так называемых «компьютерных червей» (и их разновидностей), которые в широком смысле, и в соответствии с приведённым выше определением с полной уверенностью можно отнести к компьютерным вирусам, отличается повышенной степенью автономности. Если «обычный» вирус активизируется при запуске пользователем программы, на которой он паразитирует или при отработке системой конкретных событий, например, прерываний, то компьютерный червь способен самостоятельно управлять запуском своих копий. Если обычный вирус размещается в более или менее определённых местах системы, то место размещения в системе червя предсказать крайне сложно, поскольку ему практически безразлично, где размещаться – лишь бы имелось в наличии необходимое место. Кроме того, как уже подчёркивалось, компьютерные черви нацелены не на конкретные программы или файлы, а на системы конкретной архитектуры и гораздо опаснее вирусов именно в силу своей автономности, то есть независимости от наличия в поражаемых системах некоторых специфичных условий, например, определённых файлов или программ. Вместе с тем повышенная автономность предполагает более высокую сложность компьютерного червя как программы и, как следствие, существенно больший размер, чем у обычных вирусов. Именно поэтому, в большинстве случаев, компьютерные черви состоят из нескольких модулей, сегментов кода, слишком больших, чтобы быть скрытыми в файлах операцион-

ной системы (например, такой как MS DOS или Windows, OS/2 или UNIX). Но этот недостаток, с точки зрения вирусописателя, окупается тем ущербом, который может причинить компьютерный червь, поскольку обнаружить его в системе, блокировать и, затем, уничтожить – гораздо сложнее по сравнению с обычными вирусами.

Дальше, больше … Построение, развитие и бурное распространение информационно-вычислительных сетей подвигло вирусописателей к созданию так называемых «сетевых червей»[87], которые являются подвидом вредоносных компьютерных программ под общим названием «компьютерные черви». Общепризнанным считается тот факт, что первые исследования и эксперименты с сетевыми червями были поставлены в Научно-исследовательском центре фирмы Xerox (г. Пало-Альто, США) с использованием сети Ethernet. Сам червь был представлен в виде программных сегментов, выполнявшихся на различных узлах сети под управлением ведущего сегмента. Уже в процессе проведения первых опытов достаточно ясно проявилась опасность сетевых червей, так как в процессе своей вредоносной деятельности этот подвид компьютерных червей показал свою способность к заполнению своими данными памяти атакуемых им компьютерных систем, что, в свою очередь, приводило к нештатным ситуациям и полной остановке как атакуемых компонентов, так и сети в целом. Из изложенного понятно, что, скорее всего, сетевые черви являются побочным и вряд ли ожидавшимся детищем исследований в области распределённой обработки информации.

Таким образом, с точки зрения критерия автономности, можно выделить три основных этапа развития компьютерных вирусов (Рис. 4).

Введение такого деления процесса развития вредоносных компьютерных программ на отдельные этапы будет для нас хорошим ориентиром для

[87] Сетевой червь – вредоносная компьютерная программа, представляющая собой более сложное образование по отношению к обычным компьютерным червям и распространяющаяся по сети, используя для этого средства сетевой коммуникации: «электронная почта» всевозможных видов, специальные сетевые утилиты, сетевые протоколы, сетевые программы и т. д. Сетевой червь использует атакуемые узлы в «своих» интересах для саморазмножения и дальнейшей передачи собственных копий на неинфицированные узлы сети, где они активизируются и могут использоваться как для санкционированных, так и для несанкционированных действий. В результате деятельности сетевого червя может наступить полная блокировка сети или сетей.

дальнейшего исследования возникновения новых вирусов, зарождения и протекания их эпидемий, а также совершенствования методов и средств борьбы с ними.

Например, разве мог кто-нибудь точно предсказать на первом этапе развития компьютерных вирусов появление такого вируса как «Palm.Phage», первой вредоносной программы, нацеленной на инфицирование приложений PalmPilot и записывающей свой код вместо кода приложений, в результате чего заражённые приложения оказываются неработоспособными. Приложения Pilot (.prc-файлы – «выполняемые файлы» в терминологии MS DOS и MS Windows) являются стандартными базами данных Pilot со специальным ресурсом «приложение». При запуске приложений Pilot ресурс-«приложение» активизируется системой и затем выполняет предписанные ему действия. Для работы приложения система предоставляет ему библиотеку функций, при помощи которой приложение использует системные ресурсы и ресурсы баз данных. «Palm.Phage» при старте получает доступ к своему файлу и считывает из него ресурсы CODE и DATA. Затем вирус ищет все прочие приложения и записывает в них свои вирусные ресурсы CODE и DATA, при этом соответствующие ресурсы заражаемого файла оказываются потерянными, то есть они затираются кодом и данными самого вируса. Сравните это описание с характеристиками вирусов «рождения», например, 1988–1990 г., то есть начала широкой компьютеризации России.

Рис. 4. Основные этапы развития вирусов в соответствии с критерием их автономности

И ещё несколько слов о классификации вредоносных компьютерных программ.

2.7. Программы конструкторы и генераторы вирусов

Существуют две группы компьютерных программ – конструкторы вирусов и полиморфик-генераторы, которые не являются компьютерными вирусами даже в самом широком смысле трактовки этого понятия. Вместе с тем, эти программы имеют вполне определённое предназначение, так как используются исключительно для написания новых или усовершенствования «старых» компьютерных вирусов. Именно по этой причине их появление от-

слеживается на постоянной основе, и они добавляются в базы данных всех наиболее уважаемых фирм-разработчиков антивирусных средств. Такой подход имеет своей целью также и своевременное информирование системных администраторов о наличии или появлении этих программ в сети конкретного учреждения, организации или предприятия.

Итак, конструктор вирусов это утилита, предназначенная для изготовления компьютерных вирусов. Известны конструкторы вирусов для MS DOS, MS Windows, макро-вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули, и/или непосредственно заражённые файлы.

Некоторые конструкторы снабжены стандартным оконным интерфейсом, где при помощи системы меню можно выбрать тип вируса, поражаемые объекты (com и/или exe), наличие или отсутствие самошифровки, противодействие отладчику, внутренние текстовые строки, выбрать эффекты, сопровождающие работу вируса и т.п. Прочие конструкторы не имеют интерфейса и считывают информацию о типе вируса из конфигурационного файла.

Общепризнанным фактом является то обстоятельство, что летом 1992 года была выпущена первая версия первого конструктора вирусного кода для совместимых с IBM PC компьютеров –VCL (Virus Creation Laboratory).

Затем появилась первая версия конструктора PS-MPC (Phalcon/Skism Mass-Produced Code Generator) и на его идеях в январе 1993 года был «выпестован» конструктор вирусов G2 (Phalcon/Skism's G2), который поддерживает файлы конфигурации стандарта PS-MPC, но при генерации кода вируса использует гораздо большее количество вариантов кодирования одних и тех же функций. Появились целые плеяды конструкторов, например, для создания макро-вирусов: WM97.NTVCK, Macro.Word97.Constructor.CPCK, Macro.Word97.Constructor.DW97Mvck, Macro.Word.Constructor.Cvck, WMTools.Demo, Macro.Virus.Development.Kit и т. д. В результате написание вирусов намного облегчилось, и ряды вирусописателей стали стремительно

пополняться. В целом на основе указанных конструкторов вирусов были «слеплены» тысячи и тысячи вредоносных программ.

Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения – например, открытия, закрытия и записи в файлы, чтения и записи секторов и т. д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика. Полиморфные генераторы распространяются их авторами в виде файла-архива, и основным файлом в архиве любого генератора является объектный модуль, содержащий сам генератор. Вирусописатель может подключить к своему вирусу любой известный полиморфик-генератор и вызывать его из кодов вируса.

§3. Глазами пользователя: говорим «компьютерный вирус» - подразумеваем «потери»

3.1. Масштабы ущерба

Итак, в настоящее время, несмотря на усилия конкурирующих между собой фирм-производителей антивирусного программного обеспечения, убытки, приносимые компьютерными вирусами всех «мастей», достигают астрономических величин в миллиарды долларов ежегодно. Причём цифры, приводимые в аналитических отчётах и сообщениях прессы, занижены, поскольку известно становится лишь о части инцидентов. Кроме того, компьютерный вирус, поразивший автоматизированную систему, влечёт за собой многочисленные затраты, включая затраты времени специалистов на его устранение, расходы на дорогостоящие аппаратно-технические средства и программное обеспечение. Возникают и другие проблемы – это восстановление файлов, простой системы, а также самые трудно определимые затраты – ущерб, нанесённый репутации пострадавшей фирмы. Эксперты по вопросам информационной безопасности и созданию антивирусных программ признают, что основное внимание они уделяют борьбе с вирусами и предотвращению их распространения, предпочитая не тратить время и ресурсы на точную

оценку влияния конкретной компьютерной инфекции, да и точный масштаб ущерба оценить практически невозможно – данные, приводимые различными компаниями, могут отличаться на многие миллионы долларов.

В настоящее время регистрируется до 600 успешных сетевых атак в день, тогда как немногим ранее эта цифра была вдвое меньше. В 2003 году аналитическая компания TruSecure прогнозировала рост ущерба от преступлений в компьютерной сфере на 25%, а в исследовании Gartner Group говорится, что суммы страховок от компьютерных преступлений поднимутся с нынешних 100 миллионов до 900 миллионов долларов к 2005 году. В итоге может пострадать конечный пользователь, ведь цена ведения бизнеса возрастёт. В связи с этим правительство США выступило с инициативой страхования от подобной угрозы, предложив страховщикам расширить перечень услуг и привести его в соответствие с американской Национальной стратегией безопасности в киберпространстве (National Strategy to Secure Cyberspace) [88].

Таким образом, компьютерные вирусы приносят убытки не только увеличивая затраты компаний на безопасность и восстановление потерянных данных. Теперь к статьям расходов добавились и повышенные ставки страхования. Многие страховые компании, находясь под впечатлением от масштабов электронных эпидемий последних двух-трёх лет, решили обособить потери от компьютерных вирусов от рисков общего характера. Новый параграф в договорах страхования описывает так называемые «сетевые риски», взносы по которым составляют от 5 до 30 тысяч долларов в год, что выльется, в общей сложности, примерно в миллион долларов всей суммы рисков.

Между тем, директор по исследовательской работе компании Symantec Security Response Стивен Триллинг отмечал в интервью NewsFactor, что хотя антивирусные компании не занимаются оценкой экономических последствий

[88] Ещё в мае 2000 года немецкая страховая компания Onsecure предложила достаточно неожиданный сервис – онлайновое страхование от последствий действия компьютерных вирусов. Идея состояла в том, что если ваш компьютер подвергся негативному воздействию компьютерного вируса или компьютерных вирусов, то компания возмещает его владельцу убытки, которые связаны с потерей информации. Правда общая сумма страховых выплат на то время не могла превышать 1000 немецких марок, но и страховой сбор составлял всего 1 марку в месяц.

крупных вспышек компьютерных инфекций, финансовые убытки, наносимые компьютерными вирусами, весьма ощутимы. «Разумеется, данные о таком ущербе у различных организаций, производящих их оценку, расходятся, – пояснил Триллинг, – Вполне очевидно, что потери есть и они весьма внушительны. Но трудно сказать составляла ли их сумма 10 или 100 миллиардов долларов за прошлый год». Триллинг отметил также, что с точки зрения представляемой им компании судить о вреде, наносимом компьютерными вирусами, можно по количеству заявок, поступающих от её клиентов, аналитиков и других категорий пользователей компьютерных сетей, поражённых вирусами: «Исходя из потока заявок, мы можем составить приблизительное представление о масштабах ущерба. В частности, о размерах ущерба, нанесённого такими вирусами как «SirCam» или «Nimda».

Аналитик научно-исследовательского бюро Forrester Лаура Кетцле, специалист по вопросам оценки атак вирусов и ликвидации их последствий, сообщила NewsFactor, что компании могут точно установить такие осязаемые затраты, понесённые в результате атак вирусов, как количество человеко-часов, затраченных на проведение восстановительных процедур[89], расходы на замену аппаратно-технических средств. «Однако очень трудно установить величину таких расходов, как, например, вынужденные простои, снижение производительности труда и урон, нанесённый деловой репутации. Кроме того, компании не в состоянии выделить достаточное количество специалистов по информационным технологиям для оценки подобных видов ущерба, поскольку они, как правило, в первую очередь заняты предотвращением непосредственно атак вирусов. У компаний просто нет ни времени, ни денег для сбора данных о точной величине причинённого им ущерба», – считает г-жа Кетцле.

Профессионально оценкой ущерба от действий компьютерных вирусов и их модификаций занимается находящаяся в г. Карлсбад (штат Калифорния,

[89] Восстановительные процедуры – действия, предпринимаемые для восстановления способности системы хранить, обрабатывать и передавать информацию, а также восстановление наборов данных, файлов, программ после аварии, сбоя или отказа.

США) независимая аналитическая фирма Computer Economics. В одном из интервью средствам массовой информации вице-президент по исследованиям этой фирмы Майкл Эрбшлоу подчеркнул, что оценочные данные, представляемые Computer Economics, обычно «превышают любые другие публикуемые данные», поскольку в расчётах учитывается целый ряд факторов. Он также отметил, что представляемая им фирма делает экономические оценки, исходя их трёх категорий затрат: стоимость чистки инфицированных компьютеров, расходы на ликвидацию вирусов и влияние потерь рабочего времени на производительность труда пользователей. Г-н Эрбшлоу также объяснил, что в зависимости от характера атаки вируса его фирма собирает сведения о степени заражения вирусами из 20–25 источников и проводит сопоставительный анализ ущерба по нескольким сотням компьютерных сред.

Итак, на заре вирусописания в 1988 году повальная на то время эпидемия сетевого вируса Морриса, заразившего более 6 тысяч компьютерных систем в США и практически парализовавшего их работу, принесла общие убытки, оценённые по разным источникам, примерно в 96–98 млн. долларов. Потеря доступа и вынужденный простой ЭВМ оценивались как косвенные потери, связанные с инцидентом, и обошлись в сумму около 65 млн. долларов. По данным Computer Security Institute, общий ущерб, который нанесли компьютерные вирусы за пятилетний период с 1997 по 2001 год оценивается в 54 млрд. долларов, причём по данным компании Riptech Inc. авторами 80% вирусов, атаковавших, например, американские организации, являются жители десяти стран: Великобритании, Германии, Италии, Канады, Китая, Франции, США, Тайваня, Южной Кореи и Японии. По недавним подсчётам Computer Economics стоимость ущерба, нанесённого компьютерными вирусами в 1999 году уже равнялась 12,1 млрд. долларов, в 2000 году – 17,1 млрд. долларов, а весь вред, нанесённый вирусами только за девять месяцев 2001 года, был оценён более чем в 11,8 млрд. долларов. Причём, как показало исследование, самым «дорогим» вирусом 1999 года была «Melissa», нанёсшая вред на 1,2 млрд. долларов, за ней по пятам следовал известный вирус «Ex-

plorer», который также вызвал убытки около миллиарда долларов. В 2000 году общий ущерб от вирусов в немалой степени был связан с вирусом «I Love You» – творение филиппинского студента обошлось миру в 8,75 млрд. долларов. В 2001 году ущерб от вируса «Code Red» достиг 2,62 млрд. долларов, причём 1,1 млрд. долларов стоили работы по восстановлению компьютеров и 1,52 млрд. долларов – производственные потери; ущерб от вируса «SirCam» – 1,15 млрд. долларов, а «Nimda» – 0,635 млрд. долларов. Исследование Computer Economics также затрагивало и проблему соотношения убытков к количеству заражённых компьютеров. Например, Интернет-червь «Goner», появившийся в Интернет 4 декабря 2001 года, известный также под именем W32/Gone.A, заразил примерно 860 тысяч компьютеров, что достаточно мало по сравнению с другими вирусами «лидерами», а экономический ущерб повлёк в размере 8,5 млн. долларов. Общая сумма ущерба в 2001 году, по оценке вице-президента Computer Economics Майкла Эрбшлоу, достигала примерно 15 млрд. долларов.

3.2. Действие и противодействие

Не всем компаниям появление новых опасных вирусов приносит убытки. Вирусы сегодня «кормят» целую индустрию производства антивирусного программного обеспечения. При этом рынок антивирусного программного обеспечения растёт не менее стремительно, чем другие софтверные рынки. Он оценивается уже не в одну-две сотни миллионов долларов, как это было на рубеже смены столетий в 1998–1999 годах, а в миллиарды и миллиарды долларов. В настоящее время мониторингом и борьбой с компьютерными вирусами по всему миру (в Европе, Америке, Азии, Австралии) профессионально занимаются тысячи высококвалифицированных специалистов из фирм-разработчиков антивирусных программно-аппаратных средств, а также сотни тысяч специалистов, в первую очередь, системных администраторов компаний, использующих в своей производственной деятельности современные информационные технологии. Скажем, в корпорации Symantec непосредственно разработкой антивирусных продуктов занимается более 500

специалистов, а маркетингом и сбытом еще около 1,5 тысяч человек. В Network Associates работает порядка 3 тысяч сотрудников. Компания Sophos в течение года открыла четыре своих представительства в Германии, Франции, США и Японии, исследовательскую лабораторию в Австралии, и объявила о начале строительства нового крупного центра в собственной стране. Среди производителей программ-антивирусов можно выделить пятнадцать крупнейших компаний (названия приводятся по алфавиту): Aladdin Knowledge Systems (Израиль), Command Software Systems (США), Computer Associates International (США), ESET Software (Чехия), F-Secure (Финляндия), GeCad Software (Румыния), Grisoft (Словения), Network Associates (США), Norman Data Defense Systems (Норвегия), Panda Software (Испания), Sophos (Великобритания), Symantec (США), Trend Micro (Япония), «Диалог-Наука» (Россия), «Лаборатория Касперского» (Россия).

В публикуемых обозрениях компьютерных вирусов, например ассоциацией International Customer Service Association, говорится, что значительная доля рынка антивирусного программного обеспечения на североамериканском континенте (от 80 до 90%) принадлежит двум компаниям: Network Associates и Symantec. Интересно, что, несмотря на ореол одной из самых демократичных стран мира, США предпринимают все меры, чтобы оградить свой внутренний рынок от иностранных разработчиков антивирусного программного обеспечения. При этом они не церемонятся не только с российскими и восточно-европейскими компаниями, но и со своими традиционными партнёрами из стран Западной Европы.

В Европе сложилась несколько иная ситуация. Несмотря на присутствие американских «монстров», всё большую популярность и распространение получают продукты ESET Software, F-Secure, GeCad Software, Grisoft, Norman Data Defense Systems, Panda Software, «ДиалогНауки», «Лаборатории Касперского». Это, конечно, не значит, что Network Associates и Symantec безропотно отдают столь привлекательный рынок, просто здесь их лидерство гораздо менее очевидно, чем в США.

Координаты и названия программных продуктов наиболее известных производителей антивирусных программных средств приведены в табл. 1.

Таблица 1

Координаты и программные продукты некоторых производителей антивирусных программ

Наименование производителя	Сопровождаемый продукт	Web сайт фирмы-производителя
Aladdin Knowledge Systems	eSafe Protect Desktop, Enterprise & Gateway, ViruSafe	http://www.aks.com/
Alwil Software	AVAST!, Avast32	http://www.asw.cz/alwil.htm/
Anyware Software	Anyware AntiVirus	http://www.helpvirus.com/
Computer Associates	InoculateIT, eTrust EZ Antivirus (Vet AntiVirus)	http://www.ca.com/
Cat Computer Services	Quick Heal	http://www.quickheal.com/
Central Command Software	AVX (AntiVirus expert)	http://www.centralcommand.com/
ChekWARE	ChekMate, ChekOF	http://www.chekware.com/
Command Software	Command AntiVirus	http://www.commandsoftware.com/
Cybersoft	V-Find	http://www.cyber.com/
DataPROT	F-Secure & FP-DOS	http://www.datafellows.com/
DialogueScience	DrWeb, AdInf	http://www.dials.ru/ http://www.drweb.ru/
EMD Enterprises	EMD Armor Plus	http://www.emdent.com/
ESET	NOD-iCE, NOD32	http://www.nod32.com/
F-Secure	F-Secure Anti-Virus	http://www.fsecure.com/
ForeFront	ForeFront Anti-Virus	http://www.ffg.com/products/pc/anti.html
Frisk Software	F-Prot	http://www.complex.is/
GeCAD	Romanian AntiVirus (RAV)	http://www.rav.ro/
Grisoft	AVG	http://www.grisoft.com/
HAURI	ViRobot, DataMedic, LiveCall	http://www.hauri.co.kr/
H+BEDV Datentechnik	AntiVir	http://www.antivir.de/
Hiwire Computer & Security	FrontLine	http://www.hiwire.com.sg/
Ikarus	Virus Utilities	http://www.ikarus.at/

Наименование производителя	Сопровождаемый продукт	Web сайт фирмы-производителя
Kaspersky Labs	AVP (Kaspersky AntiVirus)	http://www.avp.ru/
Leprechaun Software	Virus Buster	http://www.leprechaun.com.au/
MessageLabs	MessageLabs offer virus detection at the ISP level	http://www.messagelabs.com/
MicroWorld Software	Red Armour	http://www.microworldsystems.com/products.html
MKS	MKS Vir	http://www.mks.com.pl/
Netpro	PC ScanMaster, Server ScanMaster	http://www.netpro.com/
Network Associates	GroupShield, WebShield, VirusScan, NetShield, ePolicy Orchestrator, Anti-Virus Informant, Virex, Management Edition	http://www.nai.com/
NetZ Computing	Invircible, ResQdisk, ResQdata	http://www.invircible.com/
Norman Data Defense Systems	Norman Virus Control	http://www.norman.no/
OverByte Corporation	DisQuick Diskettes	http://www.disquick.com/
Panda Software	Panda AntiVirus	http://www.pandasoftware.com/
Parsons Technology	ViruCide Plus	http://www.parsonstech.com/utilities/
Per Systems	Per AntiVirus	http://www.persystems.com/antivir/
Portcullis Computer Security	Defuse Enterprise	http://www.portcullis-security.com/
Proland Software	Protector Plus	http://www.pspl.com/
Reflex Magnetics	DiskNet	http://www.reflex-magnetics.co.uk/
RG Software Systems	Vi-Spy, No More #*!$ viruses	http://www.rg-av.com/
Safetynet	VirusNet-Pro	http://www.safe.net/
SBABR	System Boot Areas Antivirus	http://www.sbabr.com/
SecureNet Technologies	V-Net, Macro-Blaster, Macro-Blaster 97	http://www.securenet.org/
SeQTech	multivac, virustab	http://www.compucilina.com/
Softwin	BitDefender	http://www.bitdefender.com/ http://www.softwin.ro/
Sophos	AntiVirus	http://www.sophos.com/

Наименование производителя	Сопровождаемый продукт	Web сайт фирмы-производителя
Stiller Research	Integrity Master	http://www.stiller.com/
Sybari Software	Groupware anti-virus solutions for Notes and Exchange	http://www.sybari.com/
Symantec Corporation	Norton Anti-Virus	http://www.symantec.com/avcenter/
Trend Micro Incorporated	PC-cillin, InterScan VirusWall, ScanMail	http://www.antivirus.com/
VDS Advanced Research Group	Virus Detection System (VDS), Perforin for WinWord	http://www.vdsarg.com/
VirusBuster Ltd.	VirusBuster	http://www.vbuster.hu/
Virus.com	Virus Striker	http://www.virus.com/
Virus Protection Systems Ltd.	VPS	http://www.vps.co.za/

По мнению специалистов, некоторые компании-производители антивирусного программного обеспечения придерживаются агрессивной маркетинговой политики, а их стратегия сводится к следующему: сначала посеять страх, используя своих инженеров для поиска слабых мест, а затем, играя на чувстве страха пользователей, продавать обновления к своему антивирусному программному обеспечению. С этим можно спорить[90], но отчасти, видимо, так оно и есть. Чтобы не быть голословными, приведём реальные факты.

В конце июня 2002 года в статье San Francisco Gate утверждалось, что американские антивирусные компании намеренно раздувают шумиху вокруг новых компьютерных вирусов, поднимая, таким образом, уровень продаж собственного антивирусного программного обеспечения. В качестве примера приводилось недавнее сообщение о появлении в сети первого вируса под названием «Perrun», заражающего jpeg-файлы. Как выяснилось позже, вирус

[90] В июне 2000 года Интернет-издание CNews.ru сообщало, что ведущие производители антивирусных продуктов собираются принять систему градации компьютерных вирусов. По их словам, делают они это для того, чтобы предотвратить разжигание истерии, которая началась после официального предупреждения ФБР по поводу вируса «Resume–Janet Simmons». «Такая обстановка выгодна продавцам антивирусного программного обеспечения, которые различными публикациями подстёгивают ажиотаж на этот вид продукции. Градированная же система определения вирусов удержит общество от истерии и не даст лишний раз превознести опасность от того или иного вируса, что наблюдается в последнее время», – сказал Kevin Street, технический менеджер компании Symantec.

«Perrun» в Интернет так и не объявился, так как он был отправлен автором в компанию McAfee, которая и распространила информацию о новой «смерти всему компьютерному миру». Вирус так и не стал причиной эпидемии, не разрушил крупнейшие онлайновые системы, не сделал ничего, кроме рекламирования самой компании. Дальнейшее широкое обсуждение данной проблемы на Web-сайте SlashDot привело к очевидному результату: «Антивирусные компании подобны продавцам зонтов во время дождя и единственное отличие состоит в том, что компании-производители антивирусного программного обеспечения для борьбы с вредоносными программами имеют возможность вызывать дождь самостоятельно, путём несложных маркетинговых акций». В McAfee же продолжали утверждать, что информация о вирусе «Perrun» была опубликована не потому, что он представлял какую-либо угрозу населению, а по причине новизны типа распространения. Независимые специалисты по компьютерной безопасности, впрочем, не увидели в описании ложного компьютерного вируса «Perrun» ничего нового, а аналитики отметили, что ни одна компания-производитель антивирусного программного обеспечения не может похвастаться кристальной чистотой своих намерений, и случай с jpeg-вирусом не первый и далеко не последний.

10 октября 2000 года во Франции были зарегистрированы первые случаи заражения очередной разновидностью Интернет-червя «KakWorm», и, как отмечалось в заявлении, распространённом Европейским центром по компьютерной безопасности «Secusys», реакцию подавляющего большинства крупнейших антивирусных компаний на появление этого и других новых вирусов при всём желании трудно назвать слишком быстрой. «Наш центр сообщил об обнаружении новой разновидности червя менее чем через час после его появления, и мы тут же разослали эту информацию в ведущие антивирусные компании», – комментирует Ролан Гарсиа, ведущий специалист «Secusys». По его словам, специалисты «Secusys» были крайне разочарованы скоростью реакции наиболее крупных производителей антивирусного программного обеспечения на это событие. Хотя очевидно, что именно быстрая

реакция на появление новых компьютерных вирусов является одним из главных условий предотвращения непоправимого ущерба, который они могут нанести – ведь залогом безопасности информации пользователей является установка соответствующей защиты до того, как вирус попытается проникнуть в систему и нарушит или заблокирует её нормальное функционирование.

Между тем, например, сразу за сообщениями о появлении Интернет-червя «I Love You» акции компаний-производителей антивирусного программного обеспечения поднялись в цене в диапазоне от 3 до 26%. То есть, в свете событий, связанных с распространением этого вируса, произошёл резкий рост акций специализирующихся в области компьютерной безопасности компаний. Так, акции Symantec на фондовой бирже NASDAQ выросли на 2 $^{9}/_{16}$ пункта до отметки 61 $^{1}/_{16}$ пункта (4,4%); акции McAfee выросли на 5 $^{3}/_{4}$ пункта до 28 (26%); акции Netegrity Inc. (производителя программного обеспечения для контроля Web-информации) выросли на 1 $^{1}/_{4}$ пункта до 46 $^{3}/_{8}$ (2,8%), а акции сервисной компании Unisys Corporation на фондовой бирже Нью-Йорка подорожали на $^{15}/_{16}$ пункта до 22 $^{7}/_{8}$ (4,3%). Был отмечен рост курса акций и других компаний-специалистов в области антивирусного и защитного программного обеспечения, среди которых Trend Micro Incorporated, Pilot Network Service Incorporated, Keynote Systems Inc., SonicWall Incorporated, Check Point Software Technologies Ltd., Network Associates Incorporated.

Таким образом, эпидемия Интернет-червя «I Love You», поразившего миллионы компьютеров по всему миру, оказала непосредственное влияние на курс акций высокотехнологичных компаний. В целом, после спада ажиотажа среди инвесторов, значение индекса NASDAQ осталось фактически неизменным, но в курсе акций отдельных компаний, работающих в области антивирусных технологий, наблюдались ощутимые изменения: был отмечен заметный (в среднем более 5%) рост акций компаний-производителей антивирусного программного обеспечения. По сообщению компании Symantec о результатах деятельности во втором квартале 2001 финансового года, увели-

чение розничных продаж программного обеспечения принесло рост доходов компании до 192,3 млн. долларов за квартал, что на 14% больше, чем доход, полученный за аналогичный квартал 2000 финансового года. Продажи антивирусных пакетов компании за этот период выросли на 34%.

По заявлению британской антивирусной компании Sophos, объявившей о результатах закончившегося 31 марта 2001 финансового года, её чистая прибыль составила 7,8 млн. фунтов стерлингов при обороте в 22,6 млн. фунтов стерлингов, что значительно превосходит показатели 2000 финансового года в 4,7 млн. и 14,7 млн. фунтов стерлингов, соответственно. Благоприятные финансовые показатели вдохновили компанию на создание 160 дополнительных рабочих мест и интенсивное продвижение рынка своих программных продуктов в Италию и на Сингапур.

И ещё один интересный на наш взгляд пример. Южная Корея считается одной из самых «интернетизированных» стран в мире по количеству мегабит потребляемых на душу населения: люди платят налоги, заказывают еду, покупают одежду и даже консультируются с врачом с помощью Интернет. В стране очень высокий процент широкополосных соединений, но только у 40 процентов корейских фирм к 2003 году компьютеры были защищены брандмауэрами[91], и это притом, что онлайновые транзакции занимают в Южной Корее более двух третей рыночного оборота. Такая ситуация явилась причиной быстрого распространения в январе 2003 года «великого и ужасного» Интернет-червя «Slammer». В результате проблема быстро приняла общенациональный масштаб (Ассоциация корейских страховщиков, например, заявила, что только предполагаемый объём страховых выплат составит более миллиарда вон – около 1 млн. долларов), и к её решению подключилось пра-

[91] Брандмауэр (переводится с немецкого языка как «стена») – синоним термина «межсетевой экран» или «firewall», используемого в российских средствах массовой информации.

Межсетевой экран (firewall) – является защитным барьером, состоящим из нескольких компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение межсетевого экрана). Межсетевой экран конфигурируется в соответствии с принятой в организации политикой безопасности. Все входящие и исходящие пакеты данных должны проходить через межсетевой экран, который пропускает только авторизованные пакеты.

Политика безопасности – набор законов, правил и практических рекомендаций, на основе которых строится управление, защита и распределение защищаемой информации в системе. Она охватывает все особенности процесса обработки информации, определяя поведение системы в различных ситуациях.

вительство во главе с президентом Ким Дэ Джуном. Отказ сетей отразился на азиатских фондовых рынках, но, ввиду того, что атака вируса пришлась на выходной, её эффект был несколько смягчён. За последние 13 месяцев это были самые низкие объёмы торгов на южно-корейской товарной бирже: инвесторы, пытавшиеся разместить свои заявки через Интернет, вскоре сдавались и прекращали бесплодные попытки. В результате биржевой индекс KOSPI составил лишь 2,7% от самого нижнего своего значения за последние три месяца. Акции двух крупнейших корейских провайдеров, KT Corporation (из 48 миллионов корейцев 70% имеют доступ к Интернет, и половина из них – подписчики KT Corporation) и Hanaro Telecom резко упали в цене.

А теперь угадайте с первого раза, чьи акции поднялись в цене? Правильно, ценные бумаги южно-корейских фирм сетевой безопасности Ahnlab и Hauri поднимались со скоростью до 12% в день. Более того, параллельно, пусть и не столь бурно, росли в цене и акции их японских коллег: Asgent Incorporated в общем прибавила 19% к их стоимости, а Internet Security Systems KK ни много, ни мало целых 26%.

Позвольте высказать небольшой прогноз. В ближайшем будущем конкуренция между производителями антивирусного программного обеспечения обострится. Об этом свидетельствуют как регулярно публикуемые результаты тестов, так и финансовые отчёты компаний-производителей. Продукты крупнейших европейских компаний (не только западноевропейских, но и восточноевропейских) по своей эффективности догнали своих конкурентов из США, а по некоторым показателям и обошли их – этот факт признают сами американцы, и эта тенденция, скорее всего, сохранится в обозримой перспективе. Сейчас производители антивирусного программного обеспечения активно проводят маркетинговые кампании, особенно их интересуют, и будут интересовать азиатский и восточно-европейский регионы, которые ещё не в полной мере ими освоены. Ситуация подогревается также тем, что внедрение вирусов в системы происходит зачастую через «дыры» в подсистемах безопасности, а это не может не волновать разнообразные органы, которые у нас

называют компетентными. Поскольку эти органы весьма заботятся о сохранности своей информации, они справедливо считают, что если вирус нашёл «лазейку», то почему бы в эту же брешь не пролезть кому-либо из компьютерных злоумышленников. Взять тот же компьютерный вирус: отчего бы ему не быть запрограммированным на то, чтобы, пробравшись незамеченным в систему компетентного органа, разместиться в укромном уголке и, продолжая оставаться незамеченным для хозяев, не разрушать хозяйские данные, периодически посылая конфиденциальную информацию своему разработчику.

3.3. Не взирая на громкие имена и авторитеты

Вне всякого сомнения, фирмы-производители программного обеспечения, в том числе и антивирусного, также как и государственные учреждения, осознают опасность, исходящую от вредоносных компьютерных программ и прилагают немало усилий, чтобы снизить уровень существующей угрозы компьютерным системам. Однако так и хочется сказать: «И на старуху бывает проруха!» Почему? Да вот примеры, не столько забавные, сколько показывающие, насколько изощрёнными могут быть современные компьютерные вирусы и люди, ими манипулирующие.

В конце июля 2001 года появившийся менее месяца назад, но уже успевший к тому времени причинить вред почти 300 тысячам компьютеров на всех континентах, «знаменитый» Интернет-червь «SirCam», в очередной раз напомнил о себе тем, что на сей раз его жертвой стал … Национальный центр защиты сетевой инфраструктуры (National Infrastructure Protection Center – NIPC) – одно из ведущих подразделений в составе ФБР США, занимающееся именно вопросами компьютерной безопасности. Вначале была тишина, затем последовало признание, что заражению подвергся компьютер одного из сотрудников Национального центра, но вирус успел разослать своим адресатам лишь документы, предназначенные исключительно для внутреннего пользования, то есть имеющие гриф «Для служебного пользования» (!), и никакой утечки секретной информации вследствие заражения не про-

изошло. В последующем коммюнике, опубликованном NIPC, указывалось, что вирус был получен с электронной почтой, и не был обнаружен и блокирован, хотя на компьютере была установлена последняя версия антивирусной программы, – название которой приведено не было. Как только вирус был идентифицирован, NIPC принял необходимые меры для его блокирования, однако «SirCam» уже был отправлен по всем электронным адресам, которые он нашёл на заражённом компьютере. Представитель ФБР отказался от других комментариев и, в частности, не сообщил о количестве электронных адресов, по которым из ФБР США распространялся компьютерный вирус.

Одно в этой истории «радует». По словам пресс-секретаря NIPC Дебби Вайерман: «…“SirCam” не успел распространиться по внутренней сети и нанести ощутимый вред».

В мае 2000 года система электронной почты «самой» корпорации Microsoft была инфицирована новым на то время компьютерным вирусом, который получил название «South Park», который полностью выводил из строя почтовые серверы. Вирус скрывался в приложениях к сообщению и выводил на мониторы надписи «Servus Alter!» (по-немецки «Здорово, старик!») и «Hier ist das Spiel, dass du unbedingt wolltest» («Эта та самая игра, которую ты так хотел»). А в 20-х числах января 2003 года серверы той же корпорации Microsoft, «одного из главных борцов с любыми проявлениями компьютерной преступности», не устояли и против взрывного распространения уже упоминавшегося Интернет-червя «Slammer». Компьютерный вирус проник в сеть софтверного гиганта и фактически остановил работу всех сетевых сервисов компании. К примеру, целые сутки пользователи не могли выйти на сайт активации Windows XP по причине перегрузки внутренней сети Microsoft «мусорными» пакетами, щедро рассылаемыми с заражённых вирусом «Slammer» серверов. Как именно вирус попал во внутреннюю сеть компании история тёмная, но «комичность» ситуации заключается в том, что соответ-

ствующий патч для MS SQL Server 2000, устраняющий «уязвимость»[92], которую использует «Slammer» для проникновения на сервер, был выпущен самой же Microsoft в свободное пользование за целых полгода до атаки вируса. Причём, как в составе Security Update, так и одного из последних на то время Service Pack. И вот ведь казус – выпустившая «программную заплату» Microsoft, так и не потрудилась обновить свои собственные серверы.

После этого призывы Microsoft к ежедневному латанию своих продуктов силами самих заплативших за них деньги пользователей выглядят не просто странно, а едва ли не цинично и оскорбительно, не правда ли? Microsoft вообще большой мастер «подставляться» под критику.

Хотелось бы на этом завершить наше знакомство с Интернет-червём «Slammer» в данной главе, так как более подробно о потрясшей всё Интернет-сообщество эпидемии мы будем говорить далее, но… Удивительное рядом.

17 февраля 2003 года, то есть через считанные недели после начала глобальной эпидемии вируса «Slammer» выяснилось, что несколько дней назад антивирусная компания Symantec поделилась с ног сшибающей новостью. Оказывается, специалисты Symantec идентифицировали опаснейшего Интернет-червя за несколько часов до его появления. В пресс-релизе компании Symantec говорилось буквально следующее: «Мы своевременно разослали предупреждение об опасности и методах борьбы пользователям DeepSight Threat Management System, что позволило администраторам принять меры защиты против атак». Очевидно, что специалисты Symantec знали об опасности надвигавшейся эпидемии вируса «Slammer», но почему-то молчали как рыба. Точнее сказать говорили, но только «избранным». Результат – самая

[92] Уязвимость – любая характеристика компьютерной, информационной системы или их компонентов, использование которой нарушителем может привести к реализации угрозы. Другими словами, именно из-за наличия уязвимостей в системе происходят нештатные события.

Уязвимость информации – подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению её конфиденциальности, целостности, доступности, или неправомерному тиражированию.

Уязвимость субъекта информационных отношений – потенциальная подверженность субъекта нанесению ущерба его жизненно важным интересам посредством воздействия на критичную для него информацию, её носители и процессы её обработки.

масштабная эпидемия за время существования Интернет, которая поставила на грань катастрофы всю Глобальную сеть. Ведь если бы круг посвящённых был шире, скорее всего, удалось бы избежать значительной части последствий эпидемии: в подавляющем большинстве случаев системные администраторы смогли бы остановить Интернет-червя, просто заблокировав порт 1434. Со своей стороны официальные лица Symantec объяснили свои действия следующим образом: «Вы не можете получать предупреждения, пока не являетесь клиентом Symantec DeepSight Threat Management System и не оплачиваете наши услуги». Комментарии излишни…

Реакция экспертов в области безопасности на известие о поступке специалистов Symantec была неоднозначной. Например, консультант по безопасности Diamond Technical Group Джефф Джонстоун сказал следующее: «Я думаю, что подобные действия попадают под определение «преступная небрежность». Это была не просто информация о вирусе, это были экстренные сведения о надвигающейся угрозе всей инфраструктуре Интернет. Подобный тип информации распространяется всегда среди всех членов сферы безопасности!». Напомним, что по подсчётам аналитиков, общий ущерб, понесённый мировыми компаниями в результате эпидемии вируса «Slammer» составил около 1,2 млрд. долларов. Согласно мнению аналитической компании Computer Economics, на ликвидацию последствий эпидемии затрачено порядка 1 млрд. долларов. Кроме экономического ущерба, атака вируса «Slammer» продемонстрировала уязвимость Интернет в целом и наглядно указала на одно из слабых мест, через которые можно вообще остановить работу Глобальной сети. Ранее ни один другой компьютерный вирус не угрожал фактически разорвать на части работу Интернет и нарушить коммуникации между разными регионами мира. На пике эпидемии «Slammer» вызвал замедление работы Интернет до 25%, а это значит, что доступ к каждому четвёртому сайту был или невозможен, или затруднён. Схожие нарушения были выявлены и в других службах, использующих Интернет: электронной почте, FTP-сервисах, сетевых пейджерах и т. д.

В свете вышеизложенного поведение специалистов компании Symantec, представляющей собой одного из крупнейших в мире производителей антивирусного программного обеспечения, трудно поддаётся объяснению с точки зрения здравого смысла… или, наоборот, очень даже объяснимо и предсказуемо.

В мае 2001 года главный радетель и борец в Конгрессе США за всё, что касается ужесточения мер и повышения эффективности электронных средств обеспечения безопасности информации[93], сенатор-республиканец от штата Юта Роберт Беннет, пал жертвой Интернет-червя «Homepage»[94]. Произошло это после того, как один из помощников сенатора по неосторожности открыл заражённое вложение на служебном компьютере Беннета. Представитель сенатора Мэри Коллиприст заявила, что почтовая система сенатора разослала червя более чем по двум сотням адресов, содержащихся в его адресной книге. Среди адресатов были журналисты, депутаты Юты, деловые партнёры и другие законодатели. После того как опасность распознали, были предприняты дополнительные меры защиты, а системному администратору сенатора пришлось разослать адресатам, получившим «червя от Беннета», более 200 писем-сообщений с извинениями. Случившееся заставило штат помощников сенатора по-новому взглянуть на комплекс мер, обеспечивающий защиту систем, которыми пользуется сенатор, и произвести некоторую его переоценку.

Интересным фактом является то обстоятельство, что, по словам представителя сенатора, так и остаётся не выясненным, была ли это спланированная атака на известного своей поддержкой мер по усилению безопасности в киберпространстве сенатора, чья-то злая «шутка» или случайность. Сенатор Роберт Беннет, занимавший председательский пост в комитете сената по

[93] Безопасность информации – защищённость данных от нежелательного (для соответствующих субъектов информационных отношений) её разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного её тиражирования.

[94] Подобно другим червям схожей конструкции, вирус «Homepage» поражает в первую очередь адресные книги, размножаясь и рассылая копии по всем адресам, содержащимся в поражённой книге. В отличие от других Интернет-червей «Homepage» не причиняет вреда самому заражённому компьютеру. Но, после внедрения в MS Outlook, вирус запускает Интернет-браузер и открывает один из четырёх «взрослых» сайтов, а затем «заметает следы» стираясь из папки «Входящие» и уничтожая темы сообщений.

«Проблеме 2000» всегда был одним из самых горячих приверженцев «усиления средств антивирусной защиты федерального правительства США» и, соответственно, объектом пристального внимания вирусописателей. Буквально за несколько дней до происшествия он озвучил свои планы о том, что в ближайшее время выступит с новой инициативой по кибербезопасности и кибертерроризму.

Кстати к вопросу о кибербезопасности и кибертерроризме в свете атак вирусов.

3.4. Терроризм и кибертерроризм

Практически сразу после громких террористических актов в США 11 сентября 2001 в Интернет появился деструктивный компьютерный вирус, эксплуатировавший трагедию во Всемирном торговом центре (World Trade Center) и маскирующийся под программу голосования по вопросу о вступлении США в войну. Уже 25 сентября в средствах массовой информации появились сообщения о компьютерном вирусе, получившем название «Vote Virus» и якобы призывающем к миру, а эксперты по компьютерной безопасности забили тревогу, сообщив о появлении очередного вредоносного почтового червя. Распространение вируса шло достаточно медленно, однако грозило ускориться, благодаря эмоциональному аспекту, который был в него предусмотрительно заложен. Вирус поступал по электронной почте с темой «Peace between America and Islam!» («Мир между Америкой и Исламом»), в теле письма содержалась фраза «Hi. Is it a war against America or Islam!? Let's vote to live in peace!» («Привет. Эта война направлена против Америки или против Ислама!? Проголосуем за мирную жизнь!»). К письму прикладывался файл «wtc.exe», который выдавался вирусописателем за программу голосования и, как многие другие почтовые черви, начинал действовать при открытии вложенного в письмо файла: по всем адресам, имеющимся книге MS Outlook, распространялись подобные письма. Кроме того, вирус не только замедлял скорость передачи данных в Интернет, но также разрушал каталоги на компьютере и был способен нанести ущерб даже жёсткому диску заражённой

машины. Компании Trend Micro и Symantec сообщали, что: «вирус также способен изменять главные страницы заражённых серверов, помещая на них предупреждение о мести в случае начала Соединёнными Штатами военной операции: «AmeRiCa ... Few Days WiLL Show You What We Can Do! It's Our Turn!>>>ZaCkEr is So Sorry For You» («Америка … Через несколько дней вы узнаете на что мы способны! Теперь наша очередь!>>>Zacker так скорбит о вас!»). При заражении серверов «Vote Virus» стремился удалить файлы из папки Windows и антивирусные программы, а также отформатировать систему и создать в ней «чёрный ход». По мнению большинства экспертов, автор нового вируса не был связан с террористами, а пытался сыграть на чувствах людей, считающих своим долгом высказать мнение об ответе США на террористические акты. В этом смысле схема распространения вируса чем-то напоминала схему распространения классического почтового червя «I Love You», также играющего на чувствах людей. Эксперты предупреждали, что хотя «Vote Virus» не успел широко распространиться, однако актуальность темы может повлечь за собой создание новых вирусов, эксплуатирующих ту же трагедию.

И, как в воду смотрели… Уже 26 сентября в Интернет был обнаружен новый милитаристский вариант червя «Vote Virus». Так же, как и первая версия вируса, новая модификация не слишком широко распространилась в Интернет, и его распространение в основном происходило в границах США. Однако этот вирус был не менее опасен, чем его «старший брат», поскольку после заражения он запускал процедуру форматирования жёсткого диска при очередной загрузке компьютера. Новый вирус получил название «VBS_Vote.b» и если первая версия призывала к миру, то вторая версия этого вируса была более воинственной. В теме электронного письма значилось: «This war must be done!». В теле письма содержалось столь же милитаристское воззвание: «Hi we must fight, we must remember our victims! No peace before killing terrorists!» Прилагаемый файл, который, конечно же, нельзя было открывать, назывался Anti_TeRRoRisM.exe.

Не успели улечься события, связанные с «Vote Virus», как из Южной Кореи начали поступать сообщения об обнаружении 23 октября 2001 года и довольно активном распространении в южнокорейской Сети нового компьютерного вируса, названного «Усама бен Ладен» по имени самого известного в мире террориста, которое содержится в заголовке заражённого письма. Вирус был обнаружен корейской компанией по разработке антивирусного программного обеспечения Ahnlab Co Ltd. и, по словам её представителя Джина Йун-Джанга, первое сообщение о новом вирусе пришло от одного из южнокорейских пользователей, утверждавшего, что он получил заражённое письмо по e-Mail. Автор вируса не был известен, сам же вирус распространялся довольно активно. Заражённые письма имели несколько вариантов заголовка: «Bin Laden toilette paper!!», «Sadam Hussein&BinLaden In Love» и «Is Osama BinLaden bad-loved?»; а также приложение: binladen_brazil.exe. Ущерб, наносимый этим вирусом, выражался в уничтожении программного обеспечения, замедлении работы компьютера и открытии содержащейся на его жёстком диске информации перед другими пользователями сети, к которой подключён компьютер.

Забегая вперёд, отметим, что и годовщину террористических актов 11 сентября 2001 года в Нью-Йорке и Вашингтоне вирусописатели отметили по-своему – появился новый компьютерный вирус, играющий на актуальной теме. Этот Интернет-червь был обнаружен 11 сентября 2002 года, получил наименование VBS/Nedal (Nedal – Laden наоборот) и обладал способностью распространяться и по электронной почте, и через IRC-чаты. В последнем случае он заражал программы mIRC и pIRCH. При распространении через электронную почту вирус приходил в письме с темой «Osama Bin Laden Comes Back!» («Осама бен Ладен возвращается!»). В письме содержатся слова о том, что письмо пришло от Бен Ладена, и призывы уничтожить США и Израиль. На поражённом компьютере (где расположена операционная система Windows) вирус создаёт три исполняемых файла: osama.exe, laden.exe и alta.exe. Osama.exe представляет собой вирус, заражающий другие .exe-

файлы, а третий перезаписывает файлы с расширениями «.vbs», «.vbe», «.gif», «.jpg», «.bmp», «.avi», «.mp3», «.mpg», «.zip», «.cab», «.mdb», «.xls», «.lnk», «.doc», «.txt» и «.rtf». Кроме того, alta.exe вносит изменения в системный реестр Windows и выводит на экран различные сообщения.

Советник Белого дома по безопасности в киберпространстве назвал угрозу, исходящую от подобных вирусов «цифровым Пирл-Харбором». Однако никаких доказательств того, что какие-либо страны и террористы ведут целенаправленную кибервойну против США, представлено не было. В результате уже в ноябре 2001 года некоторые американские эксперты по безопасности, а также эксперты из других западных стран стали утверждать, что кибертерроризм – это не более чем «фантазия», и полагали, что ФБР США слушает «не те советы», и поэтому раздувает бессмысленный шум вокруг атак вирусов. «Вирусы – плохое оружие для боевых действий; у них нет систем наведения, так что тот, кто их посылает, вполне может сам оказаться жертвой, если не поставит защиту; кроме того, появление противоядия от любого, даже самого сложного вируса, – это вопрос нескольких часов», – заявил Грэм Клули, старший технический консультант компании Sophos. Клули также настаивал на том, что киберпространство не станет очередным полем сражения в международных конфликтах. За всё время существования Интернет очень немногие вирусы были созданы по политическим мотивам, к тому же все они были не опасны, и с ними было легко управиться. Одновременно Клули критиковал ФБР США за создание их собственного вируса – троянской программы «Magic Lantern» («Волшебный фонарь»), которую оно собирается использовать против организаций и лиц, подозреваемых в кибертеррористической деятельности и совершении разного рода преступлений. По его словам «технология, на основе которой создаётся “Magic Lantern”, была известна ещё три года назад».

Между прочим, упомянутая Грэмом Клули программа «Made in ФБР» под названием «Magic Lantern»[95] действительно существовала и, в ноябре 2001 года, даже стала предметом довольно жаркой дискуссии между представителями компаний-разработчиков антивирусного программного обеспечения. Камнем преткновения стал вопрос, включать им в свою продукцию средства обнаружения и борьбы с троянским конём «Magic Lantern» или нет? Ситуацию ещё больше запутывало то обстоятельство, что если Конгресс США и позволит ФБР США пользоваться «Magic Lantern», то вряд ли он сможет запретить вирусописателям модифицировать новую троянскую программу для своих целей и, в дополнение к этому, «Magic Lantern» предположительно сделан на основе старых технологий, так что некоторые антивирусные программы уже способны его поймать.

Представители Symantec заявили, что если ФБР США добьётся полной монополии на использование этого средства, они не станут включать в свои продукты средства борьбы с «Magic Lantern». Уже известный нам Грэм Клули заявил, что Sophos обязательно включит средства защиты от «Magic Lantern» в свои антивирусные программы, поскольку зарубежные пользователи на вполне законных основаниях хотят обезопасить себя от любых вирусов, в том числе, и «правительственных». «Что если французская разведка, или греческая, сделают свои троянские программы? На них нам тоже внимания не обращать?», – резонно заявил Клули. В продолжение дебатов 29 ноября 2001 года на Web-сайте компании Sophos появилось официальное сообщение по поводу «Magic Lantern». Представители Sophos заявили, что пользователи давно проявляют беспокойство насчёт появления этой программы и возможности её попадания в руки злоумышленников, и заверили, что безопасность пользователей для них важнее всего. «Компания Sophos хотела бы заверить своих клиентов, что никаких просьб отключить средства обнаружения виру-

[95] Являясь частью пресловутой программы по надзору за Интернет, «Magic Lantern» внедряется на компьютер через электронную почту или известные «дыры» в программном обеспечении, установленном на нём, а затем запоминает нажимаемые клавиши и передаёт информацию прямиком в ФБР США. То есть вирус представляет собой классического «клавиатурного жучка», который перехватывает все набираемые на компьютере символы и записывает их в секретный файл, чтобы позднее использовать его в качестве улики или для дешифровки закодированных файлов и писем.

сов, созданных какой-либо спецслужбой мира, в компанию не поступало, и мы продолжаем считать, что для наших пользователей важно, чтобы подобные вредоносные программы могли быть обнаружены», – говорилось в сообщении. Это означало, что разбираться с «правительственными» троянскими программами антивирусные продукты Sophos будут без антимоний и «на общих основаниях».

В конце концов, здравый смысл и твёрдая позиция компании Sophos взяли верх и в декабре 2001 года производители антивирусных средств заявили, что не собираются исключать из своих продуктов функции обнаружения вирусов, созданных правительственными агентствами, ведущими слежку в компьютерных сетях. Представители Symantec, Network Associates и японской компании Trend Micro заявили, что не будут модифицировать свои продукты для удовлетворения нужд ФБР США, так как они считают своей важнейшей задачей обеспечение антивирусной безопасности пользователей и не собираются компрометировать себя созданием закладок для спецслужб. Кроме того, создание такой «закладки» открывает несанкционированный доступ к информации не только правительственным агентствам, но и вирусописателям со всего мира.

Теперь ожидаемое. Так и хочется сказать словами одного из персонажей известного детектива «Место встречи изменить нельзя»: «Ладно, спорщики, приехали. Там вас сейчас помирят».

Шумиха вокруг вредоносной программы привлекла пристальное внимание вирусописателей во всём мире и слухи вокруг разработки ФБР США собственной троянской программы под кодовым названием «Magic Lantern» вызвали явно нездоровый интерес у клана вирусописателей.

12 декабря 2001 года (завидная оперативность!) появилась первая ласточка – 17-летний аргентинский вирусописатель под «скромным» именем «Agentlinux» разработал троянского коня, маскирующегося под широко разрекламированный вирус а-ля ФБР. От самого бюро не последовало никаких комментариев по этому поводу, и буквально через несколько дней поступило

сообщение о появлении написанной на Visual Basic троянской программы «Malantern»[96], которая маскируется под «Magic Lantern».

Таким образом, было наглядно показано, что в случае появления «официального» «Magic Lantern» вирусописатели могут разродиться его многочисленными модификациями, и совсем не исключена возможность попадания к ним оригинального кода этой программы, который они смогут использовать в своих целях. По этим причинам отказ антивирусных компаний от детектирования «Magic Lantern» мог вызвать эпидемию, с которой пользователи не смогли бы справиться при помощи их антивирусных программ. В свою очередь это могло бы повлечь глобальный, неуправляемый хаос с непредсказуемыми последствиями. Значит, права была компания Sophos, когда отказалась отключить в своих продуктах средства обнаружения каких-либо вирусов, невзирая на то кем и с какими целями они не были созданы!

Итак, вернёмся к вопросу о кибербезопасности и кибертерроризму в свете атак вирусов. Вы верите в то, что Интернет-червь «Slammer» был создан исламскими экстремистами?

Как бы там ни было, но 6 февраля 2003 года одна из радикальных исламских группировок «Харкат-уль-моджахеддин»[97] взяла на себя ответственность за заражение Глобальной сети этим компьютерным вирусом, чья эпидемия фактически парализовала работу Интернет.

Представители этой группы вступили в переписку с Web-сайтом Computer World, в которой заявили, что: «начав «киберджихад», мы использовали Интернет для того, чтобы посеять хаос и смятение среди неверных». А в качестве доказательства своего авторства они указали на то, что в одной из первых инструкций программного кода вируса содержится число 42, которое означает сокращённое название их группы, «HUM». В латинском алфавите

[96] При запуске уничтожает каталог временных файлов операционной системы MS Windows (C:\Windows\Temp) и все файлы с расширением «.sys» в каталоге системных драйверов (C:\Windows\System32\Drivers\).

[97] Организация «Харкат-уль-моджахеддин», ранее известная как «Харкаль-уль-Ансар», базируется в Пакистане, неподалеку от индийской границы. Члены «HUM» подозреваются в организации взрыва у здания американского посольства в Исламабаде, двух покушениях на президента страны, генерала Мушарафа, похищении и убийстве американского журналиста, а также связях с «Аль-Кайдой».

буква «H» имеет порядковый номер 8, «U» – 21, а «M» – 13, что в сумме и дает число 42.

Большинство экспертов по Интернет-безопасности скептически отозвались о таком совпадении. «Автора вируса нельзя идентифицировать по его коду, – приводит свои доводы Педрам Амини из калифорнийской компании iDefense, – Схожий с использованным в вирусе «Slammer» код уже размещала на своем Web-сайте китайская группа вирусописателей «Honker Union of China», а применённый в нём математический алгоритм был представлен летом 2002 года на конференции по компьютерной безопасности «Black Hat». Однако практически одновременно с подобными высказываниями экспертов по Интернет-безопасности представитель ФБР США заявил, что «хотя группировка «HUM» и не рассматривается в качестве подозреваемой, но её возможная деятельность на ниве кибертерроризма и вероятное отношение к происшедшему тщательно изучаются. Может быть, таким образом, эта организация хочет привлечь к себе больше внимания».

В этой истории интересна не столько мера правдоподобия заявлений группировки «Харкат-уль-моджахеддин», сколько сам факт того, что религиозные фанатики при случае не прочь использовать современные информационные технологии как средство проведения атак вирусов с самыми разрушительными и непредсказуемыми последствиями для всего глобального информационного пространства. В частности и поэтому многие эксперты из государственных служб, и специалисты по безопасности из корпоративного сектора экономики предостерегают, что за нападением на Всемирный торговый центр в Нью-Йорке и Пентагон может последовать волна кибертерроризма – вопрос только во времени. Представители администрации США, например, сразу после этих терактов прямо высказывались в интервью средствам массовой информации, что «они опасаются того, что вчерашние террористические акты могут быть только началом волны атак, включающих и кибертеррористические».

На этом фоне удручает следующая информация. 23 мая 2001 года информационный портал «Yahoo!» обнародовал следующее сообщение: «Правительственному агентству, занимающемуся вопросами кибербезопасности, катастрофически не хватает персонала, и именно поэтому множество компьютерных вирусов бывает обнаружено лишь после того, как они успевают нанести ущерб». К такому выводу пришли аудиторы из Министерства финансов США, проводившие аудит в уже известном нам NIPC. По их мнению, нехватка персонала и отсутствие некоторых ключевых сотрудников NIPC подвергает риску национальную безопасность США и ослабляет защиту от вирусописателей и компьютерных вирусов, затрудняя борьбу ФБР США с киберпреступностью. «В то время как некоторые предупреждения об опасности поступают вовремя, другие, касающиеся в первую очередь компьютерных вирусов, приходят слишком поздно», – заявили представители уже упоминавшегося министерства.

Да и в Европе дела обстоят не лучше – европейские специальные подразделения также страдают от нехватки специалистов и их плохой подготовки, и поэтому «не способны бороться с киберпреступностью», заявил на совещании представителей полицейских департаментов европейских государств Юрген Шторбек, руководитель организации Europol. По мнению г-на Шторбека, государства должны объединить свои усилия в борьбе с киберпреступностью, «пока ещё не слишком поздно». Руководитель Europol полагает, что в этих условиях работники специальных подразделений должны получить дополнительное образование, которое позволит им бороться с новыми видами преступности, к которым, вне всякого сомнения, относится и распространение вредоносных компьютерных программ. Подчеркнём, что это говорилось в середине 2001 года, хотя впервые проблема преступности в сфере высоких информационных технологий рассматривалась ещё на встрече глав государств Европы в 1999 году, где было принято, например, решение об учреждении и всемерном развитии новой формы взаимодействия правоохранительных органов различных государств – национальных контактных пунк-

тов, которые позволяли бы осуществлять мониторинг и непрерывный обмен оперативной информацией. Кстати говоря, сейчас большинство компьютерных преступлений раскрывается именно благодаря международному сотрудничеству.

Несмотря на то что далеко не всё идёт гладко, отрадно, что мировое сообщество поняло – в отличие от национальных правоохранительных органов компьютерные вирусы, телекоммуникационные сети и Интернет не знают границ. И соответствующая преступность также не имеет национальных признаков.

Эпидемия Интернет-червя «Slammer», начавшаяся в январе 2003 года стала крупнейшей не только по числу заражённых им серверов, скорости и географии распространения, но и по последствиям для функционирования всей Интернет. «Slammer» это единичный случай непреднамеренной атаки вируса? Это очередной шаг кибертеррористов с целью определения наиболее слабых мест для моделирования и проведения последующей крупномасштабной атаки вирусов на Интернет? Каковы последствия эпидемии «Slammer» для развития и самого будущего Интернет? Эти вопросы должны быть далеко не безразличны не только профессионалам в области разработки антивирусных средств и борьбы с компьютерной преступностью в целом, а каждому, кто как-то связан с использованием информационных технологий и Интернет, в том числе.

По нашему глубокому убеждению эпидемия «Slammer» по своим устрашающим последствиям является проявлением самого настоящего кибертерроризма, так как речь здесь идёт о сознательном нарушении работы всемирного средства коммуникаций. Поэтому, если не принять жёстких мер по пресечению и упреждению подобных атак вирусов уже в самом ближайшем будущем ситуация может выйти из-под контроля и поставить под сомнение само существование Интернет. Вместе с тем в свете изложенных выше условий такие меры фактически нереализуемы. Работоспособная система выявления и предотвращения эпидемий вирусов не может базироваться на

сегодняшних реалиях Интернет. При возникновении эпидемии специалистам крайне трудно быстро определить её первоисточник – за исключением тех прецедентов, когда автор вируса сам демаскирует себя по глупости, случайности, неосторожности или намеренно в поисках сомнительной славы. И вот вам классические примеры.

10 декабря 2001 года в Израиле специальным подразделением полиции по борьбе с киберпреступлениями по обвинению в создании и распространении упоминавшегося нами ранее опасного компьютерного вируса «Goner»[98] были арестованы пять подростков. Первоначальное расследование, проведённое полицией, показало, что вирус был написан в ходе борьбы между двумя молодёжными группировками и распространением «Goner» подростки хотели доказать противникам своё интеллектуальное превосходство. Налицо «в одном флаконе» мальчишество, глупость и поиск сомнительной славы в среде своих сверстников, за которые, тем не менее, придётся отвечать по-взрослому, так как в соответствии с израильскими законами за подобные деяния можно получить срок заключения от трех до пяти лет. Что сказать? Доказали.

19 декабря 2002 года 22-летний британский Web-дизайнер, Симон Валлор из Лландадно (Уэльс) признал себя виновным в написании и распространении через Интернет трёх опасных компьютерных вирусов. Симон был обвинен в нарушении британского закона о противоправном использовании компьютерных технологий (Computer Misuse Act) от 1990 года путём написания и распространения вирусов. Он распространял такие вирусы как «Admirer», «Gokar» и «Redesi», причём, один из них, Интернет-червь «Gokar», в начале 2002 года заразил 27 тысяч компьютеров по всему миру. Все три вируса автоматически начинали копировать и распространять себя по всем электронным адресам заражённого компьютера, как только жертва открывала инфицированное письмо.

[98] Вирус «Goner» был признан одним из наиболее опасных вирусов. Антивирусные компании присвоили ему 4 уровень – самый высокий по разрушающему действию, оказываемому на компьютер жертвы. Он распространяется по электронной почте в виде скрин-сейвера, а также по ICQ.

Валлор был арестован в первых числах февраля 2002 года, после того как ФБР США отправило свои исследования по распространению компьютерных вирусов в отделение лондонской полиции, занимающееся расследованием киберпреступлений. Его вычислили на одном из чатов, где он под именем «Гобо» безудержно хвастался созданием очередного вируса. Перед последним судебным слушанием, на котором дизайнер признал свою вину, Валлор поместил на своем сайте нечто вроде публичной исповеди: «Я бы, конечно, хотел быть осужден условно, но, думаю, я прошу слишком о многом. Если же меня все-таки осудят, помните: «Mundis vult decipi, ergo decipaitur»[99]. Я не могу сказать, что всё в этом мире было хорошо – ну так, немного смешного, несколько шуток, немного выпитого и выкуренного. Мне есть, о чём сожалеть, однако я не стыжусь быть самим собой». В соответствии с законом Валлор проходил по статье, предусматривающей наказание в виде пятилетнего срока в тюрьме.

В начале апреля 2003 года уголовной полиции Испании удалось задержать автора вируса «Cabronator». Им оказался 27-летний программист из провинции Валенсия. Троянская программа «Cabrotor» позволяла воровать информацию с компьютера жертвы. Согласно оценкам специалистов, за несколько месяцев вирус поразил около 100 компьютеров, нанеся пользователям ущерб в несколько сот тысяч евро. Операция по поиску автора вируса называлась «Клон» и длилась с лета 2002 года. Полиции стало известно о существовании Web-сайта, где можно было скачать не только саму троянскую программу «Cabrotor», но и внимательно изучить инструкцию по её применению, заботливо размещённую автором. Конечно, такой сайт сразу вызвал большие подозрения, и полиции оставалось лишь вычислить местонахождение компьютера, откуда вирус начал своё шествие по миру. Так, по цепочке, полиция добралась до вирусописателя. В соответствии с законами Испании программист вирусописатель заслужил тюремное заключение, плюс

[99] «Мир хочет быть обманутым, так будем же обманывать его» (*лат.*).

выплату круглой суммы в качестве компенсации за ущерб, причинённый им пользователям[100].

3.5. Жертвы и разрушения

В случае масштабной эпидемии компьютерных вирусов в целях предотвращения их дальнейшего распространения приходится отключать целые сети, что несёт с собой огромный ущерб экономике всех развитых стран, но это мало эффективно, так как бороться необходимо с причиной, а не последствиями болезни. Кроме общеэкономических факторов, актуальность антивирусных мероприятий, в частности, объясняется и тем обстоятельством, что компьютерные вирусы были и остаются одной из наиболее распространённых причин потери собственниками информации[101], владельцами информации[102], пользователями информации[103] данных и прикладных программ, которые зачастую не поддаются известным технологиям их восстановления, а также не могут быть оценены в чисто экономических категориях.

В мае 2000 года ФБР США выступило с предупреждением о появлении быстро распространяющегося по мировым сетям нового вируса-червя «Killer Resume», передающегося по электронной почте посредством MS Outlook. Вирус являлся клоном («Melissa.bg») небезызвестного вируса «Melissa», разрушительную эпидемию которого деловой мир пережил в 1999 году, и распространялся через файлы, прикреплённые к письму с темой «Resume-Janet Simons». К письму был приложен текстовый файл под названием explorer.doc или resume.doc. При открытии файла вирус рассылал свои копии по всем ад-

[100] Более подробно об авторах вирусов вы можете прочитать в Приложении 2.

[101] Собственник информации – субъект, реализующий в полном объёме полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами; субъект информационных отношений, обладающий юридическим правом владения, распоряжения и пользования информационным ресурсом. Юридическое право владения, распоряжения и пользования информационным ресурсом принадлежит лицам, получившим этот информационный ресурс по наследству.

[102] Владелец информации – субъект, осуществляющий владение и пользование информацией и реализующий полномочия и распоряжения в пределах прав, установленных законом и/или собственником информации; субъект информационных отношений, обладающий правом владения, распоряжения и пользования информационным ресурсом по договору с собственником информации.

[103] Пользователь информации – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею; юридическое или физическое лицо, обладающее полномочиями доступа к информации; субъект, пользующийся информацией, полученной от её собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации либо с их нарушением.

ресам из адресной книги MS Outlook, затем записывал себя в директории автозапуска и C:\Data\normal.doc, а потом уничтожал на всех дисках от C: до Z: все файлы в корневом директории и директориях C:\MyDocuments, C:\Windows, C:\Windows\System, C:\Winnt\System32, C:\Winnt. Эксперты тогда заявили, что вирус-червь «Killer Resume» не причинил необратимый вред информации множества компьютеров только по той причине, что «был выпущен на свободу под конец рабочего дня в пятницу, в канун выходных».

В августе 2000 года специалистами по производству антивирусных программ была обнаружена первая в своём роде деструктивная троянская программа, уничтожающая данные на компьютерах Palm. Анонсированная как модернизация к программному обеспечению Palm, она маскируется под патч к shareware-версии известного коммуникационного развлекательного средства Liberty и носит название «Crack 1.1». В антивирусных базах данных она значится как Palm.Liberty.A. На самом деле троянская программа просто удаляет все программы на компьютере, оставляя нетронутыми адресную книгу, дневник и другие базы данных пользователя. Интересно, что автор программы сказал, что ни в коем случае не намеревался распространять её, и оказал содействие антивирусным компаниям в детектировании программы.

В июне 2001 года в «диком» виде был обнаружен новый, очень опасный Интернет-червь «MsWorld», который благодаря довольно быстрой реакции фирм-разработчиков антивирусного программного обеспечения не вызвал эпидемии. Червь распространялся при помощи вложенных файлов в сообщениях электронной почты MS Outlook. В теме письма было указано: «Miss World», а в тексте самого сообщения предлагалось полюбоваться на фотографии победительниц конкурса. Однако при открытии вложенного файла активизировался компьютерный червь «MsWorld», который инициировал процедуру распространения по электронной почте, получал доступ к функциям MS Outlook, считывал из адресной книги первые 50 адресов и рассылал по ним свои копии. А вот затем Интернет-червь «MsWorld» записывал в конец файла C:\autoexec.bat несколько команд, которые при запуске снача-

ла выводят сообщение: «This Everything for my Girl Friend, (CatEyes, KRSSL, SS Hostel)» и потом форматируют все системные диски. Кроме того, «MsWorld» уничтожал файлы системного реестра MS Windows system.da0 и user.da0, то есть копии данных системного реестра.

В 20-х числах августа 2001 года эксперты по компьютерной безопасности предупредили об обнаружении в Интернет сразу двух новых вредоносных программ, обладающих ярко выраженными деструктивными свойствами.

Первой программой такого рода, стал написанный на языке JavaScript, прячущийся в HTML-документах и способный модифицировать системный реестр Windows, делая операционную систему неработоспособной, троянский конь «Offensive» (другие названия: FLUG и JS@Juck). Он использует обнаруженную ещё около 10 месяцев (!) тому назад уязвимость в безопасности виртуальной Java-машины от Microsoft (использует ошибку в ActiveX Control, что позволяет выполнять злонамеренные скрипты на пользовательской машине) и распространяется в виде электронного письма формата HTML, в котором имеется единственное слово «Start», помеченное как гиперссылка. При нажатии на эту ссылку и запускается «Offensive».

Вирус при физическом перезапуске системы почём зря нехорошими словами ругает японское правительство и японцев – в результате изменения двух ключей в реестре (LoadPowerProfile и SchedulingAgent), сделанных этим «трояном», Windows выводит неприличные сообщения: «fuck japanese» и «fuck japanese government». Ну, это мы с трудом, но переживём.

А вот дальше гораздо больнее… При открытии инфицированного HTML-файла «троян» создаёт на компьютере пользователя ActiveX-объект, который запускает на выполнение зловредный скрипт, модифицирующий около 50 ключей системного реестра, – в результате чего ограничивается пользовательский доступ к компьютеру, также блокируется запуск приложений, пункт меню «Завершение работы», убираются с рабочего стола все значки. Впрочем, для краткости приведём (без описания) список ограниче-

ний, которые делает «Offensive»: отключает/удаляет меню «Run»; делает невозможными изменения в меню «Start»; отключает автозапуск CD-ROM; удаляет Favorites из меню «Start»; удаляет меню «File» из Explorer; отключает меню «Find»; удаляет меню «Folder->Options»; удаляет иконку Internet Explorer с рабочего стола и из Explorer; отключает документы из меню «Documents»; отключает/удаляет меню «LogOff»; отключает Active Desktop; отключает вызов Taskbar по правой кнопке мыши; удаляет Windows Update из меню «Start»; отключает desktop (правый клик мыши перестает работать); удаляет сетевое окружение; отключает все утилиты для редактирования системного реестра, например, Regedit; удаляет «закладки» в окнах Display Settings и System Properties.

Кроме того, скрипт также изменяет следующие установки в Internet Explorer: заменяет в главном заголовке «Microsoft Internet Explorer» на «If you have any trouble please email:findlu@21cn.com note: not for japanese&dog&pig»; изменяет кнопку «Related To» в Internet Explorer на «Fuck Japanese» и помещает ее на Toolbar (по умолчанию она имеет атрибут hidden). В окне Windows Logon вирус меняет заголовок и текст на следующий: «If you have any trouble please email:findlu@21cn.com note: not for japanese&dog&pig». «Троян» добавляет вхождение в меню по правому клику мышки на диске: «how to fuck Japan». Также изменяет свойства файлов со следующими расширениями, тем самым не позволяя им работать должным образом: exe, reg, htm, html, txt, inf, ini, dll, sys, com, bat. Изменяет ключи в секции автозапуска системного реестра, чтобы после каждого старта Windows деинсталлировались следующие программы: internat.exe, scanreg.exe, taskmon.exe, systray.exe, powprof.dll.

Поскольку «Offensive» блокирует все приложения, включая антивирусные программы, автоматическое восстановление системы становится невозможным и для устранения последствий атаки вируса необходимо восстановить или переустановить Windows, что требует определённой подготовки, времени и под силу не каждому пользователю. Троян представляет опасность

для пользователей браузера Internet Explorer всех версий от 3.0 до 5.5sp1 включительно, если только на них не установлен соответствующий патч.

Подчеркнём, что по мнению специалистов троянская программа «Offensive» не вызвала эпидемию в основном только из-за того, что она не способна распространяться самостоятельно, а также из-за весьма преклонного «возраста» используемой уязвимости.

Второй программой такого рода, стал полностью разрушающий систему троянский конь «Zeraf», который удаляет системные файлы, «убивая» тем самым операционную систему Windows и делая принципиально невозможной загрузку с жёсткого диска. Представитель Symantec старший научный сотрудник Андре Пост, в связи с появлением «Zeraf» сделал следующее заявление: «Эта троянская программа выделяется своей высокой разрушительной способностью. Кроме того, её невозможно распознать до открытия – вирус приводится в действие при запуске exe-файла, так как файл может просто переименовываться перед отправкой к очередной жертве». В итоге самым безопасным, и рекомендуемым способом борьбы с вирусом является, как это ни прискорбно, полная переустановка операционной системы.

К счастью, «Zeraf» не пытается размножаться, так что шансы случайно «подцепить» новый вирус очень малы.

21 мая 2003 года компания-разработчик антивирусного программного обеспечения Panda Software сообщила о появлении нового опасного червя. Получившая название «Petik.n» (другое название: «VBS/Petik.n») вредоносная программа, перезаписывает все файлы на инфицированном компьютере. Перед запуском процедуры уничтожения файлов «Petik.n» создаёт сотни пустых файлов с расширением «.txt» на рабочем столе Windows. Их имена начинаются со слова «stress», к которому случайным образом добавляются четыре буквы. В итоге на подвергшемся атаке вируса компьютере может быть утеряна вся информация, и восстановить её не удастся ни одним из известных программных методов. Отметим, что особенно опасен «Petik.n» для

корпоративной среды, так как в основном он распространяется через общие сетевые диски.

Широко известны случаи, когда компьютерные вирусы нарушали или блокировали работу не только отдельных правительственных учреждений, государственных предприятий, коммерческих организаций, электронных магазинов, Интернет-провайдеров и т. п., но и нарушали нормальную деятельность ведомств, муниципальных служб и крупных корпораций.

Например, в феврале 2000 года очередная модификация давно и, казалось бы, хорошо известного вируса «Melissa», уже нанесшего рекордный за 1999 год ущерб, вывела из строя правительственную систему электронной почты в округе Снохомиш (штат Вашингтон, США). Вирус ухитрился вывести из строя все серверы электронной почты, и систему удалось восстановить лишь более чем через сутки после его активизации. Распространяясь по электронной почте в виде письма с темой «Important Message» вирус активизировался при его открытии ничего не подозревающим пользователем и рассылал свои копии по адресам из адресной книги. Ровно через год канадская компания Neurocom заявила, что результаты её исследований указывают на тот факт, что миллионы почтовых ящиков различных почтовых систем, и особенно службы Hotmail, подвержены риску «троянской» атаки. Представители Neurocom заявили, что обнаружили «дыру в почтовых системах, благодаря которой «трояны» могут незаметно проникать через фильтры систем Hotmail, Yahoo!, Zdnetmail, Caramail и многих других. «Ошибки кроются в самой концепции этих фильтров», – говорится в заявлении Neurocom. Пресс-секретарь Neurocom Рози Заур сообщила журналистам, что «компания Microsoft уже связалась с нами, признала ошибку и, видимо, уже исправляет её».

В июле 2000 года Интернет-червь «Stages» атаковал компьютеры Госдепартамента США. Электронное оборудование Госдепартамента США, задействованное в переговорах по вопросу урегулирования кризиса на Ближнем Востоке было подвергнуто заражению этим вирусом, который быстро распространился на компьютеры сотрудников и аккредитованных журнали-

стов. Компьютеры, используемые дипломатическим отделом Госдепартамента США, находились под воздействием вируса «Stages» все выходные, и он «спокойно рассылал себя» с помощью электронной почты. Вирус не разрушает файлы, однако, молниеносно размножается и нарушает работу почты заражённых серверов. Спикер Госдепартамента Джули Рисайд заявила, что государственные технические службы устранили вирус 17 июля. Однако компания iDefense, работающая в области электронной безопасности, сообщила, что, по её информации, вирус спокойно продолжал размножаться и 18 июля.

Информация в каком-то смысле, курьёзна. Оказывается, не только вредоносные компьютерные программы способны нарушать или блокировать работу компьютерных систем. Примеры? Пожалуйста.

Несовместимость выпущенной McAfee в ноябре 2000 года антивирусной программы со старым сканирующим программным обеспечением, используемым при проверке компьютера, вызывала сбой работы операционной системы Windows. Принято считать, что программы, сканирующие компьютер в поисках вируса – одно из наиболее эффективных средств в борьбе с ними. Однако Network Associates подтвердила, что в последней версии файла VirusScan компании McAfee (подразделение Network Associates) содержится дефект, который вызывает зависание операционной системы Windows при её запуске. Проблема заключается в несовместимости обновлённого программного обеспечения, предназначенного для лечения заражённых вирусом ресурсов, со сканирующим «движком» VirusScan. Пользователям, столкнувшимся с этой программной ошибкой, рекомендовалось перезагрузить Windows в режиме «Safe Mode» (режиме защиты от сбоев), убрать функцию автозапуска системы VirusScan и заново установить антивирусную программу в автозагрузку только после того, как будет выпущена исправленная версия программы-сканера.

Человеческий фактор? Программист, три часа ночи, строки и строки программного кода, а к утру надо обязательно закончить и отладить свой кусок программы…

Но, и сами пользователи не безгрешны. Как свидетельствуют результаты исследования, проведённого компанией IDC в феврале 2001 года, большинство пользователей ничему не научились и не сделали для себя никаких выводов даже после всемирной эпидемии Интернет-червя «I Love You», которая принесла с собой рекордный ущерб. Так вот, 37% Интернет-пользователей продолжали открывать сообщения с заголовком «I Love You». Более того, как заявил специалист антивирусной компании Message Labs Алекс Шип, на тот момент по данным этой компании большинство пользователей так и не установили патч, закрывающий «дыру», которую использовал печально известный вирус. Человеческий фактор? Несомненно. Но, в данном случае, это не только некомпетентность, но и, извините, разгильдяйство.

В конце декабря 2002 года информационным агентством Reuters со ссылкой на газету «China Daily» были опубликованы результаты опроса пользователей компьютеров, проведённого Национальным центром КНР по борьбе с компьютерными вирусами. Картина получилась удручающей. Китайские компьютеры практически не защищены от компьютерных вирусов и до 80% от их общего числа заражены ими. Опрос проводился в течение полутора месяцев, и лишь 16% его участников сообщили, что ни разу в течение года не страдали от компьютерных вирусов. Половина опрошенных сообщила о том, что вирусы привели к потере важных данных и возникновению сложностей с доступом в Интернет с их компьютеров. Причём, во время аналогичного опроса, проводившегося в 2001 году, около трети пользователей отмечали, что они вообще ни разу не сталкивались с вирусами.

Напомним, что на начало 2003 года в КНР насчитывалось 45 млн. пользователей Интернет и по сравнению с миллиардным населением страны, это не много, но по абсолютному числу пользователей Интернет Китай прочно удерживает позиции одного из лидеров. Поэтому столь широкая распростра-

нённость компьютерных вирусов, безусловно, является важной проблемой не только для КНР, но и для Глобальной сети в целом, так как её китайский сегмент весьма обширен, и плохое состояние дел в компьютерной безопасности сетей КНР не может не оказывать существенного влияния в мировых масштабах.

Ладно, пользователи. В ноябре 2001 года Computer Science Corporation провела исследование среди технических директоров ряда корпораций, которое выявило, что многие компании по-прежнему остаются уязвимыми для атак вирусов: у 46% компаний отсутствует официальная политика информационной безопасности, а в 68% компаний не проводится регулярный анализ степени защищённости и не отслеживается состояние систем безопасности. Опрашиваемым предлагалось выбрать наиболее важные для компании проблемы, и, в итоге, ликвидация уязвимостей и повышение информационной безопасности оказались только на пятом месте по важности. В связи с этим Computer Science Corporation делает далеко не оригинальный вывод о том, что компаниям необходимо выделять специальные подразделения, которые будут заниматься исключительно информационной безопасностью. В их задачи должна входить разработка планов по информационной безопасности, а также и регулярные проверки уровня защищённости компьютерных систем.

Интересно, а у Государственного департамента США тоже отсутствует официальная политика информационной безопасности или существует финансовый «голод»? 21 мая 2002 года Госдепартамент США признал факт наличия компьютерного вируса, который распространялся от его имени и заразил компьютеры многих СМИ и государственных учреждений. Вирус, о котором шла речь, является одной из версий вируса «Klez», который активно распространяется в Интернет через приложения к письмам электронной почты. Вирус не уничтожает файлы компьютера, однако вызывает сбои в работе почтовой системы и корпоративных локальных сетей. Тем не менее, примерно в течение двух суток сотни писем с данным вирусом были отправлены с обратным адресом PR-службы Госдепартамента США. По всей видимости,

вирус попал в компьютер, который обрабатывает письма Госдепартамента США, и таким образом получил доступ к используемому списку рассылки. После этого «Klez» рассылал себя, используя обратный адрес Госдепартамента США – такая уловка не нова и часто используется создателями вирусов, так как люди меньше доверяют посланиям, полученным от незнакомцев. В результате Госдепартамент США был вынужден разослать официальные извинения всем, кого затронула эта атака вируса. Но, остаётся вопрос, куда смотрели его системные администраторы и многочисленный персонал?

Иногда компьютерные вирусы представляют собой опасность даже для жизни, чести и достоинства человека. Судите сами.

Несколько лет назад был зафиксирован случай, когда компьютерный вирус стал причиной гибели пациента. В одной из больниц Нидерландов пациент получил смертельную дозу анестезии по той причине, что компьютер был поражён вирусом и выдавал медицинскому персоналу ошибочную информацию.

В январе 1991 года Д. Бэрилек из Мельбурна (Австралия), ранее осуждённый за инфицирование вирусом компьютерной системы, был полностью оправдан вышестоящим судом. Как заявил судья, процесс носил явно тенденциозный характер, поскольку не была рассмотрена иная трактовка событий мая 1989 года в Свинбурнском колледже. Обвинение утверждало, что обучавшийся в аспирантуре этого колледжа 32-летний Бэрилек выполнял подозрительные действия на компьютерных терминалах центра, которые сразу после этого оказались инфицированными вирусом. По заявлению одного из сотрудников колледжа, полиция арестовала подозреваемого, а суд признал его виновным в незаконном доступе к компьютеру, повлекшему заражение вирусом. Бэрилек заявил протест, и вышестоящий суд Мельбурна полностью оправдал его, потребовав компенсации ущерба, нанесённого Бэрилеку незаконными действиями полиции. Судья подверг сомнению показания свидетелей, имевших личную неприязнь к подозреваемому, и заявил, что даже если Бэрилек и инфицировал компьютеры, то это произошло помимо его воли.

Компенсация компенсацией, но к тому времени после вынесения обвинительного приговора судом первой инстанции, от Бэрилека ушла жена, он потерял работу и не смог найти новую, поскольку в области программирования карьера человека, осуждённого по обвинениям подобного рода, обычно бывает полностью разрушена. Вряд ли компенсация восполнит причинённый этому человеку ущерб.

В декабре 2000 года кто-то поместил на сайте CNN.com «новость», в которой сообщалось о покушении на жизнь барабанщика известной группы «Metallica» Ларса Ульриха (напомним, что Ульрих был первым музыкантом, предъявившим претензии к системе электронного обмена музыкальными файлами, назвав её пиратской). Так вот, согласно этой информации, один из фанатов Napster подойдя к жертве, произнёс: «Ты, убил Napster», – и музыкант, якобы, чудом остался в живых после того, как затем в него были выпущены две пули. Далее сообщалось, что преступление произошло в городе Остин (штат Техас, США). На самом деле все эти события не имели места в реальной жизни, но позднее Ульрих «удостоился» оскорбительных и угрожающих действий публики, когда появился на церемонии MTV Video Music Awards 2000. На наш взгляд, подобные действия вирусописателя очень похожи на провокацию, рассчитанную на неуравновешенность психики кого-либо из фанатов. Вспомните, пожалуйста, трагичную историю с Джоном Ленноном.

В мае 2001 года компьютерный вирус, поразивший электронную почту Канады, препятствовал широкомасштабной онлайновой кампании по поиску пропавшей пятилетней девочки. Все началось с того, что Адам Тетро отправил своим друзьям массовое электронное послание, содержащее информацию о Джессике Купмэнс, которая была похищена. В ответ на своё послание он получил несколько ответов, содержащих опасный вирус, который, являясь типичной разновидностью распространяемого с электронной почтой Интернет-червя, содержал информацию о девочке, а также приложение с просьбой получить более подробную информацию по этому вопросу. После открытия

вирус «прописывался» в адресной книге, рассылался каждому, чей электронный адрес она содержала, а затем портил файлы. Матери Джессики оставалось только сетовать на то, что поиску её дочери пытаются таким образом помешать, вместо того чтобы сделать что-либо полезное.

В августе 2003 года, как только было доказано, что он стал жертвой пробравшейся на его компьютер троянской программы, с британца Джулиана Грина были сняты все обвинения в распространении и хранении детской порнографии.

В октябре 2002 года Грина арестовала полиция. После ареста он провел ночь в полицейском участке, девять дней в тюрьме и несколько месяцев на свободе, после того как был отпущен до суда под залог. За этот период бывшая жена британца выиграла судебное разбирательство по вопросу прав на их дом и семилетнюю дочь.

Это уже второй случай в Англии, когда в суде для снятия обвинений «используется» троянская программа. Аналогичное разбирательство имело место в апреле 2003 года, когда было доказано, что троянский конь может быть задействован злоумышленником для получения свободного доступа к компьютеру жертвы, и, получив доступ, этот злоумышленник может использовать компьютер жертвы для хранения своих файлов, посещения нелегальных Web-страниц или организации DoS атак. По словам Кевина Хогана, старшего менеджера специализирующейся в области компьютерной безопасности компании Symantec Security Response, троянские программы могут маскироваться под игры, картинки, файлы и папки MS Windows. «Троян вполне может превратить чей-то компьютер в прокси-сервер. Вы просто видите папку на своем мониторе, щёлкаете и запускаете вредоносную программу». По словам самого пострадавшего, Грина, он так и сделал, после чего его жизнь была полностью разрушена, так как все смотрели на него, как на извращённого полового демона. «В подобных случаях одной презумпции невиновности недостаточно», – сообщил Грин. Заодно он заявил, что намеревает-

ся предъявить иск Скотланд-Ярду и потребовать компенсацию за моральный ущерб.

§4. Работа над ошибками: причины живучести вредоносных программ и их успешного распространения

В чём причина их «живучести»?

Сегодня вроде бы уже никого не надо убеждать в необходимости построения антивирусной защиты любой более или менее «серьёзной» информационной системы. Но, как говорилось выше, несмотря на усилия конкурирующих между собой фирм-производителей антивирусного программного обеспечения, убытки, приносимые компьютерными вирусами, не падают и достигают ежегодно астрономических величин в миллиарды долларов. Причём, можно с уверенностью сказать, что эти оценки действительно явно занижены, поскольку известно становится лишь о небольшой части подобных инцидентов. Тем не менее, отношение к антивирусной защите во многом остается прохладным и формальным. Например, сотрудники издания Consumer Report в ходе проведённого среди своих подписчиков опроса в мае 2002 года сделали вывод о том, что в США владельцы домашних компьютеров уделяют недостаточное внимание защите от атак вирусов. Оказалось, что свыше 60% опрошенных обнаруживали в своих персональных компьютеров 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 в отчёте отмечалось, что при использовании антивирусных программ информационный ущерб вирусы наносили лишь в 7% случаев, тогда как без них ущерб проявлялся на каждом третьем компьютере, а главным источником вирусов является, безусловно, Интернет. При этом доля заражений по электронной почте достигала 62%, а в 13% случаев вирусы несли в себе файлы, загружаемые из Интернет.

Сейчас вряд ли встретишь организацию, в информационной сети которой не установлены какие-либо антивирусные программы. Администратор сети с готовностью отчитается, что обеспечена защита рабочих мест, серве-

ров, электронной почты и т.д. Однако проблема заключается в том, что, несмотря на наличие антивирусного программного обеспечения, угроза атак вирусов по-прежнему актуальна. Это происходит по нескольким основным причинам, приведённым на рис. 5.

Рис.5. Основные причины угрозы атак компьютерных вирусов при наличии установленного антивирусного программного обеспечения

Кроме того, следует иметь в виду, что даже самые современные и продвинутые, «навороченные» антивирусные программы без других средств защиты информации[104], то есть применения «железа» – аппаратных средств

[104] Средства защиты информации – технические, криптографические, программные и другие устройства и продукты, предназначенные для защиты информации, устройств и продуктов, в которых они реализованы, а также устройства и продукты контроля эффективности защиты информации.

защиты[105], технических мер защиты информации, организационных мер защиты информации, правовых мер защиты информации, то есть внедрения современных систем защиты информации[106] – не дают полной гарантии защиты от компьютерных вирусов и атак в информационных сетях.

Как обычные пользователи, так и профессионалы-программисты зачастую не имеют нужных навыков «самообороны», а их представления о компьютерных вирусах порой являются поверхностными. В условиях, когда компьютерные системы становятся основой бизнеса, а базы данных – главным капиталом многих компаний, создание современной антивирусной защиты прочно встает в один ряд с вопросами общей экономической безопасности организации. Особенно эта проблема актуальна для банков, которые, по сути дела, являются хранителями весьма конфиденциальной информации о клиентах, и бизнес которых построен на непрерывной обработке электронных данных. Кража, уничтожение, искажение информации, сбой и отказ компьютерных систем – вот те проблемы, которые неизбежно несут с собой компьютерные вирусы.

Согласно многочисленным специальным исследованиям, проведённым в 2001–2003 годах, пользователи несмотря ни на что продолжают открывать сомнительные электронные письма. Результаты исследований со всей очевидностью свидетельствуют, что эпидемии, вызванные компьютерными вирусами и охватившие весь мир, похоже, ничему не научили доверчивых пользователей. Исследование IDC, в частности, показало, что 14 февраля на день Святого Валентина в Великобритании «любовные письма», прибывающие вместе с деловой почтой, откроют не менее 37% пользователей. Было также выявлено следующее: пользователи в любой день года откроют электронную почту от кого-то, кого они знают, если тема сообщения будет сле-

[105] Аппаратные средства защиты – механические, электромеханические, электронные, оптические, лазерные, радио, радиотехнические, и другие устройства, системы и сооружения, предназначенные для защиты информации от несанкционированного доступа, копирования, кражи, модификации или разрушения.

[106] Система защиты информации – совокупность (комплекс) специальных мер правового (законодательного) и административного характера, организационных мероприятий, физических и технических (программных и аппаратных) средств защиты, а также специального персонала, предназначенных для обеспечения безопасности автоматизированных систем (циркулирующей в автоматизированных системах информации).

дующей: «классная шутка» (54%); «посмотри на это» (50%); «Re: Message» (46%); «без заголовка» (40%); «специальное предложение» (39%).

Едва успели в США в июне 2001 года привести в исполнение казнь Тимоти Маквея, террориста, подложившего бомбу в Оклахома-Сити, взрыв которой унёс жизни 168 человек, как в Интернет появилось видео, якобы демонстрирующее все детали этой казни. Те, кого нездоровое любопытство побудило скачать и установить на свой компьютер это «видео», на самом деле установили опасную, но давно известную под именем «Backdoor.Subseven» троянскую программу, позволяющую удалённо контролировать инфицированные компьютеры фактически на уровне системного администратора. Несмотря на то, что для современного антивирусного программного обеспечения не составляет большого труда обнаружить и уничтожить этого троянского коня и его модификации, а в интересах пользователя регулярно обновлять антивирусные базы и не скачивать из Интернет подозрительные файлы.

В июне того же 2001 года новый Интернет-червь, получивший название «DoS.Storm», избрал своей жертвой Web и почтовые серверы под управлением программного обеспечения корпорации Microsoft. Используя слабые места этих серверов, вирус забрасывал их письмами, в качестве обратного адреса которых значилось: gates@microsoft.com. Но спам вряд ли причиняет какое-либо заметное неудобство лично главе Microsoft Биллу Гейтсу, поскольку отправляемые на этот адрес письма возвращаются обратно. Однако вся эта активность оборачивается DoS-атакой на серверы Microsoft и вредит стабильной работе сетей компаний-партнёров корпорации, IIS Web-серверы которых в конечном итоге и страдают. А ведь могло бы ровным счётом ничего и не произойти, так как вредоносный код под довольно красивым названием «DoS.Storm» использует хорошо известные слабые места серверов под управлением программного обеспечения корпорации Microsoft, патчи для которых она выпустила ещё в августе 2000 года. И вот загадка: почему далеко не все системные администраторы позаботились об их установке в течение практически целого года?

«Уж сколько раз твердили миру…», – как говаривал дедушка Крылов.

В общем случае распространение компьютерных вирусов, конечно же, выгодно не самим программистам, так как они практически всегда остаются анонимными. Подобное явление можно сравнить скорее с вандализмом. Программисты вирусов занимаются этим делом не ради денег, это скорее хобби, своего рода вызов. Вместе с тем, наверняка некоторые из них зарабатывают на жизнь написанием вредоносных компьютерных программ, но они также получают и удовольствие, если смогут нарушить функционирование компьютера или организации. У них нет чувства ответственности и, плюс к тому, сейчас не требуется очень большого опыта, чтобы написать компьютерный вирус, его может разработать каждый программист, у которого есть персональный компьютер и свободное время. И, если вирус написан эффективно, то с уверенностью можно сказать, что он получит распространение. Программист, который обладает некоторым кругозором и знаниями ассемблера, а также хотя бы минимально разбирается в устройстве компьютерной техники, может написать даже достаточно сложный вирус. Например, в США издана «Малая чёрная книга компьютерных вирусов», которая содержит подробные инструкции, как писать вирусы. Любой среднего уровня программист может прочесть эту книгу, сконструировать достаточно «качественный» компьютерный вирус, а чтобы запустить вирус в обращение, нужно всего лишь занести его в компьютер, который используется другими. Сейчас существуют фирмы, которые сдают компьютеры на время, и каждый желающий может зайти в такую фирму, часок поработать на компьютере и оставить там своё творение. Те же, кто будет работать на этом компьютере потом, унёсет с собой инфицированные носители информации, так как при постоянной смене пользователей нереально всякий раз тщательно проверять компьютер на наличие вирусов.

Известно и то, насколько быстро компьютерные вирусы могут распространяться без всякого управляющего воздействия посредством коммуникационных линий. Этот процесс похож на грипп, иногда случаются настоящие

эпидемии, и ими никто специально не управляет. Таковы практически все инфекционные болезни, и компьютерные вирусы здесь не исключение. Зачастую распространению вирусов способствует и простота операционной системы, например, MS-DOS, и, в частности, отсутствие в ней защиты по паролю. Может быть, стоит снабдить операционные системы лучшей защитой против компьютерных вирусов, и вопрос закрыт? Но выполнимо ли это программными средствами? Операционные системы, обладающие недостаточной антивирусной защитой, используют сотни миллионов людей по всему миру, и чтобы затруднить проникновение вирусных инфекций, нужно внести в их программный код достаточно серьёзные изменения. Но тогда все многочисленные пользователи этих операционных систем окажутся лицом к лицу с другой средой. Таким образом, эту задачу очень трудно осуществить на практике, если не принять во внимание возможность более широкого применения аппаратных средств защиты компьютерной техники от вирусов, так как эти средства не требуют изменения ни самой среды, ни прикладного программного обеспечения, ни больших финансовых затрат.

* * *

Как вы полагаете, в перспективе общая ситуация с компьютерными вирусами станет лучше или хуже? Можно спросить и по-другому: кто победит в состязании – разработчики антивирусных средств или вирусописатели всех окрасок? Нам кажется, что они где-то уравновесят друг друга.

Разработка антивирусных средств обычно отстаёт, так как никто точно не знает, что именно предпринимают в данный момент программисты вирусов. Правда, мы можем предвосхитить многие их действия, но не во всех случаях. Если обратиться к статистике, то она обнадеживающе свидетельствует о том, что вирусы не разрабатываются в тиши и не распространяются потом сразу по всему миру. Проходит много месяцев, прежде чем какой-нибудь вирус вырастает в значительную угрозу в глобальном масштабе. К

этому моменту антивирусное сообщество успевает разработать противоядие, так что, в общем, и целом «электронный мир» остается защищённым.

Борьба с компьютерными вирусами является схваткой разумов, то есть, в общем случае, борьбой далеко не последних умов, поскольку сложные и не очень задачи, стоящие перед вирусологами, разработчиками антивирусных аппаратно-программных средств, ставят такие же, иногда незаурядные, своего рода выдающиеся личности – вирусописатели, программисты вирусов. Последние постоянно придумывают всё новые и новые, всё более и более изощрённые компьютерные вирусы, а противоположная сторона ведёт с ними перманентную борьбу. Наконец, вирусописатель придумывает компьютерный вирус, который обнаружить и надёжно нейтрализовать его зловредную деятельность крайне тяжело, но и с ним, пусть и не мгновенно, справляются. В настоящее время буквально каждые несколько секунд со «стапелей» вирусописателей сходит очередная вредоносная программа, следовательно, в данное мгновенье кто-то, пока неизвестный миру, заканчивает ваять своё произведение и вот-вот выпустит его в свет. И кто сказал, что этот компьютерный вирус не будет вирусом следующего поколения и не приведёт в трепет всё компьютерное сообщество, не будет тысячами «валить» серверы, наносить астрономический ущерб и покушаться, например, на целостность Глобальной сети? И вновь, разработчики антивирусных аппаратно-программных средств будут биться над этим и другими творениями до полной победы, но обязательно найдут на них управу, и будут ждать, задавая себе сакраментальный вопрос всех времён и народов: «Что день грядущий нам готовит?» Таким образом, появление компьютерных вирусов – один из наиболее интересных и, вместе с тем, весьма противоречивых моментов в истории технического прогресса двадцатого столетия.

Спасибо тем, кто прочитал эту, надеемся познавательную, главу, и приглашаем читателя следовать за нами дальше.

Часть 2

Летопись компьютерных преступлений – XX век

§1. Повторение – мать учения

Естественно, мы не собираемся в данном параграфе заново повторять всё или хотя бы большую часть содержания предыдущих глав. Однако считаем вполне оправданным, перед тем как взяться за дальнейшее изложение, в крайне сжатом виде пояснить некоторые понятия, которые подготовят читателя (особенно, не знакомого с рассматриваемой тематикой) к правильному восприятию последующего материала настоящей книги.

Вредоносные компьютерные программы порой сеют ужас и панику не только в среде обычных пользователей, но и, начиная с последних десятилетий прошлого века, заставляют «вздрагивать» при упоминании имён отдельных наиболее «прославленных» их представителей владельцев и специалистов крупных компьютерных систем и сетей. В течение последней четверти века эти программы прошли путь от чисто теоретической, оторванной от реальной жизни «достопримечательности» до насущно и постоянно стоящей перед всем мировым сообществом проблемы. В настоящее время вредоносные компьютерные программы могут писаться «для» и распространяться «на» любой виртуальной платформе. Однако по результатам исследования множества зарегистрированных и проанализированных крупномасштабных сетевых инцидентов[1] вполне очевидно, что наиболее тесно эта проблема связана с появлением микрокомпьютеров.

---

[1] Spafford, E. H. 1989. «The Internet worm program: an analysis». Computer Comm. Review 19, 1.

Cliff Stoll, «An epidemiology of viruses and network worms», 12th National Computer Security Conference, 1989.

M.W. Eichin and J.A. Rochlis, «With microscope and tweezers: An analysis of the Internet virus of November 1988», Proc. 1989 IEEE Symp. on Security and Privacy, Oakland, California, May 1–3, 1989.

Вредоносные компьютерные программы обживали, привнося с собой всемирную «головную боль», каждую без исключения популярную микропроцессорную платформу. Они как будто изначально были «задуманы» кем-то в виде трудноразрешимой задачи из-за их скрытности и способности к проведению целенаправленных атак против компьютерных систем[2]. Тем не менее, как мы уже указывали в предыдущем томе настоящей книги, представление многих рядовых пользователей о вредоносных компьютерных программах до сих пор ограничивается лишь не вполне осознанным ощущением угрозы и практической неизбежности её осуществления – не сегодня, так завтра.

Такому фатализму можно и нужно противопоставить хорошее знание предмета и «характера» своего противника.

Что же такое компьютерный вирус? Ранее мы уже выяснили, что наиболее лёгким для понимания сущности компьютерных вирусов[3] является их сравнение с биологическими вирусами, которые попадают в наш организм и делают нас больными. Эти микроорганизмы порождают сами себя в клет-

---

D. Seeley, «A tour of the worm», Proc. Usenix Winter 1989 Conference, San Diego, California, 1989.

[2] Fred Cohen, «Computer viruses, theory and experiments», Computers & Security, vol. 6, 1987.

[3] Компьютерный вирус (computer virus) – вредоносная программа, способная создавать свои копии (не обязательно полностью совпадающие с оригиналом) и внедрять их в различные объекты или ресурсы компьютерных систем, сетей и так далее без ведома пользователя. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус может проникать в информационные или компьютерные системы пользователя при помощи самых различных путей (способов, методов, технологий) и вызывать всевозможные последствия в широком диапазоне: от простого надоедливого напоминания о своём присутствии до чрезвычайно деструктивных (разрушительных) действий и нанесения непоправимого ущерба, например, полного уничтожения файлов.

На сегодняшний день известно шесть основных типов вирусов: файловые, загрузочные, полиморфные (призраки), невидимки, скрипт и макро вирусы.

ках-хозяевах человеческого тела и подменяют клеточную информацию таким образом, что эти клетки начинают сами воспроизводить вирусы.

Достаточно подробно мы рассмотрели и механизмы распространения компьютерных вирусов, латентный период их существования и активную фазу жизнедеятельности, которая зачастую заканчивается масштабной эпидемией. Установили, что потенциальная способность компьютерных вирусов к свободному перемещению во времени и пространстве от пользователя к пользователю в компьютерных системах означает, что атаки могут поражать и те части систем, которые считаются наиболее защищёнными. Усугубляется это тем, что в предыдущие несколько лет всё большая часть вредоносных компьютерных кодов писалась и «выпускалась» во внешнюю нерегулируемую среду и, таким образом, эти программы воздействовали на всю совокупность аппаратно-программного обеспечения. Если приплюсовать сюда также не утраченную способность к распространению среди индивидуальных компьютерных систем, то становится понятным большое беспокойство компьютерного и бизнес сообществ по поводу нарастания угрозы со стороны современных вредоносных компьютерных программ, написанных с использованием инновационных технологий и современных языков программирования.

Для исследователей компьютерные вирусы могут быть очень интересным предметом изучения: постоянно изменяясь, они требуют постоянного изменения и методов их обнаружения, методов их обнаружения, блокирования и последующего уничтожения. В отличие от исследователей для собственников и пользователей компьютерных систем компьютерные вирусы являются просто источником неприятностей, избавление от которого с наименьшими усилиями и потерями совершенно необходимая работа, которая должна быть выполнена для того, чтобы можно было нормально использовать компьютер в дальнейшем. И мы попытаемся оказать помощь пользователям компьютеров в оценке угроз, исходящих от вирусов вообще и, в частности, в понимании того, что наиболее распространённые сегодня компьютерные вирусы могут делать в действительности.

Как уже подчёркивалось, по существу компьютерные вирусы могут быть написаны под любую операционную систему, используемую универсальными вычислительными машинами. Компьютерные вирусы существуют также и для каждой общеизвестной платформы микропроцессорных электронно-вычислительных машин. В среде MS-DOS, например, программы, которые могут заражаться одним из общеизвестных вирусов, включают в себя стандартные исполняемые файлы с расширениями «*.exe» и «*.com», а также оверлейные коды[4] и различные типы загрузочных секторов.[5] Вместе с тем, даже сегодня, инфицирование компьютера новым вирусом достаточно неординарное событие и большинство заражений компьютерными вирусами, которые случаются в реальной жизни, являются следствием деятельности одного из нескольких десятков наиболее распространённых на тот момент вирусов. Для каждого из числа наиболее известных компьютерных вирусов мы постараемся дать его краткое описание, охарактеризовать основное воздействие на компьютерную систему, пути распространения с машины на машину, «симптомы», причиной появления которых он может служить, привести величину причинённого ущерба (если он действительно существует и подсчитан).

В то время как в теории компьютерных вирусов нет даже их единого определения, на практике защита от наиболее распространённых вирусов реализуется относительно просто. Некоторые характеристики у большинства известных вирусов во многом схожи, что облегчает задачу их выявления и уничтожения посредством применения различных средств, например, имеющихся в продаже коммерческих антивирусных программ, которые способны

---

[4] Оверлейный код (code overlay, англ.) – фрагмент компьютерной программы, хранящийся на внешнем запоминающем устройстве и загружаемый в память по мере необходимости. Оверлейная технология применялась в системах без виртуальной памяти.

[5] Загрузочный сектор (boot sector, англ.) – представляет собой небольшой кусочек программного кода на флоппи-диске или «жёстком» диске, который указывает компьютеру, что нужно делать, пока не загрузилась операционная система.

защитить компьютер пользователя от известных компьютерных вирусов. Однако обеспечить доступными средствами защиты безопасность целой организации – более трудная задача, чем найти метод защиты от вирусов, например, для отдельно взятой электронно-вычислительной машины.

С тех пор как был «отловлен» и зарегистрирован в середине 80-х годов первый компьютерный вирус для микро ЭВМ[6], они распространились по всему миру. Названная дата конечно условна, так как не учитывает более ранние вирусы, которые, как мы увидим, уже существовали в то время, но еще не были столь разрушительны по своим последствиям. Например, одного из рекордных результатов за всё время существования компьютерных вирусов добился «I Love You!», который в 2000 году нанёс ущерб, оцениваемый примерно в 8 млрд. долл.

Кстати, напомним, что основными симптомами поражения компьютерной системы вирусом является: замедление работы некоторых программ, увеличение размеров файлов (особенно выполняемых), появление не существовавших ранее подозрительных файлов, уменьшение объёма доступной оперативной памяти (по сравнению с обычным режимом работы), внезапно возникающие разнообразные видео и звуковые эффекты. При всех перечисленных выше симптомах, а также при других странных проявлениях в работе системы (неустойчивая работа, частые самостоятельные перезагрузки и прочее) мы настоятельно рекомендуем немедленно произвести её проверку на наличие компьютерных вирусов.

Но не только компьютерные вирусы представляют собой угрозу для системы пользователя. Следует помнить, что существуют такие разновидно-

---

[6] Dr. Harold Joseph Highland, «The BRAIN virus: fact and fantasy», *Computers & Security*, vol. 7, 1988.

Anne E. Webster. «University of Delaware and the Pakistani computer virus», Computers & Security, vol. 8, 1989.

сти вредоносных программ как компьютерные «черви»[7], которые появились в развитие собственно вирусов. Например, обнаруженный в ноябре 1988 года сетевой червь[8] в течение нескольких часов инфицировал тысячи компьютеров, вызвав, в итоге, весьма солидные потери в сфере услуг и затрату большого количества времени на искоренение его из компьютерных систем; в 2003 году вовсю бесчинствовал «червь» «Blaster», который в кратчайшие сроки поразил более миллиона компьютеров по всему миру. Подобные примеры можно приводить и приводить.

Нельзя также забывать о «троянских» программах[9], называемых также «троянскими конями»[10]. Хотя «троянский конь» и не наносит непосредствен-

---

[7] Компьютерный «червь» (worm) – программа, подобная компьютерному вирусу, но её отличие состоит в том, что ей не обязательно инфицировать другие файлы для своего размножения. Компьютерные «черви» воспроизводят (тиражируют) собственные копии (либо вырабатывают копии своих отдельных частей), проникают в компьютеры через сети и распространяются при помощи сетей, заставляя программы рассылки электронной почты отправлять письма, содержащие вирус, по имеющимся в базе адресам.

M.W. Eichin and J.A. Rochlis, «With microscope and tweezers: An analysis of the Internet virus of November 1988», Proc. 1989 IEEE Symp. on Security and Privacy, Oakland, California, May 1–3, 1989.

Fred Cohen, A Formal Definition of Computer Worms and Some Related Results, IFIP-TC11 Computers and Security V11#7, November 1992, pp 641-652.

D. Seeley, «A tour of the worm», Proc. Usenix Winter 1989 Conference, San Diego, California, 1989.

E. Spafford, «The Internet worm program: an analysis», Computer Comm. Review, vol. 19, 1989.

Vesselin Bontchev, Methodology of Computer Anti-Virus Research, Doctoral Thesis, University of Hamburg, 1998.

Sophos Data Security Reference Guide 1999/2000, Sophos Plc, 1999.

[8] Cliff Stoll, «An epidemiology of viruses and network worms», 12th National Computer Security Conference, 1989.

[9] Троянская программа (Trojan program) – строго говоря, так называемые «троянские программы» не являются собственно компьютерными вирусами, хотя, чаще всего, если нет на

ного вреда компьютеру, проникнув в систему, он позволяет компьютерным злоумышленникам получать доступ к имеющейся в нём информации, базам данных, перехватить управление компьютером и пр. Например, использовав в 2002 году «троянского коня» под названием «Qaz», электронные взломщики получили доступ к секретным программным кодам компании Microsoft. К «троянским коням», можно также добавить «бэкдор» программы[11], которые способны проникать в компьютер пользователя и, затем, скрытно действовать. Эти, сами по себе, сравнительно «безвредные» программы, проникнув в компьютер, пытаются воровать пароли[12], а также перехватывать нажатия пользователем клавиш и их сочетаний, давая возможность удалённого доступа к охраняемой информации и т. п.

Между прочим, некоторые современные компьютерные вирусы сочетают в себе все качества перечисленных программ. К примеру, таким был создан вирус «Sobig», который в августе 2003 года инфицировал примерно треть всех писем, распространявшихся в мире по электронной почте.

то особой необходимости, их фактически не разделяют. В действительности эти программы, проникая в компьютеры, не проявляют себя в качестве разрушительных программ – хотя могут вызывать деструктивные действия в системе пользователя, но, установив себя, осуществляют действия, которые сказываются на уровне конфиденциальности пользовательской информации.

[10] Ian Whalley, Testing Times for Trojans, Poceedings of the Ninth International Virus Bulletin Conference, September/October 1999.

[11] «Бэкдор» программа (Backdoor program) – это компьютерная программа, которая проникает в компьютер и создаёт так называемый «чёрный ход», через который может осуществляться контроль над инфицированной компьютерной системой без уведомления законного пользователя.

[12] Пароль (password) – заданная последовательность символов, используемая для ограничения доступа к некоторым файлам, компьютерным программам или другим областям компьютерной системы таким образом, что только тот, кто знает эту последовательность, может использовать указанную систему.

В целом ещё несколько лет тому назад именно компьютерные вирусы являлись главной угрозой компьютерным системам, так как, размножаясь и заражая другие файлы, или прикладные программы они, тем самым, причиняли серьёзный ущерб пользователю. Однако, в последнее время, вследствие широкого использования современной вычислительной техники и Глобальной сети, возникли и другие угрозы, которые могут отличаться в высшей степени разрушительным характером, что заставило пересмотреть концепцию угрозы и доопределить её пересмотренным понятием: «вредоносные компьютерные программы».[13]

Во всём мире вредоносные компьютерные программы либо заведомо написаны со злым умыслом (подавляющее большинство), либо обязаны своим рождением некачественно написанному программному обеспечению, привнесённым ошибкам программистов и пр. Таким образом, можно сказать, что вредоносные компьютерные программы – это любые программы, электронные документы (в том числе и файлы: текстовые, электронные таблицы, графические, сообщения электронной почты), которые могут служить причиной нанесения вреда, ущерба, повреждения, порчи, отказа или сбоя компьютерных систем и, как следствие, привести к потере данных, а также снижению производительности и надёжности вычислительной техники. Следовательно, сегодня в число вредоносных компьютерных программ, наряду с

---

[13] Вредоносная компьютерная программа (malicious software, malware) – этот термин используется по отношению ко всем компьютерным программам, которые содержат вредный код: собственно компьютерные вирусы, «троянские» программы, компьютерные «черви» и т.п.

Вредный код (malicious code, virus code) – фрагмент кода компьютерной программы, написанный на каком-либо языке программирования и порождающий инфицированные файлы, которые могут пересылаться в другие компьютерные системы с целью их выполнения или расшифровывания информации. Язык программирования (programming language) – набор инструкций, директив, команд и правил, которые используются для создания компьютерных программ.

собственно компьютерными вирусами, компьютерными «червями», «троянскими» и «бэкдор» программами вполне правомерно включить и ряд других.

Номеронабиратель (dialer) – программа, которая пытается установить телефонное соединение с определённым номером. Данная программа использует приём злонамеренной переадресации Интернет-соединений. В этом случае отключается законное телефонное соединение для того, чтобы использовать его для подключения к Интернет абонента-злоумышленника. Часто для пользователя первым признаком такого подключения к его номеру может послужить резкое повышение сумм к оплате, которые предъявляет ему соответствующий оператор связи.

Программа слежения (spy program) – программа (употребляется также профессиональный термин – программа-шпион), которая обычно собирает данные о пользователях Интернет и, затем, отсылает их в компании, занимающиеся рекламой. Эти программы автоматически устанавливаются на компьютер пользователя (чаще всего без разрешения самого пользователя и, даже, без его уведомления) вместе с другими программами, которые предназначены для сбора персональных данных (сведения о доступе в Интернет, деятельности, осуществляемой во время просмотра какой-либо информации и посещения Web-страниц, установленных на компьютере программах и т. п.). Если собранная программой слежения информация затем будет предана огласке, конфиденциальность персональных данных может быть нарушена.

Программы, угрожающие безопасности (security risk utilities) – вполне законные утилиты (сервисные программы), которые могут использоваться компьютерными преступниками для осуществления своих злонамеренных действий. Примером, могут служить программы для создания компьютерных вирусов или «троянских» программ.

Инструмент электронного взлома (hacking tool) – инструментарий, который предоставляет электронным взломщикам возможности по нанесению ущерба атакуемым компьютерам. Данный тип программ может быть использован компьютерным преступником для осуществления действий, кото-

рые послужат причиной проблем для пользователя компьютера-«жертвы» электронного нападения (предоставление злоумышленнику контроля над поражённым компьютером, кража конфиденциальной информации, сканирование коммуникационных портов[14] и т. п.).

Уязвимость (vulnerability) – ошибка в компьютерной программе, которая может быть использована для преодоления системы безопасности и установления контроля над компьютерами пользователей. Иными словами, под уязвимостями принято понимать дефекты или бреши в компьютерной программе или информационной системе, которые, кроме всего прочего, часто используются компьютерными вирусами как способ инфицирования вычислительной техники;

«Шутка» (joke) – безвредная программа, которая симулирует осуществление каких-либо действий с целью нанесения ущерба компьютеру пользователя. Подобные программы не являются компьютерными вирусами, но пользуются различными приёмами и ухищрениями (зачастую, психологического порядка), чтобы заставить пользователя поверить в то, что его компьютер инфицирован настоящим компьютерным вирусом.

Мистификация (hoax) – поступающее по электронной почте ложное сообщение, которое предупреждает пользователя о несуществующих компьютерных вирусах. Отсутствие мощных антивирусных средств, а также недостаток проверенной информации на данную тему способствовало появлению большого количества заведомо ложных сообщений об угрозе якобы очень опасных вирусов, которые на самом деле не существовали[15]. Первой компь-

---

[14] Порт/коммуникационный порт (port/communication port**) –** точка системы, через которую компьютер передаёт информацию (поступающую/отправляемую) посредством протокола TCP/IP.

Протокол TCP/IP (IP (Internet Protocol)/TCP-IP**)** – IP-адрес представляет собой код для идентификации каждого компьютера; протокол TCP/IP это система, применяемая в Интернет для взаимосвязи компьютеров и предотвращения конфликтов адресов.

[15] Сами по себе компьютерные мистификации компьютерными вирусами не являются.

ютерной мистификацией признано сообщение о вирусе (1988 год), который будто бы передаётся от модема к модему и использует для этого скорость 2400 бод.[16] В результате многие пользователи снизили скорость соединения своих модемов до 1200 бод.

Спам (spam) – массовая рассылка не затребованной электронной почты, которая в большинстве случаев представляет собой сообщения коммерческого характера, рекламные объявления и т. п. Подобные электронные сообщения могут носить крайне надоедливый характер и приводить к ненужному расходованию времени и различных ресурсов компьютерной системы.

В настоящее время все перечисленные выше типы вредоносных компьютерных программ широко распространены и свободно перемещаются посредством информационных сетей.

Так что же объединяет вредоносные компьютерные программы, кроме аналогии с биологическими вирусами? Ко всем компьютерным программам этого класса и, в частности, к компьютерным вирусам, применим один и тот же базовый принцип возможности их существования и активной деятельности:

загрузочные вирусы, которые обычно инфицируют главную загрузочную запись[17] «жёстких» дисков или загрузочную запись флоппи-дисков *действуют до тех пор, пока компьютерный вирус не обнаружен и не нейтрализован антивирусными средствами*;

файловые вирусы, которые могут атаковать в компьютерной системе ключевые файлы и модифицировать их, изменяя длину (объём) исполняемых

---

[16] Baud (англ.) – бод это единица скорости передачи сигнала, измеряемая числом дискретных переходов или событий в секунду.

[17] Главная загрузочная запись (master boot record, MBR) – очень важная служебная область на «жёстком диске», содержащая структуру данных, которая запускает процесс загрузки компьютерной системы. Главная загрузочная запись содержит всю информацию, необходимую для запуска стандартных программ, и может быть модифицирована компьютерным вирусом.

файлов (файлов с расширением «.exe», «.com») *действуют до тех пор, пока компьютерный вирус не обнаружен и не нейтрализован антивирусными средствами;*

другие типы компьютерных вирусов, например, макро-вирусы, которые состоят из последовательности макро команд, стремятся внедриться в шаблоны документов, и таким путём быстро инфицировать все документы, основывающиеся на данном шаблоне опять таки, *действуют лишь до тех пор, пока компьютерный вирус не обнаружен и не нейтрализован антивирусными средствами*.

Итак, этот принцип справедлив в отношении всех без исключения вредоносных компьютерных программ. Следовательно, не зависимо от времени и места действия во главу угла искоренения компьютерной заразы можно поставить интенсификацию борьбы с ней современными средствами защиты компьютерных систем.

Многие вредоносные компьютерные программы имеют в дополнение к репродуктивной компоненте программную компоненту, которая инициирует действия в соответствии с определёнными критериями, например, некой датой, каким-либо днём недели, особой комбинацией при вводе данных с клавиатуры компьютера и так далее. Часто такие программы остаются незамеченными до тех пор, пока критерий присоединённой процедуры не будет выполнен и компьютерный злоумышленник не начнёт выполнение действий, которые могут быть сравнительно безвредными и даже забавными, а могут носить разрушительный характер для компьютерной системы пользователя. Например, Вы можете увидеть двигающийся на «всех парах» через экран монитора автомобиль скорой помощи или обнаружить, что символы на экране плавно осыпаются подобно осенним листьям или столкнуться с сообщением типа «Donald Duck is a lie!». В других случаях, файлы могут быть безвозвратно утеряны или данные на «жёстком диске» зашифрованы помимо Вашей воли. А это уже не так забавно, не так ли?

§2. Оценка серьёзности угрозы со стороны вредоносных компьютерных программ

По указанным выше причинам производители антивирусных средств на постоянной основе проводят оперативную оценку серьёзности угрозы со стороны вредоносных компьютерных программ компьютерным системам пользователей. В настоящее время большинство наиболее крупных зарубежных и отечественных фирм-производителей антивирусного программного обеспечения следует выработанной ими методологии при проведении оценки серьёзности угрозы вредоносных компьютерных программ (собственно компьютерных вирусов, компьютерных «червей» и «троянских» программ[18]). И хотя методики оценки имеют свои особенности и нюансы, в обобщённом виде характеристика серьёзности угрозы компьютерным системам со стороны конкретных вредоносных компьютерных программ обычно включает в себя как непосредственно оценку опасности, так и градацию угроз при помощи заранее определённых категорий риска для конечных пользователей вычислительной техники.

Рассмотрим, в качестве примера, два исповедуемых в настоящее время методологических подхода к оценке угрозы. Первый практикует корпорация Symantec (США)[19], а второй не менее известная компания Panda Software (Испания)[20].

---

[18] Подробно см. выше в настоящей книге.

[19] Корпорация Symantec основана в 1982 году. Декларируемой целью корпорации является всестороннее партнёрство в области информационной безопасности, как с частными, так и с юридическими лицами во всём мире. В настоящее время корпорация Symantec является одним из мировых лидеров в области технологий обеспечения безопасности в Интернет, производителем широкого спектра программных продуктов в области обеспечения безопасности корпоративных и частных сетей, прикладных решений для частных лиц, различных предприятий, организаций, государственных учреждений и поставщиков услуг. Штаб-квартира корпорации находится в г. Купертино (штат Калифорния, США), и свою деятельность она осуществляет в 38 странах по всему миру. Персонал составляет более 5000 человек, а годовой доход в 2003 году составлял порядка 1,5 млрд. долл. В составе

2.1. Методологический подход, принятый компанией Symantec

Данный методологический подход к оценке серьёзности угрозы вредоносных компьютерных программ компьютерным системам пользователя содержит основные параметры, которые анализируются с целью определения степени серьёзности угроз и их последующего ранжирования. Этими параметрами обычно являются:

персонала Symantec – специалисты-вирусологи, инженеры по безопасности компьютерных систем, программисты, а также технический персонал. Они осуществляют всестороннюю, круглосуточную поддержку и защиту своих клиентов от угроз электронных нападений. Корпорация Symantec имеет свои исследовательские центры и центры реагирования, размещённые в различных регионах мира: г. Сидней (Австралия), г. Калгари (Канада), г. Дублин (Ирландия), г. Токио (Япония), г. Дублин (Ирландия), г. Американ Форк (штат Юта, США), г. Санта Моника (штат Калифорния, США). В целом корпорация предоставляет свои услуги, программные продукты и технологические решения более чем 100 миллионам пользователей в мире.

[20] Компании Panda Software представляет собой динамично развивающегося разработчика антивирусного программного обеспечения с поддержкой на многих языках, успешно работающего в высоко конкурентном секторе научных исследований и разработок в области информационных технологий, где новые решения постоянно востребованы, так как регулярно меняется характер угроз безопасности компьютерных систем. Начиная со дня своего основания в 1990 году, Panda Software ставила своей целью стать мировым лидером в обеспечении антивирусной защиты пользователя и именно по этой причине из года в год реинвестирует высокий процент своей прибыли в научно-исследовательские и опытно-конструкторские работы. Такая политика постепенно выдвинула компанию в число технологически передовых разработчиков антивирусных средств, обладающих квалифицированным персоналом, способных предложить самые передовые решения по борьбе с компьютерными вирусами. В 2003 году Panda Software расширила область своей деятельности, выпустив на рынок новое семейство продуктов, которые предоставляют пользователю защиту от любых угроз со стороны всех видов вредоносных компьютерных программ. Штаб-квартиры компании Panda Software располагаются в г. Бильбао (Испания) и г. Глендэйл (штат Калифорния, США).

распространённость конкретной вредоносной компьютерной программы «в диком виде»;[21]

ущерб, который вредоносная компьютерная программа причиняет компьютерным системам пользователя в случае их инфицирования;

скорость, с которой распространяется вредоносная компьютерная программа.

Перечисленные параметры ранжируются, то есть каждому из них присваивается соответствующий уровень опасности, который оцениваются показателями: «Высокий», «Средний» или «Низкий».

Обобщённая оценка степени опасности, которая вытекает из различных комбинаций показателей по праметрам, относится к одной из пяти заранее установленных категорий: «Категория 1» представляет собой наименьшую опасность, а «Категория 5» – максимальную.

Таким образом, в соответствии с требованиями рассматриваемого нами методического подхода, первоначально в качестве отдельного этапа выделяется оценка каждого из параметров (Этап 1) – проводится их анализ по заданным критериям. Затем, на следующем этапе (Этап 2), формируются перечни комбинаций оценок параметров, которые и дают в результате обобщённую оценку степени опасности конкретной вредоносной компьютерной программы.

Давайте рассмотрим указанные этапы оценки более подробно.

Этап 1. Составляющие опасности

1.1 «Дикость»

Критерий «дикость» представляет собой оценку пределов, в которых компьютерный вирус распространился среди компьютерных систем пользователей. Для этого должны быть учтены:

количество автономных Web-сайтов, которые были инфицированы;

количество инфицированных компьютеров;

---

[21] См. Приложение.

географическая распространённость вредоносной компьютерной программы;

возможность противодействия возникшей угрозе при помоши существующих антивирусных средств;

сложность конкретной вредоносной компьютерной программы.

Рейтинг уровня опасности

«Высокий»: 1000 инфицированных компьютеров, или 10 инфицированных Web-сайтов, или распространение не менее чем в 5 странах.

«Средний»: 50–999 инфицированных компьютеров или 2 инфицированных Web-сайта или распространение не менее чем в 2 странах.

«Низкий»: все остальные.

1.2 Ущерб

Критерий «ущерб» определяет меру вреда, который может быть нанесён компьютерным системам пользователя. Для этого должно быть учтено:

каковы условия, инициирующие выполнение каких-либо несанкционированных действий;

насколько повысится загрузка серверов, занятых обслуживанием процедур обработки и доставки электронной почты;

осуществлялось ли несанкционированное удаление и (или) изменение файлов;

происходило ли разглашение и (или) изменение конфиденциальной информации;

какое снижение производительности компьютерной системы;

привнесение ошибок в прикладные компьютерные программы, которые становятся причиной снижения эффективности работы компьютерной системы;

наличие попыток несанкционированного доступа к установленным параметрам защиты компьютерной системы, что приводит к раскрытию защищаемой информации;

усилия (масштабность мероприятий), которые необходимо предпринять для устранения нанесённого ущерба.

Рейтинг уровня опасности

«Высокий»: несанкционированное удаление и (или) изменение файлов, очень высокая рабочая нагрузка на серверы, крупномасштабный невосполнимый урон, значительные повреждения системы безопасности и снижение надёжности компьютерной системы в целом, инициирование деструктивных действий.

«Средний»: отсутствие критических изменений в установленных параметрах защиты компьютерной системы и привнесённых ошибок в прикладных компьютерных программах, сравнительная лёгкость устранения последствий нанесённого ущерба.

«Низкий»: полное отсутствие деструктивных действий, то есть не было преднамеренного разрушительного воздействия, направленного на уничтожение или повреждение компьютерной системы.

1.3. Распространение

Параметр «распространение» показывает, насколько быстро вредоносная компьютерная программа распространяет саму себя. Для этого должны быть учтены:

способы распространения (электронные атаки исполняемых кодов компьютерных программ (собственно компьютерные вирусы – Viruses); широкомасштабные атаки посредством использования возможностей электронной почты (компьютерные «черви» – Worms); распространение исключительно посредством загрузки и копирования («троянские» программы – Trojan horse));

способность к инфицированию сетевых дисковых накопителей;

трудность удаления и (или) исправления.

Рейтинг уровня опасности

«Высокий»: компьютерные «черви», сетевые программные средства, исполняемые файлы, трудно сдерживаемые угрозы (как вследствие высокой

сложности самой вредоносной компьютерной программы, так и недостаточного уровня развития технологий антивирусного программного обеспечения на момент её появления).

«Средний»: большая часть компьютерных вирусов.

«Низкий»: большая часть «троянских» программ.

Этап 2. Обобщённая оценка степени опасности

Обобщённая оценка степени опасности объединяет три упомянутые выше компоненты степени опасности для пользователей вычислительной техники.

Категория 1 – Очень низкая опасность

Представляет собой незначительную опасность для компьютерных систем пользователей. Практически отсутствуют проверенные сообщения о существовании данного компьютерного вируса в «диком виде».

Категория 2 – Низкая опасность

Данный вид угрозы характеризуется показателем «Низкий» по критерию «Дикость», и «Высокий» по критериям «Ущерб» или «Распространение». То есть вирусы, которые способны причинять компьютерным системам неординарный ущерб или распространяться при помощи стандартных компьютерных программ/подпрограмм, или обладают некоторыми признаками компьютерного вируса, которые уже были достаточно широко освещёны в сообщениях профессиональных электронных и традиционных изданий, а также иных средств массовой информации.

Категория 3 – Умеренная опасность

Этот вид угрозы характеризуется либо «Высоким» рангом критерия «Дикость», либо «Высоким» рангом двух других составляющих.

Категория 4 – Высокая опасность

Опасный вид угрозы. Атаки вредоносных компьютерных программ, принадлежащих к этой категории, трудно отражать. Код компьютерного вируса может быть загружен и разослан пользователям напрямую. В этой кате-

гории составляющей «Дикость» и одной из двух других составляющих одновременно должен быть присвоен ранг «Высокий».

Категория 5 – Очень высокая опасность

Чрезвычайно опасный вид угрозы. Атаки вредоносных компьютерных программ, принадлежащих к этой категории, крайне трудно отражать. Любой из функционирующих компьютеров может загрузить самую последнюю модификацию компьютерного вируса напрямую и запустить на выполнение его программный код, несмотря на проведение предварительного анализа с помощью какого-либо антивирусного средства. В результате почтовые серверы, например, могут приходить в неработоспособное состояние (в профессиональной терминологии – «падать»). В этой категории всем трём составляющим должен быть присвоен ранг «Высокий».

2.2. Методологический подход, принятый фирмой Panda Software

Вирусная лаборатория фирмы Panda Software устанавливает и присваивает каждому конкретному компьютерному вирусу уровень опасности сразу после проведения его исследования при первом появлении. Компания определяет уровень исходящей от каждого компьютерного вируса угрозы, которую он представляет в данное время в целях дальнейшего оперативного информирования пользователей о степени его опасности. Критериями, используемыми для определения уровня угрозы, являются его распространение и ущерб, который может быть нанесён.

Диаграмма оценки уровня угрозы в соответствии с указанными критериями приведёна на рис.1.

- **Низкий уровень угрозы:** компьютерный вирус не наносит ущерб и не получил широкого распространения.
- **Средний уровень угрозы:** компьютерный вирус либо получил относительно широкое распространение, но не послужил причиной серьёзного ущерба, либо не получил широкого распространения, но послужил причиной серьёзного ущерба.

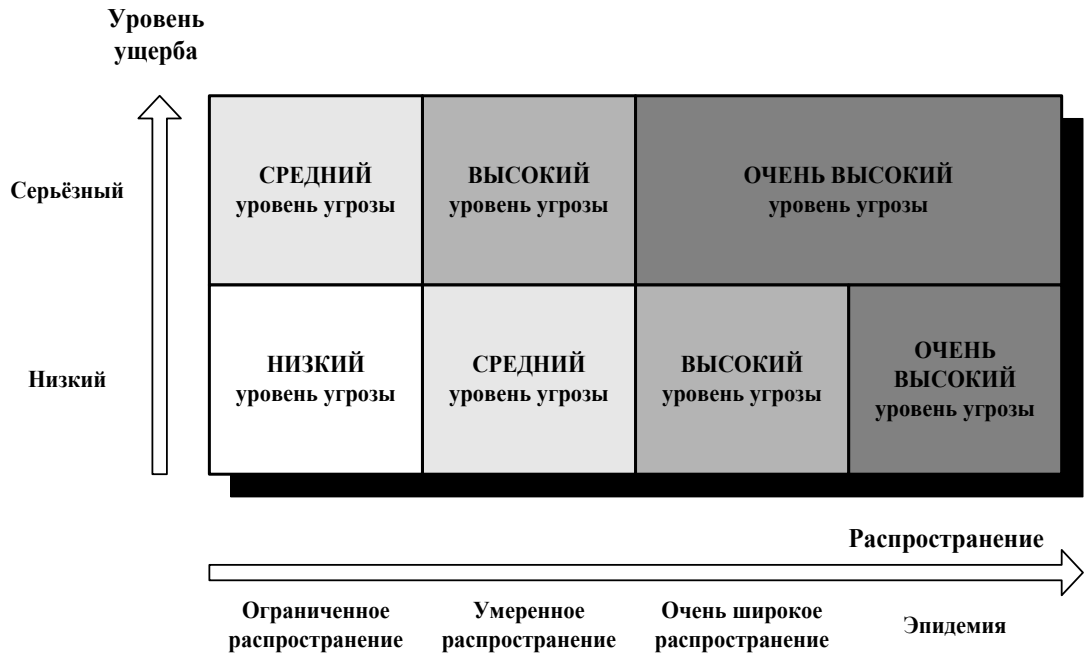

Рис. 1. Оценка уровня угрозы по критериям распространения и ущерба

- **Высокий уровень угрозы:** компьютерный вирус либо получил очень широкое распространение, но не послужил причиной серьёзного ущерба, либо получил относительно широкое распространение и нанёс серьёзный ущерб.
- **Очень высокий уровень угрозы:** компьютерный вирус либо получил очень широкое распространение и нанёс серьёзный ущерб, либо вызвал эпидемию.

Логично предположить, что уровень угрозы может изменяться в пределах от низкого уровня угрозы в какой-то момент времени до очень высокого уровня угрозы в другой период, в зависимости от того, как широко вирус распространился.

Критерий – распространение

Большинство из числа широко распространённых вирусов несут с собой и более высокую вероятность инфицирования компьютеров пользователей. Распространённость вируса определяется скоростью заражения, которая измеряется в процентах инфицированных компьютеров от общего числа проверенных на наличие этого вируса компьютеров.

Уровень распространения вируса определяется следующим образом:

- Ограниченное распространение – вирусом заражено менее 0,3% от числа проверенных компьютеров.
- Умеренное распространение – вирусом заражено 0,3–2,5% от числа проверенных компьютеров.
- Широкое распространение – вирусом заражено 2,5–3,5% от числа проверенных компьютеров.
- Эпидемия – вирусом заражено более 3,5% от числа проверенных компьютеров.

Критерий – ущерб

Ущерб может быть более или менее ощутимым: появляющиеся на экране монитора сообщения, утеря или искажение информации, сбои программного обеспечения, «зависание» компьютера, полная остановка компьютерной системы и пр.

Уровень ущерба определяется следующим образом:

- Низкий уровень: вирус вызывает приемлемые последствия. Всевозможные компьютерные программы, так называемые «безобидные» или «безвредные», которые, вместе с тем, могут предпринимать попытки нанесения ущерба пользователю, но, в итоге не инициируют разрушительные действия. Например, компьютерные вирусы, которые создают различные сообщения, появляющиеся затем на экране монитора пользователя и т. п.
- Серьёзный уровень: наносится серьёзное повреждение компьютерной системе. Например, разрушаются или видоизменяются файлы, форматируются «жёсткие» диски, отсылается информация посторонним лицам, порождается чрезвычайно интенсивный трафик на серверах, снижается быстродействие системы, открываются «бреши» в системе защиты компьютерной системы, наносится невосполнимый ущерб, возникают не устраняемые сбои и т.п.

§3. Моделирование процессов распространения вредоносных компьютерных программ

Если приведённые методологические подходы к оценке серьёзности угрозы вредоносных компьютерных программ компьютерным системам пользователя носят оперативный характер, то долгосрочной целевой установкой можно считать разработку и исследование количественных моделей, которые должны вобрать в себя характерные черты процесса распространения вредоносных компьютерных программ. Потенциальную выгоду от такой деятельности можно разделить на две основные категории.

Во-первых, математические модели могут оказать помощь в оценке, совершенствовании и принятии типовых методик, нацеленных на препятствование распространению компьютерных вирусов. Например, общеизвестно, что универсальные компьютерные системы должны обеспечивать хотя бы минимальный режим защиты, но, по существу они сплошь и рядом вполне проницаемы для компьютерных вирусов[22], значит, набор условий, при которых такое проникновение может происходить, должен быть резко ограничен. Справедливой кажется мысль о том, что от понимания количественных показателей можно будет «проложить мостик» к более глубокому пониманию уязвимости и восприимчивости современных компьютерных систем к электронной заразе, а также определить результативность предпринимаемых компьютерным сообществом усилий для подавления процесса распространения компьютерных вирусов[23]. Кроме того, результаты математиче-

---

[22] Fred Cohen, «Computer viruses, theory and experiments», Computers & Security, vol. 6, 1987.

[23] Fred Cohen, «Models of practical defenses against computer viruses», Computers & Security, vol. 8, 1989.

Maria M. Pozzo and Terence E. Gray, «An approach to containing computer viruses», Computers & Security, vol. 6, 1987.

Catherine L. Young, «Taxonomy of computer virus defense mechanisms», Proc. 10th National Computer Security Conference, Baltimore, Maryland, 1987.

Nick Lai and Terrence E. Gray, «Strengthening discretionary access controls to inhibit trojan horses and computer viruses», Proc. Summer 1988 USENIX Conf., San Francisco, California, June 20–24, 1988.

ского моделирования могут быть востребованы, и принести пользу уже на этапе конструирования нового аппаратного обеспечения, которое будет осуществлять функции по защите компьютерной системы на уровне «железа», а также в процессе разработки нового программного обеспечения для этих компьютерных систем. Иными словами, они должны предоставить дополнительные возможности для поиска разумного компромисса между ценой защищённой от вирусов компьютерной системы, простотой и экономической эффективностью, с которой новое системное и прикладное программное обеспечение сможет вписаться в технологический процесс производства и эксплуатации этих систем.

Второй важной областью применения метода математического моделирования, которая соответствует духу эпидемиологии биологических вирусов, является использование его результатов в целях исследования эпидемий, вызываемых вредоносными компьютерными программами. Она гораздо менее заметна, но в действительности может оказать существенную помощь при прогнозировании возникновения и развития эпидемий вредоносных компьютерных программ и при планировании потребностей в различных видах ресурсов, которые необходимы для того, чтобы быстро и с минимальными затратами справиться с возникшей проблемой. Сверх того, моделирование используется при проведении биологических исследований и экспериментов как у нас в стране, так и на Западе, и может применяться для определения оптимальной линии поведения в целях регулирования хода эпидемий компьютерных вирусов, а также изоляции или иммунизации заражённых компьютерных систем в отведённый для этого срок[24]

George I. Davida, Yvo G. Desmedt and Brian J. Matt, «Defending systems against viruses through cryptographic authentication», Proc. 1989 Symp. on Security and Privacy, Oakland, California, May 1–3, 1989.

[24] Winfried Gleissner, «A mathematical theory for the spread of computer viruses», *Computers & Security*, vol. 8, 1989.

Итак, создание количественных и качественных моделей процессов распространения вредоносных компьютерных программ – простых, но, вместе с тем, охватывающих существенные характеристики вычислительных сетей, в которых эти программы развиваются, может позволить сделать один из первых важных шагов на пути прекращения бесконтрольного распространения компьютерной инфекции: определить на этом пути ориентиры. В своё время Фред Кохэн показал, что абсолютная защита от вредоносных компьютерных программ невозможна, так может быть, в результате соответствующих исследований удастся однозначно доказать, что такая система защиты просто и не нужна? По существу, защитные механизмы пригодны для предотвращения широкого распространения вредоносных компьютерных программ, если скорость, с которой они обнаруживают и уничтожают вирусы выше, чем скорость, с которой вредоносные программы распространяются среди пользователей. Ведь факт, что эпидемия может произойти только в том случае, если скорость инфицирования превосходит критический порог, хорошо известен как из исследований в области биологии, проведённых во второй половине двадцатого века, так и подтвержден вычислениями, сделанными за рубежом в отношении вредоносных компьютерных программ[25].

§4. Когда деревья были большими

Ну что ж, «цели определены, задачи поставлены», как говаривал небезызвестный политический деятель прошлого века, приступим к главному – созданию летописи компьютерных преступлений.

Вы, конечно, знаете, как обычно начинаются статьи отечественных авторов по истории вирусописания или, иными словами, вредоносных компью-

---

[25] W. Goffman and V.A. Newill, «Generalization of epidemic theory, an application to the transmission of ideas», Nature, vol. 204, 1964.

A. Demers, D. Greene, C. Hauser, W. Irish, J. Larson, S. Shenker, H. Sturgis, D. Swinehart, and D. Terry, «Epidemic algorithms for replicated database maintenance», Oper. Syst. Rev., vol. 22, 1988.

терных программ? Да, вы правы, практически одинаково, примерно так: «…о появлении первого компьютерного вируса существует много разных мнений. Доподлинно известно только то, что на машине Чарльза Бэббиджа, считающегося изобретателем первого компьютера, его не было, а на Univac 1108 и IBM 360/370, в середине 1970-х годов они уже были». И дело здесь не столько во заимствовании друг у друга, хотя и оно имеет место, но в первую очередь, в том, что это – фактически не подвергаемая сегодня сомнению истина в высшей инстанции. А вот дальше форма подачи, объём и содержание материала, а также сюжетные линии у разных авторов то сближаются, то расходятся.

Итак, продолжим наш рассказ об истории возникновения вредоносных компьютерных программ, их распространении, а также о работе фирм и специалистов по устранению и локализации этого «Божьего бича» современности.

4.1. 40-е – 50-е годы: доисторический период – курьёз и теория

- В конце 30-х – начале 40-х годов независимо друг от друга в четырёх, ведущих на то время странах (СССР, США, Великобритания, Германия), возникла идея создания электронно-вычислительных машин.
- Первым в мире электронным компьютером стал английский COLOSSUS-1 (1943 год), использовавшийся для расшифровки секретного кода, который применяла Германия для передачи сообщений особой важности.
- На основе электронных ламп созданы ЭВМ I поколения (1946–1958 годы). Во всём мире насчитывается лишь несколько десятков, а к концу 50-х годов – сотен ЭВМ.
- В 1959 году фирма Intel (США) по заказу фирмы DataPoint (США) начала разработку микропроцессоров.

Руководивший информационным отделом военно-морского штаба вице-адмирал Военно-морских сил США Грейс Мюррей Хоппер и его технический персонал в 1945 году лицом к лицу столкнулись с необычными сбоями находящегося в их ведении оборудования электронно-счётных устройств, представлявших собой прообраз современных средств вычислительной техники. В результате проведённого служебного расследования причина воз-

никновения этих сбоев была оперативно выявлена и устранена, а виновником возникших технических неполадок был признан … обыкновенный мотылёк, случайно попавший внутрь одного из шаговых реле указанных устройств. Хоппер решил не вводить какой-либо новый термин для обозначения этой и аналогичных ей причин сбоев в электронно-счётных устройствах и использовал в качестве общего названия термин, применявшийся физиками Великобритании и США уже с конца XIX века в целях обозначения любого рода неполадок в электрических устройствах. Этим термином был: «bug»[26]. Адмирал не остановился на достигнутом и стал первым, кто применил термин «debugging»[27] в смысле «устранение вредного насекомого», который сейчас часто применяется для описания действий по отладке компьютерных программ и устранения сбоев и отказов вычислительной техники.

Хорошо известно, что идеи, в том числе и гениальные, появляются намного раньше их материального воплощения в виде осязаемого продукта. Так вот, в конце тех же 40-х годов выдающийся учёный из США (имевший австро-венгерские корни) Джон фон Нейман разработал достаточно стройную теорию самовоспроизводящихся математических автоматов, что можно расценивать как гениальное предвидение возможности создания самовоспроизводящихся компьютерных программ[28]. Эта теория стала как бы первым научным обоснованием возможности создания вредоносных компьютерных программ, в частности, компьютерных вирусов, но не нашла достаточного

---

[26] Bug (англ.) – жук, клоп, насекомое, личинка насекомых. В разговорном смысле слова переводится как вирус, микроб, вирусное заболевание. В науке и технике, в зависимости от области применения, переводится в следующих значениях: ошибка (в компьютерной программе или устройстве), дефект, помеха, сбой, отказ, неисправность, повреждение, подслушивающее устройство.

[27] Debugging (англ.) – изначальное значение – это устранение неполадок, неисправностей, конструктивных недостатков, ошибок, доводка, приработка, наладка (механизмов, аппаратуры и т.п.).

[28] J. Von Neumann and A. W. Burks, Theory of Self-Reproducing Automata, University of Illinois Press, Urbana, Illinois, 1966.

понимания своей значимости на перспективу и, соответственно, не сразу вызвала достойный её интерес в научных кругах того времени. Нейман продолжил свои исследования и уже в 1951 году им был предложен конкретный метод создания самовоспроизводящихся математических автоматов.

В 1959 году Л. Пенроуз написал и опубликовал в журнале «Scientific American» научную статью о самовоспроизводящихся механических структурах, в которую он включил и простую двухмерную модель подобных структур, способных, обратите внимание, к: активации, размножению, мутациям, захвату и последующему освобождению объекта.

4.2. 60-е – 70-е годы: у истоков вирусописания – Рубикон перейдён

- В 1963 году Джон Ликлидер, руководитель компьютерной лаборатории Агентства передовых исследовательских проектов (Advanced Research Projects Agency – ARPA), предложил первую весьма детально проработанную концепцию компьютерной сети.
- В 1969 году по инициативе Управления перспективных исследований Министерства обороны США (Defense Advanced Research Projects Agency – DARPA) создаётся первая локальная вычислительная сеть, получившая название Advanced Research Projects Agency NETwork (ARPANET). Со временем к ней подключаются компьютеры ведущих, в том числе и невоенных, научных лабораторий и научно-исследовательских центров США.
- В 1969 году Кен Томпсон, стоявший тогда во главе группы разработчиков, создал ассемблерный вариант операционной системы UNIX. Целью проекта было создание удобной операционной среды для проведения исследовательских работ в области программирования, а сама операционная система предназначалась для машины PDP-7 фирмы DEC – представителя семейства электронно-вычислительных машин, широко распространённого в научных лабораториях и научно-исследовательских центрах США, что подготовило почву для быстрого распространения операционной системы UNIX.
- В 1972 году к проекту Кена Томпсона подключился Деннис Ричи, которому во многом обязана своим рождением коммерческая версия системы, написанная на высокоуровневом языке программирования «С» (по-русски произносится как «си»).
- В 1973 году фирма Intel выпускает микропроцессор Intel 8080, а в 1979 году микропроцессор Intel 8086/88.
- В 1974 году создана коммерческая версия сети ARPANET, получившая название Telnet.
- В 1977 году фирма Apple Computers выпускает компьютер под несколько странным названием «Apple][» (в подавляющем большинстве отечественных и зарубежных литературных источников указывается «Apple II»,

но это неверно), который стал своего рода прообразом большинства последующих моделей персональных компьютеров, включая и IBM PC.

На основе теоретических изысканий Л. Пенроуза в области самовоспроизводящихся структур указанная двухмерная модель была реализована Ф. Шталем на машинном языке для платформы IBM 650, а Ф. Стахл, пребывая под впечатлением от идей Л. Пенроуза, изложенных всё в той же упомянутой выше статье, реализовал на том же языке биокибернетическую модель. В этой модели двигались некие существа, питаясь при этом отличающимися от нуля (в математическом смысле) словами. Если в процессе передвижения существо долго оставалось без еды, то оно умирало от истощения и, напротив, после поглощения заданного количества отличающихся от нуля слов оно порождало новое, подобное себе создание. Вместе с процедурой размножения Стахлом была предусмотрена и возможность мутаций существ, в ходе которых они могли становиться каннибалами, пожирающими себе подобные создания, но, теряющими при этом функцию размножения. Однако, поскольку электронно-вычислительные машины серии IBM 650 имели весьма ограниченный объём памяти и невысокое быстродействие, Ф. Стахл не смог получить какие-либо значимые результаты, так как в ходе пробного прогона компьютерной программы бесплодный мутант убил и съел единственное существо, ещё сохранившее способность к размножению.

1962 год принёс с собой весьма интересные события, которые, к сожалению, также как и теоретические изыскания Неймана, не удостоились сразу достойного их внимания и правильной оценки компьютерного сообщества. Мы имеем в виду тот факт, что именно в это время Виктор Высоцки, Дуглас МакИлрой и Роберт Моррис[29], специалисты-разработчики математического

[29] Виктор Высоцкий стал автором идеи игры, его коллега Дуглас МакИлрой разработал большую часть кода игры, включая подпрограмму, ответственную за воспроизведение. Наконец, третий учёный, Роберт Моррис-старший, создал смертоносный цифровой организм, который развивается и передает опыт успешных атак своему потомству. «Было ясно, что, экспериментируя с правилами, вносившими в игру некоторую неопределённость,

обеспечения из исследовательского подразделения Telephone Laboratories (корпорация Bell, США), сами того не подозревая, написали программный код, который в настоящее время специалистами-вирусологами расценивается как прообраз современного компьютерного вируса[30]. Как это случилось? Да весьма прозаически. Они придумали необычную электронную игру, названную ими «Darwin»[31], целью которой являлся захват игроками друг у друга как можно большего компьютерного пространства при помощи написанных на языке Ассемблер программ, способных исследовать игровое пространство, уничтожать друг друга и размножаться. Победителем признавался тот, кто смог уничтожить все копии программы противника и захватить «театр военных действий». Причём, уже в той компьютерной программе предусматривалось наличие в памяти электронно-вычислительной машины некоего «модуля управления», который задавал правила игры и устанавливал очерёд-

---

мы сможем оживить её после опустошительного вторжения Морриса, но нам нужно было заниматься другими делами», – вспоминает МакИлрой, который стал к тому времени профессором отделения вычислительной техники колледжа в Дортмунде.

[30] Здесь и далее мы постараемся указывать дату создания вредоносной компьютерной программы. Основываться при этом мы будем либо на дате создания, которую указал в программном коде сам вирусописатель, либо на дате или периоде его первого появления, который обычно регистрируется при описании данного вируса. Дата создания компьютерного вируса предоставляет специалистам дополнительные возможности по выявлению путей, скорости, масштаба его распространения и, следовательно, повышает достоверность последующего прогноза относительно возможного рецидива или создания новых модификаций.

[31] Darwin (англ.) – Чарльз Дарвин, английский учёный, выдвинувший теорию о происхождении человека и основным трудом которого стала книга «О происхождении видов путём естественного отбора или сохранении благоприятствуемых пород в борьбе за жизнь»

По аналогии с этой теорией в игре, в соответствии с законом естественного отбора, выживала только сильнейшая особь. Интересно, что со временем игру усложнили, и она была переименована в «Стержневую войну», так как в те годы оперативная память электронно-вычислительных машин представляла собой десятки тысяч ферритовых сердечников, каждый из которых был способен запомнить всего лишь один бит данных.

ность атак программ, созданных противоборствующими игроками. Был также создан и набор команд, использующих в качестве базы данных все остальные программы из оперативной памяти компьютера. В итоге игра превратилась в битву между компьютерными программами, стремящимися стереть или испортить программный код противника.

Не правда ли, здесь чувствуется вполне определённый прогресс по сравнению с биокибернетической моделью Ф. Стахла?

Итак, несколько ассемблерных программ, названных «организмами», в процессе игры загружались в основную память компьютера и всеми доступными методами, – естественно из числа тех которые были заложены авторами в компьютерную программу, пытались уничтожить друг друга. Созданные одним игроком организмы, то есть принадлежащие к одному «виду», должны были «убивать» представителей другого «вида» и занимать или, если хотите, захватывать «жизненное пространство». Победителем считался тот игрок, чьи организмы захватывали всю память компьютера или набирали наибольшее количество очков. Игра велась на большом участке памяти, называемом ареной и управляемом специальной программой, которая получила название «супервизор». Вид V состоял из N (V) особей, каждая особь (K = 1...N (V)) имела размер S (K) (K = 1...N (V). S (K) < MAX S) и располагалась в R (K) последовательных ячейках, начиная с головной G (K), причём R (V) точек со смещениями P (K,1) … P (K, R(V)) относительно головы, являлись защищёнными. Организм, который получал управление, мог использовать три вида обращения к программе-супервизору:

PROBE (n, 1oc) – запрос о содержании ячейки с адресом «1oc» (если эта ячейка защищена, то управление передается ее обладателю, а если нет, то возвращаются три числа – <номер вида организма, занимающего ячейку> (ноль, если ячейка свободна), <начало> и <конец> (если ячейка свободна, то начало и конец свободного участка арены, в который она входит; нули, если ячейка занята организмом));

KILL (1oc) – уничтожить организм по адресу «1oc» («1oc» должна принадлежать организму другого вида и должна быть предварительно исследована с помощью PROBE любым организмом того же вида, что и нападающий);

CLAIM (n, 1oc) – размножить организм на участок свободного пространства, включающий «1oc» (ячейка «1oc» должна быть предварительно исследована с помощью PROBE и не менее S (K) ячеек должно быть свободно, возможно в результате выполнения предыдущего обращения к KILL).

Казалось бы, всё очень просто, но эта игра стала настоящим «бестселлером» того времени. «Игра для полуночников», возникшая в фирме Bell Telephone Laboratories, быстро приобрела популярность и в других учебных и исследовательских центрах, например в исследовательском центре фирмы Xerox в г. Пало Альто и в Массачусетском институте технологии (МИТ)[32]. Статья с описанием игры была опубликована в специализированном журнале только в 1972 году, когда она уже получила очень широкое распространение в научно-исследовательских центрах и институтах. Однако из-за отсутствия в то время масштабного парка персональных компьютеров эта игра не получила распространения в среде обычных пользователей и, тем более, по определению не могла найти рынка сбыта. Заметим, что если изначально авторами игры использовался термин «организмы», то в тексте этой статьи применительно к одному из видов так называемых «организмов», был употреблён термин … «вирус».

Таким образом, дату написания программ, которые можно охарактеризовать в качестве прототипов первых компьютерных вирусов, можно отнести к 60-м годам. В одних случаях это были банальные программистские ошибки в программах, которые приводили к тому, что программный код копировал сам себя, засоряя «жёсткие» диски и, естественно, снижая показатели надёжности и производительности компьютерных систем. В других случаях созна-

[32] Н.Н. Безруков. Компьютерная вирусология. Киев, 1990.

тельные попытки создания вредоносных компьютерных программ с целью нанесения ущерба компьютерным системам и, соответственно, пользователям. Причём с течением времени удельный вес таких попыток от общего числа инцидентов становился всё больше и больше.

Видимо где-то здесь и проходит та невидимая и незафиксированная в анналах вирусописания граница, переступив которую, компьютерное сообщество, само того не заметив, перешло от этапа неспешного написания вирусоподобных программ в целях развлечения или из любопытства к этапу целенаправленной и осознанной деятельности по нанесению как можно большего ущерба компьютерным системам пользователя. И пусть мы не будем оригинальны, но, вслед за теми исследователями истории вирусописания, которые не поверхностно, а действительно глубоко и заинтересованно изучали феномен зарождения и распространения по всему миру компьютерной заразы, просто обязаны подчеркнуть: уважаемый читатель, ни в коем случае нельзя огульно ругать учёных за создание теоретической основы для появления компьютерных вирусов. Ведь в действительности научные исследования изначально были направлены не на теоретическое обоснование, а затем и прикладное применение наработанных знаний и опыта в целях начала вирусописания и последующего совершенствования компьютерных вирусов. Труды таких ученых как, например, Джона фон Неймана по изучению самовоспроизводящихся математических автоматов, легли в основу дальнейших исследований в области искусственного интеллекта и робототехники.

Между прочим, существовали попытки использования результатов научных исследований и в «мирных» целях. Например, в западных источниках иногда упоминается о полезном прообразе современных компьютерных вирусов, который был создан в конце 60-х годов в научно-исследовательской лаборатории компании Xerox. Он представлял собой системную утилиту, которая «самостоятельно» циркулировала в сети и проверяла работоспособность вычислительных устройств, включённых в сеть. Так что конкретное применение знаний на практике зависит от того, в какие руки оно попадёт.

Гиперболоид инженера Гарина вместо страшного оружия мог бы стать крайне полезным изобретением, однако не в те руки попал, и продолжение его истории вы прекрасно знаете.

В 1970 году через коммерческую сеть «Telnet» распространяется первый в истории сетевой «червь» под названием «The Creeper»[33]. Он был создан[34] для работы в среде известной в то время операционной системы Tenex и использовал для своего распространения глобальные компьютерные сети. «The Creeper» обладал малоприятной способностью к проникновению в вычислительные сети посредством модемной связи, а также мог передавать собственные копии на удалённые системы. Особой скромностью автор «The Creeper» не отличался и в инфицированных компьютерных системах этот «червь» проявлял себя посредством следующего сообщения: «I'm the Creeper … catch me if you can» («Я Creeper … поймайте меня, если у Вас получится»). Для противодействия этой вредоносной компьютерной программе впервые в истории антивирусной борьбы неизвестным, но определённо заинтересованным в благоприятном исходе борьбы с «The Creeper» программистом была написана специальная антивирусная программа, которая впоследствии получила название «The Reaper»[35]. Интересно, что сама эта программа представляла собой вирусоподобный код, который исполнял лишь отдельные функции антивирусного продукта. «The Reaper» распространялся по вычислительной сети и, в случае обнаружения программного кода «The Creeper», немедленно уничтожал его, не дожидаясь от программистов команды «фас». И, скорее всего, абсолютно правы известные отечественные и зарубежные вирусологи, когда в той или иной трактовке подчёркивают следующую мысль: «…трудно с полной уверенностью сказать, что это было: противоборство

---

[33] Creeper (англ) – ползучее насекомое или растение, сорняк, пресмыкающееся.

[34] В некоторых зарубежных источниках автором этой программы признаётся Боб Томас из компании BBN.

[35] Reaper (англ) – жнец, косарь. В переносном смысле слова может употребляться как потрошитель.

первых создателей вирусов или же обе программы были созданы одним человеком (группой людей), желавших исправить свою ошибку».

В 1972 году Агентство национальной безопасности США предупреждает разработчиков средств вычислительной техники о более чем вероятной возможности создания вредоносных компьютерных программ со «скрытой начинкой», которые могут наносить существенный ущерб пользователям. Это сообщение стало первой информацией о компьютерных программах, которые сейчас принято называть «троянскими» программами или «троянскими конями».

Произошедший в 1975 году на компьютерной системе Univac[36] 1108 инцидент можно отнести к проявлению вредоносной компьютерной программы, написанной программистом для собственного развлечения[37]. Этот «правирус» назывался «Pervading Animal»[38] (по данным из зарубежных источников того времени он имел некоторые характерные черты прототипа «троянской» программы) и, как и другие особи этой породы, самостоятельно размножался, дописывая себя в конец исполняемых файлов, но в то время не сумел нанести сколько-нибудь заметный ущерб.

Итак, краткая история «Pervading Animal», которая несколько поразному излагается в различных источниках, гласит, что в 1972–1973 годах это была компьютерная игра, суть которой состояла в том, что игрок задумывал некое животное, а программа, задавая наводящие вопросы, пыталась определить, какое животное загадал человек. Программист, написавший игру, предусмотрел в ней возможность самообучения, и когда программа давала неправильный ответ, она просила пользователя ввести дополнительные

---

[36] Universal Automatic Calculator – универсальная автоматическая счётная машина.

[37] Справедливости ради отметим, что этот случай некоторые специалисты оценивают гораздо жёстче и называют его первой настоящей эпидемией «компьютерного вируса».

[38] «Pervading Animal» (англ.) – «Проходя животное».

наводящие вопросы, которые позволили бы улучшить её способности к отгадыванию загаданного животного[39].

В 1974 году Джон Уокер, в то время программист систем Univac одной из крупных международных фирм[40], разработал собственную версию игры, усовершенствовав её таким образом, чтобы ошибки при игре с одним игроком учитывались в последующих играх. Игра получила широкое признание и: «Мне начали звонить с других установок Univac и просить ленты с игрой», – вспоминал Уокер. Более того, по почте ему стали присылать магнитные ленты для копирования: «Мне это быстро осточертело, и я задумался о том, как облегчить распространение игры. Тогда я и решил сделать ее самовоспроизводящейся». Результат не заставил себя ждать. Уже в 1975 году программа не только модифицировала себя, но и пыталась переписать свою обновлённую (улучшенную) копию в другие каталоги[41]. Если там была программа «Pervading Animal», то она стиралась. В противном случае создавалась новая копия. В результате, через некоторое время все каталоги файловой системы начинали содержать копии «Pervading Animal». Более того, если пользователь переходил с одной электронно-вычислительной машины на другую, то он переносил и свой каталог и, в результате, во всех каталогах уже этой электронно-вычислительной машины появлялась пресловутая «Pervading Animal». При этом совокупность копий «Pervading Animal» занимала

---

[39] В этот период игра была безобидна, напоминала известную игру «20 вопросов» и пользовалась популярностью у многих операторов электронно-вычислительных машин.

[40] В начале 80-х годов Уокер основал компанию Autodesk и является одним из крупнейших акционеров этой компании.

[41] Уокер говорил, что он, якобы, размышлял над возможными последствиями, опасаясь, не допустил ли какой-нибудь роковой ошибки, и только затем запустил программу. Через неделю администраторы Univac из других отделений корпорации начали сообщать о неожиданном появлении игры в их системах. По прошествии несколько недель программу стали обнаруживать в других компаниях. «Через несколько месяцев о программе стали много говорить, и всё больше людей обращались за ней, – рассказывал Уокер. – Из уст в уста она передавалась не хуже, чем копированием в каталоги».

значительное файловое пространство, что в те времена воспринималось как очень серьёзная проблема. Для устранения этого «недочёта», по аналогии с «The Reaper» против «The Creeper», была создана новая, если так можно сказать более «инфицирующая» копия «Pervading Animal», которая копировала себя не один раз, а дважды, тем самым быстро вытесняя собой старую версию игры. По истечении заданного срока она предлагала пользователю сыграть последний раз, а затем сама стирала себя с «жёсткого» диска компьютера. Несколько позже было применено абсолютно радикальное решение задачи уничтожения «Pervading Animal». Программисты разработали новую версию операционной системы «Exec 8», в которой подверглась изменениям структура файловой системы и игра в принципе была лишена способности к размножению. Тем не менее, Джон Уокер всегда утверждал, что «…модифицированная версия этой программы легко преодолела бы новые средства защиты». Ему же принадлежит следующее высказывание: «Univac нагородила кучу мер безопасности, но вот пример угрозы, с которой они ничего не смогут поделать».

В 1974 году на электронно-вычислительных машинах классов СМ 3 и СМ 4 появилась компьютерная программа, получившая название «Rabbit»[42] в связи с тем, что она кроме размножения и распространения информации по магнитным носителям вроде бы ничего не делала, а скорость размножения была очень высокой. Но, якобы совершенно безобидная «Rabbit», перезаписывая себя, занимала драгоценные в то время системные ресурсы и, естественно, понижала производительность всей компьютерной системы. Более того, начиная с определённого, критического уровня распространения, она служила причиной сбоя в работе инфицированных средств вычислительной техники.

[42] Rabbit (англ.) – кролик.

Темп жизни в последней четверти XX века продолжал увеличиваться и «род людской» быстро реагировал на появляющиеся в средствах массовой информации свежие идеи и научно-технические инновации.

Поэтому, когда в 1975 году была опубликована написанная в жанре научной фантастики книга Джона Бруннера «The Shockware Rider»[43], она мгновенно стала бестселлером[44]. В книге описывались саморазмножающиеся и распространяющиеся по сетям компьютерные программы, которые автор называл «червями». Идея, по всей видимости, произвела неизгладимое впечатление на определённые умы, несмотря на то, что её полномасштабное осуществление находилось далеко за пределами возможностей вычислительной техники того времени. В 1977 году Томас Риан написал научно-фантастический роман «The Adolescence of P1»[45], который затрагивал эту же тематику. Действующим лицом романа стал весьма «разумный», но жутковатый компьютерный вирус, занимающийся сбором информации.

Между прочим, в 1978 году в мире уже насчитывалось примерно 3 миллиона только персональных компьютеров «Apple][» и, к концу 70-х годов, в США начался бурный рост сетей для передачи данных посредством телефонных сетей. Примерно тогда же начали функционировать Bulletin

---

[43] «The Shockware Rider» (англ.) – «На гребне ударной волны».

[44] Между прочим, очень даже вероятно, что именно эта книга стала источником «вдохновения» и подвигла Морриса-младшего к созданию в 1988 году его знаменитого «червя», хотя во время выпуска книги практическая разработка такой компьютерной программы была чистым вымыслом. А ведь именно «червь» Морриса открыл эпоху широкомасштабных компьютерных эпидемий и пандемий, в пределах от нескольких часов до нескольких дней втягивающих в свою сферу влияния практически весь без исключения виртуальный мир. Впрочем, о такой знаменитости как сам Моррис-младший и его «черве» мы достаточно подробно поговорим ниже.

[45] «The Adolescence of P1» (англ.) – «Подростковый возраст П 1».

Board System[46] (BBS), прообраз современных сетей коллективного доступа, и программисты размещали на них компьютерные программы, которые всякий мог загрузить оттуда и установить на свой компьютер. В целом это время можно охарактеризовать как начало зарождения широкомасштабного компьютерного хулиганства и вандализма в форме целенаправленного и вполне сознательного написания вредоносных компьютерных программ, разрушающих данные на компьютерах жертвах или просто демонстрирующих на экранах мониторов пользователей различные картинки и псевдографику.[47]

Посмотрим, как разворачивались последующие события на ниве вирусописательства.

§5. 1980–1985 гг.: детство и отрочество

5.1. 1980 год – первые «радости»

- Microsoft анонсирует операционную систему Xenix OS – компактную коммерческую версию UNIX для процессоров Intel 8086, Zilog Z8000, Motorola M68000 и Digital Equipment PDP-11.
- Операционная система, первоначально названная фирмой-разработчиком Seattle Computer Products – QDOS, была модифицирована, к концу года переименована в 86-DOS и продана корпорации Microsoft. Началась эра MS-DOS.
- Выпущена версия 4.11 основанной на ядре UNIX операционной системы Berkeley Software Distribution (BSD), которая бесплатно распространялась среди пользователей под названием FreeBSD.
- Совместные исследования DEC, Intel и Xerox по стандартизации Ethernet завершились 30 сентября опубликованием первой редакции соответствующего стандарта.

Уже в 1980 году развитие информационных технологий даёт возможность быстро и удобно распространять компьютерные программы через упо-

---

[46] Bulletin Board System (BBS) – система электронных досок объявлений. Система, в которой через интерфейс терминального доступа можно пользоваться электронной почтой, перекачивать необходимые файлы и получать некоторые услуги Интернет.

[47] Pseudographics (англ.) – псевдографика, создание примитивных изображений, построенных из символов ASCII. Применяется для изображения таблиц, рамок, диаграмм на алфавитно-цифровом дисплее.

мянутые выше Bulletin Board System, а серверы общего доступа постепенно превращаются в глобальные банки данных, охватывающие практически все развитые страны. Но процесс глобализации и начало построения единого информационного пространства привнесли новые, незнакомые ранее проблемы. Например, такие, как ускорение разработки и, особенно, распространения вредоносных компьютерных программ, которые в случае своей активизации способны наносить компьютерным системам всё более чувствительный ущерб.

Под названием «Самовоспроизводящиеся программы» появляется первая в Западной Европе научная статья, посвящённая компьютерным вирусам. Её автором был научный сотрудник кафедры информатики университета г. Дортмунд (Германия) Йозеф Краузе[48].

Джон Шок из исследовательского центра фирмы Xerox в г. Пало Альто обнаружил небольшой, но вредоносный программный код, который представлял собой компьютерного «червя», распространявшегося в информационно-вычислительных сетях США.

В октябре 1980 года в сети APRANET была обнаружена компьютерная программа, которая вызывала появление множества сообщений «Неверный статус пользователя», что являлось следствием преднамеренной подмены и искажения адресов сообщений, посылаемых по этой сети. В результате систему выключили и провели необходимые восстановительные работы, на которые пришлось потратить целых три дня.

5.2. 1981 год – первая масштабная эпидемия и диагноз

[48] Указанная статья представляла собой препринт Дортмундского университета и, по этой причине, так и осталась малоизвестной работой, хотя и заслуживала гораздо большего внимания со стороны научного сообщества, так как в ней было сформулировано определение компьютерных вирусов, а также на языке ассемблера фирмы Simens – клона системы IBM 360, приводились листинги компьютерных вирусов.

- Корпорация Microsoft выпустила первую версию 16-разрядной однозадачной операционной системы MS-DOS, предназначенную для поставки с компьютерами IBM PC.
- Завершена разработка языка программирования «Модула-2» («Modula-2») для решения задач имитационного и математического моделирования.
- 12 августа 1981 года с рождением IBM PC в мире микрокомпьютерной индустрии появился новый промышленный стандарт.

В 1981 году на всю Северную Америку заявил о своем существовании компьютерный вирус «Elk Cloner»[49], который представлял собой загрузочный вирус[50] и распространялся посредством «пиратских» копий компьютерных игр. «Elk Cloner» инфицировал очень популярные на тот период времени компьютеры фирмы Apple Computers, выпускавшиеся под маркой «Apple][», вызвав первую в истории микрокомпьютерной вычислительной техники по-настоящему масштабную эпидемию, виновником которой стал компьютерный вирус. Когда содержащий вирус флоппи-диск вставлялся в дисковод компьютера, «Elk Cloner» оставался в нём, дожидаясь, пока в дисковод не вставят следующий флоппи-диск. Если это происходило, то он заражал новый флоппи-диск и начинал «дурачиться». Проявлял же себя этот вирус весьма многосторонне и не без выдумки: записывал свой программный код в загрузочные сектора флоппи-дисков, к которым обращался пользователь, переворачивал вверх тормашками графические изображения, выводил текст на экран дисплея в мигающем режиме и демонстрировал разнообразные язви-

[49] «Computer virus catchy, not fatal», Mike Sprengelmeyer, The Daily Northwestern, Tuesday, November 12, 1985 (Vol 107, No. 37).

[50] Загрузочные вирусы многие современные специалисты в области компьютерной вирусологии называют «ископаемыми», так как они практически полностью уничтожены и представляют собой, в основном, исторический интерес. Но, слов из песни не выбросишь, и мы ещё будем о них говорить по мере необходимости. Как правило, загрузочные вирусы характеризуются как «…компьютерные вирусы «первой волны», которые были полностью уничтожены уже первыми антивирусными программными средствами, в живом виде сейчас не существуют и присутствуют, может быть, в коллекциях некоторых вирусологов».

тельные сообщения. «Elk Cloner» подсчитывал количество запусков дисковода и на пятом выключал компьютер или демонстрировал какой-нибудь «эффект», а после пятидесятого запуска очищал экран монитора и занимался стихотворчеством – знакомил пользователя с небольшим стишком.

Elk Cloner: The program with a personality	«Elk Cloner»: программа с выдающимися чертами
It will get on all your disks	Он сядет на все ваши диски
It will infiltrate your chips	Он просочится в ваши микросхемы
Yes it's Cloner!	Да, это Клонер!
It will stick to you like glue	Он будет следовать за вами неотлучно
It will modify RAM too	Он будет также привносить поправки в память
Send in the Cloner!	Записано Клонером!

Всё непознанное вызывает у части людей взрывоопасную смесь диаметрально противоположных чувств: страх, ужас и благоговение одновременно. Поэтому такое необычное поведение вычислительной техники породило у определённого количества пользователей и околокомпьютерной публики «брожение умов», трансформировавшееся в предположение о космической взаимосвязи между компьютерными вирусами и воинственными внеземными цивилизациями, которые, возможно, таким способом пытаются захватить планету Земля.

Но не было никакого внеземного или потустороннего вмешательства. Зато налицо был пышущий здоровьем ученик девятого класса из пригорода г. Питтсбург по имени Рич Скрента[51]. Он был на «ты» с вычислительной техникой и, в частности, с моделью «Apple][» фирмы Apple Computers, а также обожал подшучивать над своими друзьями, вставляя в программы «специальные эффекты» типа вывода на экран ироничного сообщения или внезапного и внешне беспричинного отключения системного блока компьютера после нескольких сеансов абсолютно нормальной работы. «После того как я проделал это несколько раз, никто не хотел брать у меня игры, – обижался

[51] Думаем, что те, кто видел его школьную фотографию, подтвердят наше впечатление о нынешнем владельце и президенте фирмы Topix.net.

Скрента, – тогда я стал думать, каким образом заносить мои приколы на их диски». И в его светлую (без всякой иронии) голову пришла мысль написать самостоятельно распространяющуюся через диски «Apple][» компьютерную программу. Скрента придумал технологию, при помощи которой инфицированию подвергалась команда, часто использующаяся на системных дисках «Apple][». Написанная Скрентом программа мгновенно распространилась среди его родственников, друзей, просто знакомых и преподавателей, а написанная для борьбы с ней антивирусная программа оказалась не способна пресечь дальнейшее распространение вредоносного программного кода. С личных дисков пользователей вирус попадал в информационные сети, заражая сотни компьютеров. Поэтому, в дальнейшем, борьба с «Elk Cloner» велась с помощью … применения защитных наклеек на флоппи-дисках – ведь «жёсткие» диски в персональных компьютерах того времени не устанавливались.

В итоге Рич Скрента вошёл в историю вирусописания с такой характеристикой: «Программа «Elk Cloner» была превосходным, аккуратно сделанным кусочком кода, … а её автор обладал незаурядными способностями, можно сказать талантом в программировании, но использовал его не в том направлении» (Боб Хаблузел, программист-аналитик Vogelback Computing Center (США)).

5.3. 1982 год – вирус-антивирус, эксперименты и программы «черви»

- Одновременно появились PC-DOS (IBM) и MS-DOS (Microsoft) версии 1.1 с некоторыми добавленными и расширенными возможностями по отношению к предыдущей версии.
- Под названием UNIX System III выпущена первая коммерческая операционная система UNIX, в которой сочетались лучшие качества UNIX Version 7, V/32 и других вариантов UNIX, разработанных и применявшихся в корпорации Bell.
- Фирма Intel выпускает микропроцессор Intel 80286 (16 разрядный, 134 тысячи транзисторов).

В 1982 году студентом Техасского университета создан ещё один компьютерный вирус для Apple][, который был рассчитан на деятельность в

среде операционной системы DOS 3.3[52]. Не до конца отлаженная версия этого вируса «ускользнула» от автора и начала распространяться по университету. Ошибка в вирусе вызывала подавление графики популярной игры под названием «CONGO», и в течение нескольких недель все копии этой игры перестали работать. Для исправления ситуации автор запустил новый, исправленный вирус, предназначенный для «замещения» предыдущей версии. Как мы видим, идея «подобное лечится подобным» открывалась многократно[53].

Не без влияния упомянутой нами ранее книги Джона Бруннера «The Shockware Rider» в 1982 году в исследовательском центре фирмы Xerox в г. Пало Альто была создана программа «червь». Шок и Хеппс[54] проводили эксперименты с «червеподобными» компьютерными программами выполняя необходимые расчёты на простаивающих серверах одной из ранних реализаций локальной сети Ethernet. Программы «черви» вели себя довольно интересно, но время от времени выходили из под контроля и их приходилось уничтожать. Зато, в ходе опытов было однозначно доказано, что компьютерные «черви» обладают способностью к «переползанию» с сервера на сервер[55].

Идея, которой руководствовались авторы этих программ, состояла в том, что компьютерная программа, требующая значительных вычислительных мощностей, захватывала все простаивающие, но подключённые к сети электронно-вычислительные машины с тем чтобы, например, ночью использовать максимум подключённых вычислительных мощностей, а утром, когда

---

[52] Просьба не путать с более поздней операционной системой MS-DOS 3.3 для IBM совместимых персональных компьютеров.

[53] Н.Н. Безруков. Компьютерная вирусология. Киев, 1990.

[54] John Shock, Jon Hepps. The «Worm» Programs – Early Experience with a Distributed Computation, Communications of the ACM, Volume 25, 1982, pp 172-180.

[55] Vesselin Bontchev. Methodology of Computer Anti-Virus Research, Doctoral Thesis, University of Hamburg, 1998.

пользователи начинали выполнять свои вычисления, освобождать их, сохраняя промежуточные результаты вычислений. Днём программа могла бы «обходиться» одной или двумя электронно-вычислительными машинами, а ночью вновь захватывала бы все свободные вычислительные мощности. Воистину прав тот, кто считает, что в связи с этой способностью к ночной активности эту программу правильнее было бы назвать не «червём», а самым настоящим «вампиром». При проведении эксперимента по запуску «червя» в сеть, наблюдалось его неконтролируемое распространение и зависание части инфицированных электронно-вычислительных машин. Ввиду того, что, как мы уже говорили, указанный эксперимент проводился на локальной сети «Ethernet», и часть помещений с включёнными машинами на следующее утро оказалась закрытой, копии «червя» из инфицированных машин заразили другие машины. Ситуацию выправило то обстоятельство, что авторы «червя» благоразумно предусмотрели такой ход событий и незамедлительно послали по локальной сети команду о самоуничтожении всем его копиям.

5.4. 1983 год – рождение компьютерной вирусологии

- Выпущена версия 2.0 операционной системы MS-DOS предназначенная для выполнения на оригинальном IBM PC/XT, которая поддерживала функции работы с «жёсткими» дисками, имела инсталлируемые драйверы устройств и новую, UNIX-подобную иерархическую файловую систему.
- Фирмой Apple под названием «Lisa» выпускается один из первых компьютеров с графическим пользовательским интерфейсом и первый компьютер для использования в офисе, управляемый манипулятором «мышь».
- 8 марта – день выпуска персональных компьютеров IBM XT – открыл новую эру в компьютерной индустрии, в значительной степени благодаря открытой архитектуре и сравнительно низкой цене на эту модель.

Прошедший XX век во многом не похож на другие периоды истории человечества, так как был чрезвычайно богат изумительными открытиями, а также ошеломляющими изобретениями и событиями, одни из которых принесли много пользы, а другие – разрушения и катастрофы. Например, в ноябре 2003 года компьютерным сообществом отмечался юбилей, не предполагавший выражения особой благодарности и поздравлений главному винов-

нику этого события – юбилей компьютерного «вируса». Как мы уже говорили, теорию создания самовоспроизводящихся компьютерных программ выдвинул и обосновал в середине XX века Джон фон Нейман, но датой рождения компьютерной вирусологии по праву считается именно 1983 год.

Фред Кохэн[56], в то время аспирант университета Южной Калифорнии (США), первый сказал об идее, которая пришла ему в голову на недельном семинаре по компьютерной безопасности, о возможности разработки саморазмножающейся вредоносной компьютерной программы, предназначенной, в частности, для инфицирования операционной системы UNIX. В одном из интервью, вспоминая о возникновении самой идеи подобной компьютерной программы, Кохэн говорил: «Вдруг как будто лампочка вспыхнула, и я сказал себе: «Ага! Буквально через несколько секунд я знал, как написать такую программу, и то, что она действительно будет работать». Позже, в своей научной работе, посвящённой угрозе со стороны самостоятельно распространяющихся программ и возможным способам защиты от них, он дал её описание, применив термин «компьютерный вирус»[57]. Его научный руково-

---

[56] Фред Кохэн считается родоначальником современной компьютерной вирусологии. В 1986 году он защитил докторскую диссертацию под самим за себя говорящем названием – «Компьютерные вирусы». Этот труд, хотя и не смог оказать существенного влияния на дальнейший ход событий, явился знаменательной вехой в развитии компьютерной вирусологии.

Ф. Кохэн является автором многочисленных научных публикаций в области исследования всего спектра вредоносных компьютерных программ, в том числе и компьютерных вирусов.

[57] Одно только введение в компьютерный лексикон этого термина навсегда занесло имя Кохэна в анналы информационных технологий. Интересно, что даже три года спустя, когда он попросил у Национального фонда науки (США) средства на продолжение своих исследований, это ведомство ему отказало. «Они сказали, что это не актуально», – вспоминает Кохэн, являющийся в настоящее время профессором Нью-Хейвенского университета, главным аналитиком Burton Group и т. д. и т. п.

дитель Лен Эйделман[58] не только вполне осознанно стал употреблять термин «вирус» по отношению к саморазмножающимся компьютерным программам, но и предложил считать эти программы цифровым аналогом биологических вирусов.

Этот год теперь принято считать истинным годом рождения компьютерной вирусологии, но он также знаменует собой, начало эпохи миллиардных потерь из-за вирусов для пользователей, государственных и предпринимательских структур, и получения многомиллионных доходов для ведущих фирм-разработчиков антивирусного программного обеспечения. Ведь за более чем двадцать лет, прошедших с 1983 года, количество существующих компьютерных вирусов стремительно нарастало и к 2003 году, например, превысило 60000 тысяч. Некоторые из них продемонстрировали исключительную живучесть и продолжают годами «путешествовать» по городам и весям во всём мире. Отметим также, что программный код многих компьютерных вирусов с годами становился всё более и более компактным, механизмы тиражирования всё более изощрёнными и совершенными, а бесконтрольное размножение вредоносного кода по экспоненте превращает этот процесс в лавину, которая готова смести всё на своём пути.

5.5. 1984 год – мы уже умеем читать прерывания и считать циклы

- Выпущена версия 3.0 операционной системы MS-DOS.
- Операционная система UNIX установлена более чем на 100 тысячах компьютеров во всём мире.
- Фирмой Apple под названием «Macintosh» выпускается один из первых микрокомпьютеров с тщательно проработанным графическим пользовательским интерфейсом (graphical user interface – GUI).
- Создание первого компьютера типа «Laptop»[59].

---

[58] Представитель тройки знаменитых создателей алгоритма шифрования с открытым ключом. В названии известной технологии RSA (Rivest, Shamir & Adleman) буква «A» как раз и символизирует собой его фамилию.

[59] Laptop – лэптоп, портативный компьютер, предназначенный преимущественно для работы в дорожных условиях и умещающийся на коленях пользователя.

Как считает ряд известных отечественных и зарубежных специалистов, именно 1984–1985 годы следует считать «переломными» в истории компьютерных вирусов, так как в течение этого периода произошло сразу несколько заметных с точки зрения развития компьютерной вирусологии и вирусописания событий. В 1984 году американский писатель Уильям Гибсон впервые ввёл в обиход такое фундаментальное понятие как «киберпространство» (cyberspace), а в мае этого года А. К. Дьюдни, ведущий рубрики «Computer Recreations» («Компьютерные развлечения») журнала «Scientific American», опубликовал упрощенный вариант игры «Darwin»[60], названный «Core War»[61]. В этой игре два игрока пишут на языке программирования низкого уровня «RedCode» по одной собственной компьютерной программе, которые затем помещаются в большой циклически замкнутый участок памяти. Каждая команда занимает одну ячейку памяти, а управляющая программа поочередно исполняет по одной команде каждой из этих программ, подобно простой системе реального времени. Программы нападают друг на друга, но параллельно с атакующими действиями всячески пытаются свести к минимуму собственные повреждения, а также восстанавливают повреждённые неприятельской программой области. Обычная атака заключалась в применении команды записи в память (MOV). Например: команда MOV#0,1000 может сразу «убить» вражескую программу, если угодит в следующую исполняемую команду, то есть, если соблюдается условие при котором следующая выполняемая команда «противника» расположена по адресу 1000; или «ранить», если это данные или исполняемые команды; или «промахнуться», если ячейка 1000 противником не использовалась.

Публикация вызвала большой интерес в среде читателей журнала, и был даже организован некий «клуб по интересам», получившему название Международное сообщество «Войны в памяти» (International Core War Socie-

[60] Dewdney A.K. In the game called Core War hostile programs engage in a battle of bits // Scientific American, 1984, v.250, № 5.

[61] «Core War» (англ) – «Война в памяти».

ty) со штаб-квартирой, располагавшейся в США, а также отделениями в Италии, Польше, ФРГ, Японии и СССР. Далее события развивались по следующему сценарию. Итальянские программисты, Р. Черути и М. Морокути родом из г. Брешиа, отталкиваясь от замысла игры, написали компьютерную программу, которая была способна к саморазмножению в реальных условиях. В качестве аппаратного средства для установки игры они выбрали персональные компьютеры фирмы Apple Computers – модель Apple][, которые в то время были чрезвычайно популярны и стали первыми массовыми персональными электронно-вычислительными машинами, завоевавшими признание мирового компьютерного сообщества. В персональных компьютерах этой модели были установлены дисководы для флоппи-дисков и упомянутые выше программисты сумели открыть и реализовать инновационный для того времени программно-технический приём, использовавшийся затем многочисленными вредоносными компьютерными программами для инфицирования магнитных носителей информации и средств вычислительной техники: перехват функции обработчика прерывания, выполняющего чтение сектора диска[62] и заражение каждого съёмного носителя информации, вставляемого в дисковод инфицированного компьютера. Надо отдать должное живости ума итальянских друзей вирусописателей, так как они уже в процессе разработки программы поняли, что в случае её распространения среди пользователей их родного города может возникнуть компьютерная эпидемия, а, поняв и то, что указанная программа обладает очевидными свойствами компьютерного вируса, они, проведя аналогию с результатами эпидемий биологических вирусов, пришли к выводу о том, что компьютерный вирус может нести с собой опасность и наносить реальный ущерб. Несмотря на это они решили встроить

[62] Перехват функции обработчика прерывания, выполняющего чтение сектора диска (проф.) – иногда для краткости говорят «перехват прерывания по чтению», а в случае выполнения операции записи на «жёсткий» диск – «перехват прерывания по записи».

в «boot»-сектор[63] счётчик и через каждые 16 циклов размножения запускать переформатирование дискеты, но практически в последний момент отказались от этого замысла, всерьёз задумавшись о возможных последствиях.

И всё бы могло на этом и закончиться, но оба программиста были в здравом уме и твердой памяти и, естественно, не забыли об источнике своего «вдохновения».Они написали Дьюдни, в столь уважаемый ими журнал «Scientific American», весьма пространное письмо с детальным изложением своих «плодотворных» идей. Дьюдни, в свою очередь, не долго думая, в датированном апрелем 1985 года обзоре писем читателей по поводу их впечатлений от «CoreWare», фактически, без купюр опубликовал это послание, содержащее подробное описание программы-вируса, способной заражать компьютеры, и это послужило катализатором последующих событий[64]. На конгрессах программистов стали демонстрироваться коды новых программ-вирусов, компьютерные журналы помещали о них подробные статьи, не задумываясь о том, что тем самым способствуют распространению эпидемии. Ввиду того, что журнал «Scientific American» принадлежит к числу наиболее читаемых и широко известных научно-популярных журналов, как в англоязычных странах, так и во многих из тех, где английский язык считается вторым языком после родного, письмо итальянских программистов вызвало нездоровый интерес у его читателей из различных уголков мира. А дальше… совершенно верно, многочисленные сообщения из различных стран о попытках написа-

---

[63] Этот факт признаётся первым упоминанием о возможности внедрения счётчика в «boot»-сектор, а сама идея будет несколько раз открываться заново разработчиками компьютерных вирусов, в том числе и предназначенных для IBM PC.

[64] Dewdney A.K. A Core War bestiary of viruses, worms and other threats to computer memories//Scientific American, 1985, v.252, № 3.

Известный и уважаемый в кругах специалистов компьютерный вирусолог Н.Н. Безруков оценил этот поступок Дьюдни буквально следующим образом: «… Последнее, можно рассматривать как первую достаточно полную опубликованную спецификацию бутового вируса». Весьма похоже на «славу» Герострата.

ния аналогичных вредоносных компьютерных программ посыпались, как из рога изобилия. Но, «майку лидера» всё же оставили за собой граждане США, которые, собственно говоря, и составляли большинство читателей «Scientific American».

История, надо сказать, весьма поучительная, – казалось бы, можно было сделать выводы, но руки-то, как известно, чешутся, а деньги не пахнут. И в том же году В. Гибсон опубликовал научно-фантастический роман «Neuromancer», который также как и упоминавшаяся выше книга Джона Бруннера «The Shockware Rider» стала бестселлером, в котором описываются компьютерные вирусы.

В настоящее время некоторые отечественные и зарубежные специалисты-вирусологи без особых колебаний указывают на этот роман как на второй по силе импульс, после «The Shockware Rider», который стимулировал и, в определённом смысле, направил развитие дальнейших событий в реальном процессе становления вирусописания. Кроме того, под влиянием этих и подобных им книг и статей сформировалось полнокровное литературное направление, основным содержанием которого являются концептуальные подходы к созданию новых поколений компьютерных вирусов – с использованием новых технологий для их все более быстрого распространения и нанесения всё большего ущерба компьютерным системам и пользователям. Для полноты картины приведём и прямо противоположный пример. В сентябре 1984 года в США была опубликована научная статья[65], в которой было проведёно тщательное исследование одной из разновидностей файлового вируса и способности вредоносных компьютерных программ к самостоятельному размножению. Автором указанной статьи был опять-таки Фред Кохэн, и именно эту статью сейчас принято считать первой и удачной попыткой академического исследования компьютерных вирусов, результаты которого

[65] Cohen F. Computer viruses: theory and experiments // Proc. 2nd IFIP Int. Conf. on Computer Security, 1984.

стали доступны широкой общественности[66]. Ещё до того, как был реализован первый компьютерный вирус для IBM PC, Кохэн написал докторскую диссертацию на эту тему, которую и защитил в 1986 году[67]. В ней Фред Кохэн дал следующее определение компьютерного вируса: «…компьютерный вирус представляет собой программный код, который, когда он активизирован, присоединяет себя к другим программам».[68].Он стал одним из первых, кто поверил в существование компьютерных вирусов и планомерно занялся их изучением, и этозаслуживает всяческого уважения. Кохэн уже тогда предвидел скорое появление многочисленных компьютерных вирусов и первый практическим путём обосновал возможность их создания, а также спрогнозировал тот вред, который может быть ими нанесён.

В целях подтверждения своей концепции о саморазмножающихся вредоносных компьютерных программах Фред Кохэн разработал первую программу, предназначенную для инфицирования операционной системы UNIX. Демонстрация этой программы, способной внедряться в другие объекты, проходила 10 ноября 1983 года в Лехайском университете (США) на системе VAX 11/750, работающей под управлением UNIX. Таким образом, чтобы продемонстрировать потенциальную опасность, Кохэн написал действующую тестовую программу, которая показывала, как быстро, реально угрожая

---

[66] По оценке специалистов эта работа содержала полезное, хотя и недостаточно строгое формальное определение вируса и ряд важных соображений о большой потенциальной опасности компьютерных вирусов, а также о том, что для своего размножения вирусу достаточно обычных операций, реализуемых файловой системой любой операционной системы.

[67] «Computer Viruses», ASP Press, 1986.

[68] В 1984 году на 7-ой конференции по безопасности информации Фред Кохэн давал несколько иное научное определение термину «компьютерный вирус», охарактеризовав его как программу, способную «инфицировать» другие программы при помощи их модификации с целью внедрения своих копий.

безопасности мэйнфрейма[69], могут распространяться компьютерные вирусы. Он включил эту программу в команду графического представления структуры файлов UNIX, а затем провел пять опытных атак. В результате его программе удавалось «получить системные права», то есть фактически захватить управление компьютером, примерно за период от тридцати минут до часа после начала атаки. В одном случае на это потребовалось всего лишь пять минут. Эксперимент показал и достаточно высокую скорость размножения вируса (примерно полсекунды на одно заражение), а также большое количество инфицированных файлов. «Он мог распространяться, невзирая на все известные тогда технологии защиты, – говорил Кохэн. – Концепция продемонстрировала, что самым слабым звеном является пользователь с минимальными правами и что программа может быстро оказаться у пользователя с самыми широкими правами».

В 1984 году в немецком журнале «Шпигель» появилась публикация под интригующим читателя названием «Тайная инструкция»[70], которая вызвала новый всплеск эмоций по поводу целесообразности дальнейшего освещения в прессе и других средствах массовой информации тематики, связанной с вредоносными компьютерными программами. Вслед за эмоциями последовала заинтересованная дискуссия, в которой, естественно, принял активное участие и Ф. Кохэн. Например, советник по безопасности компьютеров фирмы Honeywell Information Systems Джером Лоубел довольно резко выступал за прекращение открытого публичного обсуждения данной проблемы. В ходе развернувшейся полемики Кохэн привел следующий довод в пользу дальнейшего повышения уровня осведомлённости общественности о возможной угрозе со стороны вредоносных компьютерных программ: «Суть дела заключается все же в том, что если придумать что-либо в этом роде под силу мне, то это может также сделать и кто-то другой», и этот другой может

[69] Мэйнфрейм (mainframe) –универсальная электронно-вычислительная машина.

[70] Verborgener befehl // Der Spiegel. 1984. V. 38. № 47.

оказаться «скверным парнем». Оценку корректности приведённого Ф. Кохэном аргумента в свою защиту мы оставляем за читателем.

5.6. 1985 год – осваиваем конструкцию «троянского» коня

- Выпущена версия 1.0 операционной системы MS Windows.
- Суперкомпьютер Cray-2 достиг быстродействия 2 млрд. операций в секунду и стал самой мощной электронно-вычислительной машиной на Земле.
- Фирма Intel выпускает микропроцессор Intel 80386 DX (32 разрядный, 275 тысяч транзисторов).

Важность тематики статьи Ф. Кохэна 1984 года и развернувшейся затем дискуссии для компьютерного сообщества подчёркивает тот факт, что она нашла своё отражение в различных научных изданиях и в последующие годы. Приведём пример из числа наиболее известных.

В 1995 году Р. Дирштейн опубликовал в немецком журнале KES перевод ранее упоминавшейся нами работы Ф. Кохэна[71], который был снабжён довольно обширным комментарием переводчика. Причём, статьи Р. Дирштейна с полемикой о степени опасности компьютерных вирусов продолжала появляться и в 1986 году.[72] В том же 1985 году Том Нельф начал распространять по различным BBS перечень «Грязная дюжина – список опасных загружаемых программ» («The Dirty Dozen – An Unloaded Program Alert List»), в котором были перечислены известные на тот момент программы-вандалы[73]. В дальнейшем этот список, включающий большинство выявленных троянских программ и «взломанные» или переименованные копии коммерческого программного обеспечения для MS-DOS, стал широко известен и получил сокращённое название «грязная дюжина». Список на постоянной основе актуализировался Эриком Ньюхаузом из Лос-Анджелеса, который в пояснени-

---

[71] Dierstein R. Computerviren // KES, 1985, v.1, № 3, № 4.

[72] Dierstein R. «Computer viren». Output, 1986, v.15, № 8.

«Computer viruses: a secret threat». Conference Dierstein R. Computerviren // KES, 1985, v.1, № 3, № 4.Securicom, Paris, 1986.

[73] Н.Н. Безруков. Компьютерная вирусология. Киев, 1990.

ях к нему отмечал, что «пользователи могут быть уверены только в одном свойстве своих винчестеров – в том, что рано или поздно они «полетят». Часто пользователь будет винить в этом программу, хотя на самом деле проблема связана с электроникой или механикой. Помните, что слухи о «троянских» программах легче запустить, чем остановить».

С распространением «троянских» программ стали создаваться программы защиты, которые можно рассматривать и как первые антивирусные программы.

Предположительно с 1985 года вирусописателям стал широко известен программный алгоритм, приводящий к «выжиганию» люминофора на монохромных дисплеях выпуска начала 80-х годов. Расхождения в год-два в различных литературных источниках и сообщениях средств массовой информации по этому поводу объясняются тем, что в разных странах информированность общества об инновациях была не одинаковой.

1985 год ознаменовался стремительным ростом производства и резким снижением цен на персональные компьютеры серии IBM PC. Появились модели по цене менее 1000 долларов, которые и предопределили новый этап развития компьютерных вирусов. Кроме того, нарастающими темпами и массовыми тиражами продолжилась публикация посвящённой компьютерным вирусам научно-фантастической литературы, которая, что вполне очевидно, определённо сыграла важную роль в их популяризации и привлечении к ним внимания широкой студенческой и, в целом, молодёжной среды. В частности, фабула французского детектива Терри Брентона и Дениса Бенеша «Soft-war: La Guerre Douce» раскручивается на продаже американского суперкомпьютера для метеорологической сети в СССР. Представители администрации США разрешают поставку суперкомпьютера в Советский Союз чуть ли не против своей воли, но, в то же время «предусмотрительно» санкционируют закладку «логической бомбы» в его системное программное обеспечение, которая при наступлении заданных условий начинает свою разрушительную деятельность и уничтожает всё программное обеспечение в советской метео-

рологической сети, естественным образом связанной с системами оборонного назначения СССР.

§6. 1986 год – пандемия первого компьютерного вируса для IBM PC

- Выпущена версия 3.2 операционной системы MS-DOS, которая поддерживала использование 3,5 дюймовых флоппи-дисков.
- Компания Fujitsu выпустила первые 32-разрядные микропроцессоры SPARC с частотой 16,67 МГ для Sun Microsystems.
- В компьютерных системах всё шире применяются микропроцессоры Intel 80386.
- Фирма Compaq первой среди конкурентов выпустила IBM-совместимый компьютер на базе микропроцессора Intel 80386.

В 1986 году в Западной Европе наконец-то на систематической основе стали проводиться научные исследования вредоносных компьютерных программ и, как следствие, появились первые серьёзные научные публикации, посвящённые компьютерным вирусам. Следует сказать, что их появление несколько запоздало, но лучше поздно, чем никогда.

В этом году произошла пандемия (глобальная эпидемия) первого компьютерного вируса для персональных компьютеров производства фирмы IBM – «The Brain»[74], который достаточно быстро для того времени разошёлся по всему миру и причиной такого «успеха» являлась, скорее всего, полная неготовность компьютерного сообщества к эффективному противодействию. Этот компьютерный вирус был обнаружен в «диком» виде в октябре специалистами университета г. Дэлавер (США) и вызвал в Северной Америке настоящую эпидемию на IBM-совместимых компьютерах. Поскольку эти события происходили ещё до того, как в США и мире вообще начали накапливать точные статистические данные об инцидентах, связанных с компьютерными вирусами, мы не можем дать её сколько-нибудь точную количествен-

[74] Brain (англ) – мозг. В разговорном смысле слова переводится как интеллект, разум, умница, мыслящая личность. В науке и технике, в зависимости от области применения и контекста, переводится в следующих значениях: мозговой центр, электронно-вычислительная машина, центральный процессор.

ную оценку. Однако отдельные, фрагментарные отчёты в прессе, а также неофициальные свидетельства очевидцев тех событий и разрозненные факты, позволяют сделать предположение, что вирус «The Brain» получил очень широкое распространение во второй половине 80-х годов. Более того, он был довольно частым «гостем» на компьютерах пользователей где-то до середины 1990 года, и только начиная с конца 1991 года, он стал появляться всё реже и реже, а к началу 1992 года инциденты с его участием практически прекратились.

Итак, как гласит история компьютерных вирусов, в 1986 году был создан первый компьютерный вирус для IBM-совместимых персональных компьютеров[75]. Это был загрузочный вирус «The Brain», а написали его два брата-программиста, Басид и Амияд Фарук Алви из г. Лахор (Пакистан)[76], и он

---

[75] Harold J. Highland, Computer Virus Handbook, Elsevier Advanced Technology, Oxford, England, 1990.

[76] В результате анализа происхождения компьютерных вирусов была замечена следующая закономерность: файловые вирусы имеют, в основном, западное, а загрузочные – восточное происхождение. Их «родина»: Индия, Индонезия, Новая Зеландия, Пакистан, Сингапур, Тайвань, Южная Корея. В настоящее время загрузочные вирусы принято делить на четыре группы: итальянскую, пакистанскую, новозеландскую и индийскую. В данном случае географическое название не означает, что вся группа вирусов создана именно там. В этих регионах написаны первые загрузочные вирусы, алгоритмы которых носили свои особенности и используются в качестве основных, то есть, вирус может быть создан где угодно, но отнесён, например, к индийской группе.

Представителей пакистанской группы вирусов обычно характеризуют тем, что они не пытаются инфицировать «жёсткий» диск компьютера и заражают только дискеты. «The Brain» как раз и является типичным представителем этой группы. К этой же группе можно отнести загрузочные вирусы «Hard Disk Brain», «Houston Virus», «Brain-86», «Ashar», «Den Zuk». Итальянская группа представлена загрузочными вирусами, в основном демонстрирующими незаурядные визуальные эффекты. Первым и наиболее распространённым представителем этой группы является вирус «Ping-Pong». Он появился на Западе в 1987 году, а в СССР пик эпидемии наблюдался в сентябре 1989 года. Для новозеландской группы характерно заражение Master Boot Record жёсткого диска и минимальный «хвост»,

должен был «отомстить» компьютерным «пиратам» за воровство программ у их фирмы, которая занималась продажами программного обеспечения. Время было достаточно простое, парни вроде бы честные, а о наказании за написание вредоносных компьютерных программ можно было и вовсе не беспокоиться, поэтому программный код «The Brain» содержал в себе не только имена, но и адрес, а также телефоны обоих братьев[77]. Чего уж там мелочиться …

Между тем, вирус под довольно таки напыщенным именем «The Brain» был «полноценной» вредоносной компьютерной программой. Как мы уже упоминали, оригинальная версия этого вируса является первым загрузочным вирусом для MS-DOS, получившим массовое распространение и, кроме того, способным инфицировать пяти дюймовые 360 Кб флоппи-диски (он инфицировал «boot»-сектор и изменял метки дискет на фразу '(c) Brain')[78]. От этого,

---

размером в один сектор, который содержит только оригинальный загрузчик, размещающийся не в псевдо сбойном кластере, а по определённому абсолютному адресу. Особенностью вирусов данной группы является также заражение «жёсткого» диска сразу после инсталляции в оперативную память, ещё до передачи управления стандартному загрузчику, а не после, как это делает большинство вирусов других групп. Родоначальником группы признан вирус «Stoned». Индийская группа загрузочных вирусов зародилась благодаря «деятельности» вирусописателя, проживавшего в своё время в г. Бомбей (Индия), а типичным представителем группы считается вирус «Joshi», впервые обнаруженный в Индии в июне 1990 года. У нас в стране он появился уже в июле того же года.

[77] Конечно, известны и другие вирусы, которые содержали в своём программном коде правдивую, пусть и не столь подробную информацию об их авторах. Например, в том же 1986 году в компьютерные вирусы «Burger» v. 1.1 (автор Р. Бюргер) и «Rush Hour» (автор Б. Фикс) были вставлены уведомления об авторских правах, но оба эти вируса представляли собой демонстрационные версии.

Между прочим, некоторые компьютерные вирусологи очень даже сомневаются в честности и наивности братьев Алви, так как они использовали свою программу в целях самого настоящего «вирусного маркетинга»: каждая копия «The Brain» выводила на экран мигающее сообщение с рекламой их компании Brain Computer Services.

[78] Известные варианты вируса «The Brain» включают: Brain-B/Hard Disk Brain/Houston Virus – версия для «жёсткого» диска; Brain-C – Brain-B с удалённой меткой «(c) Brain»;

по нынешним меркам, в целом незатейливого и не слишком зловредного компьютерного вируса (он не оказывал никакого побочного воздействия и не портил информацию) берёт свои истоки многочисленная и большей частью коварная субкультура, сконцентрировавшаяся на создании и распространении новых вредоносных компьютерных программ, ставших источником дорогостоящих, а зачастую и крайне разрушительных последствий[79].

Созданный якобы лишь для отмщения компьютерным «пиратам» и задуманный как утилита[80] для контроля за распространением пиратских продуктов, вирус «The Brain» решил не ограничиваться такой незначительной ролью с узконаправленной специализацией и, неожиданно для всех, выйдя за государственные границы Пакистана, вызвал масштабную по тем временам пандемию (первую в истории вирусописания для операционной системы MS-DOS), заразив тысячи компьютеров по всему миру. Подчеркнём еще раз, что успешное распространение компьютерного вируса «The Brain» было предрешено и подкреплено тем, что компьютерное сообщество того времени было абсолютно не готово к подобному развитию событий: пользователи пренебрегали даже важнейшими требованиями антивирусной защиты, а программное обеспечение, предназначенное для борьбы с компьютерными вирусами, на тот момент не получило у них необходимого признания.

Clone Virus – тот же Brain-C, за исключением того, что в нём была восстановлена загрузочная метка оригинальной версии вируса; Clone-B – тот же Clone Virus, модифицированный для разрушения таблицы FAT после наступления 5 мая 1992 года.

[79] Интересно, что хотя «The Brain» был первым компьютерным вирусом для персональных компьютеров производства фирмы IBM, он уже обладал некоторыми отличительными чертами типичного «стелс» вируса, так как при попытке чтения заражённого сектора «подставлял» его неинфицированный оригинал. По этой причине многие компьютерные вирусологи указывают на вирус «The Brain», как на первый компьютерный вирус, в котором использована «стелс» технология.

[80] Utility (англ.) – в контексте настоящей книги утилита это сервисная, обслуживающая программа.

Кстати говоря, по горячим следам событий в декабре 1986 года на форуме компьютерного «андеграунда», «специализировавшегося» в то время на взломе VAX/VMS-систем («Chaos Computer Club in Hamburg»), был представлен инфицированный демонстрационной версией «The Brain» файл, написанный в Германии программистом по имени Ральф Бюргер и получивший название «VirDem». Бюргер обнаружил, что компьютерная программа может делать собственные копии посредством добавления своего кода к исполняемым файлам операционной системы MS-DOS. И его первый авторский нерезидентный, заражающий файлы с расширением «*.com» на дисководе A: компьютерный вирус «VirDem» длиной 1236 байт, как раз и демонстрировал эту возможность.

Симптомы заражения этим вирусом были довольно очевидны, так как он увеличивал размеры файлов с расширением «*.com» и, кроме того, показывал свои сообщения. Интересно, что «VirDem» всегда пропускал первый файл с расширением «*.com» в корневом директории и, по этой причине, обычно не инфицировал файл «command.com», а также не заражал файлы с расширением «*.com» в подкаталоге второго уровня. Когда инфицированная программа запускалась на исполнение «VirDem» заражал следующий файл с расширением «*.com» и начинал «игру» с пользователем, показывая на экране монитора следующий текст: «VirDem Ver: 1.06 (Generation #) активен. Copyright by R. Burger 1986, 1987 Phone: D – xxxxx/xxxx. Это демонстрационная программа компьютерных вирусов. Пожалуйста, немедленно впишите номер. Если Вы это сделаете правильно, то Вас ждёт продолжение. Номер заключён между 0 и #». В этом месте пользователь должен был угадать правильный номер и ввести его. Если номер не был угадан, вирус выдавал следующее сообщение: «Извините, Вы ошиблись. Может быть, Вы будете более удачливы в следующей попытке» и блокировал запуск программы пользователя на выполнение. Если введённый номер был правильным, пользователь получал следующее сообщение: «Превосходно. Вы правы. Теперь можете продолжать»; после чего программа загружалась на исполнение. После того

как все файлы с расширением «*.com» на дисководе A: были инфицированы, «VirDem» показывал следующее сообщение: «Все Ваши программы в настоящий момент поражены VIRDEM.COM». В заключение подчеркнём, что при написании компьютерного вируса «VirDem» Бюргер не ставил своей целью сделать его деструктивным и распространить как можно шире в мире.

Итак, наступил новый этап в развитии вирусописания, который был связан с появлением персональных компьютеров производства фирмы IBM – самого массового компьютера в истории развития вычислительной техники.

В отличие от первого этапа, на котором разработки носили исследовательский характер и авторы выполняли эксперименты, заручившись согласием пользователей, в атмосфере второго этапа с самого начала прослеживаются черты жёсткого противостояния законных пользователей группе безответственных или уголовных элементов.

§7. 1987 год – эра загрузочных вирусов

- Выпущена версия 3.3 операционной системы MS-DOS.
- Выпущена версия 2.0 операционной системы MS Windows.
- Выпущена версия 1.0 операционной системы OS/2, которая была в состоянии использовать развитые вычислительные возможности процессора Intel 80386, и обеспечивала связь с большими машинами фирмы IBM.
- Выпущена построенная на схеме микроядра операционная система MINIX (прототип операционной системы Linux).
- Выпущен третий релиз UNIX System V и зарегистрировано четыре с половиной миллиона пользователей этой операционной системы.

После обнаружения и распространения вируса «The Brain» стали ещё чаще появляться многочисленные научно-фантастические романы, посвящённые компьютерным вирусам, а 1987 год «ознаменовался» изданием книги, вред от которой явно перевесил все те полезные сведения, которые она содержала. Эту книгу написал немецкий программист Ральф Бюргер, о котором мы уже говорили выше, и называлась она «Компьютерные вирусы: кончина высоких технологий».[81] Став первой книгой об искусстве создания и

[81] Ralph Burger. «Computer Viruses. The Decease of High Technologies», 1987.

борьбы с вирусами, она стала заодно «букварём и настольным справочником» для начинающих вирусописателей.

В 1987 году независимо друг от друга появляется еще несколько знаменитых в прошлом вирусов для IBM-совместимых компьютеров.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Alameda Boot
Другие названия	Alameda, Mazatlan, «Meritt», Peking, Seoul, Yale
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	январь 1987 года
Страна происхождения	Соединённые Штаты Америки
Длина	512 байт

Не успели закончиться новогодние каникулы, а в США (Колледж Меррит, г. Окленд, штат Калифорния) уже появился вирус «Alameda Boot» – один из первых компьютерных вирусов для IBM-совместимых персональных компьютеров, который представлял собой очень опасный резидентный загрузочный вирус. Автор так и не было точно установлен, но, по мнению сотрудников колледжа, вирус был написан ради развлечения одним из его студентов старших курсов.

«Alameda Boot» использовал следующую методику инфицирования.

Будучи один раз загруженным, вирус постоянно оставался в оперативной памяти компьютера и перехватывал функции операционной системы (прерывания INT 9 и INT 13h). «Alameda Boot» заражал главную загрузочную запись компьютера в то время, когда пользователь пытался перезагрузить систему с инфицированного им флоппи-диска. Следовательно, каждый раз, когда операционная система или программное приложение пытались обратиться к любой из этих функций, вирус активизировался и заражал всё новые файлы. Он записывал себя в «boot»-сектор флоппи-диска в дисководе A:[82] при копировании программного кода других файлов или программ. В резуль-

[82] Первоначальный «boot»-сектор сохранялся вирусом в секторе 0/39/8 (сторона/трек/сектор) и никакие проверки им при этом не выполнялись.

тате деятельности вируса все используемые флоппи-диски заражались, за исключением тех случаев, когда они обеспечивались защитой от записи.

Вирус «Alameda Boot» не использовал какие-либо особенные способы для проникновения в компьютер и последующего своего распространения, а реализовал те средства, которые обычно использовались компьютерными вирусами: сообщения электронной почты с заражёнными вложениями, загрузка программ через Интернет, FTP[83], а также флоппи-диски, CD-ROM[84], и т. п. Особо подчеркнём, что «Alameda Boot» вошёл в историю в качестве первого компьютерного вируса, который был способен безболезненно пережить «горячую» перезагрузку[85] компьютерной системы. В будущем такие вирусы перестанут быть редкостью и среди описываемых нами ниже вредоносных компьютерных программ будут встречаться регулярно, но «Alameda Boot» стал первопроходцем и поэтому навсегда вошёл в историю вирусописания.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Stoned
Другие названия	Hawaii, Marijuana, New Zealand, San Diego, Smithsonian
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	февраль 1987 года
Страна происхождения	Новая Зеландия

Компьютерный вирус «Stoned»[86] впервые был обнаружен в г. Веллингтон (Новая Зеландия) в ходе случившегося в феврале 1987 года вирусного инцидента и постепенно распространился по всему миру, сначала в Австралии и Азии, а затем США и Европе, вызвав, тем самым, масштабную эпидемию.

[83] File Transfer Protocol (FTP) – используемый в Интернет протокол передачи файлов между хост-компьютерами.

[84] Compact Disk Read Only Memory – CD ROM (англ., проф.) – компакт-дисковое запоминающее устройство.

[85] Перезагрузка компьютера в результате одновременного нажатия сочетания клавиш «Alt-Ctrl-Del».

[86] «Stoned» (англ.) – «Обалдевший».

Итак, в соответствии с сообщениями того времени, студентом университета г. Веллингтон была написана компьютерная программа, представляющая собой загрузочный компьютерный вирус, который не только инфицировал «boot»-сектора флоппи-дисков, но и мог заражать главную загрузочную запись «жёстких» дисков – Master Boot Record (MBR).

С тех пор и до наших дней вирус «Stoned», остаётся одним из наиболее известных вирусов, написанных под операционную систему DOS, а в компьютерную вирусологию он вошёл в качестве первого загрузочного вируса, поражавшего MBR компьютерных систем.

Таким образом, вирус «Stoned» заражал как загрузочные сектора флоппи-дисков, так и также главные загрузочные сектора на «жёстких» дисках. Когда компьютер загружался с инфицированного флоппи-диска, вирус сначала заражал «жёсткий» диск, а затем устанавливал себя в оперативную память. Поэтому, любой флоппи-диск, устанавливаемый затем в дисковод A:, естественно заражается. Во время каждой восьмой загрузки с инфицированного вирусом «Stoned» флоппи-диска на экране монитора появлялось следующее сообщение: «Your PC is now Stoned!»[87], которое отображалось на экране монитора в течение всего процесса загрузки компьютерной системы. Когда компьютер загружался с уже инфицированного «жёсткого» диска, вирус немедленно загружался в память и заражал флоппи-диски, но сообщение не показывал. Другие визуальные эффекты данный вирус не порождал.

С точки зрения своего распространения вирус «Stoned» похож на другие загрузочные вирусы и распространяется посредством передачи заражённых флоппи-дисков. Приведем некоторые известные сценарии заражения вирусом «Stoned».

Совместно используемые машины. Если совместно используемый компьютер однажды был загружен с инфицированного флоппи-диска, то «жёсткий» диск будет инфицирован вирусом, и компьютер будет служить в каче-

[87] «Ваш персональный компьютер обалдел!»

стве «центра» распространения инфекции. Используемые в компьютере флоппи-диски (за исключением защищённых от записи) будут заражены и разнесут инфекцию на все другие компьютеры, которые будут с них загружаться позже.

Флоппи-диски общего пользования. Флоппи-диски общего пользования, также могут служить в качестве канала распространения вируса, особенно, если они предназначены для размещения в дисководе A: и загрузка производится с него (например, демонстрационные и диагностические флоппи-диски). Такие флоппи-диски всегда должны защищаться от записи, даже если они не предназначены для загрузки операционной системы.

Не предназначенные для загрузки системы флоппи-диски. Даже не предназначенный для загрузки системы флоппи-диск, который просто показывает пользователю сообщение «Non-system disk» («Не системный диск»), когда с него пытаются загрузиться, может переносить загрузочный вирус. Такие флоппи-диски тоже имеют загрузочный сектор; он содержит маленькую программку, которая отображает сообщение «Non-system disk» и ожидает нажатия клавиш на клавиатуре. Если такой флоппи-диск инфицирован и с него, затем, пытаются загрузиться (обычно, если он случайно остался в дисководе A:, когда компьютер загружается), вирус будет инфицировать «жёсткий» диск, и загрузится в память прежде, чем появится сообщение «Non-system disk».

Эти сценарии применимы к загрузочным вирусам в целом. Несмотря на то, что детали могут отличаться, общая тенденция распространения загрузочных вирусов вполне очевидна: она ограничена несколькими возможными каналами инфицирования.

Первый симптом заражения вирусом «Stoned», это предупреждение антивирусного средства, которое сообщает пользователю об инфицировании компьютерной системы. Другие симптомы гораздо менее очевидны, и незащищённая компьютерная система может оставаться заражённой длительный период времени, распространяя инфекцию на множество флоппи-дисков, а

пользователь будет в полном неведении об этом. Сообщение «Your PC is now Stoned!» появляется только в тех редких случаях, когда система загружается с флоппи-диска – если «жёсткий» диск рабочей станции инфицирован, а все, или подавляющее большинство загрузок производится с «жёсткого» диска, пользователь так никогда и не увидит это сообщение[88]. Компьютерные системы, инфицированные вирусом «Stoned» будут показывать пользователю меньшее количество общей памяти, чем есть в действительности, если запустить утилиту, подобную «CHKDSK» из состава стандартной поставки операционной системы, но обычный пользователь не заметит никаких изменений. Единственный симптом присутствия вируса, который совершенно очевиден, это разрушение файловой системы на «жёстких» дисках, которые были изначально настроены, например, под управление архаичной DOS 2[89], но кто ей сейчас пользуется? В наше время разработаны и существуют специальные инструментальные средства, а также утилиты, которые могут восстанавливать поражённые вирусами главные загрузочные сектора.

Итак, вирус «Stoned» довольно быстро обрёл широкую известность и был достаточно тщательно изучен, поэтому любое доброкачественное антивирусное средство могло эффективно бороться с ним. Но… он постоянно увеличивал число своих версий[90] и копий, расширяя «ареал своего обитания»

---

[88] Существуют и такие версии вируса, которые вообще никогда не выводят на экран дисплея какие-либо сообщения.

[89] Вирус сохраняет оригинальный загрузочный сектор на той части «жёсткого» диска, которая обычно не используется, но использовалось для File Allocation Table (FAT) на некоторых «жёстких» дисках, установленных под операционную систему DOS версии 2.

File Allocation Table (англ.) – таблица размещения файлов, структура данных на «жёстком» диске компьютера, поддерживаемая операционной системой для отслеживания состояния различных сегментов дискового пространства.

[90] Со временем появилось целое семейство вирусов «Stoned»: «Stoned-B» – похож на «Stoned», но может также заражать «жёсткие» диски через их таблицу разделов. Инфицирует системы с контроллерами RLL, которые, в результате, будут часто зависать; «Stoned-C» – похож на «Stoned», кроме того, что сообщение не показывается; «Stoned-D»

вплоть до 1991 года, после чего достиг вершины распространения и некоторое время удерживал «завоёванные» позиции. После наивысшей точки во время ажиотажа вокруг вируса «Michelangelo» (о чём обстоятельный разговор впереди), он в течение нескольких последующих лет медленно снижал показатель своей распространённости. Однако этот – один из наиболее распространённых в мире – компьютерный вирус наблюдался, пусть и достаточно редко, ещё многие годы и «скончался в преклонном возрасте».

Наращивание области распространения, последующая остановка распространения с достижением определённого уровня и, затем, постепенное уменьшение «ареала обитания», представляют собой нормальное явление в «жизненном цикле» компьютерных вирусов. Например, в случае со «Stoned» компьютерные вирусологи указывают на обстоятельство, что инфицированная вирусом «Stoned» система разносит заразу только тогда, когда инфицированный флоппи-диск вставляется в дисковод A:, и не делает этого в других случаях. Система заражается при загрузке с заражённого флоппи-диска в дисководе A:. Кроме того, в раннем «детстве» вируса «Stoned» большинство систем использовало 5,25 дюймовые дисководы, так что именно они были прекрасным средством, которое он использовал для своего распространения по всему миру. В конце 80-х годов, однако, всё отчётливее стала проявляться тенденция к использованию 3,5 дюймовых дисководов в качестве дисковода A:. Доля компьютеров, имевших 5,25 дюймовые дисководы A:, с тех пор постоянно уменьшалась. Таким образом, снижение числа компьютерных систем, которые вирус «Stoned» мог заразить и тем самым распространяться дальше, решающим образом повлияло на его распространённость в мире.

– похож на «Stoned», за исключением того, что этот штамм может инфицировать 5,25 и 3,5 дюймовые флоппи-диски с высокой плотностью записи.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Ping-Pong
Другие названия	Ping Pong, Bouncing Ball, Italian
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	март 1987 года
Страна Происхождения	Италия

В марте в университете г. Турин (Италия) был обнаружен загрузочный компьютерный вирус, получивший имя «Ping-Pong»[91]. Такое название было дано ему за видеоэффекты, наталкивающие на аналогию со всем известной игрой в настольный теннис.

Дело в том, что основное наглядное проявление вируса заключалось в появлении на экране монитора пользователя в текстовом режиме беспорядочно движущегося светлого пятна, похожего на мячик или шарик[92]. Обычно, этот видеоэффект сопровождал каждую шестидесятую загрузку системы с заражённого вирусом «Ping-Pong» «жёсткого» диска или флоппи-диска и оставался, затем, на всё время работы системы до её выключения.

Однако даже этот симптом не мог приниматься в качестве абсолютно надёжного признака. Вирус «Ping-Pong» отображал шарик на экране монитора только тогда, когда значение системных часов во время загрузки системы отвечало определённым свойствам. Но и это не было гарантией, так как в некоторых компьютерных системах эффект скачущего шарика не проявляет себя ни при каких условиях. Так же, как и в случае с вирусом «Stoned», инфицированная вирусом «Ping-Pong» система использовала несколько меньше общей памяти, чем могла бы[93], но, в подавляющем большинстве случаев,

---

[91] Ping-Pong (англ.) – настольный теннис, пинг-понг.

[92] Видеоэффект скачущего шарика, который, двигаясь по экрану монитора, отскакивает от его границ и встречающихся символов не имеет ничего общего с мистикой или фокусом, просто для отображения на экране шарика используется знак 07h, позаимствованный автором вируса из таблицы ASCII кодов.

[93] Во время загрузки вирус «Ping-Pong» резервировал для себя некоторое количество оперативной памяти.

обычный пользователь не замечал этой разницы. В итоге, только предупреждения, исходящие от антивирусных средств, могли предоставить пользователю надёжную информацию о том, что его компьютер заражён вирусом «Ping-Pong».

Вирус «Ping-Pong» заражал загрузочные сектора флоппи-дисков, а также загрузочный сектор MS-DOS (перед тем, как заразить главную загрузочную запись) на «жёстких» дисках. Он перехватывал прерывания INT 8 и INT 13h (вспомните «Alameda Boot») и содержал в своём программном коде байт, в котором указывался номер версии вируса. Номер версии «Ping-Pong» использовал при проверке компьютера на присутствие «инфекции» и, в случае обнаружения своей более старой версии, перезаписывал поверх неё новую[94]. В целом можно сказать, что компьютерные вирусы этого семейства заражают «boot»-сектор флоппи-диска при обращении к нему и содержат команду, которая может выполняться только процессором 8086, устанавливавшимся в моделях IBM PC и PC/XT. Именно по этой причине «Ping-Pong» не распространяется на компьютерах на базе процессоров 80x86. В целом, хотя в деталях распространения и есть отличия, можно сказать, что все сценарии распространения вируса «Ping-Pong» сходны с такими же сценариями для вируса «Stoned». Средством распространения вируса «Ping-Pong» могут служить компьютеры и флоппи-диски общего пользования, а также любые другие флоппи-диски[95].

Таким образом, вирус «Ping-Pong» даже в то время представлял собой уже известный тип компьютерных вирусов, и поэтому любая надёжная антивирусная программа была способна его обнаружить, блокировать и уничтожить. Удаление этого вируса с «жёсткого» диска осуществлялось проще, чем удаление вирусов «Stoned» и «Joshi» - выпонением команды «SYS». Эта ко-

---

[94] Со временем «Ping-Pong» стал главой семейства вирусов, обзаведясь собственным потомством.

[95] Интересно, что на флоппи-дисках вирусы семейства «Ping-Pong» располагаются способом, аналогичным вирусу «The Brain».

манда, как правило, работает и на инфицированном «жёстком» диске, хотя после её выполнения для полной уверенности «жёсткий» диск полезно перепроверить. При некоторых условиях команда «SYS» может не перезаписать загрузочный сектор и, в этом случае, после резервного копирования всех важных файлов, может потребоваться переформатирование «жёсткого» диска (команда «FORMAT») или применение специальной утилиты. В любом случае, необходимо было помнить следующее правило: до проведения мероприятий по «дезинфекции» компьютера следует выключить питание компьютера и перезагрузиться с не инфицированного флоппи-диска.

Таким образом, «изюминкой» вируса «Ping-Pong» следует признать не опасность вредоносных проявлений или крайнюю сложность его выявления, блокирования и удаления из системы, а использование его автором необычных в то время видеоэффектов, что говорит о развитой фантазии вирусописателя. Между прочим, компьютерные вирусы сегодняшнего дня гораздо более изощрённы по части различного рода видеоэффектов, но, если задуматься, то в их основе лежит всё та же идея, которую «явил миру» автор вируса «Ping-Pong» и ему подобных программ. Но об этом в своё время и в должном месте.

Вы, конечно, помните, что первая пандемия компьютерного вируса связана с первым «диким» вирусом, который был написан специально для персональных компьютеров производства фирмы IBM, а имя его – «The Brain», навсегда останется в истории компьютерной вирусологии. Так вот, нам, к сожалению, всё чаще и чаще придётся говорить о вредоносных компьютерных программах, как о «виновницах» глобальных эпидемий и трудно прогнозируемого морального, а также материального и финансового ущерба.

Вирус «Vienna» был написан учащимся средней школы г. Вена (Австрия) в качестве эксперимента и достаточно быстро распространился практически по всему миру. Примерно через год вирус «Vienna» был обнаружен в Москве в летнем компьютерном лагере для детей, международной организации UNESCO. Вирус инфицировал файлы с расширением «*.com» каждый

раз, когда запускалась на выполнение заражённая им программа. При активации вируса «Vienna» каждая восьмая загрузка системы заканчивалась «горячей» перезагрузкой компьютера, в других случаях пользователь получал отказ при попытке запуска программы на исполнение.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Vienna
Другие названия	Austrian, Unesco, DOS-62, DOS-68, 1-in-8, C648, Charlie
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	апрель 1987 года
Страна происхождения	Австрия
Длина	648 байт

Пока вроде бы ничего особенного и примечательного – были написаны тысячи примерно таких же компьютерных вирусов. Но существует и другая версия появления и распространения вируса «Vienna», которая заставляет специалистов ставить его в один ряд со «знаменитостями» того времени. Дело в том, что благодаря книге упоминавшегося нами выше Ральфа Бюргера вредоносный программный код именно вируса «Vienna» стал источником «вдохновения» для целого сонма вирусописателей, написавших на его основе огромное количество штаммов и, даже, оригинальных вирусов. Кроме того, с вирусом «Vienna» связан первый случай «деассемблирования[96]» компьютерного вируса. Итак, вот другая трактовка происходивших событий.

В 1987 году появился вирус «Vienna», чьё последующее распространение фактически по всему миру получило широкий отклик общественности и породило споры о его авторе. Первым человеком, предупредившим об обнаружении способной к саморазмножению компьютерной программы, был Франц Свобода (он дал ей имя «Charlie»). Это сообщение мгновенно разошлось по всем континентам благодаря средствам массовой информации, в том числе и электронным, и привлекло пристальное внимание компьютерно-

[96] Deassembly, inverse assembly (англ.) – деассемблирование представляет собой операцию, обратную по отношению к операции трансляции программы с помощью языка программирования Ассемблер в объектный код.

го сообщества и специалистов, которые всеми доступными средствами пыталась выяснить эпицентр начинавшейся эпидемии. В результате проведённого расследования выяснилось, что Франц Свобода получил компьютерный вирус от Ральфа Бюргера, который в свою очередь, полностью отрицал этот факт и утверждал диаметрально противоположное. Доказать чьё-либо авторство так и не удалось и принято считать, что автор вируса «Vienna» неизвестен. Однако некоторые источники указывают совсем в другую сторону – на учащегося средней школы Вены, с чего мы и начали.

Но, если абстрагироваться от неудачных поисков автора вируса «Vienna», его появление было примечательно тем, что Ральф Бюргер, передал копию вируса Бернту Фиксу, который взялся за его деассемблирование. Попытка оказалась вполне успешной, но специалисты полагают, что считать его первым компьютерным вирусологом-практиком нельзя: деятельность настоящего профессионала в этой области знаний не ограничивается лишь изучением внутреннего строения вируса, но предполагает также и разработку необходимой «вакцины». Вернёмся к Бюргеру. Он, в свою очередь, получив от Фикса результаты деассемблирования вируса, внёс незначительные изменения в программный код вируса, уменьшив его способности к размножению и изменив внешние проявления, и опубликовал его в своей книге[97]. Ну, а дальше Вы уже знаете, книга популяризировала идею написания компьютерных вирусов, объясняла, как это делается, и послужила стимулом к написанию тысяч компьютерных вирусов, в которых частично или полностью реализовались идеи вируса «Vienna».

Из числа вирусных инцидентов 1987 года, безусловно, также большой интерес представляет семейство резидентных файловых вирусов «Suriv» (обратите внимание, при чтении наоборот получается слово «Virus»), появление которого связано с «плодотворной» деятельностью на ниве вирусописания

[97] Эта книга содержала исходные программные коды и других компьютерных вирусов, например, программные коды вирусов «Burger» и «Number One».

неизвестного программиста (или программистов) из Израиля. Между прочим, как и в случае с вирусом «The Brain», вопрос: «что это было, вышедший из-под контроля эксперимент или умышленное создание вредоносных компьютерных программ?», – так и остался открытым. Но, многие известные компьютерные вирусологи разделяют мнение, что всё-таки это, скорее всего, был эксперимент, и указывают при этом на фрагменты программного кода, обнаруженные позднее Израэлем Радаи в университете г. Иерусалим (Израиль).[98]

Впрочем, в то время было не до выяснения, эксперимент это или целенаправленная акция, так как «деятельность» вируса «Suriv» вызвала самую настоящую панику, о чём красноречиво говорят сообщения того времени.

«Компьютерный вирус, получивший название «Israeli» продолжает свободно распространяться… Вчера «Маарив» получила свидетельства, что вирус появился и в других местах, кроме университета в Иерусалиме. Было отмечено наличие вируса в одном из подразделений израильских сил самообороны, использующего персональные компьютеры. В настоящее время университет распространяет вакцины, позволяющие выявить вирус в памяти компьютера и уничтожить его. Однако возникла новая проблема: может появиться мутированная форма вируса, в несколько раз более вирулентная. Все зависит от источника вируса и от того, является ли его изобретатель компьютерным маньяком, занимающимся этим из спортивного интереса, или психопатом, совершенно не контролирующим свои поступки. Сообщество пользователей радуется прекращению процесса нелегального копирования программ, достигшего в последнее время невообразимых масштабов. В точности как СПИД, обусловивший распространение безопасного секса, компьютеризованный вирус может обусловить переход к практике использования только

---

[98] Исследование найденных Израэлем Радаи программных кодов показало, что автор пытался изменить процедуру внедрения в файлы с расширением «*.exe», а последняя модификация вируса являлась всего лишь отладочной версией.

легальных копий программного обеспечения», – сообщалось в газете «Маарив».

«После того как он уже нанёс значительный ущерб, вирус «Israeli» был обнаружен в учебном центре Ротенберга министерства образования. В этом центре разрабатывается компьютерный проект, в котором принимают участие десятки студентов. Заведующий центром Гидеон Гольдштейн и разработчики проекта Майкл Хазан и Гади Кац заявили, что обнаружили вирус, безвозвратно испортивший на 15000 долларов программ и два диска, содержавших результаты 7000 человеко-часов работы. Паника по поводу вируса «Israeli» переметнулась из университетского городка к владельцам компьютеров во всём Иерусалиме. Во многих магазинах покупатели сообщали о появлении симптомов заболевания на их домашних компьютерах, совпадавших с теми, которые появились на компьютерных системах в университете. Сегодня утром мы столкнулись с несколькими случаями и услышали ещё о нескольких, – сказал заведующий компьютерной лабораторией Эмануэль Марински, – это вызывает панику». Так что же это было?

«Родоначальником» всего семейства «Suriv» являлся резидентный компьютерный вирус «Suriv 1.01». Он обладал способностью к инфицированию в режиме реального времени используемых пользователем файлов с расширением «*.com». С этой целью вирус загружался в оперативную память компьютера и оставался там вплоть до его обесточивания, что позволяло ему отслеживать и перехватывать файловые операции.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Suriv 1.01
Другие названия	Israeli, Suriv-1, April 1st, Suriv01
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	апрель 1987 года
Страна происхождения	Израиль
Длина	897 байт

Поэтому, в том случае, если пользователь пытался запустить на выполнение какой либо файл с расширением «*.com», «Suriv 1.01» немедленно заражал его, что и обеспечило процесс быстрого распространения данного вируса. После того, как оперативная память компьютера заражалась в результате запуска пользователем инфицированного файла Вирус «Suriv 1.01» активизировался 1 апреля и выдавал на экран монитора следующее сообщение: «APRIL 1ST HA HA HA YOU HAVE A VIRUS» («1 апреля ха-ха-ха Вы получили вирус»). После чего работа системы блокировалась, и для возобновления рабочей сессии пользователю необходимо было полностью обесточить компьютер, а затем вновь подать питание и загрузить систему. В тело вируса автором был вставлен следующий текст: «sURIV 1.01».

Чуть позже появился следующий представитель семейства «Suriv» с увеличенной эффективной длиной файла в 1488 байт – Suriv 2.01 (другие названия: Suriv-2, April 1st-B, Israeli, Suriv02), который, в отличие от своего предшественника, стал первым вирусом, который мог внедряться в файлы с расширением «*.exe». Вирус «Suriv 2.01» также был резидентным, активизировался тоже 1 апреля, использовал тот же механизм инфицирования файлов, показывал пользователю аналогичное «Suriv 1.01» сообщение и блокировал работу системы. Вместе с тем, «Suriv 2.01» мог блокировать работу системы и без вывода на экран монитора сообщения – в любой день через час после инфицирования выполняемого файла с расширением «*.exe», если системное время совпадало с заданным вирусописателем. При этом зависание системы приводило к потере информации при редактировании. Кроме того, «Suriv 2.01» осуществлял проверку и не заражал файлы повторно.

Вирус «Suriv 3.00», строго говоря, был обнаружен в 1988 году, но, для удобства восприятия материала, приведём его краткое описание именно здесь. Итак, третий представитель семейства «Suriv» с ещё более увеличенной эффективной длиной файла в 1,813 или 1,808 байт – «Suriv 3.00» (Suriv-3, Israeli, Suriv03), сочетал в себе особенности первых двух вирусов и одинаково эффективно заражал как файлы с расширением «*.com», так и файлы с расширением «*.exe». Некоторые специалисты указывали на то, что «Suriv 3.00» является всего лишь одним из более поздних штаммов знаменитого вируса «Jerusalem», о котором речь пойдёт ниже. Текст «sUMsDos» его автором был заменён на «sURIV 3.00», но активизировался «Suriv 3.00» так же, как и вирус «Jerusalem», в пятницу тринадцатого числа, а не 1 апреля, как родоначальник семейства «Suriv 1.01», когда пользователь запускал на выполнение заражённую программу. В отличие от «Jerusalem» файлы этот вирус не удалял по той причине, что в его программном коде присутствовала ошибка. В другой день, отличный от пятницы тринадцатого числа, если вирус уже резидентно присутствовал в оперативной памяти системы 30 секунд, левая верхняя область экрана монитора превращалась в «чёрное окно».

Вирус, известный под именем «Jerusalem»[99], обнаруженный в октябре 1987 года, является одной из старейших и, вероятно, наиболее известных вредоносных компьютерных программ. Во многих отношениях он представляет собой «первичный» файловый вирус. Впервые появившись в университете Хебрев[100] (Израиль), он быстро распространился по всему миру и стал причиной глобальной вирусной эпидемии 1988 года.

---

[99] Jerusalem (англ.) – Иерусалим, один из крупнейших городов государства Израиль, всемирная историческая достопримечательность.

[100] Harold J. Highland, Computer Virus Handbook, Elsevier Advanced Technology, Oxford, England, 1990.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Jerusalem
Другие названия	Israeli, Friday the 13th, Friday 13th, PLO, 1813, 1808, Black Friday, Black Hole, Morbus Waiblingen, sUMsDos, Russian
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	октябрь 1987 года
Страна происхождения	Израиль
Длина	файлы с расширением «*.com» 1813 байт и «*.exe» 1808 байт

Когда заражённый вирусом «Jerusalem» файл запускается на выполнение, вирус резидентно загружается в память и инфицирует любой другой файл, запускаемый при помощи «исполняемой программы». Это относится ко всем программам с расширениями «*.exe» и «*.com», запускаемым из командной строки, а также оверлейным кодам, которые активизируются другими программами. Это происходит до тех пор, пока не будет отключено питание, так как этот вирус спокойно переживает «горячую» перезагрузку компьютера. Такой способ заражения представляет собой технический приём, который использовался впоследствии большинством из наиболее распространённых файловых вирусов. Если программа, инфицированная вирусом «Jerusalem», запускалась на выполнение в пятницу 13-ого числа (любого месяца или года, за исключением 1987 года), то все выполняемые программы «стирались».

Компьютерный вирус «Jerusalem» распространялся от машины к машине посредством инфицированных файлов. После того как заражённая программа перемещалась (на флоппи-диске ли, по локальной сети, загружаясь с главной вычислительной машины, BBS или любым другим способом) с одного компьютера на другой, «целевой» компьютер заражался, как только инфицированная программа запускалась на выполнение. Этот вирус был лишён способности к самостоятельному распространению на другие машины, он как бы «полагался» на пользователей, которые совместно используют компьютерные программы и на электронно-вычислительные машины, которые

могут распространять его по цепочке. Перечислим источники заражения вирусом «Jerusalem».

Совместно используемые компьютеры. При совместном использовании зараженного компьютера вирус будет распространяться через флоппи-диски каждого из пользователей на другие компьютеры, используемые теми же пользователями.

Отчуждаемые носители информации общего пользования. В пользовании находится множество флоппи-дисков и других перезаписываемых носителей информации, которые регулярно переносятся с компьютера на компьютер. Они содержат сервисные утилиты, демонстрационные версии программных продуктов и т. п. Если такой флоппи-диск будет заражён, то вирусная инфекция может очень быстро распространиться среди множества компьютеров.

Серверы локальной сети. Если на сервере локальной сети размещена инфицированная программа, которая используется множеством рабочих станций, то большая часть этих станций также будет поражена в кратчайшие сроки (иногда для этого требуется всего лишь несколько минут). При этом сам сервер может быть заражен очень легко. Одной из типичных ошибок является размещение программы «входа в систему» в общедоступном месте локальной сети, когда постороннее лицо может записать себя в качестве пользователя. Если в локальной сети зарегистрируется инфицированная рабочая станция, программа входа в систему будет заражена, и тогда каждая рабочая станция, которая регистрируется в локальной сети, будет немедленно инфицирована компьютерным вирусом.

Необходимо признать, что защищённые должным образом компьютерные системы за весь свой жизненный цикл, вплоть до списания, могут так никогда и не столкнуться с проблемой вредоносных компьютерных программ. Тем не менее, в любой крупной организации или корпорации обычно функционирует хотя бы несколько компьютеров, защищённость которых оставляет желать лучшего. В этом случае, роль «сирены» может взять на себя

только обслуживающий персонал, который должен знать симптомы, которые могут означать наличие компьютерного вируса в незащищённой системе.

Компьютерный вирус «Jerusalem» являлся одним из наиболее легко обнаруживаемых из числа общеизвестных вирусов, написанных под операционную систему DOS. Причиной тому были нарочитые эффекты и различные проявления странного поведения системы, вызванного его собственными программными ошибками, даже до его «официальной» активизации в пятницу 13-ого числа. Подобные симптомы включали:

сокращение дискового пространства и рост размера программ (когда вирус инфицировал файл, он увеличивал его размер);

периодическое явно заметное снижение производительности инфицированного компьютера (вирус переназначал прерывание INT 8 и через полчаса после выполнения инфицированной программы система могла резко снизить производительность. Пользователи описывали это явление примерно такими словами: «машина, вдруг, начала работать как модем в 1200 бод»);

затемнение небольшой прямоугольной области в левом верхнем углу экрана монитора (так называемый эффект «чёрной дыры»);

появление сообщения «Program too big to fit in memory» («Программа слишком велика, чтобы разместиться в памяти»), когда запущены определённые часто используемые программы с расширением «*.exe» (следствие программной ошибки в вирусе, который непрерывно заново инфицировал большинство программ с расширением «*.exe» и, в конце концов, их становилось слишком много для запуска);

нарушение работоспособности нескольких инфицированных исполняемых программ с расширением «*.exe»: выполнение программы блокировалось, либо появлялись сообщения о непредвиденной ошибке или невозможности загрузки функций (это следствие другой программной ошибки в вирусе, которая, иногда, разрушала часть инфицированной программы).

Первые три из этих симптомов достаточно достоверно сигнализируют о наличии вирусной инфекции, последние два могут возникать вследствие

воздействия различных факторов. Но, в любом случае, при нарушениях работоспособности компьютера лучше выполнить его проверку на наличие известных компьютерных вирусов при помощи антивирусной сервисной программы, тем более, что обычно это представляет собой быстрый и лёгкий процесс.

Кроме всего прочего, вирус «Jerusalem», как уже было сказано выше, обладал деструктивными свойствами. Во время загрузки себя в память он запрашивал у операционной системы текущую дату. Если днём недели являлась пятница, днём месяца 13 число, и год отличался от 1987 года, вирус активизировался. Как только происходила его активизация, любая исполняемая программа уничтожалась. Пользователи, как правило, замечали это достаточно быстро (так как все программы, которые они пытались запустить прекращали работу) и, обычно, предпринимали меры для восстановления данных на «жёстком» диске (программы могут быть переустановлены с оригинальных дистрибутивов или восстановлены из исходных файлов). Но, тот факт, что вирус «Jerusalem» не обладал крайне разрушительными свойствами некоторых более современных вирусов, совсем не означает, что не было особой необходимости в принятии защитных мер. Инфицированные им компьютерные системы работали со сбоями и становились источниками компьютерной заразы, передавая инфекцию другим организациям или индивидуальным пользователям. Следовательно, очистка системы от этого вируса была необходима и, чем раньше его обнаруживали, тем проще было её осуществление. Уничтожение нескольких заражённых файлов на флоппи-диске обычно не наносит большого урона, а вот проверка и последующая очистка сотен незащищённых систем – длительное и весьма затратное мероприятие. В целом, в тех случаях, когда производится зачистка системы от резидентных вирусов, сходных с «Jerusalem», очень важно убедиться, что вируса нет в оперативной памяти во время проведения этой процедуры. В противном случае резидентный вирус способен заразить систему повторно. Для гарантирования того, что его нет в памяти, выключите питание инфицированной системы и переза-

грузите её с защищённого от записи дистрибутива, о котором точно известно, что он не содержит вирусов. Кроме того, во время очистки системы используйте только те программы, о которых известно, что они не инфицированы.

Если забежать несколько вперёд и проследить дальнейшее развитие событий, связанных с вирусом «Jerusalem», то мы увидим, что к 1991 году он стал одним из наиболее известных и распространённых в мире компьютерных вирусов. До 1990 года он постепенно наращивал область своего распространения, к концу 1990 года достиг точки равновесия в большей части мира, а от начала и до конца 1991 года «удерживал» достигнутый уровень распространения, не снижая и не превышая его. После 1991 года вдруг произошла на первый взгляд странная вещь. Было отмечено лишь несколько незначительных компьютерных происшествий, связанных с вирусом «Jerusalem». Вирус, который был одним из наиболее распространённых в 1990 году резко «сдал» свои позиции и к 1995 году стал одним из наименее распространённых компьютерных вирусов. Специалистами фирмы IBM в 1994 году было зарегистрировано только пять инцидентов с вирусом «Jerusalem», а в 1995 году всего лишь одно происшествие с его участием.

Что же явилось причиной столь стремительного «вырождения» знаменитости? Это не было следствием смены типа накопителя на флоппи-дисках или смещения носителей информации от флоппи-дисков в пользу других носителей информации или «жёстких» дисков. Дело было в том, что поменялась сама вычислительная среда, произошла смена поколений как аппаратного, так и программного обеспечения. Но не стоит забегать вперед так далеко - об этом в своё время. А сейчас вернёмся обратно в конец 80-х годов.

В то время как на «южном фронте» с переменным успехом шла борьба с новым семейством компьютерных вирусов «Suriv» вирусописатели из Германии «подарили» пользователям ещё одну семью компьютерных вирусов, которая впоследствии получила общее название «17xx», – производная от эффективной длины кода двух вариантов одного и того же вируса.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Cascade
Другие названия	1701, 1704, «Blackjack», Fall, Falling Letters, Hailstorm
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	октябрь 1987 года
Страна происхождения	Германия
Длина	1701 или 1704 байта

Вредоносные компьютерные программы, входящие в эту семью имеют различные названия «1701», «1704», «Blackjack»[101], Fall[102], Hailstorm[103], «Falling Letters»[104]. Однако, наиболее известным именем для них является как бы собирательное имя «Cascade»[105].

Примечателен вирус «Cascade» тем, что он не только, подобно вирусу «Jerusalem», резидентный и файловый, но также обладает и технологией самостоятельного шифрования с использованием произвольного кода.

Таким образом «Cascade», несомненно, был первым в истории зашифрованным компьютерным вирусом. Он состоял из двух частей – шифровщика, кодирующего тело вируса таким образом, что в каждом заражённом файле оно выглядит по-разному, и самого тела вируса. После запуска файла управление передавалось шифровщику, который декодировал тело вируса и передавал ему управление. Следовательно, этот вирус можно считать предвестником полиморфных вирусов, которые не имеют постоянного программного кода, но сохраняют свою функциональность. Но в отличие от появившихся позднее по-настоящему «полиморфных» вирусов «Cascade» шифровал только тело вируса, принимая за ключ шифра текущий размер заражаемого файла, а сам шифровщик оставался неизменным, что позволяло при помощи антивирусных средств без труда его обнаруживать. Подобно вирусу «Jerusa-

[101] Blackjack (англ.) – чёрный валет.

[102] Fall (англ.) – осень.

[103] Hailstorm (англ.) – ливень, гроза с градом.

[104] Falling Letters (англ.) – буквопад.

[105] Cascade (англ.) – каскад, небольшой водопад.

lem»» вирус «Cascade» загружался в оперативную память, когда инфицированная программа в первый раз запускалась на выполнение, и оставался резидентным до отключения питания компьютерной системы, заражая файлы, которые загружались пользователем на исполнение. В отличие от вируса «Jerusalem», вирус «Cascade» заражал только файлы с расширением «*.com». Он также, иногда, становился причиной того, что все символы, отображаемые на экране монитора, начинали падать вниз, собираясь там как бы в «кучу»; вместе с тем, следует отметить, что, если год отличался от 1988, такое случалось достаточно редко.

В целом, механизм активации вируса «Cascade» основывался на замысловатом алгоритме серии проверок внутренней конфигурации компьютерной системы, типа монитора, наличия или отсутствия платы синхронизации, а также года и времени года, то есть сезона. Например, вирус «Cascade», также как и остальные члены семьи вирусов «17xx», активировался на любом компьютере с мониторами типов CGA или VGA в сентябре, октябре, ноябре или декабре 1980 или 1988 года.

Учитывая то отличие, что заражались только файлы с расширением «*.com», вирусы семейства «Cascade» распространялись посредством тех же каналов, которые использовал вирус «Jerusalem». Как и в других случаях, наиболее наглядным симптомом заражения системы вирусом «Cascade» является соответствующее предупреждение, исходящее от антивирусного средства защиты. Ведь эффект «опадающих символов» проявлялся только в том случае, если, когда вирус загружался в первый раз, системной датой на компьютере были октябрь, ноябрь или декабрь 1988 года, либо если эта дата была выставлена на первое января 1980 года.[106] Правда, в некоторых последу-

[106] Интересно, что первоначально вирус «Cascade» был задуман как «троянский» конь, и разрабатывался в качестве программы, которая должна была отключать подсветку на правой (цифровой) части клавиатуры после загрузки системы. Однако, неожиданно для самих авторов, активизация этой программы послужила причиной того, что все символы попадали с экрана вниз, собравшись там в «кучу». В конце 1987 года код «троянского коня»

ющих версиях вируса это ограничение было снято и этот эффект мог появляться в независимости от года.

Таким образом, множество компьютеров могло оставаться инфицированными этим вирусом длительное время без каких-либо очевидных проявлений. Заражённые файлы разрастались в объёме (в зависимости от штамма вируса), но обычный пользователь этого не замечал. Самые известные «члены» этой семьи компьютерных вирусов не наносили преднамеренный ущерб компьютерным системам и, если вирус выявлялся достаточно быстро, очистка компьютера заключалась всего лишь в стирании инфицированных файлов и замене их резервными копиями[107].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Lehigh
Другие названия	RC0346, MS/DJS
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	ноябрь 1987 года
Страна происхождения	Соединённые Штаты Америки

«На прошлой неделе несколько наших преподавателей-консультантов обнаружили вирусную программу, чрезвычайно быстро распространявшуюся по всему Лехайскому университету. Я подумал, что было бы полезно потратить несколько минут и предупредить как можно больше людей об этой программе, поскольку она вполне может распространиться далеко за пределы нашего университета. Мы не имеем понятия, откуда распространился вирус

был кем-то доработан под резидентный в оперативной памяти вирус. Причём пока оригинальный вирус имел эффективную длину 1701 байт, он мог инфицировать как «родные» персональные компьютеры производства фирмы IBM, так и их клоны, а вот его модификации, которые стали на три байта длиннее, утеряли способность к заражению «родных» персональных компьютеров IBM. Во всех других проявлениях вирусы «1701» и «1704» функционально идентичны.

[107] Однако было и исключение из правила. Один из последующих штаммов этой семьи вирусов – «1704-Format», после активизации пытался форматировать часть «жёсткого» диска. В этом случае действия по приведению системы в работоспособное состояние включали в себя восстановление данных на «жёстком» диске при помощи резервных копий.

... Я настоятельно рекомендую всем, кто работает в общественном доступе, периодически просматривать их собственные флоппи-диски. Кроме того, работайте с максимальной осторожностью – всегда пользуйтесь защищёнными флоппи-дисками. Это не шутки. Значительная часть наших общедоступных флоппи-дисков была наводнена этим вирусом за пару дней» (Коннет Р. ван Вик, старший консультант по работе с пользователями компьютерного центра Лехайского университета).

Так рождалась известность вируса, впоследствии названного «Lehigh», который представляет исторический интерес как один из первых файловых вирусов, а также как первый (и один из немногих) компьютерный вирус, специализирующийся на заражении лишь одного, заранее определённого файла, – в нашем случае, «command.com»[108]. На этот же компьютерный вирус специалисты указывают как на один из первых «вирусов-вандалов», то есть вирус, обладающий явными деструктивными функциями. В данном контексте нам интересен тот факт, что он был первым вирусом, нацеленным на нанесение существенного вреда пользователю посредством безвозвратного уничтожения информации.

Итак, компьютерный вирус «Lehigh» был обнаружен студенческими консультантами Вычислительного центра Лехайского университета (г. Бэтлхэм, штат Пенсильвания, США) в ноябре 1987 года[109]. Они заметили, что, начиная с 18 октября 1987 года, пользователи начали в массовом порядке возвращать выданные им флоппи-диски, заявляя об их дефектности. Хотя в условиях интенсивной эксплуатации, характерной для данного университета, они всегда быстро ломались из-за физического износа, плохо отрегулирован-

---

[108] Поскольку файл «command.com», являясь стандартным командным процессором операционной системы MS-DOS, естественно, резидентный, то есть постоянно находится в оперативно-запоминающем устройстве компьютера, именно вирус «Lehigh» формально признан первым резидентным компьютерным вирусом, заражающим оперативную память компьютера.

[109] K.R. van Wyk The Lehigh virus//C&S, 1989, v.8, №o 2.

ного дисковода или попадания грязи, скорость возврата нарастала настолько стремительно, что было решено проанализировать ситуацию. В результате исследования и был выявлен вирус, который стал причиной массового заражения компьютеров, и в течение всего лишь нескольких дней уничтожил содержимое нескольких сотен флоппи-дисков – как из публичной библиотеки университета, так и личных архивов студентов и преподавателей. Заражение вирусом происходило при загрузке компьютера с инфицированного флоппи-диска и, размножившись, вирус проявлял свою «троянскую» составляющую, уничтожая данные с «жёстких» дисков инфицированных компьютеров[110].

Давайте рассмотрим несколько подробнее сам механизм инфицирования. Вирус имплантирует своё тело в область памяти, используемую «command.com» для стека[111] и изменяет первые байты заражённого «command.com» (поэтому его длина не отличается от длины нормального) таким образом, чтобы первым получить управление после его загрузки. При запуске командного процессора вирус получает управление и становится резидентным, перехватывая прерывание INT 21. При возникновении прерывания INT 21, вирус перехватывает запросы «выполнить программу» и «найти

---

[110] Напомним, что программа «троянский конь» выглядит так, как будто она просто выполняет какую-то полезную функцию, но на самом деле программа скрытно осуществляет и другие действия, например, разрушает директорий на «жёстком» диске или портит FAT. Существенным свойством программы «троянский конь» является то, что она производит разрушения при каждом очередном запуске. Подобно Троянскому коню из древнегреческой мифологии, она маскируется под вполне безобидную программу и может выглядеть как файл с расширением «*.com» или «*.exe», предназначенный для графического вывода на экран монитора и т.п.

[111] Stack (англ.)– стек, это область памяти, функционирующая по принципу LIFO, выделяемая программе для временного хранения адресов возврата при вызовах функций и процедур, передаваемых параметров и локальных переменных.

Принцип LIFO (Last in First Out) – в вычислительной технике, экономике, а также в ряде других областей, вплоть до трудового права означает: «последним прибыл-первым обслужен»; «последним взят на работу-первым уволен» (право привилегии стажа) и т.д.

первый файл». При их обработке вирус сначала определяет, содержит ли диск «command.com». Если да, то он заражает «command.com» диска, к которому идёт обращение, и увеличивает показания специального счётчика, который записывается на «жесткий» диск, а если он отсутствует – хранится в оперативной памяти. Соответственно, перезагрузка сбрасывает счётчик на компьютере без «жёсткого» диска, в то время как на компьютере с «жёстким» диском значение счётчика сохраняется неизменным. После того как показания счётчика достигают значения 4, вирус, используя прерывание INT 26, обнуляет первые 32 сектора того диска, с которого он был загружен. Обнаружение данного вируса упрощается по сравнению с последующими поколениями файловых вирусов в связи с тем, что при заражении «Lehigh» изменяет дату создания файла. Кроме того, вирус не проверяет, защищён ли диск от записи, и не снимает атрибут «Read only». Поэтому, если «command.com» имеет этот атрибут, то вирус в него не проникает.

В заключение добавим следующее. В быстрой локализации вспышки вируса «Lehigh» сыграло важнейшую роль то, что он появился в «альма матер» современной компьютерной вирусологии – Лехайском университете, где были высококвалифицированные специалисты вирусологи. В последующие годы не было зарегистрировано случаев его появления «в диком виде» за пределами этого университета. С другой стороны, подавлению эпидемии способствовал механизм действия самого вируса «Lehigh». Во-первых, он заражал только системные файлы «command.com», оставляя все остальные исполняемые файлы нетронутыми, что резко ограничивало скорость его распространения. Во-вторых, вирус был запрограммирован на уничтожение информации на текущем диске после заражения четырёх файлов и, в результате, вместе с данными уничтожал и самого себя.

9 декабря 1987 года был впервые обнаружен компьютерный «червь», существование которого иногда ставится под сомнение, хотя и подтвержда-

ется сразу несколькими документальными источниками[112]. Ветеран движения получил название «Christmas Tree».[113] Ему было необходимо, чтобы пользователь осознанно запустил на исполнение инфицированное послание электронной почты. «Christmas Tree» также требовал немедленно отправить его в наиболее сильно страдающую фирму IBM, так как он, вероятно, является первым «почтовым сканером», призванным по настоящему искоренить сетевых компьютерных «червей» из систем именно этой компании. Установленный впоследствии автор программы – студент одного из немецких университетов Клошаль Зеллерфельд, утверждал, что просто хотел поздравить своих приятелей и не представлял, что сеть его университета подсоединена к Европейской академической научно-исследовательской сети (European Academic Research Network – EARN). Тем не менее, автор сознательно применил определённые меры маскировки, продемонстрировав неплохое понимание человеческой психологии. В начале программы стояли соблазнительные обещания, а для тех, кто ещё сомневался, запускать ли программу или посмотреть текст до конца, следовал «ненавязчивый» совет о том, что «просмотр этого файла совсем не интересен, просто наберите команду CHRISTMAS и посмотрите, что получится»: /*browsing this file is no fun at all just type CHRISTMAS from cms*/. И только после этого шёл непосредственно текст «червя», но, естественно, уже без комментария. Червь «Christmas Tree» к тому же был шутником. Перед тем как начать рассылку своих копий всем пользователям сети, чьи адреса присутствовали в соответствующих системных файлах «names» и «netlog», он показывал при запуске на экране монитора рождественскую ёлку вместе с коротким текстовым сообщением, в кото-

---

[112] Survivor's Guide to Computer Viruses, ed. Victoria Lammer, Virus Bulletin Ltd, 1993; Vesselin Bontchev, Methodology of Computer Anti-Virus Research, Doctoral Thesis, University of Hamburg, 1998; Carey Nachenberg, Computer Parasitology, Proceedings of the Ninth International Virus Bulletin Conference, September/October 1999, pp 1-25.

[113] Christmas Tree (англ.) – Рождественская ёлка.

ром содержалось поздравление с Рождеством и наилучшими пожеланиями на следующий год.

Таким образом, уже в «Christmas Tree» использовались характерные особенности человеческого поведения. С одной стороны, любопытство – открой письмо, а то так и останешься в неведении, что там внутри; а с другой стороны, желание оказать посильную помощь – требование немедленной пересылки в благих целях, причем с указыванием конкретного адресата.

На примере «Christmas Tree» хорошо видно, как даже такой «древний» «почтовый червь» мог влиять на работу информационных сетей. Написанный на языке управления заданиями REXX операционной системы VM/CMS[114] и распространявшийся посредством электронной почты «Christmas Tree» был запущен в сеть в родном университете его автора. Затем он проник через шлюз в EARN, затем в сеть Bitnet, которая, в свою очередь, имеет связь с внутренней сетью компании IBM VNet. В этой сети «червяк» размножался особенно успешно, поскольку она состоит в основном из машин и программного обеспечения фирмы IBM. Большие списки рассылки у многих пользователей этой сети привели к её перегрузке, и уже 11 декабря «Christmas Tree» резко снизил пропускную способность сети IBM, а 13 декабря вовсе парализовал эту сеть, забив её своими многочисленными копиями.

В течение двух дней, пока сеть была выключена, вся электронная почта фирмы лежала без движения. Сразу после окончания вирусного инцидента IBM были проведены работы по модернизации сети в целях исключения или, по крайней мере, затруднения подобных атак.

В 1987 году было обнаружено несколько вирусов и для не IBM компьютеров – «Apple Macintosh», «Commodore», «Amiga» и «Atari ST». Но, ни

---

[114] Фактически он был единственным из числа известных компьютерных вирусов, написанных на языке управления заданиями. Кстати, этот факт косвенно свидетельствует о мощности и гибкости REXX – несомненно лучшего из множества языков управления заданиями того времени для машин платформы IBM 360/370.

число, ни действия вирусов, написанных под отличные от IBM платформы, не впечатляют.

Например, в первой половине года появилось семейство файловых вирусов для компьютеров «Apple Macintosh», названное «Mac/nVIR-Fam», в основе которого был вирус «Mac/nVIR-A».

«Mac/nVIR-A» представлял собой лишённый каких-либо деструктивных функций файловый вирус, который инфицировал системный файл и, затем, оставаясь резидентно в памяти, заражал прикладные программы по мере того, как они запускались пользователем на выполнение. После заранее заданного числа перезапусков системы или инфицирования определённого количества программных приложений «Mac/nVIR-A» давал знать о своём присутствии, заставляя динамик компьютера, время от времени, подавать звуковой сигнал, когда пользователь стартовал систему или им запускалась заражённая программа. Если же на компьютере была установлена программа «MacinTalk», то взамен звуковых сигналов из динамика раздавался голос: «Don't Panic» («Без паники»).

Второй вирус этого семейства – «Mac/nVIR-B», обнаруженный в июне 1987 года, ничем особенным не выделялся и был практически полным аналогом «Mac/nVIR-A».

§8. 1988 год – отсроченные эпидемии, первые компьютерные мистификации и великий «червь» Морриса-младшего

- Выпущена версия 4.0 операционной системы MS-DOS, которая поддерживала использование «жёстких» дисков объёмом более 32 Мб.
- Выпущена версия 1.1 операционной системы OS/2.
- Фирмой Intel анонсирован сравнительно дешёвый микропроцессор Intel 80386SX.
- Основатель фирмы Apple Computers Стив Джобс со своей новой фирмой Next Computer создали компьютер Next и операционную систему OS NextStep.

Начало этого года было весьма спокойным и, казалось, ничто не предвещало развития в дальнейшем захватывающих событий. Однако они произошли. Но – всё по порядку.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Fu Manchu
Другие названия	FuManchu, 2080, 2086
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	март 1988 года
Страна происхождения	Тайвань
Длина	2086 или 2080 байт

В марте 1988 года появился один из первых «политических» вирусов, который отличался тем, что почём зря и очень нехорошими словами ругал тогдашних политиков и, в частности, премьер-министра Великобритании Маргарет Тэтчер, а также президента США Рональда Рейгана. Назывался этот «неблагонадёжный» вирус-хулиган «Fu Manchu».

Он представлял собой переработанную версию знаменитого вируса «Jerusalem», а возможной датой его создания считается 10 марта 1988 года. При инфицировании вирус «Fu Manchu» присоединял свой код к файлам с расширением «*.com», «*.exe», «*.sys», «*.bin», а также к любым исполняемым программам, включая и оверлейные.

В теле вируса «Fu Manchu» обязательно содержалась метка или идентифицирующая строка «sAXrEMHOr». При этом он использовал для распознавания уже инфицированных им файлов только часть этой строки, а именно: «rEMHOr».

Вирус перехватывал прерывания INT 9, 16h, 21h. Причём, все сообщения внутри тела «Fu Manchu» были зашифрованы. Во время одного из шестидесяти заражений файлов им устанавливалось значение счётчика и, затем, по достижении определенных показаний счетчика вирус расшифровывал (XOR AFh) и показывал на экране монитора следующее сообщение: «The world will hear from me again!» («Мир ещё услышит обо мне!»); после этого система самопроизвольно перезагружалась. При «горячей» перезагрузке компьютерной системы пользователем приведённое сообщение также отображалось на экране монитора заражённой системы. По прошествии 1 августа 1989 года вирус «Fu Manchu» начинал осуществлять контроль над буфером

клавиатуры, добавляя уничижительные и неприличные эпитеты к именам известных политических деятелей. В зависимости от даты он корректировал текст, вводимый пользователем с клавиатуры. Например, если вводилось одно из слов «fu manchu», «thatcher», «reagan», «botha» или «waldheim», вирус добавлял: «fu manchu virus 3/10/88 – latest in the new fun line! thatcher is a cunt reagan is an arsehole botha is a bastard waldheim is a Nazi. Не думаем, что Курт Вальдхайм имел что-то общее с фашистами, а остальное переводить вообще не хочется.[115]

22 апреля 1988 года впервые в сети Usenet состоялся международный электронный форум по проблеме антивирусной безопасности. И, в целом, начиная с 1988 года, компьютерные вирусы привлекают всё большее внимание средств массовой информации. На западе поднимается волна неподдельного интереса практически ко всему, что связано с этой темой. Уважаемые журналы и газеты регулярно публикуют соответствующие статьи и другие материалы: «Business Week», август; «Byte», июль; «Changing Times», сентябрь; «Compute!», июнь, июль, август, октябрь и декабрь; «Datamation», сентябрь и октябрь; «Design News», декабрь; «Fortune», декабрь; «Futurist», сентябрь/октябрь; «Industry Week», август; «Newsweek», две статьи в ноябре; «PC-Computing», ноябрь и декабрь; «PC Magazine», февраль, июнь и июль; «Personal Computing», июль; «Science», апрель и ноябрь; «Time», февраль и сентябрь; «US News and World Report», октябрь. Кроме того, в течение 1988 года «PC Week» издаёт серию статей – более 20, на тему компьютерных вирусов. В этом же году выходит и второй роман В. Гибсона «Mona Lisa Overdrive», развивающий это направление.

Реальному же массовому распространению электронной заразы в то время мало что мешало, так как спектр реализуемых и используемых антиви-

---

[115] Интересно, что при всём при том, вирус «Fu Manchu» претендовал на роль не обычного «электронного хулигана», а идейного борца, которому претят непарламентарные выражения. К примеру, если пользователь вводил с клавиатуры слова «fuck» или «cunt», он тут же стирал их с экрана монитора.

русных средств был ещё очень узок, а многие пользователи и даже программисты не верили в существование вирусов. Одним из таких людей был сам Питер Нортон, который объявил сообщения о компьютерных вирусах «досужим вымыслом и сравнил их со сказками о крокодилах, живущих в городской канализации Нью-Йорка»[116]. Вместе с тем, именно в 1988 году начали свою профессиональную деятельность некоторые из самых уважаемых на сегодняшний день компьютерных вирусологов.

В пятницу, 13 мая 1988 года, фирмы и университеты из разных стран мира, а также те тысячи пользователей нескольких континентов, которые ничего не слышали ранее о таком компьютерном вирусе, но работали на инфицированных им компьютерах, имели несчастье познакомиться с вирусом «Jerusalem», который именно в этот день начал беспощадно уничтожать файлы при попытке их запуска[117]. Этот вирус стал одним из первых (из числа написанных под операционную систему MS-DOS), ставших причиной настоящей пандемии, так как сообщения о заражённых компьютерах одновременно поступали из Европы, Америки, стран Ближнего Востока и Азии. Таким образом, на следующий год после своего первого появления вирус «Jerusalem», вместе с несколькими другими вирусами («Vienna», «Stoned», «Cascade»)[118], распространился по тысячам и тысячам компьютеров.

Ближе к середине года вирусописатели вспомнили о компьютерах Macintosh и выпустили в свет сразу несколько вирусов, рассчитанных на эту платформу. Например, в июне были обнаружены файловые вирусы

---

[116] Однако компания Symantec через некоторое время начала собственный антивирусный проект и, как это ни странно после приведённого высказывания, назвала его: «Norton AntiVirus».

[117] Своё название компьютерный вирус получил по месту одного из инцидентов – университета в Иерусалиме. Более подробную информацию о нём и трёх других поименованных вирусах см. выше.

[118] Более подробно об этих компьютерных вирусах см. выше – 1987 год.

Mac/INIT-29 и Mac/Scores (другие названия «ERIC», «San Jose Flu», «NASA VULT»).

Вирус Mac/INIT-29 инфицировал компьютер сразу, как только на нём запускалось заражённое программное приложение. Он был очень опасен и заражал приложения даже в том случае, если они не активизировались пользователем. Если в инфицированный вирусом Mac/INIT-29 компьютер пользователь вставлял защищённое от записи дисковое запоминающее устройство, появлялось диалоговое окно, содержащее следующее сообщение: «Disk 'disk name' needs minor repairs. Do you want to repair it?». («Диск 'имя диска' нуждается в незначительном ремонте. Вы хотите его починить?») Если пользователь попадался на эту уловку и снимал защиту, Mac/INIT-29 заражал находящиеся на нём файлы. Этот вирус заражал чуть ли не всё подряд: приложения, документы, панели управления компьютерных систем.

Компьютерный вирус Mac/Scores был предназначен как для заражения сервисной службы «Finger» операционной системы Macintosh, так и инфицирования программных приложений. Если на компьютере была установлена операционная система Macintosh версии 6.0.4 или более поздней, вирус повреждал файл «System».

Летняя жара делает человека более инертным, плюс отпуска и, видимо поэтому, июль и август прошли на удивление спокойно. Зато в сентябре появились первые признаки растущей активности отдохнувших и набравшихся новых идей вирусописателей. В этом месяце был обнаружен компьютерный вирус, получивший имя «Den Zuk»[119], также известный под названиями «Search»[120], «Venezuelan»[121], D29.

---

[119] В качестве источника идеи и ранней версии вируса «Den Zuk» (читается по-русски как «Дэн Зук») обычно указывают на вирус «Ohio». Резидентный в оперативной памяти загрузочный компьютерный вирус «Ohio», разработанный и обнаруженный в начале июня 1988 года в Индонезии, во многом был схож с «Den Zuk» и заражал исключительно 5,25 дюймовые флоппи-диски ёмкостью 360 Кб, иммунизируя их к инфицированию вирусом «Brain». При этом вирус «Ohio» показывал на экране монитора следующие текстовые

Идентификационная карточка вредоносной компьютерной программы	
Имя	Den Zuk
Другие названия	«Search», «Venezuelan», D29
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	сентябрь 1988 года
Страна происхождения	Индонезия
Длина	4608 байт

Своё имя данный вирус получил в связи с визуальным эффектом, который порождал. Если система загружалась с инфицированного флоппи-диска, а затем пользователь осуществлял «горячую» перезагрузку, вирус крупными буквами пурпурного цвета выводил на экран монитора надпись: «Den Zuk».[122]

Как выяснилось несколько позже, этот вирус, а точнее, сразу две версии одного и того же вируса были написаны Дэнни Януаром Рамдхани из г. Бандунг (Индонезия).[123] Данный вирус стал широко известен тем, что находил и уничтожал знаменитость того времени – компьютерный вирус «Brain».[124] «Den Zuk» проводил и иммунизацию носителей информации от потенциальной угрозы заражения всё тем же вирусом «Brain». Если «Den Zuk» обнаруживал на инфицируемом им флоппи-диске компьютерные вирусы «Brain» или «Ohio», то немедленно уничтожал их и изменял метку тома этого флоппи-диска на «Y.C.1.E.R.P.».

строки: «VIRUS by The Hackers YC1ERPDENZUK0 Bandung 40254 Indonesia (C) 1988, The Hackers Team».

[120] Search (англ.) – поиск.

[121] Venezuelan (англ.) – венесуэлец.

[122] Условием-ограничением для демонстрации указанной надписи являлось требование, чтобы монитор относился к одному из трёх следующих типов: CGA, EGA или VGA.

[123] В СССР был впервые обнаружен в Москве С. Алексеевым весной 1990 года.

[124] Подробно о компьютерном вирусе «Brain» см. выше, 1986 год.

Таким образом, общепризнанным фактом стало утверждение, что «Den Zuk» олицетворял собой первый полностью дееспособный компьютерный «вирус-антивирус».[125]

Формально вирус «Den Zuk» относится к резидентным в оперативной памяти загрузочным компьютерным вирусам. Все вирусы этого семейства перехватывали прерывание INT 9, 13h и заражали загрузочный сектор 5,25 дюймовых флоппи-дисков ёмкостью в 360 Кб при обращении к ним (INT 13h, ah=2,3,4,5). «Den Zuk» заражал любой флоппи-диск в дисководе, к которому получал доступ, даже если флоппи-диск не был загрузочным. В том случае, если пользователем случайно или по незнанию делалась попытка загрузки системы с заражённого не системного флоппи-диска, «Den Zuk» всё равно устанавливал себя в оперативную память компьютера, хотя такая попытка загрузки системы, естественно, завершалась неудачей. Вирусы этого семейства, как и многие другие загрузочные вирусы, конфликтовали с драйверами флоппи-дисков, поддерживавшими нестандартные форматы (например, 720 Кб). При этом система либо зависала, либо на экран монитора выдавалось системное сообщение о делении на нуль. На заражённых вирусом «Den Zuk» флоппи-дисках в программном коде можно было найти следующие текстовые строки: «Welcome to the Club – The HackerS – Hackin' All The Time The HackerS».

В целом семейство компьютерных вирусов «Den Zuk» представляло собой большую опасность. В то время как оригинальная версия вируса представляла собой программу, в которую не заложены деструктивные функции, нацеленные на нанесение какого-либо ущерба, существовали штаммы, которые могли наносить прямой вред. Эти версии «Den Zuk» содержали встроенный «счётчик», подсчитывавший количество перезагрузок системы, и после того, как его значение достигало числа в диапазоне от пяти до десяти, ини-

[125] Письмо от самого автора «Den Zuk», в котором подтверждается сказанное, было опубликовано в феврале 1991 года в столь уважаемом издании как «Virus Bulletin».

циировалась операция переформатирования флоппи-диска пользователя. Кроме того, при записи вируса на флоппи-диск никаких проверок не производилось и, в результате, он мог уничтожить часть полезной для пользователя информации, расположенной на сороковой дорожке заражаемого флоппи-диска.

Кстати, о вреде. Начиная с 1988 года, появились и циркулируют в Интернет компьютерные мистификации – ложные слухи о появлении новых, очень опасных компьютерных вирусов. И, хотя компьютерным системам они не несут с собой прямой ущерб, этого не скажешь о нервной системе многочисленных пользователей, так что совершенно безобидными их не назовешь. Получив такое сообщение, пользователи рассылают его по известным им электронным адресам, желая предупредить своих коллег, родственников и знакомых о якобы грозящей им опасности, а в итоге в сетях резко возрастает трафик, что может привести к переполнению каналов передачи данных.

В соответствии с изданной в Лондоне статьёй Фебрачи[126] одной из первых компьютерных мистификаций было появившееся в октябре 1988 года, и разосланное на станции BBS большое количество сообщений о якобы существующем вирусе, передающимся от модема к модему и использующим для этого скорость 2400 бод. Вирус-мистификация заявлял о себе следующее:

«Тема: чрезвычайно противный вирус. Область распространения: повсеместно».

Далее шёл такой, якобы авторский, текст: «Я случайно открыл миру вероятно один из наиболее неприятных компьютерных вирусов. Я закончил поздним вечером сеанс работы с BBS и этот файл промелькнул, когда я вышел из «Telix 3» и пытался запустить архиваторы «pkxarc» и «unarc», загруженные мной по модемному каналу связи. Я хорошо знал мой «жёсткий» диск и искал этот файл повсюду, но он, очевидно, записался в какие-то произвольные сектора. Благодарю Бога за крепкий кофе и недавнее резервное

[126] Ferbrache, «A pathology of Computer Viruses», Springer, London, 1992.

копирование. Обратное копирование прошло нормально, так что я вызвал BBS вновь, нашёл и загрузил этот файл. Когда я перешёл к использованию команды «dir» для просмотра списка файлов в директории, мой «жёсткий» диск был битком набит электронным мусором. Я применил программы «Procomm Plus TD», а также «PC Talk 3». Каждый раз похожие результаты. Там было нечто такое, что подвешивало моё испытательное оборудование и различные типы модемов (в это время я проводил научно-исследовательские и опытно-конструкторские работы для местной телекоммуникационной компании и имел в своём распоряжении дома собственную лабораторию). По прошествии ещё одного часа «жёсткие» диски были полностью разрушены, и стало ясно, что я подцепил наихудший в мире компьютерный вирус из числа когда-либо существовавших. Вирус распространял себя посредством модема, в данном случае представлявшего собой класс модемов со скоростью передачи 2400 бод и выше. Несущая частота использовалась мной только для обеспечения работы постоянного запоминающего устройства и отладки регистра. Вирус же переустанавливал конфигурацию битов в одном из внутренних регистров модема и, вместе с тем, портил другие регистры на моём модеме. Модем, который был инфицирован этим вирусом, передал его на другие модемы, которые использовали такую же несущую (полагаю, что те, кто использовал модемы со скоростью передачи 300 или 1200 бод невосприимчивы к этому вирусу). Вирус присоединил себя ко всем данным, поступавшим в двоичной системе исчисления, и заразил «жёсткий» диск главной вычислительной машины. Существует только один способ избавления от этого вируса – полная переустановка всех регистров модема вручную, но я так и не нашёл метод вакцинации модема против него, но, вероятно этому может послужить монтаж специального фильтра несущей. Для пересылки этого сообщения я задействовал модем со скоростью передачи 1200 бод, и предупредил системных операторов двух других BBS (от конкретных имён воздерживаюсь). Я не знаю, как и где этот вирус возник, но уверен, что это дело рук кого-то из работающих в области дистанционной передачи данных при помощи

компьютера, как, например, я сам. Вероятно, сейчас лучше всего использовать модемы со скоростью передачи, которая не превышает 1200 бод. Подпись: Майк Ро Ченль».

И ведь многие пользователи действительно поверили и последовали совету «шутника», перейдя на использование модемов со скоростью 1200 бод.

Другой типичной «шуточкой» стало предупреждение о вирусе, распространяющемся по электрической сети, изменяющем конфигурацию портов и направление вращения дисководов. Согласно этому предупреждению, всего за 12 минут вирус успел поразить 300 тысяч компьютеров в штате Западная Дакота (США).

Мистификация к тому же содержала весьма ироничное предупреждение пользователям, которое исходило как бы от Роберта Морриса III:

Date: 11-31-88 (24:60)	Дата: 31.11.88 (24:60)
Number: 32769	Номер: 32769
To: All Refer #: None	Кому: отсылать всем #: никто
From: Robert Morris III	От: Роберта Морриса III
Read: (N/A)	Читать: (н/д)
Subj: Virus Alert	Тема: вирусное предупреждение
Status: Public Message	Статус: общедоступное сообщение

Внимание: выпущен на свободу новый вирус, он хуже всего, что я когда-либо видел! Он заражает по линии энергоснабжения, садясь на линию с несущей частотой 60 Hz. Он изменяет схемы расположения выводов порта последовательного ввода-вывода данных и меняет направление вращения одного из дисков. Свыше 300 тысяч систем было поражено им только здесь в Мэфи, Западная Дакота! И это в течение всего лишь последних 12 минут.

Он атакует DOS, Unix, TOPS-20, Apple][, VMS, MVS, Multics, Mac, RSX-11, ITS, TRS-80 и VHS системы.

Для предотвращения распространения этого червя:

1) Не используйте линии энергоснабжения.

2) Не используйте аккумуляторные батареи, так как упорно циркулируют слухи о том, что этот вирус уже захватил наиболее крупные заводы по

производству аккумуляторов и заразил положительные полюсы батарей (вы можете попытаться подключиться прямо к отрицательному полюсу).

3) Не загружайте и не откачивайте файлы по линиям связи с удалённого компьютера.

4) Не сохраняйте файлы на флоппи-диски или «жёсткие» диски.

5) Не читайте сообщения. Вообще ни одного!

6) Не используйте последовательные порты, модемы или телефонные линии.

7) Не используйте клавиатуры, экраны или принтеры.

8) Не используйте выключатели, центральные микропроцессоры, просто микропроцессоры, запоминающие устройства или универсальные электронно-вычислительные машины.

9) Не используйте электрические лампочки, электрические и газовые нагреватели или устройства кондиционирования воздуха, проточную воду, документы, огонь, одежду или колёса.

Я просто убеждён, что если все мы будем дотошно следовать этим 9 не сложным правилам, вирус будет вырван с корнем, и драгоценная электронная среда наших компьютеров сохранится непорочной.

Мистификация завершалась следующей подписью: RTM III.

С той поры компьютерные мистификации буквально наводнили Интернет. Тысячи и тысячи реальных компьютерных вирусов во всём мире вызвали, чуть ли не параноидальную шизофрению в обществе, а компьютерные мистификации «подливали масло в огонь» будоража людей. Ещё одним показательным примером такой мистификации является «Good Times», появившаяся в 1994 году, но и по сей день, время от времени, встречающаяся в Интернет. Причина такой живучести заключается в том, что её автор тонко прочувствовал психологию обычного пользователя: вместо попыток самостоятельного распространения от одного компьютера к другому «Good

Times» полагается на слабости людей, которые в панике или преднамеренно (с целью напугать или подшутить) пересылают его друг другу.[127]

Теперь пристегните ремни, так как мы начинаем разговор о знаменитости из знаменитостей – сетевом компьютерном «черве» Морриса, который в ноябре 1988 года вызвал в США повальную эпидемию, заразив в считанные часы тысячи компьютеров по всей стране, и практически парализова в их работу. Причём, подчеркнём, что привела компьютерное сообщество к тому, что произошло в первые дни ноября – вся изложенная нами выше история создания вредоносных компьютерных программ, а также история создания и развития вычислительной техники.[128]

Идентификационная карточка вредоносной компьютерной программы	
Имя	«червь» Морриса
Другие названия	Internet Worm, Cornell/ Arpanet, Milnet/Arpanet, вирус Морриса
Тип	сетевой червь
Инфицируемые платформы	UNIX Berkeley 4.3 (или 4.3 BSD), Sun 3.x
Впервые обнаружен	2 ноября 1988 года
Страна происхождения	Соединённые Штаты Америки
Длина	60000 байт

В 1969 году по инициативе Управления перспективных исследовательских программ Министерства обороны США (Defense Advanced Research Projects Agency – DARPA) была создана локальная вычислительная сеть, получившая название Advanced Research Projects Agency NETwork – «Arpanet»[129]. Она создавалась в интересах исследовате-

[127] Подробнее об этой и других компьютерных мистификациях см. Приложение 1.

[128] При подготовке материала о сетевом «черве» Морриса нами использовались различные источники информации, в том числе и зарубежные на языке оригиналов, но мы хотим отдать должное статье И. Э. Моисеенкова «Суета вокруг Роберта или Моррис-сын и все, все, все...» (Москва, 1990 год). Эта работа была выполнена по горячим следам инцидента, носит характер всеобъемлющего научного исследования и предоставляет надёжную фактографическую основу для отражения событий тех дней.

[129] Данная сеть с коммутацией пакетов явилась прообразом сегодняшней сети Интернет. Официально переименована в Интернет и расформирована в июне 1989 года.

лей в области вычислительной техники и технологий для обмена сообщениями, программами и массивами данных между крупнейшими исследовательскими центрами, лабораториями, университетами, государственными организациями и частными фирмами, выполняющими работы в интересах Министерства обороны США (Department of Defence of USA – DoD). Сеть завоевала общее признание за возможность быстрого обмена данными в масштабах всей страны. Со временем был запущен процесс интеграции, и к «Arpanet» подключились, например, Массачусетский технологический институт (MIT), расположенный в штате Нью-Йорк Корнельский университет. В том же 1969 году, когда была создана «Arpanet» программисты К. Томпсон и Д. Ричи, работавшие в Bell Laboratories (филиал American Telephone & Telegraph – AT&T), разработали многопользовательскую операционную систему – UNIX, имевшую систему разделения доступа, базирующуюся на парольной защите и обладавшую дружественным по отношению к пользователям интерфейсом, мало зависящую от типа машин. Успех этой системы превзошел все самые смелые прогнозы. Но, тенденция к объединению разнотипных систем и массовое применение операционной системы UNIX, а также языка программирования высокого уровня «С» – только усложнили борьбу с вредоносными компьютерными программами.

А сейчас – внимание: летом 1988 года как раз в AT&T Bell Laboratories работал аспирант Факультета информатики Корнельского университета, который занимался «переписыванием программ системы безопасности для компьютеров, работающих под управлением операционной системы UNIX». Ну и что? Действительно, ничего особенного, обычная практика, но осталось совсем немного времени до рокового 2 ноября 1988 года, когда он станет виновником вирусного инцидента, повергшего в шок мировое компьютерное сообщество и названного «величайшим в истории нападением на национальные компьютерные системы».

Сейчас точную последовательность событий того времени восстановить практически невозможно, так как в первые часы вирусной атаки никто

об этом не задумывался, пытаясь максимально уменьшить наносимый ущерб. Плюс к тому часть информации до сих находится в закрытых источниках. Но восстановить общий ход событий вполне реально – при помощи сохранившихся сообщений того времени и более поздних публикаций.

Итак, вечером 2 ноября 1988 года вирус был обнаружен в Корнельском университете, а затем в компьютерных системах Стэнфордского университета, университета в Беркли (штат Калифорния), фирмы Rand Corporation и, потом, ближе к полуночи, в Принстонском университете (штат Нью-Джерси), университетах г. Дэвис и г. Сан-Диего, Ливерморской лаборатории имени Лоуренса, исследовательском центре в Калифорнии. Вирус распространялся по каналам TELNETD, FTPD, FINGER, RSHD, SMTP и атаковал все системы 4.3 BSD, а также Sun 3.x. Тогда ещё никто не мог представить себе, насколько масштабна эпидемия, однако было отмечено, что атаки вируса продолжаются по всей стране. На основании этого факта был сделан вывод, что национальные компьютерные системы атакуются вирусом, распространяющимся через сети, так как только это могло объяснить скорость его распространения. Причём, поведение вредоносной программы было трудно объяснить: в некоторых системах появлялись необычные файлы в директории «/usr/tmp», в электронных журналах некоторых утилит появлялись странные сообщения, а нагрузка на системы возросла так, что заканчивалось выделенное под свопинг[130] свободное место или переполнялась системная таблица процессов с неизбежной последующей блокировкой всей системы. В результате, в ночь со второго на третье ноября практически каждый час приносил всё новые сообщения о заражении компьютерных систем. Всего было инфицировано пятнадцать узлов сети «Arpanet», подключённые к «Arpanet» системы Гарвардского университета (штат Массачусетс), вычислительного центра MIT, университета Карнеги-Меллона (г. Питтсбург, штат Пенсильвания), в котором

[130] Swapping (англ.) – свопинг (проф.), подкачка, обмен: механизм подкачки в оперативную память компьютера затребованной программой недостающей страницы виртуальной памяти.

вышло из строя около 80% компьютеров, астрофизического центра Smithonian и т. д. Ближе к утру вирус замедлил скорость своего распространения, так как было поражено уже более 1000 узлов сети, и она резко снизила свою производительность. Интересно, что нештатную ситуацию в работе систем фиксировал не только технический персонал, но и процессоры самих вычислительных систем. Они стали передавать в сеть сообщения, что вследствие переполнения памяти больше не могут принимать и пересылать данные. Благодаря этому обстоятельству вычислительные центры некоторых организаций и учреждений вовремя отключились от сети и, тем самым, смогли уберечься от инфицирования. В качестве такого примера обычно приводят Технологический институт Стивенса (Stevens Institute of Technology) из штата Нью-Джерси, администрация сети которого, увидев такое предупреждение, успела отключить свою вычислительную технику от сети «Arpanet» и, тем самым, не допустила проникновение вируса в систему.

К сожалению, этот случай – исключение и, в целом, за считанные часы был нанесён существенный ущерб. Вирус распространялся через компьютерную сеть с небывалой для того времени скоростью и, в результате его зловредной деятельности нарушалась работа не только сети, но и других инфицируемых систем, останавливавшаяся, как уже указывалось выше, вследствие переполнения памяти и (или) превышения допустимого предела нагрузки. Причём администраторы систем, зачастую, не могли вмешаться в процесс, так как теряли контроль над перегруженной системой. Впервые столкнулись и с тем, что инфицировалась одна из самых распространённых (благодаря присутствию удобных отладочных средств и электронной почты) версий операционной системы UNIX – Berkeley 4.3 – многопользовательской, с системой защиты, предусматривающей аутентификацию всех пользователей при помощи системы паролей. Таким образом, вирус распространялся по крупнейшим сетям страны, включая и сети оборонного назначения, заражая одну из самых массовых операционных систем. Кроме всего прочего, было неизвестно насколько деструктивен этот вирус, а ведь в случае его

нацеленности на уничтожение или повреждение информации на «жёстких» дисках в заданное время, ущерб мог стать непредсказуемым.

Так или иначе, примерно через шесть часов после начала атаки вирус заразил от 600 до 800, а за второе и третье ноября – примерно 6000 компьютерных систем. Кроме указанных выше в списке пострадавших организаций и учреждений фигурировали: Агентство национальной безопасности США, специальные структуры стратегического авиационного командования США и NASA[131], Лос-Аламосская национальная лаборатория, исследовательские организации ВМС США, а также десятки крупнейших учебных заведений и частных компаний по всей стране. В результате вирус фактически вывел эти сети из строя, и на два дня прекратились все научно-исследовательские работы. Позже стало известно, что вирус вышел за пределы США и через столицу Великобритании, Лондон, стал распространяться дальше[132].

Вместе с тем, хотим подчеркнуть, что специалисты «не сидели сложа руки», и в одном из сообщений, разосланных по электронной почте ещё ночью 3 ноября, уже констатировалось, что электронному нападению подвергаются операционные системы UNIX 4.3 и Sun, работающие на компьютерах производства фирм DEC – VAX, а также Sun Microsystems Inc. – Sun. В том же сообщении впервые указывалось на «уязвимость» в системе безопасности утилиты электронной почты «SendMail», которую использует вирус для своего распространения[133]. Более того, оперативно выполненное исследование

[131] Например: лаборатория реактивных двигателей (Jet Propulsion Laboratory – JPL); вычислительный центр NASA в г. Хьюстон (штат Техас), где компьютерный вирус едва не вывел из строя систему управления пусками космических кораблей многоразового использования проекта «Shuttle», которую удалось своевременно отключить.

[132] Как несколько позднее сообщала ежедневная газета «Уолл-стрит джорнэл», вирус попал в Западную Европу и Австралию, где были отмечены случаи отказа компьютерных систем.

[133] Помимо ошибок в UNIX вирус использовал несколько других оригинальных идей, например, подбор паролей пользователей для входа в системы под чужим именем из списка, содержащего 481 вариант.

позволило предложить следующую схему распространения компьютерного вируса: «Arpanet» – «Milnet» – «Science Internet» – «NSF net». Специалисты Национального центра компьютерной безопасности (National Computer Security Center – NCSC) провели деассемблирование вируса и указали на то, что он «представляет собой незаурядную компьютерную программу, автор которой со знанием дела использует «известные бреши в сети «Arpanet»[134].

Заглянув немного вперёд, можно сказать, что после того как страсти поулеглись, возник вопрос о том, кто же первым обнаружил вирус? На этот вопрос так и не было получено однозначного ответа и каждая из версий имеет право на существование[135], но один ход событий кажется нам наиболее вероятным. Первым появление вируса в ночь со 2 на 3 ноября 1988 года обнаружил сотрудник Ливерморской лаборатории. Соединившись из дома с вычислительной системой своей лаборатории, он увидел, что уровень её загрузки непомерно велик, и сообщил об этом факте дежурному оператору, который, в соответствии с принятым регламентом, отключил систему от сети «Science Internet», по которой распространялся вирус. Об инциденте незамедлительно было сообщено в Управление связи Министерства обороны

---

[134]Деассемблирование и реконструкция текста вируса представляли собой сложную задачу, поскольку автором вируса были предприняты специальные меры по их затруднению, в частности, шифровка текстовых строк. Основная часть работы была выполнена Марком Эйчиным, специалистом по деассемблированию, который одновременно являлся и координатором работы других программистов.

[135] Существует версия, что извещение о появлении вируса было отправлено неизвестным лицом по компьютерной сети вместе с инструкцией по его уничтожению. Но сеть была перегружена, и многие вычислительные центры не сразу приняли сигнал. Когда же, наконец, на сообщение обратили внимание, было поздно.

Другая версия гласит, что первыми обнаружили неполадки в вычислительной системе специалисты MIT. Внимание ответственного за безопасность вычислительного центра привлекло необычное поведение компьютера. Машина интенсивно функционировала, хотя в это время на ней никто не работал, и на экран монитора данные не выводились. Через несколько минут вся память системы была забита, и она вышла из строя.

США (Defence Communication Agency – DCA), в ведении которого находилась сеть «Arpanet». В три часа ночи о вирусной атаке узнало руководство DoD, но, несмотря на оперативную реакцию на угрозу, локализовать вирус в сети было уже невозможно.

Почему именно специалисты Ливерморской лаборатории вполне могли одними из первых обнаружить вирус и поднять тревогу? Просто за полгода до рассматриваемых событий (в мае 1988 года), проводя научные исследования в рамках программы «Стратегической оборонной инициативы» (СОИ) и разработку новых видов ядерного вооружения, они уже имели дело с компьютерным вирусом. После локализации и устранения этой угрозы своим системам в лаборатории был проведён дополнительный инструктаж управленческого и технического персонала, а также проведён комплекс конкретных мероприятий, направленных на повышение эффективности защиты от электронных нападений.

Если в каких-то случаях можно говорить о том, что события «прессуют» время, то развитие истории с «червём» Морриса как раз подходит под это определение. Уже во второй половине дня 3 ноября в MIT даётся первое интервью, посвящённое исключительно этому вирусу. Вечером пользователям разослана программа, предохраняющая их системы от заражения,[136] а затем обнародовано сообщение о способе борьбы с вирусом, состоящем в размещении в библиотеке «C» внешней переменной с именем «please quit», установленной в значение отличное от нуля. Специалисты университета Беркли разработали и разослали программные «заплаты» для всех «брешей» в системном программном обеспечении, позволявших вирусу распространяться, а специалисты университета Пурду примерно в это же время разослали описание методики борьбы с вирусом, не требующей модификации си-

[136] Обратите внимание на название программы: «worm condom» – презерватив от червя, то есть уже к тому времени специалисты абсолютно точно установили, с каким типом вредоносной компьютерной программы они имеют дело.

стемных утилит. Кроме того, рекомендовалось «залатать» предложенным образом обнаруженные промахи в работе утилиты «SendMail».

Такие шаги были предприняты не случайно, а по результатам предварительного анализа, который выявил следующее:

вирус не инфицировал системы, для которых их системные программисты переписали программы, входящие в систему безопасности, с учётом обнаруженных недостатков в промышленных версиях этих программ;

вирус использовал в процессе своего распространения подсистему отладки программ;[137]

вирус был сетевым «червём», поскольку ни одна из существовавших программ в ходе электронного нападения не подверглась каким-либо изменениям.

Сразу после полуночи 4 ноября, университет в Пурду распространил по электронной почте информацию, которая содержала довольно полное описание вируса. Примерно через два часа эта информация была дополнена следующим заявлением: «вирус содержит несколько ошибок, которые могут привести к неприятностям и непредсказуемому поведению программы». Также указывалось, что «если бы даже автор тестировал программу более тщательно, он всё равно не смог бы обнаружить эти ошибки…» Вечером того же дня в специальном сообщении MIT было сделано очень важное заявление о том, что в вирусе не обнаружено деструктивного программного кода, который мог инициировать процедуры искажения или уничтожения файлов на «жёстких» дисках атакуемых им компьютерных систем.[138] Опираясь на эти

---

[137] В результате в профессиональной среде стал использоваться термин: «отладочный хук».

[138] Эта информация MIT подтвердила выводы специалистов из университета Пурду о том, что вредоносная программа является сетевым «червём» и, следовательно, не обладает деструктивными функциями, способными нанести невосполнимый ущерб. Непредсказуемость же поведения данной программы в результате наличия программистских ошибок в её коде не представляла такого уровня опасности, который был бы в случае применения

сведения, пользователи сети «Arpanet» начали формирование специальных групп, для работ по срочной модификации сервисных подпрограмм, корректировке программного обеспечения и массивов данных. Как позднее сообщил директор Национального центра информации о компьютерной преступности в г. Лос-Анджелес (штат Калифорния), мероприятия по ликвидации последствий вирусной атаки только в Лос-Аламосской Национальной лаборатории стоили порядка 250 тыс. долларов. Исследовательский центр NASA в г. Маунтин Вью (штат Калифорния) на два дня – до полного завершения восстановительных работ, отключил от своей сети 52 тысячи пользователей.

Параллельно всей этой деятельности ФБР США проводило собственное расследование, в ходе которого произошедшему инциденту был присвоен «самый высокий приоритет». Этот орган, естественно, в первую очередь интересовал совершенно определенный круг впросов: откуда стал распространяться вирус? кто его написал? как он появился в «диком» виде в сетях? Одной из первых «ниточек», ведущих следствие к автору компьютерного вируса стало небольшое сообщение, опубликованное 4 ноября в газете «Нью-Йорк Таймс». В этом материале под заголовком «Virus in Military Computers Disrupts Systems Nationwide» («Вирус в военных компьютерах разрушает общенациональные системы») Джон Марков писал, что не назвавший себя студент позвонил в редакцию и заявил, что инцидент является всего лишь «опытом, который прошёл неудачно в результате незначительной ошибки в компьютерной программе». Как велось расследование на той стадии – так и не стало достоянием общественности, но известно, что уже 4 ноября ФБР США попросило руководство Корнельского университета об открытии оперативным сотрудникам доступа к рабочим файлам всех научных работников с целью их проверки. Такое разрешение было получено, и все магнитные носители информации в университете были временно изъяты и подвергнуты анали-

---

вирусописателем деструктивных функций. Хотя резкий рост трафика в сетях привёл к значительному ущербу от деятельности «червя».

зу. В итоге проделанной работы был обнаружен файл, содержащий набор слов, использованных в качестве возможных паролей. После этого установить автора вируса не составило большого труда, им оказался Роберт Таппан Моррис-младший[139] двадцати трёх лет от роду. Долго искать его по всей стране не пришлось, так как он сам явился с повинной в штаб-квартиру ФБР США в Вашингтоне, да не один, а в сопровождении адвоката, который заявил, что вирус является «невинной проделкой отечественного гения»[140]. Более того, Моррис выразил горячую заинтересованность в том, чтобы его использовали в работах по блокированию вируса и ликвидации последствий «неудавшегося эксперимента». Его знание собственного творения конечно же было немедленно использовано, но к этому времени специалисты из ведущих научно-исследовательских организаций и сами знали о его вирусе практически всё.

Так что же представлял собой вирус Морриса? Он являлся очень сложной компьютерной программой длиной в 60000 байт[141], разработанной с расчётом на поражение операционных систем UNIX Berkeley 4.3 (или 4.3 BSD) и аналогичных ей операционных систем Sun, работающих на компьютерах фирм Sun Microsystems Inc. (Sun) и Digital Equipment Corp. (DEC). Изначально вирус разрабатывался как безвредный и имел своей целью лишь скрытное проникновение и нахождение необнаруженным в вычислительных системах, связанных с сетью «Arpanet». Компьютерные эксперты, деассемблировавшие вирус, единодушно отметили, что программа была написана с выдающимся

---

[139] О Роберте Моррисе-старшем мы упоминали выше, в связи с созданием в 1962 году электронной игры под названием «Darwin».

[140] Роберт был сыном эксперта по безопасности из National Security Agency и, возможно поэтому, с ранних лет интересовался вопросами защиты компьютеров.

Интересно, что в интервью репортеру одной из американских газет мать Морриса сказала, что роман «The Shockware Rider» Джона Бруннера, о котором мы говорили выше, был одной из наиболее «зачитанных» книг в комнате юного Роберта.

[141] На тот момент это был самый «большой» из всех известных компьютерных вирусов.

мастерством и расчётом на «бреши» в системе безопасности заражаемых операционных систем. Вирус не остался скрытым и полностью безопасным, как задумывал автор, в силу программистских ошибок, допущенных при разработке, которые привели к стремительному неуправляемому саморазмножению – он успел заразить в общей сложности около 6200 компьютеров, что составило примерно десять процентов от их общего числа в сети. Именно это обстоятельство и позволило обнаружить вирус в течение нескольких часов.

Для своего распространения вирус использовал некоторые дефекты стандартного программного обеспечения, установленного на многих эксплуатирующих UNIX системах. Он также использовал механизм, предназначенный для облегчения использования ресурсов удалённым компьютерам, который позволял запускать задачу на удалённой машине для проведения вычислений. Вирус состоял из двух частей: главной программы и программы, обеспечивающей его распространение. Главная программа после запуска на очередном компьютере собирала информацию о других компьютерах в сети, с которыми данный компьютер имел связь. Для этого она проводила анализ конфигурационных файлов при помощи прогона системной утилиты, которая давала информацию о текущем состоянии соединений в сети. Затем главная программа определяла «бреши» программного обеспечения с целью последующей пересылки себя на другие компьютеры.

Сама процедура пересылки выполнялась специальной частью вируса, называемой модулем распространения. Этот модуль представлял собой исходный текст программы, состоящей из 99 строк на языке «С», которые должны были компилироваться и выполняться на удалённой машине. Для этого исходный текст сначала передавался очередному инфицируемому компьютеру, а затем компилировался и выполнялся с использованием трёх аргументов: сетевого адреса компьютера, с которого происходило заражение, количества сетевых портов, которые нужно соединить с этим компьютером для передачи основных файлов вируса и «магического числа», которое использовалось для однократной проверки паспорта. Если инфицирующий компьютер

не получал в ответ от посланного ею модуля распространения это «магическое» число, он отсоединялся от заражаемого компьютера. Это было сделано для предотвращения попыток получения файлов вируса при помощи имитации действий модуля распространения. В состав функций модуля распространения были заложены определённые меры по его маскировке. Для этой цели он обнулял свою командную строку и немедленно создавал собственную копию. Если в процессе пересылки файлов с инфицирующей машины происходил сбой, то модуль распространения сначала удалял все пересланные файлы и только после этого возвращал управление. После запуска на очередном заражаемом компьютере модуль распространения обеспечивал пересылку всех файлов вируса на компьютеры того же типа – Sun или VAX. Каждый файл представлял собой версию вируса для компьютера определённой архитектуры.

Кроме того, модуль распространения обеспечивал создание ещё одной своей копии для рассылки по очередным сетевым адресам. Хотя в модуле распространения и предусматривалась пересылка до двадцати файлов, данной версией вируса на самом деле пересылалось только три файла. Этот факт вызвал предположение, что Моррис не собирался останавливаться на достигнутом, и собирался разработать следующую версию вируса, которая смогла бы пересылать другие командные файлы, паспорта пользователей или другие вирусы для конкретного типа компьютеров. После пересылки загрузочных модулей модуль распространения обеспечивал их сборку с местной версией системной библиотеки, которые поочерёдно вызывались с целью раскрытия паролей пользователей, работающих на данном компьютере. Если попытка заканчивалась успешно, вирус рассылал модуль распространения по всем адресам, найденным в списке уже «взломанного» абонента; если ни один из методов дешифровки паролей не давал результата, то переславший модуль распространения компьютер осуществлял удаление с «жёсткого» диска всех «следов» попытки электронного взлома, то есть созданных в процессе работы вируса файлов.

Итак, поскольку вирус Морриса распространялся с использованием сетевых средств и сам полностью обеспечивал собственную работу, то очевидно можно сделать вывод о том, что он является одним из первых полноценных представителей семейства вредоносных компьютерных программ, которые называются сетевыми «червями».

Сетевой «червь» Морриса положил предел целому этапу почти «беззубого» существования такого явления как вредоносные компьютерные программы. Они становятся всё более сложными и коварными, требуя постоянной разработки и применения новых технологий борьбы с ними. «Эпоха вирусов, не имеющих каких-либо определённых задач или целей, кончается, перед нами – эпоха точно ориентированных вирусов», – сказал в то время старший администратор фирмы бухгалтерских услуг и консалтинга фирмы Delloitte, Haskins & Sells Стивен Росс. Электронная атака сетей «червём» Морриса стала причиной резко возросшего интереса общества к средствам обеспечения безопасности, как вычислительных систем, так и объединяющих эти системы сетей. В частности, инициативной группой компьютерных вирусологов из США, участвовавших в расследовании инцидента с сетевым «червём» Морриса было предложено следующее: должна быть сформирована политика безопасности сетей, включая вопросы уголовного преследования нарушителей, операторы должны начинать уголовное преследование всех лиц, замешанных в атаке на сети, и начать регулярное обучение персонала с акцентом на обеспечение безопасности[142].

Правительственные лаборатории и исследовательские центры, занимавшиеся проблемами защиты информации, стали интенсивнее работать над созданием универсальных антивирусных средств, которые должны выявлять и блокировать угрозу со стороны компьютерных вирусов на самых ранних

[142] Роберт Моррис-старший вообще высказал мнение, что именно этот вирус позволил выявить уязвимые места, и поэтому его сын сыграл «конструктивную роль» и содействовал совершенствованию методов организации компьютерных сетей и управления ими.

стадиях[143]. К работам по борьбе с вирусами и созданию «иммунных» программ подключились Национальный научный фонд США, биржа на Уолл-стрит, другие экономические структуры и политические силы. Беспокойство, например, финансовых кругов США, легко объяснимо тем, что их конкурентоспособность во многом зависела тогда и, тем более, зависит сегодня от вычислительной техники, на базе которой функционирует вся система электронных безналичных расчётов.

После инцидента с сетевым «червём» Морриса, так как вирусные эпидемии в США и странах Западной Европы приобрели масштабый характер, о проблеме вредоносных компьютерных программ стали постоянно писать и серьёзные не компьютерные издания[144]. В репортажах, опубликованных такими ведущими газетами как «Chicago Tribune» и «New York Times» давалось достаточно подробное описание темпов распространения вируса и разработки методов борьбы с ним. Позднее в аналитических статьях и обзорах поднимались наиболее важные проблемы, относящиеся к вопросам безопасности компьютерных систем, выдвигались законодательные инициативы, направленные на предотвращение подобных случаев в будущем. Под влиянием подобных публикаций в палате представителей США было внесено два законопроекта, предусматривающих уголовное наказание за создание и распространение компьютерных вирусов.

Жёсткость предлагаемых для вирусописателей мер пресечения не кажется излишней, если учесть, что по скромным оценкам инцидент с сетевым «червём» Морриса-младшего составил восемь миллионов часов потери до-

---

[143] Однако, по мнению многих экспертов, если такие средства и удастся создать, они вряд ли станут достоянием широкой общественности, так как они будут рассматриваться правительственными структурами различных стран как своего рода «тайное стратегическое оружие».

[144] Даже некоторые советские газеты поместили краткие сообщения, из которых, правда, можно было уяснить только следующую информацию: «компьютерный вирус поразил американские вычислительные сети».

ступа и более миллиона часов прямых потерь, потраченных на восстановление работоспособности компьютерных систем. Общая стоимость всех затрат оценивалась в 98 млн. долл., причём, ущерб был бы неизмеримо больше, если бы автор вируса заложил в своё творение деструктивные функции.

В преддверие неизбежного судебного разбирательства широко обсуждался вопрос о том, как квалифицировать поступок Морриса-младшего, а он сам был отчислен из Корнельского университета с правом подачи заявления на повторное поступление через год, то есть вопрос о его вторичном поступлении был отдан на откуп администрации этого университета. Тем временем Министерство юстиции США дотошно изучало вопрос о возможности привлечения Морриса к суду на основе действующего законодательства[145]. В конце концов, поскольку инфицированные системы входили в состав компьютерной сети, контролируемой правительством США, распространение сетевого «червя» было признано действием, нарушившим закон. Но и после этого оставался неясным вопрос о том, как квалифицировать автора вируса: как преступника или как обычного хулигана. В соответствии с законом от 1986 года[146] в случае квалификации действий Морриса как «несанкционированного доступа к правительственным компьютерам», ему грозил крупный штраф и тюремное заключение сроком до 10 лет.

Только 18 января 1989 года в г. Сиракузы (штат Нью-Йорк) начался судебный процесс. Моррис-младший мог быть приговорен к штрафу в 250 тыс.

---

[145] ФБР США, например, долгое время вообще не могло сформулировать официальное обвинение в отношении автора вируса, несмотря на то, что по заказу этого ведомства были подготовлены подробные обзоры существующего законодательства, касающегося «компьютерных» преступлений. Несмотря на наличие относительно новых законодательных актов выдвинуть обвинение в отношении лица, злоупотребившего многомашинной компьютерной системой, каковой является любая компьютерная сеть, было нелегко. «У нас нет никакого опыта наказаний за такие дела», – заявил представитель ФБР.

[146] «1986 U.S.Computer Fraud and Abuse Act» – «Акт о злоупотреблениях и мошенничестве с помощью компьютеров от 1986 года».

долл. и тюремному заключению сроком до пяти лет. В ходе судебного разбирательства его адвокат утверждал, что тот якобы создал вирус для проведения эксперимента по проверке защиты компьютеров. При этом он действительно допустил ошибку, которая привела к нежелательным результатам, но не стремился нанести ущерб компьютерным системам США. 22 января 1989 года судом присяжных Моррис-младший был признан виновным. Однако его адвокат, Томас Гидобони, сразу заявил протест и направил все бумаги в окружной суд с прошением отклонить решение суда.

4 мая 1990 года суд присяжных вновь признал Морриса-младшего виновным, однако на этот раз он был приговорён лишь к трёхлетнему условному заключению, 40 часам общественных работ (аналог наших пятнадцати суток) и штрафу размером в 10 тыс. долл. Вместе с тем был создан важный прецедент – суд США впервые осудил автора компьютерного вируса, и этот приговор показал, что американское общество начало осознавать опасность растущей компьютерной преступности и предпринимать действенные меры борьбы с ней.

О дальнейшей же судьбе Морриса-младшего переживать не стоит, так как уже в январе 1989 года Рон Грюнер, президент Alliant Computer Systems Corp., в ответ на вопрос журнала ComputerWorld по поводу намерений компании нанять на работу Роберта Таппана Морриса-младшего ответил: «Некоторые очень известные в компьютерной промышленности люди начинали с хакерских проделок в самых изощрённых формах». Занавес!

В декабре 1988 года появился ещё один компьютерный «червь», который был обнаружен в сети DECNet и назван «hi.com». Однако, этот «червь» не мог конкурировать со славой сетевого «червя» Морриса-младшего и так и ушёл в небытие без многостраничных сообщений в печати. Тем более что он представлял собой достаточно типичный образчик «рождественского подарка» и проявлял себя лишь выводом на экран монитора изображения ёлки с

извещением пользователей о том, что им следует: «Stop computing and have a good time at home!!!»[147].

Итак, в результате произошедших в 1988 году событий в качестве главного итога года можно указать на радикальный перелом, который наступил в умонастроении общественности, а также в уделяемом проблеме вредоносных компьютерных программ внимании со стороны средств массовой информации и государственных структур.. Если задача борьбы с компьютерной преступностью и не стала первоочередной наряду с такими «великими» общечеловеческими задачами как решение проблем терроризма и СПИДа, то явно выдвинулась в число наиболее приоритетных и вызывающих глубокое беспокойство во всех странах с развитой информационной инфраструктурой, компьютеризированным обществом, накопившим огромные запасы драгоценных знаний на современных носителях информации.

Тем временем, по данным Промышленной ассоциации по компьютерным вирусам (США) только в 1988 году ей было зафиксировано почти 90 тысяч вирусных атак на персональные компьютеры. На самом деле количество инцидентов, связанных с компьютерными вирусами, вероятно, превосходило опубликованные цифры, поскольку большинство фирм умалчивало об этих инцидентах, опасаясь, что подобная антиреклама повредит их репутации. Другие фирмы молчали, чтобы не привлекать внимания компьютерных преступников.

§9. 1989 год – болгарский «завод» по производству вредоносных программ, вирусы-разрушители, технология «стелс», рождение журнала «Virus Bulletin»

- Выпущена версия 1.2 операционной системы OS/2.
- Фирма IBM выпускает свой первый антивирусный продукт.
- Фирма Intel анонсирует микропроцессор Intel 80486 DX, который стал первым микропроцессором со встроенным математическим сопроцессором (32 разрядный, 1,2 миллиона транзисторов).
- ARPANET официально переименована в Интернет.

---

[147] «Остановить вычислительную технику и хорошо провести время дома!!!»

Наступление 1989 года сопровождалось обсуждением неприятной темы, которая получила красноречивое название «болгарский след», в области разработки и распространения вредоносных компьютерных программ. Факты упрямо свидетельствовали о том, что, начиная с 1988 года, в столице Болгарии, г. София, образовалась очень деятельная группа лиц, которая целенаправленно разрабатывала и затем распространяла компьютерные вирусы, в том числе чрезвычайно деструктивные. Вместе с тем ведущие вирусологи отмечали, что, «возможно, значительная часть деятельности этой группы связана с прямым плагиатом». Например, действительно очень трудно объяснить, зачем программисту-болгарину вставлять в собственную программу мелодию марша «Yankey Doodle» («Янки Дудл»), который испокон века считается американским, и любим в США, да и то не всеми и не везде. Специалисты называли даже имена и место работы отдельных членов данной группы вирусописателей: некоего Владимира Бочева якобы являвшегося автором вируса, использующего мелодию «Yankey Doodle»; В. Бончева, деятельность которого предположительно квалифицировалась как «и вашим и нашим»[148]; перечислялись и сотрудники расположенной в г. София организации под названием ВМЕИ «В. И. Ленин». Мнение большинства ведущих отечественных специалистов по поводу деятельности этой группы выразил Н. Н. Безруков: «Есть основания предполагать, что деятельность болгарской группы нанесла определённый ущерб нашей стране (из упоминаемых В. Бончевым вирусов, якобы разработанных в Болгарии, некоторые близки к распространявшимся у нас вирусам CE1211R, CE1800R, CE1810R, CE2890R), поскольку многие сотни, если не тысячи, часов были потрачены на анализ и дезинфек-

[148] В. Бончев был лично знаком с В. Бочевым, о чём свидетельствовала благодарность последнего в предисловии к пакету распространяемых В. Бончевым антивирусных программ. Кроме того, Бончев в целях саморекламы распространял флоппи-диск, содержащий исходные тексты нескольких компьютерных вирусов, а также опубликовал весьма спорную статью, где всячески пытался запутать проблему ответственности за написание и распространение вирусов.

цию заражённых программ. Причём в наиболее опасном и коварном из упомянутых вирусов – CE1800R явно указано «This program was written in the city of Sofia (C) 1988–89 Dark Avenger».[149] Кроме того, особенности его реализации явно свидетельствуют о хорошем знакомстве с текстом вирусов CE2890R и CE1211R».[150]

Идентификационная карточка вредоносной компьютерной программы	
Имя	DataCrime
Другие названия	Datacrime, 1168, Columbus Day, CE1168
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	март 1989 года
Страна происхождения	Нидерланды
Длина	1168 байт

В марте 1989 года было зарегистрировано появление компьютерного вируса «DataCrime»[151] («Datacrime», «1168», «Columbus Day»,[152] «CE1168»), родоначальник одноимённого семейства вирусов, который посеял настоящую панику в средствах массовой информации некоторых западноевропейских стран, в первую очередь, Нидерландов и Великобритании, а также США и Японии.

---

[149] «This program was written in the city of Sofia (C) 1988–89 Dark Avenger» (англ.) – «Эта программа была написана в городе София (C) 1988–89 Тайный мститель».

[150] Безруков Н. Н. Компьютерная вирусология. Киев, 1990.

[151] «DataCrime» (англ.) – можно перевести как: «Информационное правонарушение» или «Информационное злодеяние». Первое сообщение об этом вирусе поступило от Фреда Фогеля из Нидерландов и, судя по выдаваемой вирусом надписи («DATACRIME VIRUS» «RELEASED: 1 MARCH 1989»), время разработки относится к самому началу 1989 года, а дата начала распространения к 1 марта 1989 года.

[152] «Columbus Day» (англ.) – День Колумба. Такое название вируса объясняется тем, что сведения о «DataCrime», перепечатанные многими изданиями, привели к искажению механизма его действия, и некоторые издания США сделали собственное, ложное предположение о том, что он написан норвежскими кибертеррористами, пытавшимися отомстить за то, что первооткрывателем Америки считается Колумб, а не норвежский конунг Эрик Рыжий.

Надо сказать, что для беспокойства имелись основания, так как вирусы семейства «DataCrime» имели крайне опасное проявление. Они были запрограммированы таким образом, что с 1 апреля до 13 октября 1989 года вели латентный «образ жизни» размножаясь на компьютерных системах, но, начиная с этой даты и до 31 декабря, инициировали процедуру разрушения файловой системы, форматируя «жёсткий» диск компьютера, что могло привести, и приводило к безвозвратной потере данных.[153]

Так что же это было? Данный вирус являлся нерезидентным файловым вирусом, заражающим файлы с расширением «*.com». При заражении компьютерной системы он дописывал себя в конец этих файлов, увеличивая их длину на 1168 байтов, и заменял пять первых байтов заражённой программы на команду перехода к началу вируса. Вирус размножался с 1 апреля по 12 октября любого года, а до этого (с 1 января по 1 апреля, начиная с 1990 года) при запуске заражённых файлов, маскируясь, сразу же передавал управление вирусоносителю и никак не проявлял себя в инфицированной компьютерной системе. Затем опять следовала активизация деструктивных функций и т.д. Сама стратегия размножения была основана на просмотре корневого каталога, а затем и остальных каталогов и подкаталогов на «жёстком» диске с последующим заражением всех найденных файлов с расширением «*.com», кроме тех, которые имели в качестве седьмой буквы имени латинскую букву «D»[154]. Если «DataCrime» не обнаруживал файлы-жертвы на логических дисках компьютера, то он последовательно просматривал дисководы флоппи-дисков, сначала A:, а затем B:. Из-за нескольких ошибок, допущенных авто-

---

[153] Таким образом, автор вируса применил приём, при котором фаза его распространения отделялась от фазы реального проявления периодом, продолжительностью в несколько месяцев. Это давало возможность незаметного для пользователей инфицирования как можно большего количества компьютеров. Однако первые случаи заражения были отмечены в Нидерландах практически сразу, а в США датируются началом июня 1989 года.

[154] Следовательно «DataCrime», также как и другие представители этого семейства, не заражал файл «command.com».

ром в программном коде, вирус инфицировал не все файлы, создавая у пользователя впечатление случайного выбора и иногда вызывал зависание системы в процессе её заражения. При запуске на выполнение инфицированного «DataCrime» файла после 12 октября любого года вирус выдавал зашифрованное в своём теле сообщение «DATACRIME VIRUS» «RELEASED: 1 MARCH 1989» («Вирус DataCrime» «Выпущен: 1 марта 1989 года»)[155] и выполнял низкоуровневое форматирование «жёсткого» диска.[156] Он форматировал первые восемь дорожек нулевого цилиндра диска C:, уничтожая MBR, загрузочный сектор, FAT и главный каталог. После этого вирус входил в бесконечный цикл, выдавая звуковой сигнал (символ «Bell»).

В последующие восемь месяцев, вслед за родоначальником, появились штаммы.[157]

---

[155] Тело вируса в целом не шифровалось, но содержащееся в нём текстовое сообщение было зашифровано с помощью команды XOR, и дешифровка выполнялась перед выдачей сообщения на экран монитора, то есть непосредственно перед срабатыванием троянской компоненты вируса.

[156] На IBM совместимых компьютерах типа PC/AT, а также системах с установленными контроллерами типа RLL или SCSI алгоритм запуска низкоуровневого форматирования не работал.

[157] «DataCrime-B» («1280», «Columbus Day», «CE1280») – обнаружен в апреле 1989 года в Нидерландах, длина 1280 байт. Этот вирус отличался от «прародителя» длиной, а также тем, что вместо файлов с расширением «*.com» заражал файлы с расширением «*.exe». Кроме того, он «научился» форматировать «жёсткий» диск с установленными контроллерами типа RLL или MFM;

«DataCrime II» («1514», «Columbus Day», «CE1514») – обнаружен в сентябре 1989 года в Нидерландах, длина 1514 байт. Этот вирус отличался от предыдущих версий длиной, а также тем, что инфицировал как файлы с расширением «*.com» (в том числе файл «command.com»), так и файлы с расширением «*.exe». Кроме того, у этого вируса было зашифровано всё тело, и он не форматировал «жёсткие» диски по понедельникам;

«Datacrime IIB» («1917», «Columbus Day», «CE1917») – обнаружен Яном Терпстра в ноябре 1989 года в Нидерландах, длина 1917 байт. Данный вирус отличался от предыдущей

Как мы видим, угроза была весьма реальной, и в Нидерландах местная полиция доступными ей методами активизировала борьбу с компьютерной преступностью. Кроме проведения оперативных мероприятий была заказана целевая разработка специальной антивирусной программы, которая могла нейтрализовать «DataCrime», после завершения которой полиция организовала её продажу непосредственно в своих участках по цене одного доллара США. Этот антивирус пользовался большой популярностью, но работал недостаточно надёжно и вызывал большое количество ложных предупреждений о наличии в компьютерной системе «DataCrime». Поэтому была выпущена вторая версия антивируса, которая, впрочем, тоже не могла похвастаться безупречной работой[158]. Тем временем, семейство компьютерных вирусов «DataCrime» из Нидерландов, где по некоторым (скорее всего завышенным) оценкам к сентябрю 1989 года было инфицировано до ста тысяч персональных компьютеров, что составляло около 10% от всего парка в стране, перекочевало в другие страны Западной Европы, а также США и Японию.

Ближе к «роковой» дате 13 октября последовала новая волна публикаций, посвящённых вирусу «DataCrime». Например, 17 сентября 1989 года в газете «Washington Post» появилось сообщение, в котором говорилось: «Компьютерный вирус, который может явиться источником деструктивных действий 13 числа в пятницу, выпущен на свободу, и через стан компьютерных пользователей прокатилась волна беспорядочных действий по защите от него своих компьютеров». На самом деле в подобных сообщениях, зачастую, описывались два разных компьютерных вируса – «DataCrime» и знаменитый «Jerusalem», который запускался 13 числа в пятницу, а в том году в октябре

версии длиной, а также тем, что во избежание обнаружения у него был изменён метод шифрования тела.

[158] Фирма IBM также оперативно отреагировала на угрозу, выпустив свой детектор «VIRSCAN», позволявший искать характерные для того или иного вируса строки (сигнатуры) в файловой системе. Причём, пользователю предоставлялась возможность самостоятельного пополнения или изменения этого набора.

13 число падало как раз на пятницу. Между тем, сообщения печати продолжали пугать обычных пользователей: «… приблизительно в День Колумба компьютерный вирус атакует MS-DOS сети», – «Federal Computer Week» от 28 августа, «Эксперты предупреждают о вирусе «DataCrime». План профилактики», – «PC Week» от 11 сентября; «NIST опасается вирусного нападения сразу после праздников», – «Government Computer News» от 2 октября; «Пятница 13-тое: вирус подкрадывается», – «New York Times» от 8 октября. После «критической» даты 13 октября, когда выяснилось, что «DataCrime» получил сравнительно небольшое распространение, тон публикаций резко изменился: «Компьютерный вирус не даёт повода для бессонницы», – «Wall Street Journal» от 13 октября; ««DataCrime» терпит фиаско в Соединённых Штатах», – «Newsbytes» от 17 октября.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Disk Killer
Другие названия	Ogre, Computer Ogre, Disk Ogre, Bx3EB
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	апрель 1989 года
Страна происхождения	Тайвань
Длина	512 байт

Несмотря на то, что появление вируса «DataCrime» вызвало неадекватную реакцию, переходящую порой все разумные границы – иные события просто были отодвинуты на второй план, она явилась как бы подготовкой к скорому появлению нескольких неординарных компьютерных вирусов, и первым из них стал обнаруженный в апреле 1989 года в г. Милпайтас (штат Калифорния, США) «Disk Killer».[159]

Компьютерный вирус «Disk Killer»,[160] также известный под названиями («Ogre», Computer Ogre, Disk Ogre),[161] был загрузочным и мог проявлять себя

[159] В СССР этот вирус попал в следующем, 1990 году.

[160] «Disk Killer» (англ.) – «Убийца диска».

[161] «Ogre» (англ.) – «Страшила». В сказках великан-людоед; также страшный человек или предмет.

крайне разрушительно. Подобно, к примеру, вирусу «Ping Pong», он заражал загрузочные сектора флоппи-дисков и операционной системы MS-DOS на «жёстких» дисках. Во время загрузки компьютера с инфицированного флоппи-диска или «жёсткого» диска «Disk Killer» загружал себя в память и затем заражал любой флоппи-диск или «жёсткий» диск, с которого позже производилась операция считывания данных (до тех пор, пока не будет произведена перезагрузка системы или компьютер не будет отключён от источника питания).

Вирус вёл подсчёт времени использования «жёсткого» диска с момента заражения компьютера и активизировался после достижения определённого значения (примерно 48 часов). Обычно это означает несколько недель с момента заражения, – в зависимости от интенсивности использования компьютера. Другими словами, если заражённый компьютер оставить в рабочем состоянии примерно на 48 часов подряд, последующая попытка считывания данных с «жёсткого» диска или флоппи-диска послужит причиной появления на экране монитора следующего сообщения: «Disk Killer» – Version 1.00 by COMPUTER OGRE[162] 04/01/1989. Warning! Don't turn off the power or remove the diskette while Disk Killer is processing! PROCESSING Now you can turn off the power. I wish you luck» («Disk Killer» – Версия 1.00 Компьютерное пугало 04/01/1989. Внимание! Не отключайте питание и не вынимайте дискету пока «Disk Killer» обрабатывает данные! ОБРАБОТКА ДАННЫХ А теперь вы можете выключить питание. Я желаю вам удачи»). После этого все данные на флоппи-диске или «жёстком» диске, с которого осуществлялась последняя загрузка системы, повреждались и становились недоступными для пользователя,[163] так как поверх них вирусом прописывался определённый символ.

«Computer Ogre» (англ.) – «Компьютерное пугало».

«Disk Ogre» (англ.) – «Пожиратель дисков».

[162] Отсюда и произошли некоторые из названий вируса «Disk Killer».

[163] Штаммы вируса «Disk Killer» отличаются друг от друга незначительными деталями условий активизации.

Если компьютер выключался немедленно после того, как впервые появлялось это сообщение, данные могли остаться без изменений. С другой стороны, если процессу дать возможность завершиться полностью, потом можно было восстановить данные при помощи программ, специально разработанных для их обратной расшифровки на «жёстких» дисках, поражённых вирусом «Disk-Killer»[164]. Однако бесспорно, что лучшее решение проблем, связанных с деятельностью «Disk-Killer», это его обнаружение и нейтрализация ещё до того, как он получит возможность активизации.

Специфика распространения вируса «Disk Killer» очень схожа с характерными чертами распространения вирусов «Stoned» и «Ping Pong»: данный вирус конфликтовал с драйверами дискет, поддерживающих нестандартные форматы (например, 720 Кб). Наличие программной ошибки в «Disk Killer» иногда приводило к тому, что он не мог инфицировать флоппи-диски и иногда происходил отказ системы при загрузке. Попытки форматирования флоппи-дисков в инфицированном компьютере также, время от времени, приводили к отказу системы. Заражённые «жёсткие» диски и флоппи-диски могли показывать дефектные сектора и уменьшать количество общей памяти, если использовались утилиты DOS, предназначенные для проверки дисков. Все эти симптомы могли быть замечены визуально и, если они наблюдались, то пользователи могли применить антивирусное средство, которое способно провести проверку системы на присутствие вируса «Disk Killer».

Заметим, что вирус «Disk Killer» был своевременно и достаточно хорошо изучен. Его выявление, блокировка, а также уничтожение в системе при помощи антивирусных средств не отнимали много времени как раз по той причине, что он потенциально очень деструктивен и, следовательно, опасен для компьютерных систем. Зная о возможности весьма разрушительных последствий деятельности этого вируса, специалисты и пользователи прило-

[164] Вирус кодирует сектора, выполняя операцию «XOR» со значениями: 0AAAAh и 05555h. Как известно, операция «XOR» обратима, поэтому и возможно восстановление перекодированной информации.

жили большие усилия для успешной борьбы с «Disk Killer». В итоге по настоящему опасный вирус не получил широкого распространения в мире, как это бывало не раз.

Пока разгоралась борьба с вирусом «Disk Killer» руководители антивирусной компании Sophos (Великобритания) Э. Уайлдинг, П. Лэймер и Я. Храске в апреле того же 1989 года задумали и осуществили амбициозный проект, который привёл к созданию независимого издания, содержащего тщательно выверенную информацию о вредоносных компьютерных программах – журнала «Virus Bulletin»[165]. Основным принципом этого издания был заявлен профессиональный подход в освещении проблемы антивирусной защиты и достоверность публикуемых в нём материалов. С тех пор и до настоящего времени авторами материалов и членами редакционного совета «Virus Bulletin» являются известные специалисты, которые представляют собой ведущие фирмы-производители антивирусных продуктов.

В мае общественным достоянием стало сообщение из Китая о первом инциденте, связанном с компьютерным вирусом, который произошёл в этой стране. 25 мая 1989 года в газете «Цзиньцзи жибао» появилась довольно скудная информация о первом случае заражения компьютерными вирусами китайских ЭВМ, которое произошло в апреле 1989 года. Сообщалось, что компьютеры алюминиевого завода Синань были заражены вирусом по имени «Chlorella».[166] За год компьютерный вирус распространился по всей огромной стране и ситуация приобрела настолько неуправляемый характер, что в конце 1989 года была проведена профилактическая проверка 12750 тысяч компьютеров. По результатам этой проверки было установлено, что почти пятая часть из них инфицирована вирусом «Chlorella». Причём специалисты предположили, что всего в Китае на тот момент было заражено никак не меньше шести тысяч электронно-вычислительных машин. По подсчётам ве-

[165] Первый номер журнала «Virus Bulletin» вышел в июле 1989 года.

[166] «Chlorella» (англ.) – «Хлорелла», другое название – «Spots» («Пятна»). В России этот вирус распространения не получил.

домств государственной безопасности Китая, в стране циркулировало никак не меньше 18 видов компьютерных вирусов, семь из которых были зарубежного происхождения. Кроме «хлореллы», в «диком» виде существовали: обладающий разрушительным действием вирус «джута» («новозеландский»), «пакистанский», «дождевые капли», музыкальные вирусы, исполняющие в 17.00 мелодию, а также некоторые другие. Появление компьютерных вирусов, угрожающих информационным системам в Китае, заставило правительство предпринять контрмеры, и в июле 1989 года Госсовет КНР поручил Министерству государственной безопасности Китая руководство борьбой с заражением компьютеров.

Начало осени было отмечено одной из первых успешных попыток объединения ведущих специалистов и крупных пользователей из разных стран для совместной борьбы с вредоносными компьютерными программами. В сентябре 1989 года журналом «Virus Bulletin» была организована и проведена первая международная конференция по указанной тематике, которая, затем, приобрела статус ежегодной. Эти конференции способствовали интенсификации обмена научными знаниями и практическим опытом между ведущими разработчиками антивирусных средств, содействовали сближению позиций в области борьбы с компьютерной преступностью, помогали систематизации результатов проводимых исследований в сфере компьютерной вирусологии. Пользователи, в свою очередь, становились более осведомлёнными о состоянии проблемы, инновационных подходах к её решению, основных тенденциях совершенствования антивирусных аппаратно-программных продуктов и т. п.

В сентябре на рынок выходит еще одна антивирусная программа – IBM Anti-Virus.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Dark Avenger
Другие названия	DarkAvenger.1800, Avenger, Black Avenger, Eddie, Diana, Sofia, Dark Avenger virus, RCE1800
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	сентябрь 1989 года
Страна происхождения	Болгария
Длина	1800 байт

И в том же сентябре, в Болгарии, создан первый вирус «Dark Avenger»[167] (довольно часто называемый «Dark Avenger.1800», «Black Avenger»,[168] «Eddie»,[169] «Diana»[170] или «Sofia»[171]), рассчитанный на противодействие антивирусному программному обеспечению и заражающий файлы в то время, когда антивирусная программа проверяла жёсткий диск компьютера. Код вируса свидетельствовал о глубоком знании его разработчиком MS-DOS, так как в нём был заложен ряд нетривиальных методов маскировки и обхода резидентных сторожей.

Например, при старте любой программы «Dark Avenger» помечал программный сегмент как последний и становился невидимым для этой программы, а по окончании работы программы помечал программный сегмент как не последний. При завершении программы «Dark Avenger» восстанавливал первоначальное значение прерывания INT 21h, если оно было изменено программой, то есть вставив себя первым в цепочку программ, получающих управление по прерыванию INT 21h, в дальнейшем он не позволял програм-

---

[167] «Dark Avenger» (англ.) – «Тайный мститель». Ранее мы с ним уже встречались как с автором вируса «CE1800R».

[168] «Black Avenger» (англ.) – «Чёрный мститель».

[169] «Eddie» (англ.) – «Эдди», уменьшительное от имени Эдвард, Эдуард.

[170] «Diana» (англ.) – «Диана», это название связано с тем, что в теле вируса содержится строка «Diana P».

[171] «Sofia» (англ.) – «София», это имя, естественно, происходит от названия столицы Болгарии.

мам встать раньше него в указанном списке. Этот метод «всплытия» позволял обойти простейших резидентных сторожей. «Dark Avenger» обходил контроль программ, следящих за прерыванием INT 13h, определяя значение этого вектора при инсталляции и, в дальнейшем, напрямую обращаясь по соответствующему адресу.

Компьютерный вирус «Dark Avenger» обладал, пожалуй, наиболее изощрённой разрушительной силой из числа всех выше описанных вирусов. Подобно многим другим рассмотренным нами файловым вирусам «Dark Avenger» загружался в память компьютера сразу же после запуска на выполнение инфицированного файла и оставался там до следующей перезагрузки системы или отключения питания. Этот вирус инфицировал не только те файлы, которые запускались на исполнение, но, также и те, которые открыты для чтения или записи, переименования, или оперирования с ними в каких-то других целях (прерывания 214Bh, 213Ch, 215Bh, 2156h, 213Dh, 212h)[172]. Такая стратегия размножения делала этот вирус очень опасным, поскольку, если в заражённой системе запустить программу, систематически просматривающую файлы во всех подкаталогах (например, ревизор), то большая часть файлов с расширением «*.com» и «*.exe» будет в результате заражена.

При запуске заражённой программы вирус сначала проверял наличие в оперативной памяти своей копии. При этом копия проверялась полностью, и в случае обнаружения изменений с этого места в память записывался исходный код вируса, что существенно затрудняло его нейтрализацию в оперативной памяти. Если вирус не находил в оперативной памяти своей копии, то он загружался в верхнюю область системной памяти, а затем резервировал для себя участок памяти при помощи манипуляций с MCB[173] и использования некоторых служебных функций операционной системы MS-DOS (выделения,

---

[172] Фактически данный вирус был первым вирусом, который мог уничтожать информацию в базах данных, а не только выполняемые файлы, и некоторые организации серьёзно пострадали в результате повреждения вирусом «Dark Avenger» их баз данных.

[173] MCB (Memory Control Block) (англ.) – блок управления памятью.

освобождения и изменения размеров выделенной памяти). При загрузке в старшие адреса оперативной памяти вирус стирал транзитную часть «command.com», поэтому при первой же команде с консоли транзитная часть вызывалась повторно, что и приводило к её заражению.

На фазе инсталляции вирус определял расположение в постоянном запоминающем устройстве (ПЗУ) обработчика прерывания INT 13h как для флоппи-диска, так и для «жёсткого» диска. Все необходимые сведения для этой цели он брал из векторов 40h и 41h, где содержатся, соответственно, адрес обработчика прерывания INT 13h в ПЗУ и адрес таблицы параметров для «жёсткого» диска. Алгоритм определения адреса прерывания INT 13 в ПЗУ, используемый вирусом не универсален и он работает не для всех типов IBM совместимых компьютеров. Помимо прерывания INT 13h, вирус перехватывал прерывания INT 21h и INT 27h. Прерывание INT 21h используется стандартным образом (отслеживаются приведённые выше подфункции), а прерыванием INT 27h вирус пользовался для того, чтобы проверять, не изменился ли вектор 21h, и при необходимости восстанавливать его. Вирус был работоспособен на версиях 3.x и 4.x MS-DOS. Проверка номера версии в теле вируса не выполнялась. Заражённые файлы с расширением «*.com» увеличивались в размере на 1800 байт, причём дата их создания и атрибуты оставались неизменными. Заражение выполнялось однократно. При заражении вирус дописывал своё тело в конец файла, вставляя в первые три байта команду перехода на начало вируса. Выравнивание на границу параграфа для файлов расширением «*.com» не выполнялось. Инфицировались файлы расширением «*.com» длиной от 1775 (6Fh) до 63148 (F6ACh) байт. Именно поэтому «command.com» была наиболее подверженной заражению этим вирусом программой. Заражение файлов с расширением «*.exe» выполнялось практически стандартно, за исключением того, что вирус не сохранял в своём теле исходной длины заражаемого файла. Однако восстановление длины программы было возможно, поскольку вирус запоминал в своём теле вполне конкретный байт. При заражении файлов с расширением «*.exe» вирус дописывался в ко-

нец файла с выравниванием на границу параграфа. Инфицировались файлы с расширением «*.exe» длиной больше 1775 (6Fh) байт. Помимо файлов с расширением «*.com» и «*.exe», вирус иногда заражал файлы данных.

Вирус «Dark Avenger» мог распространяться посредством тех же самых каналов, что и вирус «Jerusalem», но, так как «он заражал файлы при более широком спектре ситуаций, чем вирус «Jerusalem»», он мог распространяться внутри отдельно взятого компьютера очень быстро. Любая операция (такая как, например, подготовка резервных копий, поиск дисков и т. п.), которая открывает множество файлов, могла распространять вирус с очень высокой скоростью на многие программы на заражённом компьютере. Это обстоятельство, с одной стороны, увеличивало вероятность распространения вируса на другие компьютеры, но, с другой стороны, поднимало шансы на его обнаружение (поскольку вирусом изменялось большое количество файлов).

Фаза проявления данного вируса связана с разрушением определённых секторов винчестера. Примерно на каждый шестнадцатый запуск инфицированной программы «Dark Avenger» перезаписывал в первые байты произвольно взятого сектора «жёсткого» диска сообщение с довольно длинным текстом, которое начиналось со слов: «Eddie lives...» («Эдди живёт ...»), которое являлось частью его тела[174].

Симптомы присутствия «Dark Avenger», из числа тех, которые можно заметить без применения антивирусных средств, следующие: рост размера файлов, периодическое появление внутри файлов сообщения «Эдди существует ...» и общее нарушение нормальной работы системы (вызванное наложением программ с приведённым фрагментом сообщения вируса). Тем не менее, эти симптомы могли пройти незамеченными или некоторое время списываться на счёт неисправностей аппаратной части, особенно, если «жёсткий» диск был не слишком сильно наполнен информацией (так как то-

[174] В Москве получил распространение штамм вируса, в котором сообщение «Eddie lives …» было изменено на «B O R O D A мстит во времени».

гда, чаще всего, будут перезаписываться неиспользуемые сектора). Поскольку вирус «Dark Avenger» записывает своё сообщение в случайно взятые сектора на «жёстком» диске, приведение инфицированной им системы в нормальное состояние может стать очень утомительным процессом: каждый файл на «жёстком» диске и флоппи-дисках должен быть проверен на наличие сообщения вируса (естественно, что все файлы должны быть проверены и на наличие самого вируса), а также восстановлен в первоначальном состоянии, если он был повреждён. Подчеркнём, что в том случае, если антивирусная программа не умела распознавать и бороться с «Dark Avenger», то она становилась «катализатором» распространения этого вируса. Ведь программы-антивирусы открывают множество файлов для просмотра в то время, как вирус уже находиться в памяти компьютера.

Итак, давайте подведём итог. «Dark Avenger» представлял собой компьютерный вирус, который, в отличие от «DataCrime», действительно мог стать всемирной угрозой. Этот компьютерный вирус обладал двумя основными малоприятными особенностями. Во-первых, «Dark Avenger» был преднамеренно разработан так, чтобы он мог медленно, но неуклонно действуя, скрытно и коварно разрушить компьютерную систему раньше, чем станет очевидным его присутствие. Именно в этих целях «Dark Avenger» был наделён способностью хаотичной записи ненужных данных (электронного мусора) в сектора «жёсткого» диска. Таким образом, разрушительный процесс мог проходить практически незамеченным, а повреждаемые файлы, в свою очередь, могли устроить в инфицированном компьютере настоящий «затор». Во-вторых, «Dark Avenger» мог достаточно быстро разносить инфекцию. До этого резидентные вирусы заражали компьютерные программы только по мере того, как их запускали на выполнение. «Dark Avenger» мог инфицировать программы и в том случае, если они были просто открыты

Появление «Dark Avenger» явилось как бы предвестником грядущего обострения войны вирусописателей и компьютерных вирусов против антивирусных средств, их разработчиков и пользователей. Недаром в печати, и в

частности, в «PC Week» от 25 декабря 1989 года, компьютерному вирусу «Dark Avenger» дана такая характеристика: «… способен стать причиной разорения фирмы по разработке и продаже программного обеспечения».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Yankee Doodle
Другие названия	TP44VIR, Five O'clock Virus, RCE2885, Yankee Doodle2C, Летучий Голландец, Музыкальный
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	сентябрь 1989 года
Страна происхождения	Болгария
Длина	2899 байт

30 сентября 1989 года в столице Австрии, г. Вена, компьютер вдруг взял да и исполнил заокеанскую мелодию «Yankee Doodle»[175], а чуть позже тот же мотив прозвучал в Болгарии, где он стал известен под именем «TP44VIR». Сразу стало ясно – это новый компьютерный вирус, немного позже разобрались и поняли – не один, а целое семейство и опять из Болгарии. «Yankee Doodle» стал первым вирусом, играющим мелодию при запуске заражённого файла.

Этот вирус являлся файловым нерезидентным в оперативной памяти вирусом, инфицировавшим файлы с расширениями «*.com» и «*.exe». Заражение файлов выполнялось однократно и происходило при запуске на выполнение соответствующих программ, а инфицирование командного процессора «command.com» осуществлялось сразу после инсталляции вируса в верхние адреса свободной оперативной памяти. Причём работоспособность вируса не зависела от версии MS-DOS, так как проверка номера версии операционной системы в теле вируса не выполнялась. «Yankee Doodle» перехватывал прерывания INT 1, 3, 1Ch, 21h. При заражении файлов с расширением «*.com» вирус дописывал своё тело в конец файла, вставляя в первые три байта команду перехода на начало вируса, а при заражении файлов с расши-

[175] Впервые обнаружен австрийцем Александром Холи, а описан болгарином В. Бончевым под названием TP44. Кстати, фамилия автора вируса – В. Бочев, стала известна из исходного текста вируса, который попал в СССР на флоппи-диске В. Бончева.

рением «*.exe» он дописывал своё тело в конец файла с выравниванием начала вируса на границу параграфа. При инсталляции «Yankee Doodle» проверял длину исходного файла, восстанавливал истинный стартовый адрес программы и проверял наличие своей копии в памяти компьютера. Если компьютер не был заражён или был, но более ранней версией[176], то «Yankee Doodle» копировал себя в область памяти либо сразу за телом программы, либо в выделенную функцией «ALLOC» (2148h) и оставался резидентным в памяти, перехватывая прерывания 21h, 1Ch и 09h. Вирус также осуществлял проверку того, откуда загружается файл, – с защищённого флоппи-диска или нет, – и поэтому не чинил препятствий загрузке любого файла с расширением «*.com» с защищённого флоппи-диска. Интересно, что резидентная часть вируса не обнаруживалась при просмотре списка резидентных программ с помощью специальных утилит и, кроме того, он обходил контроль резидентных фильтров, следящих за записью в программные файлы.

После инсталляции в память «Yankee Doodle» в 17 часов (если быть абсолютно точными, в 16:59:53) с вероятностью 1/8 через системный динамик начинал проигрывать «Янки Дудль Дэнди». При этом никаких разрушений или операций по манипуляции с данными вирус не выполнял. Вместе с тем отметим, что «Yankee Doodle» имел многочисленные штаммы, некоторые из которых были запрограммированы, например, на поиск и модификацию других вирусов [177].

---

[176] При заражении файлов, уже инфицированных предыдущими версиями «Yankee Doodle», сначала производилось «выкусывание» программного кода более старой версии, а затем они опять заражались, теперь новым штаммом.

[177] Приведём некоторые из известных версий «Yankee Doodle».

«TP33VIR» – блокировал прерывания INT 1, 3 и таким способом мешал выделить его с помощью программ отладки.

«TP34VIR» – похож на «TP33VIR», но он резидентный в оперативной памяти.

«TP38VIR» – в данном штамме была добавлена логика, обеспечивающая обход фильтров, перехватывающих прерывание INT 21. Кроме того, именно с этой версии наблюдается

1 октября 1989 года в г. Хайфа (Израиль) был обнаружен «прославившийся» впоследствии компьютерный вирус[178]. Им стал «Frodo»[179], который стал первым в мире абсолютно полноценным файловым вирусом-невидимкой («стелс» вирус). Он представлял большую опасность из-за довольно скрытого характера распространения, а также из-за проявлений, похожих на сбои оборудования, и был разработан с целью повреждения «жёсткого» диска, если его задействуют 22 сентября любого года или после этой даты. Однако, в выявленных образцах «Frodo» содержалась ошибка, благодаря которой при попытке вывода на экран сообщения «FRODO LIVES»

эффект «самоизлечения» заражённой программы при попытке трассировки её на инфицированном вирусом компьютере.

«TP41VIR» – программный код вируса практически полностью совпадает с кодом «TP38VIR», но имеет длину в 2932 байта.

«TP42VIR» – был вариантом вируса «Vacsina» («Вакцина») и проверял систему на предмет инфицирования вирусом «Ping Pong». В случае обнаружения вируса «Ping Pong» он пытался заблокировать этот вирус, а потом изменял программный код таким образом, чтобы он уничтожил сам себя после выполнения 100 инфицирований.

«TP45VIR» – практически аналог вируса «Yankee Doodle» («TP44VIR»).

«TP46VIR» – похож на «TP45VIR», но мог определять в системе наличие вируса «Cascade», а затем уничтожать его.

«Yankee Doodle-B» – очень похож на родоначальника, за исключением длины в 2772 байта.

[178] В СССР этот вирус обнаружен Д. Н. Лозинским в августе 1990 года.

[179] Название «Фродо» связано с тем, что вирус содержит в своём коде загрузочный сектор. При записи этого загрузочного сектора в загрузочный сектор флоппи-диска и попытке загрузки выдаётся текст «FRODO LIVES» («Фродо живёт»), выполненный буквами, состоящими из символов псевдографики. Кроме того, 22 сентября это день рождения героев известной трилогии Дж. Р. Толкиена «Lord Of The Rings» («Властелин колец») – Фродо и Бильбо Баггин (Frodo and Bilbo Baggin).

Существует штамм «4096B», аналогичный «Frodo», но использующий шифровку своего тела.

(«Фродо существует»), он, обычно, просто-напросто «подвешивал» систему. Но обо всём по порядку.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Frodo
Другие названия	Frodo.Frodo, 4K, Frodo.4096, 4096, IDF Virus, Israeli Defence Forces, Century Virus, Frodo, Stealth Hiding, Virus, 100 years Virus, RCE04096
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	октябрь 1989 года
Страна происхождения	Израиль
Длина	4096 байтов

Формально данный вирус относится к файловым резидентным вирусам и при запуске на выполнение или закрытии файла (функции 214B и 213E) заражал файлы с расширениями «*.com» и «*.exe» (включая оверлеи), а также обладал способностью заражения файлов данных. Файлы инфицировались один раз, и признаком заражения служило значение поля года даты создания файла – у заражённых файлов «Frodo» изменял поле года создания файла, увеличивая его на сто, например с 1989 до 2089 и это значение использовалось позднее для определения инфицированных файлов. Вирус заражал файлы с расширением «*.com» длиной до 61440 (F000h) байт и во время заражения изменял первые шесть байтов файла. При этом приращение длины файла составляло точно 4096 байт. Инфицируемые «Frodo» файлы с расширением «*.exe» могли иметь любую длину, и при их заражении изменялся заголовок. Тело вируса дописывалось в хвост файла, а длина файла с расширением «*.exe» увеличивалась ровно на 4096 байт.

При инфицировании системы вирус находил и заражал «command.com»[180], а затем загружал себя в старшие адреса памяти, уменьшая её размер на 6 Кб, при этом он пытался замаскировать это уменьшение. Для определения положения обработчиков прерываний INT 13 и 21 «Frodo» про-

[180] Командный процессор «command.com» заражался как обычный файл с расширением «*.com».

ходил при инсталляции соответствующую часть кода с флагом трассировки. Для получения управления по прерыванию INT 21 вирус использовал так называемый «сплайсинг»[181]. Тело вируса располагалось в старших адресах оперативной памяти, но в дальнейшем его положение могло изменяться, так как вирус перемещал его в область младших адресов. «Frodo» обрабатывал двадцать функций MS-DOS («Create», «FindFirst», «FindNext», «Read», «Write», «Lseek», «Open», «Close», «Exec» и некоторые другие)[182]. При наличии вируса в оперативной памяти приращение длины заражённых файлов маскировалось, и пользователь не видел его при просмотре оглавления командой «DIR». Этот эффект обеспечивался за счёт перехвата операций, используемых командой «DIR» для считывания элементов каталога и вычитания 4 Кб из длины заражённых файлов.[183]

Более того, «Frodo» маскировал и изменение заголовка. Любая попытка доступа к инфицированному им файлу, за исключением выполнения её на заражённом компьютере, приводила к началу «выкусывания» тела вируса из этого файла. Например, при чтении заражённого файла или загрузке его в память, вирус «подставлял» файл в незаражённом виде. При открытии файла для записи вирус «выкусывал» своё тело из инфицированного файла (поскольку запись в файл могла повредить тело вируса или переместить его в середину файла), а затем снова заражал его при закрытии. Такой приём обеспечивал «Frodo» обход детектирования заражения с помощью ревизоров[184].

---

[181] Сплайсинг (splicing) – склеивание, сращивание, проф. врезка в обработчик прерывания. «Frodo» был первым компьютерным вирусом, использующим сплайсинг для получения управления по прерыванию INT 21.

[182] Все полноценные «стелс» вирусы способны обрабатывать 20 функций INT 21h и хорошо маскируются.

[183] Этот метод маскировки был заимствован из программного кода вируса «Bontchev» (другое имя – «RCE02000»), который на инфицированной машине точно также маскировал увеличение длины заражённых файлов вычитанием заранее заданной величины байт.

[184] Принято считать, что «Frodo» является первым вирусом, обходящим данный класс антивирусных программ

Если при копировании выполняемого файла создавался файл с расширением, не используемым для исполняемых файлов («*.com», «*.exe», «*.bin», «*.sys» и т. д.), то вирус «выкусывал» своё тело при копировании. При кодировании вируса использовались достаточно сложные приёмы, затрудняющие трассировку. Из-за ошибки при кодировании вирус повреждал некоторые файлы при заражении: после заражения он не обновлял информацию в заголовке файла. При запуске таких файлов MS-DOS выдавал диагностическое сообщение «ERROR in EXE File» («Ошибка в файле exe»).

Как мы уже говорили, вирус «Frodo» умел оставаться невидимым – он перехватывал прерывание INT 21h и, при обращении через MS-DOS к заражённым файлам, изменял информацию таким образом, что файл появлялся перед пользователем в незаражённом виде. Этот вирус представлял собой лишь надстройку над операционной системой MS-DOS, но не прошло и года, как компьютерные вирусы проникли внутрь ядра операционной системы, например, «стелс» вирус «Beast.512». Таким образом, технология «невидимости» продолжала бурно развиваться.

Интересно, что все без исключения специалисты – авторы публикаций о вирусе «Frodo», сходились во мнении, что он написан программистом, великолепно разбирающимся во внутреннем устройстве операционной системы MS-DOS и алгоритмах работы антивирусных программ. Вместе с тем, как профессионалы высокого уровня они выражали своё искреннее недоумение, как такой незаурядный специалист не смог найти себя в чём-то более полезном для общества, нежели написание изощрённых компьютерных вирусов?

16 октября на компьютерах VAX/VMS в сети «SPAN» была зафиксирована ещё одна эпидемия сетевого червя, который впоследствии получил название «WANK Worm». Для своего распространения «WANK Worm» использовал протокол «DECNet» и менял системные сообщения, а также системные пароли пользователей на набор случайных символов для маскировки характера передаваемой информации и затем пересылал этот набор на имя «GEMPAK» в сети «SPAN», где и происходила расшифровка полученных

данных. Отметим, что «WANK Worm» использовал в своих целях ошибки и недокументированные функции глобальных сетей того времени, передавая свои копии с сервера на сервер и запуская их на выполнение. Однако на этот раз эпидемия имела локальный характер – охватив всего лишь несколько сетей в США, и по своим последствиям не шла ни в какое сравнение с эпидемией, вызванной сетевым «червём» Морриса-младшего.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Vacsina
Другие названия	Vacsina.TP-05.A, RCE1206, TP05, VACSINA5, Sina
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	ноябрь 1989 года
Страна происхождения	Болгария
Длина	1206 байт

В ноябре появился вирус «Vacsina»[185], который стал родоначальником многочисленного семейства компьютерных вирусов (48 штаммов), получивших общее название «TP»[186]. Интересно, что последние представители этой семьи вирусов включались в листинги под знакомым нам именем «Yankee Doodle».

Вирус «Vacsina» был самым распространённым в своей семье. Формально он был файловым резидентным вирусом, заражающим файлы с расширениями «*.com», «*.exe», «*.sys» и «*.bin». Размер командного процессора «command.com», инфицированного этим вирусом (а его первоначальный размер составлял 25307 байтов) имел размер в 26509 байт. Вирус «Vacsina» «умел» заражать файлы с расширением «*.com» длиной до 63 Кб и файлы с расширением «*.exe», также длиной до 63 Кб при загрузке их в память для выполнения (214Bh). При выполнении инфицированной программы с расширением «*.com» управление командой «JMP» (E9h) передавалась в начало ви-

[185] Название связано с тем, что в теле вируса и его штаммов содержится строка «VACSINA».

[186] Первый вирус этого семейства имел болгарское происхождение. В Москве вирус «Vacsina» появился в 1989 году и был достаточно подробно описан О. Котиком в документации к его полифагу «ANTIKOT», который был первым фагом против данного вируса.

руса. Вирус узнавал длину исходного файла и проверял наличие своей копии в памяти компьютера. Если компьютер не был инфицирован, то вирус «Vacsina» копировал всю программу в свободное место в памяти и, таким образом, оставался резидентным. Затем он перехватывал прерывание INT 21h и, в итоге, при запуске любой программы получал управление, проверял, является ли запускаемая программа заражённой, и если это было не так, инфицировал эту программу. При заражении файла с расширением «*.exe» к нему дописывались 132 байта из тела вируса и изменялись три первые байта файла («JMP» на тело вируса), при этом файл преобразовывался в формат файла с расширением «*.com». Дописанные к файлу 132 байта не распространяли вирус и были лишены способности к размножению, – их действие ограничивалось настройкой адресов программы при её запуске.

При заражении очередного файла вирус «Vacsina» заставлял системный динамик издавать звуковой сигнал (символ «Bell»). Кроме того, являясь резидентным, вирус распознавал случаи загрузки программ с защищённых от записи флоппи-дисков или логических разделов «жёсткого» диска и не делал попыток инфицирования таких файлов.

Примерно в тоже время, когда появился вирус «Vacsina», в г. Сиэтл (штат Вашингтон, США) был зарегистрирован первый случай появления в «диком» виде деструктивного вируса, получившего имя «Sunday»[187], после чего сообщения о нём стали поступать от множества пользователей из разных концов страны[188]. Этот компьютерный вирус получил своё имя от дня недели, в который он удалял все запускаемые пользователем файлы, и был тесно связан с вирусом «Jerusalem». Автор «Sunday», очевидно, начал с копирования вируса «Jerusalem», а затем внёс в него свои изменения. Однако, несмотря на сходство с вирусом «Jerusalem», вирус «Sunday» получил в мире гораздо меньшую известность.

---

[187] «Sunday» (англ.) – «Воскресенье».

[188] В СССР обнаружен в марте 1990 гола в городах Ленинград и Киев, а чуть позднее в Москве. Первым отечественным полифагом для данного вируса был «AIDSTEST».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Sunday
Другие названия	Jerusalem.Sunday.A, RCE1636
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	ноябрь 1989 года
Страна происхождения	Соединённые Штаты Америки
Длина	1636 байт

Формально вирус «Sunday» был резидентным файловым вирусом, поражающим файлы с расширениями «*.com» и «*.exe». Вирус не проверял версию MS-DOS, и был работоспособен на всех версиях, начиная с 2.0 как на PC XT, так и на PC AT. При выполнении заражённой программы «Sunday» сначала проверял наличие своей копии в памяти компьютера, аналогично тому, как это делал вирус «Jerusalem», а затем устанавливал себя и перехватывал прерывания INT 21 и 8. Механизм размножения у него был стандартен – перехват прерывания INT 214B и заражение каждой подходящей запускаемой на выполнение программы, за исключением файла с именем «command.com». Ограничений на длину файлов у этого вируса не было, и поэтому он уничтожал файлы с расширением «*.com» длина которых после заражения превышала 64 Кб. Файлы с расширением «*.com» поражались вирусом «Sunday» однократно, дата их создания не менялась, а длина увеличивалась на 1636 байт. В инфицированной программе тело вируса размещалось в начале файла: со смещением 184h от начала заражённого файла расположена текстовая строка «command.com»; со смещением 351h – текст сообщения, выдаваемого вирусом на экран: «Today is Sunday! Why do you work so hard? All work and no play make you a dull boy! Come on! Let's go out and have some fun!» («Сегодня воскресенье! Зачем работать так напряжённо? Постоянная работа без игр делает Вас занудой! Живей! Давай пойдём куда-нибудь и повеселимся!»). В конец заражённого файла с расширением «*.com» записывалось пятибайтовое поле (обычно это поле содержит C8h, F7h, E1h, EEh, E7h), которое использовалось «Sunday» в качестве признака инфицирования файлов с расширением «*.com». Файлы с расширением «*.exe» заражались также

однократно, и контроль над их инфицированием происходил по тому же пятибайтному полю. При заражении файлов с расширением «*.exe» вирус дописывал своё тело в конец программы и исправлял заголовок инфицируемых файлов, запоминая некоторые поля. Как и вирус «Jerusalem», вирус «Sunday» записывал вместо контрольной суммы число «1984», а оригинальное значение контрольной суммы утрачивалось. В конец заражённого файла дописывались всё те же пять байтов.

Как уже указывалось, данный вирус имел стадию проявления, наступающую в воскресенье. В этот день вирус не заражал собой все запускаемые файлы, а, как и «Jerusalem», удалял их с диска. Перехватывая прерывание от таймера (INT 8), вирус отсчитывал один час от начала режима удаления запускаемых файлов и выводил приведённое выше сообщение. Вирус имел несколько штаммов, в одном из которых в этом месте была допущена ошибка, и данная ветвь кода никогда не выполнялась. Аналогично вирусу «Jerusalem», вирус WANK Worm мог записываться в середину «расширенных» файлов с расширением «*.exe».

Поскольку вирус «Sunday» был во многом похож на вирус «Jerusalem», неудивительно, что он распространялся посредством тех же каналов. Совместно используемые компьютеры, флоппи-диски и программы, а также серверы локальной сети представляют собой важнейшие средства распространения этого типа вирусов. Вместе с тем «Sunday» в определённом смысле, по сравнению с вирусом «Jerusalem», был менее заметен. Большинство модификаций этого вируса не стирало файлы, не служило причиной появления на экране монитора «чёрных дыр» или прокручивающихся областей, снижения скорости инфицированных компьютеров, а также не размножало инфицированные файлы с расширением «*.exe» и т. п. Симптомы, которые сопровождали вирус «Sunday», ограничивались однократным ростом размера файлов и периодическими сбоями в работе программ с расширением «*.exe», что не так просто заметить неопытному пользователю. Этот вирус появился позже вируса «Jerusalem», поэтому он был быстро изучен и практически немедлен-

но обнаруживался и удалялся любой из числа известных антивирусных программ.

Идентификационная карточка вредоносной компьютерной программы	
Имя	PrintScreen
Другие названия	нет
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	ноябрь 1989 года
Страна происхождения	Индия
Длина	512 байт

В том же ноябре 1989 года зарегистрировано появление ещё одного представителя вредоносных компьютерных программ – компьютерного вируса по имени «PrintScreen»[189], который вошёл в историю вирусописания уже тем, что был самым первым из всех известных индийских вирусов[190].

Вместе с тем, «PrintScreen» представлял собой очень опасный компьютерный вирус длиной в один сектор, который перехватывал прерывание INT 13h и заражал загрузочные сектора как флоппи-дисков, так и «жёсткого» диска при попытке считывания с них данных (INT 13h, AH=2). При этом «PrintScreen» сохранял оригинальный загрузочный сектор на флоппи-диске по адресу 0/1/3 (трек/сторона/сектор), а на «жёстком» диске – по адресу 1/3/13. Причём, этот вирус мог уничтожать один из секторов таблицы размещения файлов (FAT) или данных, – в зависимости от объёма инфицированного «жёсткого» диска.

Специалисты, отмечая опасность «PrintScreen», указывали и на низкую квалификацию его автора, так как при заражении «жёсткого» диска вирус предполагал, что его загрузочный сектор расположен по адресу 0/1/1. Кроме

---

189 «PrintScreen» (англ.) – «Распечатка (содержимого) экрана». Появившийся следом за родоначальником штамм под именем «PrintScreen.b» был надоедлив, но не опасен. Он перехватывал прерывания INT 10h, 40h. Записывался в загрузочные сектора флоппи-дисков, а при выводе символов на экран монитора конвертировал их в нижний регистр, то есть, так называемый «регистр строчных букв» – «lowercase».

[190] Обнаружен в г. Бомбей (Индия) Невилем Булсара.

того, этот вирус был задуман и написан таким образом, что при инфицировании диска с вероятностью 1/256 (в зависимости от значения своего внутреннего счётчика) «PrintScreen» должен вызывать прерывание INT 5 (печать экрана), но в программном коде допущена ошибка, в результате которой новое значение счётчика не сохранялось.

Наступил декабрь 1989 года и в графстве Кент (Англия) Джеймсом Берри был обнаружен компьютерный вирус «Chaos»[191].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Chaos
Другие названия	Chaos.1241, Merritt, Peking, Seoul, Yale
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	декабрь 1989 года
Страна происхождения	Англия
Длина	1241 байт

Формально «Chaos» был загрузочным резидентным в памяти вирусом, заражающим как флоппи-диски, так и «жёсткие» диски компьютерных систем. При запуске на выполнение заражённого файла вирус «Chaos» загружал себя в память и оставался там резидентно, отслеживая действия пользователя. Если пользователь пытался запустить какую-нибудь исполняемую программу, он инфицировал файлы с расширениями «*.com» и «*.exe», а также перезаписывал оригинальные загрузочные сектора, причём, не осуществлял их копирование в другое место. Кроме того, «Chaos» помечал все свободные кластеры[192] на флоппи-дисках и «жёстких» дисках компьютера в качестве сбойных, что не позволяло пользователю сохранять на них необходимую информацию. Заражённые вирусом «Chaos» загрузочные сектора содержали следующие текстовые строки: «Welcome to the New Dungeon» («Добро пожаловать в Но-

[191] «Chaos» (англ.) – «Хаос». В СССР не регистрировался.

[192] [192] Cluster (англ.) – кластер, в системах хранения данных, данный контекст, рассматриваемая как единое целое часть флоппи-диска, состоящая из фиксированного числа секторов, используемых операционной системой для чтения и записи данных.

вую темницу), «Chaos» («Хаос», что послужило поводом для присвоения имени) и «Let’s be cool guys» («Давайте будем клёвыми парнями»).

Этот вирус не обладал какими-то особенно деструктивными функциями, но, тем не менее, заразил множество компьютеров в Великобритании, а затем «перебрался» в другие страны и, в ряде случаев, стал причиной локальных эпидемий.

В том же декабре произошёл инцидент с первой «троянской» программой («троянским конём»), которая получила имя-аббревиатуру «AIDS»[193]. Двадцать тысяч копий этой программы было разослано неизвестным компьютерным злоумышленником на флоппи-дисках по украденным из баз данных Организации всемирного здравоохранения и журнала «PC Business World» адресам в Европе, Африке и Австралии. При использовании этих флоппи-дисков «троянский конь» автоматически внедрялся в систему, создавал собственные скрытые файлы и директории, а также модифицировал системные файлы. После девяноста загрузок операционной системы «AIDS» шифровал имена всех файлов на «жёстком» диске компьютера, делал их невидимыми[194] и оставлял на нём только один читаемый файл, высвечивая на экране монитора надпись: «Пришлите чек на 189 долларов по адресу: PO Box 7, Panama».

В результате проведённого «по горячим следам» расследования автор «троянской» программы был установлен в кратчайшие сроки, им оказался некий Джозеф Попп, который был арестован в момент обналичивания денег. Впоследствии его признали невменяемым, что, впрочем, не помешало ита-

---

[193] «AIDS» (англ.) – как известно, это общепринятая англоязычная аббревиатура неизлечимого на сегодняшний день заболевания «Acquired Immunodeficiency Syndrome» («синдром приобретённого иммунодефицита» – СПИД). Однако название вируса произошло не от указанного заболевания, а от сокращения следующего текста, которым были помечены флоппи-диски: «Aids Information Diskette Version 2.0»; которое можно перевести как «Флоппи-диск с информацией о вспомогательных средствах, версия 2.0».

[194] Присваивая им атрибут «hidden» («скрытый»).

льянскими властям заочно приговорить его к тюремному заключению за вымогательство.

В 1989 году компьютерным вирусологам много хлопот доставляли самостоятельно шифрующиеся вирусы, а также вирусы нового поколения – «полиморфные», которые использовали новые подходы в уже хорошо известной технологии невидимости: в большинстве случаев они шифровались, а в расшифровщике использовали команды, которые могли быть разными при инфицировании различных файлов.

Следует отметить и тот факт, что 1989 год стал точкой отсчёта для начала масштабных эпидемий компьютерных вирусов в Советском Союзе и, соответственно, России, так как различные вирусы («Cascade», «Jerusalem», «Vacsina», «Yankee», «Vienna», «Dark Avenger», «Ping Pong») и их многочисленные штаммы, заполонили компьютеры российских пользователей. К счастью, ведущие российские специалисты – компьютерные вирусологи, довольно быстро разобрались с принципами их работы, и практически сразу появилось несколько отечественных антивирусных продуктов, способных успешно бороться с электронной заразой.

Завершить рассказ о событиях 1989 года хотелось бы чем-то позитивным. И это возможно. Клифф Столл, сотрудник Lawrence Berkeley National Laboratory, опубликовал свою во многих отношениях пророческую книгу – «The Cuckoo's Eggs»[195], в которой предрекал, что Глобальная сеть может служить не только благородным целям улучшения коммуникаций между людьми всего земного шара и построения единого всемирного информационного пространства, но и стать мощным инструментом в руках компьютерных преступников, а также откровенных террористов. Причём Клифф Столл не только прогнозировал и указывал на растущую проблему, но и настоятельно рекомендовал выработать превентивные меры для недопущения развития событий в таком направлении.

---

[195] «The Cuckoo's Eggs» (англ.) – «Кукушкины яйца».

§10. 1990 год – полиморфизм, бронирование, многоуровневое шифрование, сегментация, многокомпонентность и многое, многое другое

- Выпущена версия 4.01 операционной системы MS-DOS.
- Выпущена версия 3.0 операционной системы MS Windows, в среде которой приложения MS-DOS выполнялись в отдельном окне на полном экране, а сами окна работали в нескольких режимах памяти: реальном (базовая 640 Кб), защищённом (версия 80286) и расширенном (версия 80386). При этом можно было запускать приложения, размер которых превышал размер физической памяти. Имела место и технология динамического обмена данными (DDE).
- Фирма Intel начала производство микропроцессора Intel 80486 DX2.

В январе 1990 года появились демонстрационные версии компьютерных вирусов, которые были разработаны в исследовательских целях независимыми друг от друга программистами и познакомили компьютерное сообщество с усовершенствованной технологией «полиморфизма», а заодно и так называемым усиленным «бронированием»[196] тела вируса. Мы ограничимся рассмотрением двух вирусов одного автора, Патрика Тоулми из округа Колумбия (штат Вашингтон, США), которые получили официальное название «Virus90» и «Virus101» и представляли собой экземпляры, недвусмысленно показывавшие, чего, в частности, можно ожидать от последующих поколений вредоносных компьютерных программ.

[196] Технология «бронирования» используется для препятствования деассемблированию программного кода компьютерного вируса.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Virus90
Другие названия	Virus-90
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	январь 1990 года
Страна происхождения	Соединённые Штаты Америки
Длина	857 байт

«Virus90» являлся опасным резидентным вирусом, записывавшим своё тело в конец файлов с расширением «*.com» на текущем логическом разделе «жёсткого» диска. При его написании Тоулми реализовал усовершенствованные способы программирования, затрудняющие трассировку и деассемблирование вредоносного программного кода. Внешними проявлениями деятельности этого вируса в инфицированной им компьютерной системе были: периодический сдвиг части символов на экране монитора и перезагрузка компьютера. Кроме того, «Virus90» выводил на экран монитора слово: «Infected!» («Заражён!»).

Интересно, что автор «Virus90», Патрик Тоулм, декларировал своё детище в качестве чисто «учебного пособия», исходный код которого может быть свободно приобретён у него всеми желающими. Однако практически сразу же ему пришлось связываться с Web-сайтами, на которые он переслал в соответствии с их просьбами «Virus90» и, извиняясь, просить о его удалении из компьютерных систем, так как «в результате проведённых переговоров с некоторыми представителями властей понял, что его идея распространения реального вируса в качестве «учебного пособия» была не продуманным поступком.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Virus101
Другие названия	Virus-101, RCE2560
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	январь 1990 года
Страна происхождения	Соединённые Штаты Америки
Длина	2560 байт

Практически одновременно с «Virus90» появился его «большой брат» «Virus101». Этот вирус стал первым известным резидентным вирусом с самостоятельно модифицирующимся инсталлятором и первым, заражающим наряду с файлами, загрузочный сектор флоппи-дисков. Он был написан Патриком Тоулми тоже в качестве «учебного пособия» и представлял собой очень опасный резидентный вирус, записывающий своё тело в конец файлов с расширениями «*.com» и «*.exe», а также инфицирующий командный процессор «command.com» с использованием алгоритма уже известного нам вируса «Lehigh»[197].

Вирус выводил на экран монитора следующий текст: «This file has been safely infected by VIRUS101 – the safe, educational virus utility. This copy furnished to John McAfee» («Этот файл был благополучно заражён VIRUS101 – безопасно, учебная программа-вирус. Данная копия передана Джону МакАфи»). Вирус поражал файлы исключительно на флоппи-дисках, и если не находил на них файлы, которые мог заразить, инфицировал загрузочный сектор. При этом он заменял в загрузочных секторах текст «Non system disk or disk error» («Не системный диск или ошибка диска») на приведённую выше фразу. В программном коде вируса «Virus101» так же, как и у его предшественника, присутствовали фрагменты, затрудняющие его трассировку и деассемблирование.

Кроме перечисленного выше, этот вирус был опасен и тем, что применял шифрование во избежание своего обнаружения в инфицированных фай-

[197] Более подробно об этом компьютерном вирусе см. выше – 1987 год.

лах, а в заголовках заражённых файлов с расширением «*.exe» устанавливал значения полей «SS:SP» в «5555:5555», не сохраняя их старое содержимое.

Ещё не закончился январь, а теоретический этап в области создания вирусов был фактически завершён появлением в «диком» виде нового поколения чрезвычайно опасных компьютерных вирусов, обладающих свойствами полиморфизма и способных заражать локальную сеть, включая файл-сервер и все рабочие станции.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Chameleon
Другие названия	1260, V2P1
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	январь 1990 года
Страна происхождения	Соединённые Штаты Америки
Длина	1260 байт

Обнаруженные в конце января в штате Миннесота (США) вирусы семейства «Chameleon» («1260», «V2P1», «V2P2» и «V2P6») были первыми представителями этого типа вредоносных компьютерных программ и «эволюционировали» из двух других ранее рассмотренных нами вирусов – «Vienna» и «Cascade»[198].

Марк Уошбурн, автор нерезидентного файлового полиморфного вируса «Chameleon», взял за его основу необходимые данные о вирусе «Vienna» из упоминавшейся нами ранее книги Ральфа Бюргера и добавил к ним принципы самостоятельной шифрации вируса «Cascade». Более того, в отличие от вируса «Cascade», вирус «Chameleon» имел возможность изменения своего внешнего вида – как тела вируса, так и расшифровщика. Такая особенность делала его практически неуязвимым для имевшегося на то время антивирусного программного обеспечения ввиду того, что оно использовало простой контекстный поиск фрагментов программного кода вируса, а у полиморфного вируса «Chameleon» постоянный код отсутствовал. Это привело к форму-

[198] Более подробно об этих компьютерных вирусах см. выше – 1987 год.

лированию новых принципов защиты от компьютерных вирусов и ускорило создание нового поколения антивирусных средств[199].

Итак, вирус «Chameleon» являлся сильно модифицированным вариантом вирусов «Vienna» и «Cascade» и обладал способностью инфицирования локальных сетей. Хотя он и не являлся резидентным, распространялся он достаточно быстро и заражал файлы с расширением «*.com», записываясь в их конец, причём, при заражении они шифровались ключом, меняющимся от файла к файлу. При поиске и заражении файлов «Chameleon» использовал технологию вируса «Vienna» и два интересных алгоритма. Первый реализовал свойство полиморфности, благодаря чему два штамма одного вируса с большой вероятностью не совпадали ни на одном байте. Основное тело вируса шифровалось в зависимости от таймера, – всего вариантов ключа 1000000h=16777216, а расшифровщик выбирался из более 3 000 000 000 000 000 000 000 вариантов (длина расшифровщика – 39 байт). Второй алгоритм достаточно успешно мешал трассировке вируса, используя динамическое шифрование и расшифровывание его программных кодов при помощи прерываний INT 1 и 3.

В пятницу, 13 апреля, из Китая стали поступать тревожные сообщения о том, что компьютеры научно-исследовательских институтов, заводов и государственных учреждений этой страны оказались сплошь заблокированы нашим старым знакомым, вирусом «Jerusalem»[200].

В 1990 году стало ясно, что болгарская «фабрика вирусов» продолжает успешно функционировать. Особой плодовитостью отличался некто «Dark Avenger» («Тайный мститель»), выпускавший в год несколько новых виру-

---

[199] Затем появились алгоритмические языки, которые могли распознавать в заражённом файле полиморфные вирусы. Кроме того, в 1992 году Евгений Касперский изобрёл эмулятор процессора для дешифрации программных кодов компьютерных вирусов, который явился весьма эффективным инструментом, способствовавшим успешной борьбе с их полиморфными представителями.

[200] Более подробно об этом компьютерном вирусе см. выше – 1987 год.

сов, использовавших принципиально новые алгоритмы заражения и сокрытия себя в системе. Именно он впервые применил технологию заражения файлов, при которой вирус, находясь в памяти компьютера, автоматически заражал все используемые и даже просто открываемые для чтения файлы. «Dark Avenger» демонстрировал изобретательность и в распространении вирусов: он активно загружал инфицированные программы на электронные станции (BBS), распространял исходные коды своих «вирусов» и активно пропагандировал идею их создания[201].

В течение этого, а также нескольких последующих лет было зарегистрировано появление множества новых компьютерных вирусов, имевших общий обратный адрес: г. София, Болгария. К таким вредоносным компьютерным программам можно отнести семейство файловых резидентных в оперативной памяти вирусов, родоначальник которого был обнаружен в апреле 1989 года[202] и стал известен под именем «Murphy» [203].

Этот вирус обладал высокой скоростью заражения, перехватывал прерывания INT 1Ch, 21h и инфицировал файлы с расширениями «*.com» и «*.exe», дописывая своё тело в конец файлов, как при запуске программ на

---

[201] В 1990 году в Болгарии была организована первая BBS (VX BBS), предназначенная для обмена компьютерными вирусами и информацией для вирусописателей. Работала станция по следующей схеме. Если пользователь передавал вирус, то взамен мог загрузить из каталога станции любой понравившийся ему вирус. Если пользователь передавал новый, интересный вирус, то получал полный доступ к ресурсам станции и мог загрузить из коллекции станции любое число вирусов. Таким образом, станция VX BBS дала мощный импульс развитию вирусописательства и представляла собой далеко не «местечковое» явление, так как доступ к ней мог получить всякий желающий из любой точки мира!

[202] В Москве обнаружен в июле 1990 года.

[203] Получил своё название в связи с тем, что в теле вируса содержится достаточно длинный фрагмент текста: «Hello, I'm Murphy. Nice to meet you friend. I'm written since Nov/Dec. Copyright (c) 1989 by Lubo & Ian, Sofia, USM Laboratory» (Привет, я Мэрфи. Приятно встретить тебя, приятель. Я написан после ноября/декабря. Охраняется авторским правом (с) 1989 Любо и Ян, София, Лаборатория USM).

выполнение, так и при открытии файлов (213B, 214B, 216C). «Murphy» мог инфицировать файлы, а также командный процессор «command.com» только в том случае, если они не имели установленного атрибута «Read Only», но при этом не имело значения, где был расположен «command.com» [204].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Murphy
Другие названия	Murphy-1, Murphy.1277, V1277, RCE1277
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	апрель 1990 года
Страна происхождения	Болгария
Длина	1277 байт

Это связано с тем, что вирус при инсталляции затирал часть копии командного процессора и, в итоге, он вызывался с «жёсткого» диска, в процессе чего и происходило заражение. Тип файла определялся вирусом правильно, независимо от используемого расширения. Заражённые файлы с расширением «*.com» увеличивались в размере на 1277 байт, а дата их создания и атрибуты оставались неизменными. При заражении «Murphy» вставлял в первые три байта команду перехода на начало вируса. Выравнивания на границу параграфа для файлов с расширением «*.com» не выполнялось, и инфицировались все файлы с этим расширением длиной свыше 1277 (6Fh) байт. Заражение файлов с расширением «*.exe» выполнялось при помощи дописывания тела вируса в конец файла без предварительного выравнивания тела на границу параграфа. Иногда в процессе инфицирования этих файлов вирус становился причиной «зависания» системы, делая её неработоспособной вплоть до перезагрузки или полного обесточивания.

При выполнении заражённой программы вирус проверял наличие своей копии в памяти и, если её там не было, записывал указанную копию в оперативную память. Став резидентным в оперативной памяти компьютера, «Mur-

[204] Инфицированный командный процессор «command.com» имел размер 27107 байт, если его первоначальный размер составлял 25307 байт.

phy» выжидал заданное время и по его истечении инициировал противный высокочастотный свист частотой около 12 КГц, который раздавался из системного динамика[205].

К маю компьютерное сообщество получило из Болгарии очередной привет от вирусописателя под псевдонимом «Тайный мститель» в виде новых модификаций – «Eddie 2», «Eddie 3» – очень опасного вируса «Dark Avenger» (он же «Eddie»)[206], а также малоприятного компьютерного вируса, получившего имя «Beast»[207].

Этот вирус представлял собой первый сегментированный резидентный файловый вирус и имел размер в 512 байт, совпадающий с размером обычного сектора операционной системы MS-DOS.

---

[205] Находясь резидентно в оперативной памяти, «Murphy» отслеживал системное время, и когда оно принимало значение между 10 и 11 часами, включал динамик, посылая на него 61h. В другое время суток вирус подобных попыток не предпринимал.

[206] Более подробно об этом компьютерном вирусе см. выше – 1989 год.

[207] «Beast» (англ.) – «Зверь», «Скотина», «Тварь». Вирус получил своё название в связи с тем, что в конце его тела содержится «дьявольское» число «666», поэтому его иногда называют «666», а также «Number-of-Beast», «Number of the Beast Virus», что можно перевести как: «Число зверя» или «Число Сатаны».

В СССР обнаружен в Москве в начале сентября 1990 года.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Beast
Другие названия	512, 512-A, Number-of-Beast, Number of the Beast Virus, 666, RC0512
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	апрель 1990 года
Страна происхождения	Болгария
Длина	512 байт

«Beast» использовал необычный метод размножения, напоминающий метод размножения загрузочных вирусов. В коде вируса использовался ряд недокументированных функций MS-DOS. Автор вируса использовал несовершенство распределения дисковой памяти в указанной операционной системе, где размер кластера обычно превышает размер сектора как минимум в два раза, и поэтому можно использовать незаполненные «хвосты» в последнем секторе для хранения части тела вируса[208]. Этот приём специалисты определили как попытку перенесения схемы загрузочного вируса на файловый вирус, так как загрузочные вирусы, в отличие от файловых, сегментированы, и их тело состоит из «головы», которая находится в загрузочном секторе, и «хвоста», который хранится в ином месте и его загрузка выполняется «головой». Вирус «Beast» считает первый сектор файла с расширением «*.com» загрузочным и заменяет его своим телом, а хвост, представляющий собой оригинальный первый сектор инфицированной программы, прячет в неиспользуемый сектор последнего кластера. Вследствие этого «Beast» мог заражать на флоппи-дисках исключительно те файлы, у которых второй сектор последнего кластера был не занят данными. Зато на «жёстких» дисках компьютера он мог инфицировать практически все файлы с расширением «*.com», так как размер кластера на них значительно больше и свободный сектор практически всегда существует. В результате инфицирования по такой схеме заражённые файлы, скопированные при помощи средств операционной системы MS-DOS

[208] Модификация первых команд осталась обязательной, иначе вирус не мог получить управление.

– команда «Copy»[209], становились неработоспособными, а вот находящийся внутри них вирус оставался вполне дееспособным.

Кроме необычного способа инфицирования файлов, вирус «Beast» использовал также и весьма неординарный механизм установки себя в оперативную память. С целью хранения собственного тела он «откусывал» первый буфер от буферного пула[210] операционной системы, переставляя указатель на первый буфер так, чтобы тот указывал на второй буфер. Поэтому определение его присутствия в оперативной памяти без полного её сканирования было возможно лишь в том случае, если было точно известно, где необходимо проводить поиск.

В соответствии с концепцией вирусов семейства «Dark Avenger» вирус «Beast» инфицировал файлы и при их выполнении, и при простом открытии. Однако имелись и различия, например, заражались файлы, у которых первыми двумя латинскими буквами расширения являлись «c» и «o», то есть файлы с маской: «*.co*».

В мае 1990 года зарегистрировано появление нового компьютерного вируса, при разработке которого были предприняты изощрённые меры по маскировке его присутствия на инфицированном компьютере. В результате ко времени своей официальной регистрации он был уже достаточно широко распространён в Западной Европе.

---

[209] Эта команда осуществляет копирование файлов байт за байтом в соответствии с указанной в элементе каталога длиной.

[210] Buffer pool (англ.) - буферного пула.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Fish
Другие названия	3584, Fish 6, European Fish Virus, RCE03584
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	май 1990 года
Страна происхождения	Германия
Длина	3584 байта

Этот вирус получил имя «Fish».[211] Он был существенно переработанной модификацией известного нам вируса «Frodo»[212], и, возможно, их авторство принадлежало одному и тому же вирусописателю.

Вирус «Fish» использовал очень сложный алгоритм сокрытия присутствия в системе и представлял собой вредоносную компьютерную программу, которая использовала как технологию «стелс», так и шифрование с очень коротким дескриптором длиной всего лишь в 14 байт. Формально вирус представлял собой резидентный файловый вирус, заражающий файлы с расширениями «*.com»[213] и «*.exe». Также как и некоторые загрузочные вирусы, «Fish» спокойно переживал «горячую» перезагрузку системы, перехватывая нажатие комбинации клавиш «Ctrl-Alt-Del». При выполнении инфицированной программы он проверял своё присутствие в оперативной памяти и, если его копии там не было, устанавливал себя в её младшие адреса. При этом, если прерывание INT 13 не было перехвачено другой программой, «Fish» перехватывал его и резервировал 8192 байта в оперативной памяти; если указанное прерывание уже было перехвачено, то вирус резервировал 4096 байтов и через произвольно заданный интервал времени инициировал «горячую» перезагрузку, в процессе которой заражал «command.com» и перехватывал прерывание INT 13.

---

[211] «Fish» (англ.) – «Рыба». Такое имя вирусу было дано в связи с тем, что иногда в теле инфицированных им компьютерных программ встречалась строка «Fish FI» и, кроме того, при просмотре оперативной памяти в то время, когда вирус находится там резидентно, можно было обнаружить названия ряда рыб.

[212] Более подробно об этом компьютерном вирусе см. выше – 1989 год.

[213] В том числе и командный процессор «command.com».

Вирус «Fish» инфицировал все открываемые файлы с расширениями «*.com» и «*.exe», длина которых увеличивалась при этом на 3584 байта, но это увеличение очень тщательно маскировалось. Визуально он проявлял себя тем, что замедлял запись в видео память, и на инфицированных им компьютерах было заметно мерцание экрана дисплея. «Fish» не обнаруживался существовавшими на тот момент ревизорами, запущенными на инфицированной системе и, кроме того, он обходил сторожей, следящих за операциями записи на «жёсткий» диск, а также постоянно перекодировал свой программный код в оперативной памяти.

В июне 1990 года усилиями проживавшего в то время в г. Бомбей (Индия) вирусописателя возникла индийская группа загрузочных компьютерных вирусов.[214]

Типичным представителем этой группы и родоначальником одноимённого семейства стал очень опасный, длиной в девять секторов, компьютерный вирус по имени «Joshi»,[215] который использовал «стелс» технологию, проникал в загрузочный сектор запоминающего устройства, постепенно захватывая всё новые и новые участки памяти. Появившись в Индии, он быстро распространился в США, европейских странах и стал одним из наиболее распространённых компьютерных вирусов того времени, что (с точки зрения вируса) выглядит как большая удача: стать участником реальных инцидентов

---

[214] Скорее всего, это был тот же человек, что и автор компьютерного вируса «PrintScreen», о котором более подробно см. выше – 1989 год.

[215] «Joshi» (англ.) – «Джоши». Название данного вируса связано с тем, что при загрузке компьютера пятого января любого года на экран выдавалось сообщение: «Happy Birthday Joshi!» («С днём рождения, Джоши!») и система останавливалась. Чтобы разблокировать систему пользователю предлагалось набрать на клавиатуре текст: «С днём рождения Joshi». Если пользователь вводил его, загрузка операционной системы продолжалась.

Интересно, что по данным Д. Н. Лозинского при программировании выдачи этого сообщения автор вируса уже тогда ориентировался лишь на цветные мониторы, игнорируя монохромные модели.

В СССР «Joshi» появился в июле того же года.

прежде, чем быть «пойманным» и засветиться какими-либо собственными характерными чертами.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Joshi
Другие названия	Happy Birthday Joshi, WM1F
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	июнь 1990 года
Страна происхождения	Индия
Длина	4086 байт

Итак, вирус «Joshi» являлся представителем похожих на «Stoned»[216] загрузочных вирусов. Он заражал загрузочные сектора 360 Кб и 1,2 Мб флоппи-дисков и главные загрузочные сектора «жёстких» дисков. При заражении флоппи-дисков, подобно вирусу «DenZuk»[217], записывал свой «хвост» на дополнительную дорожку (41 для 360 Кб и 81 для 1,2 Мб флоппи-дисков) и не проверял, заняты указанные сектора информацией или нет. Поэтому, например, если на 41 дорожке флоппи-диска были записаны какие-нибудь данные, то они уничтожались. При заражении «жёсткого» диска «голова» вируса записывалась не в загрузочный сектор логического диска C:, а в абсолютный начальный сектор, который на «жёстком» диске содержит таблицу его разделов, то есть применялся приём, аналогичный вирусу «Stoned». При этом «хвост» вируса располагался в восьми секторах, начиная с абсолютного адреса 0/0/2 –сектора, следующего за MBR[218]. Из этих восьми секторов шесть занимались «хвостом» вируса, следующий – седьмой – сектор оставался пустым, а восьмой содержал оригинальный MBR. Как и при заражении флоппи-диска, при инфицировании «жёсткого» диска «Joshi» не проверял содержимое этих секторов. Подобно какому-нибудь файловому вирусу «Joshi» перехватывал прерывания INT 8, 9, 13 и 21. Отличительной особенностью данного вируса являлось то, что он перехватывал прерывание

[216] Более подробно об этом компьютерном вирусе см. выше – 1987 год.

[217] Более подробно об этом компьютерном вирусе см. выше – 1988 год.

[218] Обычно эти сектора представляют собой неиспользуемое пространство между MBR и началом логического диска C:.

от клавиатуры, что позволяло ему выходить невредимым в случае «горячей» перезагрузки системы.

Если рассматривать вирус «Joshi» в аспекте характерных черт его распространения, то он очень схож с вирусом «Stoned». Когда компьютер загружался с инфицированного флоппи-диска или «жёсткого» диска, вирус «Stoned» загружался в оперативную память, «садился» на любые флоппи-диски, которые использовались в дисководах A: или B:, а заодно мог инфицировать и первые два из числа физических «жёстких» дисков компьютера. Вирус «Joshi» был более сложным, но все способы его распространения уже применялись вирусом «Stoned». Однако из-за большей сложности вируса «Joshi»инфицированные им системы были сильнее подвержены сбоям, чем системы заражённые вирусом «Stoned». В частности, инфицированные им компьютерные системы были не способны обеспечить корректный доступ к накопителям на флоппи-дисках. Как и с вирусом «Stoned», инфицированные «Joshi» системы имели в своём распоряжении несколько меньший объём общей памяти, чем могли бы[219], но обычный пользователь, как правило, это не замечал.

Вирус «Joshi» являлся более новым вирусом, чем вирусы «Jerusalem» или «Stoned», поэтому сначала некоторые антивирусные программы не могли его обнаруживать и, соответственно, защищать от него компьютерные системы. Он также был несколько более труден для обнаружения, чем вирус «Stoned», потому что, если «Joshi» был активным в памяти, он перехватывал попытки чтения инфицированного загрузочного сектора, и «обманывал» вызывающую программу передавая обратно образ оригинального, не инфицированного загрузочного сектора компьютерной системы. Вместе с тем обновлённые антивирусные программы быстро его выявляли и удаляли.

Вирус «Joshi» распространялся по миру, обретая всё большую известность, но оказалось, что буквально ему в «затылок дышит» очередной «ше-

[219] В оперативной памяти вирус размещался в старших адресах, «отрезая» 6 Кб у MS-DOS.

девр» вирусописателей, очень опасный резидентный загрузочный компьютерный вирус «Form».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Form
Другие названия	Form.A, Form Boot, Form 18, Form-18, Form_18, FORM-Virus
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	июнь 1990 года
Страна происхождения	Швейцария

Вирус «Form» впервые был отмечен в инциденте, который приключился в июне 1990 года. Он перехватывал прерывания INT 9, 13h и поражал загрузочные сектора флоппи-дисков при обращении к ним, а также загрузочные сектора «жёстких» дисков компьютерных систем при загрузке с инфицированного флоппи-диска. Если компьютерная система загружалась с инфицированного вирусом «Form» флоппи-диска или «жёсткого» диска, он активизировался в оперативной памяти и, естественно, заражал любой используемый в системе флоппи-диск. В отличие от знаменитого компьютерного вируса «Brain»[220] он постоянно оставался на «жёстком» диске и мог распространяться, если впоследствии система загружалась с этого «жёсткого» диска.[221] В отличие от не менее знаменитого компьютерного вируса «Stoned», вирус «Form» обладал способностью заражения флоппи-дисков любого типа, используемых в любом дисководе. Таким образом, вирус «Form» не имел каких-либо ограничений по типу инфицируемых им магнитных носителей информации того времени.

Этот вирус содержал в своём теле следующий текст: «The FORM-Virus sends greetings to everyone who's reading this text. FORM does not destroy data! Don't panic! …» («Вирус «Form» посылает поздравления всякому, кто читает этот текст. «Form» не разрушает данные! Без паники! …»). Кроме того, вирус

[220] Более подробно об этом компьютерном вирусе см. выше – 1986 год.

[221] На «жёстком» диске вирус располагался в его последних секторах, а на флоппи-диске по аналогии с вирусом «Brain». При работе с «жёстким» диском могла происходить потеря данных.

«Form» обнаруживал своё присутствие шестнадцатого числа каждого месяца, вызывая при нажатии на клавиши холостой цикл[222], а восемнадцатого числа любого месяца он инициировал слабые щелчки системного динамика компьютера, когда пользователь нажимал клавиши на клавиатуре заражённой им системы. В остальное время этот вирус вёл себя достаточно хитро, оставаясь незамеченным обычными пользователями. Таким образом, у вируса «Form» не было таких особенностей, которые сдерживали и ограничивали распространение вирусов «Brain» и «Stoned» в середине и конце 80-х годов. Этот компьютерный вирус как бы говорил, что он демонстрирует некоторые свойства и типичные манеры поведения, которые станут отличительной чертой многих будущих компьютерных вирусов.

Вирус «Form» потратил более года на то, чтобы подготовить «плацдарм для наступления» и затем начал резкое наращивание показателя своей распространённости, который неуклонно рос в течение 1992–1993 годов, сделав его самым распространённым компьютерным вирусом в мире. Примерно к концу 1994 года он достиг уровня равновесия, сравнимого с этим уровнем других знаменитых вирусов, например, «Jerusalem» или «Stoned», в пору их наибольшей «зрелости» и активности. Можно предположить, что при отсутствии в 1995 году серьёзных изменений среды окружения (например, если бы не вышла операционная система MS Windows 95), вирус «Form» оставался бы одним из наиболее распространённых в мире ещё несколько лет. Но история не знает сослагательного наклонения, и вирус «Form» ушёл в историю так же, как и его предшественники.

Не прошло и месяца, как в Нидерландах был обнаружен опасный многокомпонентный компьютерный вирус «Anthrax»[223], который стал как бы

---

[222] Blank cycle, null cycle (англ.) – холостой или пустой цикл, отсутствие реакции на нажатие пользователем клавиш на консоли.

[223] «Anthrax» (англ.) – «Сибирская язва».

«Anthrax» был загружен сразу в несколько BBS вместе с «троянской» копией антивирусной программы «USCAN.ZIP». Отталкиваясь от названия этого вируса, которое он полу-

«предтечей» первого воистину «успешного», если так можно сказать о деятельности вредоносной компьютерной программы, многокомпонентного компьютерного вируса «Flip».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Anthrax
Другие названия	RCE1040
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	июль 1990 года
Страна происхождения	Нидерланды
Длина	1040 байт

Вирус «Anthrax» представлял собой резидентный файловый загрузочный вирус, который инфицировал файлы с расширениями «*.com» и «*.exe» (включая командный процессор «command.com»), записываясь в их конец, а также MBR «жёсткого» диска и загрузочные сектора флоппи-дисков.

При запуске на выполнение инфицированной программы «Anthrax» устанавливал себя в оперативной памяти, перехватывал прерывание INT 21h и заражал указанные файлы, длина которых увеличивалась на 1040 байт. Однако в отличие от большинства известных компьютерных вирусов «Anthrax» не начинал заражать файлы немедленно. Только после того, как наступало некоторое событие, связанное с количеством введённых с клавиатуры символов, он начинал инфицировать по одному файлу при каждом выполнении какой-либо программы. При этом заражалась не сама выполняемая программа, а другой файл, выбираемый вирусом для инфицирования сначала на логическом диске C:, начиная с корневого каталога, и далее, по всему дереву каталогов, затем на логическом диске D: и т.д. В результате все хранящиеся на «жёстком» диске файлы постепенно инфицировались и разрушались.

чил от содержащейся в его теле зашифрованной текстовой строки «ANTHRAX (c) Damage, Inc.» (Сибирская язва (с) Разрушение, зарегистрировано в качестве корпорации), некоторые специалисты вирусологи предполагали его восточноевропейское происхождение.

Но титул первого «преуспевающего многокомпонентного полиморфного компьютерного вируса» следует присвоить вирусу по имени «Flip»[224], который появился в рекордно короткие сроки вслед за вирусом «Anthrax» и быстро распространился по странам и континентам.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Flip
Другие названия	Flip.2343, Omicron
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	июль 1990 года
Страна происхождения	Германия
Длина	2343 байта

Компьютерный вирус «Flip» представляет собой файловый загрузочный вирус, который устанавливается резидентно в оперативную память, снижая её общий объём на 3064 байта, перехватывает прерывания INT 10h, 1Ch, 21h, 9Fh, заражает файлы с расширениями «*.com», «*.exe» и «*.sys», а также MBR «жёсткого» диска.

Инфицирование MBR «жёсткого» диска происходило в тот момент, когда пользователь пытался загрузить систему с заражённого флоппи-диска, причём, «Flip» уменьшал размер логического диска, и в освободившееся пространство записывал первоначальный сектор MBR и свой собственный сегмент. После этого все используемые флоппи-диски, если они не закрыты от записи, также заражались. Находясь резидентно в оперативной памяти компьютера, вирус, чтобы спрятаться, применял «стелс»-технологию, модифицируя загрузочные сектора, а также инфицированные им файлы: изменение размера, даты создания, атрибутов и т. п. Вирус «Flip» записывался в конец запускаемых пользователем файлов с расширениями «*.com» и «*.exe». В файлах проявлял себя как полиморфный вирус: шифровал себя различными способами, для чего применял разные ключи и операции, а его расшифровщик не имел постоянного участка (сигнатуры) длиннее, чем два байта. В ито-

[224] «Flip» (англ.) – «Перевёртыш». Своё имя получил благодаря визуальным эффектам, вызываемым на экране монитора.

ге «Flip» имел разные свойства при каждом новом инфицировании, что затрудняло его детектирование и уничтожение. Кроме того, он заменял в исполняемых файлах набор команд (MOV DX, Data_1; MOV Data_2, DX; MOV DX, Data_3; MOV Data_4, DX) на вызов прерывания INT 9Fh.[225]

Вирус «Flip» распространялся на другие компьютерные системы при помощи CD-ROM, сообщений электронной почты с инфицированными им вложениями, посредством удалённой загрузки заражённых программ через Интернет, на флоппи-дисках и пр. Причём, его распространение осуществлялось исключительно в файлах с расширением «*exe».

Большую часть времени этот вирус вёл себя крайне скрытно, что затрудняло его своевременное обнаружение и удаление из системы. Однако второго числа каждого месяца, между 16:00 и 16:59, «Flip» обнаруживал своё присутствие визуально, «переворачивая» экран монитора (заменял его верх низом и правую сторону левой), а также меняя расположение символов на противоположное – так называемый эффект реверсирования. Вместе с тем, подчеркнём, что это проявление деятельности вируса было возможно только на мониторах класса EGA или VGA.

Казалось, что июль 1990 года уже можно было назвать весьма беспокойным, но, в этом же месяце произошел еще один серьёзный инцидент, связанный с компьютерным журналом «PC Today» (Великобритания). Дело в том, что к каждому номеру этого журнала прилагался флоппи-диск, на котором, как выяснилось позже, был записан вирус «Disk Killer»[226] и до его обнаружения было продано более 50 тысяч экземпляров.

1 августа 1990 года был обнаружен резидентный полиморфный самостоятельно шифрующийся компьютерный вирус «Whale» («Mother Fish»).[227]

---

[225] Такое сочетание команд встречается в командном процессоре «command.com» в подпрограмме, отвечающей за вывод на экран результатов работы функций MS-DOS «FindFirst» и «FindNext».

[226] Более подробно об этом компьютерном вирусе см. выше – 1989 год.

[227] «Whale» (англ.) – «Кит».

Этот вирус был наиболее сложным и изощрённым из всех известных тогда вирусов, использующих «стелс» технологию. Вирус «Whale» проникал в компьютерные системы через Интернет с инфицированными приложениями к сообщениям электронной почты, загружаемыми программами, FTP[228], на флоппи-дисках, CD-ROM и т. п.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Whale
Другие названия	Mother Fish, Whale Mutant 01
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	август 1990 года
Страна происхождения	Германия
Длина	9216 байт

Размер «Whale» составлял примерно 6 тысяч строк исходного текста, что требовало трудозатрат по его написанию от нескольких месяцев до года усидчивого труда. В более чем девяти килобайтный программный код этого вируса автор заложил несколько уровней шифровки, а также использовал ряд весьма изощрённых методов и технических приёмов, затруднявших его трассировку и деассемблирование.

Специалисты-вирусологи, исследовавшие вирус «Whale», сошлись в едином мнении, что он был разработан программистом-профессионалом, очень хорошо знакомым с программированием непосредственно входящих в состав IBM-совместимых персональных компьютеров контроллеров. В том числе, контроллера прерываний 8259 и контроллера 8255, управляющего периферийными устройствами. Так как вирус «Whale» был тщательно зашифрован и имел самостоятельно модифицирующийся инсталлятор, его обнару-

---

Данный вирус является развитием компьютерного вируса «Fish», см. выше. Наибольшее распространение получил в Западной Европе, а также Болгарии. В СССР появление этого вируса не фиксировалось, поэтому, приводимые нами сведения основываются, в основном, на материалах: «Virus forum FIDONET». «Методы и программные средства защиты».

[228] FTP (File Transfer Protocol) (англ.) – протокол передачи файлов, используемый в Интернет для обмена данными между хост компьютерами.

жение имевшимся на то время антивирусным программным обеспечением становилось достаточно сложной задачей.

О вирусе «Whale» бывший редактор «Virus Bulletin», Джо Уэллс, впоследствии вспоминал: «Я спросил хорошо известного разработчика антивирусных средств о новом вирусе, и он предсказал нарастание хаоса и мрака. В силу обстоятельств я так никогда и не опубликовал его прогноз. Это был вирус «Whale» и наилучшее описание его действенности было дано позже на конференции по вирусам в начале 1991 года. Там Стив Уайт из IBM сказал, что «мог бы вручить компьютерный вирус «Whale» каждому в этой аудитории, а он до сих пор даже не фигурировал в печати». В то время вирус «Whale» не вызвал большого интереса у прессы, там было потрачено слишком много бумаги и чернил на доказательство бесполезности антивирусной индустрии. Много времени было потрачено впустую и самими разработчиками антивирусных средств».

Кроме описанных выше событий, хотелось бы также привести краткую информацию о том, что в 1990 году были обнаружены первые из известных компьютерных вирусов отечественного «производства»: семейство вирусов, получившее общее название «Voronezh».[229]

Однако, с точки зрения хронологии, открыл историю вирусописания в России безобидный резидентный файловый вирус «Petersburg»[230] («Petersburg.529», «RC529», «Пакость 1»), который имел длину в 529 байт, перехватывал прерывание INT 21h и, подобно всем вирусам «иерусалимской» группы, записывал себя в начало файлов с расширением «*.com» при попытке их запуска на выполнение, а старое начало переписывал в конец файла. «Petersburg» не проверял версию операционной системы, но исполь-

---

[229] «Voronezh» (англ.) – г. Воронеж.

[230] «Petersburg» (англ.) – г. Санкт-Петербург.

По некоторым данным впервые обнаружен в г. Ленинград ещё в 1989 году. Уровень программирования выдавал начинающего вирусописателя, тем более что основная часть программного кода напрямую взята из вируса «Jerusalem».

зовал имя программы, которое заносилось в «Environment» версии операционной системы MS-DOS не ниже 3.0. Этот вирус никак себя не проявлял, тем более, не нёс в себе никаких деструктивных функций, но он интересен с точки зрения летописи разработки нашими соотечественниками вредоносных компьютерных программ.

Итак, следом за вирусом «Petersburg» в 1990 году один за другим стали появляться штаммы семейства вируса «Voronezh». В связи с тем, что эти вирусы ничем особым не выделялись и не получили большого распространения, ограничимся рассмотрением двух из них: «Voronezh.600» и «Voronezh.1600».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Voronezh.600
Другие названия	600, RC600, Пакость 2, Oleynikov
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	апрель 1990 года
Страна происхождения	Россия
Длина	600 байт

Вирус «Voronezh.600» появился в СССР в середине апреля 1990 года и значительного распространения не получил.[231] Это был резидентный файловый вирус, он перехватывал прерывание INT 21h, заражал исключительно файлы с расширением «*.com»[232] и не проверял версию операционной системы MS-DOS. При запуске пользователем инфицированной программы «Voronezh.600» пробовал установить себя резидентно в оперативную память и, с целью определения своего наличия в памяти, использовал стандартный для данной группы вирусов механизм – выдавал не используемое операционной системой прерывание INT 21AB, после чего просматривал содержимое регистра «AX».

Инфицирование файлов осуществлялось при их загрузке в оперативную память на выполнение (прерывание INT 214Bh. Файлы заражались од-

[231] Обнаружен А. Сессо в г. Днепропетровск. Имеет отечественное происхождение, так как в теле вируса имеется зашифрованная строка «Oleynikov S., 1990».

[232] Командный процессор «command.com» этот вирус не инфицирует.

нократно, дата и время создания заражённого файла не менялись, а длина увеличивалась на 600 байт. Минимальная длина заражаемых файлов составляла 600 байт (258h), максимальная 60000 байт (EA60h), а файлы, содержащие в первых двух байтах значение, превышающее EF60h и с установленным атрибутом «Read Only» не заражались. В инфицированной программе тело вируса «Voronezh.600» размещалось в начале файла, и он шифровал его часть длиной в 50 байт, начиная с 16 байта от начала. При попытке инфицирования файлов, расположенных на защищённом от записи флоппи-диске иногда появлялось стандартное системное сообщение «Abort, Retry, Ignore?» («Прекратить, Повторить, Пропустить»), что было вызвано ошибкой в подпрограмме обработки прерывания INT 24h.

Следующий штамм, «Voronezh.1600»[233], также значительного распространения не получил, но представлял собой последнюю и, одновременно, наиболее сложную из семейства вирусов «Voronezh» вредоносную компьютерную программу.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Voronezh.1600
Другие названия	1600, Voronezh 2.01, RC1600, Воронеж 2.01, Пакость 3
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	июнь 1990 года
Страна происхождения	Россия
Длина	1600 байт

«Voronezh.1600» являлся резидентным файловым вирусом, заражающим файлы с расширениями «*.com» и «*.exe».

Но не это было его «изюминкой». Отечественные компьютерные вирусологи «с сожалением констатировали, что в данном вирусе реализована мысль, неосторожно высказанная Д. Н. Лозинским в документации к его полифагу «AIDSTEST» (файл aidsread.me)». Быстро восприняв высказанную известным вирусоло-

[233] Обнаружен А. Н. Мартемьяновым в г. Воронеж. Имя присвоено в связи с наличием в теле вируса соответствующей текстовой строки.

гом-профессионалом идею, неизвестный вирусописатель для затруднения обнаружения вируса обычными фагами, запрограммировал его таким образом, что вирус не менял точку входа в файле с расширением «*.exe», изменяя «Relocation Table».

При заражении файлов с расширением «*.exe» тело вируса «Voronezh.1600» дописывалось в конец инфицируемых программ, а заражались они не только при запуске на исполнение, но и во время открытия.

Интересно, что хотя уровень и стиль программирования создавали у специалистов противоречивое впечатление, они выделили ряд признаков, позволивших говорить о близости «почерка», которым написаны вирусы «Voronezh.1600» и «Voronezh.600».

В августе-сентябре 1990 года в Советском Союзе появился первый из семейства обладавших деструктивными функциями очень опасных резидентных файловых вирусов, получивших общее имя «LoveChild».[234] Компьютерный вирус «LoveChild» при создании своей резидентной копии копировал себя в таблицу векторов прерываний по адресу 0000:01E0, а затем заражал файлы с расширением «*.com» при их загрузке в память, открытии и создании. Вирус подменял первые 4 байта файла на команду перехода на своё тело (STI; JMP Loc_Virus). «LoveChild» проверял версию операционной системы и, в том случае, если на компьютерной системе была установлена операционная система MS-DOS версии 3.3, предпринимал действия, маскирующие его присутствие.

[234] «LoveChild» (англ.) – «Дитя любви», «Внебрачный ребёнок». Названия данного вируса связано с тем, что в теле вируса имеются текстовые строки: «Love Child in reward for software sealing» («Дитя любви» в наказание за закрытие доступа к программному обеспечению») и «v2 (c) Flu Systems (R)» («Гриппозные программы, версия 2»).

Идентификационная карточка вредоносной компьютерной программы	
Имя	LoveChild
Другие названия	488, LoveChild.488, Flu 2, RC488
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	сентябрь 1990 года
Страна происхождения	Россия
Длина	488 байт

Это было возможно благодаря тому, что в вирусе была заложена информация об адресе обработчика INT 21h и адресе, по которому хранилось исходное значение INT 13h. Реализуя эту информацию «LoveChild» модифицировал используемую операционной системой оперативную память, перехватывая и обрабатывая вызов прерывания INT 21h непосредственно перед MS-DOS, а также, подменяя первые пять байт обработчика прерывания INT 21h командой перехода на себя «JMP FAR Loc_Virus». Обработка вирусом прерывания INT 13h заключалась в замене адреса его обработчика на первоначальное значение, что позволяло обмануть антивирусных «сторожей», отслеживающих это прерывание, но имело и побочный эффект, заключавшийся в приведении в неработоспособное состояние драйверов, которые позволяли использовать нестандартные форматы записи на флоппи-диски.

В вирус «LoveChild» были заложены деструктивные функции: в зависимости от значения счётчика времени он мог инициировать уничтожение файлов или создавать вместо файла одноимённый подкаталог. Кроме того, этот вирус периодически изменял файлы с расширением «*.exe», после чего попытка пользователя запустить их на выполнение вызывала уничтожение данных в секторах «жёсткого» диска, то есть стиралась информация, размещённая в секторах, соответствующих 0, 1, 2 и 3 головкам его записи/чтения.

Следом за родоначальником семейства был зарегистрирован его штамм, который стал известен под именем «LoveChild.2710» и был не менее опасен, чем «папаша», но особую славу снискал благодаря своим хулиганским наклонностям.

«LoveChild.2710» представлял собой очень опасный резидентный файловый вирус, использовавший технологию «стелс». Он перехватывал прерывания INT 13h, 21h и записывался в конец файлов с расширением «*.com».

Идентификационная карточка вредоносной компьютерной программы	
Имя	LoveChild.2710
Другие названия	2710, Flu 3, RC2710
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	сентябрь 1990 года
Страна происхождения	Россия
Длина	488 байт

Вирус «LoveChild.2710» проверял версию операционной системы, так как был дееспособен только в среде MS-DOS версии 3.3, делая собственную «вставку» в её программный код. В том случае, если на компьютере пользователя была установлена любая другая версия, вирус выводил фразу: «Тебе мама не говорила в детстве, что лучше DOS версии 3.30 нет?»; после чего портил главную загрузочную запись (MBR) на «жёстком» диске. При попытке запуска инфицированных программ, начиная с полуночи и до 4 часов утра, «LoveChild.2710» выводил на печать всё содержимое экрана монитора.

Один из более поздних штаммов данного вируса (четвёртая версия «LoveChild.2710») по заданным числам (22 февраля, 30 апреля, 23 июня, 24 августа, 6 октября, 5 ноября) проявлял свою хулиганскую составляющую, посылая пользователю: «Привет от ГКЧП[235]»; после чего, стирал это сообщение с экрана монитора и выводил длиннющий текст, в котором, в частности, говорилось: «Вирусисты всех стран, соединяйтесь. Объединение МММ предлагает за рубли, по ценам ниже рыночных, отечественные вирусы, совместимые с IBM PC/AT PC/XT с любой периферией. Поставка со склада в Москве. Гарантийное и после гарантийное обслуживание. У МММ не было проблем. Love Child v4 in reward for software stealing. Love Child virus family.

[235] Напомним, что аббревиатура «ГКЧП» расшифровывается как: Государственная комиссия по чрезвычайному положению.

(c) Flu Systems. Россия-Украина. Вирусы Love Child будут появляться до тех пор, пока в СССР (или как его там) не будет принят закон об авторских правах. А пока, червонец в зубы Лозинскому». Завершалась эта «шуточка» мрачновато, так как сразу же начиналось уничтожение информации на «жёстком» диске компьютера.

Таким образом, в 1990 году вирусописателями всё шире применялись инновационные технологии и параллельно им совершенствовались уже известные приёмы написания вредоносных компьютерных программ. Среди них специалисты обычно выделяют: технологию «стелс» – позволяет вирусу «прятаться» при помощи изменения размера собственного программного кода; полиморфизм – шифрование тела вирусов и изменение алгоритма расшифровывания программного кода; многокомпонентность – способность вируса к заражению как файлов программ, так и загрузочных секторов; «бронирование» – усложнение процесса деассемблирования программного кода вируса. Кроме того, именно в 1990 году возникла новая угроза: интенсивный обмен компьютерными вирусами через BBS, так как «электронные доски объявлений» к тому времени стали содержать огромное количество компьютерных вирусов, полностью подготовленных для пересылки по линиям коммуникаций.

С другой стороны, к концу 1990 года в Западной Европе, США, Японии, Южной Корее, Австралии и целом ряде других стран было доступно для применения пользователями большое количество доброкачественных антивирусных программных средств. Например, поступил в продажу не имевший на то время аналогов «Norton AntiVirus», выпуск которого означал наступление нового этапа в процессе развития мировой индустрии антивирусных продуктов.

Год завершился учреждением в декабре в г. Гамбург (Германия) Европейского института компьютерных антивирусных исследований (EICAR), который со временем стал одной из наиболее уважаемых международных ор-

ганизаций, объедившей под своей эгидой практически всех известных в мире разработчиков антивирусных средств.

§11. 1991 год – первые программы-генераторы и конструкторы вирусов, «противо-противо-вирусный» компьютерный вирус

- Выпущена версия 5.0 операционной системы MS-DOS.
- Выпущена версия 1.3 операционной системы OS/2.
- 25 августа «день рождения» операционной системы Linux.
- Фирма Intel объявляет о выпуске сравнительно дешёвого микропроцессора Intel 80486S.

В январе 1991 года Роджером Риорданом в Австралии был обнаружен компьютерный вирус «Michelangelo».[236]

Этот вирус представлял собой типичный образец загрузочного вируса[237], устанавливающего себя резидентно в оперативную память компьютера, заражающего записи в загрузочном секторе флоппи-дисков и главную загрузочную запись (MBR) «жёстких дисков»[238], но обладал одной крайне неприятной особенностью. Если заражённая им система загружалась 6 марта, причём, любого года, вирус «Michelangelo» перезаписывал поверх полезной информации пользователя в разделы «жёсткого» диска произвольные данные, то есть «электронный мусор». Такая деятельность вируса, естественно, изменяла содержимое «жёсткого» диска компьютерной системы и вся информация, ранее записанная пользователем, терялась безвозвратно.

---

[236] «Michelangelo» (англ.) – «Микеланджело». Великий итальянский живописец и скульптор, родился 6 марта 1475 года.

[237] Вариант хорошо известного нам компьютерного вируса «Stoned».

[238] Вирус сдвигал оригинальный сектор «жёсткого» диска из сектора 0, сторона 1, цилиндр 0 в сектор 7, сторона 0, цилиндр 0.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Michelangelo
Другие названия	Michelangelo.A, Stoned.Michelangelo, Stoned.March6.a, March6
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	январь 1991 года
Страна происхождения	Австралия
Длина	2048 байт

Вирус «Michelangelo» не содержал каких-либо сообщений или информации о своём авторе, который так и остался неизвестен, но исследовавший его Роджер Риордан, заметил, что 6 марта (день активации вируса) это день рождения его знакомого – Макса Телфера, и решил дать безымянному на тот момент вирусу его имя. Но Телфер не захотел, чтобы его именем был назван «предмет» столь сомнительного свойства и предложил присвоить этому компьютерному вирусу имя кого-нибудь другого из тех кто, как и он, родился в этот день. Следуя полученному совету, Риордан назвал обнаруженный им вирус «Michelangelo» и, с тех пор имя великого итальянца стало сопровождать один из самых «нашумевших» компьютерных вирусов.

Сам факт обнаружения нового вируса не представлял собой ничего особенного, так как уже в то время каждая неделя приносила с собой несколько десятков новых вирусов[239] и их штаммов. Неординарность «славы» вируса «Michelangelo» заключалась не в том, что он был «пойман» во время реального инцидента. Этот вирус был одним из тысяч компьютерных вирусов, составляющих специализированные базы данных фирм-разработчиков антивирусных средств, более того, он даже не был замечен при регистрации реальных инцидентов с компьютерными вирусами. Вирус «Michelangelo» стал знаменитостью потому, что мог послужить причиной весьма солидного ущерба вследствие всего лишь информирования пользователей IBM-

[239] В марте 1991 года на посвящённой борьбе с компьютерными вирусами конференции, Роджер Риордан продемонстрировал копию «Michelangelo». Однако компьютерные вирусологи, которым она была показана, не придали этому событию большого значения. Проигнорировали сообщение Роджера Риордана и все специализированные издания.

совместимых персональных компьютеров о его существовании, а также потому, что ущерб мог быть нанесён в точно определённый день.

Рассказ о дальнейшей истории вируса с красивым названием «Michelangelo» мы отложим ровно на год – именно тогда и происходили связанные с ним перипетии.

Итак, в марте, «Тайный мститель», автор одноимённого вируса «Dark Avenger» и других малоприятных творений, опубликовал на болгарской BBS[240] угрожающее сообщение. В этом сообщении недвусмысленно заявлялось, что он и его «коллеги» продолжают работу по созданию нового компьютерного вируса-монстра, который сможет видоизменяться одним из четырёх миллиардов (!) различных способов. Это «электронное чудовище» так и не появилось до января 1992 года, а когда появилось, выяснилось, что на самом деле оно представляло собой программный продукт, который мог ударить по всему компьютерному и бизнес сообществам неизмеримо жёстче, чем, например, рассматривавшийся нами выше вирус «Michelangelo». На самом деле это был не компьютерный вирус, а объектный файл для компоновки и последующего получения исполняемого кода вредоносных компьютерных программ. Таким образом, миру был преподнесён «подарок» в виде программы с названием «MtE».[241] Более того, в том же марте написана первая версия программы, предназначенной исключительно для создания компьютерных вирусов – «VCS» v. 1.0.[242] Эта программа предоставляла возможности по созданию компьютерных вирусов собственного «производства» даже самому обычному пользователю, весьма отдалённо знакомому с вычислительной техникой и языками программирования.

---

[240] Об этой BBS мы уже говорили выше, см. 1990 год.

[241] «MtE» (англ.) – «Мутационный движок». Производное от английского термина «Mutation Engine».

[242] «VCS» (англ.) – данная аббревиатура обозначала «Virus Construction Set», что можно перевести как «Набор для конструирования вирусов».

Дурной пример, как известно, заразителен, и следом за «пионерами» вредоносного движения последовали новые конструкторы компьютерных вирусов и их многочисленные версии.

Весна была «в разгаре», когда был обнаружен компьютерный вирус «Tequila»,[243], который представлял собой, если так можно выразиться, «эталон» компьютерного вируса, использующего одновременно практически все самые передовые на тот момент времени технические приёмы в области вирусописания: технологию «стелс», полиморфизм, многокомпонентность.[244] Но и это ещё не всё. Данный вирус являлся не только файлово-загрузочным, «стелс», полиморфным и многокомпонентным, но был также «противо-противо-вирусным» компьютерным вирусом,[245] и использовал, к тому же, технический приём туннелирования.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Tequila
Другие названия	Tequila.A, Tequila.A. MBR
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	апрель 1991 года
Страна происхождения	Швейцария
Длина	2468 байт

Вирус «Tequila» был разработан швейцарским программистом в исследовательских целях, но один экземпляр украл его знакомый, который преднамеренно заразил флоппи-диски и компьютер своего отца, работавшего в компании по производству программного обеспечения, что и способствовало быстрому распространению вируса «Tequila» в «диком» виде среди пользователей. Практически сразу же после первого сообщения об обнаружения вируса «Tequila» произошла масштабная эпидемия,

[243] «Tequila» (англ.) – «Текила», крепкий мексиканский спиртной напиток, приготавливаемый из сока определённого вида кактусов.

[244] Такие вирусы иногда обозначают английским термином «SpoM» – Stealth, Polymorphic, Multipartite.

[245] Иногда такие вредоносные компьютерные программы называют ретро-вирусами.

когда массовые инциденты с участием этого вируса фиксировались практически по всему миру.

Вирус «Tequila» записывался в конец файлов с расширением «*.exe» при их запуске пользователем на выполнение, а также в главную загрузочную запись – «MBR» «жёсткого» диска компьютера при запуске на выполнение инфицированного файла. Оригинальный сектор с «MBR» и продолжение своего тела вирус сохранял в последних секторах логического диска C:, уменьшая при этом объём «жёсткого» диска в «Disk Partition Table»[246]. Оперативную память вирус «Tequila» заражал только в том случае, если загрузка компьютерной системы осуществлялась при уже заражённой «MBR». Этот вирус перехватывал прерывания INT 13h, 1Ch, 21h и, в зависимости от значения своего внутреннего счётчика, выводил на экран монитора разноцветную картинку, содержащую символы псевдографики в кодировке ASCII (American Standard Code for Information Interchange)[247] и сопровождавшую её фразу: «Execute: mov ax, FE03/int 21. Key to go on!» (Выполнить: mov ax, FE03/int 21. Разгадка картинки впереди!) Если пользователь подчинялся требованию, на экране появлялся следующий текст: «Welcome to T. TEQUILA's latest production. Contact T. TEQUILA/P.o.Box 543/6312 St'hausen/Switzerland. Loving thoughts to L.I.N.D.A. BEER and TEQUILA forever! («Добро пожаловать, самое последнее изделие Т. ТЕКИЛА. Связываться Т. ТЕКИЛА/а.я. 543/6312 Святой Хаусен/Швейцария. Преданный мыслями Л.И.Н.Д.А. ПИВО и ТЕКИЛА навеки!»).

Интересно, что эпидемия вируса «Tequila», превратившаяся в пандемию, обошла Россию стороной, и было отмечено лишь незначительное количество случаев инфицирования им компьютерных систем.

---

[246] «Disk Partition Table» (англ.) – «Таблица разделов диска», которая представляет собой область в главной загрузочной записи (MBR), которая используется компьютером для определения доступа к диску.

[247] American Standard Code for Information Interchange (ASCII) – Американский стандартный код для обмена информацией, код ASCII.

Лето 1991 года прошло на удивление спокойно. Нет, «производство» компьютерных вирусов и их штаммов не останавливалось ни на минуту, и они штамповались по всему миру десятками, если не сотнями, но представляли собой либо ничем не примечательные поделки, либо использовали уже имевшийся и хорошо изученный специалистами арсенал технических приёмов, что позволяло своевременно пресекать их широкое распространение.

Наступление осени ознаменовалось новой эпидемией, которая началась в сентябре благодаря полиморфному компьютерному вирусу «Amoeba»,[248] когда так же, как в истории с вирусом «Tequila», практически всё мировое компьютерное сообщество вынуждено было бороться с этой вредоносной компьютерной программой.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Amoeba
Другие названия	Amoeba.2367, Maltese Amoeba, Gr
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	сентябрь 1991 года
Страна происхождения	Мальта
Длина	2367 байт

Вирус «Amoeba» был очень опасным полиморфным вирусом, резидентно устанавливавшим себя в оперативную память компьютерной системы. Он перехватывал прерывание INT 21h и записывал себя в конец файлов с расширениями «*.com» и «*.exe» при их запуске или открытии. Размер всех инфицированных этим вирусом файлов увеличивался на величину от 2504 до 2564 байт. Более того, у заражённой им системы «Amoeba» «откусывал» часть имеющейся свободной оперативной памяти, уменьшая её объём на 4096 байтов.

Деструктивная составляющая данного вируса срабатывала во время загрузки пользователем операционной системы 25 марта и 1 ноября каждого

---

[248] «Amoeba» (англ.) – «Амёба», простейший одноклеточный биоорганизм.

Судя по дате в теле этого вируса он был написан весной 1991 года одним из студентов университета Мальты, а примерно через полгода был замечен в «диком» виде и стал виновником эпидемии.

года. При загрузке системы в указанные календарные числа «Amoeba» перезаписывал информацию первых секторов «жёсткого» диска и любых флоппи-дисков, которые в данный момент использовались в системе. Кроме того, во время активации загрузки вирус высвечивал на экране монитора мигающее сообщение в виде четверостишья с философским уклоном:

To see a world in a grain of sand,	Наблюдать вселенную в песчинке,
And a heaven in a flower	И небеса в цветении,
Hold infinity in the palm of your hand	Держа бесконечность в ладони
And eternity in an hour.	И бессмертье во времени.

После завершения процесса разрушения информации вирус «Amoeba» показывал на дисплее монитора своё сообщение: «THE VIRUS 16/3/91 AMOEBA virus by the Hacker Twins (C) 1991. This is nothing, wait for the release of AMOEBA II – The universal infector, hidden to any eye but ours! Dedicated to the University of Malta the worst educational system in the universe, and the destroyer of 5X2 years of human life». («ВИРУС 16/3/91 AMOEBA вирус от Хакеров-двойняшек (C) 1991. Это пустяки, подождите выхода в свет «AMOEBA II», универсальной заразы, невидимой для любых глаз, кроме наших. Посвящён университету Мальты, имеющему наихудшую систему обучения во вселенной, а также разрушителю пяти лет человеческой жизни, помноженных на два). Затем вирус «подвешивал» компьютер.

Идентификационная карточка вредоносной компьютерной программы	
Имя	DirII
Другие названия	Dir-II.A, Dir_II, Dir-II, DirII.2048, Dir2.byway, By_Wai, Dir-II.Byway, DirII.TheHndV, DIR-Byway
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	октябрь 1991 года
Страна происхождения	Венесуэла
Длина	2048 байт

В октябре 1991 года был обнаружен вирус, «DirII», который был отнесён специалистами к новому типу компьютерных вирусов, так как он использовал собственный метод распространения.[249] Этот вирус размещал на «жёстком» диске компьютера свою единственную копию, а затем заражал установочные параметры кластерных указателей в секторах директория, чтобы указывать на себя. Но, обо всём по порядку.

Семейство «кластерных» вирусов, родоначальник которого получил имя «DirII», представляет собой резидентные и очень опасные вредоносные компьютерные программы, которые использовали «стелс» технологию и заражали файлы с расширениями «*.com» и «*.exe» при чтении и записи секторов директорий, в которых хранилась информация об этих файлах. «DirII» и его штаммы сохраняли своё тело в последнем кластере инфицированного логического диска, и этот кластер помечался как последний в цепочке кластеров.

При инфицировании файла вирусы изменяли исключительно номер кластера, указанного в служебных областях «жёсткого» диска компьютера первым кластером файла, на номер кластера, содержащего тело вируса. Таким образом, при заражении файлов их размер и содержимое кластеров с инфицированными файлами не изменялись, причём, на все заражённые файлы на логическом диске приходилась единственная копия вируса. При инициализации вирусы данного семейства проникали в ядро операционной системы MS-DOS и меняли адрес системного драйвера, ответственного за управление

[249] Вирусы этого типа были классифицированы как «кластерные» или «линк» вирусы.

дисками компьютера. После этого они перехватывали все обращения операционной системы к этому драйверу.

Автор «DirII» позаботился также и о повышенных мерах маскировки своего детища с помощью технологии «стелс» – в него был заложен тщательно продуманный программный код, реализующий указанную технологию на уровне системного драйвера. Такой приём позволил превратить «DirII» в «призрак», который не был виден в инфицированных файлах при их чтении через прерывания INT 25h и INT 21h.

Это семейство очень опасно ещё и тем, что его представители были наделены способностью прямого обращения к ресурсам операционной системы и проникали сквозь антивирусные средства защиты, а также обладали высокой скоростью распространения в компьютерной системе. Высокая скорость распространения вирусов «DirII» стала возможной благодаря удачно использованной организации механизма поиска, реализованного в среде MS-DOS: при попытке запуска несуществующего файла эта операционная система инициирует его поиск во всех каталогах, которые прописаны в «PATH». Пользуясь этим, «DirII» перехватывал обращения MS-DOS к каталогам и последовательно инфицировал файлы в тех каталогах, которые были поименованы в «PATH». Во время первой загрузки вирусы этого семейства поражали все файлы текущего каталога логического диска C:.

В соответствии с отчётами специалистов, в которых приводились данные о регистрации реальных инцидентов с компьютерными вирусами, эпицентром эпидемии вируса «DirII» следует признать Центральную Америку и, особенно, Венесуэлу, а также столицу Мексики, город Мехико. Быстро распространившись в Центральноамериканском регионе этот вирус и его штаммы «завоевали» сначала весь континент, а затем, перебравшись через Атлантический и Тихий океаны, начали «покорение» других частей света.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Monkey
Другие названия	Empire, Stoned.Empire. Monkey, Stoned .Monkey, Empire .Monkey
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	ноябрь 1991 года
Страна происхождения	Канада
Длина	512 байт

В конце 1991 года появился ещё один компьютерный вирус, представляющий определённый интерес с точки зрения истории вирусописания. Он был обнаружен в г. Эдмонтон (Канада), получил имя «Monkey» и в короткий срок распространился в США и Австралии, а затем «перекочевал» в Западную и Восточную Европу, став одним из наиболее известных и распространённых загрузочных компьютерных вирусов того времени.

Этот вирус являлся подобием и развитием известного вируса «Stoned»,[250] но более полно использовал «стелс» технологию и сохранял исходную главную загрузочную запись (Master Boot Record – MBR) в зашифрованной форме. В отличие от вируса «Stoned» он не покидал исходную таблицу разделов[251] для инфицирования дисковода. В результате дисковод становился невидимым для операционной системы MS-DOS, если компьютерная система загружалась с заражённого вирусом «Monkey» флоппи-диска.

Дополнительной проблемой, связанной с «Monkey», являлось применение технического приёма «cure-all»[252], который был разрекламирован, снискал популярность и стал общеизвестен у пользователей после того, как был испытан ими в процессе лечения своих компьютеров от нашумевшего вируса «Michelangelo»[253]. Дело заключалось в том, что указанная техника

[250] Более подробно об этом компьютерном вирусе см. выше – 1987 год.

[251] Таблица разделов (partition table) – область в главной загрузочной записи.

[252] Cure-all – панацея, лечение от всех болезней.

[253] Более подробно об этом компьютерном вирусе см. выше – 1991 и 1992 годы.

применяла недокументированную опцию утилиты FDISK[254], используя команду «fdisk/mbr», которая записывает часть программного кода MBR, но не вносит какие-либо изменения в таблицу разделов в MBR. Вследствие того, что подобные «Stoned» и «Michelangelo» компьютерные вирусы переписывают начальный вирусный код и оставляют в том же состоянии информацию о разделах технический приём «cure-all» полностью уничтожает эти вирусы. В случае с вирусами, подобными «Monkey», которые не сохраняют информацию о разделах, использование этой команды «убивает» сам компьютерный вирус, но оставляет нетронутым программный код вируса в таблице разделов.

Если брать в целом, то 1991 год можно оценить как весьма спокойный, особенно на фоне событий, которые происходили в предыдущие годы. Однако специалисты предупреждали о том, что «по всему миру возникают новые станции, ориентированные на обмен вирусами, а также появляются субъекты, решившие посвятить свою жизнь созданию вирусов: в Италии – «Cracker Jack», в Германии – «»Gonorrhoea», в Швеции – «Demoralized Youth», в США – «Hellpit», в Англии – «Dead On Arrival» и «Semaj» и другие, подобные им, личности». Кроме того, подчёркивалось, что популяция компьютерных вирусов непрерывно растёт.

Однако, параллельно с этими, негативными явлениями, усиливалась и деятельность, направленная на борьбу с вредоносными компьютерными программами. Например, такие корпорации, как Symantec и Central Point, выпустили собственные антивирусные программы – «Norton Anti-Virus» и «Central Point Anti-Virus», соответственно.

§12. 1992 год – новые приёмы маскировки, вирусы для платформы «Macintosh», первый «пермутативный» вирус и первый компьютерный

---

[254] FDISK – утилита (обслуживающая программа), предназначенная для разбиения «жёсткого» диска компьютера на разделы (логические диски). Поставляется в составе программного обеспечения операционной системы MS-DOS.

вирус, разработанный специально для операционной системы MS Windows 3.xx, а также польза и вред от околовирусной шумихи

- Выпущены версия 3.1 операционной системы MS Windows (введена поддержка шрифтов True Type, обеспечена нормальная работа в локальной сети, появились технологии Drag&Drop – перенос мышкой файлов и директорий, а также OLE – Object Linking & Embedding) и Windows 3.11 for Workgroups, в которой были расширены средства поддержки сети.
- Выпущена версия 2.0 операционной системы OS/2.
- Выпущена операционная система Windows NT 3.5, которая вобрала в себя все основные сетевые функции операционной системы OS/2.
- Выпущена версия 0.96 операционной системы Linux, которая обладала графическим интерфейсом и являлась полнофункциональной системой для работы на платформе Intel x86.
- Выпущен микропроцессор Intel 80486 DX4.
- Появился первый ноутбук с микропроцессором Intel 80486.

В январе 1992 года «Тайный мститель» выполнил своё обещание и опубликовал на BBS в Интернет окончательную версию программного кода полиморфик-генератора «MtE».[255].

Но компьютерные вирусологи хорошо знали о высокой профессиональной подготовке «Тайного мстителя» и прекрасно понимали, что его угроза годичной давности о подготовке «вируса-монстра» имеет под собой вполне реальную почву и будет им исполнена. Поэтому, параллельно с усилиями «Тайного мстителя» по созданию «MtE», специалистами были интенсифицированы научно-исследовательские работы в области полиморфизма компьютерных вирусов. Например, незадолго до появления этого полиморфик-генератора Алан Соломон и Фридрих Скуласон закончили комплекс исследований, посвящённых принципам построения и расшифровке постоянно видоизменяемых программ, а также дали своё определение термину «поли-

[255] До этого момента компьютерные вирусологи располагали отдельными фрагментами этой вредоносной программы, которых, впрочем, было достаточно для того, чтобы спрогнозировать высокий уровень её опасности.

морфный» применительно к компьютерным вирусам.[256] Опираясь на результаты проведённых работ по исследованию полиморфизма вирусов, а также итоги анализа ранее доступных фрагментов «MtE специалисты к моменту его появления уже могли обнаруживать шаблоны этого полиморфик-генератора.

Анализ окончательной версии программного кода полиморфик-генератора «MtE» подтвердил очень высокую степень его опасности, требующую принятия немедленных контрмер и продолжения теоретических и прикладных исследований в области полиморфных (или, иначе, «мимикрирующих») компьютерных вирусов, обладающих впечатляющими способностями по своей реконфигурации, что может повлечь «бум» в их написании.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Dedicated
Другие названия	Dedicated.3506#MTE
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	январь 1992 года
Страна происхождения	Болгария
Длина	3506 байт

Прогноз специалистов вирусологов сбылся и, в итоге ознакомления широкого круга вирусописателей с принципами работы и возможностями «MtE», уже в январе 1992 года появилось сразу несколько полиморфных вирусов, базирующихся на этом мутационном движке[257].

К числу этих вредоносных компьютерных программ относится

[256] Забегая немного вперёд, добавим, что в марте была напечатана статья Джона Дворака о «MtE», где рассматривались полиморфизм и многокомпонентность компьютерных вирусов.

[257] Их появление поставило производителей антивирусного программного обеспечения перед серьёзной проблемой, так как некоторые из их продуктов даже по прошествии нескольких месяцев не гарантировали 100% результата при обнаружении полиморфных вирусов, созданных с использованием «MtE».

и знаменитый вирус «Dedicated»[258], который открыл длиннющую серию вирусов, построенных с помощью полиморфик-генератора «MtE».

Компьютерный вирус «Dedicated» проникал в компьютерную систему вместе с заражёнными приложениями к сообщениям электронной почты, переносился с заражённых флоппи-дисков и CD-ROM, в процессе работы с Интернет, FTP и пр. Копии «Dedicated» распространялись на другие компьютеры вместе с инфицированными им файлами или программами. «Dedicated» использовал следующие стратегии инфицирования компьютерной системы:

при первой загрузке заражённого файла или программы вирус резидентно устанавливал себя в оперативную память и перехватывал принадлежащие операционной системе функции. После этого, каждый раз, когда операционная система или прикладная программа пытались получить доступ к любой из этих функций, вирус активизировался и заражал новые файлы;

используя полиморфизм, после завершения очередного заражения вирус шифровал разными способами своё тело, для чего использовались различные ключи и операции. В итоге, при каждом новом инфицировании вирус изменял свои параметры, что затрудняло его обнаружение при помощи антивирусного программного обеспечения.

Деятельность вируса «Dedicated» могла приводить к повреждению заражённых компьютеров, однако этот первый вирус на основе «MtE» не попал в «живую природу» и поэтому не вызвал эпидемии, а разработчики антивирусных средств получили некоторый запас времени для подготовки к отражению новой угрозы.

В 1992 году вирусописатели использовали и принципиально новые приёмы маскировки своего кода в заражённых файлах.

---

[258] «Dedicated» (англ.) – «Открывающий». Обычно употребляется в смысле открытия новой эпохи, выставки, партии изделий и т. п.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Emmie
Другие названия	Emmie.2702
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	январь 1992 года
Страна происхождения	Израиль
Длина	2702 байта

Именно такими приёмами пользовалось семейство вирусов, родоначальником которого стал впервые обнаруженный в январе вирус «Emmie»[259]. Он не использовал специфичные способы для своего распространения, копируя собственный программный код в другие файлы и программы и проникая в компьютер пользователя с помощью любого из средств, обычно используемых компьютерными вирусами: флоппи-диски, CD-ROM, сообщения электронной почты с заражёнными вложениями, загрузка программ через Интернет, FTP и т. п. Однако, в целях своей маскировки данный вирус применял различные ухищрения, шифруя заново собственное тело сразу после заражения очередного файла и применяя при этом разные операции и методы шифрования. В результате «Emmie» постоянно изменял основные характеристики своего программного кода, затрудняя работу антивирусного программного обеспечения по его обнаружению, блокированию и удалению из компьютерной системы.

Во время загрузки операционной системы вирус резидентно устанавливал себя в оперативную память и перехватывал прерывания INT 9, 10h, 17h, 21h и 27h. Поэтому, каждый раз, когда операционная система или прикладная программа пытались получить доступ к любой из этих функций, «Emmie» активизировался и инфицировал новые файлы. Кроме перечисленного выше, вирус «Emmie», как и все его последующие штаммы[260], инфицировал файлы с расширением «*.com» при их выполнении, изменял цифры, выводимые на

[259] «Emmie» (англ.) – «Эмми», уменьшительное от имени Эмма.

[260] Среди довольно многочисленных штаммов, представляющих семейство «Emmie», наиболее вредоносными считаются «Emmie.2823», «Emmie.3072» и «Emmie.3097», периодически стирающие сектора «жёсткого» диска.

экран монитора и принтер, а также повторял символы, вводимые с клавиатуры.

Обнаруженные в марте-апреле штаммы «Emmie.2823» и «Emmie 3072» использовали алгоритм самошифрования, записывали себя в конец файлов, изменяли вторую (не первую!) команду в файле на команду перехода на вирус. Оба штамма содержали в своём теле текстовые строки: «Emmie.2823» – «My name is Emmie, I am Eddie`s[261] sister …» («Моё имя Эмми, я сестра Эдди …»); «Emmie.3072» – «My name is Emmie+, I am Eddie`s sister». («Моё имя Эмми+, я сестра Эдди».)

В мае был обнаружен новый и самый опасный штамм – Emmie.3097. Сразу после того, как этот вирус устанавливал себя резидентно в оперативную память, он начинал камуфлировать своё присутствие там при помощи внесения разнообразных изменений в загрузочные сектора «жёсткого» диска компьютера, а также инфицированные им файлы. Эти изменения представляли собой: изменения размера, дат, атрибутов и т. п. Опасность такой бурной деятельности очевидна, особеннов сочетании со склонностью Emmie.3097 периодически повторять операцию стирания секторов «жёсткого» диска.

Не прошло и года после появления вируса «Tequila»[262] (который, как мы помним, был первым «противо-противо-вирусом», или «ретро-вирусом»), как всё чаще стали появляться его последователи, эксплуатирующие ту же идею. Например, в феврале 1992 года был зарегистрирован компьютерный вирус «Peach»[263], который удалял базу данных ревизора изменений пакета «Central Point AntiVirus», а антивирусная программа не находя этой базы данных считала, что запущена в первый раз и незаметно для пользователя со-

---

[261] Здесь прослеживается явный намёк автора на родство своего детища с такими знаменитостями как «Dark Avenger» и «Beast». См. 1989 и 1990 годы, соответственно.

[262] Более подробно об этом компьютерном вирусе см. выше – 1991 год.

[263] «Peach» (англ.) – «Персик». В переносном смысле слова можно перевести в значениях «Первый сорт» или «Милашка».

здавала её заново. При помощи этого приёма «Peach» обходил защиту и постепенно заражал всю систему.

Февраль и март 1992 года были ознаменованы всплеском публикаций, посвящённых нашему старому знакомому – компьютерному вирусу «Michelangelo»[264]. Как и в случае с компьютерным вирусом «DataCrime» в 1989 году, «Michelangelo» стал мелькать в заголовках прессы с начала 1992 года. Правда разница заключалась в том, что на момент появления «Michelangelo» действовало гораздо больше компаний-разработчиков антивирусных средств, которые вели жёсткую конкурентную борьбу между собой. В те недели, предшествующие 6 марта 1992 года, в мире происходили различные небезынтересные события, однако … Удивительное «взаимопонимание и сотрудничество» между средствами массовой информации и отдельными, крупными представителями антивирусной индустрии в этом вопросе, сделали довольно заурядный компьютерный вирус «Michelangelo» главным действующим лицом новостных сообщений, «гвоздём» информационных программ и «звездой» телевизионного экрана. Сообщения в печати пестрели предупреждениями об огромных разрушительных способностях «Michelangelo», описание его деструктивных характеристик транслировались по радио и в передачах главных телевизионных сетей. Статьи о «Michelangelo» постоянно появлялись в самых солидных газетах и журналах. 6 марта приближалось, количество сообщений росло как снежный ком, а их тон становился всё более истеричным. Прогнозируемое количество компьютерных систем, которые под воздействием «Michelangelo» могут быть уничтожены, выросло с сотен до тысяч и затем до миллионов[265]. Прогнозируя масштабы последствий от разрушительной деятельности «Michelangelo» представитель одной из компаний-разработчиков антивирусного программного обеспечения утверждал,

---

[264] Дополнительную информацию об этом компьютерном вирусе см. выше – 1991 год.

[265] J. McAfee, quoting expert sources on The MacNeil/Lehrer News Hour, March 5, 1992.
Joshua Quittner, «Michelangelo Virus: No Brush With Disaster», New York Newsday, April 5, 1992.

что ни много, ни мало, а «5 миллионов компьютерных систем могут быть повреждены в той или иной степени»; представитель другой компании заявлял, что «последствия его действий будут более похожи на то, как если бы в клавиатуру Вашего компьютера вылили кофе, чем Вы просто подцепили какую-то компьютерную заразу». Когда же решающая дата наступила, предсказания «о всеобщей погибели» быстро сошли на нет[266]. Вирус «Michelangelo» обнаружили на некоторых системах и на отдельных из них были разрушены данные, но всемирной катастрофы не случилось. На самом деле было трудно привести даже какое-либо значимое число достоверных происшествий, вследствие которых «Michelangelo» безвозвратно разрушил бы данные[267]. Но несмотря на то что было зафиксировано довольно незначительное количество реальных случаев инфицирования компьютерных систем вирусом «Michelangelo» (во всём мире в той или иной мере пострадало всего лишь около 10 тысяч компьютеров), уровень продаж антивирусного программного обеспечения воспарил ввысь и достиг небывалых показателей.

Небольшое количество пострадавших компьютерных систем не стало сюрпризом для серьёзных специалистов-вирусологов, чьи исследования показывали, что вирус «Michelangelo» не очень распространён и, несомненно, не относится к числу уникальных компьютерных вирусов. Например, по оценкам специалистов фирмы IBM, «примерно такое же число компьютерных систем, которые имели 6 марта отказы «жёстких» дисков якобы под воз-

---

[266] В этом плане показательны заголовки в «Los Angeles Times»: «Надвигается День страшного суда для инфицируемых PC» – 20 февраля; «Вирус «Michelangelo» жив, опасен и ожидается 6 марта» – 21 февраля; «Компьютерный вирус «Michelangelo» для персональных компьютеров» – 4 марта; «Скоро вирус «Michelangelo» поразит персональные компьютеры различных фирм» – 6 марта; «Большинство сумеет ускользнуть от кисти «Michelangelo» – 7 марта; «Немногочисленные серьёзные сбои от ужасного компьютерного вируса» – 8 марта.

[267] Michael W. Miller, «Michelangelo» Scare Ends In an Anticlimax», The Wall Street Journal, March 9, 1992.

действием «Michelangelo», могло отказать по причине рутинных сбоев в их аппаратном обеспечении». Однако важно помнить и учитывать в перспективе урок, преподнесённый шумихой вокруг этого компьютерного вируса. Сумасшествие «Michelangelo», как стали в итоге называть этот инцидент, всё равно произвело неизгладимое впечатление. Озабоченная предсказаниями широкомасштабной угрозы огромная часть пользователей, которая ранее вообще не использовала какие-либо средства антивирусной защиты, приобрела и установила современное антивирусное программное обеспечение. Выстраивались длинные очереди людей, которые желали немедленно купить антивирусное средство. Многие магазины полностью распродали все свои запасы антивирусного программного обеспечения всего лишь за неделю, предшествовавшую 6 марта.

Практически по всему миру, именно в те дни очень большое количество пользователей впервые подвергло проверке свои компьютеры на наличие вирусов. За две недели до наступления 6 марта 1992 года количество сообщений о вирусных инцидентах выросло до небывалых высот. Разумеется, этот «взрыв» произошёл не потому, что процесс распространения компьютерных вирусов вышел из-под контроля именно в эти две недели. Вернее всего, в эти дни и недели пользователями были выявлены компьютерные вирусы, которые скрытно присутствовали в компьютерных системах, просто потому, что они более интенсивно их искали. Факт остается фактом: множество пользователей проверило свои компьютеры и, следовательно, вредоносные компьютерные программы были уничтожены. Пользователи искали вирус «Michelangelo», а находили, зачастую, множество компьютерных вирусов иных разновидностей. Компьютерный вирус «Stoned»[268], например, был гораздо более распространён в то время, и обнаруживался примерно в три раза чаще, чем вирус «Michelangelo». За первые несколько месяцев после окончания «сумасшествия по поводу «Michelangelo»», было зафиксировано меньше

[268] Более подробно об этом компьютерном вирусе см. выше – 1987 год.

инцидентов с вирусами, чем в течение нескольких месяцев до того и это не удивительно.

Итак, вероятные инциденты с вирусами были пресечены прежде, чем они могли произойти, так как многие вирусы были выявлены и уничтожены, а могли бы быть обнаружены, например, только в начале апреля. Кроме того, компьютерные вирусы были обнаружены и уничтожены даже в тех системах, в которых их никогда не искали и могли не искать и дальше на протяжении длительного периода времени. Безусловно, что за немногие дни популяция компьютерных вирусов во всём мире понесла серьёзные потери.

Несмотря на благоприятное воздействие вполне очевидно, что истерия, связанная с вирусом «Michelangelo» была чрезмерной по отношению к степени его опасности. Как частные лица, так и организации всех форм собственности потратили крупные денежные средства и массу времени на предотвращение угрозы, которая была многократно меньше, чем они её себе представляли. Остаётся надеяться, что все извлекли урок из этого случая и особенно это касается антивирусной индустрии, представители которой должны быть более осторожными в заявлениях, где они дают оценку грядущей вирусной угрозы, а также средств массовой информации, которые должны беспристрастно перепроверять различные прогнозы относительно неминуемой гибели, и рассматривать такие «предсказания» более критически. Тем более что вследствие истерии, которую компании-разработчики антивирусных средств восприняли как праздник, некоторые из них чрезмерно раздули свои штаты и расходы, а в итоге оказались не готовыми к падению объёмов продаж, который произошёл во второй половине 1992 года и, естественно, разорились.

Тем, кого интересует полный, документальный обзор истерии, поднятой в средствах массовой информации в отношении компьютерного вируса «Michelangelo», мы рекомендуем прочесть статью Памелы Кейн «Анализ ви-

русной паники»[269], а также её же книгу «Справочное руководство по безопасности персонального компьютера и защите против компьютерных вирусов»[270]. Мы же резюмируем вышесказанное следующим образом: это был первый известный случай столь масштабного раздувания шумихи антивирусных компаний вокруг компьютерного вируса не для защиты пользователей от какой-либо опасности, а для извлечения коммерческой выгоды от привлечения внимания к своим продуктам.

В апреле-июне появилось сразу несколько компьютерных вирусов, ориентированных на платформу «Macintosh».

Первым из их числа стал файловый вирус, получивший имя «Mac/INIT-1984». Этот вирус заражал исключительно системные объекты баз данных и не инфицировал системные файлы и прикладные программы, а так как пользователи крайне редко обмениваются этими файлами, «Mac/INIT-1984» распространялся очень медленно. Данный вирус активизировался в том случае, если инфицированный им «Macintosh» начинал работу в пятницу, которая попадала на тринадцатое число любого месяца и года. «Mac/INIT-1984» случайным образом менял имена файлов, а также подменял имена создателя и типы файлов. Кроме того, он «исправлял» даты создания и модификации файлов на 1 января 2004 года. Деструктивная сущность этого вируса проявлялась в том, что он уничтожал до 2% данных от общего объёма информации, хранящейся на «жёстком» диске инфицированного компьютера.

Вторым стал файловый вирус, получивший имя «Mac/CODE-252», который был запрограммирован таким образом, что всю первую половину года вёл латентный образ существования, визуально никак себя не проявляя. В этот период вирус занимался скрытым распространением, инфицируя прикладные программы и системные файлы. Зато во второй половине года, начиная с июля, «Mac/CODE-252» как будто навёрстывал упущенное, выводя

---

[269] Pamela Kane «Anatomy of a Virus Scare». ISP News of May/June 1992.

[270] Pamela Kane «P.C. Security and Virus Protection Handbook».

на экран монитора, если запускалась заражённая программа или инфицированный им «Macintosh» начинал работу, следующее сообщение:

«You have a virus. Ha Ha Ha Ha Ha Ha Ha Ha Now erasing all disks... Ha Ha Ha Ha Ha Ha Ha Ha P.S. Have a nice day Ha Ha Ha Ha Ha Ha Ha Ha (Click to continue)»	«Вы заполучили вирус Ха Ха Ха Ха Ха Ха Ха Ха Сейчас стираются все диски … Ха Ха Ха Ха Ха Ха Ха Ха P.S. Славный денёк Ха Ха Ха Ха Ха Ха Ха Ха (Щёлкните мышью для продолжения)

Ни файлы, ни директории при этом не удалялись, но, если напуганный пользователь инициировал рестарт системы, он мог понести ущерб, например, в виде потери не сохранённых файлов. Кроме того, инфицирование «Macintosh» этим вирусом иногда приводило к аварийному отказу системы. Интересно, что «Mac/CODE-252» был не способен заражать прикладные программы, устанавливаемые на уже инфицированной операционной системе версии 7.0 или более поздних версий.

В июне появился третий файловый вирус для платформы «Macintosh», который так же, как и другие его собратья, получил весьма «сухое» имя «Mac/T4» и был впервые обнаружен при попытке своего распространения с играми под названием «GoMoku 2.0» и «GoMoku 2.1». Этот вирус заражал сервисную службу «Finger» операционной системы и, в тех случаях когда «Mac/T4» инфицировал системный файл, загрузка файлов с системными расширениями становилась невозможной. На «Macintosh» под управлением операционной системы System 7.0.1 или более поздних версий вирус мог стать причиной аварийного отказа компьютера, который выражался, например, в невозможности загрузки системы. Более того, «Mac/T4» пытался замаскировать свою деятельность, «притворяясь» антивирусной программой «Disinfectant»[271].

[271] «Disinfectant» (англ.) – «Дезинфицирующее средство».

Как оказалось, набивший оскомину «Тайный мститель» не сидел сложа руки после создания полиморфик-генератора «MtE» и к началу лета создал своё очередное творение, которое называлось «Bomber»[272].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Bomber
Другие названия	Bomber.4096, Commander Bomber
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	май 1992 года
Страна происхождения	Болгария
Длина	4096 байт

В историю вирусописания эта вредоносная компьютерная программа вошла по той причине, что она использовала новый м («пспособ при инфицировании компьютерной системы – «Bomber» стал первым полиморфным перестановочныермутативным») компьютерным вирусом, и специалистам-вирусологам пришлось срочно формулировать для его описания новое определение. Кстати, автор знаменитого вируса «One_Half», речь о котором впереди, пошёл по стопам «Тайного мстителя» и использовал схожий метод заражения.

Итак, «Bomber» представлял собой тщательно продуманный, полиморфный и очень сложный компьютерный вирус, который резидентно оставался в оперативной памяти компьютера и инфицировал файлы с расширением «*.com» при их выполнении. Вирус вставлял себя в середину хост файла и порождал сложные последовательности ветвящихся команд с целью встраивания своего кода в программы, которые открывались для исполнения. Он содержал подпрограммы, которые вырабатывали случайный код, вставляемый затем в случайно выбранные места в хост файле. Такие фрагменты кода компоновались в последовательности сложнейшим образом разветвляющихся команды. В данных фрагментах программного кода использовались практически все документированные инструкции архитектуры 80x86, делая

[272] «Bomber» (англ.) – «Бомбометатель», «Гранатомётчик», «Бомбардировщик». Вместе с тем, если пользоваться американским сленгом, данное слово можно перевести как «Сигарета с марихуаной».

«Bomber» крайне трудным для обнаружения. «Bomber» изменял своё тело, шифруя его при помощи различных методов по завершении каждого инфицирования и применяя при этом различные операции. В результате, вирус после инфицирования очередного файла приобретал новые свойства, которые затрудняли его обнаружение антивирусным программным обеспечением. Именно по этому пути пошли некоторые более поздние вирусописатели при разработке собственных творений, «шлифуя и оттачивая» подсказанные им идеи.

«Bomber» содержал в своём теле следующие не зашифрованные текстовые строки:

COMMANDER BOMBER WAS HERE	COMMANDER BOMBER был здесь
[DAME] [DAME]	[Дама] [Дама]

Пятого июля 1992 года объявлен к выпуску первый конструктор вирусного кода для IBM PC совместимых компьютеров – пакет «VCL»[273], а 27 июля появилась первая версия конструктора «PS-MPC»[274], который также позволял создавать резидентные вирусы. Таким образом, эти конструкторы давали вирусописателю возможность быстрого «написания» новых вирусов различных типов и модификаций и ихс дополнения большим «набором» деструктивных действий. Эти программы увеличили поток новых вирусов и, как и «MtE», подтолкнули вирусописателей к созданию ещё более мощных конструкторов. «Всё сразу стало значительно проще: захотел напакостить ближнему – садись за «VCL» и, за 10–15 минут сделав 30–40 разных вирусов, запусти их на неприятельском компьютере. Каждому компьютеру отдельный вирус!», – это сказано известным специалистом в области компьютерных вирусов по поводу ситуации, сложившейся после выхода пакета «VCL». Со времени выхода в свет конструкторов «VCL» и «PS-MPC» много воды утек-

[273] «VCL» (Virus Creation Laboratory) – «Лаборатория по созданию вируса».

[274] «PS-MPC» (Phalcon/Skism Mass-Produced Code Generator) – «Программа-генератор массового производства кода Phalcon/Skism».

ло, но, если внимательно присмотреться к перечню вирусов, содержащемуся в каком-либо из антивирусных программных продуктов, то можно увидеть массу компьютерных вирусов, которые были сконструированы с помощью «VCL» или «PS-MPC».

Идентификационная карточка вредоносной компьютерной программы	
Имя	ExeBug
Другие названия	ExeBug.A, CMOS-1, CMOS Killer, Int_0B, Exe_BUg.A, Exe_Bug, Exe_Bug.Hooker, Hooker, Swiss Boot
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	август 1992 года
Страна происхождения	Швейцария
Длина	3506 байт

В августе был обнаружен очень опасный компьютерный вирус «ExeBug»[275], который представлял собой достаточно сложную программу, инфицировавшую главную загрузочную запись «жёстких» дисков и загрузочный сектор флоппи-дисков. Этот вирус проникал в компьютерную систему вместе с заражёнными приложениями к сообщениям электронной почты, переносился с заражённых флоппи-дисков и CD-ROM, в процессе работы с Интернет, FTP и пр. Копии «ExeBug» распространялись на другие компьютеры вместе с инфицированными им файлами или программами. Более того, вирус использовал усовершенствованные технические приёмы, как для своей установки в оперативную память, так и в целях собственной маскировки от пользователя.

«ExeBug» заражал главную загрузочную запись компьютера, когда пользователь пытался загрузить систему с инфицированного флоппи-диска. В процессе инфицирования копия оригинальной главной загрузочной записи сохранялась вирусом на «жёстком» диске компьютера по адресу 0/0/17 (цилиндр/сторона/сектор, соответственно). Все флоппи-диски, использовавшиеся в заражённой «ExeBug» компьютерной системе также инфицировались, если не были защищены от записи. При заражении «ExeBug» придерживался

[275] «ExeBug» (англ.) – «Ошибка исполняемого файла».

следующей линии поведения. Во время запуска системы вирус сразу же резидентно устанавливал себя в оперативную память и перехватывал функции операционной системы (прерывание INT 13h). Поэтому, каждый раз, когда операционная система или программное приложение пытались получить доступ к собственной функции, вирус активизировался и инфицировал новые файлы.

Для инсталляции себя в оперативную память даже при загрузке с чистой системной дискеты вирус «ExeBug» использовал довольно интересный приём. Он модифицировал ячейки памяти CMOS, в которых содержится информация о дисководах флоппи-дисков, таким образом, что система переставала «видеть» все эти дисководы. При загрузке («холодной» или «горячей») такого компьютера BIOS не обнаруживал флоппи-диски и передавал управление главной загрузочной записи «жёсткого» диска, которая уже была заражена. «ExeBug» получал управление, включал флоппи-диски и загружал с них систему. Таким образом, код вируса оказывался в памяти даже при загрузке с чистого системного диска.

Другой интересной отличительной чертой вируса «ExeBug» являлось то, что он устанавливал троянскую программу в некоторые из файлов с расширением «*.exe» и преобразовывал их в программы-вирусоносители, которые выводили на экран монитора слово: «HOOKER»[276].

Деятельность данного вируса могла приводить к повреждению заражённого им компьютера. Например, на инфицированном «ExeBug» компьютере «жёсткий» диск мог оказаться недоступным, и тогда систему приходилось загружать с системного флоппи-диска. Но даже в этом случае «жёсткий» диск мог оказаться недоступным, если вирусом уже была повреждена таблица размещения файлов[277].

---

[276] «Hooker» (англ.) – «Воришка». Отсюда происходит и одно из названий вируса «ExeBug».

[277] Дело в том, что троянские программы, записанные «ExeBug» в файлы с расширением «*.exe», стирали отдельные сектора «жёсткого» диска.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Groove
Другие названия	MtE.Groove
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	сентябрь 1992 года
Страна происхождения	Германия
Длина	3646 байт

Следом за «ExeBug» появился очень опасный резидентный компьютерный вирус «Groove», который стал первым вирусом на основе «MtE», заражавшим файлы с расширением «.exe». Кроме того, он обладал свойствами «противо-противо-вируса» или «ретро-вируса» (наподобие «Tequila» и «Peach») и противодействовал большинству антивирусных программных средств того времени. Этот вирус проникал в компьютерную систему вместе с заражёнными приложениями к сообщениям электронной почты, переносился с заражённых флоппи-дисков и CD-ROM, в процессе загрузки из Интернет и т. д. Копии «Groove» распространялись на другие компьютеры вместе с инфицированными им файлами и программами.

Вирус «Groove» перехватывал прерывание INT 21h и записывался в конец файлов с расширениями «*.exe», «*.com» и «*.ovl» при их загрузке в оперативную память компьютерной системы. Вирус проявлял себя визуально, так как после заражения очередного файла выводил на экран монитора своё сообщение: «Don’t worry, you are not alone at this hour... This Virus is NOT dedicated to Sara its dedicated to her Groove (… That is my name). This Virus is only a test Virus there for be ready for my Next Test …» («Не беспокойтесь, Вы не одиноки в этот час … Этот Вирус посвящен не Саре, а её Грув (… Это моё имя). … Этот Вирус является всего лишь тест Вирусом, вот будет готов мой Следующий Тест …»).

Деятельность вируса «Groove» могла приводить к аварийным отказам инфицированного им компьютера, так как он уничтожал в директориях логического диска C: следующие файлы: nav_._no, novircvr.cts, noviperf.dat, \vs.vs, \TOOLKIT\files.lst, \CPAV\chklist.cps, \UNTOUCH\ut.ut1, \UNTOUCH\ut.ut2.

В октябре появился ещё один очень опасный резидентный компьютерный вирус, получивший имя «Invol», который обладал свойствами полиморфизма и стал первым полиморфным вирусом, заражавшим файлы с расширением «*.sys».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Invol
Другие названия	Invol (sys)
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	октябрь 1992 года
Страна происхождения	Соединённые Штаты Америки
Длина	3646 байт

Кроме того, как и вирус «Groove» он представлял собой «ретро-вирус», активно противодействующий антивирусным программным средствам. Используя полиморфизм, вирус «Invol» шифровал разными способами своё тело после завершения очередного заражения, для чего им использовались различные ключи и операции. При каждом новом инфицировании вирус изменял свои свойства, что затрудняло его обнаружение антивирусными программами. По аналогии с «Groove» он проникал в компьютерную систему вместе с заражёнными приложениями к сообщениям электронной почты, переносился с инфицированных флоппи-дисков и CD-ROM, в процессе загрузки из Интернет и его копии распространялись на другие компьютеры вместе с заражёнными файлами и программами.

Вирус «Invol» записывался в конец файлов с расширениями «*.exe» и «*.sys». При запуске на выполнение заражённого файла он анализировал на логическом диске C: файл «config.sys» и заражал первый файл с расширением «*.sys», на который указывала строка «DEVICE=», содержащаяся в файле «config.sys». В том случае, если такие файлы вирусом не обнаруживались, вирус мог создать «пустой» файл под названием «vansi.sys» и записать в начало файла «config.sys» команду «DEVICE=vansi.sys». При загрузке компьютера с этого «config.sys» вирус «Invol» оставался в памяти как системный драйвер и перехватывал прерывание INT 21h, инфицируя запускаемые файлы с расширением «*.exe».

Деятельность вируса «Invol» могла приводить к очень серьёзным аварийным отказам инфицированного им компьютера, так как девятнадцатого числа каждого месяца активизировалась его деструктивная составляющая, в результате чего на логическом диске C: полностью уничтожалась FAT (Таблица размещения файлов). Коварство «Invol» проявлялось в том, что визуально он себя обнаруживал только после завершения операции по разрушению FAT, когда выводил на экран монитора следующее язвительное сообщение: «You have helped spread this virus. This has been a message from your friendly neighborhood infection service. Thank you for your involuntary cooperation» («Вы помогли распространению этого вируса. Это послание от Вашего приятного соседа, обслуживающего инфицирование. Спасибо Вам за непреднамеренное сотрудничество»).

В том же октябре был обнаружен резидентный компьютерный вирус, получивший красивое имя «Starship»[278], обладавший свойствами полиморфизма и использующий к тому же технологию «стелс». Этот вирус использовал также и новый способ инфицирования «жёсткого» диска компьютера. Кроме указанных свойств, стоит отметить ещё одну характерную черту этого вируса: «Starship» представлял собой так называемый SPM-вирус, то есть компьютерный вирус, инфицирующий сверхоперативную память[279].

[278] «Starship» (англ.) – «Звездолёт».

[279] Scratch-pad memory – SPM (англ., проф.) – сверхоперативная память, блокнотная память.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Starship
Другие названия	Starship.2570
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	октябрь 1992 года
Страна происхождения	Соединённые Штаты Америки
Длина	2570 байт

Этот вирус заражал файлы с расширениями «*.com» и «*.exe», причём, только на флоппи-дисках в дисководах A: и B: компьютера при создании нового файла, а также главную загрузочную запись (MBR) «жёсткого» диска при попытке запуска уже инфицированного файла. Последнее обеспечивало вирусу «Starship» резидентность в оперативной памяти компьютерной системы и переносимость на другие компьютеры при минимальном числе заражённых объектов, что усложняло его своевременное обнаружение. Применение такого способа инфицирования «жёсткого» диска компьютера предполагало также, что при инфицировании заново создаваемого файла не возникает необходимость в отслеживании критической ошибки MS-DOS (прерывание INT 24h).

В процессе инфицирования файлов вирус «Starship» записывался в их конец, используя при этом механизм полиморфизма, а при заражении «жёсткого» диска располагался в его самых последних секторах и устанавливал в Таблице разбиения диска (Disk Partition Table) новый адрес активного загрузочного сектора, чтобы вместо него эта таблица указывала на код вируса. Причём, код, расположение MBR и активного загрузочного сектора оставались без изменения, исключая три байта в Таблице разбиения диска, которые как раз и указывают на активный загрузочный сектор. При обращении к модифицированной MBR и последним секторам «жёсткого» диска вирусом использовалась технология «стелс». Вирус инфицировал оперативную память при загрузке с заражённого «жёсткого» диска. Часть своей TSR-копии помещал в таблице векторов (0000:02C0), области данных BIOS (0000:04B0), основной участок кода в видеопамяти (BB00:0050), а затем перехватывал прерывания INT 13h, 20h, 21h и 27h.

После загрузки операционной системы «Starship» отслеживал моменты запуска и завершения исполняемых программ и, если программа при завершении выгружалась из памяти («Exit» – INT 20h, INT 21h и AH=0 или 4Ch), он перемещал свой код из видеопамяти в область, которая была ранее занята выгруженной программой. В том случае, если программа оставалась резидентной в памяти («Keep» – INT 27h, INT 21 и AH=31h), «Starship» приписывал к ней свой код. Автором вируса была предусмотрена и такая ситуация, когда размещённая в видеопамяти компьютера часть его кода оказывалась недееспособной. В этом случае запускался механизм самовосстановления, то есть вирусом инициировалась процедура повторного считывания его работоспособного кода с «жёсткого» диска.

Вирус «Starship» распространялся достаточно медленно и, скорее всего, это послужило одной из основных причин, по которой он не смог вызвать настоящую эпидемию. Кроме того, в его теле содержалась запись «>STARSHIP_1<»[280] и он обладал слишком явными визуальным и аудио эффектами, которые сигнализировали даже неопытному пользователю о ненормальном функционировании компьютерной системы. При заданных значениях своих счётчиков вирус выводил через системный динамик звуки передаваемой морзянки, а на экране монитора появлялась заставка в виде звёздного неба.

Однако по мнению ведущих специалистов-вирусологов, 1992 год принёс с собой гораздо более важное событие, чем, например, полиморфные вирусы и конструкторы вирусов. Ведь в конце этого года был обнаружен первый компьютерный вирус, разработанный специально для операционной системы MS Windows 3.xx. – «Win.Vir_1_4», который, говоря словами одного из отечественных специалистов, «был небольшого размера, совершенно безвредный и нерезидентный, но вполне успешно делал своё «дело»: заражал исполняемые файлы нового формата MS Windows (NewEXE)».

[280] Благодаря этой записи вирус и получил имя «Starship».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Win.Vir_1_4
Другие названия	Win.Vir_1_4.a
Тип	компьютерный вирус
Инфицируемые платформы	MS Windows 3.xx
Впервые обнаружен	ноябрь 1992 года
Длина	1024 байта

Итак, во время запуска операционной системы этот вирус инициировал поиск файлов NewEXE в текущем каталоге и записывался в них. «Win.Vir_1_4» перемещал в конец файла сегменты стартового кода и автоматических данных, а свои код и данные записывал на их место. Кроме того, он изменял значения в таблице дескрипторов сегментов и заголовки файлов NewEXE. Вирус «Win.Vir_1_4» не возвращал управление программе-носителю, а по окончании своей работы восстанавливал программу-носитель в первоначальном виде и передавал управление операционной системе MS Windows 3.xx. В тело вируса был встроен следующий текст: «Virus_for_Windows v1.4 MK92» («Вирус_для_Windows v1.4 MK92»).[281]

Несмотря на ограниченные возможности своего распространения «Win.Vir_1_4» установил вирусописателям новый ориентир и указал новую цель, открыв следующую страницу в истории создания вредоносных компьютерных программ.

В целом, в 1992 году на первые роли выходят файловые, загрузочные и файлово-загрузочные вирусы, написанные для самой распространённой в то время операционной системы MS-DOS, устанавливаемой на персональных компьютерах производства фирмы IBM. Общий рост количества инцидентов, связанных с компьютерными вирусами, сопровождается совершенствованием антивирусных средств. По всему цивилизованному миру в правоохранительных органах создаются специальные подразделения, занимающиеся борьбой с компьютерной преступностью, а достоянием общественности ста-

[281] Штамм данного вируса получил название «Vir_1_4.b» и содержал в своём теле следующую строку: «AntiWindoze Virus by Xavirus Hacker. THNX2MK!!!» («AntiWindoze вирус от Хавирус Хакер. THNX2MK!!!»).

новится всё большее количество случаев успешной борьбы с вредоносными компьютерными программами.

§13. 1993 год – «бомбы замедленного действия», усовершенствованный полиморфизм, вирусы «компаньоны», издание первого официального перечня «WildList», творения «Чёрного барона», усложнённый алгоритм шифрования, конвеер на основе конструкторов вирусов и полиморфик-генераторов

- Выпущены операционные системы Windows NT Workstation 3.1 и Windows NT Advanced Server.
- Выпущена версия 6.0 операционной системы MS-DOS с включённой в неё подпрограммой Microsoft Anti-Virus.
- Выпущена версия 2.1 операционной системы OS/2, которая была полностью 32-разрядной, обладала способностью выполнять приложения, созданные для Windows, имела высокую производительность и поддерживала большое количество периферийных устройств (всё дело заключалось в «волшебных» драйверах).
- Выпущена версия 6.1 операционной системы PC-DOS с включением подпрограммы IBM AntiVirus.
- Компания Microsoft закончила разработку новой операционной системы Windows NT для работы с корпоративными приложениями, требующими повышенной надёжности операционной системы.
- Фирмой Intel выпущен микропроцессор Pentium (3,1 миллиона транзисторов).

В этом году было зафиксировано появление так называемых «бомб замедленного действия»,[282] которые представляли собой вирусы, скрытно инфицировавшие компьютеры и активизировавшиеся при наступлении заданных даты и времени, то есть конкретного, определённого вирусописателем события, которое заведомо должно наступить.[283] Главным отличием этих программ от более ранних вредоносных программ этого класса было то, что в них обязательно включался алгоритм «троянской» программы, «троянского

[282] Об этом виде вредоносных компьютерных программ мы упоминали выше, а первой жертвой такой программы, как гласит история компьютерных преступлений, стала всемирно известная газета «The New York Times» (США).

[283] Таким событием мог стать, к примеру, день рождения автора компьютерного вируса или его приятелей, любой день какого-либо праздника или один из произвольно выбранных каникулярных дней и т.д.

коня». Такие программы наиболее часто применяются при совершении компьютерных преступлений, связанных с хищением денег с электронных банковских счетов.

В качестве примера одного из появившихся в 1993 году «новаторских» компьютерных вирусов, можно привести загрузочный вирус «PMBS»[284], функционировавший в защищённом режиме процессора Intel 80386.

Идентификационная карточка вредоносной компьютерной программы	
Имя	PMBS
Другие названия	PMBS.512, STELBOO, AMSE, Nops
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	январь 1993 года
Страна происхождения	Соединённые Штаты Америки
Длина	512 байт

Разработка именно этого вируса расценивается специалистами как «первая попытка написания вредоносной компьютерной программы, работающей в условиях защищённого режима процессора Intel 80386». Вирус «PMBS» при загрузке с заражённого «жёсткого» диска переходил в защищённый режим, устанавливал себя супервизором системы и затем загружал операционную систему в режиме виртуального окна «V86». К счастью, этот вирус оказался не жизнеспособным: второе его поколение отказывалось размножаться по причине нескольких ошибок, которые автор допустил в программном коде. К тому же он «подвешивал» систему, если какая-либо из программ пыталась выйти за пределы «V86», например, определить наличие расширенной памяти.

Итак, компьютерный вирус «PMBS» был задуман автором и представлял собой опасный резидентный загрузочный вирус, который при загрузке с заражённого «жёсткого» диска копировал себя в расширенную память, переводил компьютер в защищённый режим и запускал виртуальную машину

---

[284] Своим названием данный вирус обязан текстовой строке «PMBSVIRS», содержащейся внутри его программного кода.

К маю 1996 года было известно уже 13 различных штаммов «PMBS». Наибольшее распространение в мире получил штамм Stealth_boot.c.

(«V86»). В результате загрузка операционной системы и выполнение программных приложений происходило уже на заражённой вирусом виртуальной машине. «PMBS» не использовал какие-либо особенные способы для своего распространения, копируя собственный программный код в другие файлы и программы и проникая в компьютер пользователя посредством любого из средств, обычно используемых компьютерными вирусами: флоппи-диски, CD-ROM, сообщения электронной почты с заражёнными вложениями, загрузка программ через Интернет, FTP и т. п.

Этот вирус перехватывал все 256 прерываний (от 00h до FFh) и проверял критические ситуации. В случае возникновения ситуации чтения с флоппи-диска вирус заражал его[285] (MBR «жёсткого» диска инфицировалась при первой попытке пользователя загрузить систему с заражённого флоппи-диска), а в случае остальных критических ситуаций выводил различные текстовые сообщения. При доступе к «жёсткому» диску «PMBS» применял «стелс» технологию, проверяя ввод/вывод в порты (с использованием особенностей защищённого режима процессора i386) и изменяя соответствующие данные.

Как мы уже упоминали, автор данного вируса допустил ряд существенных ошибок при его программировании, например, неверное заражение флоппи-дисков: вирус «PMBS» записывал на них лишь ту свою часть, которая работала в реальном режиме, а отвечающую за обработку прерываний в защищённом режиме часть на диск не записывал. Поэтому при попытке пользователя загрузить компьютерную систему с такого флоппи-диска она «зависала». Перечень серьёзных ошибок можно продолжить. Поскольку вирус переходил в режим супервизора, но не давал другим программам стать супервизором, инфицированный им компьютер с процессором Intel 80386 можно было использовать только как морально устаревший к тому времени компьютер PC 86, что не оставалось не замеченным опытным пользователем.

[285] При этом инфицировались любые не защищённые от записи флоппи-диски.

Кроме того, на инфицированной «PMBS» компьютерной системе пользователь не мог реализовать доступ к расширенной памяти с помощью популярных стандартных утилит, а использование программы «MEM» (программа из состава поставки операционной системы MS-DOS) вызывало «зависание» компьютерной системы, так как она осуществляет операцию проверки расширенной памяти компьютера.

Вскоре после выхода новой версии операционной системы фирмы Microsoft – MS-DOS 6.0, в Германии был обнаружен компьютерный вирус, который получил имя «Tremor».[286] Он представлял собой первый полностью полиморфный «стелс»-вирус – использовал усовершенствованный алгоритм шифрования своего тела и был способен прятать все признаки своего присутствия в заражённой системе как от команды «DIR», так и от программ редактирования диска, а также содержал программный код, блокирующий резидентную часть антивирусного продукта CPAV (Central Point Anti-Virus), включённого в MS-DOS 6.0 под именем MSAV (Microsoft Anti-Virus).

Идентификационная карточка вредоносной компьютерной программы	
Имя	Tremor
Другие названия	Tremor.4000.A, Tremor.4000
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	март 1993 года
Страна происхождения	Германия
Длина	4000 байт

Как и «PMBS» вирус «Tremor» не пользовался какими-либо специфичными способами для своего распространения, копируя собственный программный код в другие файлы и программы и проникая в компьютерные системы при помощи средств, обычно используемых компьютерными вирусами: флоппи-диски, CD-ROM, сообщения электронной почты с заражёнными вложениями, загрузка программ через Интернет, FTP.

«Tremor» перехватывал прерывания INT 1h, 15h, 21h и резидентно оставался в оперативной памяти, контролируя обращения к операционной

[286] «Tremor» (англ.) – «Дрожь».

системе. Если в Upper Memory Block[287] оставалось достаточно свободного места, то он копировал себя в этот блок памяти. В противном случае «Tremor» корректировал последний Memory Control Block[288] обычным для подобных вирусов способом и копировал себя в блок управления памятью. Каждый раз, когда операционная система или программное приложение пытались получить доступ к системным функциям, вирус активизировался и инфицировал всё новые файлы с расширениями «*.exe» и «*.com», записывая себя в конец этих файлов и, тем самым, увеличивая их размер на 4000 байт.

Кроме того, «Tremor» трассировал вектора прерываний с целью обнаружения в оперативной памяти и последующей блокировки отдельных резидентных программ, в частности, относящихся к классу антивирусных мониторов. Данный вирус использовал для трассировки прерываний прерывание INT 1h, а прерывание INT 15h для демонстрации на экране монитора видеоэффектов. В некоторых случаях «Tremor» выводил сообщение: -=>T0R0E0M0O0R was done by NEUROBASHER/May-June'92, Germany<=-MOMENT-OF-TERROR-IS-THE-BEGINNING-OF-LIFE- («-=>T0R0E0M0O0R сделан НЕРВОУБИЙЦЕЙ/Май-Июнь'92, Германия<=-Мгновение страха является источником существования»). Иногда «Tremor» «встряхивал» изображение на экране монитора. Перехват прерывания INT 21h использовался «стелс» функциями вируса для проверки и перехвата имён файлов, которые могли быть инфицированы.

Усовершенствованный полиморфизм «Tremor» заключался в том, что он не использовал какой-либо один алгоритм при заражении файлов, а напротив, постоянно изменял своё тело, шифруя его при помощи различных методов по завершении каждого инфицирования и применяя при этом разные коды и операции. В результате, вирус после инфицирования очередного фай-

[287] Upper Memory Block – UMB (англ., проф.) – блок верхней области памяти.

[288] Memory Control Block – MCB (англ., проф.) – блок управления памятью.

ла приобретал новые свойства, которые затрудняли его обнаружение антивирусными программными средствами.

Кроме всего прочего, одним из неприятных последствий заражения компьютерной системы вирусом «Tremor» являлось резкое снижение её производительности, которое было заметно даже не слишком искушённому в вычислительной технике пользователю.

Свой «посильный вклад» в совершенствование технологий написания вредоносных компьютерных программ привнесли и авторы вирусов «Strange» и «Carbuncle», которые расширили спектр алгоритмов так называемых «компаньон вирусов».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Strange
Другие названия	Hmm
Тип	компьютерный вирус
Инфицируемые платформы	DOS
Впервые обнаружен	март 1993 года
Страна происхождения	Соединённые Штаты Америки
Длина	1536 байт

Первый из них – «Strange»[289] – представлял собой загрузочный «стелс» вирус, использовавший недокументированную программную ошибку в некоторых версиях операционных систем DOS (ранние версии PC DOS и все версии MS-DOS) и действовавший на уровне аппаратных прерываний INT 0Dh и INT 76h.

Этот резидентный загрузочный вирус занимал четыре сектора (три сектора под тело вируса плюс один сектор под старый загрузочный сектор или MBR). На «жёстком» диске он записывал старый MBR и свое продолжение, начиная с 17 сектора первого трека, а на флоппи-дисках использовал для этого последние четыре сектора диска. При загрузке системы «Strange» размещался в области верхних адресов оперативной памяти, уменьшая значение по адресу 0000:0413 на 3 и перехватывал прерывание INT 8. При появлении обработчика прерывания INT 2Ah (вектор по адресу 0000:00A8h не равен 0000:0000) восстанавливал прерыва-

[289] «Strange» (англ.) – «Странный», «Незнакомый».

ние INT 8 и перехватывал INT 21h. При загрузке командного процессора «command.com» вирус увеличивал длину области драйверов и копировал в неё своё тело. При этом восстанавливалось старое значение INT 21h и перехватывались прерывания INT 9 и INT 13h. Область памяти, занимаемая ранее «Strange», освобождалась. Если операция копирования вируса в область драйверов была невозможна, то вирус выводил на экран монитора следующую фразу: «Hmm ... Strange drivers you have, very strange ...» («Хмм … Странные у вас драйверы, очень странные…») При обработке прерывания INT 13h вирус «Strange» проверял наличие трассировки и с этой целью при помощи команды «CLI» блокировал аппаратные прерывания, засылал регистр «AX» в стек, а затем извлекал его и сравнивал содержимое стека со значением регистра. Если эти значения не совпадали, вирус возвращал код ошибки «Disk Write-Protect»[290] независимо от функции. Таким образом, прерывания INT 9 и INT 13h вирус использовал с целью получения нежелательных эффектов на клавиатуре пользователя и инфицирования дисков.

Помимо этого, «Strange» перехватывал одно из двух аппаратных прерываний – INT 0Dh[291] или INT 76h[292], которые соответствуют аппаратному запросу компьютера: «Hardware Interrupt Request»[293]. Как известно, при обращении к «жёсткому» диску аппаратные средства компьютера генерируют соответствующий IRQ (IRQ5 на PC/XT и IRQ14 на компьютерах класса IBM/AT), а центральный процессор реагирует на полученный запрос вызовом соответствующего прерывания. Для того чтобы правильно перехватить прерывание «жёсткого» диска вирус должен «узнать» класс компьютера, который им инфицируется, то есть определить тип установленного в компьютерной системе процессора. «Strange» проделывал эту операцию при помощи команды «SHR AX,CL» (AX=0002h, CL=41h): если значение регистра «AX»

---

[290] «Disk Write-Protect» – «Диск защищён от записи».

[291] INT 0Dh соответствует IRQ5 на PC/XT, «жёсткий» диск.

[292] INT 76h соответствует IRQ14 на PC/AT, контроллер «жёсткого» диска.

[293] «Hardware Interrupt Request» (IRQ) – «Запрос прерывания от аппаратных средств».

становилось равным 1 (единице), то класс компьютера определялся как i286 и выше (вирус перехватывал прерывание INT 76h); если значение регистра «AX» становилось равным 0 (нулю) класс компьютера определялся как i86 и в этом случае перехватывалось прерывание INT 0Dh). С помощью прерываний INT 0Dh и INT 76h «Strange» реализовал на «жёстком» диске компьютера «стелс» технологию. В этих целях вирус постоянно хранил в памяти оригинальную, не инфицированную им копию MBR и, в случае чтения заражённой MBR, подставлял оригинальную копию.

На компьютерах класса PC/XT при вызове прерывания INT 0Dh вирус считывал адрес дискового буфера из порта 6, а затем проверял этот сектор на наличие инфекции. Если сектор оказывался заражённым, «Strange» копировал в дисковый буфер код оригинальной MBR.

На компьютерах класса PC/AT при вызове прерывания INT 76h вирус считывал номера сектора, трека и головки через порты 1F3h, 1F4h, 1F5h и 1F6h. Если их значения соответствовали MBR, вирус записывал в эти порты адрес сектора, содержащего оригинальный MBR. В случае попытки трассировки прерывания INT 13h (с учётом того факта, что вирус проверял наличие трассировки) при чтении MBR, трассировка доходила до ROM BIOS, и изменений в значениях регистров не было, но, тем не менее, в буфер считывался оригинальный MBR, а не сам вирус! Даже если прерывание INT 13h устанавливалось непосредственно в BIOS, «Strange» и в этом случае оставался невидимым!

Идентификационная карточка вредоносной компьютерной программы	
Имя	Carbuncle
Другие названия	Carbuncle.622
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	май 1993 года
Страна происхождения	Соединённые Штаты Америки
Длина	622 байта

Второй вирус – «Carbuncle»[294] представлял собой опасный нерезидентный компаньон вирус длиной 622 байта. Интересно, что программа-файл этого вируса всегда имеет имя «carbuncl.com», и ни при каких обстоятельствах не меняет его на иное.

При запуске на выполнение программы «carbuncl.com», а на самом деле вируса, немедленно создавалась её копия (файл «carbuncl.com») в текущем каталоге. Затем вирус начинал поиск в текущем каталоге файлов с расширением «*.exe» и переименовывал их в файлы с теми же именами, но с расширением «*.crp». Для каждого переименованного файла «Carbuncle» создавал компаньон-файл с расширением «*.bat» и именем первоначального файла. Вследствие инфицирования каталога в нем появлялся файл «carbuncl.com», а вместо каждого файла с расширением «*.exe» образовывалась пара файлов с расширениями «*.bat» и «*.crp». Файл с расширением «*.bat» содержал шесть строк команд операционной системы MS-DOS. В том случае, если инфицировался файл «file.exe», то командный файл с расширением «*.bat» принимал следующий вид:

```
@ECHO OFF
CARBUNCL
RENAME          FILE.CRP
FILE.EXE
FILE.EXE
RENAME          FILE.EXE
FILE.CRP
CARBUNCL
```

294 294 «Carbuncle» (англ.) – в медицине и минералогии переводится как «Карбункул». Однако можно перевести и как «Бородавка», «Нарост».

Таким образом, при попытке запуска заражённого файла с расширением «*.exe» запускался компаньон-файл с расширением «*.bat», который переименовывал файл с расширением «*.crp» в файл с расширением «*.exe», затем выполнял его и переименовывал обратно в файл с расширением «*.crp». Если при запуске вируса значение секунд системного таймера было меньше или равно 16, «Carbuncle» записывал себя вместо первого файла с расширением «*.crp» текущего каталога и уничтожая таким образом инфицированный файл с расширением «*.exe». В теле вируса содержались также следующие строки:

```
*.crp
CARBUNCL.COM
BAT*.exe
CRP
@ECHO OFF
CARBUNCL
RENAME
PC CARBUNCLE: Crypt Newsletter
14
```

Шестая сверху строка как раз и была присвоена вирусу в качестве его имени.

В апреле 1993 года Джо Уэллс, работавший в то время в Peter Norton Product Group корпорации Symantec (штат Калифорния, США), начал собственный проект по систематизации компьютерных вирусов, существование которых в «диком» виде подтверждалось документально. Уэллс классифицировал отобранную им из различных источников (например, списков общеизвестных вирусов) информацию и представил её в виде перечня, который отправил почтой другим членам международной организации CARO (Computer Antivirus Research Organization). В сопроводительном письме содержалась просьба о подтверждении или отклонении «кандидатуры» каждого из включённых в перечень вирусов на звание «дикий». В результате, после соответствующего обобщения ответов компьютерных вирусологов, в июле 1993 года

был издан первый официальный перечень существовавших на тот момент в «диком» виде компьютерных вирусов – «WildList»[295].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Pathogen
Другие названия	SMEG.Pathogen, SMEG, Smeg.Pathogen
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	апрель 1993 года
Страна происхождения	Великобритания
Длина	3544 байта

И в том же апреле, в Великобритании был обнаружен очень сложный полиморфный и обладающий деструктивными функциями компьютерный вирус, автор которого размещал заражённые им файлы на станции BBS, что стало причиной эпидемии, а также паники среди пользователей и в средствах массовой информации, которая усугублялась тем, что далеко не все антивирусные программы того времени могли гарантированно обнаруживать этот вирус. Примерно через год, в самом начале 1994 года, там же было зарегистрировано появление его «младшего брата».

Первый из этих вирусов был назван не без доли иронии «Pathogen»,[296] а второй получил прозаическое имя «SMEG.Queeg». Обе вредоносные компьютерные программы – «Pathogen» и его «собрат» были построены на основе полиморфного движка, который известен под аббревиатурой «SMEG», а написал эти творения некий субъект, скрывавшийся под кличкой «Black Baron»[297]. Движок, используемые приёмы и автор, а также наличие сходных деструктивных функций, позволили вирусологам объединить эти вирусы в единое семейство очень опасных резидентных полиморфных вирусов, под общим названием «Smeg». Для удобства читателя в данном случае мы несколько отойдём от общего подхода, принятого нами в настоящей книге, и рассмотрим оба вируса вместе.

---

[295] Подробнее данная тематика изложена в Приложении 1 и Приложении 2.

[296] «Pathogen» (англ.) – «Болезнетворный микроорганизм».

[297] «Black Baron» (англ.) – «Чёрный барон».

Итак, написанные при помощи полиморфик-генератора «SMEG» вирусы «Pathogen» и «SMEG.Queeg» заражали MBR компьютерной системы в тот момент, когда пользователь пытался загрузить систему с инфицированного флоппи-диска[298]. После того, как главная загрузочная запись была заражена, и вирус резидентно устанавливался в оперативной памяти компьютера, он инициировал процедуру отслеживания и перехвата прерывания INT 21h, а затем, при запуске или открытии файлов с расширениями «*.com» и «*.exe», инфицировал их, записываясь в конец программного кода этих файлов. Кроме того, «SMEG.Queeg» перехватывал прерывания INT 13h и 20h. Эти вирусы не заражали файлы со следующими именами: «co*.*», «f-*.*», «sc*.*», «tb*.*», «vi*.*», «fs*.*», «vp*.*», «vs*.*», «cl*.*», «sm*.*», «fl*.*».

Оба вируса вели подсчёт количества инфицированных ими файлов, и после того, как значение встроенного в тело вируса счётчика достигало 32, «жёсткий» диск компьютерной системы выводился из строя. Причём происходило это только в заранее определённые дни недели (у «Pathogen» по понедельникам, а у «SMEG.Queeg» по воскресеньям) и период времени суток (когда текущее системное время принимало значения от 17:00 до 18:00). В случае одновременного соблюдения указанных условий вирусы активизировали свои деструктивные функции, которые блокировали клавиатуру компьютера, стирали CMOS и сектора «жёстких» дисков, а также выводили на экран монитора приведённые ниже тексты.

«Pathogen»	«SMEG.Queeg»
Your hard disk is being corrupted, courtesy of PATHOGEN! Programmed in the U.K. (Yes, NOT Bulgaria!) [C] The Black Baron 1993-4. Featuring SMEG v 0.1: Simulated Metamorphic Encryption Generator! 'Smoke me a kipper, I`ll be back for breakfast ...' Unfortunately some of your data won`t!!!!!	-п QUEEG o- ~~~~~ (C) The Black Baron 1994 Featuring: SMEG v 0.2 Better than life

[298] Все не защищённые от (несанкционированной) записи флоппи-диски, которые затем будут использоваться в инфицированной системе, естественно, также будут заражаться «Pathogen» или «SMEG.Queeg».

Ваш «жёсткий» диск разрушен испорчен благодаря по милости PATHOGEN! Запрограммирован в Соединённом Королевстве (Да, НЕ в Болгарии!) [C] «Чёрный барон» 1993-4. Использованы возможности SMEG v 0.1: имитационной метаморфической кодирующей генерирующей программы!
Закоптите мне селедку, я вернусь к завтраку ... К сожалению, некоторых из ваших данных больше нет!!!!!

-п QUEEG o-
~~~~~
(C) «Чёрный барон» 1994
Использованы возможности: SMEG v 0.2
Лучше жизни

Кроме приведённых текстов, «Pathogen» и «SMEG.Queeg» содержали в своём теле идентичную текстовую строку: «EXECOM \/:.<>+=;,«[]|OC-FCSBTIVSFPVSVLCMSLF».

В завершение рассказа об этих малоприятных программах добавим, что впоследствии, уже летом 1994 года, благодаря настойчивости и профессионализму правоохранительных органов Великобритании, автор вирусов «Pathogen» и «SMEG.Queeg» был выслежен агентами специального подразделения по борьбе с компьютерными преступлениями Нового Скотланд-Ярда, арестован и без особых антимоний препровождён в ближайшую тюрьму.

К маю 1993 года могло сложиться впечатление, что вирусописатели совсем забыли о написании новых деструктивных вирусов, рассчитанных на платформу Macintosh. Однако в конце апреля был обнаружен файловый вирус Mac/INIT-M, функционирующий в среде операционной системы System 7.0 и более поздних версий. Этот вирус инфицировал программные приложения, а также системные файлы. Mac/INIT-M активизировался в любую пятницу, которая выпадала на тринадцатое число, переименовывая файлы и директории, создавая собственные файлы, а также уничтожая файлы на «жёстком» диске компьютера и флоппи-дисках.

В первой половине года появились две версии вроде бы обычного резидентного файлового компьютерного вируса по имени «Cruncher»[299], кото-

[299] «Cruncher» (англ.) – «Прессовщик». От этого слова происходит профессиональный термин – «crunching», применяющийся в области информационных технологий для обо-
~~~~~

рый был так назван по одному из слов текстовой строки, содержащейся в его теле: «[MK/Trident] Cruncher V1.0 c». Однако этот вирус, иногда характеризуемый в качестве «доброго», получил широкую известность благодаря тому, что был первым компьютерным вирусом, который преднамеренно «сжимал» инфицированные компьютерные программы и, тем самым, предоставлял пользователю дополнительный объём дорогого в то время дискового пространства[300]. Обе версии «Cruncher» были написаны одним автором, о котором известно, что его звали Масуд Хафир и он состоял членом группы вирусописателей под названием «TridenT».[301]

Идентификационная карточка вредоносной компьютерной программы	
Имя	Cruncher
Другие названия	Cruncher.2092
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	июнь 1993 года
Страна происхождения	Нидерланды
Длина	2092 байта

«Cruncher» оставлял в оперативной памяти свою резидентную копию, перехватывал прерывание INT 21h и при запуске файлов записывался в них, используя перехват прерывания INT 24h, обработку и сохранение атрибутов и времени создания файла. Первая версия вируса (V1.0) инфицировала файлы с расширением «*.com». Пожалуй, на этом стандартность вируса «Cruncher» и заканчивалась.

В момент заражения файла он применял алгоритм компрессии данных и упаковывал заражённый файл, тем самым, освобождая дисковое пространство. В результате, длина инфицированного вирусом файла довольно существенно уменьшалась по отношению к первоначальной длине оригинального файла. Заражение и последующее «сжатие» файлов выглядели следующим образом. При запуске файла на выполнение «Cruncher», в случае наличия до-

значения одного из методов упаковки (уплотнения) данных при помощи их сложного и многократного преобразования.

[300] Обычно, после инфицирования, программы уменьшались в размере на 20–40%.

[301] «TridenT» (англ.) – «ТрезубеЦ».

статочного свободного места в оперативной памяти компьютера, считывал туда всё содержимое этого файла, а затем обычным способом инфицировал его. Таким образом, заражение файлов осуществлялось в оперативной памяти. Дописывание кода вируса и изменение начала файла происходили со считанным в память образом инфицируемого файла, но обращение к дискам не производилось. По завершении заражения «Cruncher» запускал алгоритм упаковки, код которого был включён в его тело и представлял собой часть программного кода общеизвестной тогда утилиты «DIET» версии 1.10[302]. «Сжатие» инфицированного образа файла начиналось с первого байта (команды «JMP») и завершалось последним байтом вируса. Блоки копирования и распаковки представляли собой стандартные «обкладки» указанной утилиты, поэтому при помощи соответствующей версии утилиты «DIET» можно было без особого труда «развернуть» любой файл, упакованный вирусом «Cruncher»[303]. Инфицированный и упакованный образ файла сохранялся на «жёсткий» диск вместо оригинального файла и задействованные вирусом при заражении участки оперативной памяти освобождались.

Выполнение вирусом «Cruncher» двух последних операций знаменовало собой окончание инфицирования файла. При попытке запуска заражённого файла внешне всё происходило таким образом, как будто обычный вирус был запакован утилитой «DIET». Коды блоков копирования и распаковки

---

[302] Утилита «DIET» относится к классу так называемых свободных программных средств (freeware), то есть компьютерных программ, которые можно свободно распространять. Использование в теле вируса программного кода, заимствованного из утилиты «DIET», который к тому же был чрезвычайно похож на код широко известных утилит того времени «LZEXE» и «PKLITE», затрудняло задачу корректного обнаружения «Cruncher» при помощи антивирусного программного обеспечения. Именно по этой причине некоторые из числа антивирусных программ подавали пользователю ложный сигнал о присутствии вируса «Cruncher»в упакованных при помощи «DIET» программах.

[303] В данном контексте можно говорить о полной совместимости «Cruncher» и «DIET».

восстанавливали запакованный вирус, который затем перехватывал прерывание INT 21h и резидентно оставался в оперативной памяти компьютера.

Вторая версия вируса «Cruncher» – «Cruncher.4000», имела следующие основные отличия:

инфицировались файлы как с расширением «*.com», так и с расширением «*.exe». Причём, во время заражения файлов с расширением «*.exe» проводилась проверка на наличие у них заголовка NewExe-файла, и Windows-файлы не инфицировались[304].

в некоторых случаях на экран монитора выводилось следующее сообщение:

*** CRUNCHER V2.0 ***	*** CRUNCHER V2.0 ***
Automatic file compression utility	Утилита автоматического сжатия файлов
Written by Masud Khafir of the TridenT group (c) 31/12/92	Написана Масудом Хафиром из группы TridenT group (c) 31/12/92
Greetings to Fred Cohen, Light Avenger and Teddy Matsumoto	Поздравления Фреду Кохэну, Светлому мстителю и Тэдди Мацумото

В 1993 году список компьютерных вирусов, существующих в «диком» виде, пополнился вирусом, которому было присвоено весьма мрачное имя «SatanBug»[305].

Этот зашифрованный, резидентный и «чрезвычайно» полиморфичный вирус появился в столице США г. Вашингтон (округ Колумбия) и поразил сотни и сотни компьютеров, а затем распространился в других регионах мира. В результате эпидемии «SatanBug», в первую очередь, пострадали ком-

---

[304] Кроме того, «Cruncher.4000» не заражал файлы с расширением «*.exe», если их имена начинались с комбинаций символов: «SC», «CL», «VS», «NE», «HT», «TB», «VI», «FI», «GI», «RA», «FE», «MT», «BR», «IM».

[305] «Satan Bug» (англ.) – «Дьявольский жучок». В переносном смысле слова можно перевести как смертельно опасное или беспощадное насекомое. В просторечных выражениях в американском английском слово «Satan» (также как и «tarnal») иногда употребляется в целях эмоционального усиления разговорной речи.

Своё имя вирус получил от текстовой строки, которая содержалась в его теле: «Satan Bug virus – Little Loc». Там же находилась и ещё одна строка: «COMSPEC=COMMAND.COM».

пьютерные системы государственных органов США, в том числе и Белого дома. «SatanBug» получил достаточно широкое освещение в сообщениях средств массовой информации, фирм-разработчиков антивирусного программного обеспечения и статьях в специализированных изданиях того времени.

Идентификационная карточка вредоносной компьютерной программы	
Имя	SatanBug
Другие названия	S-Bug
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	август 1993 года
Страна происхождения	Соединённые Штаты Америки
Длина	9108 байт

В целом данный вирус стал источником головной боли для многих официальных структур и рядовых пользователей. «SatanBug», о котором сообщила известная Группа наблюдения за вирусами (CIAC[306]) из Министерства энергетики США, был охарактеризован ею как «трудно излечимый» вследствие применённого его автором алгоритма шифрования. Бюллетень CIAC извещал о том, что подобные вирусу «SatanBug» зашифрованные вирусы, очень непросто удалять из инфицированных ими файлов, поскольку они присоединяются к компьютерным программам, «выкусывая» из них небольшой кусок оригинального программного кода с целью вставки на это место собственного вредоносного кода и последующего шифрования как собственного тела, так и «откушенного» ранее куска программного кода компьютерной программы. Кроме того, компьютерное сообщество уведомлялось о том, что «SatanBug» способен повреждать файлы, изменять даты их создания и отключать пользователей от локальных вычислительных сетей посредством повреждения сетевых драйверов. Консультативная служба CIAC заявляла, что этот вирус был обнаружен сразу во многих компьютер-

[306] В качестве одного из членов правительственной комиссии «Forum of Incident Response and Security Teams» CIAC выпускает специальные информационные бюллетени в тех случаях, когда в Министерство энергетики США поступают сообщения о серьёзных инцидентах, связанных с компьютерными вирусами.

ных системах Министерства энергетики США и несколько подразделений пытаются бороться с ним при помощи существующих программ детектирования компьютерных вирусов.

Однако сложный алгоритм шифрования делал «SatanBug» невидимым для выпущенных до августа 1993 года антивирусных программ-сканеров. «Эти программы должны открыть файл для сканирования, а если вирус находится в памяти, то само действие по открытию файла будет приводить к инфицированию, – уведомлял бюллетень. – Если вы запускаете инфицированный антивирусный сканер, то почти каждый исполняемый файл на диске окажется заражённым». В связи с этим фирмы-разработчики антивирусных программных средств в ускоренном порядке организовали работы по модернизации собственных продуктов для того, чтобы они могли успешно бороться с «SatanBug», который, тем временем, успешно атаковал всё новые правительственные компьютерные системы США, а также компьютеры обыкновенных пользователей. «Для восстановления инфицированной программы антивирусное программное обеспечение должно уметь расшифровывать закодированный вирус, чтобы обнаружить исчезнувшую часть файла и вернуть её на место, – констатировал бюллетень. – «SatanBug» имеет до девяти уровней шифрования, причём в каждом случае этот уровень не предсказуем». Президент Leprechan Software (г. Мариетта, штат Джорджия) Роджер Томпсон, поделился собственными впечатлениями о том, как после соответствующего звонка из правительственного агентства специалисты его компании провели все выходные дни за обновлением своего антивирусного программного обеспечения для борьбы с этим вирусом. ««SatanBug» – это сложный вирус, и его трудно обнаружить, – пояснял Томпсон. – Он содержит цикл шифрования/дешифрования, причём расшифровывает себя с помощью ключа длиной от 40 до 2000 бит. Новейшие тенденции в вирусном сообществе делают подобные программы трудно обнаруживаемыми». Представители известной фирмы McAfee Associates и компании Norman Data Defense Systems объявили о создании программных продуктов для борьбы с «SatanBug», ко-

торые удаляют вирус, оставляя файлы неповреждёнными. Кроме того, представитель компании Norman Data Defense Systems сообщил, что их программа к тому же предотвращает заражение.

Чем же ещё был интересен «SatanBug»? Этот вирус был крайне латентен и не вызывал никаких видимых симптомов заражения, то есть полностью отсутствовали визуальные эффекты или сообщения на экране монитора, которые могли бы вызвать у пользователя подозрения о заражении компьютера. «SatanBug» оставался резидентным в оперативной памяти компьютера, занимая там 9 Кб, перехватывая функции 3Dh, 4Bh и 6Ch прерывания INT 21h и инфицируя файлы с расширениями «*.com» и «*.exe»[307] при их запуске или открытии. Причём, файлы с расширением «*.com» заражались только в том случае, если их размер не превышал 1204 байта, а с расширением «*.exe», если их размер не превышал 60016 байт. Инфицированные файлы с расширением «*.exe» могли вызывать сбои системы при попытке их выполнения. «SatanBug» также удалял программный код, который добавлялся в файлы антивирусными программами McAfee (SCAN и CPAV) с целью их иммунизации.

Как указывал Дэвид Стэнг, президент компании-разработчика Norman Data Defense Systems (Фолл-Черч, штат Виржиния), вирус «SatanBug» впервые был замечен до обнаружения в «диком» виде, когда пользователь по имени «Hacker 4Life» поместил его программный код сразу на нескольких электронных досках объявлений. Основываясь на степени сложности вируса, и своем опыте работы с программами этого класса, Стэнг предположил, что: «… «SatanBug» представляет собой плод деятельности двадцатилетнего американского парня, но отнюдь не злонамеренного подростка». Однако впоследствии, с помощью специалистов компаний-разработчиков антивирусного программного обеспечения, агентам ФБР США удалось проследить путь

[307] «SatanBug» записывал себя в конец этих файлов, увеличивая их в объёме на величину от 4 до 5 Кб.

распространения «SatanBug» вплоть до его автора, и в ходе расследования выяснилось, что автором данного вируса был как раз подросток, который до этого ничем особо примечательным среди своих сверстников не выделялся.

Итак, «SatanBug»[308] являлся 100% полиморфным или кодируемым вирусом, что придавало ему практически неограниченные возможности по изменению своего кода. Для обнаружения вирусов такого класса приходилось использовать специальные методы: эмуляцию выполнения кода вируса, математические алгоритмы восстановления участков кода и данных в вирусе и т. д. Как подчёркивали известные отечественные и зарубежные специалисты-вирусологи, спустя всего лишь несколько месяцев после появления полиморфик-генератора «MtE» и печально знаменитого вируса «Dedicated»[309], который открыл эпоху вирусов, построенных с помощью этого генератора, производство полиморфных вирусов превращается в самое настоящее ремесло. «Удельный вес самостоятельно шифрующихся полиморфных вирусов становился всё больше и больше, и казалось, что одним из основных направлений в трудном деле создания вирусов становится разработка и отладка полиморфного механизма, а конкуренция среди авторов вирусов сводится не к тому, кто из них напишет самый крутой вирус, а чей полиморфный механизм окажется круче всех» – эту мысль можно считать квинтэссенцией многочисленных высказываний по поводу ситуации, сложившейся в те дни на ниве вирусописательства. С 1993 года в коллекциях вирусов многих специалистов хранятся образцы вредоносных компьютерных программ, которые представляют собой стопроцентно полиморфные вирусы. В качестве примера «аллеи славы» того времени можно привести следующий, весьма усечённый нами

---

[308] Заложенные в этот вирус идеи затем были использованы, например, при написании вируса «SatanBug.FruitFly» («FruitFly» (англ.) – «Дрозофила», плодовая мушка), который представлял собой опасный не резидентный полиморфный вирус. Он искал файлы с расширением «*.com» текущего каталога и каталогов, поименованных в строке PATH, а затем записывался в их конец. Уничтожал файлы с именами «vs.vs» и «chklist.cps».

[309] Более подробно об этом компьютерном вирусе см. выше – 1992 год.

перечень: «Bootache», «CivilWar», «Crusher», «Dudley», «Fly», «Freddy», «Ginger», «Grog», «Haifa», «Moctezuma», «MVF», «Necros», «Nukehard», «PcFly», «Predator», «Sandra», «Shoker», «Todor», «Tremor», «Trigger», «Uruguay», «SatanBug» и т. д.

К числу известных и появившихся практически в тоже время не 100% полиморфных вирусов[310] отечественные специалисты вирусологи обычно относят следующие вредоносные компьютерные программы и их семейства: «Basilisk», «Daemaen», «Invisible», «Mirea», «Rasek», «Sarov», «Scoundrel», «Seat», «Silly», «Simulation». Как справедливо указывают компьютерные вирусологи, эти вирусы также требуют тщательной расшифровки программного кода для их обнаружения, блокирования и восстановления заражённых файлов, поскольку длина постоянного кода в расшифровщике этих вирусов очень мала.

В 1993 году создаются новые электронные издания вирусописателей, появился целый ряд новых конструкторов вирусов и полиморфик-генераторов, которые совершенствовались параллельно с полиморфными вирусами, используя более сложные методы генерации полиморфного кода[311]. К завершению 1993 года было известно уже семь генераторов: «MtE 0.90» (Mutation Engine), четыре различные версии «TPE» (Trident Polymorphic Engine), «NED» (Nuke Encryption Device), «DAME» (Dark Angel's Multiple Encryptor). На основе «PS-MPC» был создан конструктор «G2» (Phalcon/Skism's G2 0.70 beta), который поддерживал файлы конфигурации стандарта «PS-MPC», однако при генерации вируса использовал большее количество вариантов кодирования одних и тех же функций. Все без исключения перечисленные программы крайне отрицательно повлияли на положение дел, связанных с компьютерными вирусами. Кроме сотен и тысяч рядовых вирусов, ма-

[310] Шифрующим себя компьютерным вирусам, в расшифровщике которых всегда присутствуют постоянные байты.

[311] Эти программы распространялись по станциям BBS в виде архивов, содержащих объектные модули, документацию и примеры использования.

ло отличающихся друг от друга и сделанных как «под копирку», в 1993 году были написаны также и действительно весьма оригинальные, изощрённые вредоносные компьютерные программы. Появляется всё больше и больше компьютерных вирусов, использующих необычные способы заражения файлов и проникновения в систему, а также другие инновационные технологии и приёмы сокрытия и разрушения данных и систем.

Вместе с тем в 1993 году наши «доморощенные» вирусописатели ничем особенным себя не проявили, хотя и нельзя сказать, что их активность была равна нулю. Но они не смогли «явить миру» какие-то новые технологии или технические приёмы при написании или распространении вредоносных компьютерных программ.

В основном дело ограничивалось массовыми «штамповками», изготовленными с помощью перечисленных выше конструкторов вирусов и полиморфик-генераторов, а также достаточно банальными компьютерными вирусами. Одной из таких вредоносных компьютерных программ стал, например, обнаруженный в сентябре резидентный полиморфный вирус, который получил имя «Metallica»[312] по текстовой строке «MetallicA», содержащейся в его теле.

[312] «Metallica» (англ.) – «Металлика». Известные штаммы «Metallica.400» и «Metallica.500» представляют собой достаточно безобидные резидентные вирусы, которые перехватывают прерывание INT 21h и записываются в конец исполняемых файлов при их запуске или открытии. Причём, если «Metallica.500» инфицирует файлы с расширениями «*.com» и «*.exe», то «Metallica.400» заражает файлы только с расширением «*.com».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Metallica
Другие названия	Metallica.1129, Metallica 2.0, Metallica_II,
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	сентябрь 1993 года
Страна происхождения	Россия
Длина	1129 байт

Этот вирус проникал в оперативную память компьютера и, оставаясь там резидентно, перехватывал функции, принадлежащие операционной системе MS-DOS. Поэтому каждый раз, когда операционная система или прикладная программа пытались получить доступ к какой-либо из этих функций вирус «Metallica» активизировался и инфицировал новые файлы. Для того чтобы затруднить своё обнаружение с помощью антивирусных программных средств он применял следующий приём: он расшифровывал себя во время заражения очередного файла и сразу после его завершения вновь зашифровывал свой программный код.

§14. 1994 год – освоение вирусами новых «ниш» продолжается и они становятся всё быстрее и опаснее: первая в России эпидемия полиморфного вируса, деструктивный вирус для платформы Macintosh, «великий и ужасный шифровальщик жёсткого диска» по имени «One_Half», отечественная «Зараза», продолжение компьютерных мистификаций

- Выпущены операционные системы Windows NT Workstation 3.5 и Windows NT Server 3.5.
- Выпущена версия 6.22 операционной системы MS-DOS.
- Выпущена операционная система OS/2 Warp 3.0, в которой, помимо дальнейшего повышения производительности и снижения требований к аппаратным ресурсам, появилась поддержка работы в Интернет.
- Выпущена версия 1.0 операционной системы Linux, в которую добавлены сетевые средства.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Shifter
Другие названия	Shifter.983, ShiftObj.983
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	январь 1994 года
Страна происхождения	Соединённые Штаты Америки
Длина	983 байта

В течение 1994 года были выявлены весьма интересные экземпляры из числа новых компьютерных вирусов. Например, в январе 1994 года появился первый резидентный вирус, заражающий объектные модули[313] и получивший имя «Shifter».[314]

Этот вирус, устанавливал себя резидентно в оперативную память компьютера, перехватывал прерывание INT 21h и записывался в середину объектных модулей при их закрытии, инфицируя их так, чтобы при компоновке модуля[315] в файл с расширением «*.com» тело «Shifter» расположилось в начале этого файла. При запуске такого файла он продолжал оставаться резидентным. При заражении объектного модуля вирус последовательно читал заголовки всех объектных записей,[316] отбирая и обрабатывая четыре типа записей: «Module End Record» (тип 8Ah), «External Names Definition Record» (тип 8Ch), «Logical Data Record» (типы A0h или A2h). При обнаружении за-

---

[313] Object module (англ.) – (проф.) объектный модуль, то есть конечный, выходной модуль программы (obj-файл). В данном контексте термин «модуль» означает структурную единицу программы.

[314] «Shifter» (англ.) – «Сдвигальщик». Это название происходит от попыток сдвига в сторону рабочей области экрана монитора, которые предпринимаются данным вирусом.

[315] Module linking (англ.) – (проф.) компоновка модуля.

В общем случае процесс компоновки представляет собой объединение объектных файлов (obj-файлов) и библиотек с целью получения выполнимого кода или динамически подключаемых библиотек – «dynamic link library» (файл динамически подключаемой библиотеки обычно имеет расширение «*.dll»).

[316] Object record (англ.) – (проф.) объектная запись, где под термином «запись» понимается структурированная единица информации. В заголовок записи входят её тип и длина.

писи типа «Data Record»,[317] «Shifter» добавлял к её смещению[318] в сегменте собственную длину в файле с расширением «*.com» (983 байта), подсчитывал и сохранял новую контрольную сумму записи. В результате все записи типа «Data Record» в заражённом объектном модуле получали смещение на 983 байта вниз по сравнению с незаражённым модулем. С помощью этого приёма «Shifter» заставлял программу-компоновщика[319] размещать программный код и данные файла с расширением «*.com» на 983 байта вниз, одновременно высвобождая место для собственного программного кода. В обращении с первой записью типа «Data Record» вирус следовал следующему правилу: если её смещение не равнялось 0100h, данный модуль им не инфицировался. Это делалось для того, чтобы «Shifter» мог впоследствии отличить объектные модули файлов с расширением «*.com» от прочих модулей с расширениями «*.exe», «*.sys», «*.lib» и т.п. Кроме того, поскольку в уже инфицированном вирусом obj-файле смещение первой «Data Record» заведомо отличалось от величины 0100h, вирус повторно не заражал эти объектные модули. Если очередная запись имела тип «Module End Record», вирус целиком помещал её в свой буфер и записывал вместо неё новую запись типа «Data Record», которая содержала программный код вируса. Смещение данной записи в сегменте равнялось 0100h и, следовательно, компоновщик помещал её в начало файла, после чего «Shifter» дописывал в конец файла ранее считанную запись «Module End Record». В том случае, если очередная запись относилась к типу «External Names Definition Record», вирус проверял текущее системное время и с вероятностью 0,25 (в каждом четвёртом случае) сдвигал в сторону рабочую область экрана монитора, а затем выводил следующее сообщение: «Shifting Objective .OBJ Virus (c) 1993 by Stormbringer Kudos for The Nightmare for his ideas and coolness. Greets go out to Phalcon/Skism, Urnst Kouch, Mark Ludwig, NuKE, and everyone else in the commu-

[317] Data Record (англ.) – (проф.) запись данных.

[318] Data offset (англ.) – (проф.) смещение (данных, информации).

[319] Linker (англ.) – (проф.) программа-компоновщик, компоновщик, линкер.

nity» («Сдвиг, реальная цель .OBJ вируса (c) 1993 от Стормбрингера Кьюдос для Ночного Кошмара за его идеи и невозмутимость. Приветствия от всей души Phalcon/Skism, Урнсту Коуху, Марку Людвигу, NuKE, а также всем и каждому в сообществе»).[320]

Интересно, что длина инфицированных вирусом «Shifter» файлов увеличивалась на различные значения. Файлы с расширением «*.com», скомпонованные из заражённого модуля, увеличивались на 983 байта по сравнению с незаражёнными, оригинальными файлами. Объектные модули увеличивались при заражении на 990 байт, так как помимо кода вируса в obj-файл записывалась служебная информация: тип, длина и контрольная сумма записи. «Shifter» пытался инфицировать только те файлы, которые должны компоноваться в файлы с расширением «*.com». Вместе с тем начальный адрес 0100h может быть задан и у большого многосегментного файла с расширением «*.exe». Следовательно, если вирус заразил объектный модуль такого файла, а затем этот объектный модуль был скомпонован в файл с расширением «*.exe», то при попытке его запуска на выполнение компьютерная система могла отказать.

Весной 1994 года в Москве разразилась первая российская эпидемия, виновником которой стал резидентный полиморфный вирус, получивший имя «Phantom1».[321] Начав свой путь в столице, этот достаточно безобидный, лишённый каких-либо деструктивных функций вирус сумел очень широко распространиться по просторам бывшего Советского Союза, отравляя жизнь неискушённых пользователей своими визуальными эффектами и отвлекая их силы и средства на борьбу с ним.

---

[320] Другие известные штаммы вируса («Shifter.758», «Shifter.760») визуально себя никак не проявляют и содержат несколько изменённый текст: «Shifting Objective Virus 3.0 (c) 1994 Stormbringer [Phalcon/Skism] Kudos go to The Nightmare!»

[321] «Phantom1» (англ.) – «Призрак 1». Известны также штаммы «Phantom1.7125» и «Phantom1.7225» («RDA-PHANTOM»).

Попадая в компьютер вполне традиционным способом «Phantom1» устанавливал себя резидентно в оперативную память компьютера, перехватывал прерывание INT 21h и записывался в конец исполняемых файлов с расширениями «*.com» и «*.exe» при их запуске или открытии. После каждого удачного инфицирования он шифровал себя, применяя для этого различные методы, ключи и операции, что позволяло изменять параметры тела вируса и, тем самым, затрудняло работу антивирусного программного обеспечения.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Phantom1
Другие названия	Phantom1.2495
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	февраль 1994 года
Страна происхождения	Венгрия
Длина	2495 байт

Данный вирус отличался «непоседливым характером» и в том случае, если пользователь в течение заданного периода времени не осуществлял операции ввода с клавиатуры компьютера, проявлял своё присутствие в инфицированной им системе специальным видеоэффектом, отображая на экране монитора человеческий череп, который снабжался текстовым сообщением «PHANTOM 1», а затем выводил текстовую строку следующего содержания: «Congratulations!!! Your computer is now infected with a high performance PHANTOM virus! Coming soon: next virus based on the _C00LEST_ mutation engine all over the world: the Advanced Polymorphic Engine! Enjoy this intro! (C) 1994 by Dark Prince» («Поздравляю!!! Ваш компьютер сейчас был инфицирован высокоэффективным вирусом PHANTOM! Ожидается: по всему миру следующий вирус, базирующийся на мутационном движке _C00LEST_: усовершенствованный полиморфный движок! Желаю приятного просмотра! (C) 1994 Чёрный принц»).

«Phantom1» содержал программистские ошибки и иногда при заражении портил файлы, так как в отдельных случаях расшифровщик не мог правильно декодировать содержащийся в инфицированных файлах программ-

ный код вируса и, в итоге, такие файлы при попытке их запуска на выполнение могли вызывать «зависание» компьютерной системы.

Кроме того, описанный выше видеоэффект не появлялся на компьютерах, работавших под управлением операционной системы MS Windows 3.x[322], а также компьютерах, где были установлены некоторые из числа наиболее популярных в то время менеджеров памяти.

В марте в Италии был зарегистрирован в «диком» виде чрезвычайно опасный деструктивный файловый вирус, предназначенный для платформы Macintosh. Этот компьютерный вирус получил имя «Mac/INIT-9403» (другое название «SysX») и инфицировал исключительно компьютерные системы с установленной итальянской версией операционной системы. Когда заражённая прикладная программа запускалась на компьютере, инфицированном «Mac/INIT-9403», она создавала невидимый пользователю объект под названием «Preference»[323]. При выполнении следующей загрузки Macintosh этот объект активизировался и инфицировал «Finder»[324], а в следующую загрузку Macintosh уже заражённый «Finder» удалял «Preference» и заражал прикладные программы. После того как «Finder» инфицировал заранее заданное количество приложений, вирус «Mac/INIT-9403» уничтожал всю информацию во всех логических разделах «жёсткого» диска. Этот вирус почти не распространился за пределы Италии благодаря слишком экзотической для других стран версии операционной системы, в которой он был дееспособен.

В том же марте в «диком» виде появились сразу два компьютерных вируса вызвавшие эпидемии, которые, то затухая, то вспыхивая с новой силой в различных регионах мира, продолжались длительное время.

---

[322] Несколько позже, с появлением MS Windows 95, выяснилось, что это утверждение справедливо и в отношении данной операционной системы.

[323] «Preference» (англ.) – «Предпочтение».

[324] «Finder» (англ.) – «Искатель».

Идентификационная карточка вредоносной компьютерной программы	
Имя	AntiEXE
Другие названия	AntiEXE.A, Antiexe.a, D3, CMOS4, NewBug, New Bug, Stoned.Anti Exe
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	март 1994 года
Страна происхождения	Россия
Длина	1024 байта

Первым «героем», признаваемым некоторыми вирусологами загрузочным резидентным вирусом 1994 года, стал компьютерный вирус, известный под именем «AntiEXE»[325]. Сразу скажем, что этот вирус действительно был далеко не подарком. Интересно также отметить, что к широкому распространению этой вредоносной программы «приложила руку» и фирма Microsoft, которая в результате банального недосмотра разослала его своим многочисленным тестёрам вместе с демонстрационной версией разрабатываемой тогда операционной системы MS Windows 95.

«AntiEXE.A» представлял собой очень опасный загрузочный вирус, который инфицировал загрузочный сектор флоппи-дисков и MBR «жёстких» дисков. Сверх того, он заражал файлы с расширением «*.exe» в том случае, если их размер превышал 200256 байт, а также препятствовал их запуску на выполнение. Вирус «AntiEXE» заражал «жёсткий» диск компьютера, когда он загружался с инфицированного им ранее флоппи-диска. Отсюда следует, что все флоппи-диски, используемые на инфицированном «AntiEXE» компьютере, также заражались и вызывали проблемы во время запуска системы.

Главным очевидным признаком заражения компьютерной системы «AntiEXE» были проблемы, которые возникали при её старте. Кроме того, становился невозможным запуск на выполнение файлов с расширением «*.exe», размер которых превосходил 200256 байт. При наличии в компьютере вируса «AntiEXE» операционная система MS Windows 95 выводила на

[325] «AntiEXE» (англ.) – «Враг EXE». Такое название вирус получил потому, что он заражал файлы с расширением «*.exe», разрушая их содержимое так, что они не моли быть запущены на выполнение.

экран монитора информационное окно с сообщением, предупреждающим пользователей о вероятном изменении прерывания INT 13h.

В результате заражения компьютерной системы вирусом «AntiEXE» происходило следующее:

инфицировался загрузочный сектор флоппи-дисков и MBR «жёсткого» диска;

оригинальная главная загрузочная запись заменялась на её инфицированную версию (оригинальная MBR с помощью «стелс» технологии пряталась в другом разделе «жёсткого» диска);

инфицировались все флоппи-диски, которые использовались на заражённом компьютере, при условии, что они не защищены от записи;

заражённые файлы с расширением «*.exe» не запускались на выполнение;

возникали трудности с корректной загрузкой инфицированного компьютера.

В процессе инфицирования вирус «AntiEXE» выполнял следующую последовательность процедур:

компьютер заражался только тогда, когда загружался с инфицированного флоппи-диска;

с инфицированного флоппи-диска вирус проникал в оперативную память компьютера и оставался там резидентно, занимая один килобайт в верхней области памяти;

оставаясь в оперативной памяти, вирус заражал все флоппи-диски, которые использовались в компьютере, для чего перехватывал прерывание INT 13h и перезаписывал вектор прерываний соответствующим прерыванием INT D3h;

прятались оригинальные загрузочные сектора флоппи-дисков и «жёстких» дисков, которые заменялись на заражённые копии. В случае с «жёсткими» дисками вирус передвигал оригинальный загрузочный сектор на сторону 0, цилиндр 0, сектор 13 диска. В случае с флоппи-дисками вирус передвигал

оригинальный загрузочный сектор на сторону 0, цилиндр 0, сектора 3, 5, 14 или 15 флоппи-диска (в зависимости от характеристик флоппи-диска: размер, плотность записи, ёмкость и т. п.).

«AntiEXE» размножался посредством флоппи-дисков следующим образом:

инфицировал «жёсткий» диск компьютера, когда он загружался с флоппи-диска, заражённого этим вирусом;

инфицировал все используемые в заражённом компьютере флоппи-диски, если они не были защищены от записи.

Конспективное рассмотрение компьютерного вируса «AntiEXE» завершим следующим сообщением журнала «Defense News» (США): «…*в 1996* году американская армия в Боснии столкнулась с многочисленными случаями заражения компьютерными вирусами «Monkey», «AntiEXE» и «Prank». В результате армейскому персоналу пришлось потратить сотни часов, отыскивая вирусы и очищая заражённые ими системы». Оцените, пожалуйста, живучесть «AntiEXE»! От себя добавим, что этот вирус окончательно покинул лидирующие двадцать «диких» вирусов в перечне «WildList» Международной организации WildList только в мае 2000 года.

Вторым «героем» стал очень опасный загрузочный резидентный компьютерный вирус, впервые обнаруженный в Швейцарии и получивший имя «Form»[326]. Со временем этот вирус стал одним из наиболее распространённых в мире и «живучих» вирусов, а его характерной чертой было то, что в отличие от большинства загрузочных вирусов он инфицировал загрузочный сектор активного раздела[327] «жёсткого» диска вместо MBR. Вирус «Form» перехватывал прерывания INT 9, 13h и заражал загрузочный сектор флоппи-дисков при обращении к ним и загрузочный сектор «жёсткого» диска при за-

---

[326] «Form» (англ.) – «Форма», «Формуляр». Вирус получил такое название от словосочетания «FORM-Virus», которое содержится в его программном коде.

[327] Active partition (англ.) – часть «жёсткого» диска, содержащая операционную систему, которая загружается при включении и перезагрузке компьютера.

грузке с флоппи-диска. Программный код «Form» занимал два сектора: вирус резервировал два свободных килобайта в основной оперативной памяти,[328] модифицируя слово по адресу 40:13. Соответственно, на компьютере с 640 Кб памяти системная утилита MEM в своём отчёте показывала 638 Кб, а утилита CHKDSK 653312 байт свободной памяти.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Form
Другие названия	Form.A, FormA, Form 18, Form-18, Form_18, Form Boot
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	март 1994 года
Страна происхождения	Швейцария
Длина	1024 байт

Итак, при заражении системы этот вирус переписывал загрузочный сектор раздела «жёсткого» диска собственным программным кодом, сохраняя оригинальный загрузочный сектор (из сектора 0, сторона 1, цилиндр 0) и сектор со своим кодом в последних двух секторах заражённого «жёсткого» диска[329]. Причём «Form» давал занять или, иными словами, не защищал каким-либо способом эти сектора от записи в них информации, так что они позже могли быть перезаписаны другими данными, что вызывало «подвешивание» «жёсткого» диска во время выполнения последовательности операций начальной загрузки[330]. Инфицируя флоппи-диск, «Form» сохранял второй свой сектор и оригинал загрузочного сектора в неиспользуемом кластере и, чтобы защитить его, помечал этот кластер в FAT как «плохой». В итоге системная утилита CHKDSK после проверки инфицированного флоппи-диска выдавала со-

[328] Conventional memory (англ.) – основная или обычная память представляющая собой первые 640 Кб оперативного запоминающего устройства для персональных компьютеров с операционной системой DOS.

[329] Этот технический приём, известный как «стелс» технология, уже неоднократно рассматривался нами на примере других вирусов.

[330] Boot sequence (англ.) – последовательность операций начальной загрузки, обращения к дискам при включении компьютера, например, сначала к A:, потом к C: и т. д.

общение о том, что в плохих секторах находится 1024 байта (1 КБ). Во время загрузки с заражённого диска вирус проверял дату использования прерывания INT 1Ah функция 4. Он сличал величину в регистре «DL» с числом 18.[331] и восемнадцатого числа каждого месяца «Form» срабатывал и через системный динамик воспроизводил щёлкающий звук всякий раз, когда нажималась какая-либо клавиша на клавиатуре компьютера. Однако это случалось только в том случае, если на компьютере не был установлен драйвер клавиатуры «keyb.com». Кстати, указанные выше проявления вируса оказывались более деструктивными для компьютерных систем с установленной операционной системой MS Windows NT, так как после инфицирования приходилось исправлять загрузочный сектор «жёсткого» диска.

Вирус содержал в своём теле текст, включавший в том числе короткое непристойное выражение, адресованное кому-то по имени Карина: «The FORM-Virus sends greetings to everyone who reading this text. FORM doesn't destroy data! Don't panic! Fuckings go to Corinne» («Вирус FORM приветствует всех, кто читает этот текст. FORM не разрушает данные! Без паники! …») Это выражение не показывалось на экране монитора, но его можно было увидеть при исследовании с помощью программы редактирования предпоследнего сектора раздела «жёсткого» диска или первого сектора в «плохом» кластере на флоппи-диске. Кроме того, вирус «Form» содержал дефектный программный код – две программистские ошибки, которые могли стать и становились источником вполне реальных проблем для пользователя. Во-первых, он не осуществлял повторную попытку чтения и «подвешивал» систему при чтении сбойного диска. Во-вторых, поскольку вирус, как мы уже упоминали, не защищал второй сектор и оригинальный загрузочный сектор DOS на «жёстком» диске, они могли быть перезаписаны другой информацией (когда этот диск без остатка заполнялся данными), делая его не способным

[331] «Form» проверял наличие в регистре именно 18-го, а не 24-го числа текущего месяца, хотя в некоторых источниках в качестве срабатывания вируса ошибочно указывается 24 число.

к загрузке системы, – в результате, при дальнейшей работе происходила потеря данных. Между прочим, вирус «Form» предполагал, что активный раздел является разделом операционной системы MS-DOS, что вызывало фатальную ошибку под управлением отличных от DOS операционных систем и компьютер переставал загружаться. Операционная система MS Windows NT проявляла себя уязвимой по отношению к этой проблеме и, следовательно, инфицированная вирусом «Form» MS Windows NT могла служить причиной серьёзного отказа всей системы. Впрочем, на компьютерных системах под управлением операционной системы MS-DOS (и 16-битной MS Windows) «Form» вёл себя достаточно незаметно, и именно такое поведение от части объясняет, почему данный вирус сумел так широко распространиться по всем континентам.

В завершение рассмотрения вируса «Form» подчеркнём, что этот вирус оказался не менее живучим, чем «AntiEXE» и окончательно покинул лидирующие двадцать «диких» вирусов в перечне «WildList» Международной организации WildList лишь в июне 2000 года!

В апреле было обнаружено семейство вирусов «SrcVir», которые заражали исходные тексты программ, написанных на языках программирования высокого уровня – «C» и «Pascal».

А в мае появился очень опасный и сложный загрузочный файловый резидентный полиморфный многокомпонентный, и использовавший к тому же «стелс» технологию компьютерный вирус «One_Half»[332], который стал причиной начала масштабной и очень продолжительной эпидемии, доставившей

---

[332] «One_Half» (англ.) – «Половина». Автором этого вируса был известный вирусописатель того времени, скрывавшийся под псевдонимом «Vyvojar», который позже разработал мутационный движок под названием «Explosion's Mutation Machine».

Такое «произведение искусства» как «One_Half просто не могло «не дать потомства», и, вскоре, один за другим появились многочисленные штаммы, составившие впоследствии целое семейство вирусов. Например: «One_Half.3518», «One_Half.3544.b-g» (6 штаммов), «One_Half.3666», «One_Half.3570», «One_Half.3577», «One_Half.Madjid».

массу неприятностей пользователям по всему миру и ставший по настоящему всемирно знаменитым. Эта вредоносная компьютерная программа использовала похожий на применённый в «Commander Bomber»[333] алгоритм инфицирования компьютерной системы и, помимо того, что «разбрасывала фрагменты» (10 «фрагментов» по 10 байт каждый) своего программного кода внутри заражённого файла, производила шифрование основного тела вируса, располагаемого в конце файла.

Идентификационная карточка вредоносной компьютерной программы	
Имя	One_Half
Другие названия	OneHalf, One_half, One_Half.mp.3544, One_Half.mp.3544.A, Mid/OneHalf3544, LEAVE, SlovakBomber, Explosion-II, Dis, Free Love
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS, Windows 3.1[334]
Впервые обнаружен	май 1994 года
Страна происхождения	Словакия
Длина	3544 байта и 512 байт (MBR)

Вирус «One_Half» относился к типу вирусов не удаляющих, а зашифровывающих диски или файлы пользователей: он последовательно шифровал информацию на «жёстком» диске, динамически расшифровывая её так, чтобы эта деятельность проходила незаметно для пользователя заражённой системы. Однако, зашифровав ровно половину «жёсткого» диска, вирус прекращал операцию расшифровки и, в результате, пользователь лишался доступа к файлам, расположенным на этом «жёстком» диске. Но, обо всём по порядку.

Проникая в компьютер, «One_Half» заражал системные области «жёсткого» диска и некоторые программные файлы. При первом запуске инфицированного файла «One_Half» инфицировал MBR первого физического «жёсткого» диска компьютера (накопитель 80h, диск C:), а при загрузке с заражён-

[333] Более подробно об этом компьютерном вирусе см. выше – 1992 год.

[334] «One_Half» полностью совместим с большинством версий операционных систем MS-DOS и Windows 3.1, но, в некоторых конфигурациях MS Windows может не загружаться, если вирус «One_Half» присутствует в оперативной памяти компьютера.

ного «жёсткого» диска перехватывал прерывания INT 13h, 1Ch, 21h и инфицировал файлы с расширениями «*.com» (включая командный процессор «command.com»), «*.exe» и «*.sys» при обращении к ним[335]. При этом «One_Half» применял «стелс» технологию, чтобы «спрятать» инфицированную MBR[336] и технологию полиморфизма для затруднения обнаружения и удаления заражённого файла при помощи антивирусного программного обеспечения[337]. В то время как вирус уже резидентно находился в оперативной памяти компьютера, он «прятал» заражённую MBR[338] и инфицированные им файлы, а пользователю «показывал» копии их оригиналов. Код расшифровщика «One_Half» был разбросан по всему файлу со случайными смещениями. При заражении «жёсткого» диска вирус считывал его MBR и просматривал таблицу разбиения диска (Disk Partition Table). В указанной таблице он искал последний DOS диск – логический диск (FAT–12/FAT–16/BIGDOS) или Extended partition, и когда находил, подсчитывал номер первого и последнего цилиндров найденного диска (или Extended partition). При этом вирус правильно обрабатывал «жёсткие» диски, которые имели объём более 1024 цилиндров и не подходили под стандарт прерывания INT 13h. Вирус «One_Half» запоминал адреса этих цилиндров и заражал «жёсткий» диск, а затем при перезагрузке системы с инфицированного им «жёсткого»

---

[335] Во время инфицирования файла «One_Half» сразу же просматривал его имя на наличие текста, связанного с антивирусным программным обеспечением. Если такие файлы находились, например: «scan*.*», «clean*.*», «findviru*.*», «guard*.*», «nod*.*», «vsafe*.*», «msav*.*», «chkdsk*.*», - то они не заражались.

[336] Когда вирус находится резидентно в оперативной памяти, он «прячет» от пользователя все сделанные им изменения в загрузочных секторах или файлах, которые были инфицированы, например: изменение размера, даты, атрибутов и т.п.

[337] Вирус шифрует себя при помощи различных приёмов после завершения очередного инфицирования для чего применяет различные ключи и алгоритмы. В итоге он постоянно меняет свои основные характеристики, что затрудняет его обнаружение.

[338] Оригинальная MBR и семь секторов тела вируса «прячутся» в последних секторах 0 цилиндра «жёсткого» диска.

диска зашифровывал сектора двух его последних цилиндров. При следующей перезагрузке системы по тому же принципу шифровались сектора ещё двух цилиндров и т. д., пока процесс не доходил до первого цилиндра. При этом вирус пользовался адресами первого и последнего цилиндров «жёсткого» диска, которые он «запомнил» ещё при его заражении. Когда количество зашифрованных цилиндров достигало половины от их общего количества на «жёстком» диске, то есть половины объёма «жёсткого» диска «One_Half» выдавал на экран монитора следующее сообщение: «Dis is one half. Press any key to continue...» («Половина является признаком нарушения непрерывности. Нажмите любую клавишу для продолжения…»). После этого вирус переходил в режим ожидания нажатия на какую-нибудь из клавиш на клавиатуре компьютера. В подавляющем большинстве случаев пользователь послушно следовал этому указанию, и вирус продолжал свою работу, перезагружая компьютер. Причём, чем чаще перезагружалась инфицированная «One_Half» компьютерная система, тем больше данных оказывалось зашифрованными.

Как мы уже упоминали, этот вирус после установки резидентно в оперативную память расшифровывал и зашифровывал сектора «жёсткого» диска динамически и, по этой причине, пользователь не замечал того, что его данные испорчены. Другими словами, пока «One_Half» находился в оперативной памяти, он контролировал все обращения к зашифрованным областям «жёсткого» диска (чтение секторов данных цилиндров) и по мере надобности их расшифровывал. Поэтому программное обеспечение компьютера внешне работало в нормальном режиме. Если же предпринимались попытки трассировки резидентной части вируса, «One_Half», со своей стороны, предпринимал достаточно эффективные меры по «подвешиванию» системы.

В случае лечения MBR имевшимися на то время антивирусными программными средствами – простого удаления вируса из MBR и оперативной памяти – чтение информации зашифрованных секторов оказывалось невозможным и все данные в зашифрованных областях «жёсткого» диска оказыва-

лись потерянными. Таким образом, появление «One_Half», кроме всего прочего, поставило перед фирмами-разработчиками антивирусных средств, в продуктах которых применялись методы общего лечения или технологии так называемой «вакцинации», неотложную задачу модернизации их программного обеспечения. Ведь хотя общее лечение и приводило к успешному удалению «One_Half» из инфицированной им MBR, например, выполнение FDISK/MBR, все данные в зашифрованных областях «жёсткого» диска терялись. Итак, широкомасштабная и продолжительная эпидемия, связанная с вирусом «One_Half» стала возможной, в первую очередь потому, что он применял сложные методы своей маскировки, а многие пользователи продолжали ограничиваться установкой простых антивирусных средств, оставляя свои компьютеры совершенно беззащитными перед такими вирусами, использовавшими усовершенствованную «стелс» технологию и многокомпонентность. Поэтому следует ещё раз подчеркнуть, что для надёжной защиты своих компьютеров от современных разновидностей вредоносных компьютерных программ следует использовать только самые последние версии антивирусных программно-аппаратных комплексов, причём, строго руководствуясь требованиями по их установке и конфигурации, изложенными в прилагаемой технической документации.

И последнее: вирус «One_Half» оказался практически столь же «жизнелюбивым» созданием, как и рекордсмены движения, компьютерные вирусы «AntiEXE» и «Form». Этот вирус окончательно покинул лидирующие двадцать «диких» вирусов в перечне «WildList» Международной организации WildList лишь в мае 2000 года.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Natas
Другие названия	Sat_Bug.Natas, «Natas .4744»
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	май 1994 года
Страна происхождения	Соединённые Штаты Америки
Длина	4744 байта

Вслед за «One_Half» был обнаружен компьютерный вирус, который также как и эта знаменитость обладал свойствами полиморфизма, многокомпонентности и использовал «стелс» технологию. Ему присвоили имя перевёртыш «Natas»[339]. Вслед за вирусом-родоначальником появились его многочисленные штаммы – «Natas.4746», «Natas.4766», «Natas.4774», «Natas.4786», «Natas.4926», «Natas.4988», которые составили целое семейство вирусов и, в основном, отличались друг от друга текстовыми строками, содержащимися в их теле[340]. Эти строки иногда представляли собой короткий текст, например: «Time has come to pay (c) 1994 NEVER-1» («Пришло время расплаты (c) 1994 NEVER-1»), а иногда и пространные стихи, как у «Natas.4774».

Эти очень опасные файловые загрузочные резидентные вирусы перехватывали прерывания INT 13h, 21h и записывались в загрузочные сектора MBR первого физического «жёсткого» диска компьютера (80h, диск C:), загрузочные сектора флоппи-дисков, а также, при обращении к ним, в конец файлов с расширениями «*.com» и «*.exe». Кроме того, вирусы семейства «Natas» заражали оверлейные файлы[341], но не инфицировали те файлы, которые открывались с помощью утилит PKZIP, PKUNZIP, LHA и ARJ., а также форматировали сектора дисков.

---

[339] Прочтите, пожалуйста, наоборот, и у Вас получится «Satan»: «Сатана».

[340] Штамм «Natas.4926» не уничтожает информацию на «жёстком» диске компьютера.

[341] Overlay file (англ.) – оверлейный файл (оверлейная программа), хранится на внешнем запоминающем устройстве и загружается в оперативную память компьютера по мере необходимости. Применялись в компьютерных системах без виртуальной памяти.

Вирусы «Natas» представляли собой тщательно разработанные вредоносные компьютерные программы, содержащие деструктивную функцию, которая в зависимости от внутренних счётчиков инициировала процедуру форматирования полезной информации на секторах «жёсткого» диска, в результате чего данные пользователя уничтожались.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Kaos4
Другие названия	Kaos.697, Kaos4.697
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	май 1994 года
Страна происхождения	Соединённые Штаты Америки
Длина	697 байт

Начиная с весны 1994 года, всё больше обостряется проблема распространения вредоносных компьютерных программ посредством различных информационных служб, порталов, электронных игр и других компьютерных программ, в том числе записанных на новых типах носителей информации.

Например, компьютерный вирус, получивший имя «Kaos4», был послан электронной почтой в группу новостей[342] (alt.binaries.pictures.erotica) в файле, названном «Sexotica». Компьютерный вирус, зашифрованный как текст, был загружен некоторыми пользователями, декодировался в исполняемой программе и запустился на их компьютерных системах[343].

---

[342] News group (англ.) – группа новостей, совокупность представляемых в Интернет информационных сообщений, которые относятся к одной и той же предметной области.

[343] При активации вирус «Kaos4» искал в пределах текущего рабочего директория первые неинфицированные файлы с расширениями «*.com» или «*.exe» и инфицировал их, записываясь в конец этих файлов. Если он не находил в текущем рабочем директории не заражённых им ранее файлов с расширениями «*.com» или «*.exe», то инициировал процедуру поиска таких файлов посредством просмотра директориев, перечисленных в «PATH=statement», выискивая в них файл, который может быть заражён. Инфицированные «Kaos4» файлы содержали следующий текст: «KAOS4/Köhntark».

Таким способом была спровоцирована локальная эпидемия. К счастью, вирус «Kaos4» являлся в полном смысле слова вирусом «посредственным вирусом». Если бы на его месте оказался более эффективный компьютерный вирус, он мог легко превратить сравнительно небольшую эпидемию в широкомасштабную. Но, как бы то ни было, вирус «Kaos4» ещё несколько лет существовал в «диком» виде и присутствовал в отчётах вирусологов из разных стран мира.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Chill
Другие названия	Chill Touch, Chill.544
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	май 1994 года
Страна происхождения	Соединённые Штаты Америки
Длина	544 байта

Другой, очень опасный резидентный зашифрованный компьютерный вирус, получивший название «Chill»[344], был найден в некоторых играх, размещённых на ZiffNet.

Он перехватывал прерывание INT 21h и записывался в конец файлов с расширением «*.com» при обращении к ним. Этот вирус содержал встроенные деструктивные функции, которые должны были инициировать форматирование части секторов первого физического «жёсткого» диска компьютера (80h). Однако эта процедура, благодаря допущенным автором вируса ошибкам в программном коде «Chill», никогда не выполнялась. Данный вирус содержал в своём теле строку: «[CHiLL TOUCH] You cannot touch these phantoms» («[ПРИКОСНОВЕНИЕ CHiLL] Вы не сможете осязать эти призраки»).

Некоторые из компьютерных игр, заражённых «Chill»[345], были загружены пользователями через CompuServe[346], но этот вирус, подобно вирусу «Kaos4», был лишён каких-либо инновационных решений и имел в программном коде серьёзные ошибки. В силу перечисленных причин этот вирус

[344] «Chill» (англ.) – «Простуда», «Озноб».

[345] А также и компьютерным вирусом, подобным «Kaos4».

[346] CompuServe – оперативная информационная служба США.

достаточно легко обнаруживался антивирусными программными средствами и, соответственно, не получил широкого распространения.

В июне 1994 года началась эпидемия компьютерного вируса по имени «AntiCMOS»[347], представлявшего собой вполне типичный загрузочный резидентный вирус, инфицировавший MBR «жёсткого» диска компьютера и загрузочный сектор флоппи-дисков, причём копии их оригиналов не сохранялись.

Идентификационная карточка вредоносной компьютерной программы	
Имя	AntiCMOS
Другие названия	AntiCMOS.A, Lenart, Anti-CMOS, Anti.a, Anticmos, AntiCMOSBoot, CMOS Killer, Gaxelle
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	июнь 1994 года
Страна происхождения	Гонг Конг, Китай
Длина	2024 байта

Главная потенциальная опасность «AntiCMOS» заключалась в том, что он обладал деструктивной функцией, которая должна была активизироваться после случайного числа попыток загрузки системы и стирать часть настроек параметров памяти CMOS[348], приводя компьютерную систему в неработоспособное состояние. Таким образом, имя этому вирусу – «ANTICMOS», было дано на том основании, что он был запрограммирован для записи в CMOS через порты 70h and 71h, в результате чего должна была удаляться служебная информация из CMOS, включая и конфигурацию «жёсткого» диска.

---

[347] В августе 1994 года к родоначальнику добавился штамм по имени «Anticmos B» (другое название: «Anticmos Lixi»), который содержал в своём теле текстовую строку: «I am Li Xibin!» («Я Ли Ксибин!»). Кроме того, если выполнялись заданные условия активизации, «AntiCMOS.B» должен был вызывать звуки через системный динамик компьютера (эта процедура никогда не выполнялась из-за ошибок, допущенных автором вируса в программном коде).

[348] CMOS (проф.) – «complementary metal-oxide semiconductor», постоянное запоминающее устройство.

К счастью, эта функция не работала из-за допущенных автором при написании программного кода вируса ошибок.

При инфицировании системы «AntiCMOS» проникал в компьютер, когда система загружалась с инфицированного флоппи-диска, и устанавливался резидентно в оперативной памяти, занимая 2 Кб в области основной (обычной) памяти[349].Перехватывал и переадресовывал прерывание INT 13 BIOS Disk I/O Services, а затем возвращал управление операционной системе для последующей обработки начальной загрузки.Находясь в оперативной памяти инфицированного им компьютера «AntiCMOS» проверял все используемые в системе флоппи-диски и, если какой-либо из них оказывался не заражённым, начинал запись своего программного кода в загрузочный сектор этого флоппи-диска, тем самым, заражая его. Проверял, откуда производится загрузка системы – с флоппи-диска или «жёсткого» диска. Если с флоппи-диска, то осуществлял проверку MBR для того, чтобы выяснить факт её заражения и, в случае, если MBR оказывалась не инфицированной, приступал к её заражению, заменяя оригинальную главную загрузочную запись инфицированной. Таким образом, могла быть уничтожена важная служебная информация, размещённая в загрузочном секторе «жёсткого» диска (метка тома, серийный номер и т. п.). После этого все попытки загрузки заражённой компьютерной системы осуществлялись только при помощи инфицированной MBR «жёсткого» диска.

Вместе с тем, «AntiCMOS» не вносил изменений в таблицу разделов, которая используется компьютерной системой для определения доступа к «жёсткому» диску и, следовательно, всегда оставалась возможность загрузки системы с защищённого от записи «чистого» загрузочного флоппи-диска с целью получения доступа к «жёсткому» диску и решения проблем с его нарушенной конфигурацией.

---

[349] Conventional Memory (англ., проф.) – основная (обычная) память. Для персонального компьютера с установленной операционной системой MS-DOS первые 640 Кб оперативного запоминающего устройства (ОЗУ).

Так как «AntiCMOS» практически не обнаруживал своё присутствие в инфицированной компьютерной системе и единственным видимым симптомом его существования служило наличие некоторых проблем при её загрузке, этот компьютерный вирус сумел широко распространиться по всему миру и по продолжительности функционирования в «диком» виде стать в один ряд с такими знаменитостями, как «One_Half», окончательно покинув лидирующие двадцать «диких» вирусов в перечне «WildList» Международной организации WildList лишь в августе 2000 года.

Идентификационная карточка вредоносной компьютерной программы	
Имя	ЗАРАЗА
Другие названия	ЗАРАЗА.a, Зараза
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	июль 1994 года
Страна происхождения	Россия
Длина	1024 байта

В августе 1994 года началась эпидемия файлового загрузочного резидентного полиморфного вируса «ЗАРАЗА»[350], который использовал крайне необычный способ своего внедрения в операционную систему MS-DOS.

Он заражал начальные сектора флоппи-дисков и файл IO.SYS на логическом диске C:, имел длину в 1024 байта и состоял из двух частей (секторов). Первая часть содержала инсталлятор вируса и подпрограмму инфицирования флоппи-дисков, а вторая часть – программный код, который встраивался в загрузочные сектора флоппи-дисков и представлял собой процедуру заражения файла IO.SYS (или его аналога типа IBMBIO.COM) на «жёстком» диске компьютера. Причём в загрузочных секторах тело вируса хранилось в зашифрованном виде.

При загрузке с инфицированного флоппи-диска вирус «ЗАРАЗА» расшифровывал себя и передавал управление специальной подпрограмме с целью заражения файла IO.SYS, которая считывала первый загрузочный сектор

[350] Известен штамм «ЗАРАЗА.b», который перехватывает прерывание INT 16h вместо прерывания INT 13h («ЗАРАЗА.a») и заражает флоппи-диски при вводе символов с клавиатуры компьютера. Проявляет себя характерным треском в системном динамике.

«жёсткого» диска (логического диска C:). Затем эта подпрограмма проверяла объём диска[351], подсчитывала адрес корневого каталога, считывала его, проверяла атрибут первой записи корневого каталога и не заражала «жёсткий» диск в том случае, если первая запись в корневом каталоге имела атрибут «VOLUME». В противном случае, то есть атрибут отличался от «VOLUME», вирус копировал в последние сектора «жёсткого» диска файл, соответствующий первому входу (стандартно это IO.SYS), и сдвигал вниз на одну позицию все записи в корневом каталоге с третьего по семьдесят седьмой[352]. После выполнения перечисленных операций вирус «3APA3A» копировал системные данные из первой записи корневого каталога в третью и устанавливал в третьей записи адрес первого кластера файла на только что созданной копии IO.SYS. Как Вы уже поняли, в результате выполнения приведённой последовательности действий в системе появлялось сразу два файла под именем IO.SYS, но на первый указывала первая запись в корневом каталоге, а на второй третья запись. В итоге вирус записывал вместо первого IO.SYS свой код и проставлял у этой записи атрибут «VOLUME».

Все описанные нами манипуляции вирус осуществлял при помощи прерывания INT 13h и выполнял эту работу весьма корректно: «жёсткий» диск проверялся на наличие свободных кластеров, правильно сохранялись все копии FAT и т. п. Атрибут «VOLUME» у инфицированного вирусом «3APA3A» системного файла IO.SYS служил двум целям: во-первых, выполнял роль идентификатора заражённого «жёсткого» диска, а во-вторых, реализовывал функцию «стелс» технологии, частично применяемой вирусом. Файл с атрибутом «VOLUME» не виден для стандартных функций операционной системы MS-DOS (например, «FindFirst/Next», «Open», «Read», «Close»), следовательно, чтобы обнаружить этот файл и прочитать его содержимое,

---

[351] Если объём «жёсткого» диска составлял менее 26 МБ, то он не инфицировался, то есть использовалась 12-битная Таблица размещения файлов (FAT).

[352] Естественно, что при этом последняя запись утрачивалась в силу того, что поверх неё записывалась предпоследняя запись.

необходимы специальные утилиты чтения дисковых секторов, подобные «DiskEditor».

В результате описанной выше процедуры логический диск C: оказывался инфицированным, но загрузочный сектор и MBR не менялись, оставаясь оригинальными. Изменениям подвергался только файл IO.SYS. Поэтому при загрузке операционной системы с заражённого «жёсткого» диска внешне весь процесс протекал точно так же, как и на не инфицированной системе (загрузка и выполнение MBR и загрузочного сектора) до момента запуска IO.SYS. Стандартный загрузчик MS-DOS сравнивал имена первых двух входов в корневой каталог со строками IO.SYS и MSDOS.SYS (или эквивалентными строками). Загрузчик искал строки, но не проверял атрибуты обнаруженных входов в каталоге. В результате он находил в первом входе строку IO.SYS, загружал соответствующий файл (вирус) в память и передавал ему управление. При загрузке с инфицированного «жёсткого» диска процедура инсталляции, получив управление, перехватывала INT 13h и оставляла вирус в памяти стандартным способом, уменьшая размер системной памяти (на слово по адресу 0000:0413). При вызове прерывания INT 13h вирус «ЗАРАЗА» обрабатывал обращения к флоппи-дискам и заражал их. Он сохранял своё продолжение и первоначальный загрузочный сектор в последних секторах корневого каталога флоппи-диска, записывая свой инсталлятор вместо загрузочного сектора, предварительно зашифровав его при помощи полиморфного алгоритма. В августе при загрузке с инфицированного «жёсткого» диска вирус расшифровывал и выводил на экран монитора следующее текстовое сообщение: «В BOOT СЕКТОРЕ – ЗАРАЗА».

Особо подчеркнём, что ни одна из существовавших на то время антивирусных программ не могла успешно бороться с вирусами подобного типа. С формальной точки зрения вирус «ЗАРАЗА» не являлся «полноценным стелс-вирусом», но его обнаружение, блокирование и лечение на «жёстком» диске компьютера весьма затруднены. Инфицированный вирусом системный файл IO.SYS не виден стандартным функциям MS-DOS и, следовательно,

может быть обнаружен только вызовами через прерывания INT 13h/25h, причём заражённый файл невозможно также ни удалить, ни переименовать. Единственный способ обнаружить вирус из среды операционной системы MS-DOS это использование стандартной команды «Label» – при её вызове MS-DOS выводит сообщение: «Volume in drive C: is IO.SYS» («Том в накопителе C: IO.SYS»), а на попытку изменения метки «жёсткого» диска MS-DOS сообщает: «Cannot make directory entry» («Не могу создать каталог ввода»). Невозможно было вылечить «жёсткий» диск и системной утилитой «SYS», так как она могла заменить только вторую копию IO.SYS, но не уничтожала сам вирус. По этой причине «жёсткий» диск становился загружаемым, но, поскольку вирус «ЗАРАЗА» считывал инфицированный IO.SYS по абсолютным адресам, сохранённым во время заражения «жёсткого» диска, по команде «SYS» и просто перемещался на новое место.

Примерно через год после задержания агентами специального подразделения по борьбе с компьютерными преступлениями Нового Скотланд-Ярда (Великобритания) автора вызвавшего в начале 1993 года настоящую панику вируса «Pathogen» и скрывавшегося под кличкой «Black Baron», летом 1994 года правоохранительными органами Великобритании была арестована уже целая группа вирусописателей, состоящая из граждан этой страны и называвшая себя Association for Really Cruel Viruses (ARCV)[353], а в начале осени ещё один автор вирусов был арестован полицией Норвегии. В результате последующих судебных процессов вирусописатели указанной группы на первый случай отделались достаточно крупными штрафами.

Очередная волна паники, связанной с компьютерными вирусами, прошла в декабре 1994 года и была связана с компьютерной мистификацией, которая заключалась в предупреждении о якобы существующем ужасном виру-

[353] Association for Really Cruel Viruses (англ.) – Ассоциация по действительно диким вирусам.

се «GoodTimes»[354], распространяющем себя по сети Интернет и заражающем компьютер при получении электронной почты. Эта компьютерная мистификация быстро вышла на международный уровень и была переведена с английского языка на многие языки мира, в том числе испанский, французский, немецкий, русский, итальянский и др. Ещё несколько лет в службы технической поддержки фирм-разработчиков антивирусных средств приходили письма от взволнованных пользователей, требующих рассказать о новом, чрезвычайно опасном компьютерном вирусе «GoodTimes», слухи о котором ходят среди знакомых пользователей сети Интернет. На самом деле такого вируса не существовало, но через некоторое время действительно появился заурядный вирус, получивший название «GT-Spoof», с текстом «Good Times», подогревший и без того нездоровый интерес к старой компьютерной мистификации.

Как мы уже упоминали ранее, в 1994 году приобретала всё большее значение и остроту проблема распространения вредоносных компьютерных программ с помощью новых каналов и носителей информации, в частности, компакт-дисков, CD-ROM. Быстро став популярными, эти диски оказались одним из основных средств распространения компьютерных вирусов. Было отмечено сразу несколько инцидентов, когда вирус попадал на мастер-диск при подготовке к реализации достаточно крупных партий CD-ROM с компьютерными программами. В результате на компьютерный рынок были выпущены большие тиражи (десятки тысяч единиц) заражённых компакт-дисков. Естественно, что об их лечении говорить не приходилось, и указанные партии готовой продукции уничтожались физически, что причиняло существенный экономический ущерб.

В целом 1994 год остался в истории вирусописания в качестве бурного и богатого событиями времени. От себя добавим, что, пожалуй, даже черес-

[354] Более подробно об этой мистификации и компьютерных мистификациях вообще можно прочитать в Томе 1 (Приложение 1. «Компьютерные мистификации и вредоносная мимикрия») настоящей книги.

чур обильного неординарными и деструктивными компьютерными вирусами.

§15. 1995 год – начало заката эры загрузочных вирусов, новые приёмы маскировки от антивирусных средств и пользователя, «двуполый» вирус, пандемии «Byway» и «DieHard2», триумфатор года макро вирус «Concept»

- Выпущена 32-х разрядная операционная система Windows 95 (другие названия: Windows 4.0, Windows Chicago).
- Выпущена операционная система Windows NT 3.51.
- Выпущена версия 1.2 операционной системы Linux, которая работала на процессорах Intel, Digital и Sun SPARC. Тираж журнала «Linux Journal» достиг 10 тысяч экземпляров.
- Выпущена версия 7.0 операционной системы PC-DOS.
- Компания Sun анонсировала технологию Java.
- Выпущен микропроцессор Intel Pentium Pro (5,5 миллионов транзисторов).
- Компания Compaq выпустила первый карманный компьютер.

Как писали специализированные издания того времени, год начался относительного спокойно, и складывалось впечатление, что всё мировое компьютерное сообщество пребывает в ожидании скорого появления анонсированной фирмой Microsoft операционной системы MS Windows 95[355]. Ничего эпохального в области вирусописания под операционную систему MS-DOS не происходило, хотя в течение года и появилось несколько достаточно сложных вирусов этого типа. В прессе регулярно публиковались статьи по поводу того, как повлияет новая операционная система на развитие индустрии антивирусных средств защиты, а также, какое воздействие она окажет

[355] Правда, некоторые компании сумели несколько потревожить «штиль», умудрившись стать организаторами очередных инцидентов, выпустив заражённые компьютерными вирусами CD-ROM. Подобные неприятности были зафиксированы у производителей программного обеспечения – CD-ROM в качестве удобного и ёмкого носителя информации становились всё популярнее и постепенно начали вытеснять традиционные флоппи-диски. Ситуация же осложнялась тем, что, в отличие от обычных флоппи-дисков, вирус с компакт-дисков невозможно было удалить, а это вынуждало пользователей просто выбрасывать их в мусорную корзину.

на вирусописателей всех мастей и стран мира. Уже тогда было очевидно, что наиболее распространённые в то время загрузочные компьютерные вирусы не смогут воспроизводиться на компьютерных системах под управлением операционной системы MS Windows 95. Отдельные компании-разработчики антивирусных продуктов начали даже предрекать начало процесса тихого угасания своего антивирусного программного обеспечения, который будет сопровождать уход со сцены морально устаревших операционных систем. Однако к августу, произошли существенные изменения в их умонастроении, но об этом – ниже.

Вместе с тем, популяризация Интернет, например, способствовала учащению DoS-атак[356], направленных на вывод из строя серверных систем. Причём, иногда применялись способы, которые на то время трудно было квалифицировать как противозаконные. Один из них – это бомбардировка почтового сервера тысячами сообщений с многократно вложенными друг в друга архивами. Установленная на сервере антивирусная программа была вынуждена проверять все вложенные архивы, последовательно их распаковывая. При этом она постепенно забирала на себя всю вычислительную мощность компьютерной системы и, в результате, она становилась недоступной для обслуживания пользователей. К примеру, в 1995 году посредством DoS-атаки на несколько часов был выведен из строя Web-сервер Yahoo!

[356] Более подробно о DoS-атаках можно прочитать в §5. Великое противостояние: зарождение и динамика, победы и поражения, успехи и просчёты // Том 1 настоящей книги.

Идентификационная карточка вредоносной компьютерной программы	
Имя	NightFall
Другие названия	NightFall.4480
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	январь 1995 года
Страна происхождения	Германия
Длина	4480 байт

Довольно сложным был обнаруженный в самом начале 1995 года в «диком виде» вирус «NightFall»[357], который получил наиболее широкое распространение в странах Западной Европы и, в короткий срок, обзавёлся сравнительно многочисленным семейством[358].

«NightFall» и его штаммы представляли собой резидентные полиморфные вирусы, использовавшие к тому же «стелс» технологию, усовершенствованные методы и приёмы, направленные против антивирусных программ.

Проникнув в компьютерную систему пользователя вместе с инфицированными сообщениями электронной почты через Интернет, посредством заражённых флоппи-дисков или CD-ROM, этот вирус устанавливал себя резидентно в оперативную память компьютера, перехватывал прерывание INT 21h и записывался в конец файлов с расширениями «*.com» и «*.exe» при обращении к ним. Так как «NightFall» использовал «стелс» технологию, он, оставаясь резидентно в оперативной памяти на протяжении всего сеанса пользователя, постоянно «перепрятывался», модифицируя с этой целью раз-

[357] «NightFall» (англ.) – «Наступление тьмы».

[358] Известны штаммы «NightFall.4518», «NightFall.4519», «NightFall.5765». Первые два вируса по своим характеристикам и проявлениям практически идентичны «главе семьи», чего не скажешь о «NightFall.5765», который иногда запускает содержащий строки «C:\NCDTREE\NAVINOC.DAT; MIMECHSYSIMFCO; -A-VICTORY-THAT-WON'T-LAST-» компаньон-вирус «NightFall.Companion» (другое имя – «Won't_Last.527»). Компаньон-составляющая этого вируса заключается в том, что она переименовывает файлы на инфицированном компьютере, а затем порождает собственные копии, которым присваивает изначальные имена переименованных ранее файлов. В результате, когда пользователь пытался открыть оригинальный файл, в действительности запускалась копия вируса.

мер, даты, атрибуты и т. п. инфицированных им загрузочных секторов или файлов. Кроме того, наличие полиморфной составляющей позволяло этому вирусу затруднять своё обнаружение при помощи перекодировки своего программного кода с использованием различных алгоритмов шифрования (ключей, операций) после каждого успешного заражения файла или программы.

Про вирус «NightFall» можно было бы сказать, что его поведение в заражённом компьютере характеризуется как достаточно скрытое. Однако иногда он явно обнаруживает своё присутствие недвусмысленным визуальным эффектом. Дело в том, что этот вирус (равно как и его штаммы) выводит на экран монитора следующее сообщение: «Invisible and silent – circling overland: \\\ N 8 F A L L///Rearranged by Neurobasher – Germany -MY-WILL-TO-DESTROY-IS-YOUR-CHANCE-FOR-IMPROVEMENTS-» («Невидимый и бесшумный – кружащий над землёй: \\\ N 8 F A L L///Перекодирован Нервоубийцей – Германия -МОЁ-СТРЕМЛЕНИЕ-К-РАЗРУШЕНИЮ-ВАШ-ШАНС-ДЛЯ-УЛУЧШЕНИЙ-»). Таким образом, латентно распространяясь при помощи копирования своего программного кода в инфицируемые файлы или программы и попутно «обманывая» установленное антивирусное программное обеспечение, «NightFall» мог бы вызвать очень широкую эпидемию по всему миру, однако указанный визуальный эффект помешал этому, так как прямо высказанная угроза действовала даже на неискушённого пользователя, как красный свет семафора, сигнализируя о том, что в его компьютерной системе не всё в порядке.

Вскоре было зарегистрировано появление весьма необычного компьютерного «вируса-гермафродита»[359] «RMNS», который остался в истории вирусописания благодаря заложенному в него автором необычному механизму инфицирования и размножения.

[359] Hermaphrodite – гермафродит, двуполый организм.

Идентификационная карточка вредоносной компьютерной программы	
Имя	RMNS
Другие названия	RMNS.MW
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	февраль 1995 года
Страна происхождения	Соединённые Штаты Америки
Длина	651 байт

Итак, двуполый «RMNS» не имел деструктивных функций и был резидентным, полиморфным компьютерным вирусом, который отслеживал и перехватывал прерывание INT 21h, а потом записывался в конец исполняемых файлов с расширением «*.com». Пока всё достаточно стандартно, но … Вирус обладал способностью делиться на две части: «Man»[360] и «Woman»[361]. Алгоритм инфицирования делился между этими частями, которые резидентно устанавливали себя в оперативную память компьютера. Затем часть «Man» перехватывала запуск файлов и вызывала часть «Woman», которая и заражала файл либо кодом «Man», либо кодом «Woman» в зависимости от текущего значения системного времени. Интересно, что при этом один и тот же файл при его повторном запуске не заражался обеими частями сразу. Таким образом, вирус «RMNS» размножался только в том случае, если в памяти присутствовали обе его части. В коде вируса содержались строки: «RMNS.MW.Man.297»: R.M.N.S Test virus R.M.N.S MW Man» и «RMNS.MW.Woman.353»: R.M.N.S Test virus R.M.N.S MW Woman».

К лету появились штаммы «RMNS», например, «RMNS.736» и «RMNS.184» (другое название: «Silly-C»), которые, по большому счёту, отличались от родоначальника только длиной и продолжали эксплуатировать идею «двуполости», не привнося в историю вирусописания ничего принципиально нового.

Всё течёт и изменяется… На смену «RMNS» пришли новые вирусы, среди которых можно отметить компьютерный вирус, отнесённый к редкой

[360] «Man» (англ.) – «Мужчина».

[361] Woman (англ.) – «Женщина».

«породе» так называемых BAT-вирусов и получивший красноречивое имя «Winstart», которое было дано ему как раз за то, что среда его «обитания» ограничивалась только одним файлом – «winstart.bat».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Winstart
Другие названия	Winstart.297
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	март 1995 года
Страна происхождения	Соединённые Штаты Америки
Длина	297 байт

По причине редкости вирусов такого типа рассмотрим его «деятельность» несколько подробнее. BAT-файл «winstart.bat» содержал четыре строки текста – @ECHO OFF (запрет вывода на экран), :s%r# (метка, в BAT-файле не выполнялась), COPY %0.BAT C:\Q.COM>NUL (копирование BAT-файла в C:\Q.COM), C:\Q (запуск C:\Q.COM) и одну строку данных: (код в двоичной системе исчисления). При запуске BAT-файла текст вируса выполнялся как последовательность перечисленных команд операционной системы MS-DOS. Шедшая далее строчка двоичного кода начиналась с метки «конец файла» – байт 1Ah. Встретив этот байт MS-DOS «решала», что файл закончился, и строчка данных не вызывала никаких побочных эффектов при выполнении BAT-файла.

Полученный в результате файл Q.COM являлся полной копией BAT-файла, и, когда управление передавалось на Q.COM, строчки BAT-файла начинали выполняться как инструкции языка программирования Ассемблер. Выглядело это примерно следующим образом. Сначала шли «пустышки»:

```
INC     AX;         '@'
INC     BP;         'E'
INC     BX;         'C'
DEC     AX;         'H'
DEC     DI;         'O'
AND     [BX+SI],    ' '
        AH;
```

Затем выполнялся код, лежащий во второй строке BAT-файла (там, где метка):

```
JNC         Install;        's%'
JC          Install;        'r#'
```

В итоге, именно эти команды передавали управление на двоичный код вируса «Winstart», который и заражал память. Заражение памяти происходило весьма необычным способом – вирус записывал себя в HMA[362]. Используя функцию INT 2Fh AX=4A02h, вирус выделял себе 173 байта (при общей длине в 297 байт), копировал в них свой код и перехватывал INT 2Fh. Адрес INT 2Fh брался напрямую из MS-DOS с использованием одной хитрости[363] (этот приём хорошо работал в наиболее популярных версиях MS-DOS – 6.0 и выше). По тому же адресу вирус записывал и указатель на свой обработчик INT 2Fh. При этом вирус внедрял свою процедуру обработки INT 2Fh в самую сердцевину операционной системы MS-DOS. Затем он переименовывал C:\Q.COM в C:\winstart.bat и уничтожал C:\Q.COM[364], помечал C:\winstart.bat атрибутом «Read only»[365] и возвращал управление операционной системе.

В результате всей вышеописанной кипучей деятельности складывалась следующая картина: в HMA резидентно установлен вирус «Winstart», который перехватывает INT 2Fh, а на «жёстком» диске C: располагается файл «winstart.bat». При запуске каждой новой копии командного процессора (файл command.com)[366] вызывается INT 2Fh с AX=AE00h (Internal Installation Check), а вирус отслеживает и ловит этот вызов, создавая на текущем диске

---

[362] High Memory Area – HMA (англ., проф.) – верхняя область памяти, то есть первые 64 Кб расширенной памяти персонального компьютера с операционной системой MS-DOS.

[363] Настоящее описание предназначено для более глубокого понимания читателем механизма инфицирования памяти вирусом «Winstart» и не претендует на роль подробной инструкции по написанию ему подобных вредоносных компьютерных программ.

[364] Это делалось ввиду того, что если файл «winstart.bat» уже физически присутствовал, то команда MS-DOS «Rename» становилась неработоспособной, и файл Q.COM нельзя было удалить при попытке переименования.

[365] «Read only» (англ.) – «Только для чтения».

[366] Например, при запуске программ из-под графической оболочки Norton Commander.

новый файл «winstart.bat». Однако делает он это только в случае одновременного выполнения двух следующих условий.

Условие 1	Условие 2
Текущий диск A: или B:	Текущий диск на 50 или более процентов заполнен какими-либо файлами[367]

Если указанные условия соблюдены, вирус создаёт на текущем диске (A: или B:) файл «winstart.bat» куда и записывает свою копию из C:\winstart.bat.

В мае филиппинские вирусописатели «подарили» компьютерному сообществу загрузочный резидентный вирус «Sampo», который не представлял собой особенного откровения, но в очередной раз подтвердил опасения вирусологов в том, что по всему миру сложились и продолжают формироваться устойчивые «команды» вирусописателей, представляющих собой различные слои общества. Такой вывод напрашивался, в частности, по прочтении текста, который «Sampo» выдавал на экран монитора тридцатого ноября каждого года: «SAMPO. Project X. Copyright (c) 1991 by the SAMPO X-Team. All rights reserved. University of the East Manila» («SAMPO. Проект X. Авторское право (c) 1991 SAMPO Бригада-X. Все права защищены. Университет Восточной Манилы»). Существование на протяжении нескольких лет этого и подобных «клубов по интересам» опасно уже в силу того, что, попадая в подобную компанию на первом курсе университета и постоянно «шлифуя своё мастерство» среди себе подобных, начинающий вирусописатель-любитель, зачастую, сам того не замечая, к окончанию учебного заведения пополняет ряды профессиональных вирусописателей.

[367] Видимо, по задумке автора вируса, «Winstart» спрятанный среди множества других файлов должен быть не так заметен пользователю во время их просмотра по команде «DIR».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Sampo
Другие названия	Sanpo, Turbo, Willop, 69
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	май 1995 года
Страна происхождения	Филиппины
Длина	297 байт

Итак, «Sampo». Этот вирус заражал только те компьютерные системы, в которых использовался уже инфицированный им флоппи-диск, поражая как загрузочный сектор флоппи-дисков, так и Master Boot Record (MBR) «жёстких» дисков. Установив себя резидентно в оперативной памяти компьютера «Sampo» перехватывал прерывания: INT 13h (во избежание обнаружения некоторыми антивирусными программами), INT 09h (для перезагрузки компьютера – после того, как он был инфицирован – отслеживает нажатие на клавиатуре сочетание клавиш «Alt-Ctrl-Del», эмулирует перезагрузку и остаётся резидентно в памяти), INT 08h (для проверки системных даты и времени, чтобы 30 ноября выводить на экран монитора приведённое выше сообщение). После заражения «жёсткого» диска компьютер лишается возможности загрузки с него и может стартовать систему только при помощи загрузочного флоппи-диска. Вместе с тем, «Sampo» не относится к когорте по настоящему деструктивных вирусов. Он не разрушает и не перезаписывает «Disk Partition Table», поэтому можно получить доступ к хранящейся в ней информации.

В заключение рассказа о «Sampo» приведём следующую такую небезынтересную информацию. Дело в том, что этот вирус был наделён способностью к трюкачеству: он пытался перехитрить пользователя, предлагая ему снять с флоппи-диска защиту от записи, используя в этих целях имя вируса «Kampana». Если в дисковод вставлен защищённый от записи флоппи-диск, антивирусное программное обеспечение может вдруг обнаружить, что он якобы инфицирован вирусом «Kampana» и попросить пользователя снять защиту для проведения лечения. «Sampo» же ожидает от пользователя именно этого действия и, пока антивирусная программа разбирается с вирусом

«Kampana», заражает флоппи-диск своей копией. Более того, в некоторых случаях «Sampo» действительно заражает дискеты «сторонним» вирусом – «Telefonica.3700».

В начале лета 1995 года появился в «диком виде» и быстро получил широкое распространение резидентный, полиморфный и использующий «стелс» и «линк» технологии компьютерный вирус «ByWay» – сообщения о заражённых им компьютерах поступали практически со всего мира.

Идентификационная карточка вредоносной компьютерной программы	
Имя	ByWay
Другие названия	Byway, Byway.A, Dir2.byway, By_Wai, Dir-II.Byway, DIR-Byway, DirII.TheHndV, TheHnd
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	июнь 1995 года
Страна происхождения	Венесуэла
Длина	2048 байт

Вирус «Byway» не использовал какие-либо особенные пути и методы распространения и проникал в компьютерную систему вместе с инфицированными приложениями к сообщениям электронной почты, во время загрузки информации или программ через Интернет, в случае использования заражённых им флоппи-дисков, CD-ROM и т. п. Вместе с тем, данный вирус использовал и передовые на то время технологии и приёмы из применявшихся авторами вредоносных компьютерных программ.

Во время загрузки системы «Byway» резидентно устанавливался в оперативной памяти компьютера и перехватывал функции, принадлежащие операционной системе. Поэтому каждый раз, когда операционная система или прикладная программа пытались получить доступ к этим функциям, вирус активизировался и заражал всё новые и новые файлы.

После того как «Byway» установился резидентно в оперативную память, он «прятался» в инфицированных им загрузочных секторах и файлах постоянно производя их модификацию, которая включала в себя: изменение размера и дат, смену атрибутов и пр.

«Byway» видоизменял связи, которые указывают операционной системе на то, где и как хранятся файлы, то есть перенаправлял их на вирус взамен оригинальных файлов. Таким образом, вместо того, чтобы вставлять свой программный код в инфицированный файл, этот вирус переадресовывал начальный кластер инфицируемого файла на заражённый кластер. Когда пользователь пытался открыть файл, в действительности запускался вирус, и нормальная работа с оригинальными файлами становилась невозможной.

После каждого инфицирования «Byway» зашифровывал себя заново, применяя при этом различные алгоритмы криптографии, ключи и операции. В итоге, вирус постоянно менял свои характеристики, что затрудняло его обнаружение при помощи антивирусного программного обеспечения.

Вирус «Byway» инфицировал исполняемые файлы с расширениями «*.com» и «*.exe» и обладал огромной скоростью распространения. Он мог заразить все найденные им на «жёстком» диске исполняемые файлы в считанные секунды. Если системное время и день месяца отвечали двум заранее заданным автором вируса условиям, «Byway» выводил на экран монитора текстовое сообщение «TRABAJEMOS TODOS POR VENEZUELA!!!» и каждые три часа (в 3:00, 6:00, 9:00, 12:00, 15:00, 18:00 и 21:00 час) проигрывал через системный динамик гимн Венесуэлы.

Более всего от эпидемии вируса «Byway» пострадали пользователи из стран Центральной Америки, а также Мексики и родины его автора – Венесуэлы, где и находился её эпицентр.

Хронологически ненамного отстал от написавшего «Byway» вирусописателя и автор получившего имя «DieHard2» опасного зашифрованного резидентного, использующего «стелс» технологию компьютерного вируса, который также как и его коллега облетел практически весь мир.

Идентификационная карточка вредоносной компьютерной программы	
Имя	DieHard2
Другие названия	DieHard2.4000
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	июль 1995 года
Страна происхождения	Соединённые Штаты Америки
Длина	4000 байт

Этот вирус перехватывал прерывания INT 10h, 21h и записывался в конец исполняемых файлов с расширениями «*.com» и «*.exe» при обращении к ним. Причём, находящаяся резидентно в оперативной памяти компьютера копия «DieHard2» была практически целиком зашифрована. Исключение составлял лишь программный код перехватчика прерываний.

Краткосрочность вызванной этим вирусом эпидемии во многом объясняется тем, что он проявлял себя сразу несколькими способами и по этой причине был слишком заметен для пользователей заражённых систем, которые начинали предпринимать меры по его удалению.

Например, по вторникам, попадавшим на 3, 11, 15 или 28 число месяца, при вызове функции «Write» операционной системы MS-DOS «DieHard2» выводил на экран монитора и в порт «COM1» строку: «SW Error». В зависимости от своего поколения вирус мог большими фиолетовыми буквами в графическом режиме отобразить сочетание: «SW». Он также содержал в своём теле текстовую строку «SW DIE HARD 2» и записывал в начало файлов с расширениями «*.asm» и «*.pas» короткие фрагменты текста[368].

Август 1995 стал одним из знаковых моментов во всемирной истории вирусописания, так как в этом месяце появились вирусы, рассчитанные на инфицирование платформы определённого программного продукта.

Компьютерное сообщество было заинтриговано и увлечено выходом новой операционной системы компании Microsoft – Windows 95, и на фоне

[368] Следует отметить, что при обращении к этим файлам «DieHard2» реализовал «стелс» технологию, и если вирус находится в оперативной памяти компьютера, эти строки не были видны.

этого эпохального события поначалу практически незамеченным прошло сообщение о появлении компьютерного вируса, использующего принципиально новые методы инфицирования и заражающего документы текстового процессора MS Word. Такая вялая реакция была вызвана также и тем обстоятельством, что это был уже не первый вирус, заражающий документы MS Word, и антивирусные фирмы к тому моменту имели на руках первый опытный образец вируса, который переписывал себя из документа в документ. В общем, так или иначе, но никто не обратил серьёзного внимания на эти, как казалось, не вполне удачные эксперименты вирусописателей, более того, профессиональное антивирусное сообщество указывало на то, что концепция макро вирусов не нова, а специалисты-вирусологи отмечали более чем простую реализацию сигнатур (подписей) макро вирусов.

В результате большинство фирм-разработчиков антивирусных программных средств оказалось совершенно дезориентированным и не готовым как к появлению компьютерного вируса нацеленного на инфицирование платформы определённого программного продукта, так и к последующему развитию событий – всемирной эпидемии или, иными словами, пандемии. И лишь со временем, осознав грозящую опасность, они начали спешно действовать, но это, особенно поначалу, были лишь полумеры. Например, несколько фирм практически одновременно выпустили документы-антивирусы, действовавшие примерно по тем же принципам, что и сам вирус, но не размножавшие, а уничтожавшие его. Постепенно фирмы-разработчики антивирусного программного обеспечения всё же закончили обновление своих баз данных и внесли необходимые изменения в основной программный код своих продуктов.

Полную неподготовленность антивирусного сообщества к появлению подобных вирусов хорошо иллюстрирует следующий пример. Когда в июле уже следующего, 1996 года специалисты «Virus Bulletin» опубликовали полный отчёт о проведённом тестировании антивирусного программного обеспечения, в нём констатировалось, что восемь из двадцати четырёх программ-

сканеров (использовавшихся в режиме «по умолчанию») не выдержали испытаний. Интересно также, что одна треть из числа проверяемых антивирусных программ пропустила и множество других компьютерных вирусов, известных на тот момент во всём мире.

Но вернёмся к самому виновнику вселенского переполоха. В течение месяца вирус «покорил» весь земной шар и продолжал победное продвижение по планете. Он заразил компьютеры миллионов пользователей текстового процессора MS Word и вышел на первые места в различных рейтингах, в том числе, по количеству публикаций в специализированных компьютерных изданиях и других средствах массовой информации. Итак, появившись, предположительно, в одном из подразделений фирмы Microsoft, вирус в мгновение ока завладел миллионами компьютеров, что и неудивительно. Ведь уже в то время обмен текстовыми документами в формате MS Word стал де-факто одним из стандартов, а для того, чтобы заразиться вирусом, достаточно было открыть инфицированный документ, и все остальные документы, редактируемые при помощи поражённого этим вирусом текстового процессора MS Word, также оказывались заражёнными. В результате, получив по Интернет такой файл и прочитав его, пользователь, сам того не зная, оказывался «разносчиком заразы», и вся переписка также оказывалась инфицированной! Таким образом, заражение через файлы MS Word, помноженное на скорость распространения информации в Интернет, стало одной из самых серьёзных проблем за всю историю существования вредоносных компьютерных программ.

Первой обнаружила, а затем исследовала этот новый тип компьютерного вируса известный компьютерный вирусолог Сара Гордон из Command Software Systems. Её коллега, Джимми Куо, на следующий же день предложил имя для этого вируса и с тех пор всему миру он известен под названием

«Concept»[369]. Он представлял собой макро вирус, который был написан на Word Basic (язык программирования, похожий на Visual Basic for Applications), который встроен в среду текстового процессора MS Word. Если говорить ещё более конкретно, вирус «Concept» был написан на основе английской версии WordBasic. По этой причине он не запускался в среде MS Word, если WordBasic был реализован на каком-либо другом языке. Вирусы под DOS запускались в среде DOS, Mac вирусы запускались в среде Mac, а вирус «Concept» запускался в среде MS Word. Таким образом, данный компьютерный вирус представлял собой межплатформенную вредоносную компьютерную программу (то есть вирус, совместимый сразу с несколькими операционными средами): он запускался на тех же операционных системах, на которых запускался и MS Word (Windows 95, Windows NT, Macintosh и т. п.).

[369] «Concept» (англ.) – «Концепция». Интересно, что компания Microsoft дала этому вирусу имя «Prank Macro» – «Макро шалость».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Concept
Другие названия	Concept.A, WM/Concept, WM.Concept, Microsoft Word Prank Macro, Prank Macro, WinWord.Concept, WordMacro.Concept, WW6 Macro, WW6, Word Macro 9508
Тип	компьютерный вирус
Инфицируемые платформы	Windows 95/98/ME/NT /2000/XP/2003, Macintosh, OS/2, MS-DOS
Впервые обнаружен	август 1995 года
Страна происхождения	Соединённые Штаты Америки
Длина	9508 байт

Итак, как мы уже говорили, буквально за месяц вирус «облетел» весь земной шар, заполонил компьютеры пользователей MS Word и прочно занял первое место в исследованиях, проводимых различными изданиями. А произошло это, во многом, благодаря тому, что компания Microsoft по недосмотру разослала тысячам OEM[370] компаний макро вирус, получивший впоследствии имя «Concept» на CD-ROM под названием «Microsoft Windows 95 Software Compatibility Test»[371]. В начале сентября произошёл очередной казус: один из крупнейших мировых производителей компьютеров Digital Equipment Corporation (DEC) распространил среди делегатов конференции DECUS, проходившей в Дублине, флоппи-диски, содержавшие этот макро вирус, но этот инцидент был быстро обнаружен и локализован.

Таким образом «Concept» стал первым, обнаруженным в «диком виде» компьютерным вирусом,написанным специально для среды текстового процессора MS Word и заражавшим файлы-документы с расширением «*.doc», а также глобальный шаблон, то есть файл «normal.dot». Этот вирус получил распространение на многочисленных компьютерных системах, где использовался MS Word, и были установлены операционные системы MS-DOS, MS Windows, Macintosh и OS/2 различных версий. Программный код вируса

[370] Original Equipment Manufacture (OEM) (англ.) – изготовитель комплектного оборудования, в отличие от производителей комплектующих изделий.

[371] «Microsoft Windows 95 Software Compatibility Test» (англ.) – «Проверка на совместимость программного обеспечения Microsoft Windows 95».

«Concept» мог распространяться при простом открытии инфицированного документа MS Word даже в том случае, если он был передан из другой операционной системы, поскольку макрос MS Word сохранялся в качестве данных и автоматически распознавал любую текущую версию этой прикладной программы. Сам вредоносный код включал в себя пять макросов: «AAAZAO», «AAAZFS», «AutoOpen», «PayLoad», «FileSaveAs» и заражал файлы-документы при их сохранении командой «Save As» (этой команде соответствует последний из перечисленных макросов – «FileSaveAs») из меню «File». Изменённый макрос сохранялся вместе с файлом. Перед инфицированием вирус «Concept» определял наличие макросов «PayLoad» и «FileSaveAs» в глобальном шаблоне: если какой-либо из этих макросов обнаруживался, вирус прекращал процесс заражения компьютерной системы; если в результате поиска эти макросы не обнаруживались, вирус начинал процесс инфицирования компьютерной системы, копируя свои макросы в глобальный шаблон MS Word.

Все указанные макросы можно было увидеть из команды «Macro» ниспадающего меню «Tools» MS Word. В заражённом файле присутствовали строки: «See if we're already installed/iWW6Iinstance/AAAZFS/AAAZAO/That's enough to prove my point» («Проверьте, установлены ли мы /iWW6Iinstance/AAAZFS/AAAZAO/Этого вполне достаточно, чтобы занять свое место»). Добавим, что кроме приведённых, «Concept» вставлял в файлы и другие фрагменты текста, например, в заражённой им системе в файле «winword6.ini» присутствовала строка: «WW6I=1». Из визуальных эффектов, вызываемых вирусом «Concept», можно выделить то, что при первой активизации вируса, то есть первом просмотре пользователем заражённого файла, на экране монитора появлялось стандартное окно сообщений операционной системы MS Windows с цифрой «1» и кнопкой «OK» внутри него.

Так что же нам осталось в наследство от того времени?

Вирус «Concept» проявил себя как крайне распространённый и «упорный», встречаясь на компьютерных системах ещё много лет и вызывая, время

от времени, локальные эпидемии[372], но, к счастью, он не обладал деструктивными функциями и, следовательно, не наносил непоправимого ущерба пользователю. Его многочисленные штаммы (Concept.AA, Concept.AB, Concept.AC, Concept.AD, Concept.F, Concept.AJ, Concept.AI, Concept.AK, Concept.AL, Concept.AM, Concept.E, Concept.FR.B, Concept.S и т. д. и т. п.[373]) отличались от родоначальника длиной, количеством макросов, языковой версией MS Word в которой были дееспособны и, что особенно отрадно, тоже не были деструктивными.

Специалистам-вирусологам пришлось в спешном порядке корректировать специальную антивирусную литературу, так как на вопрос «Можно ли заразить компьютер при чтении файла?» она безапелляционно отвечала: «Однозначно – нет!» И далее приводились длинные доказательства этого утверждения.

Большой резонанс имело и появление первого компьютерного вируса «Green Stripe»[374] (другое название: «Macro.AmiPro.GreenStripe»), написанного примерно в тоже время специально для текстового редактора «AmiPro», практически не уступавшего тогда по популярности MS Word. Исходный программный код этого вируса оказался бесплатным «приложением» к изданию Марка Людвига «Underground Technology Review»[375]. Вирус «Green Stripe» состоял из четырёх макросов (функций): «Green_Stripe_Virus», «Infect_File», «SaveFile» и «SaveAsFile». Он активизировался при открытии заражённого документа текстового редактора «AmiPro», а затем искал в текущем каталоге и инфицировал все файлы с расширением «*.sam». При заражении для каждого файла с расширением «*.sam» «Green Stripe» создавал SMM-файл, в который командой «DosCopyFile» копировал свой программ-

---

[372] Этот вирус окончательно покинул лидирующие двадцать «диких» вирусов в перечне «WildList» Международной организации WildList лишь в июне 2000 года.

[373] Сейчас известно более 100 модификаций вируса «Concept».

[374] «Green Stripe» (англ.) – «Зелёная полоса».

[375] «Underground Technology Review» (англ.) – «Обзор нелегальных технологий».

ный код. Командой «AssignMacroToFile» вирус «Green Stripe» определял макрос «Green_Stripe_Virus», который затем вызывался в момент открытия файла. После этого вирус переопределял системные макросы «SaveFile» и «SaveAsFile», по команде «Save As» заражал сохраняемые файлы, а по команде «Save» заменял в файлах строку «its» на «it's».

До конца 1995 года было написано ещё несколько макро вирусов и в результате того, что новый тип вредоносных компьютерных программ потребовал срочного переосмысления самого понятия «компьютерный вирус», а также привлечения ресурсов для борьбы с ними, появление макро вирусов вдохнуло новую жизнь в область исследований и разработки антивирусного программного обеспечения.

В сентябре 1995 года журнал «PC Magazine» (английская редакция), принадлежащий британскому филиалу издательского дома Ziff-Davis, распространил среди своих подписчиков флоппи-диск, содержащий загрузочный резидентный вирус «Sampo» о котором мы достаточно подробно говорили выше. Этот факт был скоро обнаружен, редакция журнала принесла свои извинения и предложила читателям бесплатную антивирусную утилиту. Этот случай привлёк особое внимание вследствие того, что в номере журнала, к которому был приложен инфицированный флоппи-диск, были опубликованы результаты тестов антивирусных продуктов для Novell NetWare. Прошло всего три месяца и в середине декабря 1995 года произошёл очередной «несчастный» случай. Он заключался в том, что уже другой журнал того же издательского дома Ziff-Davis – «Computer Life» – разослал своим читателям флоппи-диск с рождественскими поздравлениями, который кроме самого поздравления содержал, видимо в качестве приятного рождественского сюрприза, загрузочный вирус «Parity_Boot.B». Из-за этих случаев блестящая до того репутация издательского дома Ziff-Davis в глазах его читателей несколько потускнела.

Борьба же с компьютерной преступностью не ослабевала в течение всего года. В Великобритании с участием специального подразделения Ново-

го Скотланд-Ярда по борьбе с компьютерными преступлениями наконец-то начался и напряжённо протекал один из самых громких в этой области судебных процессов – над Кристофером Пайлом, который выступал в роли подозреваемого в создании и распространении компьютерных вирусов. 16 января в суде г. Плимут 26-летнему безработному Пайлу, известному нам под псевдонимом «Black Baron», было предъявлено обвинение в написании вирусов «Pathogen» и «Queeg», а также полиморфик-генератора SMEG[376]. Процесс длился целых 10 месяцев и только 15 ноября завершился приговором суда, в соответствии с которым Пайл был признан виновным и был приговорён к полутора годам тюремного заключения.

§16. 1996 год – деструктивность, сложность и скорость распространения вредоносных кодов неуклонно растут. Они были первыми: вирусы под операционные системы Windows 95 и OS/2, «Zhengxi», межплатформенный «Laroux» для MS Excel. Первая эпидемия вируса для Windows 3.x

- Выпущена операционная система MS Windows 95 OSR2 (OEM Service Release), в которой были устранены многочисленные ошибки MS Windows 95, расширена поддержка периферийных устройств и, самое главное, внесены серьёзные изменения в способ расположения файлов на «жёстком» диске (файловую систему) – вместо устаревшей FAT16 пользователи OSR2 могли использовать файловую систему FAT32, позволяющую сэкономить место на диске.
- Выпущены операционные системы MS Windows NT Workstation 4.0 и MS Windows NT Server 4.0.
- Выпущена операционная система OS/2 Merlin 4.0.
- Выпущена версия 2.0 операционной системы Linux с поддержкой многопроцессорных конфигураций.
- Компания Be Incorporated закончила разработку операционной системы BeOS.
- Java становится стандартной платформой для приложений Интернет, благодаря усилиям компаний Sun и Oracle совместно с Netscape, IBM и Apple.
- Выпущен микропроцессор AMD K5.

---

[376] Более подробно о «произведениях» вирусописателя под псевдонимом «Black Baron» см. выше – 1993 год.

В январе 1996 года в области вирусописания произошло два достаточно заметных события. Первое из них – это появление в Словакии мутационного движка «Explosion's Mutation Machine»[377] от ставшей к тому времени «культовой» личности – вирусописателя по кличке «Vyvojar», автора знаменитого вируса «OneHalf»[378]. Практически одновременно с появлением нового мутационного движка, компьютерное сообщество было уведомлено и о появлении в «диком» виде первого компьютерного вируса, который был написан специально под 32-битную операционную систему Windows 95 и, впоследствии, получил имя «Boza».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Boza
Другие названия	Win95.Boza, Bizatch, Boza-Bizatch
Тип	компьютерный вирус
Инфицируемые платформы	Windows 95
Впервые обнаружен	январь 1996 года
Страна происхождения	Австралия
Длина	2680 байт

Этот вирус представлял собой типичный пример недоработанной вредоносной компьютерной программы, и его возможности по распространению немедленно были подвергнуты сомнению со стороны специалистов. Но, как уже бывало в прошлом (вспомните, например, вирус «Michelangelo»), он получил весьма широкое освещение в средствах массовой информации, а также вызвал грозные уведомления пользователям от фирм-разработчиков антивирусного программного обеспечения о его опасности. Кстати, «Boza» оказался не так прост, как казалось изначально и, не смотря на программистские ошибки, умудрился всего лишь через неделю после своего обнаружения в США и Западной Европе, появиться и на российских просторах[379].

---

[377] «Explosion's Mutation Machine» (англ.) – «Мутационная машина взрывного действия».

[378] Более подробно об этом компьютерном вирусе см. выше – 1994 год.

[379] Надо отдать должное фирмам-производителям антивирусного программного обеспечения, как за их быструю реакцию на появление нового класса компьютерных вирусов, так и

При загрузке операционной системы вирус «Boza» искал PE-файлы[380] (NewEXE), создавал в файле дополнительную секцию и записывал в неё свой программный код. Таким образом, он стал первым из числа известных вирусов, способных инфицировать PE-файлы Windows 95. При заражении компьютерной системы вирус использовал вызовы «GetDir», «SetDir», «FindFirst», «FindNext», «OpenFile», «Lseek», «Read», «Write» и «CloseFile», причём производил указанные вызовы напрямую в «kernel32» без использования каких-либо ссылок на «kernel32.dll», как это делают обычные программы под Windows 95. Для того чтобы найти нужный адрес в «kernel32», вирус проверял по двум адресам его программный код и, если по какому-либо из этих адресов находится программный код обработчика, он использовал этот адрес для вызова перечисленных выше функций. Если же этот код в «kernel32» отсутствовал, вирус возвращал управление программе-носителю.

Алгоритм работы вируса был достаточно прост. «Boza» запоминал имя текущего директория, искал в нём файлы с расширением «*.exe» и проверял их на наличие PE-сигнатуры. Затем увеличивал на единицу поле «NumberOfSections» в заголовке PE, добавлял ещё один заголовок секции с именем «.vlad» и записывал свой программный код в конец файла. Новый заголовок секции создавался так, чтобы программный код вируса получал управление при запуске инфицированного им файла. При запуске «Boza» искал и заражал не более трёх файлов. Если в текущем директории не оставалось незаражённых файлов с расширением «*.exe», он переходил на один директорий выше. Перед возвращением управления программе-носителю вирус «Boza» переходил в первоначальный директорий, имя которого он запоминал перед началом процедуры поиска файлов.

за то, что менее чем через неделю был создан эффективной антивирус, способный вполне успешно бороться с вирусом «Boza».

[380] PE (Portable Executable) (англ., проф.) – машинонезависимый исполняемый файл, то есть формат загружаемого кода, представляющий собой одиночный исполняемый файл с расширением типа «*.ocx», «*.dll» или «*.exe».

Данный вирус проверял системную дату и 31-ого числа каждого содержащего его месяца выводил на экран монитора стандартное окно сообщений Windows 95, в заголовке которого помещалась строка: «Bizatch by Quantum/VLAD», а в самом окне довольно пространный текст, содержащий, в частности, такой фрагмент: «The taste of fame just got tastier! VLAD Australia does it again with the world's first Win95 Virus. From the old school to the new…» («Вкус славы становится все слаще! Австралийская VLAD делает это снова – теперь это первый в мире вирус под Windows 95. От старой школы – новой…»). Отметим также, что в связи с наличием в коде вируса «Boza» чисто программистских ошибок, заражённые файлы иногда оказывались испорченными, и при их запуске операционная система Windows 95 выводила на экран монитора сообщение об ошибке.

Вирус «Boza» был обнаружен в России в самом конце января, а в начале февраля, судя по сообщениям в прессе того времени, он уже перестал быть редкостью в московском компьютерном сообществе. Причём, по данным фирм-производителей антивирусных средств, распространению вируса «Boza» в Москве активно способствовали местные вирусописатели. К счастью для пользователей «Boza» не был резидентным вирусом и не обладал деструктивными функциями.

Тем временем в Санкт-Петербурге началась эпидемия весьма сложного полиморфного вируса «Zhengxi»[381] написанного российским программистом из Санкт-Петербурга Денисом Петровым. Как отмечали тогда ведущие отечественные вирусологи: «…компьютерные вирусы семейства «Zhengxi» относятся к наиболее сложным из известных вредоносных компьютерным программ. Они используют несколько методов заражения файлов, сложный полиморфный механизм, двойную шифровку кода вируса и т. д. В этих вирусах реализованы также «свежие» идеи, позаимствованных и из других вирусов,

[381] Данное семейство вирусов представляют собой также штаммы – «Zhengxi.2370.B», «Zhengxi.7271», «Zhengxi.7307», «Zhengxi.7313».

например, поражение файлов с расширением «*.exe» в их середину напоминает вирус «Lucretia», заражение файлов с расширением «*.obj» – вирус «Shifter», инфицирование архивов – вирус «Dementia», а полиморфный механизм представляет собой усовершенствованный вариант движка SMEG».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Zhengxi
Другие названия	Zhengxi.A
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	февраль 1996 года
Страна происхождения	Россия
Длина	7168 байт

Этот действительно очень опасный полиморфный вирус применял «стелс» технологию, заражал файлы не только с расширениями «*.exe», но и «*.obj», а также «*.lib», дописывал дропперы[382] с расширением «*.com» в архивы, созданные с использованием наиболее популярных программ архивации данных (ZIP, ARJ, RAR) и содержал следующие текстовые строки: «Abnormal program termination. The Virus/DOS 0.54 Copyright (c) 1995 Zhengxi Ltd. Warning! This program for internal use only!» («Аварийное завершение программы. Вирус/DOS 0.54 Авторское право (c) 1995 Компания с ограниченной ответственностью Zhengxi. Внимание! Эта программа только для внутреннего использования!»).

При инфицировании оперативной памяти программный код вируса получал управление из различных точек в зависимости от заражённого объекта.

[382] Как мы уже говорили, так называемые «дропперы» вирусов можно отнести к «троянским» программам («троянским» коням). Они представляют собой заражённые файлы, программный код которых не определяется известными на тот момент версиями антивирусных программкак компьютерный вирус. Например, файл упаковывается «экзотическим» или мало известным архиватором, или шифруется с использованием какого-либо специального математического алгоритма, что не позволяет антивирусному программному средству идентифицировать и ликвидировать инфекцию. Таким образом, в результате использования «неполноценных троянцев» вирусописатели обычно достигают сразу две основные цели: скрытая установка «троянских» или других вредоносных компьютерных программ и защита от антивирусного программного обеспечения.

Если запускался инфицированный файл с расширением «*.exe» (так называемый метод заражения «appending») или дроппер с расширением «*.com», «Zhengxi» получал управление непосредственно при выполнении заражённого файла (команда «JMP_Virus» в начале файла с расширением «*.com» или CS:IP на вирус в заголовке файла с расширением «*.exe»). В файлах, заражённых другим методом – «inserting», вирус получал управление из своей программы-загрузчика. В файлах, скомпонованных с заражёнными файлами (с расширениями «*.obj» и «*.lib»), вирус получал управление при помощи располагавшейся в произвольном месте файла команды «Call». В любом из приведённых выше случаев управление передавалось полиморфному расшифровщику, который состоял из двух основных циклов. Первый цикл расшифровывал второй цикл и снимал первый уровень шифровки с программного кода «Zhengxi», второй цикл восстанавливал программный код вируса в оригинальном виде и передавал управление инсталлятору, который перехватывал прерывание INT 1, трассировал INT 21h и искал в кодах INT 21h некоторую заданную последовательность байтов[383]. В том случае, если таковая обнаруживалась, вирус сохранял её в своём теле и записывал вместо неё команду «Far Call» на адрес обработчика INT 25h («Absolute Disk Read»). Затем «Zhengxi» сохранял 5 байт обработчика INT 25h и записывал на их место команду «FAR JMP» на своё собственное тело. Таким образом, вирус использовал одну и ту же подпрограмму для перехвата прерываний INT 21h и INT 25h, а для того чтобы разделить вызовы различных прерываний, он анализировал адрес, откуда пришёл вызов. Если вызов поступал от обработчика прерывания INT 21h, «Zhengxi» передавал управление своему обработчику прерываний INT 21h, а в противном случае управление передавалось вирусному обработчику INT 25h.

[383] Такие байты присутствуют в кодах обработчика прерываний INT 21h MS-DOS версий 5.x и 6.x.

Кроме того, при заражении оперативной памяти «Zhengxi» проверял несколько условий и не инфицировал компьютерную систему, если выполнялось хотя бы одно из них:

компьютер работает под управлением операционной системы MS Windows;

загрузка производилась с флоппи-диска (дисковод A: или B:);

прерывания INT 8, 13h, 28h указывают на один сегмент;

день создания заражённого файла близок к текущей дате (два старших бита номера дня создания файла совпадают с двумя старшими битами текущего дня).

Интересно, что при выделении памяти под свою резидентную копию «Zhengxi» использовал вызовы MS-DOS («ChMem» и «AllocMem») и устанавливал себя в основную область оперативной памяти. Однако в дальнейшем он мог перемещаться и в другие адреса оперативной памяти, включая её верхнюю область.

Файлы с расширением «*.exe» «Zhengxi» инфицировал тремя различными методами. Два из них («appending» и «inserting») мы уже упоминали выше, когда рассматривали процесс заражения оперативной памяти, а также заражал содержимое самораспаковывающихся архивов ZIP, ARJ и RAR, например, созданные утилитой ZIP2EXE архивы. Сначала вирус проверял файл с расширением «*.exe» на наличие заархивированных данных и, если таковые им обнаруживались, в архив дописывался дроппер с расширением «*.com». Затем «Zhengxi» проверял длину файла, заражая только файлы длиной более 1024 байт, а также длину загружаемого модуля. Если длина загружаемого модуля была больше 32 Кб, вирус заражал его методом «inserting», в противном случае, методом «appending».

При инфицировании файла методом «appending» вирус считывал его заголовок, шифровал этот заголовок полиморфным методом и записывал в конец заражаемого файла. Затем полиморфным методом «Zhengxi» шифровал свой программный код, дописывал к концу файла и модифицировал заго-

ловок файла таким образом, чтобы CS:IP указывали на программный код вируса. Следует отметить, что при шифровке заголовка файла и тела вируса использовались различные полиморфные циклы. При запуске файла цикл расшифровки восстанавливал только код вируса, но не заголовок файла, который был зашифрован другим полиморфным циклом, и «Zhengxi» не содержал в своем теле этот второй цикл. Для последующей расшифровки заголовка вирус при заражении файла запоминал стартовые значения генератора случайных чисел (который определяет работу полиморфного механизма) и при восстановлении заголовка генерировал полиморфный код с теми же начальными значениями генератора случайных чисел. В итоге получался тот же код, который использовался при зашифровке заголовка файла, и для расшифровки заголовка вирус запускал именно этот код.

Если длина загружаемого модуля была более 32 Кб, вирус «Zhengxi» применял метод «inserting»: искал в модуле процедуры языка программирования C (или Pascal) и записывал в них свой загрузчик. В результате код вируса получал управление не непосредственно при запуске заражённого файла, а при вызове этой процедуры. Причем такая подпрограмма могла быть крайне редко выполняемой (например, вывод сообщения о специфичной ошибке) и вирус долгие годы существовал латентно внутри файла и активизировался лишь в случае соблюдения неких редко возникающих условий. При инфицировании методом «inserting» «Zhengxi» считывал следовавшие сразу же после заголовка файла с расширением «*.exe» первые 6 Кб загружаемого модуля и искал стандартные заголовки процедур языков программирования C или Pascal, которые, в большинстве случаев, начинаются с команд: «PUSH BP»; «MOV BP, SP». Находя такие команды, вирус просматривал следующие 54h байта на наличие команд «RET» и «CALL FAR» и, если одна из них находилась, «Zhengxi» прекращал процесс инфицирования файла. Он делал это не из человеколюбия, а для того, чтобы не испортить код найденной процедуры или не исказить настраиваемый адрес, потому что затем вирус считывал 54h байта этой процедуры, записывал в неё код своего загруз-

чика, шифровал своё тело и записывал его в конец. После этого «Zhengxi» сохранял в конце файла код процедуры и вторую часть кода своего загрузчика, – шифруя их при помощи команды «SUB», и дописывал блок случайных данных. Если код загрузчика получал управление, вирус определял имя файла-носителя, считывал из него и расшифровывал своё продолжение, а затем передавал на него управление. Продолжение загрузчика восстанавливало код процедуры языка программирования C (или Pascal), выделяло из обычной или верхней областей оперативной памяти отдельный блок, считывало в него программный код вируса и передавало на него управление.

В случае инфицирования архивов «Zhengxi» создавал в памяти заражённый файл с расширением «*.com» и записывал его в архив. Такие заражённые файлы начинались с команды перехода – «JMP» – на расшифровщик вируса, затем шли случайные данные и зашифрованный программный код тела вируса. Причём имя для этих файлов выбиралось случайным образом[384]. При дописывании файлов в архив вирус не использовал никаких внешних утилит, а модифицировал служебные поля самостоятельно. Он также не запаковывал файл, а записывал его «как есть» методом «stored» и не заражал архивы повторно.

При инфицировании объектных модулей файлов с расширениями «*.obj» и «*.lib» «Zhengxi» проверял записи модуля, искал записи с кодом или данными («LEDATA»), по аналогии с заражением файлов с расширением «*.exe» по методу «inserting» просматривал их на наличие процедур языка программирования C (или Pascal), а затем замещал заголовок C (или Pascal) командой «CALL NEAR» и дописывал в «LEDATA» свой зашифрованный программный код. Как и в случае с инфицированием файлов с расширением «*.exe» методом «inserting», «Zhengxi» мог долгие годы существовать ла-

[384] Например, «haif.com», «ucm.com», «doo.com», «vlg.com» – реальные имена, полученные отечественными вирусологами в ходе проведения исследований вируса «Zhengxi» и его штаммов.

тентно, прежде чем активизироваться для заражения файлов с расширениями «*.obj» и «*.lib».

Кроме всего перечисленного выше, «Zhengxi» реализовал «стелс» технологию на уровне прерывания INT 25h: при чтении сектора с заголовком инфицированного файла он подставлял оригинальный заголовок, а при просмотре секторов директория указывал длины файлов, которые были до их заражения. Тем не менее, подчеркнём, что хотя в подавляющем большинстве случаев «Zhengxi» оставался невидимым для пользователя, возможности «стелс» технологии были реализованы не достаточно полно и при некоторых условиях вирус терял свойства «невидимки».

В заключение добавим, что наиболее очевидным и опасным проявлением деструктивной деятельности вируса «Zhengxi» можно признать тот факт, что при заражении файлов в архивах, созданных при помощи программы архивирования ZIP, он проверял поля заголовков и, если обнаруживалась запись «stored», а файл был создан или модифицирован в 1996 году или позже, вирус последовательно (от C: до Z:) «просматривал» абсолютно все директории на всех доступных логических разделах «жёсткого» диска компьютера и стирал все обнаруженные им файлы, а затем и сами директории.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Tentacle
Другие названия	Win.Tentacle.1958, Win.Tentacle
Тип	компьютерный вирус
Инфицируемые платформы	Windows 3.x
Впервые обнаружен	март 1996 года
Страна происхождения	Франция
Длина	1958 байт

В марте 1996 года была зарегистрирована первая эпидемия компьютерного вируса для операционной системы Windows 3.x (Windows 3.11 и более ранние версии), который появился во Франции и заразил там компьютерные сети госпиталя и других учреждений. Вызвавший эту эпидемию нерезидентный и не обладающий деструктивными функциями

вирус впоследствии стал широко известен под именем «Tentacle»[385], благодаря тому, что он был одним из первых компьютерных вирусов, специально разработанных под 16-битные версии операционной системы MS Windows и успешно распространялся в «диком» виде.

При запуске «Tentacle» искал исполняемые (NewEXE) файлы в текущем директории, а затем и в директории C:\WINDOWS, записывая свой программный код в конец каждого из обнаруженных файлов этого типа. Таким образом, вирус постепенно инфицировал все NE файлы в указанных директориях. В процессе заражения он создавал и использовал временный файл C:\TENTACLE.$$$, куда последовательно – блок за блоком, копировал данные инфицируемого файла, корректировал эти блоки, а затем дописывал свой программный код в конец файла и переносил полученный вариант в заражаемый файл. Начиная с полуночи и до четверти первого ночи (то есть с 0:00 до 0:15) «Tentacle» инициировал проверку только что зараженного файла на наличие ресурсов, содержащих иконки. Если такой ресурс обнаруживался, вирус замещал иконку на другую, код которой содержался в его теле. Кроме того, начиная примерно с 1950 байта от конца заражённого файла, «Tentacle» вставлял текстовую строку, которую, впрочем, никогда не выводил на экран монитора: C:\TENTACLE.$$$ C:\WINDOWS*.

Ещё одним «первопроходцем» в своей узкопрофессиональной области деятельности следует признать обнаруженный в июне 1996 года нерезидентный и достаточно безобидный компьютерный вирус «OS2.AEP», который вошёл в историю вирусописания вследствие того, что стал первой вредоносной компьютерной программой для операционной системы OS/2, вполне корректно заражающей её файлы с расширением «*.exe».

[385] «Tentacle» (англ.) – «Щупальце».

Идентификационная карточка вредоносной компьютерной программы	
Имя	OS2.AEP
Другие названия	OS2.AEP.A
Тип	компьютерный вирус
Инфицируемые платформы	OS/2
Впервые обнаружен	июнь 1995 года
Страна происхождения	Соединённые Штаты Америки
Длина	1024 байта

До этого вирусологи и пользователи OS/2 сталкивались исключительно с такими компьютерными вирусами, которые записывались вместо файла, уничтожая его или действуя методом «компаньон»[386]. Корректность же работы «OS2.AEP» проявлялась, например, в том, что он при инфицировании файлов операционной системы OS/2, записывал себя в них, а затем проводил корректировку точек входа их заголовков.

При активизации вирус искал файлы с расширениями «*.exe» и «*.dll», проверял наличие у них заголовка NE (маркёр OS/2) и записывался в середину файла. При заражении «OS2.AEP» брал номер сегмента кода, содержащего точку входа в файл, и сдвигал все остальные сегменты вниз, вставляя своё тело в образовавшуюся «брешь». Завершив эти операции, вирус корректировал NewEXE-заголовок заражённого файла, а также системные таблицы ссылок и внешних имён. В завершение своей деятельности «OS2.AEP» возвращал управление программе-носителю.

Отметим также, что при заражении «OS2.AEP» использовал вызовы операционной системы OS/2: «DosAllocSeg», «DosFreeSeg», «DosChgFilePtr», «DosClose», «DosFindFirst», «DosFindNext», «DosOpen», «DosRead», «DosWrite». В теле вируса содержались следующие текстовые строки: (C)

[386] Как мы уже говорили в первом томе настоящей книги, так называемые компаньон вирусы, представляют собой вирусы, которые не вносят изменения в файлы. Алгоритм этих вирусов действует так, что они создают свою копию для файлов с расширением «*.exe», то есть файлы-спутники, у которых тоже имя, но с расширением «.com»), например, для файла «point.exe» они создают файл «point.com». Этот вирус пристраивается к com-файлу не изменяя exe-файл. При запуске файла, операционная система первым выполняет com-файл, в котором вирус, а затем com-файл запускает exe-файл.

1995 American Eagle Publications Inc., All rights reserved. *.EXE *.DLL DOSCALLS. ((C) 1995 Публикации корпорации Американский орёл, Авторские права защищены. *.EXE *.DLL DOSCALLS.)

Точно также как и «Boza» другой компьютерный вирус, названный «Hare»[387], получил широкое освещение в средствах массовой информации. Уже первичные оценки «Hare» были полярными и разделили вирусологов на два больших «лагеря», которые можно условно назвать лагерем пессимистов и лагерем оптимистов. По словам, например, редактора Virus Bulletin Ина Волли, «выявить «Hare» необычайно трудно. К тому же он очень быстро распространяется, очевидно, по Интернет. Версии нового вируса, правда, пока неактивные, уже обнаружены в ряде стран, в том числе в США». Другие специалисты оценивали этот вирус как «ничем не примечательную программу, кишащую многочисленными ошибками». Так или иначе, но сообщения об обнаружении «Hare» в «диком» виде поступали в течение нескольких месяцев из различных стран мира от Канады до Южно-Африканской Республики и от стран Западной Европы до США.

[387] Hare (англ.) – Харе, в кришнаитском религиозном учении имя Господа, означающее «Уносящий все грехи Своего преданного».

Известны также штаммы этого вируса – «Hare.7750», «Hare.7786».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Hare
Другие названия	Hare.7610, Euthanasia, HDEuthanasia, HDEuthanasia.7610, Krsna
Тип	компьютерный вирус
Инфицируемые платформы	Windows 95
Впервые обнаружен	июль 1996 года
Страна происхождения	Новая Зеландия
Длина	7610 байт

Однако судите сами. Итак, «Hare» был задуман автором как очень опасный резидентный файловый загрузочный полиморфный и использующий технологию «стелс» вирус с целью широкого распространения посредством передачи и загрузки по Интернет. Но, с другой стороны, данный вирус действительно представлял собой вредоносную компьютерную программу, имеющую программистские ошибки, снижающие её «эффективность».

Все вирусы, относящиеся к семейству «Hare» записывались в конец файлов с расширениями «*.com» и «*.exe», а также в главную загрузочную запись (MBR) винчестера и загрузочного сектора флоппи-дисков. В файлах они трижды шифровались и, как в файлах, так и в заражённых секторах применяли полиморфизм. При запуске инфицированного файла вирус расшифровывал себя, заражал MBR, трассировал и перехватывал прерывание INT 21h, а затем возвращал управление программе-носителю. В компьютерных системах, функционирующих под управлением MS Windows 95, он перехватывал также прерывание INT 13h. Затем вирус записывался в файлы при их запуске, закрытии или при выходе в режим работы MS-DOS (AH=0,31h,4Ch). Интересно, что «Hare» при открытии уже инфицированных файлов с расширением «*.exe» лечил их и, кроме того, не заражал файлы, соответствующие следующим маскам: «tb*.*», «f-*.*», «iv*.*», «ch*.*» и «command*.*». Не заражал он также и те файлы, в имени которых содержалась буква «V». При загрузке с инфицированного флоппи-диска «Hare» записывался в MBR и возвращал управление первоначальному загрузочному коду, при этом вирус не оставлял в оперативной памяти компьютера свою резидентную копию. При заражении MBR вирус трассировал INT 13h или напрямую работал с портами

контроллера, затем записывал свое продолжение (15 секторов) в трек, находящийся за пределами объявленного размера «жёсткого» диска. Потом он «усердно» затирал Disk Partition Table, и в результате этого команда FDISK/MBR могла вызывать полную потерю данных на «жёстком» диске.

При загрузке из инфицированного MBR-сектора «Hare» восстанавливал Disk Partition Table для того, чтобы нормально загрузилась операционная система MS-DOS (в данный момент «стелс» технология на уровне прерывания INT 13h вирусом ещё не задействовалась), а затем уменьшал размер оперативной памяти (одно слово по адресу 0000:0413), копировал свой программный код в «вырезанный» участок оперативной памяти, перехватывал прерывание INT 1Ch и передавал управление первоначальному MBR-сектору. Перехватив INT 1Ch «Hare» переходил в режим ожидания загрузки MS-DOS, после чего восстанавливал размер оперативной памяти и перехватывал прерывания INT 13h, 21h и 28h. При первом же вызове прерывания INT 28h, для того чтобы обойти установленное антивирусное аппаратно-программное обеспечение, вирус вновь вносил изменения в оригинальную Disk Partition Table. При вызовах прерывания INT 13h вирус перехватывал обращение к флоппи-дискам и инфицировал их. Под свой основной программный код «Hare» форматировал дополнительный трек, а при обращениях к уже заражённым флоппи-дискам выполнял заложенный в него алгоритм по технологии «стелс».

Специалисты вирусологи отмечали также то, что при заражении MBR «Hare» перехватывал прерывание INT 16h и проделывал при этом «довольно странные манипуляции с клавиатурой»: заменял или самостоятельно записывал в буфер клавиатуры буквы «Y» и «N», как будто пытаясь самостоятельно ответить на запрос BIOS о записи в MBR «жёсткого» диска, – если такая функция поддерживалась данной версией BIOS. Подмечен был также и тот факт, что «Hare» весьма странным образом генерировал свой полиморфный

код[388]. При заражении «жёсткого» диска он заполнял его самый последний сектор случайными данными и никогда больше их не изменял, а потом, при загрузке с инфицированной MBR или запуске заражённого файла, считывал эти данные из последнего сектора. Интересно, что при повторном инфицировании компьютерной системы (например, после лечения антивирусными средствами) «Hare» обнаруживал эти данные в последнем секторе, но никак не изменял их. Эти данные использовались им как генератор случайных чисел при запуске своего полиморфного генератора: при заражении разных файлов или секторов на вход генератора поступали одни и те же псевдослучайные данные, и в результате он выдавал на выход один и тот же программный код, и все файлы и сектора, заражённые на одном и том же компьютере, содержали один и тот же полиморфный цикл расшифровки, и зашифрованы были одними и теми же ключами. Вирус увеличивал длину файла на случайное число (длина вируса плюс длина случайного расшифровщика). Естественно, что на одном и том же компьютере длина файлов увеличивалась на одно и то же значение. В итоге все файлы/сектора, инфицированные на конкретном компьютере, можно было определить обычным методом поиска по маске самого вируса. Некоторые специалисты комментировали это следующим образом: «Зачем все это проделывается – непонятно. Видимо, для того, чтобы ввести в заблуждение разработчиков антивирусных программ и спрятать файл или диск, который послужил причиной заражения компьютера». Кроме всего перечисленного добавим: старшие версии «Hare» при загрузке с инфицированного «жёсткого» диска с вероятностью 1/16 меняли случайные данные в его последнем секторе и генерировали другие полиморфные циклы при заражении файлов и флоппи-дисков.

Вирус «Hare», обладал деструктивными функциями. Например, при запуске инфицированного файла он искал строку «WIN=» в области «Environ-

[388] Специалисты-вирусологи отмечали, что «Hare» обладал уникальными способностями генерации очень большого набора разнообразных инструкций.

ment» и уничтожал файл \SYSTEM\IOSUBSYS\hsflop.pdr в каталоге операционной системы MS Windows. При заражении оперативной памяти он проверял системную дату и 22 августа и 22 сентября выводил на экран монитора следующее текстуальное сообщение: «HDEuthanasia[389] by Demon Emperor: Hare Krsna, hare, hare...»[390]; а затем приступал к уничтожению всех файлов, расположенных на всех без исключения «жёстких» дисках компьютера.

Возвращаясь к началу нашего обсуждения компьютерного вируса «Hare» предоставим читателю самому определиться с тем «лагерем», который ему ближе. От себя же скажем, что автор «Hare» потрудился на славу и явно стремился нанести пользователю как можно больший ущерб и не его «вина», если он допустил по незнанию, невнимательности или каким-то другим причинам программистские ошибки, которые, в итоге, не позволили его детищу развернуться во всю ширь задуманного.

---

[389] Euthanasia (англ.) – эвтаназия, намеренное умерщвление неизлечимо больного человека с целью облегчения его страданий. При добровольной эвтаназии больной сам принимает решение о том, чтобы ему помогли умереть. Это может достигаться с помощью активных мер (обычно путём назначения специальных лекарственных веществ) или путём пассивной эвтаназии – преднамеренного отказа от лечения. При принудительной эвтаназии общество или человек, воздействуя собственным авторитетом на другого человека, отдаёт ему приказание покончить с жизнью, например, младенца, который не может чётко выразить свои желания. Не существует ни одной страны, в которой принудительная эвтаназия была бы признана легально, однако во многих обществах одобряется добровольная эвтаназия. (Большой толковый медицинский словарь Oxford, том 2 (Н – Я). Oxford University Press, АСТ, Вече. – 1998).

[390] Штамм «Hare.7750»: ««HDEuthanasia-v2» by Demon Emperor: Hare Krsna, hare, hare...»; штамм «Hare.7786»: ««HDEuthanasia-v3» by Demon Emperor: Hare Krsna, hare, hare...»

Идентификационная карточка вредоносной компьютерной программы	
Имя	Laroux
Другие названия	ExcelMacro/Laroux, ExcelMacro.Laroux, Excel.Laroux, XM/Laroux.a, XM.Laroux
Тип	компьютерный вирус
Инфицируемые платформы	Windows 95/98/ME/NT /2000/XP/2003
Впервые обнаружен	июль 1996 года
Страна происхождения	Южно-Африканская Республика
Длина	2 макроса

Июль 1986 года вошёл в историю вирусописания тем, что двумя нефтедобывающими компаниями в ЮАР и на Аляске практически одновременно был «отловлен и дактилоскопирован» другой примечательный компьютерный вирус, изначально привлекший пристальное внимание всего международного антивирусного сообщества.

Им стал вирус, получивший название «Laroux»[391] и прославившийся тем, что он был первым компьютерным вирусом для MS Excel, успешно инфицирующим крупноформатные электронные таблицы данной программы. Примечательно, что компьютерный вирус «Laroux», как ранее вирус «Concept», – также представлявший собой «знаменательную веху» в истории вирусописания, был всесторонне исследован всё той же Сарой Гордон из Command Software Systems.

Как и у MS Word вирусов, принцип действия «Laroux» основывался на наличии в файлах так называемых макросов – программ на языке программирования Visual Basic, которые могут быть включены в электронные таблицы MS Excel так же, как и в документы MS Word. Таким образом, оказалось, что встроенный в MS Excel язык программирования позволяет создавать компьютерные вирусы. Например, в действительности активный код вируса «Laroux» состоит из двух макросов по имени «Auto_Open» и «Check_Files», которые хранятся в таблице по имени «laroux»[392], которой присвоен атрибут «hidden» – спрятанный. Когда инфицированный файл с электронной табли-

[391] «Laroux» (фр.) – «Лару».

[392] Отсюда и происходит название вируса.

цей впервые открывается компьютерной пользователя, макрос «Auto_Open» автоматически запускает MS Excel, который, в свою очередь, запускает макрос «Check_Files». Это происходит каждый раз, когда активируется электронная таблица. После этого макрос «Check_Files» копирует таблицу с программным кодом вируса в файл с электронной таблицей, который хранится под именем «personal.xls» в стартовом директории MS Excel (по умолчанию, это директорий \MSOffice\Excel\XLStart). Файл «personal.xls» является как бы «глобальным макросом электронной таблицы», и хранимый там макрос автоматически доступен для всех других таблиц MS Excel в системе. Поэтому, операция копирования этого макроса в «personal.xls» распространяет инфекцию на все другие электронные таблицы, открываемые или создаваемые в будущем на инфицированной системе.

Вирус «Laroux» не содержал преднамеренно включённых в его тело деструктивных функций и в процессе своей «жизнедеятельности» лишь размножался, причём оставался работоспособным только в компьютерных системах, которые функционировали под управлением операционных систем MS Windows, использующих MS Excel версий 5 и 7. В среде операционной системы Macintosh вирус «Laroux» не работал. Кроме того, он довольно медленно распространялся. Впрочем, приведём текст заметки «Продолжение бактериологической войны», которая была опубликована в средствах массовой информации и представляет собой квинтэссенцию суждений специалистов-вирусологов того времени о «Laroux»: ««Столетняя война» между авторами компьютерных вирусов и разработчиками антивирусных программ то стихает, то разгорается с новой силой. Сейчас конфликт обострился в связи с выходом на сцену, с одной стороны, новых опасных вирусов, а с другой, нескольких обновлённых программных продуктов, нацеленных на их поиск и ликвидацию. Вирус, который получил название ExcelMacro.Laroux, влился в появившееся год назад семейство макро-вирусов, став родоначальником новой ветви – он поражает электронные таблицы MS Excel. Laroux ведёт себя так же, как теперь уже общеизвестный вирус Word.Concept. Последний пере-

даётся с документами, созданными в MS Word. Laroux же «путешествует» вместе с электронными таблицами, которыми пользователи обмениваются по e-Mail или с помощью других средств. National Computer Security Association (Национальная ассоциация по компьютерной безопасности – NCSA) считает Laroux вирусом относительно безопасным, хотя и способным вызвать «аномалии в приложениях» некоторых систем. По всей видимости, распространяться Laroux будет медленнее, чем Word.Concept, ведь MS Excel используется не столь широко, как MS Word, а пользователи пересылают электронные таблицы гораздо реже, чем текстовые документы».

Этот прогноз оказался достаточно точен. Например, лишь через восемь месяцев, в апреле 1997 года, «Laroux» добрался до Москвы и стал причиной эпидемии во многих фирмах, учреждениях и организациях.

Родоначальник этого семейства породил многочисленное «потомство» в виде различных штаммов, которые ещё долгое время донимали пользователей, а очередная версия этого вируса под названием «X97M/Laroux.A» удостоилась чести попасть в основной список «The WildList» Международной организации WildList и продержалась там в числе двадцати наиболее распространённых в мире вирусов до августа 2000 года! Сам патриарх оказался ещё более «живучим» и окончательно покинул «славную» двадцатку только в октябре того же года.

Между тем, по данным IBM, уже к августу 1996 года каждый день «из-под пера» вирусописателей в среднем появлялось не менее шести новых вредоносных компьютерных программ. Согласитесь, цифра весьма впечатляющая, и ситуация могла бы перерасти в вообще неконтролируемую компьютерным сообществом, но, к счастью, большинство из написанных вредоносных кодов так и не попало в «свет» в «диком» виде. Однако, по словам президента NCSA Питера Типпета «на среднестатистический персональный компьютер заносилось примерно два неизвестных вируса в месяц». В этой и без того непростой ситуации два вирусописателя, скрывавшиеся под красно-

речивыми псевдонимами «Nightmare Joker»[393] и «Wild Worker»[394], почти одновременно выпускают конструкторы макро вирусов для немецкой и английской версий MS Word.

В августе был зарегистрирован в «диком» виде новый компьютерный макро вирус, который был весьма тщательно зашифрован, состоял из девяти макросов «AutoExec», «AutoOpen», «FileSaveAs», «FilePrint», «FilePrintDefault», «InsertPayload», «Payload», «DropSuriv», «FileExit» и содержал антивоенную патетику, за что и получил имя «Nuclear»[395].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Nuclear
Другие названия	Nuclear.a, Macro.Word.Nuclear, WM/Nuclear.A, Word Macro 9509
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT/2000/XP/2003
Впервые обнаружен	август 1996 года
Страна происхождения	Соединённые Штаты Америки
Длина	10556 байт

При заражении MS Word «Nuclear» специально не проверял, за исключением «AutoExec», наличие перечисленных выше имён макросов в компьютерной системе, но если макросы с такими именами уже существовали, он заменял их своими, причём оригинальные макросы уничтожались, а файлы-документы инфицировались в дальнейшем при их закрытии (использовался макрос «FileSaveAs»). Автором вируса «Nuclear» было задумано его проявление в

---

[393] «Nightmare Joker» (англ.) – «Кошмарный тип».

[394] «Wild Worker» (англ.) – «Нелегальный исполнитель».

[395] «Nuclear» (англ.) – «Ядерный». Известны штаммы этого вируса «Nuclear.b» и «Nuclear.c».

Штамм «Nuclear» вирус «Nuclear.b» не содержит DOS-вирус и меньше на два макроса (DropSuriv, FileExit). Процедура вставки текста в документ содержит ошибку и, в результате, в конец текста добавляется пустая страница и выводится сообщение об ошибке WordBasic.

Штамм «Nuclear» вирус «Nuclear.c» содержит пять макросов: Payload, AutoExec, AutoOpen, FileSaveAs, InsertPayload. Макрос Payload содержит закомментированные строчки, которые удаляют все файлы с диска C:.

файлах-документах тремя способами. Во-первых, он должен был запускать COM/EXE/NewEXE вирус; во-вторых, добавлять строки текста при печати документов и, в третьих, вносить изменения в системные файлы. Однако вирус содержал большое количество программистских ошибок, поэтому первое и третье из действий не выполнялись так, как было запланировано автором.

Итак, рассмотрим «работу» данного вируса в идеале. При запуске MS Word активизировался макрос «AutoExec», который, в свою очередь, организовывал вызов макроса «DropSuriv», ежедневно в период с 17:00 до 18:00 проверявшего показания системного времени и инфицировавшего систему COM/EXE/NewEXE-вирусом («Ph33r»). Причём в этих целях макрос «DropSuriv» использовал известную системную утилиту «debug.exe». Сначала он проверял наличие файла C:\DOS\debug.exe и, если таковой присутствовал в указанном директории, «Nuclear» создавал в директории C:\DOS временный файл «ph33r.scr». В этот файл записывался шестнадцатеричный дамп вируса и команды программы «debug» (создать файл, ввести шестнадцатеричный дамп, выполнить полученный код, выйти в операционную систему DOS). После этого вирус создавал временный файл «exec_ph.bat», куда записывал следующие строки:

```
@echo off
debug < ph33r.scr > nul
```

и выполнял этот командный BAT-файл.

В результате программа «debug» создавала в оперативной памяти копию «Nuclear» и выполняла её. Вирус перехватывал прерывание INT 21h и затем заражал выполняемые файлы. Так как запуск BAT-файла происходил в фоновом режиме, пользователь даже не подозревал, что его компьютерная система подверглась инфицированию, причем сразу двумя вирусами («Nucle-

ar» и «Ph33r»). После завершения работы BAT-файла макрос «DropSuriv» удалял из компьютерной системы файлы «ph33r.scr» и «exec_ph.bat»[396].

При печати документов MS Word, если значение секунд текущего системного времени больше 55, «Nuclear» в конец выводимого на печать текста добавлял следующие строки: «And finally I would like to say: STOP ALL FRENCH NUCLEAR TESTING IN THE PACIFIC!» («И в заключение я хотел бы сказать: ПРЕКРАТИТЕ ВСЕ ФРАНЦУЗСКИЕ ЯДЕРНЫЕ ИСПЫТАНИЯ В ТИХОМ ОКЕАНЕ!»).

Интересно, что строчки добавлялись в конец файла непосредственно перед печатью и пользователь, обычно, не обнаруживал их на экране монитора, так как для отображения подавляющего большинства документов MS Word требовалось больше одной страницы экрана монитора.

И, наконец, пятого апреля при запуске инфицированного MS Word или открытии заражённого документа «Nuclear» портил системный файл IO.SYS снимая с него все атрибуты и обнуляя его длину, а также системный файл MSDOS.SYS, опять таки снимая с него все атрибуты, но почему-то не обнуляя его длину по аналогии с IO.SYS. В завершение «трудов праведных» «Nuclear» стирал файл командного процессора – «command.com».

Вот такой странный вирус-пацифист с явными деструктивными наклонностями! Поневоле подумаешь, что либо у автора «Nuclear» наступило явное раздвоение личности.

Тем временем продолжали происходить очередные вирусные инциденты с участием компании Microsoft. Например, на её Web-сайте, в одном из файлов MS Word, содержащем документы посвященые технической поддержке программных продуктов Microsoft в Швейцарии был обнаружен макро вирус «Wazzu». Несколько позже этот же вирус был обнаружен на CD-ROM, распространённых Microsoft на проходившей в Швейцарии выставке

[396] Так должно было происходить по замыслу автора вируса, но, как мы уже упоминали, программный код «Nuclear» содержал ошибку и вирус фактически потерял способность к инфицированию COM/EXE/NewEXE-файлов.

компьютерных технологий «Orbit». Но и на этом проблемы Microsoft с «Wazzu» не закончились – в сентябре вирус попал на компакт диск Microsoft Solution Provider и, благодаря этому, получил очень широкое распространение во всём мире. Что же это за вездесущий компьютерный вирус, помотавший нервы специалистам столь уважаемой и всемогущей компании, а заодно и ничем неповинным пользователям?

Идентификационная карточка вредоносной компьютерной программы	
Имя	Wazzu
Другие названия	Wazzu.a, Macro.Word. Wazzu, WM/Wazzu.A
Тип	компьютерный вирус
Инфицируемые платформы	Windows 95/98/ME/NT /2000/XP/2003
Впервые обнаружен	сентябрь 1996 года
Страна происхождения	Швейцария
Длина	658 байт

Компьютерный макро вирус «Wazzu» содержал один единственный макрос «AutoOpen», который запускался автоматически и инфицировал документы MS Word (версии 6.0 и более поздние) при их открытии, а также копировал программный код макроса «AutoOpen» в системную область MS Word – глобальный шаблон «normal.dot» при открытии заражённого данным вирусом документа и, тем самым, заражая его. Начиная с этого момента, каждый открываемый документ MS Word автоматически инфицировался в случае его открытия пользователем. При этом «Wazzu» не был зашифрован его автором и легко обнаруживался по текстовым строкам внутри инфицированного файла: «RndWorddo», «wazzu do», «RndWorddRgV».

После заражения очередного документа MS Word или после инсталляции в компьютерную систему вирус перемещал случайно выбранное внутри документа слово. В этих целях он брал два случайных адреса в заражённом документе, удалял слово по первому адресу и вставлял его по второму. «Wazzu» повторял эту процедуру до трёх раз в зависимости от значения счётчика случайных чисел. Затем вирус, также в зависимости от счётчика случайных чисел, вставлял в случайно выбранную позицию внутри докумен-

та слово «wazzu». Для выполнения всех указанных манипуляций в единственный макрос вируса «AutoOpen» было включено три подпрограммы:

«MAIN» – основная подпрограмма, вызывавшаяся системой при запуске макроса «AutoOpen»;

«Payload» – вызывавшаяся подпрограммой «MAIN», перемещала слова и вставляла в инфицируемый документ выражение «wazzu».

«RndWord» – вызывавшаяся подпрограммой «Payload», выбирала в документе случайный адрес, то есть новую позицию слова.

В итоге, в зависимости от значения системного счётчика случайных чисел, «Wazzu» модифицировал документ MS Word, перемещая с вероятностью 20% каждое из трёх слов и вставляя с вероятностью 25% выражение «wazzu» в инфицируемый документ.

Попробовали – понравилось! И посыпались, как из мешка, всё новые штаммы этой «звезды» на ниве вирусописания. Тем более что в 1996 году «Wazzu» стал одним из наиболее широко распространённых в мире вирусов. Как мы уже упоминали ранее, причиной этому послужили несколько неприятных инцидентов с данным вирусом: заражённый файл слишком долго находился на Web-сайте компании Microsoft, а несколько инфицированных им документов были случайно тиражированы на CD-ROM. Кроме того, «Wazzu» обзавёлся многочисленным семейством, которое со временем составило около тридцати «родственников». Приведём их краткое описание с точки зрения отличий от родоначальника – «Wazzu».

«Wazzu.b,i» – отличаются от оригинала строкой-комментарием: < - - - - - - - here 's the payload;

«Wazzu.c, t, ac» – ничем особым не выделяются и не имеют подпрограммы «Payload», но содержат подпрограмму «RndWord» обращения к которой отсутствуют;

«Wazzu.d, f, q, w, ad» – не имеют ни «Payload», ни «RndWord». Кроме того, «Wazzu.f», самый короткий представитель семейства, так как его двоичный образ занимает всего лишь 318 байт;

«Wazzu.e, h» – зашифрованные «Wazzu». «Wazzu.h» имеет ошибки, и поэтому может вызывать зависание MS Word или сообщение об ошибке;

«Wazzu.g, r» – также зашифрованы. «Wazzu.g» содержит подпрограмму «EatThis» вместо «Payload». С вероятностью в 10% эти вирусы выводят стандартное окно сообщений Windows с текстом: «Microsoft Word. This one's for you, Bosco»;

«Wazzu.k» – является подпорченным «Wazzu»;

«Wazzu.l» – отсутствуют подпрограммы «Payload» и «RndWord». С вероятностью в 10% добавляет выражение «wazzu!» в конец документа;

«Wazzu.m, s» не имеют подпрограммы «Payload», но вызывают её, результатом чего является сообщение об ошибке MS Word;

«Wazzu.u, aa, ad» – практически полностью совпадают с «Wazzu», но не вставляют в документы выражение «wazzu»;

«Wazzu.x» – не содержит подпрограмм «Payload» и «RndWord», но обладают следующей строкой: «The Meat Grinder virus – Thanks to Kermit the Frog, and Kermit the Protocol»;

«Wazzu.y, z» – совпадают с «Wazzu» за исключением мелких изменений, например, в вирусе «Wazzu.y» все символы табуляции заменены на пробелы.

Однако на фоне нескончаемых штаммов «Wazzu» наконец-то появился и «борец за справедливость», коим без сомнения стоит признать «AntiWazzu».

Идентификационная карточка Вредоносной компьютерной программы	
Имя	AntiWazzu
Другие названия	Macro.Word97.Anti Wazzu, AntiWazzu.A, WM/Anti Wazzu.A
Тип	компьютерный вирус
Инфицируемые Платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые Обнаружен	ноябрь 1996 года
Страна происхождения	Соединённые Штаты Америки
Длина	1335 байт

Эта программа состояла из двух макросов «AutoOpen» и «Temp-cdg» и распространялась при открытии файлов с расширением «*.doc», то есть документов MS Word. При инфицировании «AntiWazzu» удалял макрос «AutoClose», если он присутствовал в документе и, таким образом, боролся как со всем семейством вирусов «Wazzu», так и с некоторыми другими вирусами.

Причём «AntiWazzu» был запрограммирован так, что после 1 апреля 1999 года он «пел свою лебединую песню», активизируя процедуру самоуничтожения, которая удаляла из компьютерной системы пользователя макрос «AutoOpen», содержащий его основной программный код.

Клин клином вышибают!

25 ноября 1996 года на Филиппинах состоялась встреча восемнадцати членов группы APEC (Asia-Pacific Economic Cooperation). Во время заседания один из компьютеров, обслуживавших мероприятие, стал вести себя подозрительно. По предположениям, с флоппи-диска одного из дипломатов в него попал компьютерный вирус, и его атаке подвергались документы MS Word. Специалисты, обслуживающие APEC, обратились за помощью в компьютерные компании Австралии и Океании. Быстрее всех отреагировала австралийская SAS International, фирма довольно известная в этом регионе мира. Специалисты SAS быстро идентифицировали вирус и уничтожили его. Как потом стало известно, для борьбы с вирусом использовалась российская программа, созданная в антивирусном центре Евгения Касперского – AVP MacroKiller. Дальнейшим заседаниям APEC компьютерные вирусы больше не мешали, но примечательно, что на следующее утро национальный канал

австралийского телевидения первым сюжетом показал пятиминутное интервью президента компании SAS International г-на Рода Фьюстера.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Punch
Другие названия	Win95.Punch.9262, Win95.Punch
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	декабрь 1996 года
Страна происхождения	Соединённые Штаты Америки
Длина	9262 байт

В декабре появился первый резидентный вирус для Windows 95 «Punch»[397], который загружался в систему как VxD-драйвер, перехватывал обращения к файлам и заражал их.

Итак, по порядку. Вирус «Punch» инфицировал EXE-файлы (формата PE – Portable Executable) Windows 95 и стал первым известным резидентным вирусом для этой операционной системы. Он загружался в компьютерную систему как VxD-драйвер, перехватывал обращения к файлам и записывался в их конец. Сам процесс инфицирования проходил в два этапа. При запуске заражённого EXE-файла вирус записывал на «жёсткий» диск VxD-файл (дроппер вируса), содержащий код вируса в формате VxD, и регистрировал этот VxD в файле «system.ini». Затем возвращал управление программе-носителю и больше никак не проявлял себя вплоть до следующей перезагрузки компьютера. Когда Windows 95 загружалась в очередной раз, в системную память загружались все VxD-драйверы, описанные в файле «system.ini», включая VxD с программным кодом «Punch». Вирус оставался в оперативной памяти резидентно, а затем инфицировал открываемые EXE-файлы формата PE. Он имел несколько ошибок, некорректно заражая некоторые системные файлы, и в результате вызывал большое число системных сообщений об ошибках. «Punch» содержал несколько текстовых строк, часть из которых использовалась при обращении к системным ресурсам и функциям: «KERNEL32», «CreateFileA», «WriteFile», «ReadFile», «SetFilePointer»,

[397] «Punch» (англ.) – «Петрушка», «Перфоратор».

«CloseHandle». Другие строки «Punch» использовал при поиске и модификации системных файлов и заражении компьютерной системы: «c:\win95\system.ini», «c:\windows\system.ini», «c:\win95\system\vvfs.vxd», «c:\windows\system\vvfs.vxd». Кроме того, в PE-заголовок вирус записывал секцию с именем: «QuantumG», а последняя строка использовалась для подписи его автора.

При запуске заражённого EXE-файла «Punch» записывал в системный каталог свой VxD-дроппер. Для этого он вызывал системные функции KERNEL32 GetLogicalDriveStringsA (#350) и SetEnvironmentVariableA (#372) и определял системные параметры и указатели на функции работы с файлами «CreateFileA», «WriteFile», «ReadFile», «SetFilePointer», «CloseHandle». Используя их, вирус вызывал функцию «CreateFileA» и пытался создать файл vvfs.vxd по адресу C:\WIN95\SYSTEM\. Если такого директория не существовало, он создавал такой файл в C:\WINDOWS\SYSTEM\. Если и такой директорий не существовал, «Punch» возвращал управление программе-носителю. В ином случае он записывал в этот файл 9262 байта кода и данных, которые имели формат VxD-файла (LE EXE-файл) и содержали его программный код. Затем «Punch» открывал или файл C:\WIN95\system.ini, или файл C:\WINDOWS\system.ini, искал там строку «ice=» («device=») и вставлял в неё строку вызова созданного перед этим VxD-файла. Таким образом, перед заражением – device=some.vxd; после заражения – device=vvfs.vxd,some.vxd. При этом «Punch» проверял строку «device=» и не записывал повторный вызов своего VxD, если он там уже присутствовал. Затем вирус закрывал файл «system.ini» и возвращал управление программе-носителю. В результате инфицирования компьютерной системы в директории «SYSTEM» теперь находился новый VxD-файл, а файл «system.ini» был модифицирован таким образом, что при очередных загрузках Windows 95 загружался и новый VxD.

При загрузке Windows 95 «Punch» в VxD-файле получал управление, проверял номер версии DOS IFS Manager (DOS Installable File System Manag-

er), перехватывал вызовы IFS API и оставался в памяти Windows 95 как VxD-драйвер. Перехват IFS API очень похож на перехват прерывания INT 21h, используемый TSR-программами DOS. Перехватчик получал управление непосредственно перед системными драйверами и мог выполнять практически любые действия на файловом уровне. «Punch» перехватывал только одну функцию – открытие файла («OpenFile» – IFSFN_OPEN) и, следовательно, заражал файлы при их открытии (при этом VxD перехватывал все вызовы на открытие независимо от принадлежности активной программы: Windows 95 или окно DOS под Windows 95, и заражал также файлы, открываемые в окне DOS).

При заражении файла «Punch» проверял его формат и заражал только те EXE-файлы, которые имели формат Portable Executable (PE). Затем он считывал и корректировал необходимые поля PE-заголовка, добавлял в PE-заголовок описание одной новой секции с именем «QuantumG», записывал свой код и данные (всего 10185 байт) в конец файла в только что созданную секцию. Вирус также правил секцию ресурсов и описание ресурсов для того, чтобы иметь возможность обращаться к функциям KERNEL32 при запуске заражённого EXE-файла. Для того чтобы не заражать файлы дважды, он проверял имя последней секции файла и сравнивал её со строкой «QuantumG».

При заражении файлов вирус не принимал во внимание их атрибуты и время/дату создания или модификации. В результате «Punch» не заражал файлы с атрибутом «ReadOnly» и изменял время/дату последней модификации файла. Также он не проверял расширение имени файла, а только его формат. По этой причине заражёнными оказывались не только файлы с расширением «*.exe», но и файлы с расширениями «*.dll», «*.cpl», «*drv» и прочие файлы, имеющие формат PE EXE. Вирус при инфицировании записывал в VxD и EXE-файлы различное число байт – 10185 при заражении PE EXE и 9262 при заражении VxD. Это было вызвано тем, что VxD и PE EXE-файлы имели различные форматы и загружались в память различными способами, а, следовательно, должны были иметь и различные точки входа. Поэтому

«Punch» при заражении EXE-файлов дописывал к ним дополнительный блок кода, который записывал VxD-файл вируса в директорий SYSTEM. Длина EXE-файлов при инфицировании возрастала на различные значения: вирус сначала увеличивал длину файла до границы секции, а затем дописывал к нему свои 10185 байт.

Из-за многочисленных ошибок большого распространения этот вирус так и не получил и остался в анналах вирусописания только потому, что был первым резидентным вирусом под операционную систему Windows 95, но покопаться специалистов-вирусологов в своём содержимом он заставил.

Завершая наш рассказ о богатом событиями 1996 годе, можно констатировать следующее.

В третьем квартале предыдущего года вирус «Concept» и появившийся через год похожий на него вирус «Laroux» заставили компанию Microsoft начать борьбу с новым племенем межплатформенных файловых вирусов, которые могли присоединяться к сообщениям электронной почты и путешествовать по миру посредством распространения по глобальной сети Интернет. Хотя эти вирусы редко приводили к серьёзным повреждениям в системах и данных, радости они не доставиляли никому. «От вирусов «Concept» действительно трудно избавиться, поскольку мы получаем очень много файлов по Интернет, а сотрудники распространяют их по офису, – говорил Марк Бейкер, менеджер информационной службы компании Productivity Point International. – Они идут волнами, но, в среднем, мы тратим на борьбу с ними около часа каждую неделю». Питер Типпет, президент National Computer Security Association (NCSA), заметил, что: «из порядка 6000 различных вирусов, известных нам, около 5% были написаны с целью повредить информацию. Тем не менее, они вполне успешно отравляют пользователям жизнь… Вирусы внедряются в текст программ, взаимодействуют с другими макросами и иногда могут всё испортить».

Около 5% вирусов того времени, созданных на основе макросов текстового процессора MS Word, могли оказаться причиной более серьёзных

сбоев во время выполнения операций по выводу документов на печать, сохранению файлов и так далее. По данным NCSA на конец 1986 года в 49% случаев при обнаружении вируса в компьютерной системе им оказывался «Concept», а вероятность «подхватить» вирус выросла по отношению к 1985 году в 10 раз.

В этой обстановке Microsoft приняла решение о распространении через свой Web-узел бесплатного программного обеспечения, предназначенного для удаления вируса «Concept», а также программы, обеспечивающей защиту от возможного заражения в будущем. Но некоторые системы все же были инфицированы повторно и Питер Пас, старший менеджер подразделения, занимающегося редактором MS Word, был вынужден выступить перед компьютерным сообществом с заверением, что «Microsoft очень серьёзно взялась за проблему вирусов», и текущая версия редактора MS Word, а также последующие версии MS Office будут иметь встроенную систему безопасности, не позволяющую открывать заражённые файлы». Цену этому заявлению с высоты сегодняшнего дня мы знаем очень хорошо.

В течение 1986 года появилось великое множество новых макро вирусов и некоторые из них (например, «Nuclear», «Wazzu») даже получили достаточно широкое распространение, став своего рода «знаменитостями», но все они в той или иной степени задействовали методы, уже использовавшиеся ранее вирусом «Concept», который, что совершенно очевидно, к середине года стал одним из наиболее распространённых в мире компьютерных вирусов среди всех их видов и разновидностей.

Тем временем, уже спустя некоторое время после появления вируса «Boza» практически каждую неделю вирусологи объявляли о появлении всё новых вирусов, которые инфицировали операционные системы, отличные от DOS. Стало абсолютно ясно, что именно такие вирусы в скором времени выйдут на первый план, закрыв проблематику вирусов под операционную систему DOS. И, как пишут специалисты-вирусологи, «это действительно произошло вместе с постепенным «отмиранием» DOS и распространением

новых операционных систем и программного обеспечения для них. Так как в ближайшем будущем все существующие DOS приложения были замещены их аналогами для Windows 3.x, Windows 95 и OS/2, проблема вирусов под DOS сошла на нет, оставив после себя лишь неприятные воспоминания у всего компьютерного сообщества».

Если ещё несколько лет назад эпидемия компьютерного вируса могла добираться из Северной, Южной Америки или Западной Европы в Россию несколько месяцев, то в 1996 году скорость распространения вирусов настолько увеличилась, что в отдельных случаях для этого уже вполне хватало и нескольких суток. Компьютерные инфекции в эпоху скачкообразного развития глобальных компьютерных сетей стали гораздо быстрее перемещаться между странами и континентами. Более того, в конце 80-х годов, когда информацию переносили с компьютера на компьютер на флоппи-дисках, «стандартный набор» компьютерных вирусов в Советском Союзе, например, достаточно сильно отличался от аналогичного «набора» на Западе. К середине же 90-х годов вредоносные компьютерные программы, созданные российскими вирусописателями стали быстро проникать в США и Западную Европу и, наоборот, новые вредоносные программы зарубежных вирусописателей стали обнаруживаться в России во всё более сжатые сроки.

Итак, в целом 1996 год можно считать начальным этапом широкомасштабного наступления вирусописателей на операционные системы Windows 95, Windows NT, а также на приложения MS Office компании Microsoft. Именно в этом году появилось сразу несколько десятков компьютерных вирусов для операционных систем Windows 95 и Windows NT. В некоторых из них вирусописатели применяли совершенно неизвестные до этого приёмы и методы инфицирования компьютерных систем, добавляли в них изощрённый механизм полиморфизма, усовершенствованную «стелс» технологию, сложные алгоритмы шифрования и т. п.

Таким образом, компьютерные вирусы вышли на новый виток своего развития, захватив «плацдарм» для последующего фронтального штурма но-

вых на тот момент высот – 32-битных операционных систем. Примерно за полтора-два года компьютерные вирусы для 32-битных операционных систем Windows повторили примерно те же стадии развития, какие ровно за 10 лет до этого прошли вирусы под операционную систему DOS. Казалось бы, история повторяется, но новые вирусы представляли собой совершенно иной, технологически более высокий уровень вирусописания, что потребовало для ведения успешной борьбы с ними ускоренной выработки и применения новых технологий, приёмов и антивирусных аппаратно-программных комплексов.

§17. 1997 год – макро вирусы множатся, совершенствуются, мигрируют в MS Office 97 и превращаются в проблему номер один. Они были первыми: вирус под операционную систему Linux, использующий протокол FTP сетевой вирус-червь, самостоятельно шифрующийся вирус для Windows 95, черви mIRC и PIRCH

- Выпущена операционная система Windows NT Server 4.0 Enterprise Edition.
- Выпущена версия 2.1 операционной системы Linux, новые версии выходят каждую неделю.
- Выпущен микропроцессор Intel Pentium MMX.
- Появляется новое поколение микропроцессоров Intel Pentium II (7,5 миллионов транзисторов).

Начало 1997 года ознаменовалось появлением новых макро вирусов для MS Word, в частности, для его версии, входящей в пакет прикладных программ MS Office 97.

В январе в Венесуэле был обнаружен в «диком» виде инфицирующий документы MS Word 97 с использованием «стелс» технологии зашифрованный макро вирус, который получил имя «Cap»[398] и стал одним из самых распространённых в мире компьютерных вирусов.

Этот вирус проникал в компьютерную систему вместе с заражённым файлом-документом (расширение «*.doc») текстового процессора MS Word и

---

[398] «Cap» (англ.) – «Колпак», «Предел». Всего существует более 50 штаммов вируса «Cap».

осуществлял проверку глобального шаблона (файл «normal.dot») на инфекцию. Если глобальный шаблон ещё не был инфицирован, то «Cap» заражал его. Как только это происходило, вирус начинал заражать все документы MS Word, которые основывались на этом шаблоне.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Cap
Другие названия	Cap.a, WM/Cap.a, WM/Cap, WM/CAP.A, WordMacro/CAP.A
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	январь 1997 года
Страна происхождения	Венесуэла
Длина	10 макросов

«Cap» состоял из десяти макросов, выполняющих соответствующие функции:

«CAP» – процедура заражения;

«AutoExec», «AutoOpen, «FileOpen», «FileSave», «AutoClose», «FileClose», «FileSaveAs» – вызов процедуры заражения;

«ToolsMacro», «FileTemplates» – запрет пункта меню (используется «стелс» подпрограммой).

«Cap» не только запрещал вызов меню работы с макросами, но и удалял ссылки на них из основных меню «Files» и «Tools». Помимо запрета пунктов меню «ToolsMacro» и «FileTemplates» вирус отключал выполнение автоматических макросов при открытии документов MS Word, что делало практически невозможным их лечение средствами текстового процессора, поскольку по причине запрета пункта меню работы с макросами («ToolsMacro») пользователь лишался возможности создания и запуска какого-либо лечащего макроса. Лечение невозможно было выполнить и при загрузке MS Word, так как автоматический запуск макросов также был отключён. Кроме того, «Cap» эмулировал «FileSaveAs», и при попытке пользователя сохранить инфицированный файл под другим именем на «жёсткий» диск записывался пустой документ. Интересно, что номер своего поколения «Cap» хранил в описании макроса «ToolsMacro», а в макро коде вируса содержались следующие строки закомментированного текста: «C.A.P: Un virus social.. y ahora

digital. «j4cKy Qw3rTy» (jqw3rty@hotmail.com). Venezuela, Maracay, Dic 1996. P.D. Que haces gochito? Nunca seras Simon Bolivar, Bolsa!»

Кроме того, вирус «Cap» был способен оценить то, к какой языковой версии относится установленный на данном компьютере текстовый процессор и, в случае необходимости, инсталлировал соответствующие макросы. Например, если вирус инфицировал немецкую локализацию MS Word, то он инсталлировал следующие макросы: «DateiÖffnen», «DateiSpeichern», «DateiSpeichernUnter», «DateiSchließenOderAllesSchließen».

Вирус «Cap» было трудно распознать, потому что он не порождал никаких визуальных эффектов: ничего не выводил на экран монитора и не делал никаких предупреждений об инфицировании компьютерной системы. Не использовал он и экзотические или специальные методы и каналы для своего распространения, проникая в компьютерную систему при помощи обычных средств, используемых вирусами: флоппи-диски, CD-ROM, сообщения электронной почты с инфицированными вложениями, загрузка через Интернет, FTP и т. п.

Февраль принёс с собой ещё одну новость – был обнаружен в «диком» виде первый вирус, написанный под операционную систему Linux[399] и получивший название «Bliss»[400].

[399] Некоммерческая версия операционной системы UNIX, предназначенная для использования на персональных компьютерах.

[400] «Bliss» (англ.) – «Блаженство».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Bliss
Другие названия	Bliss.a, Linux.Bliss, Linux/Bliss.A
Тип	компьютерный вирус
Инфицируемые платформы	Linux, UNIX
Впервые обнаружен	февраль 1997 года
Страна происхождения	Соединённые Штаты Америки
Длина	17892 байта

Таким образом, компьютерные вирусы взяли ещё одну командную высоту. Впрочем, специалисты-вирусологи были вполне готовы к такому ходу событий, что находит своё подтверждение в одном из характерных заявлений тех лет: «До сегодняшнего дня, то есть более чем за четыре года разработки вирусов для Linux не было зарегистрировано ни одного случая их появления в «диком» виде. Но это не помешало им идти вперед в своём развитии. Вирусописатели изобрели вирусы для Linux, работающие в фоновом режиме, а также большое количество вполне работоспособных троянских программ для этой платформы. Можно с полной уверенностью заявить, что если бы Linux имела хотя бы половину популярности операционной системы Windows, то соотношение количества вирусов для этих операционных систем на сегодняшний день было бы диаметрально противоположным».

Вскоре у вируса «Bliss» появился потомок в лице его штамма под названием «Bliss.b». Оба родственника представляли собой нерезидентные вирусы, заражающие выполняемые файлы операционной системы Linux и были написаны на языке GNU C. Они имели формат «ELF» и были работоспособны только на компьютерных системах под управлением операционной системы Linux. При запуске вирусы искали выполняемые файлы и инфицировали их, сдвигая содержимое файла вниз и записывая себя на освободившееся место. При этом в конец файла добавлялась строка-идентификатор: для «Bliss» – «infected by bliss: 00010002:000045e4»; для «Bliss.b» – «infected by bliss: 00010004:000048ac». Первое шестнадцатеричное число в идентификаторе (00010002 и 00010004) представляло собой номер версии вируса, а

второе (000045e4 и 000048ac) его длину в байтах (вирусы имели длины 17892 и 18604 байт, соответственно).

При запуске заражённого файла «Bliss» искал не более трёх ELF-файлов и записывался в них, а «Bliss.b» обладал способностью к инфицированию большего количества файлов. Если в текущем директории все файлы оказывались заражёнными, вирусы просматривали другие директории компьютерной системы, искали в них выполняемые файлы и заражали их. После инфицирования они возвращали управление программе-носителю.

В операционной системе Linux предусмотрено разграничение доступа, то есть пользователь и программы имеют доступ к файлам и директориям в зависимости от установленных привилегий. То же относится и к вирусам: они заражали файлы только в тех директориях, к которым имел доступ запустивший их пользователь. Таким образом, если пользователь обладал системными привилегиями, вирусы могли распространиться по всему компьютеру. При работе вирусы выводили различные «отладочные» сообщения, но никаких деструктивных действий не предпринимали.

В феврале – апреле 1997 года макро вирусы активно «мигрировали» в пакет прикладных программ MS Office 97. Эти «пионеры» отличались тем, что в своей массе являлись лишь конвертированными в новый формат макро вирусами, изначально написанными для текстового процессора MS Word и MS Excel более ранних версий. Ограниченные возможности работы, а в некоторых случаях и абсолютная несовместимость макро вирусов, созданных, например, для MS Word 5.0, MS Excel 5.0 с MS Office 97 определялась присутствием новой версии языка программирования VBA 5.0, который сильно отличался от Word Basic и VBA 3.0. Однако за первой волной практически сразу пришла вторая волна компьютерных вирусов, которые были уже чётко ориентированы на работу с пакетом прикладных программ MS Office 97.

В марте был обнаружен зашифрованный макро вирус «ShareFun»[401], инфицировавший документы текстового процессора MS Word версий 7, 8 (файлы с расширением «*.doc») и открывший ещё одну страницу в истории вирусописания, так как именно он стал первым компьютерным вирусом, использовавшим для своего распространения не только стандартные возможности MS Word, но и возможности современной электронной почты, в частности, почтовой программы MS Mail.

Идентификационная карточка вредоносной компьютерной программы	
Имя	ShareFun
Другие названия	Macro.Word.ShareFun, WM/Sharefun.A, WM. ShareFun.A, ShareFun.a
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	март 1997 года
Страна происхождения	Соединённые Штаты Америки
Длина	1259 байт

«ShareFun» состоял из девяти макросов, выполнявших соответствующие функции:

«AutoExec» – «пустышка»;

«AutoOpen», «FileClose», «FileExit», «FileSave», «FileOpen», «FileTemplates» – заражают документ или область глобальных макросов;

«ToolsMacro» – заражает документ или область глобальных макросов, блокирует меню Tools/Macro (используется «стелс» подпрограммой);

«ShareTheFun» – рассылает копии вируса по Microsoft Mail.

Этот вирус заражал файлы и компьютерную систему при открытии-закрытии документов MS Word, а также обращениях к пункту меню «Tools/Macro».

Проявлял себя «ShareFun» крайне необычным для того времени способом – рассылал инфицированные документы MS Word по MS Mail, если эта система была установлена. Необходимая процедура (макрос «ShareTheFun») вызывалась при открытии файлов («AutoOpen») с вероятностью в 25%. При

[401] Несколько позже появился очень похожий на родоначальника штамм «ShareFun.b», длина которого составляла 1511 байт.

вызове она сохраняла текущий, уже инфицированный документ на «жёстком» диске (C:) под именем «doc1.doc», выбирала из списка адресов MS Mail три случайных адреса и посылала по этим адресам заражённый файл: C:\doc1.doc. Заражённые письма представляли собой пустой лист под заголовком: «You have GOT to read this!» («Вам поневоле придётся читать это!»). После отправки сообщения вирус немедленно закрывал MS Mail, а адресат, если он вскрыл вложение к полученному сообщению, инфицировал свою компьютерную систему. Если же система MS Mail не была установлена, «ShareFun» выдавал команду перезагрузки операционной системы.

В апреле компьютерное сообщество поджидало очередное крайне неприятное событие. Был зарегистрирован первый сетевой вирус-червь, использующий для своего распространения протокол передачи данных – FTP (File Transfer Protocol) и получивший красивое имя «Homer»[402].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Homer
Другие названия	W97M.Homer, Win.Homer
Тип	сетевой червь
Инфицируемые платформы	Windows 95/98/ME/NT /2000/XP/2003
Впервые обнаружен	апрель 1997 года
Страна происхождения	Италия
Длина	50 983 байта

Резидентный вирус «Homer» был написан на языке программирования «C++» специально под операционную систему Windows и, как некоторые из его предшественников, инфицировал файлы формата NewEXE (NE). При запуске заражённого файла он перехватывал прерывание INT 21h и оставался Windows-задачей

[402] «Homer» (англ.) – «Почтовый голубь».

Известно пять штаммов этого вируса, которые имеют довольно большие размеры от 40 до 54 килобайт, но только два из них действительно заражают файлы, а остальные не делают этого по причине ошибок в программном коде.

(процессом)[403]. Кстати, перехват прерывания происходил разными способами в режимах «real/protect mode DPMI» или «Windows API hooking». «Homer» заражал файлы при их запуске, записываясь при этом в их конец и модифицируя NewEXE-заголовки. Некоторые из штаммов вируса были способны перехватывать также сетевые сообщения. В исходном тексте «Homer» присутствовал комментарий, в котором говорилось о том, что данный вирус перехватывает вход пользователя на удалённый ftp-сервер и посылает свою копию в директорий «incoming», при этом он использовал File Transfer Protocol. В программном коде этого вируса содержался следующий текст: «HOMER virus by Kernel Panik, Italy, april 1997» («Вирус «Почтовый голубь» от Кернел Пэник, Италия, апрель 1997»).

В контексте настоящей книги инцидент с вирусом «Homer» интересен, прежде всего, тем, что он неопровержимо свидетельствует о начале проникновения компьютерных вирусов в глобальные сети уже весной 1997 года. Причём всё указывает на то, что вирус «Homer» – одна из самых первых попыток вирусописателей создать новое поколение сетевых вирусов, опирающаяся как на опыт прошедших лет, так и на новые технологии и идеи.

Попытка написать вирус-супервизор – «PMBS»[404], в течение четырёх лет оставалась единственной из известных. И только в мае 1997 года вирусописатель из Москвы «обнародовал» весьма работоспособную реализацию функционирующего в защищённом режиме процессора фирмы Intel (i386) файлового компьютерного вируса по имени «PM.Wanderer»[405]. Этот факт вызвал ряд публикаций, авторы большинства из которых сходились в следующем: «Пока непонятно, станут ли в дальнейшем вирусы-супервизоры действительной проблемой для пользователей и разработчиков антивирусных программ. Скорее всего, нет, так как такие вирусы должны «засыпать» на

---

[403] В зависимости от штамма эта задача либо имела своё собственное окно, либо оставалась невидимой для пользователя.

[404] Более подробно об этом компьютерном вирусе см. выше – 1993 год.

[405] «PM.Wanderer» (англ.) – «PM.Скиталец».

время работы новых операционных систем (Windows, Win95/NT, OS/2), что позволяет их (вирусы) легко обнаружить и удалить. Однако полноценный вирус-супервизор, использующий технологию «стелс» может принести немало неприятностей пользователям «чистой» DOS, ведь обнаружить такой стелс-вирус под DOS не представляется возможным».

Идентификационная карточка вредоносной компьютерной программы	
Имя	PM.Wanderer
Другие названия	PM_Wanderer.3684, PM.Wanderer.3684
Тип	компьютерный вирус
Инфицируемые платформы	MS-DOS
Впервые обнаружен	май 1997 года
Страна происхождения	Россия
Длина	3684

Проникнув в компьютер пользователя при помощи заражённого флоппи-диска, CD-ROM, сообщения электронной почты или через загрузку программ посредством Интернет, вирус устанавливал себя резидентно в оперативную память компьютерной системы и инфицировал файлы с расширениями «*.exe» и «*.com» – за исключением командного процессора «command.com» – при их запуске или открытии. В процессе заражения файлов «PM.Wanderer» шифровал себя полиморфным методом и записывался в начало файлов с расширением «*.com» и в середину файлов с расширением «*.exe» (между EXE-заголовком и основным телом файла). Первоначальный программный код (данные) файла вирус записывал в его конец. При запуске инфицированного файла вирус копировал себя в расширенную область оперативной памяти, переходил в защищённый режим процессора i386 и перехватывал прерывания INT 1 (трассировка) и INT 9 (клавиатура). Именно в результате перехода в защищённый режим «PM.Wanderer» становился невидимым для стандартных антивирусных программ и утилит просмотра памяти операционной системы.

С целью перехвата функций запуска и открытия файлов операционной системы «PM.Wanderer» использовал специфику отладочного режима процессора i386, устанавливая одну из отладочных точек останова на адрес INT 21h. В результате, когда управление передавалось на INT 21h, процессор ге-

нерировал прерывание INT 1, вирус получал управление и заражал файлы. Для «PM.Wanderer» характерно, что он не устанавливал себя в оперативную память в том случае, если не находил инсталлированного в компьютерной системе EMS-драйвера. На время работы операционной системы Windows «PM.Wanderer» выключал свой отладочный механизм перехвата INT 21h и восстанавливал его только после выхода пользователя из Windows при первом же нажатии на какую-либо клавишу.

Этот вирус, хотя и содержал программистские ошибки, тем не менее, был вполне работоспособен, но в отдельных случаях «подвешивал» систему. В его теле содержалась следующая текстовая строка: «WANDERER, (c) P. Demenuk» («СКИТАЛЕЦ, (с) П. Деменюк»).

Июнь 1997 года остался в памяти многих представителей компьютерного сообщества в качестве даты появления первого известного самостоятельно шифрующегося вируса для Windows 95 по имени «Mad»[406]. Он был российского происхождения и его разослали сразу на несколько станций BBS в Москве, что и явилось причиной последовавшей вскоре достаточно крупной эпидемии.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Mad
Другие названия	Mad.a, Win95.Mad, Win95.Mad.2736
Тип	компьютерный вирус
Инфицируемые платформы	Windows 95
Впервые обнаружен	июнь 1997 года
Страна происхождения	Россия
Длина	2736

Ведущие отечественные специалисты-вирусологи, исследовавшие «Mad», оценили его «как написанный в Москве неопасный нерезидентный, но зато впервые использующий технологию самостоятельного шифрования своего программного кода вирус для операционной системы Windows 95».

Отмечалось также, что «Mad» функционировал вполне корректно и побочных явлений – типа зависания си-

[406] «Mad» (англ.) – «Бешеный».

стемы или появления системных сообщений об ошибках – не вызывал. Этот вирус инфицировал выполняемые файлы (PE EXE-файлы) операционной системы Windows 95. Во время запуска системы он искал в текущем, а затем и в родительском директории, выполняемые файлы и записывался в их конец. Причём, во время заражения «Mad» не добавлял новую секцию к инфицируемому файлу, а увеличивал размер последней секции, записывая туда свой программный код, изменяя характеристики этой секции и адрес стартовой процедуры.

В теле вируса содержались следующие строки: «GetProcAddress», «GetModuleHandleA», «KERNEL32», «USER32», «MessageBoxA», «FindFirstFileA», «CreateFileA», «CloseHandle», «ReadFile», «WriteFile», «SetFilePointer», «FindNextFileA», «GetLocalTime», «SetCurrentDirectoryA», «GetCurrentDirectoryA», «*.eXe [MAD for Win95] version 1.0 BETA! (c) Black Angel`97».

Кроме того, в зависимости от значения системного времени «Mad» выводил на экран монитора в окне сообщений Windows приведённый ниже текст:

Multiplatform Advanced Destroyer	Многоплатформенный продвинутый разрушитель
Hello user your computer is infected by MAD virus	Привет пользователь, твой компьютер инфицирован вирусом MAD
Welcome to my first virus for Windoze 95 ...	Милости просим, мой первый вирус для Windoze 95 ...
Distribution & Copyright by Black Angel 1997	Распространение и авторское право Чёрного ангела 1997

Однако, несмотря на заметное подражание, «высот славы» знаменитого болгарского вирусописателя, скрывавшегося под псевдонимом «Dark Avenger»[407] («Тайный мститель») или даже англичанина Кристофера Пайла, известного под псевдонимом «Black Baron»[408] («Чёрный барон») и приговорённого судом к полутора годам тюремного заключения за написание компьютерных вирусов, наш доморощенный компьютерный злоумышленник не

[407] Более подробно об этом вирусописателе и его «творениях» см. выше – 1989–1991 годы.

[408] Более подробно о «произведениях» вирусописателя под псевдонимом «Black Baron» см. выше – 1993–1995 годы.

достиг, и имени его не осталось в истории вирусописания. Чего ему не хватило? Знаний? Упорства? Мы надеемся, что всё гораздо проще. Автор, воплотивший в вирусе «Mad» идею самостоятельного шифрования, во время перестал тратить попусту своё и чужое время и сейчас работает в одной из уважаемых фирм-разработчиков программного обеспечения. Уж не антивирусного ли?

В ноябре 1997 года была предпринята неудачная попытка написания многоплатформенного вируса, который мог бы работать не только под управлением операционных систем DOS и Windows, но также был бы в состоянии заражать и файлы операционной системы Mac OS. Этому вирусу, по большому счёту вирусу-неудачнику, было присвоено красивое имя: «Esperanto»[409].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Esperanto
Другие названия	Esperanto.a, Esperanto.4733,
Тип	компьютерный вирус
Инфицируемые платформы	Windows 95, Mac OS, DOS
Впервые обнаружен	ноябрь 1997 года
Страна происхождения	Соединённые Штаты Америки
Длина	4733

Он поражал выполняемые файлы операционной системы DOS (файлы с расширениями «*exe.» и «*com.»), EXE-файлы (NewExe) операционной системы Windows и EXE-файлы (PE) операционной системы Windows 32. «Esperanto» также содержал блок, являвшийся MDEF-ресурсом Mac OS и умел заражать её системные файлы. Однако его «миграция» с IBM-совместимого персонального компьютера на платформу Macintosh и обратно была практически невозможна, так как при запуске инфицированных файлов операционных систем DOS и Windows вирус не обращал внимания на файлы Macintosh, если они вдруг оказались на IBM-совместимом персональном компьютере. Примерно то же самое происходило и на Macintosh. По этому поводу специалисты-вирусологи не без доли юмора

[409] «Esperanto» (англ.) – «Эсперанто», универсальный язык общения.

говорили, что «заразить другую OS вирус в состоянии, видимо, только если пользователь скопирует его «руками»».

При запуске инфицированных файлов операционной системы DOS «Esperanto», не мудрствуя лукаво, перехватывал прерывание INT 21h и оставался резидентно в оперативной памяти DOS. После этого он заражал файлы при их запуске и при вызовах системных функций DOS «FindFirst» и «Next».

При запуске инфицированных файлов операционной системы Windows «Esperanto» не оставался в оперативной памяти резидентно, а искал файлы с расширениями «*exe.» и «*com.», заражал их и, после этого, возвращал управление программе-носителю. Причём при заражении файлов он проверял их внутренний формат и инфицировал разными способами, записываясь в конец файлов и изменяя их заголовки. Кроме того, в NE-файлах операционной системы Windows «Esperanto» создавал новую секцию, а в PE-файлах операционной системы Windows 32 дописывался к последней секции.

Во время запуска инфицированных файлов операционной системы Window32 вирус проверял системное время и в зависимости от его значения выводил стандартное окно сообщений, в котором отображался пространный текст на английском и испанском языках. В тело вируса вставлены строки, которые используются при заражении файлов операционной системы с Windows 32 расширением «*.exe»:

```
KERNEL32.DLL USER32.DLL GetModuleHandleA GetProcAddress MessageBoxA
CreateFileA CreateFileMappingA MapViewOfFile UnmapViewOfFile CloseHandle
FindFirstFileA FindNextFileA FindClose LoadLibraryA GetLocalTime
```

Совершенствование и популяризация технологий Интернет и, в частности, технология Internet Relay Chat (IRC)[410], вызвали пристальный интерес вирусописателей, поэтому появление новых, ориентированных на них вредо-

[410] Internet Relay Chat (IRC) (англ.) – (проф.) глобальная система, посредством которой пользователи могут общаться друг с другом в реальном времени, (жарг.) посиделки в Интернет.

носных компьютерных программ не заставило себя долго ждать, и они стали появляться одна за другой.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Acoragil
Другие названия	mIRC/Acoragil.a, mIRC.Acoragil
Тип	червь IRC
Инфицируемые платформы	Windows, UNIX, DOS
Впервые обнаружен	декабрь 1997 года
Страна происхождения	Соединённые Штаты Америки
Длина	1536

В декабре 1997 года компьютерное сообщество было проинформировано о «поимке» вредоносных компьютерных программ принципиально нового типа – червей mIRC, использовавших каналы IRC. Забегая немного вперёд, скажем, что компанией Microsoft в очередной версии утилиты эта «уязвимость» была устранена и первые, довольно-таки простые черви IRC, остались лишь в истории вирусописания.

Но идея запомнилась, и чуть позже появились уже многокомпонентные черви IRC, которые также, как и их «прародители», были нацелены на поражение управляющих файлов «script.ini», «events.ini» и т. д., но осуществляли свои действия наподобие червей для электронной почты, то есть потенциальной жертве присылался исполняемый файл с расширением «*.exe», «*.com», «*.bat» и т. д., который при запуске на выполнение поражал оригинальный управляющий файл.

Давайте рассмотрим обозначенную тему несколько подробнее. Итак, создание двух первых представителей червей IRC[411] относят к концу 1997 года. Оказалось, что мощная и разветвлённая система команд клиентов IRC, – версия клиента для операционной системы Windows, известная как mIRC, – содержала в себе опасную «уязвимость» в системе безопасности, позволявшую на основе их файлов сценария работы («скриптов») создавать компью-

[411] Первые два вируса этого типа получили названия «Acoragil» и «Simpsalapim» по используемым ими кодовым словам, так как непосредственно после ввода пользователем в текст сообщения «Acoragil» или «Simpsalapim» они автоматически отключали его от канала.

терные вирусы, которые были способны «перемещать» свой программный код на компьютеры пользователей сетей IRC по соответствующим каналам. Сама «уязвимость» заключалась в совпадении директория для хранения файлов, загружённых через IRC, с директорием, в котором размещался управляющий файл «script.ini». В результате компьютерный злоумышленник мог передать на удалённый компьютер файл «script.ini» (содержащий тело червя), который автоматически замещал оригинальный управляющий файл. Таким образом, при размножении черви пересылали командами mIRC свой код в файле «script.ini» каждому новому пользователю, который подключается к каналу.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Simpsalapim
Другие названия	mIRC/Simpsalapim.a, mIRC.Simpsalapim
Тип	червь IRC
Инфицируемые платформы	Windows, UNIX, DOS
Впервые обнаружен	декабрь 1997 года
Страна происхождения	Соединённые Штаты Америки
Длина	583

«Acoragil» по кодовым словам пересылал системные файлы операционных систем DOS, Windows или UNIX. Причём, обычно кодовые слова выбирались таким образом, чтобы не слишком бросаться в глаза пользователя, например: «hi», «cya» или определённый артикль английского языка «the». Интересно, что один из штаммов червя «Acoragil» пересылал компьютерному злоумышленнику файл паролей UNIX, а для захвата канала IRC червь «Simpsalapim» использовал троянскую часть своего кода, и если mIRC владельца канала был инфицирован, то после ввода кодового слова «ananas», компьютерный злоумышленник перехватывал управление каналом.

В целом можно констатировать, что принцип действия червей IRC был примерно одинаков. При помощи команд IRC «скрипт» автоматически посылался с инфицированного компьютера каждому вновь присоединившемуся к каналу пользователю. Присланный файл-сценарий замещал оригинальный, и при следующем сеансе работы уже вновь заражённый клиент рассылал червя

IRC, который использовал особенности конфигурации клиента (всех версий mIRC младше 5.31 и всех версий PIRCH до PIRCH98), вследствие чего принимаемые файлы всех типов помещались в корневой директорий клиента, а тот, в свою очередь, содержал также и основные «скрипты» клиента, включая автоматически загружаемые mIRC-«скрипты» «script.ini», «mirc.ini» и PIRCH-скрипт «events.ini». Данные «скрипты» автоматически исполнялись клиентом при старте и в дальнейшем использовались как основной сценарий его работы.

В результате проведённых в кратчайшие сроки ведущими отечественными и зарубежными специалистами-вирусологами исследований нескольких десятков различных «скрипт» червей, созданных с импользованием опыта «выпущенных» в сети первых двух червей IRC, оказалось, что они представляют собой достаточно простые компьютерные программы. Вместе с тем «безобидными» их никак не назовёшь, так как некоторые представители этого типа вирусов содержали «троянскую» начинку и, в соответствии с заранее заданными ключевыми словами, запускали деструктивные действия на инфицированных компьютерах пользователей.

С этой точки зрения весьма характерен появившийся несколько позже первый известный червь PIRCH под названием «Events»[412], который по определённой команде стирал все файлы на «жёстком» диске компьютера. Имея длину 1829 байт, он рассылал свои копии каждому пользователю, присоединившемуся к каналу, и по ключевым словам выполнял набор заданных вирусописателем действий: по команде «.query» проводил «проверку», по результатам которой определял, инфицирована или нет система, а по команде «exit» завершал работу клиента. По другим командам червь активизировал деструктивную функцию и стирал все файлы с логического диска C:, предоставлял

[412] «Events» (англ.) – «События». Другие названия: pIRCH.Events.a, pIRCH.Events, mIRC/Events.

компьютерному злоумышленнику удалённый доступ к информации на инфицированном компьютере и т. д.

В «скрипт» языках клиентов mIRC и PIRCH существовали операторы для запуска обычных команд операционной системы и исполняемых модулей (программ) операционных систем DOS и Windows. Эта возможность «скриптов» IRC послужила основой для появления «скрипт» червей нового поколения, которые помимо «скриптов» заражали компьютеры пользователей EXE-вирусами, устанавливали «троянских коней» и т. п. «Скрипт» черви работоспособны только в том случае, если пользователь разрешает копирование файлов из сети на свой компьютер. Данная опция клиентов IRC называется «DCC autoget» – получение файлов по протоколу DCC автоматически и без предупреждающего сообщения. При отключённой опции инфицированный файл принимается, помещается в директорий клиента и в следующем сеансе работы продолжает своё распространение. При этом пользователь не получает никаких предупреждающих сообщений.

Итак, в завершение нашего рассказа о ключевых событиях 1997 года подчеркнём, что количество разнообразных макро вирусов непрерывно росло и к концу года счёт пошёл на тысячи. Открыв новую страницу вирусописания в августе 1995 года с появлением компьютерного вируса «Concept», аккумулируя весь опыт, накопленный авторами вредоносных компьютерных программ за десятилетие непрерывной работы и совершенствования, макро вирусы, пожалуй, представляли собой наиболее масштабную проблему вирусологии того времени.

§18. 1998 год – совершенствование вирусов для 32-разрядных Windows, а также «троянских» программ и утилит скрытого администрирования продолжается. Они были первыми: макро вирусы для СУБД Access, для Access и Word одновременно, для PowerPoint, вирус-червь для платформ Power Macintosh, вирус-паразит на Java-файлах, HTML-вирус и Его Величество «Chernobyl»

- Выпущена операционная система Windows 98, в которую были встроены Internet Explorer 4.0, Outlook и поддержка нескольких мониторов, а также была улучшена поддержка универсальных драйверов и API DirectX.

- Выпущена операционная система Windows NT Server 4.0 Terminal Edition.
- Выпущена версия 2.1.110 операционной системы Linux. В процесс тестирования, программирования и обсуждения вовлечено около десяти тысяч программистов со всего мира.
- Выпущен микропроцессор Intel Xeon для высокопроизводительных серверов.
- Выпущен микропроцессор AMD K6.

В январе этого года, в рамках выполнения своего нового проекта по борьбе с вредоносными компьютерными программами – «VB 100%» – журнал Virus Bulletin на постоянной основе начал тестирование антивирусных средств. Целью данного проекта являлась оценка антивирусных программ по критерию эффективности обнаружения компьютерных вирусов, появление которых было зарегистрировано в «диком» виде. Впоследствии этот проект получил широкое признание компьютерного сообщества и, в частности, фирм-разработчиков антивирусных продуктов.

Идентификационная карточка вредоносной компьютерной программы	
Имя	DeTroie
Другие названия	Win32.HLLP.DeTroie, W95/HLLP.Detroie.D, W32/Cheval.gen
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	январь 1998 года
Страна происхождения	Франция
Длина	примерно 440 байт

Самое начало 1998 года ознаменовалось также появлением в «диком» виде, с последующей эпидемией, семейства вирусов под названием «DeTroie»[413], инфицировавших выполняемые файлы 32-х битных операционных систем Windows и, к тому же, обладавших способностью передачи компьютерному злоумышленнику информации о поражённом компьютере.

«DeTroie» был написан на языке программирования Delphi (Дэльфи) и заархивирован при помощи программы «PE-Pack». После проникновения в компьютерную систему пользователя при помощи традиционных каналов он

[413] «DeTroie» (фр.) – «Троянец». Известны также штаммы Detroie.C, Detroie.D, Detroie.E.

устанавливал себя резидентно в оперативную память, отслеживая и перехватывая функции операционной системы. В результате, каждый раз, когда операционная система или установленное на компьютере прикладное обеспечение пытались получить доступ к каким-либо из этих функций, вирус активизировался и инфицировал всё новые и новые файлы с расширением «*.exe».

Кроме того, семейство вирусов «DeTroie» обладало деструктивной функцией, состоявшей в том, что они стирали содержимое заражённых файлов, заменяя его собственным программным кодом. Таким образом, инфицированные файлы становились непригодными для выполнения и, более того, восстановлению не подлежали, а когда пользователь пытался открыть оригинальный файл, в действительности запускалась копия «DeTroie».

К счастью, вследствие использования вирусописателем специфических библиотек, присутствовавших только во французской версии операционной системы Windows, эпидемия не вышла за границы франкоговорящих стран.

Идентификационная карточка вредоносной компьютерной программы	
Имя	BackOrifice
Другие названия	BO, Backdoor.BO
Тип	«троянская» программа
Инфицируемые Платформы	Windows95/98/ME/NT /2000/XP
Впервые Обнаружен	январь 1998 года
Страна происхождения	Соединённые Штаты Америки
Длина	284160 байт

22 января 1998 года в США была обнаружена «троянская» программа, которая стала первым «троянским конём», дававшим возможность злоумышленникам управлять инфицированным компьютером на расстоянии, и получила красноречивое название «BackOrifice»[414]. Собственно говоря, «BackOrifice» представлял собой мощнейшую утилиту скрытого администрирования удалённых компьютеров и сетей, и недаром в одном из сообщений на принадлежащей хакерам Web-странице заявлялось: «… «BackOrifice» является системой удалённого администрирования, позволяющей пользователю контролировать компьютеры

[414] «BackOrifice» (англ.) – «Задний вход».

при помощи обычной консоли или графической оболочки. В локальной сети или через Интернет, BO предоставляет пользователю больше возможностей на удалённом Windows-компьютере, чем имеет сам пользователь этого компьютера».

Итак, «BackOrifice» являлся идеальным средством несанкционированного управления компьютером. Как правило, программа проникала в компьютер через электронную почту в виде вложенного исполняемого файла. Пользователь, поддавшийся привлекательному названию, например, «ознакомьтесь с новой версией … (далее, шло наименование программного продукта)» и по неосторожности запустивший этот файл, сам открывал прямой канал для внедрения «троянской» программы в его компьютер[415]. Интересно, что классифицировать «BackOrifice» как вредную «троянскую» программу позволила лишь её характерная особенность, которая заключалась в отсутствии предупреждения об инсталляции в компьютерную систему и запуске на выполнение.

При активизации «троянский» конь устанавливал себя в системе и затем постоянно отслеживал её функционирование, не выдавая легальному пользователю каких-либо сообщений или предупреждений о своём присутствии или деятельности. Между прочим, в списке активных приложений, которые пользователь может просмотреть при помощи системных средств, нет даже ссылок на «BackOrifice», и в итоге владелец компьютерной системы обычно не догадывался о присутствии нежелательного «гостя» – троянской программы, а в это время его компьютер оставался открытым для осуществления удалённого управления истинным «хозяином» – злоумышленником, внедрившим вредоносную программу в систему пользователя.

«BackOrifice» распространялся как пакет из нескольких прикладных программ и технической документации к ним. Все эти программы были

[415] Как раз из-за такого способа распространения эти программы получили название «троянский» конь. Об этом типе вредоносных компьютерных программ мы достаточно подробно говорили выше.

написаны на языке программирования «C++»[416] и откомпилированы в Microsoft Visual C++, имели формат «Portable Executable» (PE) и могли выполняться только в среде 32-разрядной операционной системы Windows. Основной программой в пакете являлась «boserve.exe», которая представляла собой «серверную» компоненту «BackOrifice» и работала в режиме ожидания вызовов от удалённых «клиентов». Второй программой являлась «boconfig.exe», которая конфигурировала «сервер» и по аналогии с компьютерными вирусами позволяла «прикрепить» «boserve.exe» к каким-либо другим файлам. При запуске таких приложений компьютерный вирус «выкусывает» их из инфицированного файла и запускает на выполнение без каких-либо побочных эффектов. В пакете также присутствовали ещё четыре программы: две «клиентские» утилиты (консоль и графический интерфейс), которые позволяли «клиенту» управлять удалённым «сервером», а также две утилиты компрессии (и декомпрессии) файлов, которые использовались для копирования файлов с или на удалённый «сервер».

При запуске «BackOrifice» создавал файл «windll.dll» в системном каталоге операционной системы Windows, определял адреса нескольких Windows API[417], искал свою копию в оперативной памяти и, обновляя свою версию, выгружал её оттуда, если она была обнаружена. Затем он копировал себя в системный каталог Windows и регистрировал в реестре как автоматически запускаемый процесс: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices. После выполнения указанных действий «BackOrifice» перехваты-

---

[416] «C++» – язык программирования высокого уровня, разработанный Бьёрном Страуструпом (Bjarne Stroustrup) в AT&T Bell Laboratories (Муррей-Хилл, Нью-Джерси) в 1983 году. Объединяет возможности языка Си с возможностями объектно-ориентированного програмирования.

[417] API (Application Programming Interface) (англ.) – интерфейс прикладного программирования.

вал один из сокетов[418] Windows (по умолчанию – 31337) и оставался в памяти этой операционной системы как приложение без активного окна и ссылки в списке приложений (так называемое скрытое приложение). Затем основная процедура перехвата сообщений ожидала поступление команд от удалённого клиента. Причём, сокеты команд передавались в зашифрованном виде. В зависимости от команды «BackOrifice» выполнял следующие действия:

отсылал злоумышленнику имена компьютера и пользователя, а также информацию о самой системе: тип процессора, размер памяти, версия системы, установленные устройства и т. д.;

давал разрешение на удалённый доступ к «жёстким» дискам;

искал файлы на «жёстких» дисках;

посылал или принимал файлы, уничтожал, копировал, переименовывал, а также исполнял любой файл;

создавал или уничтожал директории;

упаковывал или распаковывал файлы;

отключал текущего пользователя от сети;

«подвешивал» компьютер;

высылал список активных процессов;

выгружал указанный процесс;

подключался к сетевым ресурсам;

получал и отправлял кэшированные пароли (которые использовались пользователем в течение текущего сеанса), искал пароль для заставки экрана монитора – «ScreenSaver» (расшифровывал и отправлял);

выводил стандартные окна сообщений Windows;

читал или изменял системный реестр;

открывал или перенаправлял другие сокеты TCP/IP;

поддерживал протокол HTTP и эмулировал Web-сервер;

проигрывал звуковые файлы;

---

[418] Сокет (проф.) – технология, используемая для связи компьютеров в сетевой среде.

перехватывал, запоминал и потом отсылал строки, вводимые с клавиатуры в момент подсоединения компьютера к сети;

и т. д. и т. п.

Список можно продолжить, тем более что «BackOrifice» также позволял расширить список своих функций при помощи подключаемых им ресурсов – «plug-in»[419], которые могли передаваться на «сервер», устанавливаться на нём в качестве части «троянской» программы и в последующем выполнять фактически любые несанкционированные действия на инфицированном компьютере.

В завершение позвольте сформулировать несколько простых требований, которые помогут избежать проникновения в компьютерную систему «троянской» программы «BackOrifice» и подобных ей вредоносных компьютерных программ. Назовём их «правилом трёх «никогда»:

никогда не запускайте вложенные в сообщения электронной почты файлы (даже если они получены от знакомых лиц), предварительно не проверив их антивирусными средствами;

никогда не запускайте программы, полученные на мобильных накопителях (флоппи-дисках, CD-ROM, магнитооптике и т. д.) из источников, не заслуживающих доверия;

никогда и никому не сообщайте паролей доступа к компьютеру.

Практически следом за «BackOrifice» появилось несколько аналогичных программ скрытого администрирования компьютеров в сети с удалённого терминала: «NetBus», «Phase» и прочие. Все они в той или иной степени помогали компьютерному злоумышленнику брать под свой контроль компьютерные системы, в том числе просматривать содержимое «жёстких» дисков заражённого компьютера, копировать файлы, уничтожать конфиденциальные данные и т. п.

---

[419] Plug-in (англ.) (проф.) – подключаемая программа, дополнительный программный модуль (к существующей системе программного обеспечения).

Идентификационная карточка вредоносной компьютерной программы	
Имя	Paix
Другие названия	Macro.Excel4.Paix, Excel4.Paix, XF/Paix.A, Formula.Paix
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT/2000/XP/2003, MS-DOS
Впервые обнаружен	февраль 1998 года
Страна происхождения	Франция
Длина	1480 байт

В конце января – начале февраля 1998 года компания Network Associates первой сообщила о том, что во Франции был выявлен компьютерный макро вирус нового типа, названный «Paix»[420] и заражавший документы MS Excel версии 4.0 и более ранних. Отличался этот вирус от остальных макро вирусов для MS Excel использованным в нём языком программирования[421]. Автор вируса не использовал VBA, как в большинстве макро вирусов такого класса, вместо этого он применял язык Macro Formula 4.0 MS Excel 4. Интересно, что использованный метод инфицирования позволял заражать не только электронные таблицы унаследованных версий MS Excel, но и версий 5.0, 7.0, а также 97.

Итак, данный макро вирус для своего внедрения в электронные таблицы MS Excel использовал не обычную для вирусов область макросов, а формулы, которые, оказывается, также могли содержать самостоятельно размножающийся программный код. Иными словами, «Paix», в отличие от ранее известных вирусов, копировал себя не в листы макроопределений, а непосредственно в клетку электронной таблицы в виде формулы.

Наиболее частым каналом распространения вируса «Paix» являлась пересылка заражённых им файлов по Интернет, а размножался он способом, обычным для других вирусов под MS Excel, перехватывая системные собы-

---

[420] «Paix» (франц.) – «Покой», «Мир».

[421] В версиях MS Excel того времени использовались два макро языка: один на базе Visual Basic for Application (VBA), а второй был унаследован от более ранних версий MS Excel (вплоть до MS Excel 4.0).

тия (активизацию окна – «OnWindow») и копируя свой программный код в каждую активизируемую пользователем электронную таблицу.

В процессе первого открытия инфицированного файла вирус получал управление, проверял путь к текущему документу и, в зависимости от него, создавал файл-носитель с именем «xlsheet.xla» или в том же директории, или в директории C:\WINDOWS. Затем файл «xlsheet.xla» регистрировался как MS Excel «Add-In», после чего этот файл подгружался при старте самого MS Excel.

В результате после заражения MS Excel «Paix» оставался перманентно активным и инфицировал все открываемые и создаваемые электронные таблицы стандартным способом. Инфицированный файл содержал в себе текстовую строку: «Enfin la Paix ... !!! GO»[422]. Кстати, в случае попытки сохранения инфицированного файла MS Excel он предлагал пользователю сохранить его как файл по имени «Enfin la paix». Хотя вирус «Paix» и имел французское происхождение, на что ясно указывали имена процедур и язык текста, он представлял собой потенциальную угрозу для всех пользователей в мире, так как был способен размножаться в любой национальной версии MS Excel. Между прочим, первоначально даже сотрудники Symantec Antivirus Research Center[423] были введены в заблуждение и сообщали, что «вирус «Paix» воздействует только на франкоязычные версии MS Excel». Лишь после дополнительных исследований ими было установлено, что новый вирус работает и в англоязычных версиях MS Excel. Кроме того было установлено, что вирус действует только на версиях MS Excel для совместимых с IBM персональных компьютерах, а в MS Excel for Mac он не встречается.

«Paix» состоял из пяти процедур: «auto_ouvrir», «activation_feuille», «protect», «auto_fermer» и «!!! GO». Причём все перечисленные процедуры, за исключением последней, при активизации вызывали подпрограмму инфици-

---

[422] «Enfin la Paix ... !!! GO» (франц.) – «Наконец-то покой … !!! ВПЕРЁД».

[423] Symantec Antivirus Research Center (SARC) – Антивирусный исследовательский центр компании Symantec.

рования. Процедура «!!! GO» активизировалась и, в зависимости от системного счётчика случайных величин, с вероятностью 2% закрывала все открытые пользователем электронные таблицы, одновременно удаляя с экрана монитора все активные на данный момент элементы MS Excel[424], а также заменяла на экране монитора строку «Microsoft Excel» на «Enfin la Paix ...». Особо подчеркнём, что обычный пользователь не имел средств для обнаружения «Paix» в своей компьютерной системе, так как «увидеть» вирус при помощи обычных методов (например, просмотра макросов) было невозможно – «Paix» наделял свой модуль атрибутом «VeryHidden» («Полностью скрытый»), который не мог быть отменён из меню MS Excel. Поэтому для просмотра модуля вируса следовало написать специальную программу на встроенном языке MS Excel.

Однако на сей раз разработчики антивирусных средств среагировали оперативно и не дали эпидемии превратиться в пандемию, несмотря на то что такие предпосылки существовали, например, как мы уже указывали выше, ориентация автора «Paix» на использование такого эффективного канала распространения вируса как пересылка заражённых файлов по Интернет. Буквально в считанные дни та же корпорация Symantec опубликовала на своём Web-узле программу детектирования и лечения для нового типа вирусов электронных таблиц MS Excel.

В конце марта был обнаружен макро вирус «AccessiV»[425] – первый вирус для популярной «настольной» СУБД Access, так и не ставший по аналогии с вирусами «Concept» и «Laroux» предметом шквала публикаций в средствах массовой информации и пристального внимания всего компьютерного сообщества, так как привычка – великая сила, а все начали привыкать к тому, что прикладные программы, входящие в пакет MS Office от компании Mi-

[424] Кнопки на «ToolBar», меню, «StatusBar».

[425] В специальной литературе автором вируса называется шестнадцатилетний вирусописатель из Англии по имени Mark Watkin, создавший свою группу под названием «Diffusion Virus Team» («Команда распространения вирусов»).

crosoft, являются лакомым объектом для вирусописателей и последовательно сдают свои позиции, становясь жертвами атак со стороны вредоносных компьютерных программ.

Идентификационная карточка вредоносной компьютерной программы	
Имя	AccessiV
Другие названия	JetDB_Access-1, AccessiV.a, Strain
Тип	компьютерный вирус
Инфицируемые платформы	Windows 95/98
Впервые обнаружен	март 1998 года
Страна происхождения	Великобритания
Длина	1 модуль, 1 макрос

В целях обеспечения своей работоспособности «AccessiV» пользовался тем, что СУБД Access, так же как и другие прикладные программы пакета MS Office, поддерживала специальные программы – макросы, написанные на языке VBA[426]. И оказалось, что возможности этого языка, встроенного в MS Access, содержат всё необходимое для функционирования вируса: процедуры поиска файлов (баз данных MS Access) и создания в них новых макросов вируса. Тем не менее, специалисты-вирусологи отмечали, что «…скорее всего, вирусы нового типа не получат широкого распространения по той причине, что обмен базами данных MS Access происходит не так часто, как с документами MS Word или электронными таблицами MS Excel. Однако в пределах предприятия Access-вирусы могут принести немало хлопот пользователям и системным администраторам». Кроме того, следует отметить, что сама идея вирусов под MS Access стала довольно популярной в среде вирусописателей и, соответственно, компьютерные вирусы постепенно расширяли ареал своего обитания, поражая всё новые и новые операционные системы и приложения.

Итак, общую суть работы вируса «AccessiV», впрочем, как и других компьютерных вирусов, написанных под СУБД Access, можно, в общем случае, изложить следующим образом. Вследствие того, что MS Access является

[426] Напомним, что в принятой для СУБД Access терминологии «скрипты» называются макросами (macro), а макросы модулями (module).

частью пакета Office 97, вирусы под эту СУБД представляют собой такие же макросы на языке VBA, как и другие вирусы, заражающие прикладные программы Office 97. Вместе с тем, отличительной чертой следует признать то, что в данном случае вместо автоматических макросов в системе присутствуют автоматические «скрипты», которые вызываются системой в случае наступления определённых событий (в качестве конкретного примера, назовём «Autoexec»). Упомянутые «скрипты» способны впоследствии вызывать необходимые макро программы. Следовательно, при заражении баз данных MS Access вирусу необходимо заменить какой-либо автоматический «скрипт», и скопировать в инфицируемую базу данных свои собственные макросы. Ввиду того что язык «скриптов» недостаточно развит и в его состав не включены необходимые для этого функции, осуществить инфицирование «скриптов» без дополнительных макросов невозможно.

Таким образом, алгоритм работы «AccessiV» достаточно прост. При инфицировании в базе данных замещался «скрипт» «Autoexec» и в базу данных копировался дополнительный макрос с именем «Virus». В момент открытия заражённой базы данных управление передавалось на «скрипт» «Autoexec». В заражённых базах данных этот «скрипт» вызывал расположенную в макросе вируса функцию «AccessiV» и уже она искала файлы базы данных СУБД Access в текущем директории, инфицируя их. Сам поиск осуществлялся по маске «*.mdb».

Вирус «AccessiV» вёл себя в компьютерной системе латентно и никаких визуальных или иных эффектов в заражённой им компьютерной системе не вызывал, но его тело содержало следующий текст: «Find MS Database File! Find another MS Database File!» («Искать файл MS Database! Искать другой файл MS Database!»). Кстати, известный штамм этот вируса – «AccessiV.b» – был практически аналогичен «AccessiV», а незначительные отличия состояли в том, что в марте он выдавал на экран монитора в стандартном окне сообщений Windows следующий текст: «AccessiV – Strain B. I am the AccessiV virus, Strain B. Written by Jerk1N, of the DIFFUSION Virus Team. AccessiV was/is

the first ever Access Virus!!! («AccessiV – Штамм В. Я вирус AccessiV, Штамм В. Написан Jerk1N из Команды распространения вирусов. AccessiV был/есть первый вирус под Access!!!). Затем «AccessiV.b» создавал и запускал файл с расширением «*.com», инфицированный вирусом «Jerkin.443».

Под занавес рассмотрения компьютерного вируса «AccessiV.b» отметим, что в случае с MS Access задача создания антивирусных программ значительно усложнялась в силу того обстоятельства, что структура баз данных MS Access имела сложный формат (гораздо сложнее, чем форматы документов MS Word или таблиц MS Excel) и не существовало простых испытанных способов обнаружения и удаления вируса из базы данных. Мнение большинства ведущих специалистов-разработчиков антивирусных продуктов можно выразить следующим образом: «Лечение баз данных MS Access является более сложной задачей, чем удаление прочих макро вирусов, поскольку в случае с MS Access необходимо обезвредить не только вирусные макросы, но и автоматические «скрипты». А так как значительная часть работы MS Access возложена как раз на «скрипты» и макросы, то некорректное удаление или деактивация какого-либо элемента может привести к невозможности операций с базой данных, некорректное замещение автоматических «скриптов» может привести к потере данных, хранящихся в базе».

Примерно в то же время что и «AccessiV» был зафиксирован первый многоплатформенный, применявший «стелс» технологию макро вирус, получивший название «Cross»[427] и заражавший базы данных и документы сразу двух разных прикладных программ пакета MS Office: Access и Word[428].

---

[427] «Cross» (англ.) – «Гибрид».

По содержащемуся внутри вируса тексту автором «Cross» считается французский вирусописатель, который известен под псевдонимом VicodinES.

[428] Непосредственно за появлением «Cross» было выявлено несколько макро вирусов, способных переносить свой программный код из одного продукта MS Office в другое.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Cross
Другие названия	Macro.Access/Word97. Cross
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98
Впервые обнаружен	март 1998 года
Страна происхождения	Франция
Длина	550 Кбайт

По признанию специалистов состоящая из двух частей общая структура этого вируса была далека от банальной, а размер исходных кодов просто впечатлял, составляя: часть MS Word – около 150 Кбайт и часть MS Access – примерно 400 Кбайт. Этот вирус был обнаружен на одном из Web-узлов и прислан для исследований в одну из ведущих уже тогда отечественных компаний-разработчиков антивирусных программ – «Лабораторию Касперского», в виде двух заражённых файлов: базы данных MS Access и документа MS Word. В каждом из этих двух файлов присутствовало по одной копии вируса, которая размножалась либо в среде MS Word либо в среде MS Access: вирус из документа MS Word заражал документы текстового процессора, а вирус из базы MS Access заражал другие базы этой СУБД. Итак, вирус «Cross» обладал возможностью переноса инфицированных файлов из MS Word в MS Access и обратно.

Проведённые вирусологами исследования показали, что у обеих частей «Cross» одинаковая структура и каждая из них состоит из трёх блоков: процедуры заражения «родных» файлов («Infect»), подпрограммы переноса в другое приложение MS Office («Transfer») и блока шестнадцатеричных данных (BIN). Причём блок BIN в обеих частях вируса содержал в себе данные, которые использовались для заражения «чужого» приложения MS Office, то есть в части вируса под MS Word блок BIN содержал упакованный вирус для MS Access и, наоборот, блок BIN в части вируса под MS Access содержал упакованный вирус для MS Word. Шестнадцатеричные данные в блоке BIN содержались в «стандартном» для макро вирусов формате, позволявшем записать их на «жёсткий» диск и конвертировать в файл при помощи утилиты «Debug» операционной системы MS-DOS. Следует отметить, что данные в

блоке BIN были упакованы в формате MS «Cabinet», и вирусу дополнительно требовалось провести распаковку этих данных при помощи стандартной утилиты MS Extract. Распаковка блоков BIN в обеих частях вируса давала два инфицированных файла: базу данных MS Access (которой вирус MS Word заражает MS Access) и документ MS Word (которым вирус Access заражает MS Word). Обе новые копии вируса также способны размножаться в «родной» среде и записывать инфицированные файлы в «чужую» прикладную программу MS Office. Однако в обоих случаях код вируса в новых заражённых файлах не полностью совпадал с «родителями»: процедуры «Infect» и «Transfer» идентичны, однако полученная пара содержит отличный от «родительского» блок BIN.

Изучение вирусологами очередного уровня шестнадцатеричных данных показало, что в них присутствует ещё одна пара заражённых файлов – база данных MS Access и документ MS Word, но, в отличие от предыдущих вирусов, эта пара не может переместить свой программный код из MS Access в MS Word и обратно, размножаясь только в «родной» среде. Таким образом, первоначальной паре инфицированных файлов было дано определение – «матрёшка»: внутри вируса лежит ещё один, который в свою очередь содержит третий вирус:

Различия между частями вируса для MS Access различных уровней состояло только в блоке BIN, а процедуры «Infect» и «Transfer» полностью идентичны (такое же утверждение было признано справедливым для вирусов под MS Word), за исключением вируса последнего уровня, в котором отсутствует «Transfer» и BIN. Кроме того, проследив развитие частей вируса «Cross» снизу вверх, специалисты отметили, что результирующая пара частей вируса получена двухшаговым «усовершенствованием» изначальных вирусов третьего уровня: к ним была добавлена процедура «Transfer» и дописан блок BIN. С результатом такого «усовершенствования» (с вирусами второго уровня) была проделана аналогичная операция и, в результате, появи-

лась пара частей вируса аналогичная той, которая затем и была обнаружена в Интернет и прислана для исследования специалистами.

Анализ программного кода позволил утверждать, что методы размножения в «родном» приложении (блоки «Infect») ранее уже встречались в других вирусах. В случае части вируса под MS Word его процедура заражения использовала функции «Import/Export» языка VBA MS Office97: при помощи функции «Export» вирус записывал свой исходный текст в дисковый файл, а функцией «Import» вставлял его в открытые документы. Вирус под MS Word содержал один модуль с именем «X», в котором было обнаружено десять процедур: «AutoOpen», «AutoClose», «AutoExit», «AutoExec», «FindAx», «MakeBat», «DropKey», «DropDetox», «CheckKey» и «Info». Причём, процедура заражения содержалась в «AutoOpen», которая также удаляла пункты меню «Tools/Macro» и «Tools/Templates and add-ins» (технология «стелс»). Процедура «FindAx» искала MS Access в директории C:\ProgramFiles\MicrosoftOffice\Office\ и заражала его частью вируса под MS Access. Прочие процедуры при активизации вызывали «AutoOpen» (инфицирование), а процедура «Info» содержала следующие строки текста:

Cross.Poppy Word Component --[Cross is a blend of SexR-1 and Detox]-- by VicodinES/Sin Code IV (same person – mixed up letters)	Cross.Poppy элемент Word --[Cross это смесь SexR-1 и Detox]-- от VicodinES/Sin Code IV (персона та же – буквы перепутаны)

Кроме того, было установлено, что часть вируса для «Access» при размножении использовала методы, ранее обнаруженные в вирусе «AccessiV»: поиск файлов по маске «*.mdb» в текущем директории и дописывание в них своего программного кода; а также поиск установленного MS Word в директории C:\ProgramFiles\MicrosoftOffice\Office\ и инфицирование его частью вируса для MS Word. При заражении MS Word из MS Access вирус «Cross» создавал в директории автоматического запуска MS Word инфицированный шаблон «data.dot» (запакованный в блок BIN). Он копировал этот шаблон в два директория: C:\Progra~1\Micros~1\Office\Startup и C:\Progra~1\Micros~2\Office\Startup. Если эти директории отсутствовали, ви-

рус не мог заразить MS Word. При последующей загрузке MS Word заражённый «data.dot» автоматически загружался в оперативную память и часть вируса под MS Word получала управление.

Результирующий вирус под MS Access (вирус первого уровня) содержал программистскую ошибку: данные в блоке BIN перекрывали 64 Кбайта и при их конвертировании в файл на «жёстком» диске утилитой «Debug» происходила потеря части информации. В результате MS Access вирус первого уровня принципиально не мог инфицировать MS Word, однако вирус второго уровня не содержал этой ошибки, и заражение происходило «правильно». Добавим, что MS Access вирус первого уровня при некоторых системных условиях не мог размножаться даже в «родной» среде – это происходило при выполнении одной их функций MS Access и, в результате, выдавалась ошибка о нехватке оперативной памяти. В «Лаборатории Касперского» эта ошибка проявлялась на тестовом компьютере с установленными 24 Мб оперативной памяти, но на компьютере с 64 Мб оперативной памяти вирус размножался без каких-либо ошибок.

При заражении MS Access из части вируса под MS Word на «жёстком» диске создавался инфицированный файл «data.mdb» (база данных MS Access), а затем, командой «Start» вирус запускал MS Access и передавал ему файл «data.mdb» в качестве параметра. В результате MS Access загружал заражённый файл, вирус получал управление и инфицировал другие базы данных MS Access.

Иногда специалисты-вирусологи предлагают считать 1998 год неофициальным годом начала создания «виртуального оружия второго поколения», а виновником признаётся подававший большие надежды в области программирования двадцатичетырёхлетний студент пятого курса тайваньского Технологического института Tatung, который обладал необходимыми знаниями для написания 32-х разрядных приложений Windows на языке программирования Ассемблер и, к тому же, каким-то образом получил доступ к недокументированным особенностям MS Windows 95.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Chernobyl
Другие названия	CIH, CIH.C, CIHV, PE_CIH, W95/CIH-10xx, Tshernobyl, CIH.1019, W95/CIH.1003, PE/CIH; Win95.CIH, W95/CIH, Win32.CIH, Spacefiller, Spacefiller
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME
Впервые обнаружен	апрель 1998 года
Страна происхождения	Тайвань
Длина	около 1 Кбайта

В первом семестре 1998 года вирусописатель трудился, «не покладая рук», и вирус у него, как подчёркивают специалисты, получился великолепный: «компактный, рационально написанный и тщательно отлаженный. Настолько тщательно, что на заражённой машине он был практически незаметен». И вот апофеоз славы – летом 1998 года все антивирусные компании и службы мира сообщают о новом вирусе, выпускают предупреждающие пресс-релизы и вносят его в базы данных своих антивирусных программ. В России дошло до того, что осенью 1998 года чуть ли не каждый второй (!) CD-ROM, сфабрикованный отечественными компьютерными пиратами, содержал программы, заражённые этим вирусом.

Впрочем, давайте обо всём по порядку. Этот чрезвычайно опасный компьютерный вирус, наиболее широко известный сейчас, в том числе и в России, под именем «Chernobyl»[429], был впервые обнаружен в апреле 1998 года в г. Тайбей, административном центре провинции Тайвань, Китай. Как сообщало информационное агентство Associated Press «в соответствии с официальным заявлением властей Тайбея автором этого вируса был студент-старшекурсник Чен Инг-Хау (Chen Ing-Hau)», и поэтому первоначально его творение вошло в историю вирусописания под именем «CIH», которое является производной от инициалов вирусописателя и употребляется достаточно часто до сих пор. Для своего распространения вирус использовал различные средства и каналы передачи, но не применял какие-нибудь специфические

[429] «Chernobyl» (англ.) – «Чернобыль».

способы. Однако до появления вируса «Chernobyl» считалось, что максимум, что могут «натворить» компьютерные вирусы – это повредить информацию на «жёстком» диске, но никак не аппаратную часть компьютера, а этот вирус оказался первым, который поражал программу BIOS-setup и тем самым выводил из строя сам компьютер[430].

«Chernobyl» представлял собой деструктивный вирус, который мог разрушать данные, и пользователи, которые загружали свои компьютерные системы 26 апреля, теряли всю свою информацию[431]. Интересно, что первыми распространителями и, одновременно, одной из первых жертв этого вируса стали несколько групп компьютерных пиратов, которые занимались нелегальным тиражированием компьютерных игр через Интернет[432]. В результате «Chernobyl» очень быстро распространился по всему миру и, по некоторым оценкам, например, только в Южной Корее было выведено из строя более одного миллиона компьютеров, а общий ущерб превзошёл 250 млн. долл. Хотя этот вирус уже более чем «старый», специалисты компании Symantec до последнего времени предупреждали пользователей, что «… вирус «Chernobyl» всё ещё может где-то существовать в «диком» виде и нанести непо-

---

[430] В некоторых случаях для восстановления работоспособности компьютера требовалась замена материнской платы.

[431] Так как 26 апреля в тот год приходилось на воскресенье, многие организации в этот день просто не включали компьютеры, но всё равно «Chernobyl» исхитрился нанести ощутимый ущерб. Впрочем, он не носил такого глобального характера, как в следующем году.

[432] Первой жертвой вируса были несколько испорченных институтских компьютерных систем, после чего он «угомонился» и перешёл в стадию естественного размножения. Автора вируса вычислили, но он отделался выговором, его не исключили из учебного заведения и не стали подвергать судебному преследованию. В итоге Чен Инг-Хау успешно закончил обучение, а затем отправился на обязательную срочную двухлетнюю службу в армию Тайваня. Позднее декан факультета Ли Чи-Чен, на котором учился Чен Инг-Хау, объяснил представителю Associate Press мягкость наказания тем, что: «Чен Инг-Хау просил студентов не распространять его вирус».

правимый ущерб компьютерам пользователей, которые применяют либо устаревшие антивирусные средства, либо вообще их не используют».

Итак, «Chernobyl» инфицировал выполняемые файлы с расширением «*.exe» 32-х разрядных операционных систем Windows 95/98/ME и мог нормально функционировать только под указанными операционными системами, то есть и был неработоспособен под Windows NT и Windows 2000. Он заражал программы под операционными системами Windows 95/98 и ME, оставаясь резидентно в оперативной памяти компьютерной системы. Несмотря на то, что файлы Windows NT не могли быть инфицированы, так же как и файлы на компьютерах, работающих под управлением Windows 2000, вирус мог резидентно оставаться в оперативной памяти этих операционных систем. Вирус «Chernobyl» был недееспособен на компьютерах, работающих под управлением операционных систем DOS и Windows 3.x, а также компьютерах платформы Macintosh. Благодаря необычному способу заражения, применённому в этом вирусе, инфицированные «Chernobyl» файлы могли иметь тот же самый размер, что и оригинальные: вирус скрупулёзно искал пустые, неиспользуемое участки в файле, затем он «расчленял» себя на маленькие частички и вставлял эти фрагменты программного кода внутрь заражаемых файлов на неиспользованное пространство.

Примерно до середины 1999 года стало известно три очень похожих штамма вируса «Chernobyl», которые принято обозначать как «Chernobyl» v.1.2, v.1.3 и v.1.4[433]. Первые две версии активизируются при загрузке компьютерной системы 26 апреля – эта дата приурочена к катастрофе на Чернобыльской атомной электростанции в г. Чернобыль (СССР), которая произошла 26 апреля 1986 года. Третья версия вируса – 1.4, активизировалась при загрузке 26 числа любого месяца, в том числе и апреля.

[433] Первая версия вируса «Chernobyl» v.1.1 осталась у его автора, никогда не распространялась, и поэтому отсчёт ведётся со второй версии – v.1.2.

Процесс загрузки у всех трёх версий вируса «Chernobyl» был идентичен. Во время первой загрузки «жёсткий» диск перезаписывался случайными данными[434], и процесс начинался с самого начала «жёсткого» диска (сектор 0), продолжаясь по бесконечному циклу. Перезаписывание секторов «жёсткого» диска выполнялось безостановочно до тех пор, пока не происходил аварийный отказ системы. В результате компьютер переставал загружаться как с «жёсткого» диска, так и с системных флоппи-дисков или CD-ROM. К тому же данные, которые были перезаписаны на «жёстком» диске, было либо очень трудно, либо попросту невозможно восстановить, и их полное восстановление было реально только с резервной копии. В процессе второй загрузки «Chernobyl» инициировал постоянные попытки нанесения неустранимых повреждений компьютерной системе. Во время этой загрузки им проводились атаки на Flash BIOS (часть компьютера, которая инициализирует и управляет взаимосвязями и потоками данных между системными устройствами, включая «жёсткий» диск, последовательный и параллельный порты, а также клавиатуру. Именно Flash BIOS отвечает за загрузку компьютера и его взаимодействие с периферией) и осуществлялись попытки разрушения всех хранящихся там данных. В итоге, когда пользователь пытался загрузить компьютер, он не получал никакой информации на экране монитора (эффект «чёрного экрана»), и устранить эту проблему мог только квалифицированный технический специалист.

После заражения компьютера вирусом «Chernobyl» возникали следующие визуальные эффекты:

когда компьютер загружался, на экране монитора появлялось следующее сообщение: «DISK BOOT FAILURE, INSERT SYSTEM DISK AND PRESS ENTER» («Неисправный загрузочный диск, вставьте системный диск и нажмите ввод»)

---

[434] Через механизм VxDCall записывает на «жёсткий» диск случайную информацию, уничтожая главную загрузочную запись, загрузочные сектора обеих таблиц FAT и отдельные фрагменты данных, а также портит содержимое Flash BIOS материнских плат.

MS Access → MS Word → MS Access
MS Word → MS Access → MS Word
MS Access →
MS Word →
MS Access
MS Word →
MS Access →
MS Word

– это сообщение показывало, что компьютер не может загрузиться, а причиной служило произведённое вирусом форматирование «жёсткого» диска;

если компьютер загружался с диска отличного от C: и дисковод C:/ был доступен, то на экране монитора появлялось следующее сообщение: «INVALID DRIVE SPECIFICATION» («Неисправный дисковод») – это означало, что система не может распознать «жёсткий» диск, потому что информация на нём уже полностью стёрта.

Инфицирование компьютерной системы «Chernobyl» производил в соответствии со следующим алгоритмом:

резидентно устанавливался в оперативную память компьютера;

отслеживал, когда файл с расширением «*.exe» запускался на выполнение[435];

инфицировал файлы с расширением «*.exe», не вызывая каких-либо подозрений у пользователя, так как инфицированные файлы не изменяли свой размер (в этих целях, как мы уже отмечали, вирус помещал свой программный код на неиспользуемых участках внутри этих файлов – файлы с расширением «*.exe» в формате PE (Portable Executable) содержат достаточно много пустого пространства и по этой причине «Chernobyl» использует их в качестве мишени);

[435] Для этого он захватывал так называемую «монтируемую файловую систему» – IFS (Installable File System).

на компьютерах под управлением операционных систем Windows 2000 Pro и Windows NT «Chernobyl» устанавливал себя в оперативную память каждый раз, когда заражался запущенный на выполнение файл с расширением «*.exe»;

заражал все доступные пользователю файлы с расширением «*.exe» или систему в компьютерах под управлением операционных систем Windows 98 and Windows 95.

Итак, в апреле 1998 года была зарегистрирована первая эпидемия вируса «Chernobyl», начало которой произошло на Тайване, где неизвестные компьютерные злоумышленники разослали инфицированные файлы в местные конференции Интернет и сообщения о заражении компьютерных систем поступали сотнями. По данным компании Trend Micro вирус «мгновенно» выбрался за пределы Тайваня, вызвав эпидемии в Китае и Гонконге, стал распространяться по миру с ошеломляющей скоростью и был обнаружен ещё в нескольких странах Юго-восточной Азии, а затем перекочевал в Россию, причём сообщения поступали сразу из различных городов. Всего лишь через неделю после этого его эпидемии были зарегистрированы в Японии, Корее, Австрии, Австралии, Израиле и Великобритании. В течение нескольких последующих недель «Chernobyl» распространился буквально по всему миру, и эпидемии были зарегистрированы практически во всех странах Восточной и Западной Европы (Франции, Германии, Норвегии, Румынии и т. д., в частности, очень серьёзно пострадала Швеция), а также Северной и Южной Америке и ЮАР. Можно сказать, что вспыхнувшая на Тайване эпидемия быстро превратилась в массовую, а затем плавно переросла в пандемию. Сообщения о заражении компьютерных сетей, а также персональных компьютеров, стали исчисляться тысячами.

В мае «Chernobyl» проявил себя уже в США, где по халатности заражёнными оказались сразу несколько популярных Web-серверов, распространявших заражённые им игровые программы. Вероятнее всего, именно эти файлы на игровых серверах послужили и причиной повальной эпидемии

макро вируса «Word» в Северной Америке – то ослабевавшей, то вспыхивавшей в течение нескольких лет[436]. Жертвами вируса стали не только единичные пользователи, неосторожно установившие программное обеспечение с инфицированного Web-узла или CD-ROM, но и целые компании. Двадцать шестого июля 1998 года «Chernobyl» поразил в США несколько тысяч персональных компьютеров. Стюарт Хэнли, вице-президент по международным операциям компании Ontrack Data, дал следующий комментарий: «Я был удивлен, когда в середине дня начали поступать звонки. Если честно, я и не предполагал, что мы с этим столкнёмся. Может быть, неожиданным это оказалось потому, что 26 число прошлого месяца пришлось на воскресенье. 26 июля была среда – для большинства это обычный рабочий день… Домашним пользователям восстановление информации обойдётся в сумму от 400 до 1100 долл., в зависимости от «размеров бедствия». Для организаций, в которых поражено несколько персональных компьютеров, предусматриваются скидки».

К концу 1998 года стало практически невозможно подсчитать общее количество поражённых компьютеров, количество выброшенных плат и другие материальные потери, так как слишком велик был поток обращений пострадавших пользователей в различные антивирусные компании и сервис-центры. В первом приближении о масштабах заражения компьютеров вирусом «Chernobyl» можно судить, например, по данным британского журнала «Virus Bulletin»: этот вирус стабильно входил в десятку самых распространённых в мире. В России, по данным «Лаборатории Касперского», вирус также был среди самых распространённых, а специальное исследование положения дел, проведённое 29 ноября 1998 года на радио рынке в Митино совместно с московским представительством компании Microsoft, показало,

---

[436] По результатам многочисленных рейтингов распространённости и нанесённого ущерба «Chernobyl» уверенно опережал такие знаменитости как вирусы «Concept», «Word» или «Excel.Laroux».

что 14 из 20 (или 70% !!!) закупленных пиратских CD-ROM, были инфицированы какой-либо из версий вируса.

Кроме всего прочего, вирус «Chernobyl» был обнаружен в пиратских копиях программного обеспечения, распространяющегося по конференциям FIDO и Интернет; инфицированные им файлы были обнаружены и на нескольких российских Web-сайтах. Заражёнными оказались копии программ нескольких партий CD-ROM, причём не пиратских. Одна из фирм-разработчиков программных продуктов сообщила о том, что обнаружила вирус на последней стадии тестирования своего программного обеспечения, то есть непосредственно перед изготовлением мастер-диска.

Таким образом, пользователи операционной системы Windows подверглись реальной опасности инфицирования своих компьютеров, особенно в случае использования программного обеспечения, полученного из непроверенных источников. Естественно также, что те пользователи, которые использовали устаревшие антивирусные программы или совсем их не применяли, каждый месяц 26-го числа рисковали потерять не только программы, установленные на «жёстком» диске компьютера, но и некоторые компоненты аппаратного обеспечения. Поэтому фирмы-разработчики антивирусных средств настоятельно рекомендовали всем без исключения пользователям не полениться и заменить свои программы и их версии на самые свежие продукты.

В начале апреля 1999 года компания IBM объявила о том, что несколько тысяч персональных компьютеров «Aptiva» моделей 240, 301, 520 и 580, выпущенных в период с 5 по 17 марта и проданных в США, в процессе производства оказались заражены вирусом «Chernobyl». Представительница корпорации IBM Стэйси Пина сказала: «Это произошло из-за ошибки оператора. Вирус попал в компьютеры через проверочные дискеты и не был обнаружен, так как оператор своевременно не обновил антивирусное программное обеспечение на сервере, используемом для копирования программ... То, что произошло, – недочёт производственного процесса. У нас очень высокое

качество контроля. Виноват конкретный работник». Следует отметить, что это не последний случай непреднамеренного распространения вируса фирмами-производителями. Например, в июле 1999 года группа разработчиков «Cult of the Dead Cow» распространила CD-ROM со своей разрекламированной программой Back Orifice 2000, заражённый вирусом «Chernobyl».

Через год после появления вируса «Chernobyl», 26 апреля 1999 года, сработала «логическая бомба», заложенная в его программный код, и её «взрыв» превзошёл все самые смелые ожидания. По различным оценкам, в этот день по всему миру пострадало около полумиллиона компьютеров. У некоторых из них оказались уничтоженными данные на «жёстких» дисках, а у других ещё и испорчены микросхемы на материнских платах. Данный инцидент тогда стал настоящей компьютерной катастрофой, так как эпидемии компьютерных вирусов и их последствия никогда ранее не были столь сокрушительными, масштабными и убыточными. По сообщению радиостанции «Эхо Москвы» в России вирус «Chernobyl» поразил более 100 тысяч компьютеров. 27 апреля были парализованы локальные сети многих российских и крупных зарубежных коммерческих и государственных организаций, банков, органов безопасности, информационных агентств и т. д.

Например, в Екатеринбурге был сорван выпуск нескольких электронных газет, а в Воронеже была приостановлена работа местной телерадиокомпании и компьютерной сети УВД, где хранится сверхсекретная информация о преступном мире Черноземья. Правда в Информационном центре УВД, ни одна база данных не пострадала. Во-первых, сверхсекретная информация хранится в локальных сетях, куда никакая почта не проникнет, а во-вторых, воронежские милиционеры оказались готовы к вирусному «вторжению» и приняли все меры для нормальной работы компьютеров. Правда, «пострадавшие» все-таки есть. Например, «завис» компьютер в пресс-службе УВД и в некоторых других подразделениях, которые не были готовы к атаке вируса «Chernobyl». Всего же число жертв вируса в Воронеже перевалило за сотню. С утра понедельника 26 апреля в ведущих сервисных центрах Воронежа ца-

рил необычный ажиотаж. Владельцы «персоналок», как частные лица, так и представители солидных организаций, со всех концов города везли свои внезапно переставшие работать компьютеры.

Итоги «вирусной атаки» в другом областном центре Черноземья – Белгороде, выглядели следующим образом. 26 апреля владельцы оргтехники буквально атаковали сервисные центры города. Все сдаваемые в ремонт компьютеры оказались заражёнными вирусом «Chernobyl» и при включении машины просто не желали загружаться. По официальным данным, таких компьютеров насчитывалось более 200 штук, и наиболее уязвимой оказалась сетевая техника. Серьёзно пострадала компьютерная база Белгородской технологической академии строительных материалов и одного из крупных коммерческих банков города. Многие из пострадавших пытались самостоятельно бороться с вирусом, поэтому точных данных о количестве «пострадавших» нет. Наиболее вероятным и опасным путём распространения компьютерных вирусов в Белгороде признаны контрафактные CD-ROM с программным обеспечением и играми, а также сеть Интернет – особенно из-за любителей посещать порнографические и «хакерские» Web-сайты.

Количество телефонных звонков и обращений по электронной почте, поступивших от пострадавших пользователей в московский офис «Лаборатории Касперского», превысило две сотни. Количество «умерщвлённых» и пострадавших компьютеров в каждом случае колебалось от одного до нескольких десятков и даже сотен. Специалисты Лаборатории Касперского подсчитали, что 26 числа в головной офис компании поступила информация об одной тысяче разрушенных компьютеров. Евгений Касперский по этому поводу заявил: «Естественно предположить, что лишь около одного процента пострадавших пользователей позвонили непосредственно нам. Подавляющее большинство обращалось в местные компьютерные технические центры или самостоятельно восстановило разрушенные компьютеры. Учитывая это, можно утверждать, что по России в этот день от вирусной эпидемии пострадало не менее ста тысяч компьютеров. Оценить материальный ущерб, видя

такие громадные цифры, я просто не берусь. Также не берусь оценить количество компьютеров, пострадавших во всём мире. Если даже российский парк компьютерной техники оценить как два-три процента от мирового, то это число может возрасти до шестизначных цифр».

Информационное подразделение ЗАО «ДиалогНаука» 27 апреля 1999 года сообщало: «Служба технической поддержки ЗАО «ДиалогНаука» за 9 часов работы с утра 26 апреля получила около 500 звонков и свыше 100 электронных писем из более чем 20 городов России о случаях срабатывания вируса. За последние несколько лет это самый крупный случай срабатывания компьютерного вируса, к тому же приводящий к потере данных и временному выводу из строя компьютеров… Восстановление данных на дисках практически невозможно. В любом случае, в результате этих операций компьютер не грузится, и зачастую это выглядит как поломка. В службу технической поддержки фирмы «Красная волна», занимающейся сборкой и продажей компьютеров, за первую половину дня 26 апреля 1999 года обратились более 50 клиентов, которые были уверены, что у них вышел из строя блок питания».

Вы, конечно, помните известную пословицу: «Кому война, а кому и мать родна!» Видимо, сообразуясь с ней, и живёт некий субъект, которому абсолютно безразлично когда, как и над чем «хохмить». Мы имеем в виду следующую историю. В адрес ZD Net Россия пришло письмо от Игоря Панасенко, системного администратора фирмы ЛЭНК (г. Апатиты Мурманской обл.) со следующей информацией: «3 июля не выявленные пока злоумышленники разослали письмо, начинающееся словами: «Дорогой Друг! Лаборатория Касперского разрабатывает новую систему доставки бесплатных модулей». Тема письма: «AVP предупреждает и защищает от вирусов!!!» В письмо был вложен архив Nocih.zip, содержащий исполняемый модуль Nocih.exe, и «Лаборатория Касперского» действительно разработала бесплатную утилиту с таким именем, предназначенную для борьбы с вирусом «Chernobyl». Однако вложенная в письмо утилита отличалась от оригинальной тем, что была

заражена «троянским конём» «Coced.227», ворующим пароли Windows. В письме были указаны настоящие адрес и телефоны «Лаборатории Касперского», но подлог выдавал неверный адрес электронной почты: avp_lab@mail.ru». Комментируя эту ситуацию менеджер «Лаборатории Касперского» по работе с партнёрами OEM Олег Линник рассказал, что «в последнее время участились случаи рассылки так называемых «троянских коней». За прошлый месяц от имени компании подобные письма рассылались трижды, однако злоумышленники до сих пор не найдены. «Лаборатория Касперского» никогда не занималась, и не будет заниматься подобного рода рассылками, – заявил он. – Мы всеми возможными способами боремся с компьютерными пиратами, использующими наше имя». Почему-то думается, что автор вируса «Chernobyl» по-своему порядочнее, чем автор приведённой фальшивки!

Кроме России из стран СНГ наиболее активно вирус «Chernobyl» проявил себя на Украине. В Киеве первый пострадавший от воздействия данного вируса принёс свой компьютер в сервисный центр «ЕПОС» уже в 9 часов утра. К обеду в сервисном центре ждало своей очереди 28 «жёстких» дисков, а прошивка нового BIOS производилась, как на заводском конвейере. Одного специалиста пришлось выделить специально только для того, чтобы отвечать на телефонные звонки по «горячей линии», которые продолжались до девяти часов вечера. Что же произошло? Собственно, то, что и ожидалось, так как эпидемия началась уже давно. В последнее время большинство компьютеров, поступавших в сервисный центр вследствие различных поломок, было, ко всему прочему, еще и заражено вирусами (в том числе и «Chernobyl»). Так что 26 апреля разрушающая способность вируса лишь активизировалась, и нельзя сказать, что знавшие об угрозе специалисты молчали о ней. Многие фирмы в Киеве, в том числе и «ЕПОС», давно предлагали в качестве одной из своих услуг регулярное проведение антивирусного контроля. Вопросы борьбы с вирусами регулярно поднимались на страницах компьютерных журналов. Например, 1 марта вышел третий номер журнала «CHIP» с об-

ширным материалом по компьютерной вирусологии, который начинался подборкой с напоминанием об опасных свойствах как раз вируса «Chernobyl». Здесь же приводились подробные рекомендации о том, как избежать вирусной атаки, но «пока гром не грянет, мужик не перекрестится!»

Во всю свою мощь «Chernobyl» развернулся в Азии и на Ближнем Востоке, где эта деструктивная компьютерная программа по состоянию на 27 апреля 1999 года уничтожила данные, хранящиеся на «жёстких» дисках сотен тысяч компьютеров. Удар был нанесён в понедельник в тринадцатую годовщину разрушения ядерного реактора, и администраторы компьютерных сетей в этих регионах приступили к оценке обстоятельств и устранению последствий произошедшего. В то же время вирус нанёс ущерб и другим частям мира, например, США, Европе. Однако там удар был смягчён благодаря тому, что за время, прошедшее с момента появления вируса «Chernobyl», многие компании, – парк компьютеров которых составляли работающие под управлением операционных систем Windows 95 и Windows машины, – предприняли комплекс защитных мероприятий, в том числе, установили новые антивирусные средства[437]. В большинстве случаев в Азии и на Ближнем Востоке необходимость подобных мероприятий была попросту оставлена без внимания. Кроме того, мы знаем, что «Chernobyl» часто использовал для своего распространения пиратские копии программного обеспечения, которое процветает в этих регионах мира[438].

---

[437] Судя по различным сообщениям из США, на этот раз было поражено примерно 10 тыс. систем, а общий ущерб составил сотни миллионов долларов. Например, по сообщению, информационного портала Infoart, только в группу реагирования на нарушения компьютерной защиты (Computer Emergency Response Team) Университета Карнеги-Меллона поступило 228 сообщений о заражении в общей сложности 2328 компьютеров.

[438] По оценкам Теда Ло, директора тайского системного интегратора Tygre Systems, более 20% всех CD-ROM в Тайланде заражены вирусом «Chernobyl».

Список стран Азии и Ближнем Востока, наиболее пострадавших от вируса «Chernobyl» 26 апреля 1999 года, можно представить следующим образом.

Китай. Государственные средства массовой информации сообщали о более чем 100 тыс. поражённых компьютеров.

Южная Корея. Правительство принесло официальные извинения за непринятие своевременных действий по предупреждению эпидемии и оценило её масштабы в 240 тыс. атакованных вирусом компьютеров, а также 250 млн. долл. нанесённого ущерба. Однако промышленные круги заявили о 600 тыс. повреждённых вирусом компьютеров. Как сообщала Сьюзен Орбух, представитель отделения в Южной Корее фирмы-разработчика антивирусного программного обеспечения Trend Micro, «Министерство информации и связи этой страны сообщило, что разработчики антивирусных программ получили сигналы об инфекции примерно от 1000 частных фирм, 200 государственных и общественных организаций и 300 университетов. Верховному суду Кореи пришлось задержать разбирательство нескольких дел ввиду утраты свидетельских показаний, хранившихся в электронных базах данных на компьютерах».

Индия. По заявлениям экспертов и официальных лиц более 30 тыс. компьютеров было выведено из строя. Ведущие отрасли промышленности, банки и другие финансовые учреждения не были готовы к эпидемии компьютерного вируса.

Израиль. Израильские специалисты по восстановлению информации представили следующее заключение: атака вируса вызвала настоящую катастрофу, так как в ходе эпидемии были выведены из строя тысячи компьютеров, включая компьютеры, принадлежащие основным финансовым учреждениям страны, разведывательным службам и крупным провайдерам Интернет.

Египет. Многие компании в Каире были вынуждены предоставить своим служащим выходной день и отправить их по домам, так как компьютерные системы этих организаций были парализованы вирусом. «То, что случи-

лось, – это настоящее стихийное бедствие», – заявил представитель одной из крупнейших египетских машиностроительных фирм.

Страны Персидского залива. Представители различных отраслей промышленности Объединённых арабских эмиратов (ОАЭ) оценили последствия атаки вируса в 5–10% повреждённых компьютеров от общего числа занятых в индустрии ОАЭ. В соответствии с отчётными данными, наибольший уровень нанесённого ущерба зарегистрирован в Катаре, где последствия атаки вируса далеко превысили «эпидемиологический» предел.

Турция. По сообщениям РИА «Новости» вирус успешно атаковал ряд крупных частных банков, полицейские участки, военные учебные заведения в Анкаре, аэропорт в Измире на турецком побережье Эгейского моря, архив радио и телевидения, кадастровые записи недвижимости, государственную телекомпанию TRT, некоторые правительственные учреждения, а также компьютерные сети многих частных турецких учреждений. По данным информационного агентства Associate Press всего в Турции, пострадало свыше 300 тыс. компьютеров.

Итак, урок, казалось бы, должен быть усвоен. Но не тут то было…

В среду, 26 апреля 2000 года, компьютерный вирус «Chernobyl» «вновь активизировался и опять нанёс серьёзный ущерб Южной Корее, уничтожив информацию на «жёстких» дисках в сотнях компаний», – сообщало информационное агентство Reuters со ссылкой на Министерство информации Южной Кореи. По словам представителей министерства, они получили более 2000 жалоб от пользователей, пострадавших от этого известного вируса, который активизируется в день Чернобыльской катастрофы. Тем не менее, в этом году в Южной Корее вирус нанёс гораздо меньше ущерба, чем в прошлом, а большинство пострадавших представляло собой индивидуальных пользователей и сотрудников небольших компаний.

Вирус не оставил без своего «внимания» и другие страны и континенты, хотя здесь разрушения выглядят менее впечатляюще: Венгрия (более 200 компьютеров), ЮАР (более 200 компьютеров), Чехия (около 40 компьюте-

ров). Незначительные инциденты (от 1 до 15 компьютеров) были зарегистрированы в Финляндии, Норвегии, Эстонии, Швеции, Франции, Гонконге, Японии, Греции, Словении, Исландии. В России на $18^{\underline{00}}$ по московскому времени «Лаборатория Касперского» зарегистрировала около 65 случаев срабатывания вируса «Chernobyl», а в общей сложности было повреждено более 350 компьютеров.

Как обычно, не обошлось и без недоразумений.

В конце декабря 2000 года информационному порталу ZDNet стало известно, что в течение последнего времени на Web-сайте фирмы 1С в файле с «заплаткой» для игры «Корсары» (версия 1.04, файл sd_patch104_rus.exe) распространяется вирус «Chernobyl». Точный период времени, в течение которого данное обновление было доступно на Web-сайте компании для свободной загрузки, как и число пользователей, установивших у себя это обновление, оставались неизвестными. По информации ZDNet, попытки обратить внимание модератора общего форума 1С по играм на данную ситуацию велись более суток, но ни к чему не привели. В субботу в ответ на звонок в службу консультаций 1С по играм женский голос сказал, что «они этого не знают», и что это первое сообщение, поступившее к ним по данной проблеме. Также имелась информация, что в воскресенье всем руководителям фирмы были разосланы письма в связи со сложившейся ситуацией. В понедельник ZDNet обнародовал информацию, в которой говорилось, что файл с последней версией «заплатки» к игре «Корсары», выложенный на Web-сайте фирмы 1С, инфицирован вирусом «Chernobyl» и в тот же день 1С сняла со своего Web-сайта ссылку на него, а в разделе «Новости» поместила информацию следующего содержания: «Вниманию тех, кто скачал обновление v.1.04 к игре «Корсары» в период с 22.12 по 24.12. Файл с обновлением по недосмотру был заражён вирусом «Chernobyl». Всем, кто скачал и установил эту «заплату», советуем срочно воспользоваться антивирусной программой». Кроме того, всех, скачавших этот файл, попросили срочно связаться с линией консультаций 1С. Позднее глава фирмы 1С Борис Нуралиев рассказал корре-

споненту ZDNet, что непреднамеренное распространение вируса произошло «по вине нового сотрудника, не выполнившего определённые технологические установки». Однако, как отметил Нуралиев, это не снимает вины с самой фирмы, хотя такой случай, по его словам, произошел впервые. По данным компании 1С, с 22 декабря, дня выхода и опубликования обновления к «Корсарам», его успело скачать «не так много пользователей» – около 75. «Мало кто качает файлы в выходные дни, большинство делает это на работе, – отметил Борис Нуралиев. – Часть этих людей нам известна, и мы разошлем им отдельное письмо».

Наступил март 2001 года, и разработчик антивирусного программного обеспечения – McAfee, порадовал пользователей следующим известием. Появился Интернет-червь «Anjulie»[439] (другое название – VBS/Anjulie@MM), представляющий собой VBS-скрипт и распространяющийся как вложение в электронные письма. Для рассылки сообщений червь использовал MS Outlook и рассылал себя по всем адресам из адресной книги. Помимо этого он сбрасывал на заражённую машину вирус «Chernobyl». При активизации червь устанавливал себя в систему, копировал себя в директорий Windows\Temp с именем «t4umhf5.vbs», а также записывал на поражённый компьютер в этот же каталог ещё один файл «ale32.exe», который представлял собой копию вируса «Chernobyl». После этого червь, используя MS Outlook, производил почтовую рассылку своих копий. Параметры письма при этом были следующие:

Тема:	Read the true history on Angelina Julie	Читаёте правдивую историю Ангелины Джулии
Тело:	Your life	Ваша жизнь
	Your work	Ваша работа
	Your lovers	Ваши возлюбленные

Вложение: «AngelinaJulie.txt.vbs» или «T4UMHF5.VBS» (имена вложений могли варьироваться).

[439] «Anjulie» (англ.) – «Ангелина Джулия».

Для обеспечения своего выполнения при каждом старте операционной системы червь регистрировал себя в секции автозапуска системного реестра: HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\T4UMHF5=C:\WINDOWS\TEMP\T4UMHF5.VBS. И в завершение своих злодеяний «скрипт» запускал на выполнение файл «ALE32.EXE», который в свою очередь загружал в память инфицированного компьютера вирус «Chernobyl». Сам «скрипт» содержал следующий текст: «AlevirusSCS VxBrasil:)», а в файле с расширением «*.exe» содержался фрагмент текста: «AlevirusSCS v666 VxBrasil».

Воистину «популярность» вируса «Chernobyl» не знала в то время границ! Как вы думаете, куда ещё мог бы проникнуть этот злодей? А что, если взять да и отправить его в космос? Например, в форме такого сообщения: «26 апреля 2001 года специалисты NASA зарегистрировали одновременный выход из строя сразу трёх компьютеров, осуществлявших общий контроль систем управления на международной космической станции (МКС). Это стало для них настоящим потрясением. По словам астронавтов, которым удалось осуществить короткий сеанс связи с Хьюстоном, они ощутили три толчка, которые явились прямым следствием выхода из строя одного компьютера за другим. Причём последний толчок был настолько сильным, что им оторвало канадскую «руку манипулятор», испытания которой должны были начаться в среду. Более того, астронавтам пришлось отложить запланированную корректировку орбиты и вырабатывать план её изменения при помощи корабля «Endeavour». Однако если в ближайшее время МКС не поднять на более высокую орбиту, экипаж придётся эвакуировать, а станцию затопить. Представители NASA сообщали, что причиной произошедшей аварии был вирус «Chernobyl», который каждый год активизируется 26 апреля. В связи с этим в самое ближайшее время на станцию будет отправлена свежая версия Антивируса Касперского и специалист по его установке». Ну и шуточки у вас, скажет читатель, ведь 26 не Первое апреля – День смеха!

Хорошо, но что Вы скажете об этом: в июле 2001 года ливанцы насмерть испугались компьютерного вируса. Слух о том, что некий вирус под названием «Chernobyl» может заражать и сотовые телефоны, привёл к перебоям в работе ливанской телефонной сети из-за её перегрузки. В панике граждане Ливана срочно отключали свои мобильные телефоны и переходили на традиционные телефонные аппараты, советуя своим друзьям и знакомым сделать, как можно скорее, то же самое. В итоге, суета и паника как раз и привели к перегрузке телефонной сети, на несколько минут прервав её работу, а убытки из-за несостоявшихся телефонных звонков были оценены в десятки тысяч долларов. На фоне продолжавшегося ажиотажа Парламент Ливана был вынужден провести специальное расследование с целью выяснения источника этих необоснованных слухов о великом и ужасном вирусе «Chernobyl».

В заметке «Ведомостей» под названием «Компьютерные технологии: безопасность для каждого» от 1 октября 2001 года вирус «Chernobyl» приводится в качестве примера «специфического случая живучести»: «С 1999 года по-прежнему каждый год 26 апреля даёт знать о себе вирус «Chernobyl». Хотя количество пострадавших от этого вируса с каждым годом уменьшается: 26 апреля 1999 года в службу технической поддержки ЗАО «ДиалогНаука» поступило 600 обращений, в 2000 году – 200, а в 2001 году – лишь несколько десятков».

А как поживал всё это время автор вируса «Chernobyl»? Правоохранительные органы проявили упорство в расследовании вирусного инцидента и осенью, 18 сентября 2000 года, Чен Инг-Хау задерживают и переводят из казармы в тюремную камеру. Там он содержится несколько месяцев, и его допрашивают не только тайваньские полицейские, но и специальные агенты Федерального бюро расследований США. По окончании следственных действий состоялся суд, на котором выяснилось, что на острове Тайвань компьютеров пострадало не слишком много, и поэтому сажать автора вроде бы и не за что. Причём ни одна из тайваньских компаний так и не подала на него

иск, и поэтому создателя вируса «Chernobyl» отпустили на волю. Между тем, наконец-то был предъявлен иск и не компьютерными компаниями, а неким частным лицом – студентом, чей компьютер реально пострадал от вируса «Chernobyl». Иск от частного лица о нанесении конкретного ущерба по тайваньским законам карается достаточно строго, и Чен Инг-Хау вряд ли мог бы радоваться, если бы дело было доведено до суда, и он получил бы три или более лет заключения. Но время шло, интерес к делу судебному Чену со стороны общественности резко снизился, и судебное расследование так и не было доведено до конца. Более того, Чен Инг Хау оказался кем-то вроде национального героя, и после демобилизации получил предложения от ряда крупных тайваньских фирм заняться интересной и высокооплачиваемой работой. Информационный портал Infoart в своей публикации «Автора вируса «Чернобыль» взяли на работу по специальности» сообщал следующее: «Тайваньской компании Wahoo International Enterprise[440] пришлось побороться с несколькими конкурентами, чтобы залучить к себе на работу известного 24-летнего вирусописателя Чен Инг-Хау, как только он закончил службу в тайваньской армии. В своё время он был арестован за распространение компьютерного вируса «Chernobyl», который он создал. Вирус «Chernobyl», известный также под названием Win95.CIH, начал свою работу 26 апреля этого года. Это была одна из самых разрушительных компьютерных эпидемий в истории. Убытки составили сотни миллионов долларов. Однако вскоре после ареста Чена выпустили, поскольку по тайваньским законам в его действиях не было состава преступления. Теперь Чен Инг-Хау предстоит тестировать компьютерное оборудование, выпускаемое компанией Wahoo. Руководство компании считает его редким по квалификации специалистом, поэтому его приняли на работу с распростёртыми объятьями».

[440] Компания-разработчик аппаратного и программного обеспечения, в том числе для операционных систем Linux.

В результате, по последним, весьма скудным сообщениям тайваньской прессы Чен Инг-Хау продолжает исполнять свои престижные и высокооплачиваемые служебные обязанности в одном из структурных подразделений компании-производителя мультиязычного клона Linux – Wahoo International Enterprise. Тем не менее, представители антивирусных компаний посчитали, что сам факт ареста и открытия уголовного дела против Чен Ин-Хау является суровым предупреждением всем авторам вирусов: рано или поздно они будут наказаны за свои поступки. Компании же, которые берут на работу таких людей, по мнению экспертов, идут на большой риск, поскольку авторы вирусов могут продолжить писать свои разрушительные программы на своём рабочем месте.

Исходя из вышесказанного, можно сделать единственный вывод: вирусы успешно внедрились в повседневную жизнь компьютерного сообщества, и покидать её в обозримом будущем не собираются. В завершение истории о вирусе «Chernobyl» подчеркнём также следующее: главная рекомендация по борьбе с компьютерными вирусами заключается в том, что необходимо серьёзно относиться как к защите от вредоносных компьютерных программ, так и к их авторам.

В начале мая был зарегистрирован резидентный полиморфный вирус «HPS», инфицировавший файлы в формате PE с расширениями «*.exe» и «*.scr»[441] – первый полиморфный вирус, написанный специально под 32-х битную операционную систему Windows.

[441] «*.scr» – файл «Заставки» (проф. screensaver) экрана монитора. Заставки обычно выводят на экран монитора движущиеся изображения. Запуск заставки происходит в автоматическом режиме после простоя компьютера в течение заданного времени и использовалась в первых персональных машинах во избежание преждевременного выгорания специального покрытия экрана монитора (люминофора).

Идентификационная карточка вредоносной компьютерной программы	
Имя	HPS
Другие названия	Win95.HPS, W95/HPS, Hanta, Hantavirus Pulmonary Syndrome
Тип	компьютерный вирус
Инфицируемые платформы	Windows 95/98
Впервые обнаружен	май 1998 года
Страна происхождения	Испания
Длина	5124 байта

При старте системы «HPS» расшифровывал свой программный код и пытался определить базовый адрес модуля «kernel32.dll». Затем с помощью недокументированных приёмов вирус определял адрес функции «VxDCall» и проверял наличие своей копии в оперативной памяти. В том случае, если программный код «HPS» в оперативной памяти отсутствовал, то, используя адрес «VxDCall», вызывались функции «PageReserve» и «PageCommit», посредством которых вирус выделял себе блок оперативной памятии копировал собственный код. После этого «HPS» перехватывал вызов функции «VWIN32_Int21h_Dispatcher» и устанавливал для него собственный обработчик. Этот вирусный обработчик возвращал ответ «я тут» на запрос о наличии собственной копии в оперативной памяти, а также при открытии файлов в формате PE вызывал процедуру их инфицирования. При вызове функций «FindFirst» и «FindNext» вирус использовал так называемую «стелс» технологию и «прятал» приращение длин инфицированных им файлов.

При своей установке в оперативную память «HPS» генерировал свою полиморфную копию, которой затем заражались все файлы в текущем сеансе работы пользователя[442].

В процессе инфицирования файлов вирус «HPS» записывал себя в область последней кодовой секции, изменяя её характеристики и точку входа в исполняемый модуль. Кроме того, он удалял файлы данных антивирусных программ «anti-vir.dat», «chklist.ms», «avp.crc», «ivb.ntz» и имел в своём про-

[442] Такие компьютерные вирусы получили название «медленные полиморфики» – Slow Polymorphic.

граммном коде противоотладочные механизмы, основывающиеся на установке отладчиками обработчиков исключительных ситуаций (SEH). В теле «HPS» содержался защифрованный текст: <Hantavirus Pulmonary Syndrome (HPS) Virus BioCoded by GriYo/29A>.

Присутствие этого вируса в компьютерной системе можно было определить вследствие вызываемого им на экране монитора видео эффекта. Если вирус установился в оперативную память операционной системы Windows в субботу, то при открытии графических изображений в неупакованных файлах формата BMP, в том числе и фирменной заставки операционной системы, вирус переворачивал их справа-налево. Повторного переворачивания графических изображений не происходило, так как «HPS» помечал такие файлы, записав в них метку «DEADBABeh».

В мае 1998 года появился первый компьютерный вирус «RedTeam»[443] заражающий выполняемые файлы Windows с расширением «*.exe» (NE EXE) и рассылающий инфицированные файлы в Интернет по электронной почте при помощи почтовой программы Eudora[444].

Идентификационная карточка вредоносной компьютерной программы	
Имя	RedTeam
Другие названия	Win.RedTeam
Тип	компьютерный вирус
Инфицируемые платформы	Windows 3.xx
Впервые обнаружен	май 1998 года
Страна происхождения	Австралия
Длина	4766 байт

Для заражения файлов вирус оставался в оперативной памяти как резидентная программа и записывался в Windows-файлы при их запуске. При рассылке инфицированных сообщений «RedTeam» самостоятельно разбирал внутренний формат баз данных электронной почты Eudora и добавлял в «Outbox» сообщения, со-

[443] «RedTeam» (англ.) – «Красная бригада».

[444] До этого был известен макро вирус по имени «ShareFun», рассылающий себя при помощи программы MS-Mail. Более подробно о компьютерном вирусе «ShareFun» см. выше – 1997 год.

держащие заражённое вложение. Причём, так как уже в то время большинство систем и программ электронной почты использовало стандартизированные протоколы обмена данными, получить заражённое письмо и активизировать «RedTeam» мог очень широкий круг пользователей, даже не применявших программу Eudora.

Вирус «RedTeam» не обладал способностью автоматического запуска себя на компьютерной системе, получившей инфицированное сообщение. При открытии и просмотре письма вирус не заражал систему, для этого требовалось не только открыть письмо, но и запустить вложенный в него инфицированный файл с расширением «*.exe». И здесь автор вируса проявил себя в качестве знатока человеческой психологии, так как именно к таким действиям подталкивал неискушённого пользователя текст сообщения, в котором говорилось, что появился новый вирус по имени «RedTeam» против которого создана антивирусная программа, которая вложена в настоящее письмо.

Этот вирус представлял собой реальную угрозу для глобальных компьютерных сетей, поскольку использовал для своего распространения среду наиболее популярной среди пользователей операционной системы Windows и одну из самых распространённых систем электронной почты – Eudora, насчитывавшую порядка 18 млн. активных пользователей. Евгений Касперский, получив образец вируса «RedTeam» из Польши и исследовав его, спрогнозировал будущее следующим образом: «вирусы, использующие для своего распространения протоколы глобальных сетей и, в первую очередь, – электронной почты, станут в скором будущем настоящим бедствием для пользователей всей планеты». К сожалению, этот прогноз сбылся.

Пресса того времени писала: «Справедливости ради нужно отметить, что на грабли наступает не только компания Microsoft. …Конфуз недавно случился и с компанией Corel». Это было сказано по поводу того, что вирус

под названием «AutoStart»[445] был обнаружен на компакт-дисках с дистрибутивом новой версии Corel DRAW 8.0 для Mac OS. Готовая к отправке в торговую сеть партия CD-ROM оказалась инфицированной этим вирусом. Большую часть заражённого тиража удалось выявить и изъять ещё до его поступления в магазины, однако примерно 5–7% коробок было уже продано потребителю.

Идентификационная карточка вредоносной компьютерной программы	
Имя	AutoStart
Другие названия	Autostart.9805, Auto Start.9805.a, Hong Kong
Тип	вирус-червь
Инфицируемые платформы	Macintosh
Впервые обнаружен	май 1998 года
Страна происхождения	Гонг-Конг, Китай
Длина	53602 байта

«Autostart» был первым вирусом-червём, специально разработанным для платформ Power Macintosh. Этот червь прятался в загрузочных секторах различных томов, и размножался через них. Файлы он не заражал, записывал себя в корневой каталог с установленным атрибутом «AutoStart», а потом в папку «Extensions». Передавался через диски с файловой системой HFS или HFS+ (включая флоппи-диски, магнитооптику и т. д.), распространялся по сети. По этим признакам он относится к категории вирусов-червей. Первоначальное заражение требовало включенной опции «AutoStart» в «QuickTime» и выше, а отключаться она начала, начиная с версии 2.5.

Вирус «Autostart» был наделён деструктивной функцией – способностью удаления файлов. Он «стирал» с «жёсткого диска» файлы с расширениями «*.data», «*.cod», «*.csa» и «*.dat». Кроме того, система могла неожиданно перезапускаться после того, как вставлялся новый диск или устанавливался том. К тому же вирус-червь создавал два невидимых файла, именуемых «Desktop Print Spooler» (в папке «Extensions») и «DB» (в корневых директориях заражённых драйверов). В итоге, процесс «Desktop Print Spooler» оста-

[445] «AutoStart» (англ.) – «Автоматический старт».

вался постоянно активным в компьютерной системе, что, естественно, снижало её производительность.

Несколько позже вирус «Autostart» обзавёлся сразу пятью штаммами: «AutoStart.9805.b (длиной в 54779 байт); «AutoStart.9805.c» (длиной в 52734 байта); «AutoStart.9805.d» (длиной в 53280 байт); «AutoStart.9805.e» (длиной в 54003 байта); «AutoStart.9805.f» (длиной в 54051 байт).

Идентификационная карточка вредоносной компьютерной программы	
Имя	Marburg
Другие названия	W95.Marburg.A, Win95.Marburg, W95/Marburg
Тип	компьютерный вирус
Инфицируемые платформы	Windows 95/98
Впервые обнаружен	июль 1998 года
Страна происхождения	Испания
Длина	8590 байт

20 июля 1998 года был обнаружен резидентный полиморфный вирус, получивший название «Marburg»[446], также как и «HPS», – один их первых полиморфных вирусов, написанных под 32-х разрядную операционную систему Windows. Кстати, достаточно быстрому распространению этого вируса способствовало, в частности, то обстоятельство, что его содержали CD-ROM, сопровождавшие английскую, словенскую, шведскую, а позднее и итальянскую редакции журнала PC Gamer. Этот же вирус содержался и в программе электронной регистрации CD-ROM MGM Interactive под названием «Wargames PC».

Этот резидентный для текущего сеанса работы инфицированной программы полиморфный вирус был написан под 32-х разрядную операционную систему Windows и заражал файлы формата PE (расширения «*.exe» и

[446] «Marburg» (англ.) – в медицине название вируса, которое происходит от имени открывшего его немецкого учёного. Известен синдром Марбурга, проявляющийся как сумма признаков рассеянного склероза. Следует отметить, что «Marburg» был первым из известных «полноценных» полиморфных вирусов для среды Windows 95. Это «медленный полиморфик», и в текущем сеансе работы вирус заражал файлы своей одной сгенерированной полиморфной копией.

«*.scr»), которые искал в текущем директории, а затем последовательно в директориях \Windows и \Windows\System. Причём в связи с наличием программистских ошибок «Marburg» не мог размножаться в среде операционной системы Windows NT.

Во время запуска инфицированного файла он искал «kernel32» и адреса 24 процедур, всегда начиная с процедур «GetModuleHandleA» и «GetProcAddress», необходимых ему для дальнейшего размножения. При поиске «kernel32» вирус «Marburg» использовал алгоритмы работы очень похожие на аналогичные алгоритмы вируса «Cabanas». Итак, в целях инфицирования файлов вирус искал в таблице импортируемых процедур ссылки на «GetModuleHandleA» и «GetProcAddress» и запоминал их адреса; если такие ссылки отсутствовали, вирус сканировал программный код модуля «kernel32». В случае отсутствия указанных процедур, «Marburg» возвращал управление программе-носителю, а в противном случае – для активизации полиморфик-генератора[447] – выделял блок оперативной памяти для копирования в него своего программного кода, производил копирование и приступал к поиску файлов формата PE, инфицируя их. В процессе заражения файлов вирус шифровал свой программный код полиморфным кодом и записывал его в последнюю секцию файла, предварительно увеличив её размер.

В целях перехвата управления при запуске «Marburg» при помощи различных приёмов вносил исправления в программный код и таблицы заражаемого файла. В зависимости от структуры файла он либо записывал собственный адрес в PE-заголовок, тем самым заменяя стартовый адрес программы, либо, не изменяя стартового адреса, записывал в точку входа в программу команду передачи управления на свой код «JMP_Virus», или записывал в точку входа полиморфный код, который затем передавал управление на код вируса той же командой – «JMP_Virus».

---

[447] Полиморфик-генератор вируса «Marburg» не страдал оригинальностью и лишь практически отдельными деталями отличался от аналогичного полиморфик-генератора, содержавшегося в вирусе «HPS».

Перед началом инфицирования файлов «Marburg» удалял файлы данных антивирусных программных средств: «anti-vir.dat», «chklist.ms», «avp.crc», «ivb.ntz». Интересно, что при заражении вирус проверял имена файлов и «обходил стороной» файлы антивирусных программ PANDA, F-PROT, SCAN, наравне с файлами, в именах которых присутствовал символ «V». В зависимости от системной даты (при запуске инфицированного файла через три месяца и точно в тот час, когда он был заражён) «Marburg» по случайным позициям на экране монитора выводил в различные места «Рабочего стола» Windows до нескольких десятков иконок «Ошибка» – красный круг с белым крестом посередине. В своём программном коде вирус содержал достаточно объёмный фрагмент текста, в первом блоке которого перечислялись имена всех функций, используемых вирусом, а второй блок представлял собой текст, по первому слову которого данный вирус и получил своё имя: [Marburg ViRuS BioCoded by GriYo/29A] KERNEL32.dll USER32.dll.

В связи с появлением в «диком» виде таких вирусов как «HPS» и «Marburg» разработчикам антивирусных программ пришлось срочно адаптировать к новым условиям методики обнаружения полиморфных вирусов, рассчитанных до этого только на вирусы под DOS. Как сообщали специалисты компании «ДиалогНаука»: «…вслед за первым резидентным вирусом для 32-разрядных платформ Windows «вирусописатели» из группы 29A создали и выпустили в свет два неопасных резидентных полиморфных вируса Win95.HPS и Win95.Marburg, так называемые «медленные полиморфики», генерирующие при установке в память свою полиморфную копию, которой в дальнейшем будут заражаться все файлы в текущем сеансе. Win95.Marburg является на сегодняшний день первым «полноценным» полиморфным вирусом для Windows 95. Увы, распространение новых вирусов уже началось».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Class
Другие названия	Class.A, Class.Poppy, W97M.Class.A.Gen, W97M.Class
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	июль 1998 года
Страна происхождения	Соединённые Штаты Америки
Длина	1 модульVBA5

Обнаруженный в июле 1998 года написанный на языке программирования VBA VBA 5, использующий «стелс» технологию полиморфный макро вирус «Class»[448] был родоначальником многочисленного семейства вредоносных компьютерных программ, которые стали одними из первых известных вирусов, написанных специально для работы в среде MS Word 97 (SR1), и содержал два макроса в одном модуле «ThisDocument».

Обнаруженный в июле 1998 года написанный на языке программирования VBA VBA 5, использующий «стелс» технологию полиморфный макро вирус «Class»[449] был родоначальником многочисленного семейства вредоносных компьютерных программ, которые стали одними из первых известных вирусов, написанных специально для работы в среде MS Word 97 (SR1), и содержал два макроса в одном модуле «ThisDocument».

Инфицирование системы происходило при открытии пользователем заражённого файла, и при этом «Class» экспортировал свой программный код в файл C:\class.sys, вставляя его в макрос «normal.dot». Инфицирование документов осуществлялось аналогичным методом при их закрытии пользователем. Полиморфная составляющая вируса «Class» заключалась во вставке в программный код вируса строк комментария, который содержал имя пользователя, текущее время и дату, а также служебную информацию об активном в данный момент печатающем устройстве. Кроме того, автор вируса, в целях сокрытия его программного кода, впервые реализовал следующий подход: в

[448] «Class» (англ.) – «Класс».

[449] «Class» (англ.) – «Класс».

результате выполнения последовательности специальных команд «Class» при заражении получал возможность вставки своего модуля не в область макросов документа, как это происходило в случае с обычными макро вирусами, а в область так называемых классов MS Word[450]. Вирус записывался не как дополнительная макро программа, а как неотъемлемая часть текстового процессора MS Word. Такое ухищрение делало модуль вируса «Class» невидимым в пунктах меню «Tools/Macro» и «File/Templates». Кроме того, «Class» отключал опцию «VirusProtection», а тридцать первого числа выводил на экран монитора стандартное окно сообщений Windows, имевшее следующий вид:

This Is Class	Это – Класс
X-X-X-X-X-X-X-X-X-X-X	X-X-X-X-X-X-X-X-X-X-X
X VicodinES /CB /TNN X	X VicodinES /CB /TNN X
X-X-X-X-X-X-X-X-X-X-X	X-X-X-X-X-X-X-X-X-X-X

Известные штаммы вируса «Class» обычно имеют отличия от своего родоначальника, но не столь значительные, чтобы они были признаны в качестве инновационных решений или неизвестной технологии вирусописания.

Штамм «Class.b» в процессе инфицирования в качестве имени владельца операционной системы Windows записывал в системный реестр имя «Clazz», а случае попытки пользователя просмотреть программный код вируса с вероятностью в 25% устанавливал пароль «Clazz» на активный документ или с той же вероятностью удалял все документы из текущего директория.

Штамм «Class.c» в части размножения и полиморфизма ничем не отличался от родоначальника – «Class». По четырнадцатым числам каждого месяца с июня по декабрь этот штамм выводил на экран монитора текстовое сообщение, в котором обзывал пользователя заражённой машины: «I think [UserName] is a big stupid jerk! Class.Poppy.» («Я думаю [имя пользователя] – напыщенное тупое ничтожество! Class.Poppy.»)

---

[450] Область классов MS Word – это область стандартных процедур обработки событий в ядре MS Word. Кстати, именно отсюда и происходит имя вируса.

Штамм «Class.d» отключал антивирусную защиту компьютерной системы, подменял имя пользователя и название организации, на которых зарегистрирована данная копия операционной системы Windows. Для этого он изменял в системном реестре соответствующие значения: HKLM\Software\Microsoft\Windows\CurrentVersionRegisteredOwner = «VicodinES/CB/TNN» и RegisteredOrganization = «-(Dr. Diet Mountain Dew)-». По четырнадцатым числам каждого месяца с июня по декабрь этот штамм выводил на экран монитора текстовое сообщение, практически аналогичное сообщению «Class.c»: «Class.Poppy. I think [UserName] is a big stupid jerk!» («Class.Poppy. Я думаю, что (имя пользователя, взятое вирусом из системы) – напыщенное тупое ничтожество!»)

Штамм «Class.e» использовал временный текстовый файл C:\Clinton.sys и содержал ссылки на Билла Клинтона и Монику Левински по всему программному коду. На экране монитора случайным образом (вероятность 1 к 100) появлялось следующее сообщение: «Monica Blows Clinton! -=News@11=» («Моника надувает Клинтона! -=Новости@11=-»). Семнадцатого числа каждого месяца после августа на дисплее пользователя появлялось следующее сообщение: «Today is Clinton & Monica F___ -Fest Day!» («Сегодня Клинтон и Моника F___ -Праздничный день!»)

Штамм «Class.q» показывал на экране монитора по четырнадцатым числам каждого месяца, с июня по декабрь, текстовое сообщение, практически аналогичное сообщению «Class.c» и «Class.d»: « I Think <user name> is a big stupid jerk! VicodinES Loves You/» («Я думаю, что (имя пользователя, взятое вирусом из системы) – напыщенное тупое ничтожество! VicodinES любит Вас/»).

Интересно, что многочисленные, но достаточно заурядные вирусы семейства «Class», оказались не только большими «жизнелюбами», распространившись по всему миру, но и весьма устойчивыми к враждебным проявлениям со стороны компьютерного сообщества, далёкого от слов благодарности им за повседневное присутствие рядом с пользователем в течение не-

скольких лет подряд. Например, два представителя этой дружной семьи – «Class.d» и «Class.q» – удостоившись в декабре 1998 года чести быть включёнными в основной перечень наиболее распространённых в мире вирусов в «диком» виде «WildList» Международной организации WildList, а окончательно покинули лидирующую двадцатку только в феврале 2001 года и октябре 2000 года, соответственно.

В августе появился первый известный компьютерный вирус, заражающий выполняемые модули языка Java[451] (Java applications[452]) – «StrangeBrew»[453]. Этот вирус не представлял какой-либо опасности для пользователей Интернет, поскольку на удалённом компьютере невозможно использовать необходимые для его размножения функции. Вирус не мог размножаться и при запуске под известными браузерами[454], так как система немедленно выдавала сообщение о подозрительном «applet»[455] и прекращала

---

[451] Java (англ.) – язык Java (произносится «Джава») представляет собой машинонезависимый объектно-ориентированный язык, разработанный фирмой Sun Microsystems для создания распределённых прикладных Web-систем.

[452] Java-based application (англ.) – приложение, использующее технологию Java.

[453] «StrangeBrew» (англ.) – «Странный напиток». Вирусная процедура имела имя «Strange_Brew_Virus ()», и именно отсюда вирус получил своё название. Отметим также, что строка «Strange_Brew_Virus» видна в заражённых файлах при просмотре их любым текстовым редактором.

[454] Browser (англ.) – браузер (иногда неправильно употребляется термин «броузер»), программа (ускоренного) просмотра, средство визуализации объектов, навигатор. Например, Web-браузер это система поиска и просмотра информации (Web-страниц) в Интернет.

[455] Applet (англ) – проф. (произносится «аплет»), небольшая прикладная программа на языке Java, которая может быть встроена в страницы HTML, передана из Интернет вместе с документом как присоединение для его надлежащего представления у пользователя (например, «Календарь»). Аплеты отличаются от «полных» приложений Java тем, что имеют ограничения по доступу к определённым ресурсам локального компьютера (таким, как файлы, модемы и др.) и запрет коммуникаций с другими компьютерами в сети (кроме того, с которого данный аплет послан). Такие приложения конфигурируются под собственный набор свойств (например, принтеры, драйверы видео, звука и т. д.).

его выполнение. «StrangeBrew» был работоспособен только в том случае, если были разрешены функции доступа к дисковым файлам, то есть инфицированный файл запускался как полнофункциональное приложение Java – Java application. Однако «StrangeBrew» проиллюстрировал тот факт, что компьютерными вирусами могут быть атакованы приложения, интенсивно используемые при просмотре Web-серверов.

Идентификационная карточка вредоносной компьютерной программы	
Имя	StrangeBrew
Другие названия	JavaApp.StrangeBrew, Java.StangeBrew, JV/StrangeBrew
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003/UNIX
Впервые обнаружен	август 1998 года
Страна происхождения	Австрия
Длина	2826 байт

Вирус «StrangeBrew» специалисты-вирусологи отнесли к группе паразитных вирусов, которые характерны тем, что присоединяют себя к программе-«хозяину» таким образом, чтобы она оставалась работоспособной и после инфицирования. В частности, «StrangeBrew» присоединял свой код к Java-файлам с расширением «*.class», которые являются выполняемыми файлами, включающими в себя аплеты и программные приложения языка Java. Собственно Java-файлы с расширением «*.class» во многих отношениях похожи на файлы стандартных приложений с расширением «*.exe», используемых операционными системами Windows 95 или Windows NT; однако Java-файлы

HTML (Hypertext Markup Language) (англ.) – язык гипертекстовой разметки, способ описания документов в WWW. Язык HTML использует набор тегов, вводимых в текстовые документы, которые указывают браузеру или другой программе, каким образом информация должна выводится на экран. С помощью тегов в документе могут быть определены (размечены) части, главы, разделы, абзацы, списки, рисунки, таблицы, колонтитулы, индекс, содержание и т. д. Внутри каждого блока можно изменять шрифт, размер символов, цвет текста, выделять текст курсивом и/или делать его полужирным. Просмотр HTML документа осуществляется с помощью браузера. HTML является подмножеством языка SGML, использует чистый ASCII текст, широко применяется для создания страниц WWW.

с расширением «*.class» могли быть использованы одновременно на любой поддерживающей Java-технологию компьютерной системе. Это означает, что вирус «StrangeBrew» способен успешно размножаться буквально на десятках различных компьютерных платформ, в то время как традиционные компьютерные вирусы обычно способны распространяться лишь в одной или нескольких вычислительных средах. Например, как мы видели, знаменитый вирус «Chernobyl» мог инфицировать лишь операционные системы Windows 95 и Windows 98. А «StrangeBrew», напротив, был одинаково работоспособен под управлением Windows 95, на UNIX-серверах, а также суперкомпьютерах CRAY и других платформах.

Этот вирус мог инфицировать как файлы аплетов Java, так и файлы приложений Java. Аплеты Java являются программами, написанными на языке Java, которые обычно загружаются из сети и могут запускаться только при помощи Web-браузеров (например, таких как Internet Explorer или Netscape Navigator), а Java-приложения представляют собой автономные программы, которые могут быть запущены на компьютере вне какого-либо браузера. Вместе с тем, вирус «StrangeBrew» мог распространяться только тогда, когда запускался заражённый им файл приложения Java. Инфицированные аплеты Java не могли распространяться изнутри правильно сконфигурированного Web-браузера, такого как Internet Explorer или Netscape Navigator, потому что заражённые им аплеты вызывали сбой, который фиксировался системой защиты браузера и процесс немедленно завершался. Это означает, что во время навигации по Интернет невозможно заразиться «StrangeBrew», так что обычные пользователи Интернет могли не опасаться этого вируса – он распространялся при запуске инфицированного приложения Java. Однако лишь небольшое количество компаний или пользователей интенсивно работали с приложениями Java, что делало риск такого заражения крайне незначительным.

В дополнение к определению «паразитный», специалисты-вирусологи (о чём мы говорили выше) определили «StrangeBrew» и как компьютерный

вирус прямого действия. Это означает, что как только вирус перехватывал контроль над инфицированным приложением, немедленно следовала попытка заражения других файлов. Сразу же после окончания инфицирования вирус передавал управление приложению-«хозяину» и завершал собственную работу. «StrangeBrew» не устанавливал себя в оперативную память компьютера, не соблюдал какую-либо последовательность инфицирования и не наносил пользователю материального ущерба.

Данный вирус заражал приложения таким способом, что не всегда оказывался способным получить управление, когда пытался инфицировать уже запущенное приложение (будет получено управление или нет зависело от того, каким образом используется приложение-«хозяин» Java, а также от программной логики). Если же вирус получал управление, то он работал в два этапа. На первом этапе он искал в текущем директории уже инфицированные файлы с расширением «*.class». В том случае, если заражённые «StrangeBrew» файлы были найдены, вирус загружал в оперативную память инфицированный файл, который содержал программную логику вируса, а также алгоритм инфицирования файлов. После этого вирус переходил ко второму этапу процесса инфицирования, который мы опишем ниже. Если вирус не обнаружил в текущем директории уже заражённые файлы, он прекращал процесс заражения и возвращал управление приложению-«хозяину» Java.

Итак, если «StrangeBrew» обнаружил инфицированный им файл и загрузил его содержимое в память, он начинал искать новые файлы с целью их заражения. Если файл с расширением «*.class» имел размер, который можно было разделить без остатка на 101, то вирус предполагал, что файл уже инфицирован им. Такое допущение принималось по той причине, что «StrangeBrew» модифицировал длину всех заражаемых файлов до кратной 101 величины. Однако такая логика приводила к тому, что вирус не заражал файлы, которые соответствовали данному критерию, хотя и не были поражены «StrangeBrew». Перед тем, как инфицировать файл с расширением «.class»,

который до того не был заражён, вирус проверял этот файл на пригодность для инфицирования, основываясь при этом на некоторых внутренних критериях. Если файл не был готов для заражения, «StrangeBrew» вставлял нужное количество байтов в файл, чтобы увеличить его размер до кратного 101. Этот приём позволял вирусу, не задерживаясь, «проскакивать» файлы, непригодные, с его точки зрения, для инфицирования во время последующих попыток заражения. Если «StrangeBrew» находил файл с расширением «*.class», который подходит для инфицирования, он вставлял свой программный код в этот новый файл-«хозяин» (файл, который заразился вирусом, именуется файлом-«хозяином»). Вирус заражал файлы с расширением «*.class», создавая новый раздел в файле и добавляя в него собственную программную логику из соответствующего раздела. «StrangeBrew» вставлял этот новый раздел перед всеми логическими секциями оригинальной программы файла-«хозяина». Вирус как бы «латал» логику оригинальной программы-«хозяина», чтобы передать управление на заново созданную и внедрённую логику вируса. В процессе внесения этих изменений «StrangeBrew», на самом деле, подменял возможности программы-«хозяина» по обработке ошибок, и это служило причиной некорректного функционирования некоторых инфицированных им программ. Тем не менее, большинство приложений Java работали по-прежнему правильно. Кстати, «StrangeBrew» был способен модифицировать количество таблиц и полей в файле.

Этот вирус пытался инфицировать каждый подходящий файл с расширением «*.class» в текущем директории перед тем, как вернуть управление приложению-«хозяину», увеличивая размеры каждого файла примерно на 3890 байт. Кроме того, «StrangeBrew» также подменял в директории дату и метку времени (например, изменения или создания) каждого файла, который был им обработан. Однако указанные действия вируса были довольно слабо проработаны его автором, и в результате в его программном коде содержалось несколько весьма серьёзных ошибок, которые могли приводить к некорректному инфицированию файлов и, как следствие, сбоям в работе всей ком-

пьютерной системы. Если вирус вызвал отказ системы в процессе заражения, то приложение-«хозяин» Java разрушалось и дальнейшее инфицирование прекращалось.

Вирус «StrangeBrew» мог вызвать нештатную перезагрузку системы, что могло послужить причиной какого-либо дополнительного ущерба после инфицирования или возможных повреждений (по причине некорректного заражения) выполняемых файлов Java. Этот вирус не представлял собой непосредственной угрозы для типичных конечных пользователей или корпораций. Вместе с тем, любой, кто ведёт разработки в среде Java/WWW, попадал в группу риска, так как его Java-файлы с расширением «*.class» могли быть заражены или разрушены. Кроме того, пользователи, системы которых были инфицированы «StrangeBrew», отмечали, что их Java-приложения требовали больше времени для загрузки во время запуска на выполнение или сбоили во время работы, а если инфицированный Java-аплет непреднамеренно загружался и запускался внутри Web-браузера, то на экране монитора могли появляться различные сообщения.

Проникновение вредоносных компьютерных программ в Глобальную сеть продолжалась нарастающими темпами, и вирусы, заражающие «скрипты» языка Visual Basic (VBS-файлы), которые широко применялись для написания Web-страниц, перешли в разряд практически повседневных творений вирусописателей. Учитывая нарастающую опасность со стороны этих программ «Лаборатория Касперского» подготовила и обнародовала весьма подробное исследование возможной угрозы, исходящей от VBS-вирусов. Интересно, что, ознакомившись с материалами, некоторые «…специалисты поспешили заклеймить компанию «нарушителем спокойствия» и назвали этот шаг возмутительным нагнетанием вирусной истерии среди пользователей». Но когда в скором времени глобальные эпидемии VBS-вирусов стали происходить одна за другой, компьютерное сообщество осознало, что выводы исследования и соответствующий прогноз на ближайшую перспективу нашли своё полное подтверждение, а вирусы, инфицирующие «скрипты» языка VBS

во второй половине 1998 года заняли первое место среди наиболее распространённых и опасных вредоносных компьютерных программ.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Rabbit
Другие названия	VBScript.Rabbit, VBS.Rabbit, VBS/Rabbit.a
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT/2000/XP/2003
Впервые обнаружен	ноябрь 1998 года
Страна происхождения	Соединённые Штаты Америки
Длина	546 байт

На этом фоне в ноябре появился резидентный загрузочный VBS-вирус, получивший имя «Rabbit»[456] и давший жизнь одноимённому семейству.

В принципе, семейство «Rabbit» в целом не претендует на какую-то особую оригинальность, так как все его представители действовали по хорошо известной к тому времени схеме: перехватывали прерывание INT 13h и записывались в загрузочные сектора флоппи-дисков и главную загрузочную запись (MBR) «жёсткого» диска.

Вирус «Rabbit» и его штамм «Rabbit.b» полностью укладываются в рамки «верных последователей» общей концепции построения VBS-вирусов. Причём родоначальник – «Rabbit», очень заметен в системе с того момента, как только он открывает окно DOS на выполнение. Более того, пятнадцатого числа каждого месяца «Rabbit» и «Rabbit.b» создают «The CodeBreakers.URL[457]» для связи с Web-сайтом автора вируса, устанавливают соединение и показывают на экране монитора одно из следующих сообщений – «VBSv v1.0 by LordNatas[458]/CodeBreakers» («VBSv v1.0 от Владыки Сатаны/Взломщики программ») или «VBSv v1.1 by LordNatas/CodeBreakers»

---

[456] «Rabbit» (англ.) – «Кролик». В имени вируса явно прослеживается намёк на его быстрое размножение.

[457] URL (сокр. от Uniform Resource Locator) (англ.) – унифицированный указатель информационного ресурса (стандартизованная строка символов, указывающая местонахождение документа в Интернет).

[458] Этот приём, тогда оригинальный, мы уже встречали у одноимённого вируса. Прочтите, пожалуйста, слово «Natas» наоборот. Что у Вас получилось? Правильно – «Satan».

(«VBSv v1.1 от Владыки Сатаны/Взломщики программ») соответственно. В теле этих вирусов содержатся строки «Rabbid.a: [Rabbit!]» (Кролик.a: [Кролик!]) и «Rabbid.b: Rabbit» (Кролик.b: Кролик). Штамм «Rabbit.c» представлял собой переработанную автором версию VBS-вируса «Rabbit». Этот штамм несколько более сложный по отношению к родоначальнику «Rabbit» и «Rabbit.b». Пятнадцатого числа каждого месяца он создавал «cb.url» для связи с Web-сайтом автора вируса, устанавливал соединение и показывал на экране монитора следующее сообщение: «VBSv v2.0 by Lord Natas/CodeBreakers» («VBSv v2.0 от Владыки Сатаны/Взломщики программ»»).

Логическим продолжением VBS-вирусов стало появление первого полноценного HTML-вируса, которому было присвоено имя «Internal»[459].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Internal
Другие названия	HTML.Internal, VBS.Prepend
Тип	компьютерный вирус
Инфицируемые Платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые Обнаружен	ноябрь 1998 года
Страна Происхождения	Соединённые Штаты Америки
Длина	9262 байта

Компания Central Command, первой обнаружившая этот вирус, заявила, что он безвреден, то есть не содержит деструктивных компонент. И, тем не менее, его появление породило множество проблем – не меньше, чем появление первых макро вирусов. Как и макро вирусы, HTML-вирус «Internal» был построен на технологиях Microsoft и заражал компьютер пользователя, только если тот заходил браузером Internet Explorer на страницу с вирусом, находящуюся на сервере Internet Information Server (IIS)[460]. Когда пользователь посещал инфицированную «Internal» страницу, вирус выводил в статусную строку сообщение «HTML.Prepend/Internal» и запускал программу на VBS, которая искала на локальном диске все файлы с расширениями «*.htm»

[459] «Internal» (англ.) – «Втутренний».

[460] Internet Information Server (IIS) – информационный сервер Интернет. Сетевой сервер, поддерживающий многочисленные протоколы; передает информацию преимущественно на языке HTML, используя протокол передачи гипертекста (HTTP)).

и «*.html». Итак, заголовок заражённых HTML-файлов содержал инструкцию, которая объявляла вирусный скрипт, как автоматически выполняемый при открытии файла браузером, то есть при открытии заражённой HTML-страницы управление автоматически передавалось на код вируса. Основная процедура вируса с вероятностью 1/6, в зависимости от значения системного датчика случайных чисел, вызывала процедуру инфицирования, которая, как мы уже упоминали, искала все файлы с расширениями «*.htm» и «*.html» в текущем, и всех родительских каталогах, а потом записывалась в их начало. При заражении первоначальное содержимое файлов сдвигалось вниз, и по этой причине вирус «Internal» не портил файлы и визуально (при просмотре браузером) инфицированные HTML-страницы никак не отличались от незаражённых. Первая строка программного кода вируса содержала текст-идентификатор: «<html> <!--Internal-->».

Вирус, приходящий из Интернет и способный модифицировать файлы, менять установки и запускать скрипты на машине пользователя, потенциально очень опасен, но решение этой проблемы достаточно просто. Если установить в Internet Explorer уровень безопасности не ниже «Medium», браузер будет предупреждать о том, что скрипт пытается модифицировать файлы пользователя. Итак, появление инфицирующего HTML-страницы компьютерного вируса «Internal» специалистов не шокировало, так как компьютерные злоумышленники ранее освоили систему скриптов операционной системы Windows, то есть программы на командном языке Windows – Microsoft Scripting Host. Большинство вирусологов указывало: «Опаснее всего то, что вирус в состоянии распространяться через сеть Интернет – современные браузеры выполняют заражённые скрипты на локальном компьютере, даже если они расположены на удалённом Web-сервере».

Идентификационная карточка вредоносной компьютерной программы	
Имя	Attach
Другие названия	Macro.PPoint.Attach, Power-Point.Attach
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	декабрь 1998 года
Страна происхождения	Соединённые Штаты Америки
Длина	1 макрос

Специалистам-вирусологам постепенно стало очевидным, что усилия вирусописателей начали концентрироваться вокруг сетевых приложений и дело идет к появлению полноценного сетевого вируса-червя, использующего возможности операционной системы Windows, MS Office и заражающего удалённые компьютеры, Web-серверы, а также активно распространяющегося по электронной почте. Компьютерные злоумышленники активизировали свои усилия, направленные против приложений Microsoft Office, и в кратчайшие сроки после написания первого компьютерного вируса для MS Access – в начале декабря 1998 года – компьютерное сообщество столкнулось с новым представителем вредоносных компьютерных программ: был выявлен первый компьютерный вирус, инфицирующий файлы презентаций MS PowerPoint и получивший имя «Attach»[461].

30 декабря «Лаборатория Касперкого», в сообщении под заголовком «Обнаружен первый вирус, заражающий файлы MS PowerPoint» обнародовала следующую информацию: «Так же, как и прочие вирусы, заражающие приложения MS Office (Word, Excel и Access), новый вирус является макро программой на встроенном в MS Office языке программирования Visual Basic for Applications (VBA) и использует те же методы размножения. Вирус перехватывает некоторые системные события, при которых активизируется вирусная программа, затем ищет на диске незаражённые файлы презентаций MS PowerPoint и копирует в них свой код. Скорее всего, макро вирусы, заражающие файлы MS PowerPoint, не станут причиной глобальных вирусных

[461] «Attach» (англ.) – «Довесок».

эпидемий, таких как эпидемии Word-вирусов «Concept» и «Cap» и вируса под MS Excel «Laroux», поскольку файлы-презентации достаточно редко переносятся с компьютера на компьютер. Однако не следует пренебрегать данным типом вирусов. Язык VBA является универсальным для всех приложений MS Office, поэтому вполне реально появление вируса, заражающего не только файлы MS PowerPoint, но и документы и таблицы MS Word и MS Excel. В результате, если такой вирус проникнет в систему, то окажется недостаточным вылечить только зараженные файлы MS Word и MS Excel – если вирус проник в файл MS PowerPoint, то каждый раз при запуске презентации вирус будет активизирован и система вновь окажется заражённой. Более того, MS PowerPoint позволяет встраивать в файлы презентаций Word-документы и Excel-таблицы, причём вставка файла происходит целиком – от первого до последнего байта».

Итак, «Attach», первый известный вирус, заражающий файлы презентаций MS PowerPoint, также как и другие вирусы, заражающие приложения MS Office, был написан на языке программирования VBA и для своего распространения использовал его инструкции, функции и особенности работы самого MS PowerPoint. Он содержал один макрос, включавший «функцию события» по имени «UserForm_Terminate», которая активизировалась всякий раз, когда закрывалась «пользовательская форма» – «UserForm», диалог, окно сообщения, кнопка и т. п. Таким образом, функция «UserForm_Terminate» представляла собой главную процедуру «Attach» и содержала код размножения вируса. При активизации вирусная процедура искала файлы с расширением «*.ppt» в директории C:\My Documents и во всех его поддиректориях, – открывая их и копируя туда макро код «Attach». Вследствие некоторых особенностей построения внутренней структуры MS PowerPoint вирус был способен получить управление, активизироваться и размножаться тогда и только тогда, когда в инфицируемом им файле с презентацией находилась хотя бы одна форма – «UserForm». В силу указанного условия-ограничения вирус «Attach», до того как перейти к процедуре инфицирования, в обязательном

порядке просматривал файлы на присутствие в них формы «UserForm» и, если таковой не было найдено, прекращал их заражение. Интересно, что «Attach» вел достаточно латентный «образ жизни» и не проявлял себя при помощи визуальных или каких-либо иных броских эффектов, поэтому обычный пользователь мог очень долго не догадываться о том, что его компьютер стал источником заразы. В теле вируса содержались строки комментария, первая из которых использовалась им в качестве идентификатора инфицирования: «<!--Internal--> PPT.Attach v0.1/Internal» («<!--Внутренний--> PPT.Attach v0.1/Внутренний»).

Итак, в 1998 году нарастают вирусные атаки на MS Windows, MS Office и сетевые приложения. Появляются новые вирусы, использующие более сложные приемы заражения компьютеров и новые методы проникновения через компьютерные сети. Кроме вирусов на арену выходят «троянские» программы, ворующие пароли доступа в Интернет, а также утилиты скрытого администрирования. Как обычно, было зафиксировано несколько инцидентов с заражёнными компакт-дисками. Несколько компьютерных журналов распространяли на своей обложке диски с программами, заражёнными вирусами под операционную систему Windows, например, «Marburg» и «Chernobyl».

В целом, чем более популярными становятся компьютеры, чем больше их объединено в сети, тем более изощрённые способы их защиты приходится разрабатывать и применять фирмам-производителям антивирусных средств.

§19. 1999 год – они были первые: использующий MS Outlook современный Интернет-червь под Windows, похищающий ключи системы шифрования PGP макро вирус, макро вирус для Access, Word и PowerPoint одновременно, записывающий свой код в файлы помощи Windows вирус, вирус для Corel DRAW! и приложений Corel PHOTO-PAINT, Corel VENTURA. А также Её Величество «Melissa» и многое другое

- Всё компьютерное сообщество развитых стран, в том числе и России, работает над устранением программной ошибки в представлении дат («Проблема 2000»).
- Выпущена операционная система Windows 98 SE (Second Edition), в которую встроен Internet Explorer версии 5.0 с оптимизированным

инициализирующим ядром, а в стандартную поставку добавлено несколько утилит (FrontPage, Web Publisher и т.п.).

- Фирмой Intel выпущен микропроцессор экономичного класса – Intel Celeron.
- Появляется новое поколение микропроцессоров Intel Pentium III (8,2 миллиона транзисторов, SSE).

В 1999 году в ответ на растущую угрозу со стороны компьютерной преступности в целом и, в частности, вирусописателей, а также мошенников, занимающихся электронными махинациями в Интернет, была создана международная неправительственная организация CyberPolice. Организация является некоммерческой и её цель – оказание всесторонней помощи обычным пользователям в защите от компьютерных преступников.

Примерно с начала 1999 года, антивирусная индустрия формально разделяется на две группы компаний в соответствии с их отношением к возможным инцидентам накануне и в первые недели после Нового года. Одни компании настойчиво продвигали идею о том, что компьютерный андеграунд в лице электронных взломщиков и вирусописателей всего мира готовит обществу неприятный «сюрприз» в виде сотен тысяч исключительно опасных вредоносных компьютерных программ, способных потрясти весь мир. В результате такого понимания ситуации всем пользователям рекомендовалось незамедлительно установить или модернизировать уже установленные антивирусные средства. Представители другой группы производителей антивирусных продуктов в рамках противостояния первой группировке всячески успокаивали испуганных пользователей всеми доступными им средствами. Подчеркнём, что этот спор так и не получил однозначного решения. Да, действительно, при переходе в новый 2000 год обвала вирусов-«монстров» не произошло, и лишь отдельные компьютерные системы отказали или имели сбои в нормальном функционировании. Однако авторы данной книги, непосредственно участвовавшие в решении «Проблемы 2000» в России и принимавшие прямое участие в работе оперативного штаба нашей страны в ту новогоднюю ночь, готовы подтвердить, что сбои и отказы были, и не только у

нас, но и в Японии, США, Великобритании и т. п., но были быстро локализованы и устранены. В завершение этой темы зададим скептикам единственный вопрос: «Вы можете гарантировать, что всё прошло бы столь же «гладко», если бы, начиная с 1998 года, не проводились широкомасштабные работы по инвентаризации всех без исключения государственных систем, а затем необходимые мероприятия по устранению выявленных недочётов, вплоть до полной реконструкции приоритетных компьютерных систем?»

В остальном 1999 год не стал исключением из правил, компьютерные вирусы не заставили себя долго ждать, и в январе компьютерное сообщество получило новогоднее поздравление от вирусописателей – разразилась глобальная эпидемия обнаруженного в «диком» виде Интернет-червя, который получил имя «Ska»[462]. Это был первый современный червь под операционную систему Windows[463], открывший новый этап в развитии вредоносных программ, интенсивно использующий для своего распространения программу MS Outlook, ставшую к тому времени корпоративным стандартом в США, а также во многих странах Европы и мира.

[462] «Ska» (англ.) – «Ска», танцевальный музыкальный стиль, основанный на одноимённом исконно ямайском стиле, близко родственном рэггей и рокстэди.

[463] Данный червь не дееспособен на компьютерах, работающих под управлением операционных систем Macintosh, UNIX и Linux. Кроме того, вследствие программистских ошибок в коде «Ska» не может распространяться в среде операционной системе Windows NT.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Ska
Другие названия	Ska.exe, W32/Ska.A, Ska.a, W32/Ska.A-m, I-Worm.Happy, W32. Ska, PE_SKA, Happy, Happy99, Happy00, Happy, W32/Happy, Trojan.Happy99, W32/ Ska-Hapyy99, Wsock
Тип	червь
Инфицируемые платформы	Windows 3x/95/98/ME/ NT/2000/XP/2003
Впервые обнаружен	январь 1999 года
Страна происхождения	Франция
Длина	10000 байт

Во второй половине января компьютерными злоумышленниками были разосланы заражённые письма[464] на несколько серверов международных агентств новостей в Интернет[465], которые были инфицированы именно вирусом «Ska»[466]. Буквально через несколько дней стала поступать информация о регистрации сотен инфицированных компьютеров, и наибольшее количество таких сообщений о появлении в компьютерах «червя» было зарегистрировано в западноевропейском сегменте Интернет, особенно во Франции. Финская фирма Data Fellows (Хельсинки), специализирующаяся на защите информации, предупреждала, что: «…пока червь злобствует в Европе, но, по всей вероятности, быстро окажется в Америке. Он не пытается разрушать файлы на заражённых машинах, зато без ведома жертвы рассылает электронные письма и объявления для телеконференций и способен не только снизить производительность сети, но даже вывести из строя корпоративный сервер электронной почты». Старший инженер Data Fellows по обслуживанию программного обеспечения Дон Таката добавлял: «Если у вас в сети 100 персональных компьютеров, и каждый пользователь просматривает письма с 9

[464] Червь «Ska» не использует дисковые файлы как основные объекты для размножения и распространения своих копий, а рассылает собственный программный код в сеть Интернет в виде вложений в электронные письма.

[465] Предположительно «червь» был выпущен в Глобальную сеть при непосредственном участии самого автора, французского вирусописателя известного под псевдонимом «Spanska».

[466] Péter Ször, Happy Gets Lucky, Virus Bulletin, April 1999.

утра, эта гадость начинает расползаться и неизбежно замедлит работу сети. Я не удивлюсь, если она забьёт почтовый сервер».

Червь «Ska» распространялся в виде вложенного в письмо файла под именем «happy99.exe», при запуске которого на экране монитора появлялся напоминающий фейерверк видео эффект и поздравление с Новым Годом. Пока пользователь наблюдал окно с изображением красивого новогоднего салюта «Ska» подменял файл «winsock32.dll», который предоставляет компьютеру возможность выхода во внешний мир – Интернет. После этого всякий раз, когда пользователь входил в программу электронной почты или телеконференции, червь отправлял свои копии по указываемым пользователем адресам. Любой вид операций через порты 25 или 119 запускал программу рассылки «спама». Кроме того, «Ska» вызывал процедуру инсталляции своего программного кода в систему: копировал себя в системный директорий операционной системы Windows, перехватывал функции работы с Интернет, конвертировал свой код в формат почтового вложения и добавлял его к отсылаемым письмам. Фактически, инсталлированный в систему червь начинал рассылать свои копии по всем адресам в Интернет, куда пользователь отсылал свои сообщения. Он запоминает в файле «liste.ska» в системном директории все адреса, на которые пользователем рассылаются письма. Этот «лог-файл» имеет ограниченный размер и содержит до пяти килобайт данных, то есть примерно до 200 адресов, на которые червь передал свои копии. Во время установки в систему «Ska» изменяет только те файлы, которые находятся в системном директории операционной системы, создавая в нём файлы под именами «ska.exe» и «ska.dll», а также сохраняя файл «wsock32.dll» под именем «wsock32.ska» и дописывая в него сегмент своего кода. Иногда он регистрирует файл «ska.exe» в системном реестре. Данный червь содержит строки текста, часть из которых зашифрована: «Is it a virus, a worm, a trojan? MOUT-MOUT Hybrid (c) Spanska 1999. Happy New Year 1999!! begin 644 Happy99.exe end \Ska.exe \liste.ska \wsock32.dll \Ska.dll \Ska.exe.» («Это вирус, червь, троян? MOUT-MOUT Гибрид (c) Spanska 1999. С Новым 1999 Годом!!

начало 644 Happy99.exe окончание \Ska.exe \liste.ska \wsock32.dll \Ska.dll \Ska.exe.»).

В связи с появлением «червя» «Ska» и ему подобных творений специалисты-вирусологи сформулировали некоторые обязательные правила поведения пользователя, которые актуальны и по сей день. Например, ни в коем случае нельзя запускать файл «happy99.exe» вне зависимости от того, откуда он был получен, даже если письмо отправлено с адреса, который Вам хорошо известен и которому Вы абсолютно доверяете. Необходимо помнить, что выполняемые файлы, получаемые из Интернет могут оказаться опасными для компьютера, так как в них могут содержаться вредоносные компьютерные программы, которые инфицируют компьютер каким-либо новым вирусом, а также разрушить данные на «жёстком» диске, отослать компьютерному злоумышленнику в Интернет конфиденциальную информацию, установить программу скрытного управления с удалённого адреса и т. д.

В целом можно сказать, что открытие полученных из Интернет файлов MS Office с отключённой защитой от макро вирусов и запуск непроверенных выполняемых файлов чрезвычайно рискованное дело. Об этом пользователь должен помнить всякий раз, когда он получает очередное электронное письмо с вложенным в него файлом.

Кстати, Интернет-червь «Ska», впервые появившись в начале 1999 года, оказался весьма «живучим» созданием и на протяжении длительного времени входил в число двадцати наиболее распространённых в мире вредоносных компьютерных программ[467].

Практически одновременно со «Ska» компьютерное сообщество было оповещено о появлении первого макро вируса для MS Word, который зани-

[467] Sophos PLC, Top ten viruses reported to Sophos Anti-Virus in June 2000.
Network Associates Virus Patrol reports, personal communications. 2000.

мается тем, что, похищает ключи представлявшей собой де-факто стандарт Интернет в области шифрования – системы шифрования PGP[468].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Caligula
Другие названия	Caligula.a, W97M.Cali.a, W97M/Caligula, W97M/Caligula.a
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT/2000/XP/2003
Впервые обнаружен	январь 1999 года
Страна происхождения	Соединённые Штаты Америки
Длина	1 модуль VBA

Этот своеобразный макро вирус, наречённый именем «Caligula»[469], попадал в компьютер вместе с заражённым документом в формате MS Word. Оказавшись на новой машине, он, «не откладывая в долгий ящик», инициировал проверку на предмет установки в компьютерной системе копии программного обеспечения PGP. В случае обнаружения такой системы, вирус «просматривал» системный реестр, находил используемые ключи, соответствующие популярной программе шифрования PGP – являющейся общей программой шифрования, которая обладает характеристиками эффективной конфиденциальности, и переходил в директорий, где находилась эта программа, а при при активации производил в нём поиск файла базы данных секретных ключей шифрования, который хранил «чувствительную» пользовательскую информацию. В случае обнаружения этого файла, «Caligula» инициировал FTP-сессию и незаметно для пользователя передавал автору вируса на удалённый компьютер найденный им файл. Хотя для чтения содержимого секретного ключа PGP обычно требовался пароль, «Caligula» демонстрировал мощную технику получения «чувствительной» информации из атакуемой цели – он инициировал исходящие сеансы, используя встроенную команду компьютера «ftp.exe» для связи со своим автором. Поскольку большинство

[468] PGP (Pretty Good Privacy) (англ.) – система PGP, набор алгоритмов и программ для высоконадёжного шифрования сообщений с использованием открытых ключей.

[469] «Caligula» (лат.) – «Калигула», имя римского императора; в переводе с латинского означает «сапожок».

правил файрволов позволяло пользователям извлекать FTP файлы извне, вирус мог использовать такой протокол, как FTP, для инициирования соединений с домашней базой из сети компьютера-жертвы атаки. Визуально вирус «Caligula» проявлял себя тем, что во время закрытия инфицированного документа MS Word 31 числа любого содержащего эту дату месяца, выводил на экран монитора в стандартном окне сообщений Windows текст: «WM97/Caligula (c) Opic [CodeBreakers 1998]» и «No cia, No nsa, No satellite, Could map our veins». Кроме того, результаты работы вируса проявлялись в следующем: отключались макро опции в MS Word, и поэтому сочетания клавиш «Alt+F8» и «Alt+F11», а также опции «Tools/Macro» становились недееспособными; в опции «Свойства» меню «Файл» – модифицировалась закладка «Общие»; инфицировались документы MS Word (файлы с расширениями «*.doc»).

Вот так! Теперь для «расправы» над PGP у компьютерных злоумышленников всё было готово – появился пример для подражания: макро вирус, который похищает ключи системы шифрования PGP. «Это вам не простое «format c:»!, – отмечали специалисты-вирусологи. «Если им удастся набрать достаточно много ключей, они смогут подделывать цифровые подписи, получать доступ к различным системам и читать защищённые документы», – высказывал свои предположения хорошо известный читателю эксперт по компьютерной безопасности Фред Кохэн, который был одним из первых авторов сообщений о «Caligula» в списке почтовой рассылки Интернет по вопросам обеспечения безопасности. Информационный портал Infoart, подытоживая в январской заметке «Вирус Caligula похищает PGP-ключи» высказывания ведущих специалистов-вирусологов по поводу появления данного вируса, сообщал: «Широко распространено мнение о непреодолимости этой системы защиты[470]. Однако новый вирус Caligula может поколебать её репутацию. Он принадлежит к новейшему классу вирусов, который некоторые

[470] Имеется в виду система шифрования PGP.

специалисты называют вирусами-шпионами. Эти вирусы создаются с целью похищения информации, хранимой на чужих компьютерах».

Помните, мы рассматривали макро вирус «Cross»[471]? Следом за ним появилось ещё несколько макро вирусов, переносящих свой программный код из одного приложения MS Office в другое. В этих вирусах всё интенсивнее применялись новые технологии и приёмы усложнения процедуры их обнаружения, блокирования и удаления и, в первую очередь, это «стэлс» технология и полиморфизм.

Наиболее заметным из подобных «Cross» вирусов стал обнаруженный в США многоплатформенный макро вирус, известный под именем «Tristate»[472].

---

[471] Первый вирус, заражающий два различных приложения MS Office: Access и Word. Подробнее об этом вирусе см. в предыдущем, 1998 году.

[472] «Tristate» (англ.) – «В трёх состояниях». Существует много штаммов этого вируса с многочисленными названиями (O97M.Tristate.a, O97M.Tristate.b, O97M.Tristate.c, Macro.Office.Triplicate.c, O97M.Triplicate.c, O97/Crown.b и т.п.), но, по определению известной компании Symantec, различия среди этих вариантов настолько несущественны, что рассматривать их имеет смысл лишь при техническом разборе макро кода. Мы последуем этому совету и рассмотрим всё семейство сразу.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Tristate
Другие названия	O97M.Tristate, Macro. Office.Triplicate.a, Triplicate, O97M/ Hopper, PP97M/Tristate.a, O97M.Tristate.a, O97M /Tristate.c, O97/Crown
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	январь 1999 года
Страна происхождения	Соединённые Штаты Америки
Длина	1 модуль VBA 5

Этот вирус проявлял себя как весьма латентный, не содержал деструктивных процедур, но являлся первым известным вирусом, заражающим более двух компонент MS Office, и одним из первых макро вирусов, инфицирующих презентации MS PowerPoint. Таким образом, «Tristate» был способен заражать файлы сразу трёх программ из состава MS Office: Word, Excel и PowerPoint; инфицируя документы MS Word 97, а также электронные таблицы MS Excel 97 и слайды MS PowerPoint. Причём процедуры инфицирования каждого из приложений MS Office были различны. При рассмотрении этого представителя вредоносных компьютерных программ давайте воспользуемся богатым опытом специалистов компаний разработчиков антивирусного программного обеспечения Trend Micro и «Лаборатории Касперского», досконально изучивших это творение и одними из первых выпустившие эффективные средства борьбы с ним.

Итак, вирус «Tristate» отключал антивирусные защиты MS Word, MS Excel и MS PowerPoint. Причём, если защита MS Word выключается при помощи обычных команд Visual Basic, то защита MS Excel и MS PowerPoint отключается непосредственно в системном реестре операционной системы Windows. При этом «Tristate» отключает их во всех возможных местах расположения в директориях: «CURRENT_USER», «LOCAL_MACHINE» и «USERS».

Этот вирус содержит три процедуры, написанные на языке программирования Visual Basic for Application (VBA 5), – «Document_Close()» для MS Word 97, «Workbook_Deactivate()» для MS Excel 97 и «actionhook()» для PowerPoint 97. Каждая из этих процедур при активизации под соответствующим

приложением MS Office вызывает подпрограмму размножения вируса, переносящую его в другие объекты данного приложения и в два других приложения MS Office.

Заражение из документа MS Word. При активизации из заражённого документа MS Word вирус немедленно отключает антивирусную защиту MS Word, проверяет область глобальных макросов (файл «normal.dot») на инфицированность и, если этот файл не заражён, «Tristate» запускает процедуру заражения компонентов MS Office, которая состоит из трёх частей: заражение MS Word, заражение MS Excel и заражение MS PowerPoint. Процедура, заражающая MS Word, является наиболее простой. Код вируса обычным копированием переносится в область глобальных макросов MS Word (файл «normal.dot»). При инфицировании MS Excel вирус пытается запустить новый экземпляр MS Excel, вызвав функцию «CreateObject» («Excel.Application»), а потом ищет в стартовом директории MS Excel файл с именем «BOOK1» (файлы из этого каталога автоматически загружаются при старте MS Excel). Если такого файла не было обнаружено, «Tristate» переходил к заражению MS Excel. Во время процедуры инфицирования он отключал встроенную в MS Excel защиту от макро вирусов и создавал новую таблицу, копируя в её область макросов свой программный код, записывал эту таблицу в стартовый директорий MS Excel в файл с именем «BOOK1». Процедура заражения MS PowerPoint во многом похожа на заражение MS Excel. Вирус запускает новый экземпляр MS PowerPoint, ищет в системном шаблоне MS PowerPoint (файл с именем «Blank Presentation.pot») модуль, который называется «Triplicate» и, если не находит, заражает этот файл. Отключает встроенную в MS PowerPoint защиту от макро вирусов, создаёт новый модуль «Triplicate» в файле «Blank Presentation.pot», копирует туда свой вирусный код, добавляет в этот же файл новую скрытую форму и устанавливает процедуру активации этой формы на свой код. Эта процедура будет вызываться каждый раз, когда пользователь «щёлкает» компьютерной мышью по данной форме. В завершение вирус проверят текущий активный документ и,

если вирусный код в нём не обнаружен, заражает его. Данная часть процедуры заражения работает в том случае, когда система уже заражена и MS Word закрывает новый еще неинфицированный документ.

Заражение из таблиц MS Excel и презентаций MS PowerPoint. Вирусные процедуры, которые активизируются при открытии заражённых файлов MS Excel и MS PowerPoint, очень похожи друг на друга за исключением некоторых деталей. Прежде всего, вирус проверяет наличие файла «BOOK1» в стартовом каталоге MS Excel, и если такой файл не обнаружен, то вирус считает систему ещё не заражённой и встраивается в неё. Сначала «Triplicate» заражает MS Word. При заражении MS Word вирус за две попытки получает экземпляр объекта «Word.Application». Сначала он пытается получить экземпляр уже запущенного приложения и использует для этого функцию «GetObject()», затем, если произошла ошибка обращения к объекту, вызывает «CreateObject()». Такой подход реализуется для того, чтобы «Triplicate» получил возможность записи своего кода в файл «normal.dot», который в случае активизированного MS Word оказывается закрыт от записи. Если MS Word не активен, вирус получает объект «Word.Application» обычным способом, то есть посредством функции «CreateObject()». Затем вирус удаляет из шаблона «normal.dot» весь содержащийся в нём программный код и создаёт там новую процедуру с именем «DisableAV()», копируя туда часть своего кода, а затем вызывает и удаляет её. Эта процедура отключает антивирусную защиту MS Excel и MS PowerPoint в системном реестре. Потом «Triplicate» копирует свой код в область глобальных макросов («normal.dot»).

Инфицирование MS Excel/PowerPoint. На этом этапе процедура заражения переносит код вируса из MS Excel в MS PowerPoint, или наоборот, в зависимости от типа уже заражённого приложения. Данная процедура совпадает с процедурой, использующейся «Triplicate» при заражении MS Excel и MS PowerPoint из документа MS Word.

В случае если вирус стартовал из электронной таблицы MS Excel, то в конце своей работы он также заражает текущую таблицу MS Excel. Процеду-

ра активации вируса в MS PowerPoint имеет дополнительную деталь: она вызывается с вероятностью 1/7 в зависимости от значения системного датчика случайных чисел.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Ethan
Другие названия	Ethan.a, W97M_Ethan, W97M/Ethan.a, Ethana, W97M.Ethan.a, Ethan Frome, W97M/Ethan.gen, Macro.Word97.Ethan
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT/2000/XP/2003
Впервые обнаружен	февраль 1999 года
Страна происхождения	Соединённые Штаты Америки
Длина	1 модуль VBA

1 февраля в США был обнаружен резидентный в среде MS Word макро вирус «Ethan»[473] без деструктивных функций, первыми признаками инфицирования компьютерной системы которым являлись наличие на диске C:\ временного текстового файла «Ethan.___» и изменённые свойства документов приложения MS Word 97.

Итак, вирус «Ethan» состоял всего лишь из одной макрокоманды «Document_Close» и инфицировал документы приложения MS Word 97 при закрытии заражённого документа, а также глобальный шаблон «normal.dot». Благоприятным фактором распространения вируса «Ethan» по всему миру и причиной вспышек эпидемий с его участием на протяжении нескольких лет послужило то обстоятельство, что в MS Word макросы автоматически запускаются при открытии любого документа, его закрытии, сохранении и т. д. Кроме того, имеется так называемый общий шаблон «normal.dot» и макросы, помещённые в общий шаблон, автоматически запускаются при открытии любого документа. Если учесть, что копирование макросов из документа в документ (в частности, в общий шаблон) выполняется всего одной командой, то среда MS Word представляется идеальной для существования макро вирусов подобных «Ethan».

---

[473] «Ethan» (англ.) – «Этан». Это имя, производная от идентификатора в виде метки, которая содержится в исходном программном коде вируса.

При заражении вирус выключал встроенную защиту от вирусов MS Word (опцию «VirusProtection») и предупреждение об изменении файла «normal.dot».

После попадания в систему вирус помещал свою единственную макрокоманду «Document_Close» в начало модуля, написанного на языке VBA – «ThisDocument», который представлял собой модуль в шаблоне MS Word 97. При инфицировании документа или общего шаблона вирус использовал временный текстовый файл «C:\Ethan.___», являвшийся источником его вирусного программного кода. Данному файлу вирус «Ethan» присваивал атрибуты системный и скрытый.

При закрытии документов в зависимости от системного счётчика случайных чисел «Ethan» с вероятностью 1/3 изменял служебные поля документов на следующие:

Название файла: Ethan Frome[474]
Автор файла: EW/LN/CB
Ключевое слово: Ethan

Интересно, что если ранее компьютер пользователя был заражён вирусом «Class», о котором мы достаточно подробно говорили, и в системе находился файл «class.sys», помещённый в неё этим вирусом, то в случае обнаружения такого файла «Ethan» удалял его. Кроме того, этот вирус не инфицировал файлы документов MS Word, если обнаруживал, что они содержат кириллицу. И в том, и в другом случаях – сомнительное благородство.

Менее чем через неделю после своего появления «Ethan» стал одним из самых распространённых в мире. Во введённой в действие 7 февраля 1999 года фирмой McAfee функционирующей в режиме реального времени карте распространения вирусов в мире этот вирус уже занимал седьмое место в десятке самых распространённых вредоносных компьютерных программ, существовавших на тот момент времени в «диком» виде. Карта была создана на

---

[474] Вирус «Ethan» изменяет название документов на «Ethan Frome» отнюдь не случайно. Дело в том, что это название книги, написанной в 1911 году Эдит Вортон.

основе обработки файлов 780 тыс. подписчиков (и разовых пользователей) службы McAfee.com.

В процессе создания карты были просканированы почти 39 млрд. файлов. При этом примерно в 20% просканированных компьютеров были найдены вирусы, а всего вирусы были найдены в 18 млн. файлов.

Идентификационная карточка вредоносной компьютерной программы	
Имя	SK
Другие названия	Win95.SK, Win95.SK.7977
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME
Впервые обнаружен	февраль 1999 года
Страна происхождения	Россия
Длина	7977 байт

Очередную головную боль пользователям операционной системы Windows и фирмам-разработчикам антивирусных программ принсли с собой инциденты с участием получившего название «SK»[475] первого вируса, который кроме инфицирования выполняемых файлов, содержал необычную подпрограмму, посредством которой он записывал свой код в файлы помощи Windows (HLP-файлы). Кроме инфицирования HLP-файлов вирус также добавлял свои копии в архивы наиболее популярных форматов, заражал ядро операционной системы и оставался резидентно в памяти компьютера как системный драйвер Windows. В заражённых файлах он шифровался полиморфным кодом, использовал малоизвестные адреса и функции Windows, а также содержал большое число программистских ухищрений, затрудняющих процесс его исследования.

С середины февраля по российским информационным каналам начинают распространяться пресс-релизы, в которых указывается, что вирус «SK» стал причиной крупномасштабной эпидемии, как в России, так и во всем мире, но «Лаборатория Касперского» заявила, что «… данная информация не соответствует действительности. Наши эксперты провели детальный анализ

[475] Это название происходит от номера порта (534Bh), с помощью которого вирус проверяет своё наличие в оперативной памяти – шестнадцатиричное 534Bh это как раз и есть «SK» в ASCII-кодах.

вируса и оценили вероятность его широкого распространения как очень низкую». Во-первых, вирус содержал ошибки, одна из которых приводила к тому, что вирус оказывался несовместим со многими конфигурациями Windows. При запуске вируса в таких конфигурациях система выдавала стандартное сообщение об ошибке в своем ядре. Во-вторых, вирус заражал файлы крайне медленно. С большой долей вероятности запуск вируса «SK» в обычных условиях мог не привести к инфицированию каких-либо других файлов в системе. В-третьих, при запуске наиболее популярных в России антивирусных программ вирус уничтожал всё содержимое «жёстких» дисков, включая и все свои копии. Таким образом, даже при условии того, что автор вируса разослал его в электронные конференции, масштабная эпидемия «SK» становилась маловероятной. Если неосторожный пользователь и запускал вирус на своём компьютере, его дальнейшее распространение прерывалось по одной из трёх причин: либо вирус вызывал ошибку, и система зависала, либо ни один файл на компьютере пользователя не заражался, либо вирус уничтожал систему и самого себя. Вместе с тем ведущие отечественные вирусологи признавали, что «в целом, «SK» является действительно сложным[476] и неординарным вирусом, что вызвало естественный профессиональный интерес со стороны антивирусных экспертов. Однако, наряду с этим, новый вирус стал причиной необоснованной рекламной шумихи». Например, эксперты «Лаборатории Касперского» вполне допускали, что: «вирус, возможно, и был заслан в конференции, и по этой причине заражёнными оказались несколько десятков или даже сотня компьютеров, что никак нельзя назвать эпидемией. Тем более эпидемией, вышедшей за пределы России: как показали исследования, вирус способен размножаться из инфицированных HLP-файлов только на тех компьютерах, где установлена поддержка русско-

[476] Самым интересным в вирусе «SK» является отнюдь не его сложность, а механизм внедрения в HLP-файлы Windows. О возможности заражения HLP-файлов Windows было известно давно, однако ранее подобное не встречалось. Вирус «SK» стал первым известным вирусом, способным записывать свой код в файлы этого типа.

го языка». Так что «возникновение мировой эпидемии вируса «Win95.SK» так же вероятно, как появление популяции пираний в реке Москва или крокодилов в канализации Петербурга», – добавил Евгений Касперский.

Давайте рассмотрим технические детали этого очень опасного резидентного полиморфного вируса, заражавшего исполняемые файлы для Windows в формате Portable Executable (PE-файлы), файлы помощи Windows (HELP-файлы), а также внедрявшего свои копии в архивные файлы форматов «*.arj», «*.ha», «*.rar» и «*.zip».

При заражении PE-файлов вирус «SK» не изменял» стартовый адрес программы, а записывал в таблицу настраиваемых элементов своё основное зашифрованное тело и внедрял в точку входа или, чаще всего, в случайную область стартовой сегментной секции до 168 байт полиморфного кода, который расшифровывал основной вирусный код в область программного стека и передавал ему управление. Затем, он проверял наличие своей резидентной копии в памяти компьютера и для этого читал байт из порта 534Bh, а потом сравнивал его со значением 21h. Если из порта прочиталось именно это число, то вирус восстанавливал исходные, замещённые им программные байты, и завершал свою работу. Если же система еще не была инфицирована, «SK» производя некоторые манипуляции с глобальной и локальной дескрипторными таблицами, устанавливал новый селектор с системными привилегиями и переключался в нулевое кольцо защищённого режима. А в этом режиме вирус уже имел право использовать системные вызовы на уровне драйверов виртуальных устройств, что он в дальнейшем и делал.

Для начала вирус восстанавливал 168 оригинальных байт в стартовой сегментной секции программы, а затем определял, существует ли в системе процесс с идентификатором 202h. Обычно под таким номером в операционной системе Windows регистрировался системный отладчик «SoftICE». Если он был обнаружен, то вирус прекращал свою попытку дальнейшей установки в память и возвращал управление программе-вирусоносителю. Если же «SoftICE» в системе не был найден, «SK» выделял себе блок памяти разме-

ром 24 Кб в системной области, копировал в него 7977 байт своего кода и устанавливал свои обработчики на «IO_Handler» и на «IFSMgr_FileSystemAPIHook»: первый контролирует чтение из порта 534Bh и возвращение значения 21h для отклика «я здесь», а второй – открытие, переименование и обращение к атрибутам файлов, анализируя данные файлы и пытаясь произвести их инфицирование. При перехвате «IFSMgr_FileSystemAPIHook» вирус переустанавливал на себя системную функцию «IFSMgr_InstallFileSystemAPIHook» и при попытке каким-либо виртуальным драйвером установить свой новый обработчик «IFSMgr_FileSystemAPIHook» удалял из цепочки обработчиков свой файловый обработчик, который находился последним в этой цепочке, устанавливал запрошенный драйвером обработчик и поверх него вновь устанавливал свой обработчик. Таким образом, вирусный обработчик всегда «стоял последним в очереди» и «всплывал наверх» в цепочке драйверов, обслуживающих «IFSMgr_FileSystemAPIHook». Этот алгоритм «всплытия» был позаимствован автором «SK» у рассмотренного нами выше вируса «Chernobyl»[477] и предназначен для обхода антивирусных резидентных сторожей. Также при открытии файлов на запись и непосредственно записи в файлы вирус «SK» использовал прямые вызовы драйвера файловой системы (FSD – File System Driver), обходя всю цепочку драйверов виртуальных устройств, обслуживающих файловые запросы.

Сразу же после установки в память «SK» открывал файл \Windows\system.ini и искал в ней переменную «shell=», а затем копировал указанный в ней файл (обычно «explorer.exe») в файл с новым расширением, отличным от исходного в последней букве, увеличенной на единицу. Например, файл «explorer.exe» копировался в файл «explorer.exf» и заражал данный скопированный файл. После чего вирус создавал в системно»м каталоге Windows файл «wininit.ini», в котором в разделе [rename] указывал, что файл «ex-

[477] Более подробно об этом компьютерном вирусе см. выше – 1998 год.

plorer.exf» необходимо скопировать в «explorer.exe», и «explorer.exf» после этого удалить. В результате, после первой же перезагрузки операционной системы она запускала этот уже инфицированный файл.

При открытии, переименовании или доступе к атрибутам файлов с расширениями «*.exe», «*.dll», «*.scr» или «*.hlp» вирус «SK» пытался их инфицировать. Для того чтобы заразить файлы «PortableExecutable exe», «*.dll» или «*.scr» он анализировал их заголовок и заражал только те файлы, у которых присутствует таблица-секция настраиваемых элементов и её размер не менее 8148 байт. Вирус определял адрес и размер стартовой сегментной секции и разбивал её для себя на блоки по 8404 байт. Затем он выбирал случайным образом порядковый номер такого блока, читал его в память и сканировал его содержимое для поиска определённых вирусом некоторых последовательностей байтов. Как правило, такие искомые последовательности байтов присутствуют во всех программах, созданных с помощью компиляторов языков программирования высокого уровня (например, C++, Pascal). Именно такими инструкциями (например, «PUSH EBP; MOVE EBP,ESP») обычно начинаются программные функции. Если требуемые вирусом байты были обнаружены, проверялось условие, чтобы найденная программная функция была не менее 168 байт (то есть в пределах 168 байт не должно быть инструкции возврата «RET»). В случае положительного результата «SK» запоминал адрес этой функции (адрес обнаруженной последовательности байтов) и продолжал поиск. В итоге, если была найдена хотя бы одна подходящая для внедрения вируса функция, выбирался случайный адрес из всех зафиксированных вирусом «SK» адресов функций. В том случае, если вирус не нашёл в 8404 байтах ни одной подходящей ему процедуры, он выбирал для внедрения своего кода стартовый адрес программы. Затем вирус приступал к генерации своего зашифрованного тела и соответствующего ему полиморфного расшифровщика. Этот расшифровщик записывался в область ранее выбранного адреса программной функции (оригинальные 168 байт сохранялись в теле вируса), а основное тело – в таблицу настраиваемых элементов, при-

чём с вероятностью 1/8 «SK» мог изменить в заголовке название самой этой сегментной секции на совершенно случайное. В конце заражения заголовок PE-файла корректировался с учётом внесённых вирусом изменений и файл был инфицирован.

Специалисты ЗАО «ДиалогНаука» указывали, что «механизм такого заражения файлов явно позаимствован из вирусов семейства «Zhengxi»[478]. И что же получается в результате? А то, что при запуске такого заражённого файла вирусный код может никогда не получить управления, если программная функция, в которой он «поселился» не будет вызвана самой программой. Вирус может «годами жить» в таком файле, пока, наконец, или сама программа, или пользователь, управляющий ей, не выполнят каких-либо действий (например, нажмет кнопку «F1»), повлекших за собой передачу управления программной функции, на месте которой и «живет» этот самый вирус. Вирус также использует ещё один, взятый у «Zhengxi», приём для распространения своей копии. Он внедряет в архивные файлы «*.arj», «*.ha», «*.rar» и «*.zip» свои полиморфные DOS-копии со случайными именами и расширениями «*.com» или «*.exe». К архивам приписывается созданный вирусный файл в неупакованном формате («store») и соответствующим образом корректируются необходимые для такой записи служебные поля архивных файлов». Все описанные выше ухищрения были позаимствованы автором «SK» у вирусов «Chernobyl» и «Zhengxi», но вирус использовалует также оригинальный, ни разу не встречавшийся ранее способ своего распространения посредством файлов помощи операционной системы. Таким образом, было показано на практике, что обычные HELP-файлы (HLP-файлы) могут распространять вирусный код. Вирус «SK» анализировал расширения «*.hlp» открываемых файлов и проверял их формат на принадлежность именно к этому типу файлов. Если HELP-файл подходил для заражения и ещё не был инфицирован, вирус записывал в конец файлов вирусные макро команды, корректиро-

[478] Более подробно об этом компьютерном вирусе см. выше – 1996 год.

вал служебное поле «System» и переносил байты информации, относящиеся к данному объекту, сразу за своими макро командами. Потом вирус «SK» корректировал в заголовке HELP-файла новый размер изменённого файла, создавал свою полиморфную DOS копию и записывал её в конец HELP-файла по методу оверлея для файлов с расширением «*.exe»[479]. Вирусные макро команды проверяли существование на «жёстком» диске файла C:\NTLDR и, в случае его отсутствия, создавалт на диске C: файл со случайным именем, в который записывали 380 байт некоего зашифрованного «вирусного пускателя». Проверка файла C:\NTLDR нужна была для того, чтобы не стартовать в среде Windows NT, так как под этой операционной системой вирус был недееспособен. Затем этот «пускатель» запускался средствами макро команд, и в качестве параметра ему передавался полный путь открытого инфицированного HELP-файла. «Пускатель» расшифровывал себя, открывал HELP-файл, имя которого ему было передано в качестве параметра командной строки, читал из него полиморфную DOS копию, записывал эту копию в файл, из которого и стартовал сам, запускал этот файл на выполнение и по окончании его работы удалял его, уничтожая следы своего присутствия на «жёстком» диске.

«Таким образом, «полиморфная DOS копия» вируса это обычная 16-разрядная полиморфная копия вируса, в принципах создания и работы которой также прослеживается плагиат из вируса «Zhengxi». Но, механизм заражения системной памяти оригинален и не был замечен ранее в других вирусах. Назовём этот 16-разрядный вирус для краткости «дроппером», так как он не является инфицированным объектом, а выполняет функции переносчика заразы. Итак, этот дроппер работает только в DOS-сессии операционной системы Windows. В любой другой операционной системе он пытается завершить свою работу. Причём инструкции, контролирующие операционную

[479] Размер полиморфной копии не учитывается системой и игнорируется при открытии такого файла.

среду, имплантированы непосредственно в полиморфный расшифровщик. Также в расшифровщике могут присутствовать и команды, проверяющие наличие в памяти отладчика «SoftICE» и прекращающие работу «дроппера» в случае его нахождения», – подчёркивают ведущие эксперты ЗАО «Диалог-Наука».

После расшифровки вирус «SK» проверял наличие своей резидентной копии в памяти компьютера, читая байт из порта 534Bh, и с помощью интерфейса DPMI[480] переключался в 16-разрядное пользовательское кольцо защищённого режима. Далее, манипулируя вызовами DPMI и дескрипторной таблицей, вирус осуществлял переключение в 32-разрядное третье кольцо защищённого режима – управление получал 32-разрядный вирусный код, который работал в инфицированных PE-файлах, из режима виртуальной машины DOS-сессии вирус попадал в защищённый режим приложения операционной системы Windows. Затем «SK» оказывался на системном (нулевом) кольце защищённого режима и размещал свою резидентную копию в области системных драйверов виртуальных устройств. Причём, заражение любого файла – исполняемого, архива или файла помощи, вирус производил только через минуту после предыдущего заражения.

После всего описанного выше становится вполне очевидным, что вирус «SK» был очень сложен и опасен. Кроме всего прочего, при открытии программ, начинающихся на «ADIN» или «AVPI», а также, с большой долей вероятности, при открытии файлов, начинающихся на «_AVP», «AVP», «VBA» или «DRW», вирус «SK» уничтожал все файлы на всех логических дисках компьютера, после чего «вешал» систему, вызывая системную функцию «Fatal_Error_Handler». Этот вирус также удалял в директории Windows файл «command.pif» и содержал в своём теле следующий текст: «<C> 1997 VBA Ltd. E-mail:support@vba.minsk.by».

[480] DPMI (DOS Protected Mode Interface) – проф. интерфейс защищённого режима DOS.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Marker
Другие названия	Macro.Word97.Marker, W97M/Marker.kk, WM97/Marker-a, W97M/Spooky
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	февраль 1999 года
Страна происхождения	Соединённые Штаты Америки
Длина	3708 байт

22 февраля 1999 года был обнаружен вирус «Marker.c», дополнивший обширное семейство уже знакомых пользователям надоедливых резидентных в среде MS Word макро вирусов «Marker»[481]. Однако именно этот штамм стал наиболее известным, так как распространился по всему миру и долгое время не покидал всевозможные рейтинговые таблицы ведущих зарубежных и отечественных специализированных изданий.

Макро вирусы семейства «Marker» инфицировали область глобальных макросов (шаблон «normal.dot») при закрытии заражённого документа, однако некоторые версии вирусов делали это и во время открытия, и во время сохранения документов MS Word[482]. В процессе заражения вирусы семейства дописывались к уже существующим макросам документа, если таковые присутствовали. Вирусы этого семейства содержали строку текста, по которой они определяли начало своего программного кода. В различных версиях вируса эта строка могла различаться, например: «<- this is a marker!» (<-это маркер!) или <- this is another marker! (<-это другой маркер!).[483]

Вирусы семейства «Marker» особенно интересны тем, что они вели отчёт об инфицированных компьютерах, дописывая к своему коду строки-комментарии, в которые были включены дата и время инфицирования, а также персональная информация о пользователе (например, адрес пользова-

---

[481] «Marker» (англ.) – «Маркёр».

[482] «Marker.c» инфицирует шаблон «normal.dot» во время открытия, закрытия и сохранения документов MS Word.

[483] «Marker.c» содержит в своём теле следующий текст: «<- this is a -marker! at the beginning of the document» (<- это маркёр! начало документа).

теля в том виде, как он хранится в Windows). После инфицирования компьютерной системы вирус извлекал пользовательскую информацию, которую можно посмотреть вручную через меню MS Word, а затем с использованием встроенной команды «ftp.exe» эта информация загружалась на FTP сайт вирусописателя. Причём, вирус проверял, чтобы информация передавалась единожды, устанавливая с этой целью специальный флаг в реестре операционной системы Windows. Кроме того, вирусы семейства «Marker» отключали в MS Word защиту от макросов.

Техника использования «ftp.exe» чем-то напоминала уже применявшуюся рассмотренным нами вирусом «Caligula», что позволяет сделать следующее предположение – «Caligula» и семейство «Marker» написаны одной и той же группой вирусописателей, известной под названием «CodeBreakers». Ведь, по своей сути, вирус «Caligula» тоже использовал реестр Windows для ограничения числа сеансов исходящей связи. Вполне вероятно также, что эти вирусы были разработаны в качестве своеобразного отклика на одну из публикаций 1997 года, где описывались практические приёмы атаки на PGP и предсказывалось «светлое будущее для «шпионящих» вирусов». Поддерживая регистрацию времени инфицирования, шпионящий агент позволял своему оператору изучать связь между членами целевой организации. Например, сообщение, перечисляющее персональную информацию о жертвах и времени инфицирования, могло быть использовано для того, чтобы сделать вывод о том, насколько тесно эти индивиды работают вместе. Такая информация может быть использована, к примеру, для электронной атаки выбранной цели или электронного нападения при помощи использования элементов социальной инженерии.

Вирусы семейства «Marker» проявляли себя различными способами. Родоначальник «Marker» в июле, начиная с 23-го числа, выводит достаточно длинные текстовые сообщения, а «Marker.c» и некоторые другие штаммы ведут себя в инфицированной системе очень скрытно и не выводят на экран монитора никаких собственных сообщений или предупреждений, но зато

«втихую» посылают свои «отчёты» о заражённых ими компьютерах на определённый ftp-сервер.

Кроме того, «Marker.c» создаёт в системном реестре следующую запись: HKEY_CURRENT_USER\Software\Microsoft\MSSetup(ACME)\UserInfo LogFile = True.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Melissa
Другие названия	Melissa.a, W97M.Melissa W97M.Melissa.a, W97M/Melissa.C.Src, WM97/Mailissa, Maillissa, Mid/Melissa, W97M/Mailissa, W97M/Melissa-mm WM97/Melissa@mm, W97M/Assilem, Macro.Word97.Melissa, W2001MAC/Melissa, Assilem, ANNIV, Elecciones, Elecciones2000, W97M_MELISSA, W97M/Elecciones2000, Kwyjibo, Resume, RESUME.WORM
Тип	вирус-червь
Инфицируемые платформы	Windows95/98/ME/NT/2000/XP/2003
Впервые обнаружен	февраль 1999 года
Страна происхождения	Соединённые Штаты Америки
Длина	3706 байт

В конце марта 1999 года мир буквально потрясло известие о внезапно начавшейся глобальной эпидемии первого макро вируса для MS Word, включавшего в себя функциональность Интернет-червя, который получил красивое имя «Melissa»[484] и, впоследствии, стал одной из самых больших знаменитостей в ряду вредоносных компьютерных программ, обзаведясь к тому же весьма обширным семейством[485]. Эта эпидемия была достаточно быстро погашена, но успела принести ощутимый ущерб компьютерным системам во всём мире, и вирус-червь «Melissa» навсегда остался в истории вирусописания[486].

---

[484] Melissa (англ.) – женское имя «Мелисса», бот. «Мята лимонная».

[485] Известны следующие штаммы: .A (обнаружен 29.03.99), .AC (обнаружен 01.11.99), .AG (обнаружен 01.11.99), .AK (обнаружен 01.11.99), .AL (обнаружен 17.01.01), .AM (обнаружен 07.03.01), .AO (обнаружен 16.03.00), .AU (обнаружен 27.03.00), .BE (обнаружен 05.00), .BI (обнаружен 07.00), .BG (обнаружен 26.05.00), .I (обнаружен 09.01.01), .L (обнаружен 09.99), .M (обнаружен 07.07.99), .O (обнаружен 19.12.00), .Q (обнаружен 22.07.01), .R (обнаружен 07.08.01), .U (обнаружен 15.10.99), .V (обнаружен 20.10.99), .W (обнаружен 17.01.01), .X (обнаружен 01.01), .Z (обнаружен 01.11.99), .gen (обнаружен 21.01.02).

[486] Melissa virus creator pleads guilty, BBC News Online, 9 December 1999.

Melissa Computer Virus Writer, David Smith, Pleads Guilty in Federal Court, ICSA, 9 December 1999.

Ian Whalley, Melissa – The Little Virus That Could, Virus Bulletin, May 1999.

Этот макро вирус и его штаммы, одновременно являющиеся червями, активизировались в среде MS Word и отключали макрокоманды защиты текстового процессора. При открытии пользователем инфицированного документа, он автоматически посылал электронную почту первым 50 адресам[487] (некоторые штаммы имели другие или вообще не имели ограничений) во всех адресных книгах MS Outlook (с использованием MAPI[488] запросов), а для присоединения инфицированного документа использовался MS Outlook. Когда пользователь открывал или закрывал заражённый документ, «Melissa» сначала проверял по параметру ключа реестра HKEY_CURRENT_USER\Software\Microsoft\Office\ «Melissa?», была ли массовая рассылка электронной почты и, если параметр ключа реестра имел значение «Melissa?», устанавливал себя в «Kwyjibo» (для штаммов справедливо «Elecciones2000»=«Pacocha:-P», «MelissaFX», «Mmmmmmm?», «MP?»), производя массовую рассылку.

Причём, в противном случае, вирус-червь не инфицировал уже заражённый компьютер второй раз. Для некоторых штаммов «Melissa» создавались их копии в следующих файлах: C:\Data\normal.dot и C:\Windows\StartMenu\Programs\StartUp\explorer.doc. Вирус-червь постоянно находился в модуле «ThisDocument» (в этом модуле удаляется любой резидентный код), который переименовывался вирусом в «Melissa» и получал управление, когда документ открывался или закрывался, используя команды обработчика «Document_Open» и «Document_Close». Обработчик «Document_Open» отвечает за дублирование, используя MS Outlook, а обра-

---

Carey Nachenberg, Computer Parasitology, Proceedings of the Ninth International Virus Bulletin Conference, September/October 1999.

[487] Подобно рассмотренному нами выше «Ska» вирус-червь «Melissa» делал это абсолютно незаметно для пользователя и от его имени.

[488] MAPI (Messaging Application Programming Interface) – проф. интерфейс прикладного программирования для электронной почты корпорации Microsoft.

ботчик «Document_Close» за удаление файлов, используя язык программирования VBA.

«Melissa» инфицировал документы (используя нормальные механизмы заражения макро вирусом) и при отсутствии MS Outlook – следующим образом:

пользователь открывает документ, содержащий инфекцию – вирус-червь;

вирус-червь инфицирует новый для этого компьютера документ (пользователь не имеет установленного MS Outlook);

пользователь посылает по электронной почте документ другому пользователю, который не заражён, но имеет MS Outlook;

когда другой пользователь открывает инфицированный документ на своём компьютере, документ рассылается по электронной почте в 50 адресов через MS Outlook.

«Melissa» всячески пытался скрыть следы своей деятельности, отключая следующие пункты меню MS Word:

инструментальные средства, тем самым, предотвращая доступ пользователя к листингу макрокоманд (при запуске вирус-червь отключал макрокоманду защиты вируса в параметрах MS Word и использовал некоторые ухищрения для сокрытия себя от эвристических сканеров);

макро защиту, устанавливая значение HKCU\Software\Microsoft\Office\9.0\Word\ Security\Level для отключения опции меню «Tools/Macro/Security» (отключение этого пункта меню предотвращает доступ пользователя к изменению уровня защиты).

Кроме того, для сокрытия своих действий вирус-червь отключал следующие параметры:

подсказку для сохранения нормального шаблона – параметр «SaveNormalPrompt»;

подтверждение преобразования при открытии – параметр «ConfirmConversion»;

макро вирусную защиту – параметр «VirusProtection».

Интересно, что штамм «Melissa.X», изначально созданный для Macintosh Word, был способен инфицировать и MS Word для операционных систем Windows.

В течение десятого часа десятого дня каждого месяца «Melissa» мог сохраняться 5 раз в файлах, имена которых выбирались из дня, года, месяца и секунд текущего времени. Первоначально этот вирус-червь запускался в файле «list.doc», более поздние штаммы обычно запускались под именем «anniv.doc», но могли иметь и другие имена. В теле «Melissa» содержится текст: «Melissa modified, !hello aisyalaM», и комментарии: «WORD/Melissa written by Kwyjibo «Works in both Word 2000 and Word 97 «Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!» Word -> Email | Word 97 <--> Word 2000 ... it's a new age!» («Модифицированная Melissa, Привет, Малайзия! (*прим.* написано наоборот)», и комментарий: «WORD/Мелисса написан Квийбо «Работает в Word 2000 и Word 97 «Червь? Макро вирус? Вирус для Word 97? Вирус для Word 2000? Решайте сами!» Word -> Email | Word 97 <--> Word 2000 ... это новое поколение!»). 25-ого декабря вирус-червь мог отображать на экране монитора стандартное окно сообщений Windows с текстом «(C) 1999 CyberNET. Vine... Vide... Vice... Moslem Power Never End... You Dare Rise Against Me... The Human Era is Over, The CyberNet Era Has Come!!!» («(C) 1999 CyberNET. Виноградная лоза... Смотри... Порок... Мусульманская мощь никогда не иссякнет... Вы посмели бунтовать против меня... Эпоха человека закончена, наступила эра CyberNet!!!») и вставлять случайное число цветных форм в текущий документ MS Word. Кроме указанных визуальных эффектов «Melissa» мог три раза подавать звуковой сигнал и высвечивать на экране монитора окно сообщения с текстом: «MS Word. Please Check Your OutLook Inbox E-Mail!» («MS Word. Пожалуйста, проверьте Ваш MS Outlook Inbox E-Mail!»).

Разные штаммы «Melissa» могли производить целый набор действий по изменению, удалению файлов и т. п., обобщённый перечень которых можно представить следующим образом:

изменение файла C:\autoexec.bat для попытки форматирования диска C:, когда компьютер будет перезагружен;

попытки удаления всех файлов на логических дисках C: ... Z: при наступлении 9 апреля;

удаление данных с сетевых дисков M:, N:, O:, P:, Q:, S:, F:, I:, X:, Z:, H: и L:;

удаление файлов C:*.*, C:\MyDocuments*.*, C:\Windows*.*, C:\Windows\System*.*, C:\Winnt*.*, C:\Winnt\System32*.* и A-Z:*.*;

удаление системных файлов с целью создания неустойчивости в работе компьютерной системы;

попытки удаления файлов корневых директорий с локальных дисков F:, H:, I:, L:, M:, N:, O:, P:, Q:, S:, X: и Z:;

попытки удаления файлов «io.sys», «command.com», «ntdetect.com» и «suhdlog.dat» в корневом директории на логических дисках C: и D:;

изменение параметров настройки MS Word и инфицирование документов;

разрушение сервера электронной почты;

потребление большого количества сетевых ресурсов и быстрое распространение.

«Melissa» мог предоставить другим пользователям доступ к вашему компьютеру, что могло привести к потере конфиденциальной информации вследствие пересылки её по электронной почте компьютерному злоумышленнику:

сделать диск C: доступным для совместного использования, позволив другим пользователям в сети видеть «жёсткий» диск как «MelissaFX»;

отослать системную информацию: имя пользователя, название компьютера и организации, параметры настройки часового пояса и т. п. по не-

скольким адресам электронной почты: infx@iname.com, fafx@fastermail.com и apfx@apexmail.com;

использовать функции MAPI в MS Outlook, чтобы отыскивать текущие параметры пользователя и пароля для входа в систему сервера.

После всего сказанного Вы, наверное, согласитесь, что даже в условиях, когда ежедневно появляются десятки новых компьютерных вирусов, такой образчик вирусописательства как «Melissa» представлял собой для компьютерного сообщества неординарное событие. Впервые вирус-червь «Melissa» появился в Интернет 26 марта, а затем события разворачивались подобно катящемуся с горы снежному кому. «Он распространялся так быстро, что мы не могли изолировать его в каком-нибудь географическом регионе. По скорости распространения этот вирус побил все рекорды», – заявлял Уильям Орвис, сотрудник отдела информационных технологий всемирно известной Ливерморской лаборатории[489]. На многих Web-узлах были отключены почтовые системы, чтобы остановить волну самостоятельно распространяющихся писем в электронной почте. Даже такие гиганты индустрии как Microsoft, Intel, Dell, Lockheed Martin, Lucent Technologies были вынуждены временно отключить свои корпоративные службы электронной почты, продемонстрировав всему миру уязвимость своих почтовых серверов перед лицом угрозы со стороны такой вредоносной компьютерной программы.

В тот же день 26 марта весь персонал SARC был вызван на работу для борьбы с этой заразой. Потребовался примерно час для создания процедур обнаружения вируса и лечения заражённых им файлов. Антивирусные программы были отправлены всем пользователям, сообщившим о вирусе. Кроме того, они были размещены на серверах, которые автоматически отправляли их всем, кто направлял в Symantec образцы «Melissa». Специалисты SARC работали и ночью, постоянно тестируя и публикуя все новые определения

---

[489] Один из ведущих национальных научно-исследовательских центров США, разработчик термоядерного, лазерного и нейтронного оружия.

вируса для Norton AntiVirus, а вся работа, включая исследование и описание вируса-червя, была полностью закончена только к трём часам ночи 27 марта. Следующие два дня сотрудники SARC отвечали на многочисленные звонки и давали интервью прессе. Впервые за последние несколько лет в воскресенье 28 марта с предупреждением об угрозе вируса «Melissa» к общественности обратились ФБР США и NIPC[490] США, и в понедельник им потоком пошли звонки от пострадавших или обеспокоенных пользователей. В распространённом заявлении NIPC, говорилось о многочисленных сообщениях по поводу распространения вируса в коммерческих, государственных и военных системах: «Эксперты по компьютерной безопасности характеризуют «Melissa» как самый быстро распространяющийся вирус, какой они когда-либо встречали. Число заражений растёт, как снежный ком, несмотря на характерное для выходных дней снижение трафика электронной почты». Представители CERT[491] в Университете Карнеги-Меллона сообщили, что к вечеру воскресного дня вирусом были поражены более 100 предприятий и организаций. «Сотни и тысячи машин на каждом из них лишены способности принимать, и отправлять почту, – сказал руководитель центра Джефф Карпентер. – Однако это ничто по сравнению с тем, что может произойти в понедельник».

В этой и без того «грозовой» атмосфере, как нарочно, для ещё большего обострения сложившейся ситуации, в Интернет конференции «alt.sex» были обнаружены сразу два новых вируса. Причём один из них оказался «Melissa» для MS Excel, который должен был делать то же самое, что и «Melissa» для MS Word, но, как показал тщательный анализ, оказался нежизнеспособ-

---

[490] NIPC (National Infrastructure Protect Center) – Центр защиты национальной инфраструктуры, – специальная организация, созданная с целью защиты национальных информационных ресурсов.

[491] CERT (Computer Emergency Response Team) – Группа компьютерной скорой помощи. Организация, следящая за угрозами безопасности сетевых компьютеров, в том числе и в Интернет.

ным[492]. Тем временем специалисты в области информационных технологий спешили предупредить пользователей о проблеме, рекомендуя им не открывать вложенные в сообщения документы и обновить своё антивирусное программное обеспечение. «Пользователи могут оказать существенное влияние на распространение эпидемии, – сказал директор NIPC Майкл Вейтис. – Я призываю их проявлять бдительность при чтении электронных писем в течение нескольких следующих дней и сообщать о подозрительных поступлениях администратору».

Как часто бывало и раньше, в погоне за сенсацией специалистам стали досаждать средства массовой информации. Однако произведённая «Melissa» шумиха дала и положительный эффект, так как эта эпидемия лишний раз показала, как важно пользоваться антивирусными средствами, а также окончательно открыла глаза сомневающимся на тот факт, что на смену создававшим относительно безопасные штамповки вирусописателям приходят опасные и квалифицированные злоумышленники, которые ориентированы на кражу из незащищённых компьютерных систем сведений, имеющих конфиденциальный характер, таких как информация о кредитных карточках и др.

Вирус-червь «Мелисса» произвёл беспрецедентные разрушения в системах электронной почты огромных корпораций и отдельных пользователей по всему миру, став первым в длинном списке крайне вредоносных вирусов и «червей» и заставив крупных производителей антивирусных средств обратить внимание на создание управляемых служб защиты. «Думаю, было бы ошибкой считать, что пользователи сегодня готовы отразить все угрозы и обезопасить себя от всех ошибок, которые могут возникнуть в «защищённом периметре» их систем. Управляемые службы – единственный выход из положения. Сейчас очень многие производители предлагают службы. Это

[492] Тем не менее, в SARC была создана программа для обнаружения и лечения этого вируса, а главное, его возможных модификаций.

весьма разумно», – заявлял, например, аналитик компании Yankee Group Меттью Ковар.

Как утверждал Джеф Джонсон, директор компании Meta Secur E-com, вирус-червь «Мелисса», распространявшийся по электронной почте, затронул так много компаний потому, что «последние применяли приобретённые системы защиты без должного руководства». По заявлению представителей McAfee, компания Elron Software уже запланировала объединить разработанное McAfee антивирусное программное обеспечение с семейством собственных продуктов Internet Policy Management, что позволит поставщикам услуг предложить своим клиентам более надёжную защиту от вредоносных компьютерных программ.

Symantec приобрела за 20 млн. долл. подразделение компании L-3 Network Security, занимавшееся оценкой рисков уязвимости систем и предлагавшее консультации по вопросам защиты, с целью улучшения качества пред и после продажного обслуживания заказчиков, что свидетельствовало о намерении компании утвердиться на рынке управляемых служб.

Примеры можно множить…

Вместе с тем существовали и другие точки зрения. Как отмечал менеджер подразделения Debit Point of Sale Products корпорации Visa Марк Перл, его компания «не намерена обращаться к услугам независимой фирмы, поскольку обладает ресурсами, достаточными для самостоятельной поддержки систем защиты, однако подобные службы могут оказаться весьма полезными для многих фирм». Неуверенность в том, что предоставление производителями антивирусного программного обеспечения управляемых служб принесёт заметную пользу наиболее явно звучит в заявлении уже упоминавшегося Джефа Джонсона: «Я думаю, что обращаться за подобного рода помощью к конкретному производителю антивирусов довольно опасно, поскольку в таком случае вы будете «привязаны» к определённому программному обеспечению. Я бы не рекомендовал использовать в качестве поставщика управляемой службы компанию, которая продаёт вам свои продукты».

Итак, вирус-червь «Melissa» вызвал эпидемию мирового масштаба, поразил десятки тысяч компьютеров и нанёс ущерб, измеряемый десятками миллионной долларов. А где же главный герой? Правоохранительные органы США, занимающиеся киберпреступностью, быстро отреагировали на эпидемию «Melissa», автор был вычислен по телефонному номеру в службе America Online и 1 апреля 1999 года арестован по обвинению в нарушении общественных коммуникаций, сговоре и хищении компьютерных услуг. Это был 31-летний программист из штата Нью-Джерси, некий Дэвид Л. Смит. В записке по делу, представленной в Верховный суд штата заместитель генерального прокурора по надзору Кристофер Д. Бабб утверждал, что Смит не воспользовался своим правом сохранять молчание и ответил на все вопросы следователей, когда полиция проникла в его квартиру. «Смит признался, в числе прочего, в создании макро вируса «Melissa», нелегальном доступе в систему электронной оперативной службы America Online для внедрения этого вируса в киберпространство и в нарушении работы персональных компьютеров, использованных для распространения «Melissa»», – подчеркнул Кристофер Д. Бабб.

Уже 9 декабря 1999 года Дэвид Л. Смит предстал перед судьёй Верховного суда округа Монмут (Нью-Джерси) Джоном Рикарди за создание и распространение вируса-червя «Melissa», причём, ему вменялась статья, по которой он максимально мог быть осуждён на 10 лет тюремного заключения и приговорён к штрафу в размере 400 тыс. долл. Однако судебные разбирательства затянулись, и окончательный приговор был вынесен лишь в начале марта 2002 года. В суде на обвинения в «безнравственности» Смит ответил, что в основе созданного им вируса лежали программы, найденные в Интернет, и что «Melissa» не портила данные, а только лишь «ухудшила работу электронной почты, которая и так отравляла жизнь многим». Однако суд пришёл к выводу, что ущерб от деятельности вирусописателя составил более 80 миллионов долларов, и по его решению Смит был оштрафован на 5 тыс. долл., и ему грозило 5 лет лишения свободы. Но, как сообщала Associated

Press, «власти сократили срок, сославшись на помощь в предоставлении информации относительно других создателей вирусов». В итоге создатель компьютерного вируса-червя «Melissa» 33-летний Дэвид Л. Смит был признан виновным и осуждён на 20 месяцев заключения в федеральной тюрьме США «за совершение компьютерных взломов, рассылку вредоносных программ и многомиллионный ущерб, причинённый в 1999 году работе электронной почты во всём мире».

Таким образом, Дэвид Л. Смит стал одним из первых осуждённых создателей компьютерных вирусов. Вынесенный вердикт суда он назвал «колоссальной ошибкой». Несколько другого мнения придерживается известный нам главный технический советник антивирусной компании Sophos Грэхэм Клули, который заявил: «Это весьма недвусмысленное послание всем вирусописателям. Распространение вирусов может приводить к нанесению солидного финансового ущерба. Власти подготовлены к установлению личностей, причастных к распространению вирусов, и передаче их в руки Фемиды. Самое время людям стать взрослыми и начать вести себя, как ответственные члены электронного сообщества».

В апреле разразилась эпидемия вируса «Chernobyl», о чём мы подробно говорили в материале за 1998 год, а уже 7 мая вирусы освоили новую «нишу» – популярный графический пакет Corel DRAW.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Gala
Другие названия	GaLaDRieL, CS.Gala
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	апрель 1999 года
Страна происхождения	Португалия
Длина	1 модуль

Вирус, получивший имя «Gala»[493], написанный на «скрипт» языке Corel SCRIPT и не обладающий какими-либо деструктивными возможностями, стал первым известным в мире компьютерным вирусом, способным заражать файлы Corel DRAW!, а также файлы приложений Corel PHOTO-PAINT и Corel VENTURA. Ведущие специалисты-вирусологи сразу оценили вероятность широкого распространения этого вируса как крайне незначительную, так как число пользователей, использующих «скрипты» Corel DRAW или обменивающихся ими, невелико. Однако он был первый и, уже благодаря этому, безо всякого сомнения, вошёл в историю вирусописания.

При активизации заражённого «скрипта» вирус начинал поиск в текущем директории других «скриптов» CorelDraw, то есть файлов с расширением «*.csc», считывал их содержимое и искал первый инфицированный и первый незаражённый «скрипты». Затем «Gala» считывал свой программный код из инфицированного «скрипта» и копировал его в начало заражаемого в настоящий момент. При этом первоначальное содержимое заражаемого «скрипта» сдвигалось вниз, и он оставался в работоспособном состоянии. Таким образом, при каждом старте вирус инфицировал лишь один «скрипт» файл и сразу после этого передавал управление на оригинальный «скрипт» код инфицированного файла.

В процессе заражения «Gala» использовал временный файл «mallorn.tmp», сначала записывая в него программный код заражаемого «скрипта», а потом замещая инфицируемый файл своим программным кодом и до-

[493] «Gala» (англ.) – «Торжество».

писывая к нему данные из файла «mallon.tmp», то есть первоначальное содержимое инфицируемого файла.

Визуально вирус «Gala» вел себя скрытно и проявлялся только 6 июня, когда выводил на экран монитора следующее текстовое сообщение: «GaLaDRieL ViRUS bY zAxOn/DDT. Ai! lauriл lantar lassi sъrinen!.Yйni ънytime ve rбmar aldaron, yйni ve linte yuldar vбnier mi oromardi lisse-miruvyreva Andъne pella Vardo tellumar nu luini yassen tintilar i eleni ymaryo airetбri-lirinen ....» Кроме того, вирус содержал комментарии, расположенные в самом начале и в самом конце его программного кода: «REM ViRUS GaLaDRieL FOR COREL SCRIPT bY zAxOn/DDT. REM END OF ViRUS GaLaDRieL bY zAxOn/DDT».

Интересно, что сама возможность существования вируса «Gala» для Corel DRAW! основана на том факте, что эта программа, как и некоторые другие мощные системы обработки графической информации, поддерживает дополнительные программы, написанные на «скрипт» языках. Эти «скрипты» используются для настройки Corel DRAW! под конкретные задачи, решение которых не входит в стандартные возможности пакета. «Скрипт» язык в Corel DRAW! «родственен» языку Visual Basic, применяемому в MS Office, и поддерживает большое количество функций, в том числе функции работы с файлами. Следовательно, «скрипты» Corel DRAW! позволяют искать файлы, читать из них и писать в них, искать в них необходимые данные, то есть имеют всё самое необходимое для создания вирусов.

Идентификационная карточка вредоносной компьютерной программы	
Имя	PrettyPark
Другие названия	I-Worm.PrettyPark, W32/PrettyPark-mm, W32.PrettyPark, W32/PrettyPark, W32/PrettyPark.a, W32/PrettyPark.37376-m, TROJ_PRETTY_PARK, W32/Pretty.gen@MM, W32/Pretty
Тип	вирус-червь, «троянский» конь
Инфицируемые платформы	Windows95/98/ME/NT/2000/XP/2003
Впервые обнаружен	май 1999 года
Страна происхождения	Франция
Длина	37376 байт

18 мая был зарегистрирован в «диком» виде и сразу вызвал эпидемию вирус-«червь» быстро распространяющий свои копии через Интернет и обладающий «троянской» компонентой, который получил название «PrettyPark»[494] и был написан на языке программирования «Delphi» специально под 32-х разрядные версии операционной системы Windows[495].

Этот вирус-червь попадал в компьютерную систему в виде письма с вложенной ложной утилитой «PrettyPark», являющейся на самом деле кодом червя. При запуске он инсталлировал себя в операционную систему и затем рассылал свои копии по адресам, обнаруженным в адресной книге Windows – Windows Address Book, информируя автора «PrettyPark» через каналы IRC о заражении компьютера. Червь использовался и как утилита удалённого доступа к компьютеру (так называемая «Backdoor»-программа), представляя собой выполняемый файл Windows в формате PE EXE длиной 37376 байт и упакованный архиватором «WWPack32». После распаковки он становился 58 Кб файлом, созданным при помощи компилятора языка «Delphi». Причём «чистый» код занимал всего лишь порядка 45 Кб, что считается очень небольшой величиной для программных приложений, написанных на языке «Delphi». Вместе с тем в 45 Кб код «уместилось» такое количество функций, которого вполне достаточно

[494] «PrettyPark» (англ.) – «Прелестный парк».

[495] В среде операционных систем Windows 3.x, а также DOS, Linux, Macintosh, OS/2 и UNIX «PrettyPark» неработоспособен.

для реализации процедур распространения «PrettyPark» через Интернет, а также воровства паролей и удалённого управления компьютерной системой.

При запуске инфицированного файла червь проверял системную память Windows и искал в ней свою уже загруженную копию. Если таковой не было, червь оставался в оперативной памяти операционной системы как невидимое в списке задач, то есть скрытое, приложение и запускал процедуру своей инсталляции. Эта процедура копировала заражённый файл в системный директорий Windows под именем «files32.vxd» и регистрировала его в системном реестре таким образом, что файл «files32.vxd» запускался при старте каждой выполняемой программы. С этой целью «PrettyPark» создавал новый ключ по имени exefile\shell\open\command, который был ассоциирован с файлом «files32.vxd», то есть копией червя, в системном реестре в HKEY_CLASSES_ROOT. Этот файл имел расширение «*.vxd», однако он являлся не VxD-драйвером Windows, а абсолютно нормальной программой 32-х разрядной операционной системы Windows. В том случае, когда при инсталляции червя происходила ошибка, червь активизировал screensaver «sspipes.scr» или, если этот файл не был обнаружен, «PrettyPark» выводил на экран монитора другую заставку – «Canalisation3D.SCR».

Затем червь инициализировал канал доступа в Интернет и запускал две дополнительные процедуры своего процесса: первая вызывалась один раз в 30 секунд, а вторая – один раз в 30 минут. Первая процедура при её вызове каждый раз пыталась выйти на связь с одним из заданных IRC-каналов и при помощи специальных команд передать сообщение о своей активности автору «PrettyPark», который таким образом отслеживал процесс распространения червя и получал информацию об инфицированных компьютерах. Список IRC-каналов, в которые передавались сообщения, выглядит следующим образом: irc.twiny.net, irc.stealth.net, irc.grolier.net, irc.club-internet.fr, ircnet.irc.aol.com, irc.emn.fr, irc.anet.com, irc.insat.com, irc.ncal.verio.net, irc.cifnet.com, irc.skybel.net, irc.eurecom.fr, irc.easynet.co.uk. Будучи опознанным «хозяином», червь мог управляться как программа удалённого админи-

стрирования системы («Backdoor») и при помощи набора команд высылать ему конфиденциальную информацию: имя компьютера, имя и код продукта, системную конфигурацию, информацию о владельце компьютера и организации, путь к корневому директорию, расположение поддиректориев и файлов, номер версии, пароли доступа в Интернет и ICQ, номера и псевдонимы ICQ, адреса электронной почты, имена («логины») и пароли удалённого доступа, телефонные номера для доступа в Интернет и т. п. Кроме того, программа удалённого администрирования системы могла выполнять и ряд других функций, например, сообщать техническую информацию об установленных «жёстких» дисках, периферии и пр., создавать и уничтожать директории, создавать, уничтожать и запускать файлы и т. д. Также необходимо подчеркнуть, что существующее соединение с IRC открывало для злоумышленника специальный «чёрный ход» в системе защиты, через который компьютер-жертва потенциально мог быть в любое время использован для несанкционированного получения и запуска на выполнение файлов.

Вторая процедура, которая вызывалась один раз в полчаса, открывала адресную книгу Windows, считывала из неё список адресов в Интернет, а затем посылала по ним сообщение, причём письмо могло быть отослано не только на персональный адрес, но и по адресу какой-либо конференции в Интернет. Поле «Subject» этого сообщения содержало следующий текст: «C:\CoolProgs\Pretty Park.exe» Само сообщение пустое, но к нему присоединена копия червя в виде файла «PrettyPark.exe».

Вирус «PrettyPark» и его штаммы быстро распространились по всему миру, и вызванные ими эпидемии, то вспыхивая, то затухая, продолжались на протяжении нескольких последующих лет. Недаром, например, известная фирма-разработчик антивирусного программного обеспечения Network Associates даже весной 2000 года информировала своих пользователей в следующих выражениях: «Вирус «PrettyPark», который свирепствовал в прошлом году, вернулся в новой модификации, и ей оказались инфицированы компьютеры сразу двенадцати крупных корпоративных и правительственных сетей!

… Вообще говоря, вирус был вновь обнаружен ещё в середине февраля, но в то время его квалифицировали как довольно безобидный. Однако, согласно поступающим сейчас отчётам, «PrettyPark» распространяется чрезвычайно быстро». Информационный портал Infoart в сообщении под заголовком ««South Park»[496] – вирус, созданный по мотивам мультипликационного сериала» добавлял к этой картине свои краски: «В настоящее время в европейских странах среди детей большую популярность приобрёл мультипликационный сериал «SouthPark». Письмо, заражённое вирусом, содержит иконку с изображением одного из персонажей телесериала – Куле, а также подпись пользователя, с компьютера которого был отправлен e-mail, то есть получатель на первый взгляд не обнаружит ничего необычного, хотя письмо содержит опасный вирус». Известный разработчик антивирусного программного обеспечения компания Finjan Software сообщала о появлении второй версии вируса-червя «SouthPark» в следующих выражениях: «Вирус PrettyPark II рассылается по электронной почте в присоединённом файле. Попав на компьютер, вирус каждые 30 минут рассылает себя по адресам из адресной книги в почтовой программе Microsoft Outlook. На компьютеры с другими почтовыми программами он не действует. Кроме того, что этот червь может вывести из строя почтовые серверы из-за их перегрузки, он ещё и рассылает пароли с компьютера-жертвы в несколько чатов. Следует отметить, что первая версия этого вируса рассылалась в файле, заархивированном с помощью утилиты «WWPack». В новой версии, наверное, чтобы запутать антивирусные программы, файл «PrettyPark.exe» размером 60928 байт распространяется в неупакованном виде. В письме с вирусом в поле «тема» указывается «C:\CoolProgs\PrettyPark.exe», а само письмо содержит только указанный присоединённый файл».

---

[496] «SouthPark» – «Южный парк», известен также под именем PrettyPark II. Официальное название этого вируса-червя «Pretty.worm.unp». По данным Computer Associates впервые его появление в «диком» виде было зафиксировано в Австрии.

Компания McAfee тоже опубликовала предупреждение о появлении вируса-червя «SouthPark», который: «является новым вариантом ранее обнаруженного червя «PrettyPark» и представляет довольно большую опасность, так как он может инициировать массовую рассылку писем по электронной почте с последующим выходом из строя почтовых серверов из-за их перегрузки. Вирус «SouthPark» уже обнаружен в сетях ряда ведущих компаний США, а также в компьютерных системах американских правительственных организаций, университетов и Интернет-компаний. Червь «SouthPark» поражает компьютеры с операционными системами Windows 9x/NT, причём внешних симптомов заражения пользователь может и не обнаружить… В отличие от вируса «Melissa», который рассылал себя по 50 первым адресам из адресной книги пользователя заражённого компьютера, вирус «SouthPark» рассылает себя по всем адресам из адресной книги, причём делает это каждые 30 минут. В этом отношении «SouthPark» гораздо опаснее вируса «Melissa». Кроме того, вирус пытается подключиться к IRC-серверу (чат) и послать туда информацию о пользовательском компьютере. По этому же каналу вирус может получать и команды злоумышленника, то есть вирус «SouthPark» одновременно является и троянским конём».

Идентификационная карточка вредоносной компьютерной программы	
Имя	ExploreZip
Другие названия	I-Worm.ZippedFiles, ZippedFiles,Worm. ExploreZip, W32/Explore Zipm, W32/ExploreZip
Тип	вирус-червь
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	июнь 1999 года
Страна происхождения	Израиль
Длина	210432 байта

В начале лета, 6 июня, разразилась эпидемия чрезвычайно деструктивного, подобно вирусу «Melissa», и одного из самых опасных и «дорогостоящих» для компаний Интернет-червя по имени «ExploreZip»[497], который, впервые появившись в Израиле, стал планомерно уничтожать документы в компьютерах США, Великобритании, Германии, Франции и Чехии и других стран. Он представлял собой выполняемый файл, который после внедрения в систему уничтожал файлы некоторых популярных приложений. Хотя этот «червь» и не получил такого же распространения, как «Melissa», оценки нанесённого им ущерба были гораздо выше. Специалисты-вирусологи подчёркивали, что: «Этого и следовало ожидать – за нашумевшим вирусом «Melissa» последовал аналог с деструктивной компонентой, и на этот раз Microsoft испытала мощь собственных технологий на себе». В течение двух дней, четверга и пятницы, вирус «ExploreZip» распространился по всему Интернет и поразил сети крупнейших компаний, включая и Microsoft. Лондонская компания Guy Martin потеряла за четверг 14 тыс. файлов, с помощью Microsoft одолела заразу, но в пятницу опять была инфицирована одним из клиентов. Sky Television и Financial Times, General Electric, Southern и Credit Suisse First Boston также подверглись нападению и их компьютерные файлы были повреждены, а Data Fellows UK даже сообщила, что «ExploreZip» целиком «положил» почтовые системы Boeing и Price Waterhouse Coopers, оставив 300 тыс. человек без электронных коммуникаций. Особенно пострадали системы электронной

[497] Steven Braggs, Richard Wang, Seek and Destroy, Virus Bulletin, August 1999.

коммерции, во многом полагающиеся на передачу данных по электронной почте.

Несмотря на своевременные меры по нейтрализации этого «червя», предпринятые антивирусными компаниями, в декабре 1999 года был зарегистрирован рецидив штамма «ExploreZip». Отличие этой модифицированной версии заключалось в том, что его тело было заархивировано утилитой сжатия Neolite. Таким образом, если антивирусная программа не поддерживала этот формат сжатия, «червь» становился для неё невидимым. А таких программ на тот момент было 100%, и только в январе 2000 года в «AntiViral Toolkit Pro» (AVP) была интегрирована поддержка файлов, обработанных утилитой Neolite.

Но давайте рассмотрим данного «монстра» поближе, используя при этом доступные материалы специалистов-вирусологов, вынужденных в своё время «препарировать» и скрупулёзно изучить эту опасную компьютерную заразу. Вирус-червь «ExploreZip», поражающий компьютеры под управлением 32-х разрядных версий операционной системы Windows[498], распространял свои копии через Интернет и по локальной сети. На компьютер попадал обычно в виде письма с вложенным файлом с расширением «*.exe», а именно – «Zipped_Files.Exe», являющимся на самом деле кодом «червя». Этот файл представлял собой программу длиной в 210 Кб, написанную на языке программирования «Delphi», и его большую часть занимали библиотеки, классы и данные «Delphi», а примерно 10 Кб занимал программный код самого «ExploreZip». При запуске «червь» инсталлировал себя в операционную систему Windows и начинал рассылать свои копии в виде писем электронной почты. В целях сокрытия своей деятельности он при запуске инициировал вывод сообщения об ошибке: «Error. Cannot open file: it does not appear to be a valid archive. If this file is part of a ZIP format backup set, insert the last disk of the back-

[498] Под управлением операционных систем Windows 3.x, Macintosh, UNIX и Linux недееспособен.

up set and try again. Please press F1 for help». («Ошибка. Не могу открыть файл: он не является действующим архивом. Если этот файл является частью многотомного набора резервирования в формате ZIP, вставьте последний диск этого набора и повторите попытку. Пожалуйста, нажмите F1 для подсказки»); и в фоновом режиме выполнял свои процедуры.

Для инсталляции своей копии в операционную систему «червь» копировал себя в каталог Windows под именем «_setup.exe» и в системный каталог Windows под именем «explore.exe», например: C:\Windows_setup.exe, C:\Windows\System\explore.exe. После этого «ExploreZip» регистрировался в конфигурационном файле Windows таким образом, что при каждом запуске операционной системы автоматически выполнялась его копия. Для этого он прописывал в конфигурационный файл команду автозапуска «run=», которая указывала на одну из копий «червя» – «_setup.exe» или «explore.exe». В зависимости от версии Windows процесс регистрации происходил одним из двух способов. «Червь» регистрировал себя или в файле «win.ini» (в случае Windows 95 и Windows 98), или в системном реестре (под Windows NT). В первом случае в файле «win.ini» секция [windows] дополнялась новым значением команды «run=»: файл win.ini: [windows] run=[имя файла-червя]. Во втором случае запись происходила в ключ системного реестра: HKEY_CURRENT _USERSoftware\Microsoft\WindowsNT\CurrentVersion\Windows: run=[имя файла-червя].

В зависимости от различных условий «червь» регистрировал там одну из своих копий, например: run=_setup.exe, run=C:\WINDOWS\SYSTEM\Explore.exe или run=C:\WINNT\SYSTEM32\Explore.exe. Потом «ExploreZip» мог менять имя своего автоматически запускаемого файла на второе, затем изменять его на первое и т. д. Таким образом, в конфигурационных файлах могли быть обнаружены оба варианта строки «run=». После инсталляции в систему «червь» оставался резидентно в памяти Windows и был активен вплоть до очередной перезагрузки, но не имел активного окна и был невидим для пользователя за

исключением списка задач. Копия «червя» при этом была видна под одним из имён и зависила от того, какая их копий была выполнена: «Zipped_files», «Explore», «_setup». Причём «червь» не проверял свое присутствие в памяти операционной системы и мог быть выполнен неоднократно, и тогда в списке задач были видны сразу несколько его копий. Будучи активным в памяти операционной системы «ExploreZip», запускал четыре «нитки» своего процесса: инсталляция, распространение заражённых писем и две нитки уничтожения файлов. Вторая, наиболее важная «нитка», рассылала с инфицированного компьютера электронные письма, в которые была вложена копия «червя». Для этого «червь» использовал установленную электронную почту, поддерживающую стандартный протокол MAPI: MS Outlook, MS Outlook Express и т. д. При помощи MAPI «ExploreZip» активизировал установленного в системе почтового клиента, пытаясь подсоединиться к нему четырьмя различными способами. После подсоединения к электронной почте «червь» постоянно отслеживал почтовый ящик, проверял входящие сообщения и «отвечал» на них. Письмо-ответ имело ту же «Тему», что и оригинальное письмо, а тело письма-ответа содержало следующий текст: «Hi [имя адресата] I received your email and I shall send you a reply ASAP.Till then, take a look at the attached zipped docs». («Привет [имя адресата] Я получил письмо и отвечу на него при первой же возможности. Пока взгляните на вложенный ZIP-архив с документацией»). Если «червю» удалось определить имя пользователя, то сообщение подкреплялось подписью этого пользователя; если же имя пользователя не было определено – «червь» использовал собственную подпись.

Копия «червя» вкладывалась в письма в виде файла «Zipped_Files.Exe». Он не отвечал на письма дважды и не отвечал на свои собственные письма. Такие письма он определял по символу табуляции, которые добавлял к уже «отвеченным» и отсылаемым заражённым письмам. «Червь» также проверял статус письма и отвечал только на непрочитанные письма. Здесь следует отметить, что оба этих условия (не отвечать на письмо дважды, и отвечать только на непрочитанные письма) опциональны в процедуре рассылки писем

и передаются в неё в виде параметров. В данном «черве» они были установлены в положениях, запрещающих повторную рассылку, однако их значения могли быть легко изменены, что могло привести к массовой рассылке заражённых писем и переполнению почтовых баз данных и лимитов трафика локального провайдера Интернет. В результате процедура рассылки инфицированных писем выглядела следующим образом. При первом старте «ExploreZip» сканировал ящик входящих сообщений и отвечал на все непрочитанные, помечал их при этом символом табуляции и больше не обращал на них внимания. Затем он постоянно проверял этот ящик и, как только в нём оказывалось новое сообщение, немедленно создавал «ответ» с приведённым выше текстом, и отправлял его по указанному в письме адресу отправителя.

«ExploreZip» также распространял свои копии по локальной сети и был в состоянии заражать удалённые компьютеры, если директории Windows на них были открыты для чтения и записи. Для заражения удалённых компьютеров «червь» перебирал все доступные сетевые диски и искал на них файл «win.ini». Если такой файл был обнаружен в каком-либо директории, он копировал туда свой файл «_setup.exe» и на том же диске записывал команду «run=_setup.exe» в конфигурационный файл операционной системы, то есть при следующем перезапуске Windows на удалённом компьютере загружала и выполняла копию «червя».

Кроме всего прочего, вирус «ExploreZip» имел крайне опасную деструктивную функцию, активизируя при каждом запуске два параллельных процесса, которые просматривали локальные и сетевые диски, поддиректории, искали и портили файлы с расширениями «*.c», «*.h», «*.cpp», «*.asm», «*.doc», «*.xls», «*.ppt», то есть исходные тексты программ и файлы MS Office. «Червь» портил файлы таким образом, что их содержимое стиралось, а длина файла становилась нулевой. Восстановлению такие файлы не подлежали. Причём указанные выше процессы искали файлы по-разному. Первый процесс постоянно сканировал логические диски с C: до Z: и портил на них

подходящие файлы, второй процесс делал то же самое с «жёсткими» дисками, подключёнными как сетевые ресурсы (сетевые диски общего доступа).

Таким образом, автору «ExploreZip» удалось удачно скомбинировать плодовитость вируса-червя «Melissa» с разрушительной силой вируса «Chernobyl».

Уже 11 июня в сообщении под красноречивым заголовком «На счету у разрушительного червя тысячи жертв» специалисты компаний Symantec и Network Associates заявляли следующее: «…получился вредоносный код «ExploreZip», распространяющийся по совместимым с MAPI системам электронной почты, таким как Microsoft Exchange, и сметающий всё с «жёсткого» диска. Это первая успешная попытка совместить возможности вирусов «Chernobyl» и «Melissa». «ExploreZip» классифицируется как Интернет-червь[499], так как автоматически распространяется по Интернет посредством e-mail-сообщений… «Червь» пока не причинил ужасных разрушений. Пострадали лишь несколько тысяч компьютеров в США, Германии и Франции. В США заражению подвергся ряд компьютерных фирм, включая и Microsoft. Системные администраторы General Electric стараются изолировать «червя», отключив систему электронной почты компании… Один пользователь, не пожелавший назвать свое имя, получил «червя» через письмо от корреспондента из Microsoft и лишился большинства файлов на «жёстком» диске. «Он коварнее, чем «Melissa», так как приходит в ответ на реальные сообщения», – рассказывает этот пользователь».

Прошло ещё четыре дня, и 15 июня информационное агентство Associated Press ознакомило компьютерное сообщество со следующей информацией: «Новая компьютерная инфекция – червь «ExploreZip», распространилась в четверг через Интернет на десятки тысяч компьютеров по всему миру и привела к поломке нескольких корпоративных систем электронной почты. В

---

[499] Eugene Spafford, The Internet Worm Program: an Analysis, Purdue University Technical Report CSD-TR-823.

понедельник, после относительного затишья, имели место новые вспышки эпидемии. Среди пострадавших – компании Microsoft, Intel, Boeing, SBC Communications, AT&T. Многие компании в четверг просто полностью отключились от Интернет, дабы предотвратить заражение своих компьютеров. Однако имевшие место в понедельник новые вспышки эпидемии объясняются тем, что «червь» передаётся не только по электронной почте: он также распространяется по локальным сетям, когда пользователи открывают файлы на компьютерах друг друга. Достаточно открыть письмо «с сюрпризом» на одном из компьютеров компании, и через довольно короткое время могут оказаться заражёнными все машины, связанные с первой через локальную сеть… Уже с середины прошлой недели ФБР США пытается вычислить автора «червя», но пока о результатах ничего не сообщается (автора «Мелиссы» вычислили довольно быстро). Однако больше настораживают сообщения специалистов, которые озабочены «преемственностью» в создании последних вирусов. Червь «ExploreZip» стал своего рода результатом «скрещивания» вируса-червя «Melissa» (который отличался скоростью распространения и относительной безвредностью) и вируса «Chernobyl» (которому понадобилось довольно много времени, чтобы широко распространиться, однако разрушения он нанёс серьёзные). «ExploreZip» унаследовал в этой эволюции «лучшие черты» – он быстро распространяется и наносит серьёзный вред. И, хотя код «ExploreZip» сложнее, чем код «Melissa», специалисты предсказывают, что вирусописатели будут использовать его для создания новых модификаций, которые могут появиться уже в ближайшее недели».

Не так часто инциденты, происходящие в области компьютерной безопасности, имели тревожные последствия для всех остальных сфер применения информационных технологий, но широкое распространение в мире «ExploreZip» стали относить именно к таким явлениям. Проводя аналогию между «ExploreZip» и знаменитым червём Морриса[500], разрушившим системы

[500] Более подробно о сетевом «черве» Морриса см. в настоящей книге – 1988 год.

информационной безопасности в 1988 году, и анализируя сходство и различие двух этих вторжений, нельзя не отметить, что за прошедшие десять лет компьютерный мир продвинулся довольно далеко. Код червя Морриса для того времени был написан очень элегантно. Самопроизвольно распространяющаяся программа искала в стандартных таблицах UNIX-серверов ссылки на удалённые соединения, анализируя одновременно уязвимые места в таких службах, как Finger и Sendmail, и через обнаруженные бреши копировала себя на другие серверы. Данный механизм распространения оказался весьма эффективным для проникновения в относительно открытую среду Интернет, какой она была в конце 80-х. «Червь» искусно маскировался, и обнаружить его было совсем непросто. Отрицательный эффект заключался в многократном копировании тела «червя» (что, кстати, было вызвано ошибкой в исходном коде); это в конце концов приводило к полному исчерпанию системных ресурсов. Одиннадцать лет спустя, уже после того, как защитные средства типа межсетевых экранов получили достаточно широкое распространение, червь «ExploreZip» повторил успех своего предшественника, сумев поразить массу компьютерных сетей путём простейшего тиражирования своего кода с одного узла на другой. Однако особенности технического прогресса 90-х внесли свои коррективы, и новый вирус сделал ставку на слабое место современных ему средств сетевой защиты. Этой брешью оказалась электронная почта. Благодаря пониманию разработчиками психологии любопытных пользователей «червь» успешно распространялся от одного компьютера к другому. Конечно, после того как вирусу Морриса удалось поразить множество компьютерных систем, были приняты меры, чтобы сделать их гораздо более защищёнными. Но, пользователи …

Широкое использование электронной почты стало наиболее действенным методом массового заражения компьютерными вирусами, а 1999 год в этом смысле был очень показателен и продуктивен: начался с «праздничного» вируса «Ska» и завершался, забегая вперёд, штаммом всё того же «ExploreZip». Пора бы сделать выводы, а точнее, вспомнить прописные истины –

не открывать никаких присоединённых файлов из незнакомых или малознакомых источников. Да и «проверенные» респонденты могут подводить. Но пользователям по-прежнему не терпелось запустить совершенно незнакомый исполняемый модуль и, судя по всему, подобная беспечность будет характеризовать компьютерное сообщество ещё очень долго.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Freelink
Другие названия	Freelinks, Freelink.a, VBS/FreeLinks VBS/ Freelink–mm, VBS/ Freelink, VBS.FreeLink
Тип	вирус-червь
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	июль 1999 года
Страна происхождения	Аргентина
Длина	12046 байт

В июле появился распространявшийся по электронной почте и через каналы IRC Интернет-червь, написанный на языке VBS, получивший название «Freelink»[501] и прославившийся тем, что стал как бы одним из «предтечей» печально известного вируса «LoveLetter».

Будучи запущенным, «скрипт» червя создавал на «жёстком» диске в системном директории операционной системы Windows файл «rundll.vbs» и изменял системный реестр таким образом, что этот файл запускался на выполнение при каждом старте компьютерной системы. Затем червь выводил на экран сообщение: «This will add a shortcut to free XXX links on your desktop. Do you want to continue?» («На ваш рабочий стол будет добавлена бесплатная порнографическая ссылка. Вы хотите продолжить?» Если пользователь отвечал «Yes» («Да»), «Freelink» создавал на рабочем столе пиктограмму-ссылку на порнографический Web-сайт в Интернет, после чего копировал инфицированный файл в корневые директории всех сетевых дисков компьютера.

«Freelink» распространялся через электронную почту, используя программу MS Outlook. Процедура распространения этого червя очень похожа на аналогичную процедуру в вирусе «Melissa», а сообщение электронной по-

[501] «Freelink» (англ.) – «Свободная связь».

чты, которое создаёт эта процедура, содержит «скрипт» червя во вложенном файле.

Subject: Check this	Тема: Проверьте это
Message: Have fun with these links	Сообщение: позабавьтесь с этими ссылками

Файл «rundll.vbs», о котором мы упоминали в самом начале описания «Freelink», также являлся «скрипт» программой, и при выполнении она создавала в директории операционной системы файл «links.vbs», который работал так, как описано выше. Затем он на всех «жёстких» дисках компьютера в директориях «MIRC» и «PIRCH98», а также в директории «ProgramFiles», куда обычно инсталлируется подавляющее большинство прикладных программ, и в их поддиректориях искал программы «mirc32.exe» и «pirch98.exe» (популярные программы для работы с IRC). Если какая-либо из этих программ была найдена, «Freelink» создавал новый файл «script.ini» для MIRC или «events.ini» для PIRCH. Этот файл содержал команды отправки файла червя «links.vbs» каждому пользователю IRC, который подключается к тому же каналу IRC, к которому подключён инфицированный компьютер.

Особенно «Freelink» интересен тем, что одновременно стал не только одним из «пращуров» печально известного вируса «LoveLetter», но и являлся также, в определённом смысле слова, преемником такой знаменитости, как «Melissa», которая автоматически рассылала себя, прикрепляя заражённый файл к письмам, по первым 50 адресам из адресной книги MS Outlook на инфицированном компьютере. Впоследствии эта характеристика была усовершенствована и использована вирусописателем при создании вируса «Freelink», поэтому, так же как и «ExploreZip», он отправлял свою копию уже на все адреса, найденные на инфицированном компьютере.

Между прочим, компьютерные эксперты чуть позже заявили, что знают того, кто мог сделать и запустить в Интернет этого «червя». По их мнению,

это был некий компьютерный злоумышленник по кличке «Zulu»[502], который в то время, по их информации, проживал в Аргентине. Брюс Хьюджес, менеджер компании ICSA.net, которая занимается проблемами компьютерной безопасности, заявил, что в прошлом году «Zulu» выкладывал исходный код «Freelink» на один из Web-сайтов, посвящённых вирусам. Также «Zulu», по словам того же Хьюджеса, является автором известных вирусов «Monopoly» и «Bubbleboy», что и делает его «первым подозреваемым среди ряда известных создателей вирусов», – заключил менеджер компании ICSA.net. При этом «Zulu» не занимался распространением собственных разработок, ограничиваясь публикацией кода и предоставляя всем желающим возможность заняться уголовно наказуемым вредительством на свой страх и риск.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Termite
Другие названия	Toadie, Toadie.7800.a, HLLP.Toadie, HLL. Toadie.7800
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003/DOS
Впервые обнаружен	август 1999 года
Страна происхождения	Соединённые Штаты Америки
Длина	7800 байт

Август 1999 года ознаменовался обнаружением интересного нерезидентного зашифрованного файлового вируса непосредственного инфицирования[503] по имени «Termite»[504], который, кроме заражения файлов операционных систем DOS и Windows, также прикреплял свои копии к письмам, отправляемым по электронной почте с помощью программы «Pegasus», и делал

[502] «Zulu» (англ.) – «Зулус», представитель южноафриканского племени Наталь. Зулусский язык относится к языкам банту, распространён в ЮАР и Зимбабве, всего носителей этого языка – 8 млн. чел.

[503] «Termite» отнесён к так называемой группе вирусов непосредственного инфицирования, поскольку, будучи запущенным пользователем, он самостоятельно осуществляет поиск других исполняемых файлов и их заражение при запуске пользователем файла «toadie.exe».

[504] «Termite» – «Термит».

попытки своего распространения по каналам IRC.

Производители антивирусного программного обеспечения оперативно предупредили пользователей о появлении новой инфекции, которая заражала все хранящиеся на «жёстком» диске выполняемые файлы с расширением «*.exe» операционных систем DOS и Windows, а также чрезвычайно быстро распространялась через чат-клубы Интернет и по электронной почте в виде исполняемого файла под названием «toadie.exe». Однако «Termite» был не способен самостоятельно пользоваться электронной почтой для своего распространения, то есть был лишён возможности автоматической рассылки, как «Melissa», и с одной системы на другую он мог быть перенесён только с инфицированным исполняемым файлом. «Зато «Termite» способен очень быстро размножаться через чат-клубы Интернет, причем «вирусоноситель» может не подозревать о своей роли», – говорилось в заявлении фирмы Network Associates, одного из производителей, опубликовавших предупреждение о вирусе «Termite». Особо яркими визуальными эффектами этот вирус не отличался, но выводил на экран инфицированного компьютера при запуске исполняемого файла окно DOS с сообщением «You are infected with Toadie» («Вы заражены Тоди»), однако пользователи мощных быстродействующих машин могли видеть этот текст в течение лишь очень короткого времени.

Родоначальник – «Termite», породил три штамма, которые портили заражённые файлы, и использовать их после этого было невозможно.

Несколько выше мы упоминали вирусописателя из Аргентины, скрывавшегося под кличкой «Zulu», которого специалисты-вирусологи считают автором как «Freelink», так и известных вирусов «Monopoly» и «Bubbleboy».

Так вот, нерезидентный «скрипт» вирус-червь «Monopoly» (другое название VBS/Monopoly) был написан в августе 1999 года и 7 числа этого месяца был зарегистрирован в «диком» виде. Сообщения, распространяемые этим червём, имели тему «Bill Gates joke» («Билл Гейтс – объект насмешки»), а в самом сообщении говорилось «Bill Gates is guilty of monopoly. Here is the proof. :-» («Билл Гейтс повинен в монополии. Вот доказательство. :-»), и к

нему прикреплялся написанный на языке VBS файл под названием «monopoly.vbs». Если пользователь запускал это вложение, «Monopoly» пытался разослать себя всем без исключения адресатам, которые упоминались в адресной книге MS Outlook. Кроме этого, червь записывал на «жёсткий» диск компьютера файл в формате JPEG[505] под названием «monopoly.jpg» во временный директорий системы и затем высвечивал на экране монитора диалоговое окно, в котором содержались практически идентичное приведённому выше заявление «Bill Gates is guilty of monopoly. Here is the proof» («Билл Гейтс повинен в монополии. Вот доказательство»), а также картинка в формате JPEG. На картинке был изображён совет Монополии с Биллом Гейтсом в центре. По углам прямоугольника совета были размещены изображения Microsoft. Однако, и это не всё. «Monopoly» также отсылал системную информацию по следующим адресам электронной почты: monopoly@mixmail.com, monpooly@telebot.com, mooponly@ciudad.com,.ar mloponoy@usa.net, yloponom@gnwmail.com. Эта информация включала: имя компьютера[506], регион, язык, версию, начальную страницу для Microsoft Internet Explorer и содержание адресной книги MS Outlook пользователя. Таким образом, червь «Monopoly» выполнял и функции «троянской» программы-шпиона.

Специалисты лаборатории Anti-Virus Emergency Response Team (AVERT) компании Network Associates, одного из ведущих поставщиков антивирусного программного обеспечения, первыми предупредили пользователей о появлении нового опасного макро вируса по имени «Thus»[507], поража-

---

[505] JPEG – проф. метод сжатия изображений и соответствующий графический формат, часто используемый в WWW. Характерен компактностью файлов и более быстрой передачей, чем GIF, но медленным декодированием и «потерей» деталей изображения.

[506] Имя компьютера (computer name) – проф. уникальное имя компьютера, которое идентифицирует компьютер в сети.

[507] «Thus» (англ.) – название вируса представляет собой сокращение от английского «Thursday» («Четверг») и символизирует собой день недели, в который данный вирус должен активизироваться.

ющего документы MS Word 97 и обладающего к тому же ярко выраженными деструктивными функциями.

Идентификационная карточка вредоносной компьютерной программы	
Имя	Thus
Другие названия	Thus.a, W97M/Thus, W97.Thursday, W97. Thursday.a, W97M. Automat.K, W97M/ Thursday
Тип	компьютерный вирус
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	сентябрь 1999 года
Страна происхождения	Соединённые Штаты Америки
Длина	3 макроса

Более того, вскоре большинство ведущих антивирусных компаний подняло оцениваемую степень риска заражения вирусом «Thus» (или «четверговым» вирусом) со средней до высокой, – сразу же вслед за появлением отчётов о его широком распространении и обнаружении во многих банках и других финансовых учреждениях США и восьми стран Европы (включая Германию, Францию, Ирландию, Швейцарию) всего лишь через сутки с момента его появления[508].

«Thus» проникал в компьютер пользователя вместе с инфицированным документом MS Word (файлы с расширением «*.doc»). Сразу после этого он автоматически заражал глобальный шаблон MS Word (файл «normal.dot»), увеличивая его размер, который в норме равен 27 Кбайт, и быстро распространялся по всем документам этого текстового процессора, основанным на данном шаблоне. «Thus» содержал три процедуры «Document_Open», «Document_Close» и «Document_New» и инфицировал область системных макросов при открытии заражённого документа, а остальные документы заражал при их открытии, закрытии и создании. В начале программного кода вируса содержалась комментарий-метка «Thus_001», и он проверял её наличие для того, чтобы определить, инфицирован документ или нет. Это делалось во из-

[508] «Thus» распространяется через документы, а не рассылает сам себя по почте, как «Melissa» или «ExploreZip».

бежание повторного заражения. Данный вирус отключал также защиту от макро вирусов в Word 97 – функцию «MacroWarning»[509].

Кроме того, проникнув в компьютер, «Thus», словно бомба с установленным на 13 декабря часовым механизмом, ждал своего часа. То есть вирус «Thus» являлся как бы «спящим», он оставался пассивным в системе до назначенной даты, когда просыпался и начинал выполнять свою миссию, пытаясь удалить все файлы в корневом директории и поддиректориях корневого директория на «жёстком» диске пользовательского компьютера. Исключение составляли только те файлы, которые имели один из следующих атрибутов: системный (S), невидимый (H), только для чтения (R).

Вирус «Thus» только в течение первых суток своего распространения заразил около 5 тыс. компьютеров и затем надолго вошёл в число самых распространённых вирусов в мире.

[509] Следовательно, если «чистый» документ, содержащий макросы, не вызывает обычного предупреждения, это может быть признаком заражённости компьютерной системы вирусом .

Идентификационная карточка вредоносной компьютерной программы	
Имя	BubbleBoy
Другие названия	Bubbleboy, VBS. Bubble Boy, I-Worm. BubbleBoy, VBS/Bubble Boy, VBS/BubbleBoy @MM, I-Worm.Bubble Boy, VBS/BubbleBoy. Worm, VBS/BubbleBoy -a, VBS_BUBBLEBOY
Тип	вирус-червь
Инфицируемые платформы	Windows95/98/ME/NT /2000/XP/2003
Впервые обнаружен	ноябрь 1999 года
Страна происхождения	Соединённые Штаты Америки
Длина	4992 байта

8 ноября компьютерное сообщество буквально потрясло известие о появлении первого представителя нового поколения червей-невидимок, которые распространяются по электронной почте без использования вложенных файлов и проникают в компьютерные системы сразу же после прочтения заражённого письма[510].

Первым из них стал Интернет-червь «BubbleBoy»[511]. В те дни, пресса и специалисты-вирусологи высказывались следующим образом: «Похоже, в мире компьютерных вирусов начинается новая эра. Казалось бы, «Melissa» и «ExploreZip» исчерпали возможности почтовых вирусов, ан нет. Новое чудо программистской мысли называется «BubbleBoy» и тоже рассылается по почте. Отвратительная особенность его заключается в том, что вирус заражает компьютер, даже если вы почту не читаете, и сообщение с заголовком «BubbleBoy is Back!» не просматривали. Достаточно, чтобы в Outlook Express был включён предварительный просмотр сообщений. При включённом предварительном просмотре вирус запускается, заражает компьютер и рассылает себя дальше по адресам, содержащимся в адресной книге, – участия пользователя не требуется. «BubbleBoy» не содержит деструктивных элементов, но, несомненно, найдётся добрая душа, которая рано или поздно их туда вставит» (InfoArt News Agency).

---

[510] Ian Whalley, Bursting the Bubble, Virus Bulletin, December 1999.

[511] «BubbleBoy» (англ.) – «Мальчик-пузырь», название происходит от одноимённой серии шедшей в то время по телевидению комедийной «мыльной оперы» Seinfeld, популярной в США.

«…вирус I-Worm.BubbleBoy относится к новому поколению Интернет-червей, представляющих реальную опасность для компьютерных пользователей и корпоративных сетей. I-Worm.BubbleBoy является первым известным Интернет-червём, способным распространяться по электронной почте, не прибегая к использованию вложенных файлов... Все ранее обнаруженные Интернет-черви использовали стандартный приём самостоятельной рассылки при помощи вложенных файлов. «BubbleBoy» внедряется на компьютер сразу же после прочтения заражённого письма и незаметно для пользователя рассылает себя по адресам из адресной книги почтовой программы MS Outlook» («Лаборатория Касперского»).

«Ну, вот и дождались. В великой и ужасной сети появился новый компьютерный вирус «BubbleBoy», который является первым вирусом, который заключён в теле e-mail и начинает работать сразу же, как только вы ПРОСМОТРЕЛИ это письмо. То есть для заражения компьютера вирусом вполне достаточно открытия тела письма, в то время как ранее вирусы скрывались в приложенных к письму файлах. Как это работает? Очень просто – сейчас подавляющее большинство e-mail клиентов способны просматривать письма, написанные на HTML. Более того, они делают это автоматически. А новоявленный вирус содержится как раз в коде HTML. Написан он на языке VBS. Правда, «BubbleBoy» совершенно безобиден, но он только первая ласточка» (Компьюлента).

«Обнаружена очередная разновидность компьютерной гадости. Основное отличие нового вируса от всех остальных заключается в том, что для заражения компьютера пользователю не нужно ни запускать приложенную к сообщению программу, ни даже просто открывать само письмо. Разработчики антивирусных программ компании Network Associates получили вирус от анонима вечером в минувший понедельник. До сих пор считалось, что вы защищены от вирусов, если только не открываете приложенные к сообщению дополнения. Однако с появлением этого вируса всё изменилось. Теперь можно утверждать, что если вы просто пользуетесь программами для работы с

электронной почтой – в особенности Microsoft Outlook – вам необходимо либо установить антивирусные программы, либо перестать читать поступающие сообщения. Несмотря на то, что присланный в Network Associates вирус не уничтожает информацию и не крадёт пароли пользователя, в скором времени следует ожидать появления более опасных и разрушительных разновидностей. Особенно неприятным стало то, что зараза переселяется в компьютер даже в тех случаях, когда пользователь не открывает само письмо. Outlook Express позволяет ознакомиться с содержанием полученной корреспонденции, используя окно предварительного просмотра, а этого оказывается достаточно для заражения» (Агентство Reuters).

Через несколько дней комментарии стали спокойнее, и в них стало прослеживаться желание глубоко разобраться в произошедшем, а также, по возможности, удержать пользователей от паники и типичных ошибок.

«… «Червь», ранее существовавший в коллекциях представителей компьютерного андеграунда, теперь имеет свободное хождение в сети Интернет. Это означает, что пользователи должны быть максимально внимательны к обеспечению антивирусной безопасности. «BubbleBoy»… является первым известным «червём», способным распространяться по сети Интернет без использования вложенных файлов и проникать в компьютеры сразу же после прочтения заражённых писем электронной почты… Чтобы распространять свои копии червь использует два нестандартных приёма. Первый приём – червь использует возможность MS Outlook создавать письма в формате HTML. Письма в этом формате могут содержать скрипты, которые будут автоматически выполнены в момент, когда пользователь откроет письмо. Червь использует это, чтобы активизироваться сразу при открытии письма. Другой приём червь использует, чтобы обойти настройки безопасности в Internet Explorer. Для этого он использует уже известную брешь в защите Internet Explorer 5.0, называемую «Scriptlet.Typelib security vulnerability». Эта брешь даёт возможность скриптам создавать файлы на диске без каких-либо предупреждений об этом пользователя. Червь использует её, чтобы создать

HTA-файл (HTML-приложение, новый тип появившийся в IE5), который содержит основной код червя. Этот файл создаётся в каталоге автозагрузки Windows и как следствие запускается при следующем старте. Будучи запущенным из файла на локальном диске компьютера червь получает доступ к ресурсам компьютера, берёт адреса электронной почты из адресной книги Outlook и отправляет по этим адресам заражённые письма» («Лаборатория Касперского»).

«Все пользователи Интернет давно знают (но не всегда учитывают), что в полученном письме от неизвестного отправителя открывать присоединённый файл опасно, это может активизировать присланный в нём вирус. Как оказывается, теперь выполнение этой заповеди не гарантирует от инфекции. Появился вирус-червь нового типа. Он называется «BubbleBoy». Чтобы он начал свою вредоносную деятельность, достаточно просто открыть письмо электронной почты, в котором его прислали. Активизировавшись, вирус рассылает сам себя по всем адресам, содержащимся в адресной книге почтовой программы Outlook или Outlook Express. То есть он ведёт себя, как известный вирус «Melissa». Пользователь сразу может не понять, что его машина заражена вирусом. Он проявляет себя только тем, что в регистрационных данных изменяется имя пользователя компьютера и название его организации, соответственно, на «BubbleBoy» и «Vandelay Industries». Определить, что к вам пришло заражённое письмо, очень просто. В заголовке письма в строке «Тема» стоит фраза «BubbleBoy is back!». Тело письма начинается с фразы «The BubbleBoy incident, pictures and sounds», кроме того, в письме приведён URL-адрес, оканчивающийся на «bblboy.htm». Вирус заражает только те машины, на которых установлен браузер Internet Explorer 5 и Windows Scripting Host (WSH) – всё это входит в стандартный комплект поставки Windows 98 и Windows 2000. Вирус не действует на компьютеры с Windows NT. Для работы вируса также необходимо наличие почтовой программы Microsoft Outlook или Outlook Express. В Outlook для активизации вируса требуется открыть письмо, вирус не опасен, если письмо не открывается, а про-

сматривается при включённой опции автопросмотра (видно только начало письма). В Outlook Express вирус активизируется и при автопросмотре. В любом случае вирус не опасен, если в Internet Zone в браузере Internet Explorer 5 установлен высокий уровень защиты… На первый взгляд вирус BubbleBoy не опасен, он не производит каких-то катастрофических действий на компьютере пользователя. Опасность состоит только в возможной перегрузке почтовых систем при одновременной отправке множества заражённых писем. Специалисты по антивирусной защите назвали вирус «BubbleBoy» концептуальным. Пока он не несёт разрушений, но на его основе могут быть созданы более опасные вирусы. Вирус был разослан анонимным отправителем (возможно, его автором) по нескольким фирмам и организациям, занимающимся разработкой средств антивирусной защиты. Если вирус разослал его автор, то он, по-видимому, хотел узнать мнение специалистов о своём творении. «BubbleBoy» написан на языке VBS и использует для заражения системы управляющие элементы Active X. Теперь пользователи при работе с электронной почтой должны следовать новой заповеди – не открывать письмо с темой «BubbleBoy is back!», а лучше настроить системы фильтрования и сканирования почты на удаление сообщений с такой темой. Ну, и не надо забывать про старое правило – никогда не открывайте файлов, присланных неизвестным отправителем» (InfoArt News Agency).

Итак, что же у нас в «сухом остатке»? Неизвестный миру программист-фанат американского сериала Seinfeld написал вирус, действовавший по принципу саморазмножающегося червя, который мог распространяться через клиентские программы MS Outlook и MS Outlook Express. «BubbleBoy», не был похож ни на что, с чем до сих пор приходилось сталкиваться специалистам по антивирусным программам. Он не таился во вложенном в письмо файле, а представлял собой «скрипт» программу на языке Visual Basic, «прицепляющуюся» к адресной книге MS Outlook и рассылающую письма по всем содержащимся в ней адресам. Для его активизации было достаточно простого открытия письма. По видимому, создатель этого вируса, желая при-

влечь к себе внимание, разослал «BubbleBoy» в антивирусные компании и поместил его на нескольких Web-сайтах. Причём, как это следует из многочисленных комментариев специалистов, «BubbleBoy» мог стать предвестником более крупных неприятностей. Ведь всего за месяц до того, на конференции издания Virus Bulletin (Ванкувер, Канада) как раз обсуждалась возможность создания подобных вирусов, а всего лишь за несколько дней до появления «BubbleBoy» в «диком» виде на нескольких посвящённых защите Web-сайтах появились рассуждения о том, как можно было бы сделать такой вирус и, по словам вице-президента по новым технологиям компании Trend Micro Дэна Шрейдера, это совсем не сложно. «Это интересное, но очень страшное и чрезвычайно мощное средство, – сказал он тогда. – Правда, пока оно не вышло на волю, но уже к концу дня большинство антивирусных компаний внесут этот вирус в свои определения». В целом «BubbleBoy» ещё раз доказал, что по мере совершенствования антивирусной технологии совершенствуются и вирусописатели. «Сам по себе «BubbleBoy» не очень опасен. Однако он очень интересен для нас, так как служит доказательством верности концепции», – заявлял директор по продуктам защиты Computer Associates Нарендер Мангалэм.

Сейчас прошло более пяти лет с момента появления первого вредоносного кода, способного запускаться автоматически (без вмешательства пользователя), благодаря уязвимости MS Outlook и MS Outlook Express, и именно после него многие вирусы стали использовать данный метод распространения. Вслед за «Bubbleboy» в 2000 году, появился «KakWorm», который долгое время оставался в числе наиболее распространённых в мире вредоносных компьютерных программ, а несколько позже ещё две знаменитости – «Klez» и «Bugbear», продемонстрировавшие всю опасность заражения подобными вирусами и заставившие многих пользователей задуматься о безопасности своих компьютеров. Таким образом, своим появлением «Bubbleboy» предзнаменовал наступление новой эпохи умышленного использования многочисленных «уязвимостей» в программном обеспечении.

Идентификационная карточка вредоносной компьютерной программы	
Имя	FunLove
Другие названия	FunLove.4099, W32/FunLove.4099, W32.FunLove.4099, Fun LovingCriminal, Win32.FLC, W32/FunLove, W32.FunLove, W32/Flcss, W32/Funlove, W95/FunLove, Win32.FunLove, Win32.FunLove, PE_FUNLOVE
Тип	вирус-червь
Инфицируемые платформы	Windows95/98/ME/NT/2000/XP/2003
Впервые обнаружен	ноябрь 1999 года
Страна происхождения	Соединённые Штаты Америки
Длина	4099 байт

9 ноября в Европе и США было зарегистрировано массовое заражение компьютерных систем резидентным паразитическим файловым вирусом-червём «FunLove», который был работоспособен под 32-х разрядными операционными системами Windows и стал первым вирусом, способным распространяться через локальную сеть. Этот вирус заражал PE EXE файлы (выполняемые файлы Windows) на локальных и сетевых дисках и, благодаря своей способности размножаться по локальной сети, мог инфицировать всю корпоративную сеть с одной рабочей станции, если ей были предоставлены права записи на сетевые диски.

Получив первоначально управление, вирус записывался в системную папку \Windows\System (Windows 9x/Me) или \Winnt\System32 (Windows NT/2000/XP/2003) под именем «flcss.exe». Этот файл запускался вирусом и становиля его резидентной частью. Первоначально он заражал файлы в папках ProgramFiles и Windows, включая их любые поддиректории, присоединяясь к последней секции файла формата PE с передачей управления на себя. «FunLove» запускался как скрытое Windows приложение(Windows 9x/Me) или как сервис (Windows NT/2000/XP).

В ОС Windows NT/2000/XP/2003 вирус воздействовал на систему безопасности файлов и использовал подпрограмму, исправляющую файлы «ntoskrnl.exe» (ядро Windows NT), а также загрузчик NTLDR. Это предоставляло полный доступ ко всем файлам и пользователям после следующего рестарта системы, независимо от их первоначальной защиты, что приводило к

тому, что даже имеющий самые низкие права в системе «Гость», получал полный доступ к любому файлу системы, независимо от уровня его защищённости, мог читать и изменять все файлы, включая и доступные в нормальном режиме работы только администратору системы.

В итоге «FunLove» мог распространяться повсюду, независимо от фактических ограничений доступа на компьютере, и никакие данные не могли считаться защищёнными от модификации любым пользователем. Причём вирус исправляет загрузчик таким образом, что никакие сообщения об ошибке (в нашем случае изменялось ядро) не выводились. Следовательно, операционная система успешно загружалась, несмотря на то, что контрольная сумма не соответствовала оригинальной. Вирус мог изменять ядро и компоненты загрузчика по сети, в том случае, если компьютер обладал достаточными правами и имел доступ к системному диску на Windows NT. «FunLove» выполнялся как сервис, он мог распространяться на локальных дисках, инфицируя файлы, которые являются обычно недоступными после входа в систему. Например, он мог инфицировать «explorer.exe» на системе Windows NT.

Кстати, поскольку вирус инфицировал управление ActiveX (файлы с расширением «*.ocx»), всегда существовала возможность инфицирования систем через программу просмотра сети, которая поддерживает управление ActiveX.

В теле вируса содержались строки: «~Fun Loving Criminal~», «flcss.exe», «FLC» и «WINNT\System32\ntoskrnl.exe». Присутствие вируса «FunLove» можно было заметить по присутствию файла с именем «flcss.exe» в системной папке, замедлению работы компьютера, выше описанным строкам в его теле.

При распространении вирус инфицировал файлы «*.exe», «*.scr» и «*.ocx» сначала на локальных дисках, а затем, в зависимости от случайного значения показателя системного времени на локальных или сетевых дисках. После исследования сети вирус заново сканировал локальные диски. Таким

образом, в процессе заражения системы вирус сканировал все локальные диски от C: до Z:, затем просматривал дерево поддиректориев сетевых ресурсов и заражал все PE-файлы с расширениями «*.exe», «*.scr» и «*.ocx». При этом «FunLove» записывал свой код в последнюю секцию файла и добавлял в стартовый адрес файла инструкцию «JumpVirus», которая обеспечивала его запуск из последней секции файла перед выполнением самой программы.

«FunLove» оказывал противодействие антивирусным средствам. Он проверял имена файлов и не заражал файлы по следующим маскам: «aler*», «amon*», «_avp*», «avp3*», «avpm*», «f-pr*», «navw*», «scan*», «smss*», «ddhe*», «dpla*», «mpla*».

Вот таким был появившийся 9 ноября вирус-червь «FunLove», и неудивительно, что практически сразу после регистрации в «диком» виде, причём фактически одновременно в Западной Европе и США, пошли сообщения о его неблаговидной сущности и деятельности.

Под заголовком «Вирусы крепчают» прошла краткая информация агентства Reuters: «Внезапно ворвался и на несколько дней застопорил всю работу завода Dell в Ирландии, снабжающего компьютерами Европу, Ближний Восток и Африку, коварный вирус W32.FunLove.4099 (по классификатору Symantec). Заражёнными оказались компьютеры, с которых производилась установка программного обеспечения на только что собранные персоналки. Сборку пришлось приостановить до тех пор, пока вирус с позором не был изгнан за ворота завода. Тем не менее, в нормальное русло работа вернулась только к понедельнику (заражение было обнаружено в четверг, 10 ноября)». На следующий день тем же агентством Reuters эта информация была дополнена заметкой «Вирус вывел из строя завод Dell в Ирландии»: «В четверг представители Dell сообщили Reuters, что после обнаружения так называемого вируса «FunLove» в системе, используемой для загрузки программного обеспечения в производимые заводом настольные и портативные компьютеры, завод остановился и не работал с прошлого четверга по понедельник, а 12 тыс. готовых изделий было возвращено для повторного техническо-

го контроля. «В понедельник мы возобновили производство, и всё наладилось», – сказала представительница компании. Она отказалась сообщить величину финансовых потерь от инцидента, но отметила, что они гораздо меньше той суммы, которую указала в своей публикации ирландская Times (14 млн. ирландских фунтов, или 18,43 млн. долл.). Корпорация Dell утверждает, что в возвращённых компьютерах вирус не обнаружен, а упущенное время завод наверстает. Вирус «FunLove» поражает настольные персональные компьютеры и серверы с операционными системами Windows и использует новую стратегию атаки на систему защиты сетей Windows NT». В материале «Новый вирус «FunLove» – легко найти, но трудно уничтожить» информационное агентство Ananova заявляло следующее: «Поступило сообщение об обнаружении нового вируса «FunLove». Его особенность состоит в том, что он достаточно легко поддаётся обнаружению, но его очень сложно уничтожить. Как только он инфицирует компьютер, вирус размещается в памяти и начинает заражать файлы с такой скоростью, что антивирусные программы могут не справиться с полной дезинфекцией. К примеру, для компьютеров на базе Windows NT обычные приложения от Symantec уже не подходят. Нужна специальная программа. На компьютерах на базе Windows 95 и 98, вирус удалить несколько проще. К счастью, сам по себе вирус относительно безвредный. Он записывает в файлы название музыкальной группы «Fun Loving Criminal», но, по некоторым сообщениям, он также ослабляет и систему безопасности компьютера, что делает его менее защищённым перед возможными атаками».

А что говорили специалисты? Их реакция была весьма быстрой, но без особых признаков шумихи. Представители практически всех ведущих компаний, специализирующихся на разработке средств антивирусной защиты, сообщили о появлении нового компьютерного вируса, получившего название «FunLove» и способного атаковать систему защиты файлов 32-х разрядных операционных систем Windows. Было также указано на то, что вирус прикрепляет себя к файлам с расширениями «*.exe», «*.scr» и «*.ocx» и распро-

страняется дальше, когда пользователь обращается к заражённому файлу на сервере, причём только тогда, когда он работает в режиме DOS. Специалисты подчёркивали и то обстоятельство, что на компьютере конечного пользователя «FunLove» действует следующим образом: на экране появляется надпись «Fun Loving Criminal», а затем вирус пытается произвести перезагрузку компьютера, что может привести к потере данных в открытых приложениях. Пользователей предупреждали, что более серьёзные последствия могут появиться, если «FunLove» попадёт в систему сетевого администратора. В этом случае он меняет установки системы защиты, и права администратора становятся доступны всем пользователям.

В своей информации «Внимание! Вирус, опасный вирус» от 13 ноября AVERT сообщила, что вирус «W32/FunLove.4099» следует относить к среднему классу их классификации вирусов: «Пользователи, первыми обнаружившие «FunLove» девятого ноября, сообщили, что он быстро распространяется как на системных серверах, так и на машинах пользователей. Вирус размещает файл «flcss.exe» в системных папках операционной системы, и начинает свою бойкую работу по инфицированию других файлов («*.exe», «*.scr» и «*.ocx»), причём не пропускает ни одного поддиректория. Пытается перезагрузить компьютер. Также из особенностей стоит отметить, что при загрузке Windows/WinNT, вирус получает те же права, что и пользователь, то есть если «FunLove» появился на машине с логином системного администратора, то, скорее всего, будут инфицированы все компьютеры сети. Выход один – устанавливать обновлённые антивирусные средства». Центр антивирусных исследований (AntiVirus Research Center, SARC) корпорации Symantec добавлял: «…вирус, на техническом языке называемый «W32.FunLove», вывел из строя серверы крупной европейской компании, а затем был обнаружен в США. По словам директора SARC Чарльза Рене, этот вирус не должен распространяться слишком быстро, так как неспособен тиражировать себя через электронную почту, как это делает вирус «Melissa». Зато он использует новый способ атаки на систему защиты файлов операционной системы Win-

dows NT, а распространяется «FunLove» по сети. «С точки зрения эволюции вирусов это определённый шаг вперёд», – завершил Рене свой комментарий».

Как это часто бывает с вредоносными компьютерными программами, их эпидемии наносят не только прямой материальный ущерб, но и подрывают авторитет вполне респектабельных компаний. С этой точки зрения вирус «FunLove» не стал «приятным» исключением. 25 апреля 2000 года корпорация Microsoft опубликовала сообщение «Вместе с файлами для обновления Windows NT распространялся вирус», в котором предупреждала о том, что «…некоторые файлы, предназначенные для обновления операционных систем Microsoft Windows NT Server version 4.0 и Microsoft Windows NT Workstation version 4.0, доступные для скачивания на Web-сайте Microsoft Premier Support, могут быть заражены вирусом «W32.FunLove.4099»». Несмотря на то что к тому времени «FunLove» был довольно старым и легко уничтожался антивирусными программами, пользователям был важен сам факт его распространения через Web-сайт, принадлежащий корпорации Microsoft, представители которой вынуждены были заявить: «заражённые файлы с обновлениями для операционной системы Windows NT 4.0 были доступны пользователям в период с 6 по 20 апреля 2001 года. В настоящий момент корпорация временно прекратила доступ пользователей к потенциально опасным файлам». Таким образом, корпорация опять оказалась в эпицентре скандала, связанного с распространением компьютерных вирусов. На следующий день корпорация Microsoft уточнила своё предупреждение, добавив следующее: «…некоторые из файлов для латания «дыр», доступные для скачивания на Web-сайтах «Золотых сертифицированных партнёров», также могут быть заражены вирусом «FunLove»». В итоге гигант софтверной индустрии посоветовал пользователям, скачивавшим что-либо с указанных Web-сайтов, обратиться на всякий случай в соответствующие службы технической поддержки. В копии заявления корпорации, которую английский онлайновый журнал «The Register» получил лично от корпорации по почте, было сказано: «Microsoft предполагает, что период заражения указанных файлов колеблется в

пределах примерно двух недель». Там же корпорация официально объявила, что временно прекратила доступ пользователей к потенциально заразным файлам, точное число которых неизвестно.

Но и на этом история не закончилась, так как информационная служба CNET обнародовала информацию о том, что Microsoft заразила компьютерные сети своих крупнейших деловых партнёров. Согласно её данным, от вируса «FunLove», поразившего серверы корпорации, пострадали 26 из числа её ключевых партнёров. Причём «менеджеры Microsoft пока не знают, откуда взялся вирус на серверах, и не могут сказать, когда сеть компании стала представлять угрозу для компьютеров партнёров». По словам представителя Microsoft Курта Пауэрса «на одном из серверов не было установлено антивирусное программное обеспечение». Именно на этом сервере, являющемся, кстати, частью сети Premier and Gold, находились 30 тысяч обновлений и «заплат» для скачивания основными партнёрами Microsoft. Вплоть до 19 апреля партнёры компании спокойно скачивали «FunLove» с этого сервера вместе с обновлениями и лишь 20 апреля Microsoft отключила этот сервер. По словам г-на Пауэрса: «Microsoft сейчас точно знает, компьютеры каких из её партнёров пострадали, и занимается оповещением их представителей». «Следует отметить, что вирус «FunLove» не относится к числу очень опасных, – заявил директор по исследованиям Systems Administration Networking and Security (SANS) Institute, Алан Паллер. – Таким образом, по всей видимости, этот вирус нанёс ущерб скорее не компьютерам, а репутации компании Microsoft».

Вирус «FunLove» прославился, помимо всего прочего, и тем, что успешно распространялся … корпорацией Hewlett-Packard вместе с драйверами для принтеров, доступными для скачивания с австралийского сервера компании, обслуживающего весь азиатско-тихоокеанский регион. В частности, оригинальный «подарок», был преподнесён её японским клиентам. В течение двух-трёх суток драйверы для нескольких принтеров, которые можно было скачать с Web-сайта поддержки компании, были заражены вирусом

«FunLove». Сама компания узнала о досадном недоразумении только после того, как ей начали в изобилии присылать письма пользователи. Опять-таки пострадала репутация.

В начале ноября 2001 года в США был отмечен первый случай распространения компьютерного вируса на лицензионном DVD с видеопрограммой. Как Вы думаете, кто стал «героем дня» на этот раз? Первопроходцем был вирус двухлетней давности «FunLove», который оказался на DVD-диске с популярным на Западе мультипликационным сериалом «Powerpuff Girls»[512] знаменитой кинокомпании Warner Brothers, а если быть ещё точнее, на DVD-диске с его серией «Meet the Beat Alls». Диски поступили в продажу в Америке в середине октября, а 1 ноября компания Warner Brothers срочно отозвала всю партию, пообещав возместить убытки и выпустить новые DVD в течение нескольких недель. Проникновение вирусов на тиражируемые носители – флоппи-диски и CD случалось и раньше, но с DVD такое приключилось впервые. Антивирусная компания Sophos рекомендовала всем, купившим диски «Meet the Beat Alls», вернуть их или уничтожить. Причём были все основания полагать, что заражённая партия успела проникнуть и за пределы США через онлайновые магазины, – мультсериал весьма популярен и вне США, а название серии «Meet the Beat Alls» созвучно композиции «Meet the Beatles» группы «The Beatles», вариации которой используются в мультфильме. Вирус «FunLove» был спрятан среди утилит для создания screensaver'ов и «обоев» из сцен мультфильма… Как старый вирус проник в мультфильмы, неизвестно. Специалисты полагают, что это произошло из-за недобросовестности одного из работников, изготавливавших матрицу DVD. Представитель фирмы Sophos по этому поводу философски заметил: «Старые вирусы никогда не умирают, они лишь прячутся в тёмных углах и директориях».

[512] «Powerpuff Girls» (англ.) – «Крутые девчонки».

Но и это ещё не рекорд. 24 января 2003 года (!) скандинавская компания Norway's Data Inspectorate, которая обеспечивает безопасность компьютерных сетей и баз данных, признала себя виновной в том, что непреднамеренно разослала вирус «FunLove» своим подписчикам. Как сообщало информационное агентство Ananova, вирус был разослан более чем 1700 подписчиков компании под видом рекомендаций по компьютерной безопасности. Выяснение обстоятельств столь досадного для компании инцидента показало, что «FunLove» проник во внешний почтовый сервер и, воспользовавшись данными контактного листа, начал немедленно распространять себя по адресатам. После того как стало известно о произошедшем недоразумении, специалисты службы безопасности Norway's Data Inspectorate сразу же выключили систему рассылки сообщений, но было уже поздно, так как вирус успел разослать себя по всем адресам. «К сожалению, вирус обогнал нас и успел разослать себя всем подписчикам компании, – констатировал опечаленный пресс-секретарь Norway's Data Inspectorate. – Самое ужасное состоит в том, что мы отправили вирус тем людям, которые на самом деле нуждались в рекомендациях по компьютерной безопасности».

Microsoft, Hewlett-Packard и Norway's Data Inspectorate могут утешаться хотя бы тем, что они далеко не одиноки. Бывает и хуже, например, сопровождавший ноябрьский номер от 1999 года венгерского журнала «Uj Alaplap» компакт диск, помимо набора по настоящему полезной информации, содержал и крайне неприятный сюрприз: сразу два макро вируса для MS Word – «Class.b» и «Opey.a»!

24 ноября[513] 1999 года был обнаружен обладающий крайне опасной деструктивной функцией и поражающий компьютеры под управлением операционных систем Windows вирус-червь с «троянской» компонентой, которому присвоили имя «ExploreZip.pak». В первые же дни своего распространения

[513] По данным компании Symantec. В некоторых источниках иногда встречаются даты 8, 15 и, даже, 21 декабря.

по планете он собрал обильный урожай: заражёнными оказались многие крупные компании и организации США, Германии, Греции, Канады, России, Чехии и других стран. Вирус поразил не менее 12 компаний, шесть из которых представляют собой сферу высоких технологий и, кроме того, было выведено из строя несколько тысяч персональных компьютеров.

Идентификационная карточка вредоносной компьютерной программы	
Имя	ExploreZip.pak
Другие названия	W32/ExploreZip.Pak, W32/ExploreZip.pak-m, Worm.ExploreZip.Pak, W32/ExploreZip.worm.pak, MiniZipWorm, I-Worm.ZippedFiles, W32/Explorezip.b, Worm.ExploreZip (pack), MiniZip, TROJ_EXPZIPWMPAK
Тип	вирус-червь
Инфицируемые платформы	Windows95/98/ME/NT/2000/XP/2003
Впервые обнаружен	ноябрь 1999 года
Страна происхождения	Израиль
Длина	120495 байт

Фактически эта вредоносная компьютерная программа уже встречалась нам в июне 1999 года в виде «родоначальника» семейства – вируса-червя «ExploreZip», и мы достаточно детально рассмотрели его основные технические характеристики. Поэтому не будем больше заострять на них внимание, так как у его штамма «ExploreZip.pak» они очень схожи с «родительскими»[514]. Давайте лучше рассмотрим его деструктивную составляющую, а затем сразу же перейдём к мнению средств массовой информации и специалистов-вирусологов относительно этого вируса-червя.

Итак, деструктивная функция. При каждом запуске «ExploreZip.pak» активизировал два параллельных процесса, которые сканировали локальные, сетевые диски и поддиректории, где искали и портили файлы с расширения-

[514] Обнаружившие первыми «ExploreZip.pak» эксперты компании Symantec указывают на тот факт, что главным его отличием от «ExploreZip» является применённое вирусописателем «сжатие» кода «ExploreZip.pak» при помощи специальной утилиты архивации Neolite, которое, тем не менее, не мешает ему нормально функционировать без разархивирования «вручную». Именно вследствие применённой архивации размер файла «ExploreZip.pak» примерно на 40% меньше оригинального кода «ExploreZip».

ми «*.c», «*.h», «*.cpp», «*.asm», «*.doc», «*.xls», «*.ppt», представляющие собой исходные тексты программ и файлы пакета MS Office. Причём червь портил файлы таким образом, что их содержимое стиралось, а длина становилась нулевой, и восстановлению они не подлежали. Упомянутые выше процессы осуществляли поиск файлов различными способами. Первый процесс постоянно сканировал логические диски от C: до Z: и портил на них указанные выше файлы, а второй процесс делал то же самое с «жёсткими» дисками, подключёнными как сетевые ресурсы (так называемые сетевые диски общего доступа – «shared drives»).

По свежим следам событий специалисты ZDNet, например, заявляли следующее: «Ещё не успели появиться на страницах компьютерных изданий подробные описания особенностей проснувшегося вируса «Prilissa» – преемника «Melissa», как новый модернизированный «червь» Worm.ExploreZip.Neolite, прозванный MiniZip, поразил компьютеры десятков ведущих корпораций. Вырвавшись на свободу, вирус стирает содержимое документов Microsoft Office, оставляя после себя файлы нулевой длины. Вирус распространяется по почте и не вызывает подозрений у неискушённого пользователя. Самораспаковывающийся архив WinZip использует редкий формат компрессии, усыпляющий бдительность антивирусных программ, для которых не был установлен свежий апдейт. Прикрепляемый к письму файл имеет название zipped_files.exe. Текст сообщения гласит: «Я получил ваше письмо и отвечу на него, как только смогу, пока же взгляните на эти документы». Письмо с вирусом не просто рассылается по электронным адресам, включённым в адресную книгу заражённого компьютера, но отправляется в ответ на входящие послания. Таким образом, пользователь не задумывается об опасности, наивно полагая, что файл прислал коллега по работе. Единственной ошибкой, допущенной создателем вируса, можно назвать его запуск в Сеть в конце прошлой рабочей недели. Компании, разрабатывающие антивирусное программное обеспечение, за выходные успели подготовить спасительную вакцину. Эксперты полагают, что если профилактические ме-

ры в виде инструктажа сотрудников компаний будут приняты во время, то разрушительных последствий удастся избежать».

2 декабря под заголовком ««MiniZip» – новый клон вируса «ExploreZip»» компания Algorithm Media опубликовала следующий материал: «Во вторник вирусологи компаний Network Associates, Symantec и Trend Micro предупредили о том, что новая версия вируса «ExploreZip», стирающего информацию с жёсткого диска, поразила уже не менее 12 компаний, шесть из которых работают в сфере высоких технологий. Выведены из строя несколько тысяч ПК. Вариант «ExploreZip» почти вдвое меньше предшественника: его размер всего 120 Кб. «MiniZip» действует точно так же, как «ExploreZip», который стирает файлы и может распространяться по электронной почте. Малый размер «MiniZip» объясняется тем, что автор вируса компрессировал оригинальный код «ExploreZip». Из-за этого антивирусное программное обеспечение не узнаёт известный вирус. Впервые «MiniZip» появился на прошлой неделе. «ExploreZip», «отец» «MiniZip», впервые появился 11 июня. Червь использует для своего распространения программы электронной почты, поддерживающие MAPI, такие как Microsoft Outlook, Outlook Express и Exchange. Он рассылается в виде вложения в сообщения под именем «zipped_files.exe». Тело письма ничем не примечательно. В нём сказано: «Я получил твоё сообщение и отвечу, как только смогу. Пока взгляни на прилагаемые документы». После запуска «MiniZip» преобразуется в оригинальную программу «ExploreZip». Он отыскивает все дисководы, обозначенные на компьютере, и заражает их. Затем он автоматически отвечает на все непрочитанные электронные письма. «MiniZip» может выводить сообщение об ошибке, информирующее пользователя о том, что файл не является настоящим архивом. Червь копирует себя в директорий C:\Windows\System под именем «Explore.exe», а затем изменяет файл «win.ini» таким образом, чтобы вирус активизировался при каждом запуске Windows».

Таким образом, специалисты-вирусологи в результате проведённого анализа программного кода «ExploreZip.pak» быстро сошлись во мнении, что

вирус-червь «ExploreZip», который наделал много шума в июне этого года, сейчас вернулся в виде своей новой версии. Однако «ExploreZip.pak» обладал одной несомненной «изюминкой». Многие антивирусные программы сканируют и архивные файлы, но автор «ExploreZip.pak» использовал малоизвестную программу архивации «Neolite», что делало вирус невидимым для систем защиты. В результате, по состоянию на начало декабря, в соответствии с заявлением специалистов Trend Micro, «…обновив своё антивирусное программное обеспечение, пользователи пока могут только замедлить распространение вируса «MiniZip»».

Так что на тот момент пользователю, пожалуй, можно было дать лишь один, но зато не теряющий актуальности совет: «Не запускайте на исполнение прикреплённые файлы из подозрительных писем, особенно, если в них присутствует вышеупомянутый текст».

День 3 декабря 1999 года стал примечательным из-за обнаружения сразу же в США, Европе и Австралии, где он поразил несколько десятков компаний, очередного творения бразильского вирусописателя по кличке «Vecna»[515] – очень сложного и опасного вируса «Babylonia»[516], открывшего новую страницу в области создания вредоносных компьютерных программ[517]. Это был первый резидентный паразитический Windows вирус, сочетавший в себе возможности вируса, Интернет-червя и «троянской» программы и к тому же имевший функции удалённого самообновления: ежеми-

[515] Автор вируса прикрывается псевдонимом «Vecna» и, по мнению специалистов Symantec, это член известной интернациональной латиноамериканской группы вирусописателей «29A» (в шестнадцатеричном коде – «666»). Например, другой член той же группы по кличке «Zulu», о котором мы говорили выше, считается автором вируса «Bubbleboy».
Вместе с тем через год, в январе 2001 года, представитель антивирусной фирмы Aladdin Knowledge Systems заявил, что они вычислили автора вируса «Babylonia», сетевая кличка которого действительно «Vecna», но он, якобы, принадлежит к числу членов группы под названием «VX-BRAZIL».

[516] «Babylonia» – англ. «Вавилония», древнее государство на юге Месопотамии.

[517] Marius van Oers, Digital Rivers of Babylonia, Virus Bulletin, February 2000. P. 6–7.

нутно он пытался соединиться с расположенным в Японии сервером и загрузить оттуда список вирусных модулей. В случае обнаружения в списке модуля, более «свежего» по сравнению с установленным на заражённом компьютере, «Babylonia» автоматически загружал его[518].

Идентификационная карточка вредоносной компьютерной программы	
Имя	Babylonia
Другие названия	W95/Babylonia, Win95. Babylonia, W795/ Babylonia.plugin, W95/ Babylonia.exe, W95/ Babylonia.hlp, W95/ Babylonia.irc, W95/ Babylonia.bat, Babylonia.exe, in95.Babylonia, Win95_Babylonia, W32 /Babylonia-m
Тип	вирус-червь
Инфицируемые платформы	Windows 95/98
Впервые обнаружен	декабрь 1999 года
Страна происхождения	Бразилия
Длина	11036 байт

«Вирус «Babylonia» «заряжен» новыми усовершенствованными функциями несанкционированного удалённого администрирования, что даёт основание определить его, как очень опасный. Этот вирус, обнаруженный во вторник, явился одним из самых сложных вирусов, выпущенных в конце года. При помощи вируса автор может удерживать контроль над удалённым компьютером, внедрять дополнительные «троянские» программы и утилиты удалённого администрирования, уничтожать данные, извлекать конфиденциальную информацию и т. п., а также обновлять версию вируса, которым инфицирована машина. Последнее затрудняет эффективное лечение из-за того, что обновление может быть послано раньше, чем появится антивирусная программа, способная уничтожить текущую версию. В отличие от своих почтовых предшественников, вирус распространяется через популярный Интернет чат-сервис IRC», – характеризовали «Babylonia» в своём сообщении от 7 декабря специалисты «Лаборатории Касперского».

[518] Позже подобный технический приём удалённого самообновления был использован авторами таких «червей» как «Sonic», «Hybris» и пр.

Вирус «Babylonia» внедрялся в компьютерные системы под управлением Windows 95 и Windows 98, инфицируя несколько типов файлов: файлы PE EXE (выполняемые файлы Windows) и файлы помощи Windows, то есть файлы с расширением «*.hlp». Кроме того, он заражал библиотеку работы с сетями «wsock32.dll» и обладал возможностями несанкционированной загрузки из Интернет дополнительных вирусных модулей. Последнее обстоятельство позволяло «Babylonia» получить практически полный контроль над инфицированной системой. Кстати, вирус использовал специфические команды Windows 95 и Windows 98, что делалало его неработоспособным на компьютерах под управлением Windows NT и Windows 2000.

Внедряясь в систему, вирус создавал в корневом директории диска C: файл «babylonia.exe» и записывал в него код «троянской» программы длиной 4 Кб, которая представляла собой самостоятельное приложение, не связанное с самим вирусом. Причём вирус не инфицировал файл «babylonia.exe», так как был запрограммирован вирусописателем на заражение файлов длиной более 8 Кб. После запуска файла «babylonia.exe», программа регистрировала себя в качестве «сервиса», следовательно, её нельзя было увидеть в списке активных задач, затем она копировала себя в системный директорий операционной системы как файл под именем «kernel32.exe» и регистрировала его в секции автозагрузки системного реестра: HKLM\Software\Microsoft\Windows\ CurrentVersion\Run. После завершения подготовительных «мероприятий», программа связывалась по Интернет с находящимся в Японии Web-сайтом сомнительной принадлежности, и производила загрузку с него файла «vecna/virus.txt», содержащего список дополнительных модулей, которые могли использоваться «троянской» программой, и их местонахождение. Затем программа поочерёдно загружала эти файлы из Интернет и, если в данный момент соединение с Интернет отсутствовало, – указанный или указанные в файле «virus.txt» Web-сайт или Web-сайты были недоступны, – «троянская» программа оставалась в оперативной памяти компьютера, каждую минуту пытаясь получить эти дополнительные модули. «Троянская» программа вы-

гружалась из памяти только тогда, когда файлы были уже полностью загружены и запущены на выполнение. Интересно, что все файлы с находящегося в Японии Web-сайта имели особенный формат – идентификационную метку заголовка, метку версии и адрес подпрограммы. Поэтому файлы, загружаемые с указанного Web-сайта, выполнялись как встраиваемые модули, с помощью которых автор «Babylonia» мог использовать инфицированные компьютеры так, как ему это было необходимо.

8 декабря 1999 года в материале под заголовком «Обнаружен вирус нового типа – W95.Babylonia» известное онлайновое информационное агентство Lenta.ru сообщало следующее: «Во вторник компании, разрабатывающие антивирусное программное обеспечение, сообщили о появлении нового вируса W95.Babylonia, который распространяется через IRC (Internet Relay Chat), маскируясь под программу для решения «Проблемы 2000» на отдельно взятом компьютере. Как сообщает Reuters со ссылкой на экспертов Computer Associates и других компаний, занимающихся проблемами компьютерной безопасности, W95.Babylonia является вирусом нового типа. По словам специалистов, он крайне опасен, поскольку его автор имеет возможность дистанционно менять вирус уже после заражения компьютера. Таким образом, «Babylonia» представляет собой новый уровень развития вирусных программ. Как пишет Wired News, для заражения пользователю достаточно посетить тот канал IRC, на котором распространяется вирус. Заражение происходит через IRC-клиент, программу mIRC, либо при запуске исполняемого файла. Вирус опасен для пользователей ОС Windows. Согласно описанию вируса, данному экспертами из Computer Associates, вирус раз в 60 секунд обращается к некому японскому сайту в поиске дополнительных приложений, расширяющих его возможности. Обнаружив эти дополнения, вирус сгружает их на заражённый компьютер. В настоящее время существует четыре таких дополнения. На заражённом компьютере вирус действует крайне цинично: может переформатировать «жёсткий» диск, уничтожает файлы или

же считывает пароли пользователя. Кроме того, «Babylonia» старается заразить все исполняемые файлы и файлы Help в заражённой системе».

По поводу нового компьютерного вируса, который распространяется через чат-сеансы в Интернет и автоматически обновляется, подкачивая из Web-сайта дополнительные модули, старший научный сотрудник компании Symantec Эрик Чейн заявил следующее: «Это только верхушка айсберга и способность вируса к самосовершенствованию имеет принципиальное значение. Создатели вирусов всё чаще используют сетецентрические идеи… Эксперты опасаются, что в будущем могут появиться более совершенные варианты. Или, что не менее опасно, автор вируса в любой момент может придать ему разрушительную силу. Все или некоторые из признаков вируса могут меняться. Автор волен добавлять новые модули, изменяющие вирус, уже заразивший компьютер пользователя. При этом может меняться как способ его распространения, так и его разрушительная нагрузка. Завтра он может начать распространяться, например, через MS Outlook». «По иронии судьбы, способ обновления вируса напоминает технологию LiveUpdate самой Symantec – она используется для поддержания в актуальном состоянии антивирусной программы. Подобный способ самообновления через Web-сайт применяется в индустрии программного обеспечения уже несколько лет», – прокомментировал эти высказывания Роберт Лемос, CNET News.com.

21 декабря интересное сообщение поступило от антивирусной фирмы Trend Micro: «…Проникнув на компьютер, вирус ждёт, пока пользователь вновь установит соединение с Интернет, после чего инициирует соединение с Web-сайтом, известным под названием «SOK4EVER», откуда производится загрузка дополнительных вирусных модулей. Принадлежит этот сайт группе «любителей» вирусов под названием «Source of Chaos»[519] и располагается он в Японии. Вернее, теперь уже можно сказать в прошедшем времени – принадлежал группе «Source of Chaos» и располагался в Японии, так как этот

[519] «Source of Chaos» (англ.) – «Источник хаоса».

Web-сайт, с которого производилась рассылка новых вирусных модулей, закрыт. Вирус «Win95.Babylonia», конечно же, не обезврежен, но не столь опасен, как раньше, поскольку функции несанкционированного удалённого администрирования он уже лишён».

* * *

Вот мы и подошли к концу истории вирусописания в 90-х годах двадцатого века и вступаем на порог нового тысячелетия, которое, без сомнения, внесёт свою палитру и дополнит летопись развития и распространения вредоносных компьютерных программ. Так что же мы имеем на этом рубеже?

По данным экспертов Environmental Resources Research Institute (ERRI) США к концу 1999 года произошла вспышка написания вирусов под операционную систему Windows 95. Появились такие изощрённые вредоносные компьютерные программы как «Explore.Zip» и «Babylonia», а также многочисленные штаммы ранее знаменитых вирусов, например, вируса «Melissa». Причём, компьютерные эксперты-вирусологи прогнозировали, что это всего лишь небольшое количество от числа предполагаемых сложных, использующих новые технологии вирусописания компьютерных программ, появление которых ожидается уже в 2000 году. Исследователи корпораций Network Associates, Symantec, McAfee и многих других ведущих фирм-разработчиков антивирусных продуктов высказывали предположения относительно того, что переходный период в новое тысячелетие будет чрезвычайно активным с точки зрения потенциального ущерба, который могут принести с собой новые компьютерные вирусы, особенно те из них, которые будут использовать человеческую психологию. По мнению многих ведущих отечественных и зарубежных специалистов, новые вирусы станут разрабатываться таким образом, чтобы воспользоваться недостаточной осведомлённостью, халатностью или невнимательностью пользователей, общим страхом перед неизвестностью, которую несёт с собой каждый новый тип вредоносной программы.

Ряд новых вирусов, таких как усовершенствованный «FreeLink», будут представлять собой ещё большую опасность, особенно для тех, кто интенсивно пользуется электронной почтой. Вредоносные программы этого класса будут распространяться всё шире, и в них будут применяться новые программистские приёмы написания и алгоритмы реализации. Ещё в большей степени проявятся тенденции к разработке вредоносных программ, способных нанести большой ущерб пользователю, например, при помощи массового автоматического распространения через электронную почту при каждом запуске под разными именами, что может приводить к «взрывному» росту трафика в сетях и, соответственно, перегрузке серверов. Исследования вирусологов показали, что станет прогрессировать динамика роста расходов, связанных с ликвидацией вирусных инцидентов и эпидемий, так как на полное восстановление от атак более совершенных вирусов будет требоваться всё больше и больше времени, в течение которого простаивает компьютерная техника, а также персонал организаций и учреждений. Немаловажное значение будет иметь и резкое увеличение скорости распространения вирусов. Если первым вредоносным программам зачастую требовались месяцы для того, чтобы перебраться с континента на континент или вызвать сколько-нибудь значительную эпидемию, то со временем этот срок сократился до недель, а, например, знаменитый вирус «Melissa» распространялся по всему миру уже в течение 9 дней. Таким образом, скорее всего вредоносным компьютерным программам будущего потребуются для этого если и не секунды, то считанные часы и минуты. Результаты исследования специалистов США из антивирусной лаборатории International Computer Security Association (ICSA) дают основания утверждать, что показатели инфицированности парка компьютерной техники в относительных величинах продолжают расти по всему миру, несмотря на значительную защиту персональных компьютеров и серверов современными антивирусными программами. Причём, прогноз на ближайшее будущее весьма неутешителен – относительная доля инфицированных вирусами компьютеров продолжит свой рост.

С учётом указанных выше тенденций специалисты ведущих лабораторий и исследовательских центров, таких как ERRI и ICSA, сходятся во мнении, что лучшей защитой в настоящее время считается защита компьютеров самими пользователями. В связи с этим, эксперты советуют не использовать программы полученные из неизвестных или малознакомых источников», чаще обновлять антивирусные программы, копировать данные с «жёстких» дисков и хранить копии в надёжном месте, а в случае наличия особо критической информации широко применять современные антивирусные аппаратно-программные комплексы.

Ждём Вас, уважаемый читатель, в следующей главе, где мы будем рассматривать историю вирусописания начала XXI века, и очень надеемся на то, что Вы её прочитаете с тем же интересом, что и предыдущие.

ПРИЛОЖЕНИЕ 1

КОМПЬЮТЕРНЫЕ МИСТИФИКАЦИИ И ВРЕДОНОСНАЯ МИМИКРИЯ

Так называемые «компьютерные мистификации» (computer hoaxes) представляют собой сравнительно недавнее и несколько изолированное от остальных вредоносных компьютерных программ «изобретение».

К этой категории компьютерных программ относят, например, заведомо ложные сообщения о новых ранее неизвестных компьютерных вирусах. Кроме того, программисты, периодически ловят друг друга, а также малокомпетентных или излишне доверчивых пользователей, как на безобидных, так и на достаточно неприятных, а порой, даже опасных шутках и розыгрышах с «электронной начинкой». Больше всего компьютерных мистификаций регистрировалось в 1997–1998 годах. При этом наиболее «удачные» мистификации и шутки входят в историю вирусописания и получают собственные имена, например: «AOL4FREE.COM», «Buddlylst», «Bud Frogs warning», «Cancer chain», «Disneyworld», «Deeyenda Maddick», «Eicar», «Get more money», «GoodTimes», «Hackingburgh», «Hacky B-day», «Irina», «Join the Club», «Join the Crew», «Joke.Win32.Errore», «Joke_FakeFormat», «Londhouse», «National Bank Chain», «NaughtyRobot», «Penpal Greetings», «Sandman homepage warning», «Win a holiday» (приведены в алфавитном порядке) и т. п. Некоторые из этих вирусоподобных программ-шуток (например, Joke.Win32.Errore, Joke_FakeFormat) даже удостоились особого внимания специалистов-профессионалов в области борьбы со зловредными компьютерными программами. Причина такого внимания проста. Например, якобы абсолютно «безобидные» компьютерные программы очень точно имитируют процесс форматирования жёсткого диска, что если и не приводит к порче записанной на нём информации, то в

состоянии довести любого «мирного» пользователя до полного расстройства его нервной системы.

Иезуитская жестокость «шутки» состоит в том, что прекратить начавшийся процесс пользователь не может, и способен лишь наблюдать за тем, как ложный вирус вполне правдоподобно симулирует уничтожение данных с жёсткого диска компьютера. И весьма сомнительным выглядит в этой ситуации иногда встречающийся тезис о том, что «нельзя исключать воспитательное воздействие такого рода розыгрышей на беспечных пользователей, которые, попавшись на уловку «шутников», в другой раз будут осмотрительнее, когда снова возникнет желание запустить незнакомую программу». У всех людей разный характер, и не каждый способен учиться даже на собственных ошибках. Тем более что в том случае, если неопытный пользователь получил по e-Mail письмо с правдоподобным предупреждением об «ужасном» компьютерном вирусе и переслал это сообщение всем своим знакомым, у которых есть электронные адреса, он принял на его взгляд самое правильное и своевременное решение. И его можно понять. Содержание письма, предупреждающего пользователя о вирусе, обычно создаёт впечатление, что весь Интернет в опасности и родина в огне. В письме всячески нагнетается атмосфера: говорится, что вирус, самостоятельно и в считанные секунды воспроизводит себя в колоссальных количествах копий, заражает не только компьютер самого пользователя, но и все подряд компьютеры тех людей, которым пользователь направлял когда-либо сообщение по электронной почте. В итоге, «семена» компьютерных мистификаций, красочно рассказывающих о несуществующих вирусах, падают на благодатную почву – люди опасаются «электронной инфекции» и стараются узнать о новых путях её распространения. Кроме того, рассылка писем с предупреждениями обычно занимает считанные минуты, но даёт человеку уверенность, что он сделал доброе дело и предостерёг кого-то от надвигающейся опасности.

Естественно, специалисты-вирусологи, программисты и даже просто опытные пользователи, которые сталкивались с проявлениями реальных вредоносных компьютерных программ, быстро идентифицируют послание в качестве компьютерной мистификации, запугивающей начинающих пользователей, которых иногда ласково называют «чайниками». Однако надо учесть, что ускоренная компьютеризация в мировых масштабах принесла с собой резкое повышение в компьютерном сообществе доли именно «чайников», и поэтому миллионы человек готовы «по первому зову» пересылать свои сообщения по e-Mail всюду, куда только можно и нельзя: в телеконференции, списки рассылок и, всенепременно, своим родственникам, коллегам по работе и просто знакомым.

Итак, обычно компьютерные мистификации рассылаются в электронные конференции, а также личными письмами по большому количеству адресов и в рассылаемых письмах-сообщениях, как правило, присутствует строка, призывающая пользователя переслать данное электронное письмо по как можно большему числу других адресов с целью незамедлительного информирования о грозящей опасности как можно большего количества пользователей. Встречаются также другие варианты подобных сообщений о вирусах: в графических и звуковых файлах, CMOS, BIOS и т. п. И всё-таки особой «популярностью» пользуются сообщения, в которых пользователям доверительно говорят о том, что в Интернет появился новый вирус, распространяющийся в письмах и (или) через WWW-сайты и уничтожающий всю информацию на инфицированных им компьютерах. Эта информация распространяется в Глобальной сети вполне осознанно и, затем, начинает множиться пользователями, которые искренне надеются вовремя предупредить и обезопасить компьютерную общественность от нависшей над ней «смертельной» опасности. Чаще всего текст сообщений, содержащийся в компьютерных мистификациях, учитывает слабые места человеческой психологии и оформляется в драматических выражениях, но, вместе с тем, сохраняет и правдоподобие, например:

«Осторожно!!! Опасно!!!! Если Вы получили письмо с заголовком … (далее следует текст заголовка электронного письма), то ни в коем случае даже не пытайтесь открыть его на своём персональном компьютере! В случае его открытия на Вашем жёстком диске будут безвозвратно уничтожены все без исключения файлы и прикладные программы! Постарайтесь … (далее следует какой-либо совет, безобидный или нет, зависит от темперамента, характера, изобретательности и чувства юмора автора мистификации). Пожалуйста, перешлите это предупреждение всем-всем своим родственникам, знакомым и коллегам по работе, так как возможно именно в данный момент новый вирус готовится нанести непоправимый вред их компьютеру, а они ничего о нём не знают и ни о чём не догадываются!» Вы думаете, что мы это придумали? Да нет. Сообщение, подобное по смыслу приведённому, получило название «Join the Crew» и относится к наиболее известным мистификациям.

Осенью 1998 года пользователи компьютеров были встревожены сообщениями о том, что по Интернет распространяется коварный и опасный вирус, которому не в состоянии противостоять ни одно из существовавших на тот момент антивирусных программных средств. Как выяснилось позже, причиной всей этой паники стала «компьютерная шутка», которая была запущена ещё в феврале 1997 года – по Интернет прошла информация о действующем в Глобальной сети вирусе «Join the Crew», который заражает компьютеры посредством электронной почты при получении и открытии писем. То сообщение выглядело следующим образом: «Warning!!! If you receive an e-mail titled «Join the crew». Do not open it! It will erase everything on your hard drive! Send this letter out to as many people you can ... this is a new virus and not many people know about it!»[1] Существовали и другие варианты этого послания, однако все они имели примерно одно и то же содержание: «Новый, неуязвимый вирус в электронной почте распространяется по

[1] Внимание!!! Если Вы получили письмо с заголовком «Join the crew» – не открывайте его! Это сотрёт все данные на вашем диске! Перешлите это письмо как можно большему числу людей ... это действительно новый вирус и очень немногие знают о нём.

Интернет и стирает все данные на жёстком диске! Сообщите об этом всем, кому только можете!». Действовало практически безотказно, так как множество обычных пользователей верило этому посланию и, в результате, копии письма-предупреждения тысячами, если не миллионами писем, рассылались испуганными людьми друг другу по Интернет, что придавало этому мифическому вирусу всё большую и большую известность. Ну, чем не вирус, основанный на весьма тонком знании людской психологии? Ведь пользователи занимались тем, что за них обычно делают многие почтовые вирусы: забивали Интернет посланиями, увеличивая сетевой трафик, и сеяли панику среди других пользователей. Но такого компьютерного вируса не было и в помине, а была очередная компьютерная мистификация, рассчитанная на непрофессионалов. Добавим ещё один интересный штрих – вредоносные программы, действительно способные заражать компьютеры при открытии электронного письма, появились на свет только через несколько лет после описываемых событий. Что это? Предвидение, склонность автора компьютерной мистификации к прорицанию или отличное, профессиональное знание предмета, в дополнение к пристальным наблюдениям за человеческой психологией?

Компьютерные мистификации порой действительно предвосхищают появление реальных вирусов со свойствами придуманными авторами «шуток». Если абстрагироваться от компьютерных мистификаций, то интересно будет узнать, что некоторые идеи, использованные первоначально в качестве основы для шутки иногда становятся осязаемой действительностью. Например, утверждают, что создатели операционной системы UNIX и языка программирования высокого уровня «С» – Кен Томпсон, Деннис Ричи и Брайан Керниган признались в том, что и UNIX и язык программирования «С» были задуманы в качестве первоапрельской шутки. Томпсону приписывается следующее высказывание: «В 1969 году AT&T завершила работу над проектом операционной системы Multics. Брайан и я только что начали работу с ранней реализаций Паскаль,

разработанной в лаборатории профессора Вирта в Швейцарии, и находились под впечатлением элегантности, простоты и мощи этого языка. Деннис как раз прочитал «Уставший от колец» – весёлую сатиру на знаменитую трилогию «Властелин колец». Шутки ради мы решили написать пародии на среду Multics и Паскаль. Деннис и я отвечали за операционную среду. Глядя на Multics, мы спроектировали новую систему настолько сложной и запутанной, чтобы максимально «испортить жизнь» рядовым пользователям, назвали её UNIX, как пародию на Multics, добавив много других достаточно рискованных аналогий».

U.S. News & World Report, Ted Koppel's Nightline, другие журналы и авторы многих книг попались на «первоапрельскую шутку», в которой говорилось, что американские военные якобы послали опасный вирус в компьютерную систему иракской системы ПВО во время операции «Буря в пустыне». Сообщалось, что США, вероятно, поместили заражённую вирусом плату ПЗУ в принтер, который должны были провезти в Ирак в обход эмбарго ООН. Эта же история была напечатана в журнале «Infoworld» 1 апреля 1991 года на странице 39, там же было указано, что это всего лишь шутка. Кстати, если говорить о PC, то только PostScript принтер способен передать данные обратно в компьютер, и даже если бы в таком принтере содержался вирус, маловероятно, чтобы это был выполнимый код, который мог бы быть перенесён на компьютер и активизирован. Но ведь верили…

Несомненно, что особенных «успехов» на ниве компьютерных мистификаций добились программисты вредоносных компьютерных программ, которые для того чтобы беспрепятственно перемещать их с компьютера на компьютер, выдумывают изощрённые приёмы и сюжеты, заставляющие пользователя поверить в то, что попавшая к нему в компьютер, например, по электронной почте программа не несёт с собой никакой опасности. Мы уже говорили о таких «изделиях» знатоков человеческих душ, как Интернет-червь «I Love You» и его многочисленных модификациях, которые обычно объединяют под общим названием

«любовные письма». Подобные компьютерные вирусы, играя на психологии человека и его любопытстве, безжалостно обманывали и продолжают обманывать наивных пользователей, а также излишне любопытных и любителей случайных знакомств. В качестве примера иногда приводят Интернет-червя «MyParty», который представляет собой компьютерный вирус ничем особо не выделяющийся среди подобных ему программ. Но, автор вируса придумал утончённый способ обмана пользователей и … «MyParty» обрёл неувядаемую славу далеко за пределами довольно узкого круга исследователей истории компьютерных вирусов. А суть дела заключалась в том, что к электронному письму, в котором от первого лица достаточно живо рассказывалось об очень весёлой вечеринке, прикреплялось вложение, которое и оказывалось самым настоящим вирусом. «Ну, и что?», – скажете Вы. Действительно, ничего особенного, но подавляющее большинство обычных пользователей, никогда не общавшихся с операционной системой MS DOS, не знало и не знает, что расширение «.com» означает не только часть адреса Web-сайтов, но и является признаком выполняемого файла. Так что всё происходящее далее вполне предсказуемо. Ничего не подозревающий пользователь одним элегантным щелчком своей ненаглядной «мышки» обретает нового «друга» в лице вируса «MyParty», а заодно, и сопутствующие ему проблемы.

Несмотря на неизбежные повторы и «ремейки», появляющиеся из года в год предупреждения о несуществующих компьютерных вирусах каждый раз заново нарушают спокойствие пользователей. Интересно, что иногда электронные шуточки обладают свойством обратного эффекта или «эффектом бумеранга», как Вам больше нравится. Например, настойчивые слухи о распространяющемся через e-Mail вирусе «GoodTimes» зародились и циркулировали в Интернет в течение длительного времени. И, в данном случае, частое повторение возымело действие – вирус с таким названием действительно появился, но он, естественно, не имел ничего общего с тем мистическим «GoodTimes».

В начале декабря 1994 года по сетям Интернет и FIDO прошло сообщение о вирусе (которому заочно было присвоено имя «GoodTimes»), якобы повально заражающему компьютеры посредством электронной почты при получении и чтении писем. Сообщение выглядело следующим образом: «Here is some important information. Beware of a file called GoodTimes. Happy Chanukah everyone, and be careful out there. There is a virus on America Online being sent by E-Mail. If you get anything called «Good Times», Don't read it or download it. It is a virus that will erase your hard drive. Forward this to all your friend. It may help them a lot». Этот краткий текст вызвал настоящую панику среди пользователей Интернет. Было зафиксировано даже несколько сообщений о действительно заражённых компьютерах. Однако все они поступали из косвенных источников, и никто в натуральном виде так никогда и не встретил это «чудовище» по той простой причине, что такого компьютерного вируса не существовало в материальном мире. Тем не менее, весной 1995 года история с «GoodTimes» получила своё продолжение благодаря новому сообщению на ту же тему о вирусе, который распространяется по всем адресам e-Mail, присутствующим в почтовых ящиках Inbox и SentMail. Как и в предыдущем случае, вирус обнаружен не был, но тогда же, в очередном номере журнала вирусописателей «VLAD» появились исходные тексты настоящего компьютерного вируса, названного его автором «GoodTimes», и это был самый обычный вирус для MS DOS, который не имел никакого отношения к сетям и Интернет. В итоге «GoodTimes», вместе с «полезными приложениями» к обычному тексту электронного письма, начал своё реальное распространение.

Аналогичные истории происходили и в 1999 году, когда пользователей пугали, например, якобы содержащей «заразу» экранной заставкой «Budweiser Frogs.zip». В мае этого года специалисты начали получать многочисленные запросы с просьбой о разъяснении смысла приходящих писем следующего содержания: «Кто-то рассылает очень “хорошую” экранную заставку, Budweiser Frogs “buddylst.zip”. Если вы её загрузите, то

потеряете всё!!! Ваш жёсткий диск будет повреждён и любой получит ваше имя и пароль из Интернет. Не загружайте его ни при каких обстоятельствах!!! Он поступил в обращение вчера, насколько мы можем судить. Пожалуйста, разошлите это сообщение. Это новый, очень вредный вирус и немногие о нём знают. Информация поступила вчера утром от компании Microsoft. Пожалуйста, поделитесь этой информацией со всеми, кто имеет доступ в Интернет. И ещё раз, передайте эту информацию всем, кто находится в вашем списке адресов для того, чтобы предотвратить нежелательные последствия. AOL говорит, что это очень опасный вирус и не существует средств защиты от него в данный момент времени. Пожалуйста, предпримите все меры предосторожности и перешлите это сообщение всем вашим друзьям, с которыми вы поддерживаете связь в режиме on-line». Письмо представляло собой пример классической мистификации, преследующей целью раздувание вирусной истерии, и не имело под собой никаких сколько-нибудь серьёзных оснований. Естественно, специалисты советовали игнорировать подобные сообщения, не рассылать их своим друзьям и знакомым, а также соблюдать бдительность и предельно осторожно относиться к вложенным в электронные сообщения файлам, так как они могут содержать опасные вредоносные программы.

В декабре 1999 года российский разработчик средств антивирусной защиты компания «ДиалогНаука» сообщила о том, что в её офис поступило письмо от одного из администраторов локальной сети из Мурманска. В этом городе объявился человек, выдающий себя за ученика Д. Н. Лозинского и предлагающий за большие деньги проверить и вылечить компьютеры от нового страшного вируса «Mozart», который якобы заработает 1 января 2000 года и нанесёт непоправимый ущерб. Он будет «портить» Flash BIOS, разгонять жёсткие диски до критичной скорости так, что они будут сгорать, выводить из строя видео карты, память и т. п. «ДиалогНаука» отреагировала крайне оперативно и официально заявила, что «не имеет к этому человеку

никакого отношения. Более того, такого вируса не было, а придуман он в целях обмана доверчивых людей». Финита ля комедия.

Пользователей продолжали запугивать и в последующие годы.

В мае 2000 года в «компьютерном сообществе» циркулировало уведомление пользователей с вполне серьёзным предупреждением о не существующем вирусе «Win a holiday», а также письмо с «антивирусным предупреждением от IBM».

О распространяемой по e-Mail фальшивке под названием «Win a holiday» («Выиграй отдых») компьютерным пользователям сообщила финская компания-разработчик антивирусного программного обеспечения F-Secure. Ложное e-Mail сообщение содержало предупреждение о несуществующем вирусе, который якобы стирает информацию на жёстком диске, и предлагало разослать это сообщение по другим адресам. F-Secure рекомендовала игнорировать это послание и не пересылать его своим знакомым во избежание распространения ложной информации. Примерно в те же дни фирма IBM уведомила компьютерных пользователей о распространяемом от лица компании фальшивом предупреждении о вирусе, который, как говорилось в этой компьютерной мистификации, является ещё более разрушительным, чем знаменитая «Melissa». Ложное сообщение, адресованное пользователям PC и Apple Macintosh, впервые появилось в конце марта под заголовком «Let's watch TV» («Давайте смотреть ТВ») и не получило широкого распространения, но затем его появление было отмечено вновь, вскоре после вирусной эпидемии с «любовными письмами». Теперь мистификация распространилась достаточно широко, возможно как реакция на обеспокоенность компьютерных пользователей в связи с вирусами, подобными вирусу «I Love You». Компьютерная мистификация имела вариации, встречаясь также под именами «Wobbler», «California IBM» и «Kali». IBM предупредила пользователей, что это сообщение является обманом, и настоятельно советовала получателям игнорировать его, а также удалить это письмо и не пересылать его другим.

В январе 2001 года, в связи с многочисленными запросами российских пользователей, уже отечественным специалистам пришлось давать разъяснения по поводу ненормальной ситуации, сложившейся вокруг того же, якобы разрушительного компьютерного вируса «California IBM», а также вируса «GirlThing» и официально заявить, что оба так называемых «вируса» не что иное, как компьютерная мистификация, и они не представляют абсолютно никакой угрозы для компьютеров, более того, они попросту не существуют! Первые обращения от российских пользователей начали поступать в ноябре 2000 года, однако к январю 2001 года, в связи с тем, что ряд изданий опубликовали непроверенные данные, началась настоящая вирусная истерия.

Обе мистификации написаны по стандартному сценарию и наделали шума во многих странах Европы, в частности существовали английская, нидерландская и датская версии. Суть мистификаций сводилась к следующему. Пользователь получает письмо от знакомого адресанта с пересылкой новости о якобы крайне опасном вирусе, против которого пока не существует никакой защиты. Обычно, в подобных сообщениях содержалась ссылка на известную компанию, как правило, не имеющую отношения к разработке антивирусных средств. Текст же представлял собой однотипное предупреждение, например такое: «По сообщению «Microsoft» эти вирусы обладают большой разрушительной силой, ещё большей, чем у вируса «LoveLetter». Пока, против них нет никакого антивируса. Они пожирают всю информацию на жёстком диске, разрушают браузеры MS Internet Explorer и Netscape Navigator. Ни при каких обстоятельствах не открывайте файлы с такими названиями. Пока мало, кто в курсе. Перешлите это сообщение как можно большему количеству Ваших знакомых». Специалисты убедительно просили пользователей не поддаваться провокации, так как при пересылке вирусных мистификаций друзьям и знакомым тратится своё и чужое время и, кроме того, это способствует возникновению необоснованной паники. В целях обеспечения безопасности

при получении подобного письма давался совет о его немедленном уничтожении.

В начале сентября 2000 года по бескрайным просторам Интернет прокатились две неприятные и уже упоминавшиеся нами компьютерные «шуточки»: «Joke.Win32.Errore» и «Joke_FakeFormat». Первая из них представляет собой программу-«шутку», имитирующую форматирование жёсткого диска. При запуске она выводит несколько ложных сообщений об ошибке в MS Windows:

Errore interno di Windows 345 all'indirizzo 4E6F:942A

Errore interno di Windows 591 all'indirizzo 93C0:6210

Errore interno di Windows 712 all'indirizzo 7ED5:89C2

Errore interno di Windows 128 all'indirizzo 6542:EF21

Errore interno di Windows 591 all'indirizzo 63F0:81B2

ERRORE FATALE 14

А затем выводит запрос на форматирование диска C:

Sei veramente sicuro di voler formattare l'hard disk? [Yes] [No] [Cancel]

Вне зависимости от ответа (Yes, No или Cancel) программа имитирует форматирование жёсткого диска. Пользователь при этом не может прекратить выполнение этой операции, а на самом деле никакого форматирования не происходит, и все данные на жёстком диске остаются в целости и сохранности. По окончании «форматирования» программа выводит на экран «мусор», ещё несколько сообщений и завершает свою работу.

«Joke_FakeFormat» представляет собой фактически аналогию предыдущей программы-шутки «Joke.Win32.Errore» и также имитирует форматирование жёсткого диска. После запуска программы нажатие на любую кнопку вызывает запуск форматирования. Пользователь при этом не может прекратить выполнение этой операции. На самом деле никакого форматирования не происходит, все данные на диске опять-таки остаются в

целости и сохранности. По окончании «форматирования» кнопка «Close» закрывает программу.

15 января 2001 года компания McAfee сообщила о появлении в Интернет очередной компьютерной мистификации под названием «WAZUP». Мистификация представляла собой довольно длинный текст на французском языке и предупреждала пользователей о несуществующем компьютерном вирусе, который якобы непоправимым образом портит жёсткий диск, уничтожая на нём все системные файлы, а также все файлы с расширениями «*.zip», «*.doc» и «*.jpg». Кроме того, неизвестные доброжелатели предупреждали, что этот «вирус» якобы отправит имя и пароль доступа пользователя в Интернет. Всем, кто получил подобное письмо, компания McAfee посоветовала проигнорировать его, удалить и не распространять дальше по Глобальной сети. В сентябре 2001 года та же компания McAfee предупредила о появлении в Интернет новой компьютерной мистификации под названием «Pikachus Ball». Мистификация представляла собой письмо на ломаном испанском языке с ложным сообщением о новом вирусе. Текст мистификации гласил о том, что компания Symantec якобы опубликовала предупреждение о вирусе, который распространяется по электронной почте в присоединённом файле «pikachusball.exe» и портит жёсткие диски. Компания McAfee разъяснила, что это e-Mail сообщение от первого и до последнего слова обман и советовала всем пользователям, получившим подобное письмо, сразу же удалить его и не распространять фиктивную информацию далее.

Следует ещё раз напомнить, что вирусные мистификации могут обладать отнюдь не столь «безобидным» характером как в большинстве из приведённых выше случаев и носить разрушительный характер, приводя, например, к повреждению операционной системы. Но и в этом случае всё делается как бы исподтишка, руками самих пользователей.

В мае 2001 года появилась компьютерная мистификация, которая провоцировала пользователей на удаление системных файлов. Пользователи,

были встревожены появлением нового, чрезвычайно опасного вируса, скрывающегося в файле «sulfnbk.exe», однако в действительности такого вируса не существовало, и все сообщения о нём были, затем, классифицированы специалистами как компьютерная мистификация. Но, до этого предупреждения о ложном вирусе начали массово распространяться и вызвали настоящую панику среди около компьютерной общественности и неопытных пользователей. Как указывалось в тексте сообщения о вирусе, он якобы содержится в файле «sulfnbk.exe» и запрограммирован на активизацию 1 июня. Как обычно бывает в случаях с компьютерными мистификациями, сообщалось, что никакие антивирусные программы не в состоянии обнаружить его и потому наилучшим способом избавления от этой угрозы является немедленное удаление файла-носителя вируса. Однако, файл «sulfnbk.exe» абсолютно безопасен и, более того, он является частью операционной системы и входит в стандартную поставку MS Windows. Программа представляет собой MS Windows-приложение и используется для резервного копирования файлов с длинными именами, а ёе удаление влечёт за собой изменение функциональности системы в целом, что может сделать невозможным проведение некоторых операций на данном компьютере. Между тем, как сообщал Центр по проблемам информационной безопасности (SecurityPortal.com), его специалистам удалось получить «оригинальный sulfnbk.exe»[2] и установить причину и истоки возникновения этой мистификации. Дело в том, что первоначально эта программа, которую обвиняли во вредоносности, на компьютере инициатора фальшивого предупреждения действительно была заражена Интернет-червём «Win32.Magistr», который на тот момент входил в десятку наиболее распространённых вирусов. В результате «новость» о несуществующем вирусе разрослась до неимоверных размеров.

[2] Именно тот файл, с которого и началась эта компьютерная мистификация, а не файл «sulfnbk.exe», который входит в стандартную поставку MS Windows.

В июне 2001 года в Интернет появилась очередная компьютерная мистификация под названием «ANTICRISTO», которая имела все присущие подобным провокациям черты. В ней сообщалось о появлении самого «страшного вируса в истории», который уничтожает всю информацию на жёстком диске, и, конечно же, настоятельная просьба переслать эту информацию как можно большему количеству пользователей. Ко всему прочему в сообщении утверждалось, что якобы компании Microsoft и McAfee подтвердили необычайно высокую степень деструктивной способности описываемого «вируса». Но такого «вируса» не существовало, и это сообщение являлось классической компьютерной мистификацией. Рекомендации специалистов были достаточно стандартны: «Ни в коем случае не следует пересылать подобные письма! Этим Вы только засоряете Интернет никому не нужной информацией, отвлекаете и напрасно беспокоите ваших коллег, знакомых и незнакомых людей. Если вы получили подобное «предупреждение», уничтожьте его и не принимайте во внимание».

14 марта 2002 года сразу несколько западных онлайновых изданий сообщили об обнаружении электронного письма, которое якобы содержало фальшивый патч, разосланный компанией Microsoft. При ближайшем рассмотрении обнаружилось, что, хотя в поле отправителя указан e-Mail в домене Microsoft.com, реально письмо было отправлено с другого адреса (martinnk@erols.com). Текст письма предлагал пользователям установить патч, прилагаемый во вложении письма, чтобы обезопасить себя от нескольких уязвимостей в браузере MS Internet Explorer и ссылался на сообщение на сайте Microsoft, которое касалось обнаружения уязвимостей. Более того, заплата от Microsoft с именем «q216309.exe» действительно существовала, однако «родной» патч имел размер 2,41 Мб, в то время как прикреплённый к письму файл имел объём всего лишь 123 Кб. В силу указанных причин пользователям, получившим такого рода сообщение, рекомендовалось незамедлительно удалить фальсифицированную программную «заплатку».

В конце апреля 2002 года сначала появились слухи о новом опасном вирусе, якобы содержащемся в файле с названием «jdbgmgr.exe» на компьютерах под управлением операционной системы MS Windows, а затем по этому поводу в службы технической поддержки компаний-разработчиков антивирусных средств начало поступать множество обращений пользователей из различных стран.

В действительности «jdbgmgr.exe» является стандартной утилитой (программа для отладки работы Java-приложений), входящей в поставку всех наиболее распространённых версий MS Windows, таких как Windows 95/98/NT/ME/2000/XP. Её удаление или модификация может повлечь за собой изменение функциональности операционной системы и, в некоторых случаях, иметь негативные последствия. Сам файл «jdbgmgr.exe» не является компьютерным вирусом, но, как и любой другой exe-файл, может быть инфицирован. Так, опасный полиморфный вирус «Win32.Magistr» почему-то тяготеет к этой программе и часто заражает именно её. Последнее обстоятельство и стало причиной распространения вирусной мистификации: инициатор слухов обнаружил на своём компьютере «Win32.Magistr», посчитал, что заражённый файл «jdbgmgr.exe» является компьютерным вирусом, и разослал сообщения об этом всем своим знакомым. Обратите внимание на то обстоятельство, что приведённая схема обнаружения и распространения «jdbgmgr.exe» абсолютно аналогична ранее приведённой причинно-следственной цепочке, связанной с мистификацией в отношении файла «sulfnbk.exe», который также является стандартной утилитой MS Windows. В основном, рекомендации пользователям были выданы весьма стандартные: воздержаться от распространения необоснованных слухов и поставить об этом в известность всех своих знакомых, поверивших в несуществующий вирус.

Кроме того, в специальном заявлении одного из наиболее известных отечественных разработчиков антивирусного программного обеспечения «ДиалогНаука», в связи с этой компьютерной мистификацией,

подчёркивалось следующее: «Важно понимать разницу при получении предупреждения-мистификатора о новом “вирусе” и письма, содержащего вложение с именем “jdbgmgr.exe”. Если же Вы получили сообщение, во вложении к которому содержится файл “jdbgmgr.exe”, то очень может быть, что это вложение содержит вирус. ДиалогНаука рекомендует немедленно удалить подобное сообщение, не открывая само вложение. Если такое письмо пришло от знакомого корреспондента, попросите его подтвердить направление Вам такого файла и направить его ещё раз, желательно в заархивированном виде. Если Вы обнаружите “jdbgmgr.exe” в своём системном каталоге, то знайте, что, скорее всего, это просто чистый файл (на всякий случай можно проверить его с помощью сканера). Опасность такой мистификации очевидна. Удаление программы “jdbgmgr.exe”, которая является системным компонентом MS Windows, может повлечь за собой сбой в работе операционной системы. Причем сделаете это Вы, своими собственными руками! Не говоря о времени, бесцельно потраченном на рассылку всем друзьям и знакомым бесконечных писем, предупреждающих о появлении новой опасности. В том случае если Вы поверили письму-мистификации и всё-таки удалили утилиту “jdbgmgr.exe”, восстановить её можно путём установки обновлённой версии программы MS Internet Explorer».

Изложенное со всей очевидностью свидетельствует о том, что компьютерные мистификации не такое уж редкое явление, и в настоящее время существуют даже «электронные справочники», а также специализированные сайты по компьютерным мистификациям. Они имеют постоянно обновляемые списки самых популярных на текущий момент мистификаций, что позволяет избегать излишней нервотрёпки и не засорять Интернет поддерживающими панические настроения среди пользователей посланиями. Архивы этих сайтов содержат сведения о подавляющем большинстве мистификаций прошлых лет, а также в них попадают не только розыгрыши, связанные с вирусной угрозой, но и разного рода «лотерейные»

письма, «послания счастья», обращения от участников финансовых пирамид, просьбы о помощи от несуществующих пациентов, страдающих неизлечимыми болезнями и прочие сообщения такого же характера. Так в первой половине 2001 года на сайте CollegeClub.com регулярно появлялись дневниковые записи смертельно больной Кэйси Николь и пользователи Интернет направляли в её адрес открытки, подарки и денежные пожертвования. Но затем на сайте появилось сообщение о её смерти и некая Дебби Свенсон призналась, что этот персонаж является плодом её фантазии. В результате делом заинтересовалось ФБР США, которое усмотрело в действиях Свенсон действия, квалифицируемые как банальное компьютерное мошенничество, так как на имя мнимой больной приходили денежные пожертвования. От уголовной ответственности Свенсон спасло только то, что размер присвоенной суммы в ходе осуществлённой компьютерной мистификации оказался сравнительно небольшим – несколько сот долларов.

В 2001 году по Интернет рассылалось письмо, предупреждающее о появлении нового, чрезвычайно опасного компьютерного вируса, распространяющегося в сообщениях электронной почты под заголовком «Virtual Card for You» и имеющего вложенную виртуальную карточку (vCard). При запуске этой карточки, содержащийся в ней вирус, якобы, незаметно для пользователя рассылает свои копии по всем адресам электронной почты, найденным в адресной книге, после чего уничтожает всю информацию на жёстком диске компьютера. В предупреждение могли также включать информацию о том, что по сообщению телекомпании CNN (США) вирус в течение нескольких часов уже вызвал панику в Нью-Йорке и, как обычно сообщалось, что все антивирусные средства бессильны перед реальной опасностью. Так вот, это «предупреждение» являлось классической компьютерной мистификацией «с бородой», и, несмотря на то, что история этой «шутки» брала своё начало в декабре 1999 года, когда были отмечены первые случаи её распространения, даже более чем через год наблюдалась очередная вспышка нездорового интереса к несуществующему вирусу.

В то время считалось, что электронные карточки безопасны и их запуск, даже если они получены из неизвестного источника, не представляет опасности для компьютера или информационной системы. И вдруг – история с заражёнными карточками, распространяющимися по электронной почте, обрела своё материальное воплощение. Были опубликованы данные об обнаружении серьёзной ошибки в системе безопасности почтовых программ MS Outlook и MS Outlook Express, которая делала возможным переполнение буфера данных в процессе обработки карточек, содержащих больший объём информации, чем установлено. В итоге данные могли попадать в защищённые сегменты системной памяти и запускаться на выполнение. В лучшем случае, это влечёт за собой «зависание» самой почтовой программы, а в худшем, в компьютер могут внедриться настоящие вирусы. Вот Вам и «безобидная» компьютерная мистификация. Безусловно, полезным в этой истории является тот факт, что ещё раз подтверждено следующее правило, сформулированное квалифицированными специалистами в данной области знаний: «…очень важно максимально осторожно относиться к любым вложенным файлам, вне зависимости от их формата, и своевременно устанавливать дополнения к используемым операционным системам и прикладным программам».

Итак, компьютерные мистификации не столь уж и безобидны, как это может показаться на первый взгляд. Они приводят к вирусной истерии, которая отнюдь не вносит упорядоченность и уверенность в «стройные» ряды пользователей. Кроме того, в стремлении предупредить знакомых о потенциальной опасности пользователи тратят своё и чужое время, рассылая по Интернет ненужные послания и, тем самым, увеличивают интенсивность и без того напряжённого трафика в Глобальной сети. Более того, компьютерные мистификации притупляют бдительность пользователей, которые, привыкнув к ложным тревогам (вспомните весьма поучительную притчу о мальчике и волках), могут не поверить правдивому сообщению о действительно появившейся новой вредоносной программе. Поэтому при

получении подозрительного письма рекомендуется посетить специализированные ресурсы, о которых мы уже упомянули чуть выше и, если полученного Вами электронного сообщения нет в перечне известных на тот момент мистификаций, можно проконсультироваться по этому поводу в соответствующем подразделении фирмы-разработчика антивирусных аппаратно-программных средств. По нашему мнению, наиболее квалифицированные специалисты этого профиля находятся в известных российских компаниях, и мы рекомендуем установить контакт именно с ними. Тем более что в этом случае вы не понесёте лишних расходов на связь, отсутствует языковой барьер, да и осведомлены отечественные специалисты об активных вирусах, которые на текущий момент угрожают пользователям в российском сегменте сети Интернет, лучше своих зарубежных коллег. Однако специалисты предупреждают: у компьютерных мистификаций есть и другая, не менее опасная сторона, нет никаких гарантий, что какие-то вирусописатели не станут создавать компьютерные вирусы, называя их именами известных мистификаций. Из этой предпосылки проистекает главное правило: ни в коем случае нельзя открывать вложенные файлы, полученные из неизвестных или сомнительных источников.

Теперь, как нам кажется, самое время объединить обычно выделяемые типичные черты «классических» компьютерных мистификаций в единую систему (Рис. П.1).

Таким образом, замысел классической компьютерной мистификации состоит в том, что сочиняется предупреждение о чрезвычайно опасном вирусе, которого не существует в природе. Это предупреждение рассылается как можно большему числу пользователей с просьбой принять необходимые меры по обнаружению и удалению «вируса», а затем высказывается просьба о рассылке сообщения по всем имеющимся в наличии у пользователя адресам. В результате, такой рассылки в компьютерном сообществе возникает очередная волна вирусной истерии.

Чтобы избежать этого, специалисты дают вполне определённые советы. Приведём их как крайне важные с точки зрения успешной борьбы с компьютерными мистификациями. Во-первых, ни в коем случае не пересылайте сообщение другим. Самый надёжный способ – просто удалить это письмо. Во-вторых, как можно быстрее уведомите отправителя, что он стал жертвой компьютерной мистификации. Есть вероятность, что он не успел переслать «предупреждение» другим, помогите ему сохранить доверие к себе и не нервировать зря его коллег и партнёров. Даже если Вы получили письмо от знакомого человека, но считаете его неожиданным и странным, то лучше переспросить отправителя, действительно ли сообщение принадлежит ему, так как наиболее распространённый тип компьютерных вирусов – черви, отправляют заражённые файлы с инфицированных компьютеров так, что их владельцы об этом даже не догадываются.

Мы достаточно подробно рассмотрели такое неприятное явление, как компьютерные мистификации, но пока за скобками осталась тенденция современных вредоносных компьютерных программ к использованию жульнических приёмов, методов и трюков для повышения своей «живучести». А ведь не зря в последнее время в заголовках уважаемых электронных изданий и традиционных средств массовой информации всё чаще мелькают сообщения следующего содержания: «Опаснейший червь маскируется под обновление для системы безопасности», «Лже обновление уничтожает данные системного диска», «От имени антивирусной компании была произведена массовая рассылка троянской программы», «Злоумышленник обманом заставляет пользователей устанавливать к себе на компьютеры троянских коней», «От имени известной компании распространяется опасный вирус», «Новый вирус маскируется под программу “заплатку” от Интернет-червя», «Интернет-червь в роли мастера маскировки под программные продукты».

Все эти сообщения объединяет одно характерное свойство, которое присуще некоторым живым организмам от обычных микробов в воздухе до хамелеонов на земле или камбалы в море, и называется оно «мимикрия».

Рис. П.1. Основные характерные черты компьютерной мистификации

В нашем случае с полным правом можно сказать: вредоносная мимикрия. Вы можете задать вопрос, а причём здесь мимикрия, почему её нужно рассматривать в связи с компьютерными мистификациями? Ответ прост. Далеко не каждый человек способен или желает разрабатывать далеко идущие коварные планы и плести хитроумные интриги. Но мы глубоко убеждены в том, что если конкретный индивидуум начал заниматься написанием психологически утончённых посланий о ложных вирусах, он рано или поздно попробует создать изощрённую вредоносную компьютерную программу, которая будет использовать психологические приёмы в целях инфицирования компьютеров как можно большего числа пользователей. Пожалуй, единственным и реальным ограничением может стать лишь недостаточная компьютерная грамотность указанного индивидуума. Естественно, справедливо и рассуждение от противного за одним уточнением: современному вирусописателю обычно чего-чего, а компьютерной грамотности как раз хватает, и здесь в качестве ограничения может выступать только недостаточное знание человеческой психологии. Но представьте себе, что некий субъект представляет собой сплав и того, и другого. Вот тогда-то и происходят прецеденты, когда фактически невозможно провести чёткое разграничение между «бескорыстной» компьютерной мистификацией и вирусописательством, распространением компьютерных вирусов с точно обозначенной и, чаще всего, меркантильной конечной целью.

Впрочем, давайте рассмотрим конкретные примеры, которые относятся фактически к нашим дням.

В марте 2001 года «Лаборатория Касперского» предупредила пользователей о регистрации случаев массовой рассылки вредоносных программ с электронных почтовых ящиков ряда известных российских бесплатных почтовых систем. Рассылка производилась от имени Лаборатории и содержала следующий текст: «“Лаборатория Касперского” благодарит Вас за решение приобрести лицензионную версию Антивируса

Касперского. Мы уверены, что Вы оцените все преимущества приобретения товаров через Интернет. Это исключает необходимость приложения существенных усилий для совершения покупки: всё будет доставлено по каналам передачи связи или курьерской службой сразу Вам домой! Это даёт возможность работать на легальном лицензионном программном обеспечении, которое, в отличие от украденных копий, даёт право пользоваться круглосуточной технической поддержкой, своевременно получать обновления антивирусных баз и новые версии самой программы и рассчитывать на оперативную помощь, если с Вашим компьютером случилась беда. Кроме того, Вы будете способствовать разработке новых антивирусных технологий и дадите нам понять, что наша работа действительно Вам нужна!» В качестве «бесплатной нагрузки» письма содержали вложенный файл «avpscript_check.exe», который является троянской программой «SubSeven», и если пользователь запускал файл, то в компьютер внедрялась утилита класса «Backdoor» для скрытого управления с удалённого терминала. Это позволяло полностью контролировать все действия владельца заражённого компьютера: отслеживать посещаемые ресурсы; создавать, удалять, копировать файлы и директории; похищать конфиденциальную информацию, в том числе пароли и логины входа в Интернет. Причём, на тот момент первая версия «SubSeven» была известна более года, были известны и несколько десятков модификаций этой вредоносной программы. Более того, они давным-давно были внесены в базы данных компаний-разработчиков антивирусных средств, продукты которых блокировали их в случае обнаружения попыток проникновения на компьютеры пользователей. «Это далеко не первый случай, когда злоумышленники прикрываются именами антивирусных компаний для рассылки вредоносных кодов. Нам было приятно узнать, что ни один из пользователей, кому «посчастливилось» в этот раз получить троянскую программу «SubSeven», не поддался на этот дешёвый трюк вирусописателей и не запустил заражённые файлы. Это говорит об очень высоком уровне

информированности российских пользователей об основных принципах компьютерной безопасности», – сказал руководитель информационной службы «Лаборатории Касперского». В заключение было подчёркнуто, что публично распространяемые информационные материалы компании никогда не содержат вложенных файлов, тем более исполняемых, и если они получены по электронной почте в виде письма, то, скорее всего это фальшивка или компьютерная мистификация, которая может содержать опасный программный код.

В мае 2001 года Интернет-червь «VBS.Hard», распространяемый в электронных письмах и рассылающий себя с заражённых компьютеров, маскировался под сообщение компании Symantec. При своём распространении он, как и многие другие вирусы такого типа, использовал почтовую систему MS Outlook Express и рассылал себя всем адресатам. В результате поражённый компьютер рассылал столько заражённых писем, сколько адресов хранилось в адресной книге. Интернет-червь был написан на скрипт языке Visual Basic Script (VBS), запускался только в операционных системах с установленным MS Windows Scripting Host (в Windows 98/2000 он установлен по умолчанию) и распространялся в электронных письмах с прикреплённым VBS-файлом, который, собственно, и является телом вируса. В теме письма содержалось антивирусное предупреждение «FW: Symantec Anti-Virus Warning». Далее в письме за подписью якобы главного разработчика компании Symantec Ф. Джонс сообщалось, что в прикреплённом файле содержится подробное описание вируса. После запуска червь создавал поддельную страницу с ложной информацией о вирусе и, кроме того, прописывал в реестр поддельную страницу о вирусе как стартовую страницу для MS Internet Explorer.

В середине августа 2001 года специалисты по антивирусной безопасности предупредили о появлении нового опасного компьютерного вируса Win32.All3gro.A, который распространялся в электронном письме с темой «New antivirus tool» и вложенным файлом «antivirus.exe». Как

обещалось в письме, прилагаемая программа должна была избавить компьютер от всех возможных вирусов. Однако вместо того, чтобы выполнять указанные в письме полезные функции, «антивирус» в зависимости от дня недели удалял документы или системные файлы и рассылал свои копии по адресам из книги MS Outlook. Таким образом, Win32.All3gro.A был специально предназначен для доверчивых пользователей, напуганных последними на то время масштабными эпидемиями вирусов «CodeRed», «SirCam» и других.

В конце августа 2001 года производители антивирусных средств предупреждали компьютерных пользователей о появлении нового вируса, рассылающего себя в письмах, исходящих якобы от службы технической поддержки компании Microsoft. В адресе отправителя значилось «Microsoft Support» support@microsoft.com, а тема указывалась как: Invalid SSL certificate. Текст же письма начинался словами: «Hello, Microsoft Corporation announced that an invalid SSL certificate that web sites use is required to be installed on the user computer to use the https protocol». Действие замаскированного под письма службы технической поддержки вируса было достаточно разрушительным, так как он кодировал exe-приложения случайным ключом, делая их абсолютно бесполезными.

18 октября 2001 года Интернет-издание CNews.ru сообщило о том, что был обнаружен опаснейший Интернет-червь «Redesi», который маскируется под обновление для системы безопасности продуктов Microsoft.

Были выявлены сразу две версии этого червя (их отличия состояли лишь в теме и тексте рассылаемых сообщений, они предлагали либо защиту от вирусов, либо просмотр порнографии), распространяющего свои копии по электронной почте и способного уничтожить все данные системного диска. Название вложенного файла случайным образом выбиралось из списка: «si.exe», «rede.exe», «disk.exe», «common.exe» и «userconf.exe». При запуске заражённого вложенного файла Интернет-червь внедрялся в компьютер, получал доступ к MS Outlook и при помощи этой почтовой программы

рассылал свои копии всем получателям из адресной книги. 11 ноября 2001 года червь активизировал встроенную деструктивную функцию и уничтожал данные на диске C: заражённого компьютера. Для этого он записывал в файл «autoexec.bat» команду форматирования жёсткого диска, которая автоматически выполняется при следующей перезагрузке компьютера. Интересно отметить, что деструктивная функция работала только в случае, если на компьютере жертвы короткая системная дата соответствовала форматам «dd/mm/yy» или «mm/dd/yy».

11 ноября 2001 года компания «ДиалогНаука» сообщила об очередной попытке использовать имя и широкую известность основного продукта компании – антивируса Doctor Web. На сей раз под видом «новейшей, условно-бесплатной» разработки антивирусной программы DrWebUpgrade была разослана троянская программа. Злоумышленники воспользовались если и не самыми изощрёнными, то вполне действенными методами – потенциальных жертв попросту обманывали и убеждали, что в компанию «новейшая разработка» попала с адреса drwebupgrade@freemail.ru, а письмо с «коммерческим предложением» содержит текст следующего содержания: «Вашему вниманию предлагается новейшая разработка компании «ДиалогНаука» – антивирусная программа DrWebUpgrade, позволяющая с высокой степенью достоверности обнаруживать и эффективно бороться с новым поколением stealth и worm-вирусов. Данное программное обеспечение распространяется как shareware, то есть условно бесплатно. Программа сохраняет работоспособность и функциональность на протяжении 30 дней. Если Вы хотите использовать антивирусную программу DrWeb для защиты Вашего компьютера, то должны установить полную версию программы DrWeb, об условиях приобретения которой можно узнать, посетив сайт компании «ДиалогНаука» – лидера в разработке антивирусных программ – www.dialognauka.ru». Пикантность ситуации заключалась в том, что для пущего правдоподобия в конце содержится похвала в адрес компании, однако троянская программа от этого не перестаёт ею быть. А теперь

скажите, что это? Компьютерная мистификация? Тогда причём здесь вполне реальная троянская программа? На наш взгляд, этот, и некоторые другие примеры, представляют собой смесь «жанров»: маскировка под известный и уважаемый «бренд» – мимикрия; рассылка письма с использованием психологических приёмов – компьютерная мистификация; внедрение обманным способом в компьютер троянской программы с целью удалённого управления и получения конфиденциальной информации – компьютерное мошенничество.

В конце апреля 2002 года компания Cisco Systems предупредила о появлении в Глобальной сети почтовых сообщений, разосланных неизвестными от имени подразделения компании по безопасности и содержащих Интернет-червя «Klez.h». Представителям Cisco Systems пришлось срочно оправдываться, официально заявляя, что компания не имеет никакого отношения к данной рассылке и ищет возможность снижения количества распространяемых в Интернет подделок. Как сообщается в официальном заявлении Cisco Systems, все сообщения, распространяемые самой компанией, в том числе и в рассылках по безопасности, имеют цифровую подпись. Аналогичные сообщения, с подделанным обратным адресом, распространялись и от лица известной компании-разработчика антивирусного программного обеспечения Sophos, которой также пришлось официально объявить, о том, что она не имеет никакого отношения к данным письмам и не занимается распространением компьютерного вируса «Klez.h». В обоих случаях налицо камуфляж под известный и уважаемый «бренд» – мимикрия, но опять-таки с элементами компьютерной мистификации.

В мае 2002 года была распространена информация о регистрации массовой рассылки троянской программы «TrojanDownloader.Win32.Smokedown», замаскированной под программу лечения Интернет-червей типа «Klez».

С одного из австралийских серверов была произведена массовая рассылка этой троянской программы, замаскированной под антивирусную

утилиту для борьбы с Интернет-червём «Klez». Вредоносная программа была разослана по электронной почте. Заражённые письма имели формат HTML, и в них содержалась рекомендация «принять срочные меры» против нарастающей угрозы со стороны компьютерного вируса «Klez». Кроме того, говорилось, что технические службы за последние несколько дней выявили более 20 тысяч случаев заражения Интернет-червём «Klez». Всё письмо было написано на английском языке, а в качестве отправителя указан абонент «Kaspersky Labs» и адрес «support@kaspersky.com». В действительности вредоносная программа была разослана с австралийского почтового сервера, а приведённая информация об отправителе умышленно фальсифицирована. Более того, в теле письма также содержался замаскированный Java-скрипт, который незаметно загружал с удалённого сервера троянскую программу «Smokedown» и устанавливал её на компьютер. Для этого вредоносный код использовал брешь в системе безопасности MS Internet Explorer, которая была обнаружена ещё в конце марта 2001 года и подробно описана в соответствующем бюллетене компании Microsoft.

2 июня в общедоступной системе домашних страниц «Народ.ру» был обнаружен Web-сайт с красноречивым названием «Выпускные экзамены 2002». На нём анонимный автор предлагал посетителям загрузить файл с экзаменационными билетами по литературе и математике. При его запуске на компьютер действительно копировался список тем сочинений, якобы для последующих выпускных экзаменов, а в качестве бесплатного приложения – троянская программа «CrazyBilets», которая незаметно для владельца инфицированного компьютера создавала свою копию в системном каталоге Windows под именем «system.exe» и регистрировала её в ключе автозапуска системного реестра. Будучи активизированным, «CrazyBilets» просматривал содержимое буфера обмена данными, искал в нём пароли и передавал их «хозяину» по электронной почте. Таким образом, посторонние лица могли получать управление заражённым компьютером и контролировать все действия пользователя.

Данный инцидент демонстрирует приверженность вредоносных компьютерных программ к мимикрии под самые «горячие» темы дня, наравне, например, с маскировкой под громкие имена и торговые марки. Используя заинтересованность пользователей в том или ином событии, вирусописатели камуфлируют ими свои создания и, в этом случае высокая степень заражения гарантирована, например, желающих просмотреть список экзаменационных билетов всегда найдётся немало.

20 августа 2002 года были выявлены случаи массовой рассылки по электронной почте и инфицирования компьютеров троянской программой «TrojanDownloader.Win32. Apher». Программа рассылалась с анонимных адресов общедоступных почтовых служб, хотя сами сообщения имели поддельный адрес отправителя info@microsoft.com. Заражённые письма имели следующий вид:

От: info@microsoft.com. Тема: Protect Your NetWare with Kaspersky Anti-Virus.

Вложенный файл: AAprices.exe.

Далее шёл текст на английском языке по поводу официального выпуска программы Kaspersky Anti-Virus 4.0. Если пользователь имел неосторожность запустить вложенный в письмо файл, то «TrojanDownloader.Win32.Apher» автоматически инициировал соединение с удалённым Web-сайтом, и загружал оттуда утилиту несанкционированного управления «Backdoor.Death.25». В свою очередь, эта программа позволяет незаметно управлять инфицированным компьютером: просматривать и пересылать секретную информацию, создавать, копировать и удалять файлы и многое другое.

В ноябре 2002 года появилось сообщение о том, что по рассылке «Лаборатории Касперского» распространяется компьютерный вирус. И действительно, в Интернет появились электронные письма с предупреждением о новом компьютерном вирусе «I-Worm.Bridex», заражённые именно этим Интернет-червём. Злоумышленникам удалось

похитить список подписчиков рассылки антивирусных новостей и воспользоваться им в своих криминальных целях. В итоге компании пришлось срочно распространять рекомендации, в которых она настоятельно рекомендовала удалять письма, содержащие вложенный файл «readme.exe», обновить антивирусные базы, а также установить заплатку, ликвидирующую «дыру» в MS Internet Explorer. Кроме того, были принесены официальные извинения всем подписчикам электронных новостей, и выданы гарантии об оказании неотложной помощи в случае заражения «I-Worm.Bridex».

В ночь с 4 на 5 марта 2003 года от имени всемирно известной Yahoo! была произведена массовая рассылка поддельных поздравительных открыток, содержащих троянскую программу-шпиона «WMpatch» с целью похищения информации у пользователей российской платёжной системы WebMoney.

По разным оценкам это сообщение получили от нескольких сотен тысяч до миллиона адресатов. Вредоносные письма-фальшивки были разосланы с адреса «greeting_cards@yahoo.com» и при посещении указанного в письме адреса пользователю предлагалось скачать файл «viewcard_680fe23d52.asp.scr» и запустить его для просмотра открытки. В действительности этот файл представлял собой троянскую программу «WMpatch», которая после активизации загружала на инфицированный компьютер с того же Web-сайта две свои дополнительные компоненты. Одна из них (файл «dbole.exe») модифицировала файл «wmclient.dll» для перехвата финансовых транзакций по системе WebMoney, а другая (файл «sickboy.exe») обеспечивала 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 платёжной системы.

Только за 2002–2003 годы было обнаружено более 20 разнообразных вредоносных программ, в том числе и использующих приём мимикрии под имена известных и уважаемых компаний, пыталось похитить средства у

участников WebMoney. Почему же WebMoney постоянно подвергается атакам вирусов? Ответ прост – эта платёжная система является одной из самых популярных российских платёжных систем, позволяющих пользователям осуществлять покупки напрямую через Интернет. Популярность WebMoney является главной причиной того пристального внимания, которое уделяет ей компьютерный андеграунд, ищущий всё новые и новые способы для достижения своих целей.

В мае 2003 года был обнаружен новый сетевой червь, получивший название «Palyh». Вредоносная программа распространяется в электронных письмах и ресурсам локальных сетей и маскируется под сообщения службы технической поддержки Microsoft. Причём, уже во второй декаде мая было зарегистрировано большое количество случаев заражения компьютеров в разных странах мира.

Червь «Palyh» доставляется на целевой компьютер в виде файла, вложенного в письмо электронной почты или записанного в систему через локальную сеть. Он активизируется при запуске этого файла-носителя, после чего заражает компьютер и запускает процедуру распространения. При установке вирус копирует себя под именем «msccn32.exe» в системный каталог Windows и регистрирует этот файл в ключе автозапуска системного реестра. Таким образом, червь «Palyh» обеспечивает свою загрузку в память компьютера при старте операционной системы (по причине ошибки, в некоторых случаях он копирует себя в другие каталоги, и поэтому функция автозапуска иногда не работает). После этого червь начинает процедуры своего распространения. Для рассылки по электронной почте он сканирует файлы с расширениями «*.txt», «*.eml», «*.html», «*.htm», «*.dbx», «*.wab» и выделяет из них строки, похожие на электронные адреса. Затем вирус в обход установленной почтовой программы подключается к используемому SMTP-серверу и рассылает через него на эти адреса свои копии.

В качестве отправителя все письма червя «Palyh» используют фальсифицированный адрес (support@microsoft.com), но содержат различные

заголовки, тексты и имена вложенных файлов. Следует отметить, что все файлы имеют расширение «*.pif» (например, «password.pif»), хотя на самом деле являются обычными exe-файлами. В данном случае вирус использует ложное представление пользователей о безопасности pif-файлов и недочёт MS Windows, так как известно, что эта операционная система обрабатывает файлы не по расширению, а по внутреннему формату. Для распространения по локальной сети червь сканирует другие сетевые компьютеры и, если находит на них каталоги автозапуска Windows, записывает туда свои копии.

Таким образом, в целом червь «Palyh» обладает рядом особенностей, которые представляют собой опасность для владельцев компьютеров. Червь, например, имеет функцию загрузки с удалённых Web-серверов дополнительных компонентов, то есть он в состоянии незаметно устанавливать свои более «свежие» версии или внедрять в систему программы-шпионы. И, кроме того, мимикрия под сообщения службы технической поддержки Microsoft даёт ему «фору» в том смысле, что каждый пользователь знает эту фирму, повседневно пользуется её программными продуктами, поэтому сообщение от одной из её служб обычно не вызывает у пользователя недоверия, что называется «с порога».

В июле 2003 года специализированное подразделение фирмы-разработчика антивирусного программного обеспечения Panda Software обнаружило нового червя, который получил название «Lohack.B». Он попадает в компьютеры пользователей с электронным письмом на испанском языке и маскируется под письмо от государственного органа власти или антивирусной компании.

То есть, этот вредоносный программный код массового распространения использует современные методы социального инжиниринга, заставляя пользователей считать, что заражённое письмо получено от Министерства науки и техники Испании или компании Panda Software. Идея не нова, мы уже видели попытки подобной мимикрии, но обращает на себя внимание то обстоятельство, что здесь пользователя

пытаются обмануть «подсовывая» ему не только известный «бренд», но и название государственного органа, который в Испании как раз и является главным борцом с компьютерными вирусами. Надо сказать, что это достаточно тонкий психологический ход по усыплению внимания пользователей, особенно испанских.

Таким образом, приведённые примеры со всей очевидностью показывают, что компьютерные мистификации и мимикрия вредоносных компьютерных программ очень часто представляют собой фактически две стороны одной медали.

ПРИЛОЖЕНИЕ 2

ПОРТРЕТ ВИРУСОПИСАТЕЛЯ

Иногда интересно прочитать и вспомнить, что на заре вирусописания, то есть тогда, когда появлялись первые компьютерные вирусы, частенько удавалось устанавливать личности вирусописателей, да они их обычно и не очень-то тщательно скрывали, зная, что фактически отсутствует законодательная база для привлечения их к ответственности. В результате история донесла до нас, например, экзотические для нашего уха имена двадцатитрёхлетнего Брудера Амгада и девятнадцатилетнего Басита Фаруда Алви из города Лахор (Пакистан), которые взяли, да и «разродились» компьютерным вирусом под непрезентабельным названием «Душманские мозги». Но, уже через два-три года, когда практически каждый желающий того студент начал создавать компьютерные вирусы, наступил период, когда в подавляющем большинстве случаев их авторы предпочитали оставаться в тени. Вирусы являлись миру сотнями[3], но практически все они были без «изюминки» и, кроме того, фактически копиями один другого, так как отличались между собой лишь несколькими командами или их перестановкой, то есть создание вирусов было поставлено на конвейер. И только наступление эпохи глобальных компьютерных сетей позволило ведущим на то время вирусописателям заявить о себе громкими именами и кличками. В целях распространения их идей издаются специальные газеты и журналы, посвящённые написанию вредоносных компьютерных программ,

[3] В частности, благодаря появлению в свободном пользовании конструкторов вирусов, при помощи которых можно создавать новые вирусы даже при минимальных знаниях об операционной системе и языке программирования Ассемблере, или даже вообще не имея об этом никакого представления, а также генераторов полиморфик-вирусов.

проводятся конференции по созданию вирусов и т. п. Так кто же всё-таки пишет вирусы?

Общепризнанно, что основную массу компьютерных вирусов создают школьники и студенты, которые либо изучают, либо завершают курс обучения языкам программирования и в создании вредоносных программ видят возможность пробы собственных сил. Эта, *первая группа*, вирусописателей обычно пишет вредоносные программы только для самоутверждения, не претендует на всемирную славу и, чаще всего не ставит перед собой цель как можно более широкого распространения своих творений, в основном награждая ими в «шутку» своих однокашников и знакомых. Вместе с процессом взросления у этой группы авторов вирусов меняется мотивация поведения, изменяются жизненные ориентиры и система ценностей, они начинают больше думать о будущей карьере, которая не совместима с сомнительной славой «ваятеля вирусов», и через некоторое время синдром вирусописательства затухает, а его продукты мирно доживают свой век вместе с носителями информации, на которых они хранятся, если хранятся вообще.

Вторую группу составляют опять-таки молодые люди, в число которых в качестве «идеологов» чаще всего входят студенты, которые, может быть, и «не хватают звёзд с небес», но вполне сознательно создают компьютерные вирусы и распространяют их среди пользователей. Чаще всего «продуктом жизнедеятельности» этой группы вирусописателей являются либо различные версии ставших «классическими» вирусов, либо достаточно простые программы-вирусы, которые к тому же содержат в себе многочисленные ошибки и огрехи. Вместе с тем, хочется отметить, что бывают и исключения, позволяющие вирусописателю из этой группы создать вполне работоспособный и достаточно изощрённый компьютерный вирус. Что это? Мгновенное озарение или случайность – другой вопрос, но факт остаётся фактом.

Иногда вирусописатели второй группы объединяются по интересу в «коллектив», и обычно в этих компаниях можно встретить молодых людей примерно того же возраста, чья основная профессия весьма далека от программирования и, естественно, написания вредоносных компьютерных программ. Они обычно составляют ближний круг приятелей истинного зачинщика – вирусописателя-«гуру» и представляют собой как бы почётный кортеж, но при определённых условиях и наличии способностей к программированию, вполне способны через некоторое время выйти на первые роли не только в своём замкнутом круге лиц, но и в сообществе вирусописателей в целом.

Замечено, что у этой группы вирусописателей первопричиной, дающей стимул к написанию компьютерных вирусов, обычно выступает ощущение недооценки своей «гениальной» личности либо по жизни в целом, либо на основном месте работы, где их не устраивает род деятельности, заработная плата, карьерный рост и т. п.

Процесс написания компьютерных вирусов для второй группы сильно облегчился вместе с появлением макро-вирусов, поскольку вместо трудоёмкого для понимания языка программирования Ассемблер для написания макро-вирусов теперь можно было выучить только довольно простой язык программирования Бейсик, да к тому же были разработаны конструкторы вирусов и генераторы полиморфик-вирусов.

Вот примеры личностей, которые в целом подходят под характеристику второй группы вирусописателей.

14 февраля 2001 года некий житель Нидерландов объявил себя автором вируса-червя «Анна Курникова», поразившего тысячи компьютеров по всему миру. Вирус был отмечен в США, Европе, Японии и Австралии. Новоявленный вирусописатель оставил в конференции в Интернет своё послание, подписав его «OnTheFly», в котором заявил, что признаёт себя автором вируса, который он создал при помощи генератора вирусов «[K]Alamar's Vbs Worms Creator». Он также сказал, что написал вирус не

«для забавы». «OnTheFly» сообщал, что является поклонником известной теннисистки: «Она заслуживает внимания, не так ли?» — писал он на своей Web-страничке. Также «OnTheFly» заявил, что одной из причин того, что он решил написать вирус, стал отчет IDC, в котором сообщалось, что большинство людей так ничему и не научилось после эпидемии Интернет-червя «I Love You». «OnTheFly» считал, что в быстром распространении вируса виноваты сами пользователи, которые после всех предупреждений продолжают, как ни в чём не бывало открывать исполняемые файлы, приложенные к письму. И в заключение «OnTheFly» добавил, что и в мыслях не держал навредить кому-либо, а если кто-то заразился, так «в конце концов, это их собственная ошибка».

Представители Excite@Home сообщили, что компания попыталась идентифицировать первоначального распространителя оригинальной версии вируса через систему форумов, и уверена в том, что этот человек живёт в Нидерландах. Предполагалось, что именно форум Excite стал первым сайтом, где появился вирус «Анна Курникова».

Уже на следующий день полиция городка Сник, что на севере Голландии арестовала подозреваемого в создании вируса-червя «Анна Курникова». Им оказался 20-летний студент из северной провинции Голландии. Незадачливого вирусописателя вычислили в течение буквально нескольких часов после его заявления об авторстве по причине небрежности в заметании следов – благодаря сообщениям, оставленным им в Интернет-конференциях.

Однако вирусописатель успел в сопровождении своих родителей прийти в местный полицейский участок и сдаться. В официальном заявлении голландской полиции говорилось, что молодой человек «явился с повинной после того, как стали ясны губительные последствия работы вируса. Он посоветовался со своими родителями и решил сдаться властям». В случае признания его вины подозреваемому, отпущенному под подписку до дня суда, грозило до четырёх лет тюремного заключения.

А вот истинный автор вируса-червя «Анна Курникова» оказался более сообразительным и известности не захотел. Уже на следующий день после ареста любителя славы вирусописатель, известный под именем «Kalamar», написавший генератор вирусов «[K]Alamar's Vbs Worms Creator», с помощью которого и был создан вирус-червь «Анна Курникова», убрал эту программу со своего сайта. 18-летний вирусописатель, проживающий в пригороде Буэнос-Айреса, сообщил, что впервые услышал об эпидемии вируса «Анна Курникова» (известного также как VBS/SST, VBS_Kalamar, VBS/OnTheFly) по одному из местных телеканалов. Kalamar, который «очень много знает о компьютерах, – как гордо сообщила его мать, – весьма скептически относится к своей неожиданной известности и заявил, что убрал программу с сайта, так как не хотел, чтобы о нём все говорили». Похвальная скромность и предусмотрительность одновременно…

Итак, 12 сентября 2001 года формальный создатель компьютерного вируса «Анна Курникова» должен был предстать перед судом. Имя 20-летнего обвиняемого так и не было раскрыто средствам массовой информации, известно было лишь то, что молодой человек проживает в голландском городке Сник. Несмотря на тот факт, что по голландским законам тому, кто причинил подобный ущерб компьютерным системам во всём мире, полагается до четырёх лет тюремного заключения, официальные лица утверждали, что в данном случае молодому человеку грозит максимум 6 месяцев неволи. Напомним, что создатель вируса сам сдался властям, после того как фотография известной теннисистки облетела весь мир, выведя из строя множество компьютерных систем.

Прокурор запросил для 20-летнего вирусописателя наказание в виде 240 часов общественных работ, а также конфискации компьютера и модема. Грэхэм Клули, старший технический консультант британской фирмы Sophos, выражая удивление мягкостью предполагаемого наказания, сказал в интервью Newsbytes, что он был поражён запросом прокурора. «Учитывая то, что вирус «Анна Курникова» в то время был в пятёрке самых

распространённых вирусов и принёс ущерб на уровне вируса «Melissa», прокурорский запрос «посылает неправильные сигналы индустрии». Ранее, сразу после того, как Ян де Вит объявил себя автором вируса, ему были предъявлены обвинения в преднамеренном распространении через компьютерную Сеть данных с целью причинения ущерба, что грозило вирусописателю наказанием в виде 6 месяцев тюрьмы и штрафа в 100 тысяч гульденов (41 тыс. долл.).

28 сентября 2001 года 20-летний вирусописатель Ян де Вит наконец-то услышал решение суда – он должен отработать 150 часов на благо нации. Сам горе-преступник вовсе не собирался причинять мировым компьютерным системам ущерб в таком масштабе, его целью было, скорее, привлечение внимания людей к себе и звезде тенниса. Для такой страны, как Нидерланды, данный случай носит беспрецедентный характер: до сих пор ни один из жителей этой страны не нёс ответственности за подобные деяния.

В Великобритании в сентябре 2002 года полицией был арестован молодой человек, подозреваемый в создании компьютерного вируса «T0rn». Ему 21 год и проживает он в Сербитоне, пригороде на юго-востоке Большого Лондона.

Этот вирус циркулировал по Интернет в 2001 году и заражал компьютеры, работающие под управлением операционной системы Linux. «T0rn» содержал в себе ряд троянских функций, а позже на его основе был создан другой Linux-вирус, «Lion». Впрочем, заметного распространения вирус «T0rn» не получил и ущерб от него оказался невелик. Тем не менее, Скотланд-Ярд назвал арест создателя «T0rn» большим успехом, так как в Великобритании вирусописателей, в большинстве случаев, не удается не только арестовать, но и вообще найти. Поэтому успешное окончание годичного расследования, которое британские полицейские проводили совместно с ФБР США, было признано несомненным успехом. Вскоре после ареста, в связи с незначительным ущербом, нанесённым вирусом,

подозреваемый был отпущен на поруки до окончания расследования его дела.

В феврале 2003 года та же британская полиция арестовала двоих подозреваемых в создании компьютерного вируса «TK». Этот вирус, подобно Интернет-червям «CodeRed» или «Slammer», атакует серверы и не очень известен широкой публике, однако ущерб от его действий оценивается в 9 млн. долларов, и со времени своего появления он успел заразить около 18 тысяч компьютеров по всему миру. Вирус «TK» использовал «дыру» в Web-сервере IIS от Microsoft. Заразив компьютер, он открывал на нём «чёрный ход» для злоумышленника и тот мог получить полный контроль над инфицированной машиной. Адрес заражённой машины червь направлял в специально созданный чат-канал на одном из IRC-серверов.

Считается, что вирус был разработан группой «THr34t-Krew» и двое арестованных могут иметь к ней самое прямое отношение. После ареста в их домах были проведены обыски, а компьютеры подозреваемых конфискованы для проведения расследования. Оба арестованных проживают в графстве Дерхем на северо-востоке Англии. Одному из подозреваемых 19 лет и он работает электриком, а другому 21 год и он числится временно неработающим.

Набравшись знаний и вволю попрактиковавшись на создании «конвейерных» компьютерных вирусов и вирусов-модификаций своих знаменитых предшественников, некоторые из вирусописателей второй группы плавно и, зачастую, даже незаметно для себя пополняют ряды *третьей группы* программистов вредоносных кодов, которая представляет собой наибольшую опасность для всего компьютерного сообщества.

Именно в недрах этой группы обдумывают новые, эксклюзивные алгоритмы работы вирусов, способы использования недокументированных и малоизвестных путей проникновения вредоносных кодов в системные области данных, а также всё более совершенные методы последующего распространения компьютерных вирусов в информационных сетях. Тем

самым, представители третьей группы пишут и дают «путёвку в жизнь» всё новым поколениям компьютерных вирусов, построенных на новых технологических решениях. Одной из причин, заставляющих вроде бы талантливых людей направлять свои способности на разработку изощрённых компьютерных вирусов, является всё тот же, что и у представителей второй группы вирусописателей, комплекс неполноценности, иногда причудливо сочетающийся с неуравновешенной психикой.

Вредоносные компьютерные программы, которые создаются представителями третьей группы вирусописателей, специалисты в области разработки антивирусных средств защиты обычно обозначают термином «профессиональные компьютерные вирусы». Эти тщательно продуманные и отлаженные программы создаются профессионально эрудированными в своей области знаний и, иногда, очень одарёнными программистами. «Профессиональные» вирусы часто выполнены по технологии «стелс» и (или) являются полиморфик вирусами, заражают не только файлы, но и загрузочные сектора дисков, и выполняемые файлы операционных систем.

Во второй половине июня 2000 года ФБР США только начало развёртывать мероприятия по поиску автора недавно появившегося на тот момент Интернет-червя «Stages.worm», который распространялся по электронной почте, как и его ближайший собрат Интернет-червь «Love bug».

Но, эксперты-вирусологи заявили, что они уже знают того, кто мог создать и запустить в Глобальную сеть этот вирус. По их мнению, это вирусописатель «со стажем», который выступает под именем «Zulu» и, по их информации, проживает в Аргентине. Брюс Ньюджес, менеджер ICSA.net, компании, которая занимается проблемами компьютерной безопасности, заявил, что в прошлом году «Zulu» уже выкладывал исходный код «Stages.worm» на один из Web-сайтов, посвящённых вирусам. Он, по словам того же Ньюджеса, является автором и других известных вирусов: «Bubbleboy», «Monopoly» и «Freelinks». «Это делает его первым

подозреваемым среди ряда широко известных создателей вирусов», – заключил менеджер компании ICSA.net.

В середине сентября 2000 года властями Тайваня вновь был задержан Чен Ин-Хау, автор крайне разрушительного вируса «Чернобыль». Военные власти Тайваня уже интересовались личностью Чена в апреле 1999 года, но дальше допросов дело не пошло, хотя ему и грозило уголовное наказание от трёх лет тюрьмы. Чен избежал этого наказания лишь потому, что тогда не имелось никаких официальных жалоб от тайваньских компаний. Напротив, благодаря написанию знаменитого компьютерного вируса он получил престижную работу в крупной компании, связанной с деятельностью в области высоких информационных технологий. Поводом для нового ареста Чен Ин-Хау послужили обвинения, предъявленные тайваньским студентом, который пострадал от вируса «Чернобыль» в апреле 2000 года.

Напомним, что «Чернобыль» был обнаружен «в живом виде» на Тайване в июне 1998 года. Автор этого вируса заразил компьютеры в местном университете, где он в то время проходил обучение. Через некоторое время заражённые файлы были разосланы в местные Интернет-конференции, и вирус выбрался за пределы Тайваня: за последующую неделю вирусные эпидемии были зарегистрированы в Австрии, Австралии, Израиле и Великобритании. Затем вирус был обнаружен в нескольких других странах, включая и Россию. Примерно через месяц заражённые файлы были обнаружены на нескольких американских Web-серверах, распространяющих игровые программы. Этот факт, видимо, и послужил причиной последовавшей глобальной вирусной эпидемии. 26 апреля 1999 года (примерно через год после появления вируса) заработала «логическая бомба», заложенная в его код. По различным оценкам, в этот день по всему миру пострадало около полумиллиона компьютеров – у них оказались уничтожены данные на жёстком диске, а на некоторых плюс к тому испорчены и микросхемы на материнских платах. Данный инцидент стал настоящей компьютерной катастрофой, так как вирусные эпидемии и их

последствия никогда до того не были столь масштабными и не приносили таких убытков. В 2000 году «Чернобыль» вновь проявил себя по всему миру. Только в Южной Корее ущерб от этого компьютерного «монстра» оценивался в 250 млн. долларов.

В начале августа 2001 года Федеральное управление Германии по безопасности информационных технологий (BSI) объявило, что некие представители голландского компьютерного андеграунда признали своё авторство в создании Интернет-червя «CodeRed». Специалист по вирусам в BSI Франк Фельцман сказал, в частности, что голландские вирусописатели из группировки «29a» заявили о своём авторстве на одном из Интернет-форумов, однако у BSI нет никаких доказательств, что они действительно авторы вируса «CodeRed». По мнению Фельцмана, это заявление может ещё более запутать следы и затруднить поиск настоящего автора опасного вируса. Он также отверг идею о том, что вирус был разработан в Китае, несмотря на известную надпись «Взломано китайцами», которая появляется на заражённых компьютерах.

Тем временем в США продолжалось распространение как минимум двух новых версий вируса «CodeRed», а Фельцман оказался прав лишь наполовину. В начале сентября 2001 года предполагаемый автор Интернет-червя «CodeRed» был «виртуально» найден в Китае. По словам Кейта Родса, руководителя Бюро расследований Конгресса США, автор этого вируса действовал из университета, расположенного в китайской провинции Гуандон. При этом Родс заявил, что пока официальные подозрения не выдвигаются ни против определённой страны, ни против физического лица, но расследование по этому делу ведётся американскими властями с 19 июля 2001 года, когда Интернет-червь «CodeRed» заразил в США за 9 часов 250 тысяч компьютеров.

По сведениям Национального центра по защите инфраструктуры (NIPC) в общей сложности на момент публикации сообщения об авторстве

китайцев в создании «CodeRed» заражению подверглось уже 975 тысяч серверов.

В мае 2002 года Дэвид Смит, автор печально известного вируса «Melissa», был приговорён в городе Ньюарк, штат Нью-Джерси к 10 годам тюремного заключения в федеральной тюрьме США. Смит был обвинён ещё в декабре 1999 года в создании и распространении вредоносной компьютерной программы, ущерб от которой оценивают примерно в 1,2 млрд. долларов. Впрочем, ему предстоит провести за решёткой только 20 месяцев – это срок, к которому за два года до этого приговорил его федеральный суд, а по американскому законодательству обвиняемый не может получить от суда штата больший срок, чем от федерального суда США. Кроме отбывания заключения, Смиту придётся уплатить штраф в размере 5 тысяч долларов.

Смит признал себя виновным в нанесении ущерба общественным коммуникациям и на суде сказал, что с его стороны это было «колоссальной ошибкой», но так и не признал себя уголовным преступником. Тем не менее, судья Лоуренс Лоусон счёл необходимым дать ему максимально возможный срок (хотя бы фактически и условно), в назидание другим вирусописателям. «Как вы сами сказали, теперь вас все будут звать «ходячей Мелиссой, – сказал судья Лоусон Смиту, – но вы можете это исправить». Судья посоветовал подсудимому выступить перед старшеклассниками и студентами с лекциями о том, какой страшный ущерб способны причинять компьютерные вирусы.

Смит стал первым гражданином штата Нью-Джерси, который приговорён к тюремному заключению за распространение компьютерного вируса и одним из первых программистов, осуждённых за создание компьютерного вируса. Напомним, что вирус «Melissa» передавался через электронную почту с пометкой «Важное сообщение» и вызывал автоматическую рассылку ещё 50 аналогичных писем, что приводило к замедлению работы почтовых серверов или полной невозможности их

функционирования. В момент своего создания вирус «Melissa» был одним из самых опасных вирусов, хотя он физически не устранял файлы с компьютеров пользователей.

А теперь давайте перейдём к истории, которая касается вирусописателей, относящихся к третьей группе, и получившая прямо-таки детективный оттенок в освещении как электронных, так и традиционных средств массовой информации. Это история поисков автора знаменитого Интернет-червя «I Love You».

Пожалуй, самой первой информацией об авторе Интернет-червя «I Love You», которая казалась более или менее достоверной, стало сообщение, датированное началом мая 2000 года, о том, что им является филиппинский школьник. Ведь в каждом рассылаемом письме среди прочего содержалась строчка «I hate to go to school» («Я ненавижу ходить в школу).

Интернет-червь, который получил официальное название «I-Worm.LoveLetter», был запущен в Глобальную сеть приблизительно в 3:00 по Восточноевропейскому времени. Все антивирусные компании свидетельствовали, что этот вирус был самым опасным, самым быстро распространяющимся и мог принести самый большой за всю историю ущерб. Действие вируса начиналось после того, как пользователь открывал (на некоторых MS Outlook системах это происходит автоматически) присоединённый файл «love-letter-for-you.txt.vbs, который представлял собой скрипт на языке Visual Basic. Будучи запущенным, вирус заменял файлы двенадцати типов, находящиеся на всех доступных дисках, своими копиями: vbs, vbe, js, jse, css, wsh, sct и hta, а также, что странно, jpg, jpeg, mp3, mp2.

Но не успели полиция и журналисты сосредоточиться на филиппинском школьнике, как представитель филиппинской фирмы Supernet заявил, что располагает данными в отношении человека, являющегося истинным создателем Интернет-червя «I Love You». Считалось, что именно с двух адресов электронной почты, расположенных на сервере Supernet, началось распространение новой глобальной эпидемии, и поэтому к словам

представителя Supernet сразу же прислушались. Так вот, по словам представителя фирмы, ранее тот же человек пытался проникнуть в их компьютерную сеть, в связи с чем ему отключили доступ в Интернет через этого провайдера. К сожалению, полиция Филиппин располагала только отрывочными сведениями об этом человеке, в частности, был известен телефонный номер, из которого можно было заключить, что создатель вируса проживает (или проживал) в одном из пригородов столицы Филиппин Манилы. Был также назван возраст этого человека – 23 года, и по запросу ФБР США филиппинская полиция немедленно начала проводить оперативно-розыскные мероприятия по поиску автора вируса.

А на следующий день, 6 мая, эксперт по компьютерным вирусам Фредерик Бьорк из университета Стокгольма (Швеция), заявил, что ему удалось идентифицировать злоумышленника, написавшего и распространившего Интернет-червя «I Love You». Автор –немецкий студент, обучающийся в данный момент в Австралии – скрывается под псевдонимом «Spyder», его настоящее имя Михель, возраст чуть больше 20 лет. На след немецкого студента шведскому эксперту удалось, по его словам, выйти по следам, оставленным неким Михелем в конференциях Usenet. Как отметил Бьорк, немецкий хакер разослал вирус с одного из филиппинских адресов в Интернет, что, однако, совершенно не означает, что он и сам там физически находился. Полиция и провайдеры, продолжавшие тем временем расследование, заявили, что вирусописатель живёт в пригороде Манилы, а вирус был отправлен через провайдера Supernet.

Ранее Бьорк помог обнаружить автора знаменитого вируса «Melissa», что, впрочем, не могло составить большого труда, так как он забыл убрать свои личные данные пользователя, которые MS Word автоматически прописывает в каждый документ. Но, словам этого эксперта многие доверяли, хотя в то же время многие шведские компьютерные эксперты весьма сдержано прореагировали на заявление своего коллеги.

Итак, пока Бьорк фактически направлял поиск автора Интернет-червя «I Love You» в Австралию, на Филиппинах события шли своим чередом.

10 мая на свободу за недостатком улик был выпущен 27-летний филиппинский банковский служащий Рионел Рамонес, арестованный по подозрению в причастности к авторству Интернет-червя «I Love You». Обвинение основывалось на показаниях Интернет-провайдера от 5 мая, о которых мы говорили выше и которые указывали, что источником вируса является компьютер, расположенный в квартире Рамонеса, где он и проживал со своей подругой Ирэн де Гузман. Однако эти улики были признаны недостаточными, и он был отпущен вплоть до появления дополнительных фактов по этому делу. Тем не менее, Рамонесу предстояло предстать перед властями 19 мая для допроса в рамках предъявленного ему предварительного обвинения.

Поиски автора вируса продолжались с прежней настойчивостью, и уже 15 мая филиппинская полиция заявила, что подозревает одну из подпольных группировок вирусописателей Филиппин в создании и распространении Интернет-червя «I Love You», эпидемия которого принесла к тому времени миллиардные убытки по всему миру. Речь шла о группе из Манилы, известной в Глобальной сети под псевдонимом «GRAMMERSoft». На подозрения навёл сам псевдоним, так как это слово неоднократно встречалось в программном коде самого вируса. Кроме этого, полиция не сделала никаких заявлений по поводу того, располагает ли она ещё какими-либо доказательствами относительно участия членов группы в создании и распространении вируса.

Буквально несколькими часами позже как гром, пусть и среди не совсем ясного неба, прозвучало заявление на пресс-конференции 23-летнего филиппинского студента Онела де Гузмана, что он, возможно, случайно выпустил злополучный компьютерный вирус в Интернет. Несмотря на такое косвенное признание, он отрицал авторство и употреблял слово «возможно». В результате, по состоянию на 15 мая список подозреваемых увеличился до 4

человек. В нём, помимо самого Онела де Гузмана, теперь фигурировали его сестра Ирэн де Гузман, её приятель Рионел Рамонес и ещё один студент Михель Буэн. Национальное бюро расследований Филиппин не исключало, что этот список мог вскоре пополниться. Расследование продолжалось в прежнем темпе, но никаких арестов полиция пока больше не производила, а спикер парламента Филиппин в интервью местной газете довольно легкомысленно заявил, что гордится тем, что в стране есть такие гении, которые, к сожалению, сошли с правильного пути. Может быть, у него было спокойно на душе оттого, что на Филиппинах вирус практически не нанёс никакого ущерба, так как компьютеризация в стране находится на низком уровне.

Всего лишь через сутки список подозреваемых в причастности к созданию Интернет-червя «I Love You» стремительно «разбухает». Филиппинская полиция на тот момент оперировала списком уже из 53 человек, которые могли иметь хотя бы какое-либо отношение к этому делу. Все 53 подозреваемых получили повестки на допрос к следователю.

В этот же день филиппинский студент Михель Буэн, один из подозреваемых, категорически опроверг все обвинения в свой адрес. Подозрения основывались на том факте, что программа, используемая в его дипломном проекте, для создания вируса могла быть объединена с работами другого подозреваемого, Онела де Гузмана. Буэн полностью отрицал свою причастность и объявил себя полностью невиновным. При этом он выразил готовность содействовать властям в расследовании этого дела.

Однако ровно через двое суток после этих событий дома у одного из главных подозреваемых по делу об Интернет-черве «I Love You» были найдены улики, подтверждающие его причастность к созданию вируса. На дискете, которая находилась в доме Онела де Гузмана, нашли два компьютерных вируса. Обыск в доме проводили силы Национального бюро расследования Филиппин, и найденный на дискете вирус был очень похож на Интернет-червя «I Love You». Как сообщил Элфрен Менесес, руководитель

подразделения Национального бюро расследований по борьбе с компьютерными преступлениями, в его создании принял самое непосредственное участие Михель Буэн, второй основной подозреваемый по этому делу, так же, как и группа «GRAMMERSoft». Нахождение второго вируса на дискете было связано с определёнными трудностями для специалистов, так как файл с диска был уже удалён, но его удалось восстановить.

После завершения такого важного этапа расследования на Филиппинах наступило более чем двухнедельное затишье, и только новость из Австрии, обнародованная 1 июня 2000 года несколько освежила пейзаж после битвы. Благодаря совместным усилиям полиции Австрии и Германии 31 мая был арестован 28-летнний распространитель одной из модификаций вируса «I Love You». Он был задержан после того, как полиция провела следственные мероприятия по приказу Министра внутренних дел Отто Шилли. Арестованный сознался в содеянном, и не отрицал свою вину.

8 июня наконец-то стало понятно, почему восемнадцать дней продолжалось подозрительное безмолвие. Власти Филиппин были вынуждены закрыть судебное дело против 27-летнего банковского служащего Рионеля Рамонеса, подозреваемого в распространении Интернет-червя «I Love You» по причине отсутствия в стране законодательной базы, рассчитанной на подобные инциденты. Сторона обвинения сказала, что расследование не смогло предоставить суду достаточно улик для обоснования статьи нелегального использования паролей кредитных карт или банковских счетов с целью хищения денег. Рамонес утверждал, что его перепутали с кем-то другим, хотя следствие вышло на его квартиру. Адвокат другого подозреваемого, Онела де Гузмана, заявил, что его клиент мог переслать вирус случайно. К тому времени, вирус уничтожил множество пользовательских файлов, отправил множество паролей доступа в Интернет своему владельцу и спокойно распространялся через адресные книги

инфицированных компьютеров. Были затронуты такие структуры, как Пентагон США и Британский парламент.

Через пять дней, 13 июня, филиппинские власти сообщили, что студенту Онелу де Гузману, подозреваемому в создании и распространении Интернет-червя «I Love You», всё-таки будет предъявлено обвинение. Как заявил глава Национального бюро расследований Филиппин Федерико Опинион, наказание вряд ли будет суровым, поскольку в стране отсутствует соответствующая законодательная база.

30 июня Федерико Опинион подал прошение в Министерство юстиции Филиппин с просьбой выдвинуть официальное обвинение против главного подозреваемого в авторстве вируса «I Love You», 23-летнего студента Онела де Гузмана. При этом он сам признал, что у Бюро нет прямых доказательств в его причастности к созданию и распространению вируса, а есть только косвенные улики. Против другого подозреваемого, Михеля Буэна, никаких обвинений пока не выдвинуто, однако Бюро не исключает возможность того, что это будет сделано позже.

И вот 21 августа ввиду недостаточности улик дело против бывшего студента Компьютерного колледжа Манилы, филиппинца Онела де Гузмана, подозреваемого в создании Интернет-червя «I Love You», который всегда отрицал обвинения в создании вируса, наделавшего бед во всем мире, было закрыто. Спасло его то обстоятельство, что в мае 2000 года, когда вирус начал распространяться на Филиппинах, ещё не существовал закон об ответственности за подобные правонарушения, появился он только в июне.

5 сентября филиппинские следователи обратились в Министерство юстиции Филиппин с просьбой пересмотреть решение суда о снятии обвинений с человека, подозреваемого в создании компьютерного вируса «I Love You». Так как новый закон о компьютерных преступлениях не может быть применён в случае с Онелем де Гузманом, следствие решило обвинить его в ряде «обычных» преступлений, таких как кража информации и вандализм.

Онел де Гузман между тем совсем перестал отрицать возможность того, что это именно он выпустил Интернет-червя «I Love You» в Глобальную сеть, но своё авторство в создании вируса категорически отрицал. Поскольку за время эпидемии появилось несколько модификаций «I Love You», стало очень сложно доказать причастность Онеля де Гузмана к краже паролей.

Таким образом, вся эта криминальная история с Интернет-червём «I Love You» обернулась для него лишь исключением из колледжа. Создатель всемирно известного Интернет-червя «I Love You» Онел де Гузман остался фактически безнаказанным.

Четвёртую группу авторов компьютерных вирусов эксперты-профессионалы в области разработки антивирусных средств обычно называют общим собирательным термином «исследователи» и выделяют их в обособленную, стоящую несколько особняком от других вирусописателей категорию людей. По их определению, «эта группа состоит из довольно сообразительных программистов, которые занимаются изобретением принципиально новых методов заражения, скрытия, противодействия антивирусам и т. д. Они же придумывают способы внедрения в новые операционные системы, конструкторы вирусов и полиморфик генераторы. Эти программисты пишут вирусы не ради собственно вирусов, а скорее ради «исследования» потенциалов «компьютерной фауны». Обычно авторы подобных компьютерных вирусов не выпускают их в свет, но активно пропагандируют свои идеи через многочисленные электронные издания, посвящённые созданию вирусов. При этом опасность от таких «исследовательских» разработок ни в коем случае нельзя умалять, ведь даже случайно попав к представителям вирусописателей из третьей группы, инновации рано или поздно (обычно рано) практически стопроцентно включаются во вредоносные коды, и дают жизнь как отдельным экземплярам не имеющих в прошлом аналогов, так и новым поколениям компьютерных вирусов.

На информационном портале ZDNet 6 февраля 2003 года была опубликована информации, согласно которой для создания Интернет-червя «Slammer» использовался демонстрационный код, опубликованный экспертом по безопасности информационных технологий Дэвидом Литчфилдом из компании NGS Software, и автор на этом не собирается останавливаться.

Интернет-червь «Slammer», заражающий серверы под управлением системы баз данных Microsoft SQL Server 2000, вызвал одну из крупнейших в истории глобальную эпидемию, которая затронула практически все страны мира. Литчфилд признал, что код «proof of concept», написанный им для демонстрации ошибки в программном обеспечении Microsoft SQL, использовался в качестве «шаблона» для червя SQL. Тем не менее, он также заявил о том, что не намерен отказываться от дальнейшей практики публикации кодов. По мнению Литчфилда, примеры кода играют важную и благотворную роль для безопасности Интернет. Во-первых, демонстрационный код помогает разработчикам учиться на чужих ошибках, а во-вторых, позволяет системным администраторам, производителям сканеров безопасности и поставщикам оборудования для обнаружения проникновений, быстрее выпускать и обновлять свои продукты.

Очевидно, что Литчфилд является ярким представителем четвёртой группы вирусописателей и его позиция весьма спорна, так как публикация демонстрационных кодов это своего рода провокация для вирусописателей. Однако сам Литчфилд считает, что, следуя этой логике, любая информация о наличие бреши в продукте может явиться лакомым куском для вирусописателя, который, при желании может использовать на своё усмотрение обнародованную уязвимость. Тут дело лишь в его квалификации. Бог ему судья.

Пятая группа авторов компьютерных вирусов представляет собой различных по своему общественному положению и образовательному уровню людей, которые с помощью написания и распространения

вредоносных программ надеются привлечь внимание компьютерной общественности к какой-либо проблеме, кажущейся им очень важной, неотложной и не заслуженно обойдённой вниманием. Здесь, обычно, ведущими мотивами могут быть как политические требования, так и проблемы личного мировоззрения, убеждённости собственной правоты во взгляде на построение современного общества и пр. Такие вирусописатели редко бывают злостными злоумышленниками и, если добиваются поставленной цели, то очень редко продолжают свою деятельность в области написания и распространения компьютерных вирусов. Для них паблисити, собственно говоря, является конечной целью. Исключение представляют, конечно же, фанатики всех мастей, которые лишь прикрываются благородными лозунгами и теориями.

Вот вам и представители этой группы вирусописателей.

22 октября 2000 года на Филиппинах был арестован подозреваемый в распространении компьютерного вируса «Erap Estrada», имеющего политический оттенок и направленного против президента этой страны Эрапа Эстрады. Девятнадцатилетний молодой человек был арестован в своём доме агентами Национального бюро расследований Филиппин, и в ходе обыска у него были изъяты дискеты и компьютерное оборудование. Как сказал Элфрен Менесес, руководитель подразделения Национального бюро расследований по борьбе с компьютерными преступлениями, «все изъятые улики переданы в отдел электронной обработки данных для дальнейшего изучения и анализа».

Позднее, в связи с тем, что арестованный ранее не был замечен в подобных деяниях, он был отпущен на свободу до окончания расследования этого дела.

В конце второй декады 2001 года на многих почтовых серверах было зарегистрировано появление нового компьютерного вируса «Injustice» («Несправедливость»), созданного, по всей видимости, в поддержку народа Палестины. Вирус не наносил вреда жёсткому диску компьютера, и поэтому

был классифицирован антивирусными компаниями как вирус средней степени опасности. Распространялся он через почтовые службы, используя при этом сведения, содержащиеся в адресной книге пользователя. Вирус содержал послание «От вас я такого не ожидал», а также вложенный файл «injustice.txt.vbs», который активировался после его открытия пользователем. Запущенный файл отправлял загрузившего его пользователя на сайты, освещающие палестинскую проблему, предварительно сообщив: «Не беспокойтесь, этот вирус не опасен. Он не причинит вреда вашей системе. Его предназначение помочь палестинскому народу жить в мире на своей земле». Появление вируса «Injustice» было зарегистрировано даже на сайте правительства Израиля.

Британская антивирусная компания Sophos в начале марта 2002 года сообщила, что под псевдонимом «Gigabyte» обнаружен автор первого вируса на языке программирования «C#». На домашней странице «Gigabyte» сказано, что она является 17-летней студенткой, увлекающейся современной электронной музыкой и кикбоксингом. По её словам, целью создания вируса было стремление доказать, что женщины тоже могут создавать компьютерные вирусы, а также выступить против дискриминации по половому признаку. Майк Кэсс, руководитель отделения .NET в Microsoft, заявил о своей озабоченности тем фактом, что женщины начинают заниматься написанием вирусов: «Я просто не понимаю, что она хотела этим сказать. Такими поступками она не сможет ни причинить людям вред, ни принести им пользу».

В конце марта 2003 года шведская полиция задержала автора компьютерного вируса «Ganda», который за неделю инфицировал несколько тысяч компьютеров во всём мире, рассылается по электронной почте в письмах с предложением экранных заставок и использует для своего распространения интерес Интернет-пользователей к войне в Ираке.

Интернет-червь «Ganda» распространяется в виде файлов, прикреплённых к заражённым письмам, внедряет свою компоненту внутрь

исполняемых Win32 PE exe-файлов, активно противодействует антивирусным программам, является приложением Windows (PE exe-файл), имеет размер 45056 байт и написан на языке Assembler. Заголовок и текст выбираются из списка 10 вариантов на шведском языке и 10 вариантов на английском языке в зависимости от текущего установленного языка. Имя вложения: «xx.scr» (где xx – любые два символа в диапазоне от «a» до «z»). В одном случае экранная заставка состоит из спутниковых фотографий Ирака, в другом, темой экранной заставки является проамериканская пропаганда, некоторые из вариантов вообще не имеют отношения к войне в Персидском заливе.

Обнаружить автора вируса удалось благодаря содержавшимся в нём жалобам на шведскую школьную систему. Как оказалось, автор Интернет-червя «Ganda» живёт в городе Хэрнёсанд, что в 400 км к северу от Стокгольма и таким образом пытался привлечь к своим проблемам внимание журналистов. Задержанный признался в создании вируса и признал свою вину, а в его доме был произведён обыск. Прокурор Кристина Бролин заявила, что вирусописателю будет предъявлено обвинение в нарушении законодательства о компьютерных преступлениях и причинении материального ущерба. Максимальным наказанием по этим статьям является тюремное заключение на четыре года. Впрочем, если учесть, что вирус «Ganda» не получил широкого распространения, можно ожидать, что наказание окажется не таким жестоким.

Итак, мы, пожалуй, привели достаточно примеров характеризующих вирусописателей. Давайте рассмотрим не менее любопытные случаи неуклюжих попыток их перевоспитания или, даже, упреждения втягивания студенческой среды в процесс бесконтрольного написания вредоносных компьютерных программ при помощи квалифицированных педагогов университета.

В феврале 2001 года средства массовой информации с удивлением сообщали о решении мэра голландского городка Сник, который собрался

предложить работу автору нашумевшего вируса «Анна Курникова». Напомним, что 20-летний голландец, распространявший вирус по электронной почте, сдался властям всего за неделю до этого события, был арестован голландской полицией и впоследствии отпущен до суда домой в сопровождении родителей. Как утверждал мэр Сника, где он был арестован, «это очень талантливый молодой человек, и такие способности надо использовать в нашем компьютерном департаменте». Стоит отметить, что автором вируса этого человека можно назвать с большой натяжкой, так как червь был создан им с помощью найденного на просторах Интернет генератора вирусов «[K]Alamar's Vbs Worms Creator», позволяющего даже начинающим пользователям выпускать свои собственные вирусы. Молодой человек был отпущен властями только до суда, однако, мэр города заявил, что хотел бы пригласить его для «серьёзного разговора». Правда, до начала работы на государственной службе юноше придётся закончить учёбу.

История на этом не закончилась и, видимо воодушевлённый неожиданным вниманием, которое принёс городу его земляк автор Интернет-червя «Анна Курникова», мэр действительно предложил 20-летнему вирусописателю пройти собеседование на предмет трудоустройства, объявив об этом по национальному телевидению. Мэр не уточнил, какую именно должность готов предоставить автору вируса, но предположил, что по окончании учебы в колледже тот «будет хорошим экспертом по компьютерной безопасности» и его ожидает «серьёзное интервью».

Чрезмерно увлёкшись популизмом, мэр вряд ли подумал о последствиях своего поступка, по сути, поощряя молодёжь к написанию вредоносных программ. Ведь благодаря таким деятелям многие молодые люди могут начать подумывать о том, что писать вирусы это «круто» (тем более что для этого не обязательно быть семи пядей во лбу), что вследствие этого можно легко стать знаменитым и получить хорошую работу.

Недавно внимание специалистов по компьютерной безопасности привлёк факультет вычислительной техники университета города Калгари в

канадской провинции Альберта. Его профессора с осени 2003 года решили ввести в учебную программу новый курс «Computer Viruses and Malware» («Компьютерные вирусы и вредоносные программы»), посвящённый написанию вирусов, троянов и прочих зловредных программ. Основной темой курса станет рассказ студентам, о том, как пишутся вирусы, чтобы те узнали о них всё и могли квалифицированно разрабатывать способы борьбы с ними. Описание нового курса выглядит следующим образом: «изучение разного рода вредоносных программ, какими являются компьютерные вирусы, черви и троянские кони, которые ежегодно приносят ущерб, равный миллиардам долларов по всему миру». Вводя в учебную программу новый курс, администрация университета, конечно же, не ставит своей целью плодить вирусописателей, и создание нового курса оправдывается тем, что, зная приёмы написания вредоносных программ, выпускники смогут более эффективно бороться с такими программами. Помимо собственно приёмов создания вирусов студенты будут изучать юридические и этические аспекты подобной деятельности. Будет уделено внимание и общим проблемам компьютерной безопасности.

Преподавать новый курс назначен профессор Джон Эйкок, который сравнил его с медицинским исследованием. «Мы должны относится к компьютерным вирусам также как и к биологическим. Чтобы медики могли справиться с последними биологическими вирусами, такими как “Sars”, они должны понимать, что собой представляет вирус и как он распространяется. Почему борьба с вирусами для компьютеров должна быть другой?»

Несмотря на жёсткую критику со стороны профессионалов по информационной безопасности, руководство университета не собирается отменять занятия по этой дисциплине. По мнению же представителей антивирусных компаний, новый курс представляет собой серьёзную опасность и может способствовать значительному росту числа вирусов в Глобальной сети, причём вирусов достаточно совершенных.

По словам старшего технического консультанта фирмы Sophos Грэма Клули, создание студентами новых вирусов не несёт в себе ничего позитивного, а лишь повышает вирусную опасность. Клули также задаёт вопрос о том, будет ли университет нести юридическую и финансовую ответственность в случае, если учебные вирусы выберутся на свободу и нанесут значительный ущерб экономике.

Тем не менее, согласно информации издания «InformationWeek», университет прислал заявление, в котором говорится, что «после рассмотрения всех выдвинутых претензий факультет вычислительной техники университета Калгари принял решение продолжить введение в программу обучения курса “Компьютерные вирусы и вредоносные программы”, как и планировалось ранее». В специальном обращении подчёркивается, что компьютерные вирусы будут создаваться исключительно в лабораториях университета и не причинят вреда Интернет. В учебном заведении считают, что обучение написанию вирусов необходимо для подготовки специалистов, которые в будущем смогут успешно создавать антивирусные программы, поскольку «невозможно обучать методике борьбы с вирусами без знания того, как они создаются».

Университет сообщает, что студентам в рамках учебного курса будут прививать нравственность, законопослушность и, чтобы свести опасность распространения создаваемых вирусов к минимуму, предполагается полностью оградить все компьютеры, расположенные в учебной лаборатории, от внешнего мира и пресечь любую возможность унести написанные вирусы с собой. По окончании курса планируется очистить все жёсткие диски от вредоносных программ. «Интересно, а мозги студентов в конце курса они тоже собираются очистить?» – заметил руководитель научно-исследовательского центра Spire Security, занимающегося проблемами компьютерной безопасности Линдстрём. Кроме того, Линдстрём добавил: «Это очень смешно. Существует множество способов достичь того же уровня знаний и без обучения написанию деструктивных программ. Мы

же не проводим занятия по половому воспитанию, заставляя студентов заниматься сексом в аудиториях! Тактика и методика разрушения и защиты резко отличаются друг от друга. Наивно полагать, что создатель вирусов будет создавать хорошие антивирусные программы». Его позицию поддержали и многие другие специалисты по безопасности в области информационных технологий.

Интересно, чем закончатся такие эксперименты? Мы получим шестую группу вирусописателей? Или наоборот? Ну, что ж, ждать осталось недолго…

Как показывают приведённые выше примеры, в целом общественное мнение по отношению к авторам вирусов должно быть крайне негативным, хотя и могут быть определённые нюансы. Авторам компьютерных вирусов необходимо недвусмысленно дать понять, что их «труд» никогда не будет уважаемым ремеслом и никогда не будет оплачен обществом материально. Более того, в случае уличения в этой деятельности вирусописатель, в зависимости от последствий содеянного, может быть подвергнут наказанию в широком диапазоне законно применяемых мер: от крупного штрафа и административного наказания до наступления уголовной ответственности, сопряжённой с длительным тюремным заключением.

Со своей стороны авторам компьютерных вирусов, особенно относящих себя к «профессионалам», стоит задуматься о том, не слишком ли накладно для них подобное времяпрепровождение. Ведь для того, чтобы написать хорошо отлаженный компьютерный вирус и заложить в него оригинальные идеи, необходимо затратить довольно много сил и времени, причём гораздо больше, чем требуется для того, чтобы разобраться в вирусе и занести его в базу данных или даже написать специальный антивирус. Кроме того, настоящий талант, если он действительно существует, по крайней мере, бессмысленно растрачивать впустую и обладающему им в области программирования всегда можно найти для себя другое, более привлекательное и, в конце концов гораздо более доходное занятие.

Итак, вирусы могут быть разными – от просто навязчивых до ужасающе разрушительных, и об этом написано достаточно, а вот о самих создателях вирусов известно гораздо меньше и, в заключение нашего маленького исследования личности вирусописателя воспользуемся характеристикой, которую даёт им Сара Гордон.

Сара Гордон с 1992 года занимается исследованиями в области кибертерроризма и типологии создателей вирусов. В результате обобщения накопленных фактографических данных она попыталась представить портрет среднестатистического создателя вирусов. И вот что у неё получилось: «Обобщённый портрет выглядит следующим образом: представитель “сильного” пола в возрасте от 13 до 26 лет, в меру умный, либо обуреваемый желанием самоутвердиться и стать членом какого-либо сообщества, либо движимый местью, социально-политическими мотивами, желанием продемонстрировать слабость технологий, а то и просто любопытством. Такой “писатель”, как правило, создаёт вирусы не с целью сознательного причинения вреда, а чтобы “находиться на переднем крае технологий”, продвигая их вперёд. Имидж “продвинутого” программиста, давно уже прилепившийся к программистам вредоносных кодов во многом благодаря стараниям прессы, способствует романтизации этого занятия. Так что для того, чтобы покончить с ними и вирусами, возможно, нужно просто перестать считать создателей вирусов “крутыми” парнями».

Да будет так!

ПРИЛОЖЕНИЕ 3

ЧТО ЭТО ТАКОЕ – «ДИКИЙ» ВИРУС?

В настоящее время существуют десятки тысяч компьютерных вирусов, включая их многочисленные разновидности, штаммы. Вероятность «встречи» с большинством из них для пользователя крайне мала по причине их ничтожного распространения, и экземпляры этих вирусов можно найти только в коллекциях специалистов-вирусологов, специальных энциклопедиях компьютерных вирусов или специализированных базах данных фирм-разработчиков антивирусных средств; такие компьютерные вирусы в настоящее время принято обозначать собирательным именем «Zoo»[4].

Даже для квалифицированного специалиста-вирусолога было бы очень тяжёлой задачей составить исчерпывающий список компьютерных вирусов класса «Zoo», не говоря о том, чтобы без посторонней помощи и больших затрат времени предоставить подробную информацию по поводу того, чем они характерны и как действуют. Многие пользователи лишь где-то, когда-то, что-то и от кого-то слышали об этих вирусах. Более того, когда с вирусом из числа «Zoo» вдруг сталкиваются специалисты какой-либо организации, им, как правило, приходится обращаться к поставщику используемых данной организацией антивирусных средств или начинаются длительные поиски в различных энциклопедиях компьютерных вирусов, чтобы получить хотя бы какую-нибудь информацию об этом редком, зачастую давным-давно

[4] Zoo (англ.) – зоопарк, «безопасные животные», живущие в клетке, под контролем, в отличие от «диких», живущих где угодно. В переносном смысле слова этот термин может быть переведён и употребим как «разношёрстная компания».

«вымершем», «ископаемом» вирусе, который уже не способен причинить какой-либо вред компьютерной системе или сети. Такое положение дел послужило первоначальным импульсом к тому, что исследователи, поставщики, разработчики и специалисты по испытаниям антивирусных средств постепенно начали концентрировать своё внимание на компьютерных вирусах, существующих в так называемом «диком виде»[5] и способных реально распространяться, инфицируя компьютерные системы.

Понятие «дикого» вируса[6] является очень важным и, пожалуй, одним из основополагающих.

Довольно долгое время результатами тестирования дееспособности антивирусного программного обеспечения являлись цифры, связанные с обнаружением компьютерных вирусов, относящихся к классу «Zoo». Но, совершенно очевидно, что такие испытания не могли стать надёжным показателем готовности конкретного антивирусного продукта к встрече с угрозой, исходящей от вирусов, реально действующих в данный момент в мире и наносящих ощутимый ущерб пользователям.

Можно получить два результата по итогам тестирования совокупности файлов, инфицированных вредоносными компьютерными программами. Первый результат может быть получен при помощи простого подсчёта того, какой антивирусный продукт выявляет больше инфицированных файлов, – в этом случае мы не получим информации относительно того, какой продукт наиболее успешно находит и уничтожает вирусы, которые известны как несущие действительную угрозу миру вычислительной техники. Второй результат, который будет говорить о действенности антивирусных продуктов, может быть получен только посредством подсчёта выявленных и удалённых вирусов, с которыми пользователь реально сталкивается, то есть как раз вирусов, встречающихся в «диком» виде.

---

[5] Real World Anti-Virus Reviews and Evaluations-the Current State of Affairs. Sarah Gordon and Richard Ford. Proceedings 19th National Information Systems Security Conference. Baltimore Maryland. October 1996.
По-английски термин «в диком виде» передаётся при помощи следующего словосочетания: «In the Wild».

[6] Термин «дикий» вирус (wild virus) в зарубежных и отечественных источниках сейчас употребляется в качестве аналога и наравне с термином «в диком виде».

Для того чтобы несколько глубже вникнуть в предмет, вкратце рассмотрим историю возникновения и принятия компьютерным сообществом термина «в диком виде» или «дикий вирус».

Насколько можно судить из сопоставления сведений, содержащихся в зарубежных источниках, затрагивающих рассматриваемую нами и смежную тематику в области компьютерной вирусологии, общепринятое сейчас выражение «в диком виде» было впервые неформально использовано в 1990 году специалистом Исследовательского центра Ватсона фирмы IBM Дэйвом Чессом для описания реальных происшествий, происходящих в мире с участием компьютерных вирусов[7]. Несколько позже Алан Соломон вспоминает и употребляет этот термин в процессе своего общения с коллегами из Великобритании[8]. Затем, летом 1992 года, термин «в диком виде» неожиданно появляется в публикации одного из специальных периодических изданий («Virus Bulletin»), в тексте сообщения от Роджера Риордана[9], где он говорит об инцидентах с участием компьютерных вирусов. В сентябре 1992 года данный термин, уже официально, употребляется в докладе Джеффри Кефарта и Стива Уайта на международной конференции, проходившей в г. Эдинбург (Шотландия)[10], в котором наглядно продемонстрировали, что лишь небольшая часть от общего количества компьютерных вирусов «несёт ответственность за подавляющее большинство реальных инцидентов, связанных с вирусами, и это как раз и есть компьютерные вирусы, которые существуют в диком виде».

Примерно тогда же для оценки воздействия существующих вирусов на компьютерные системы редакция журнала «Virus Bulletin» провёла прикладное исследование свойств «диких» вирусов с использованием подборки образцов, специально разработанных специалистами. Основные характеристики вирусов, включённых в эту подборку, были смоделированы с

[7] David Chess. Private e-mail conversation.
[8] Alan Solomon. Private e-mail conversation.
[9] Roger Riordan. Private e-mail conversation.
[10] Measuring Computer Virus Prevalence. Jeffrey O. Kephart and Steve R. White. Proceedings of the Second International Virus Bulletin Conference. Edinburgh, Scotland, September 2–3, 1992.

учётом совокупности сведений, полученных в итоге отбора и сопоставления фактической информации о вирусах, содержащейся в отчётах, которые присылались в «Virus Bulletin». Причём, данные отчётов перепроверялись компетентными компьютерными вирусологами с той целью, чтобы в подборку не попали вирусы, которые пусть и существовали, но не получили реального распространения в мире – вирусы класса «Zoo». Таким образом, было проведено не чисто теоретическое исследование, а напротив, впервые на практике был осуществлён успешный эксперимент, в ходе которого из последующего рассмотрения сознательно были исключены вирусы, относящиеся к классу «Zoo». Рассмотренный подход к классификации вирусов на практике подтвердил и то, что именно неуклонный рост количества компьютерных вирусов «в диком виде» сопровождается ростом реальной угрозы с их стороны компьютерным системам. Иными словами, вирусы, относящиеся к классу «Zoo», не оказывают какого-либо заметного влияния на общий уровень угрозы компьютерным системам со стороны вредоносных компьютерных программ.

Вследствие описанных выше событий, подавляющее большинство компьютерных вирусов перестало рассматриваться специалистами в качестве действительной угрозы компьютерным системам. Однако вирусы класса «Zoo» оставались весьма распространёнными и в рекламных целях продолжали учитываться разработчиками антивирусного программного обеспечения[11] при продвижении своей продукции на рынок, поскольку обычные пользователи при приобретении таких средств ещё достаточно долго по инерции ориентировались на то антивирусное программное обеспечение, которое демонстрировало им наиболее высокие количественные показатели в отношении способности обнаруживать вирусы, включая и крайне «экзотические» вирусы, принадлежащие к классу «Zoo».

[11] Real World Anti-Virus Reviews and Evaluations-the Current State of Affairs. Sarah Gordon and Richard Ford. Proceedings 19th National Information Systems Security Conference. Baltimore Maryland. October 1996.

В связи с новым подходом к классификации компьютерных вирусов возникли некоторые достаточно очевидные проблемы. Например, поскольку количество вирусов «в диком виде» продолжало расти, появилась необходимость разработки концепции, а затем, на её основании, и документа под названием «The WildList»[12], предложенного Джо Уэллсом.

В основе его идеи лежала концепция вируса «в диком виде», использованная сначала «Virus Bulletin» и, позже, воспринятая всем международным компьютерным сообществом. Уэллс рассортировал отчёты о вирусных инцидентах, полученные от компьютерных вирусологов со всех континентов. Любой компьютерный вирус, упоминание о котором встречалось в двух или более отчётах, стал считаться существующем в «диком» виде. В некоторых случаях вирус упоминался в отчёте, полученном только от одного компьютерного вирусолога, и такие вирусы были помещены Уэллсом в отдельный раздел «The WildList». Этот, дополнительный, раздел перечня позволяет прогнозировать, какие компьютерные вирусы в ближайшем будущем могут попасть в основной раздел «The WildList», а какие, скорее всего, покинут его, а также помогает специалистам отслеживать тенденции и развитие ситуации с компьютерными вирусами в большинстве регионов мира[13].

Однако, признание и введение в широкий обиход «The WildList» повлекло за собой другие проблемы. Например, отставание содержания этого перечня от реальной ситуации с распространённостью вирусов «в диком виде». Временная задержка выхода публикаций «The WildList» по отношению к моменту обнаружения вирусов (то есть, наличие временного лага) является наиболее частой причиной выражения неудовольствия и аргументом против использования этого перечня в качестве полного множества вирусов, которые существуют на данный момент «в диком виде».

---

[12] «The WildList» (англ.) – «Перечень существующих «в диком виде» компьютерных вирусов». Ведётся, начиная с июля 1993 года.
Пример этого документа приведён в следующем Приложении.

[13] Со временем «The WildList» был дополнен таблицей плотности распределения компьютерных вирусов, см. Приложение 2.

Такое запаздывание вызвано тем, что отчёты о вирусных инцидентах собираются от десятков респондентов со всего мира, которые, в свою очередь, составляют собственные перечни «диких» вирусов, подготавливая их на основе сообщений пользователей, обращающихся в службы технической поддержки компаний-производителей антивирусных средств. На практике вирус может попасть в «The WildList» через месяц или даже два месяца после того, как он был впервые обнаружен конкретным пользователем. В настоящее время для совершенствования этой процедуры трудно предложить кардинальное решение, хотя в данном случае может помочь, например, применение методов оптимизации электронного документооборота, которые способны обеспечить автоматизацию процесса составления и распространения «The WildList», а также предполагают формализацию и унификацию отчётных форм для заполнения участниками этого проекта.

Суммируя сказанное выше в отношении истории возникновения термина «в диком виде» и того, как это понятие трансформировалось в идею составления «The WildList», следует подчеркнуть, что де-факто этот перечень стал общепринятым стандартом, который берётся во внимание в ходе разработки, например, антивирусных сервисных программ для выявления вирусов, существующих «в диком виде». То есть несмотря на отдельные недочёты, следует признать, что «The WildList» представляет собой наиболее успешную попытку каталогизации тех компьютерных вирусов, которые действительно распространены в мире, хотя определение «в диком виде» вряд ли можно считать идеальным. Между прочим, показатель эффективности обнаружения компьютерных вирусов «в диком виде» является частью системы критериев, предъявляемых, например, Национальной ассоциацией по компьютерной безопасности (National Computer Security Association – NCSA) США при сертификации антивирусных продуктов.

Вместе с тем, отметим следующее обстоятельство. Важность быстрого реагирования фирмы-разработчика на появление новых вирусов «в диком виде», ускоренной подготовки данных для «The WildList» и, естественно, своевременного обновления антивирусных продуктов сейчас никто не оспаривает. Однако и оповещение о появлении нового «дикого» вируса посредством использования электронной почты или при помощи использования других сервисных возможностей Интернет, автоматическая рассылка сигнатур вируса всем фирмам-разработчикам антивирусного программного обеспечения, не гарантируют оказания своевременной и действенной помощи конкретному конечному пользователю. Это объясняется тем обстоятельством, что в процессе передачи данных между компьютерными системами задействуется всё больше различных технологических решений, используется всё больше различных программно-аппаратных платформ и комплексов, с учётом особенностей которых затем и применяются те или иные меры по борьбе с вирусами в части их обнаружения, локализации и уничтожения, а также последующего восстановления систем.

Таким образом, представляется достаточно очевидным, что, вероятнее всего, действительно эффективное решение проблемы компьютерных вирусов лежит в плоскости масштабного применения новых антивирусных технологий, а также технических приёмов и подходов, например, изначальной иммунизации компьютерных систем при помощи современных, легко модифицируемых по мере необходимости аппаратно-программных средств, устанавливаемых производителем компьютера и способных изначально обеспечить пользователю необходимую защиту его системы от вредоносных компьютерных программ, в том числе и компьютерных вирусов «в диком виде».

Причём «The WildList» и подобные ему документы, в этом случае, по прежнему следует расценивать как важнейший инструмент, позволяющий повысить информированность компьютерного и бизнес сообществ,

государственных структур, а также отдельных пользователей в области реальных угроз их компьютерным системам со стороны вредоносных компьютерных программ, в том числе и компьютерных вирусов.

ПРИЛОЖЕНИЕ 4

ПЕРЕЧЕНЬ
МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИИ «THE WILDLIST»

Данный документ является обобщённым перечнем компьютерных вирусов существовавших в «диком» виде по состоянию на январь 2004 года.

Перечень составлен по данным отчётов, предоставленных в Международную организацию WildList[14] (WildList Organization International) 76 профессиональными компьютерными вирусологами или их группами со всего мира.

Код	Участник	Регион	Организация	Продукт
Ac	Алан Канди	Новая Зеландия	Applied Insight	–
Ad	Алан Дайер	Гонг Конг	Yui Kee Co. Ltd.	F-Prot

[14] Организация официально учреждена в апреле 1996 года Джо Уэллсом и Сарой Гордон, и её главное предназначение определяется как: «выполнение целевой задачи по предоставлению точной, своевременной и всеобъемлющей информации о компьютерных вирусах «в диком виде» пользователям и разработчикам антивирусных продуктов». «The WildList» представляет собой подготавливаемый организацией на регулярной основе список компьютерных вирусов обнаруженных «в диком виде» и переданных в организацию добровольными участниками проекта. Эти добровольцы представляют собой высококвалифицированных специалистов в области компьютерной вирусологии и разработки антивирусных средств, которые работают «респондентами» в своё свободное время. В WildList Organization International функционирует совет директоров, который состоит из пяти членов организации. Кроме того, в организации действует, например, «защитник прав пользователей» (User Ombudsman) – Ричард Форд, который рассматривает запросы и пожелания пользователей и сообщает о них совету директоров организации. Форд за годы работы в исследовательском центре Томаса Дж. Ватсона фирмы IBM и, главным образом, в качестве редактора «Virus Bulletin» накопил большой практический опыт и хорошо осведомлён о потребностях как пользователей и производителей, так и поставщиков антивирусных продуктов. Консультантами совета директоров являются Ник Фитцджеральд, который является координатором дайджеста «Virus-L» и Роджер Томпсон, работающий в ICSA руководителем подразделения в области вредоносных кодов. Бывший редактор «Virus Bulletin» Фитцджеральд имеет обширный опыт в тестировании антивирусного программного обеспечения.

Код	Участник	Регион	Организация	Продукт
Ae	Амир Эльбаз	Израиль	eAladdin	eSafe Protect
Ak	Ахмад Кашур	Сирия	CompuKashoor	Dr Solomon's
Al	Эндрю Ли	Великобритания	Team Anti-Virus	–
Am	Андреас Маркс	Германия	Univ. of Magdeburg	–
Ao	Энду Чианчиотто	США	Symantec	–
As	Алекс Шипп	Великобритания	MessageLabs	StarScan
Ay	Алиса Майерс	США	McAfee (US)	VirusScan
Bd	Богдан Думитру	Румыния	Softwin SRL	–
Cb	Карл Бреттвилль	Норвегия	Norman ASA	NVC
Cr	Костин Райу	Румыния	Kaspersky Labs	KAV
Cs	Кристиан Шмид	Австрия	DataPROT Linz	F-Prot
Dp	Дэвид Филипс	Великобритания	Open University	–
Dr	Дэвид Ротенберг	Бразилия	Maple Informatica	–
Ei	Эдди Виллемс	Европейское Сообщество	EICAR	–

Код	Участник	Регион	Организация	Продукт
Ek	Евгений Касперский	Россия	Kaspersky Labs	KAV
Ew	Эдди Виллемс	Бельгия/Люксембург	Data Alert Int'l	VirusScan
Fp	Франсуа Паже	Франция	McAfee (France)	VirusScan
Gb	Джеральд Баттен	Канада	Independent	–
Gr	Greg Romania	США	ICSA Labs	–
Is	Роберт Фримэн	США	ISS	–
Jd	Жуст де Рэймекер	Португалия	RSVP	–
Jg	Жорди Гарсия	Испания	SATINFO	VirusScan
Jh	Джо Хартман	США	Trend Micro	PC-cillin
Jj	Джонг Пурисима	–	Trend Micro	PC-cillin
Jk	Джимми Куо	США	McAfee (Independent)	–
Jm	Хосе Мартинес	Перу	HackSoft S.R.Ltda	TH AV
Jp	Джозеф Пичлмайер	Австрия	Ikarus Software	–
Jy	Джэймс Янеза	–	Trend Micro	PC-cillin
Kb	Кеннет Бэчтел	США	Team Anti-Virus	–
Kd	К. Т. Дэвис	Индия	Pioneer Micro	Vaxine

Код	Участник	Регион	Организация	Продукт
Ls	Люка Самбуччи	Италия	Min. Comunicazioni	–
Ma	Мэттью Хэм	Великобритания	Virus Bulletin	–
Mh	Микко Хиппонен	Финляндия	F-Secure Corp.	F-Secure
Mo	Мартин Овертон	Великобритания	Independent	–
Ms	Марек Селл	Польша	Marek Sell, Ltd.	MkS_vir
Mt	Мирослав Трнка	Словакия	Eset	NOD32
Mx	Михаэль Хи	Канада/США	Fortinet, Inc.	FortiGate
Oz	Якуб Камински	Австралия	Computer Associates	VET
Pb	Павел Баудис	Чехия	Avast!	ALWIL Software
Ph	Пер Хеллквист	Швеция	Symantec	NAV
Pm	Паоло Монти	Италия	Future Time	NOD32
Pr	Петер Радатти	США	CyberSoft, Inc.	Vfind
Pt	Петер Теобальд	Индия	IT Secure Software	VirusScan
Ra	Рубен Ариас	Аргентина	RALP	Integ Master
Rf	Ричард Фоули	Ирландия	Reflex Magnetics	TBAV
Rg	Рэй Глэс-	США	Tavisco Ltd.	Vi-Spy

Код	Участник	Регион	Организация	Продукт
	старший			
Rp	Ронни Пинеда	Филиппины	Mannasoft Corp.	VirusScan
Rv	Робеот Виберт	Канада	Independent	–
Rz	Ричард Звиненберг	Нидерланды	Norman Data Defense	NVC
Sa	Сигги Стефниссон	Исландия	FRISK Software	F-Prot
Sf	Сноре Фагерлянд	Норвегия	Norman ASA	NVC
Sh	Ша-Ли Хсих	США	Computer Associates	Inoculate IT
Sj	Санжай Каткар	Индия	Cat Computer Services Quick Heal	–
Sk	Сеок-Чул Квон	Корея	HAURI	ViRobot
Sm	Сейджи Мукарами	Япония	JCSR	–
So	СиХаенг Чо	Южная Корея	Ahnlab, Inc.	V3.
Sr	Субраманья Рао	Индия	Proland Software	Protector Plus
Ss	Сзилард Стэнж	Венгрия	VirusBuster Ltd.	Virus Buster
St	Стюарт Тэйлор	Великобритания	Sophos Plc.	Sweep
Ta	Тьарк Ауэрбах	Германия	H+BEDV	AntiVir

Код	Участник	Регион	Организация	Продукт
			GmbH	
Tc	Цветан Чальавски	США	Command Software	F-Prot Pro
Td	Торальв Дирро	Германия	U of Hamburg	VirusScan
Ti	Торбен Иммих	Дания	Swanholm Distrib	NAV
Tm	Тарас Маливанчук	Израиль	iRiS Software	AntiVirus Plus
Wl	Организация «WildList»	–	Организация «WildList»	–
Ws	Вольфганг Стиллер	США	Stiller Research	Integ Master
Xc	Хабьер Казалис	Испания	Panda Software	Panda
Za	Дэрил Песели	По всему миру	Microsoft Corporation	–
Zb	Джеймс Вольф	США	независимый эксперт	–
Zv	Корпоративная группа	–	–	–
Zw	Корпоративная группа	–	–	–
Zx	Корпоративная группа	–	–	–
Zy	Корпоративная группа	–	–	–

Код	Участник	Регион	Организация	Продукт
Zz	Корпоративная группа	–	–	–

В основе отчётов респондентов (участников проекта) лежат реальные инциденты с участием компьютерных вирусов, причём образцы вирусов получены или выявлены непосредственно респондентами. Непроверенные сведения о вирусах в отчёты не включаются. Некоторые из вредоносных программ, включённых в этот перечень, могут не вполне соответствовать традиционному определению компьютерного вируса. Однако эти программы также как и «традиционные» компьютерные вирусы распространяются среди различных групп пользователей и несут им угрозу, поэтому они и включаются в перечни «The WildList». Кроме того, настоящий документ представляет собой некое обобщение с нарастающим итогом, а не просто отчёт о том, какие вирусы были выявлены на протяжении прошедшего месяца. Получаемые ежемесячно от большинства респондентов данные добавляются к прежним сведениям, и на основе информации от этих же респондентов принимается решение об удалении вирусов из перечня. Данный перечень нельзя рассматривать и в качестве списка «наиболее распространённых вирусов», хотя впоследствии многие из включённых в него вирусов, в силу своей специфичности, становятся таковыми.

Таким образом, включение вируса в перечень свидетельствует о том, что он принадлежит к множеству реально действующих на тот момент, то есть «диких» вирусов.

В основной список «The WildList» включаются вирусы, которые неоднократно упоминаются в отчётах участников из разных регионов мира. Иными словами, компьютерный вирус заносится в этот список в случае выполнения следующего условия: проверенная информация о существовании

данного компьютерного вируса «в диком виде» поступила как минимум от двух респондентов, проживающих в различных регионах мира.

Компьютерный вирус, сообщение о существовании которого поступило только от одного респондента, включается в дополнительный список.

После исключения вируса из основного списка «The WildList» он иногда, вследствие произошедшего рецидива, вновь включается в него. Такие компьютерные вирусы помечаются символом «***». Вирусы, впервые включённые в основной список в отчётном месяце, отмечаются символом плюс (+).

Основной список

Название вируса	**Другое(ие) имя (имена)**	**Дата**	**Код участника**
AntiCMOS.A	Lenart	1/95	Ph Sj So Zz
AntiEXE.A	D3, New Bug	9/94	Fp Sj Zz
BAT/Mumu.A		6/03	Am Ph Sh So St Tm Zz
Bleah	Bleah.D	2/02ё	Fp Jg Sk So
Form.A	Form 18	7/94	Ph Zz
JS/Kak.A-m		2/00	Ao As Dp Fp Jd Jw Mo Oz Pb Ph Sj Zv Zz
NYB.A	B1	7/94	Sj So Zz
O97M/Tristate.C	Crown.B	4/99	As Fp Jw Kd So Zv
Ripper	Jack Ripper	4/02	Ew Sk So
VBS/Haptime.	Help	6/01	Ao As Ay Fp Jm Jw Ms Ph Sj Sk So

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
A-mm			Ta Zv Zy Zz
VBS/LoveLetter.A-mm	BugFix	5/00	Ao As Ei Ew Jd Jw Ph Sk Sm So Zv Zz
VBS/LoveLetter.AS-mm	Plan.A	10/00	Ao As Fp Ms Ph So Zv
VBS/LoveLetter.C-mm		10/00	Ao As So
VBS/Netlog.A	Network	3/00	Sm So
VBS/Redlof.A-m		10/02	Ao As Dp Ek Fp Jg Jm Jp Jw Jy Kd Ms Mt Ph Sf Sj Sk Sm So St Ta Tm Wl Zv Zy Zz
+VBS/Sling		1/04	Ao Mt
VBS/Stages.A-mm	ShellScrap	7/00	Ao As Jd Ph
VBS/Tam.A-m		2/01	Ao As Fp Ph
VBS/VBSWG.AQ-mm		7/02	As Sk
VBS/VBSWG.J-mm	Anna K	2/01	Ao As Ei Ew
VBS/VBSWG.K-mm	NeueTarife SST	2/01	Ei Ew
VBS/VBSWG.X-mm	HomePage, SST	5/01	Ao As Ew Jd Ph
W32/Acebot	Newbiero	6/02	Ao So

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
W32/Aliz.A-mm		11/01	Ao As Ph
W32/Aplore.A-mm	Aphex	6/02	Ao As Zz
W32/Apost.A-mm		10/01	Ao As Zz
W32/BadTrans.A-mm	13312	5/01	Al Ao As Dp Fp Gr Jd Kd Ph Sf Sg Sr St Tm Zz
W32/BadTrans.B-mm	29020	11/01	Al Am Ao As Dp Ei Ek Ew Fp Jd Mo Oz Pb Ph Sf Sj Sm Sr St Zv
+W32/Bagle.A-mm		1/04	As Is Jg Jy Sj So Ta Zy
W32/Beast.A	W95/HLLP.41472	6/03	Ao Tm
W32/Benjamin.A-mm		6/02	Ao Ms
W32/Bibrog.C-mm		4/03	Ac Sh St Tm
W32/Blaster.A		9/03	Al Ay Dp Ei Ew Jg Jw Jy Ms Mt Ph Pm Rz Sj Sk So St Xc Zv
W32/Blaster.B		9/03	Dp Kd Ph Rz Sk So Xc
W32/Blaster.C		9/03	Sj Sk So Xc
W32/Blaster.E		9/03	Al Mt Ph So St Xc
W32/BleBla.B-	Verona.B	12/00	Ao As Kd Sj Zz

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
mm			
W32/Braid.A-mm		11/02	Am As Ek Fp Jd Jm Jp Kd Ms Mt Oz Ph Sk So St Zv Zy Zz
W32/BugBear.A-mm		10/02	Al Am Ao As Ay Dp Ei Ek Ew Fp Gr Jd Jm Jp Jw Ls Mo Ms Mt Oz Pb Ph Rv Rz Sf Sg Sj Sk Sm So Sr Ss St Tc Xc Zv Zz
W32/BugBear.B-mm		6/03Al	Am Ay Dp Ei Ek Ew Fp Is Jg Jk Ls Mo Ms Mt Oz Pb Ph Pm Rz Sf Sg Sh Sj Sk So Sr St Tm Wl Xc Zy Zz
W32/Cervivec.A		4/02	Ao As
W32/Choke.A		7/01	Ao Ei
+W32/Cissi-mm		1/04	Ao So Ta
W32/Colevo-mm		9/03	Ay So Ta
+W32/Darby.F-mm		1/04	As Mo
+W32/Darker		1/04	Ao Ta
W32/Datom.A		9/02	Ao Ek Fp Ms Oz Pm Sk So St
W32/Deborm.Q		4/03	Ac Mo Oz Ph Sh St Tm
W32/Deborm.R		4/03	Ac Jw Ph St Tm
W32/Deloder		5/03	Am Ao Mt Pm Sk Sm So St Tm

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
W32/Dumaru.A-mm		9/03	Al As Ay Dp Is Jg Jk Jp Mo Mt Oz Pb Ph Rz Sg Sj Sk So Ss St Wl Zv Zy Zz
W32/Dumaru.C-mm		10/03	As Ph So Ta
W32/Dumaru.H-mm		10/03	Jg Jp Kd Pb Ph So Zy Zz
+W32/Dumaru.Y-mm		1/04	Am As Is Mo Ta Zy
+W32/Dumaru.Z-mm		1/04	As Ta Zy
W32/Elkern.A	WQK.A	12/01	Ao As Kd Ph Sk So
W32/Elkern.B	WQK.B	2/02	Ei Ew Kd
W32/Elkern.C	WQK.C	5/02	Al Ao As Ay Ei Ek Ew Jd Jg Jm Jw Kd Ph Rv Sh Sj Sk So St Tc Tm Zy Zz
W32/Fizzer-mm		5/03	Ac Al Am Dp Fp Jg Jw Kd Mt Oz Ph Rz Sg Sh Sj Sk Sm So Sr Ss St Ta Tc Tm Zv Zy Zz
W32/Frethem.F-mm		7/02	Kd Sm So Zz
W32/Frethem.K-mm		1/03	Kd Sk
W32/Frethem.L-mm		9/02	Am Ao Ph
W32/Funlove.4		12/99	Ao As Ay Ei Ew Fp Jg Jj Jm Jw Jy Kd

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
099			Mo Ms Mt Oz Ph Rv Sf Sh Sj Sk Sm So Sr St Wl Xc Zv Zy Zz
W32/Ganda-mm		4/03	Ac Al Am As Ay Dp Ei Ek Ew Fp Is Ls Mo Mt Pb Ph Pm Sf Sg Sj Sk Sm So Sr Ss St Tm Xc Zv Zy Zz
W32/Gant.B-mm		6/03	Ac Ta
W32/Gibe.A-mm		3/02	Ao As Dp Jd Jw Mo Ms Oz Ph Sg Sj Sm So St Zv
W32/Gibe.B-mm		3/03	Al Am As Ay Fp Mt Ph Rz Sf Sg Sh Ss St Wl Zv Zy Zz
W32/Gokar.A-mm		1/02	As Mo
W32/Goner.A-mm		12/01	Ao As Ei Fp Jd Jg Jy Ph So St Zv Zz
W32/Gop.A-mm	Invery.A	2/02	As Dp
W32/Hai.A		10/01	Ao Oz So
W32/Hantaner		1/03	Dp Jg Ms Ph Rz So St Zz
W32/HiGuy.A-mm	Tettona	7/02	Ao As Dp Fp Ph St Zz
W32/Holar.D-mm		4/03	Ac St
W32/Holar.H-		6/03	As Ay Ph St Ta Tm Zv

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
mm			
W32/Hybris.A-mm	Hybris.22528 -mm	1/01	Jw Ms Ph Sk So
W32/Hybris.B-mm	Hybris.23040-mm	12/00	Al Am Ao As Ay Dp Ei Ek Ew Fp Is Jd Mo Oz Pb Ph Sm Sr Ss St Zz
W32/Hybris.C-mm		12/00	As Dp Ek Ph St
W32/Hybris.D-mm	Hybris.25088-mm	1/01	Am Dp Ei Ek Fp Ph Sj St
W32/Inmota		10/03	Jg So
W32/Israz-mm		9/03	Ao So Sr
W32/Jeefo		7/03	Ay Jg Ms Sj So St Tm
+W32/Jitux		1/04	Ao Ta
W32/Klez.A-mm		12/01	Ao Jg Kd Sk So St
W32/Klez.E-mm		2/02	Al Am Ao Dp Ei Ek Ew Fp Jd Jm Jp Kd Mo Ms Mt Pb Ph Rv Sf Sj Sk So Sr Ss St Zv Zy Zz
W32/Klez.G-mm		3/02	Ei Pr Sk So St
W32/Klez.H-mm		5/02	Al Am Ao As Ay Dp Dr Ei Ek Ew Fp Gr Is Jd Jg Jj Jk Jm Jp Jw Jy Kd Mo Ms Mt Oz Pb Ph Pm Rz Sf Sg Sh Sj Sk Sm So Sr Ss St Tc Wl Xc Zv Zy Zz

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
W32/Kriz.4050		11/00	Ao As Kd Mo Ms Sj Sk So
W32/Lirva.A-mm		1/03	Am Ay Ei Ek Ew Fp Gr Jp Kd Mo Ms Mt Oz Ph Pm Sf Sg Sj Sk Sm So Ss St Xc Zv Zy Zz
W32/Lirva.C-mm		1/03	Ay Ek Jd Jp Mo Ms Mt Oz Ph Pm Sf So Ss St Zy Zz
W32/Lovelorn-mm		11/03	Is Ph Sj So Zy
+W32/Lovgate.A-m		1/04	St Ta
W32/Lovgate.B-m		5/03	So St
W32/Lovgate.C-m		3/03	Ay Fp Kd Oz Rv Rz Sh Sj So Tm Zv Zz
+W32/Lovgate.E-mm		1/04	As Ta
W32/Lovgate.F-m		4/03	Ac Ay Fp Jw Kd Oz Ph Sf Sh Sj Sk So Sr Ss St Tm Zz
W32/Lovgate.G-m		4/03	Am As Pm Rz Sj Sk So Ss Tm Zv Zy Zz
W32/Lovgate.I-m		6/03	Ac Sj So St
W32/Lovgate.J-m		6/03	Sk Ta

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
W32/Lovgate.K-m		6/03	Sk So Ta
W32/Lovgate.L-m		6/03	Ac As Ph Sk So St Ta Tm Zz
W32/Magistr.A-mm	Disembowler	4/01	Am Ao As Ay Dp Ei Ek Ew Fp Gr Kd Mo Ms Oz Pb Ph Sf Sg Sk Sm Ss St Tc Zy Zz
W32/Magistr.B-mm		10/01	Al Am Ay Dp Ei Ew Fp Jd Jw Jy Kd Mo Ms Oz Ph Sf Sg Sj Sk So Ss St Tc Zv Zy Zz
W32/Magold.A-mm		6/03	As Ss St Ta
W32/Magold.E-mm		7/03	As Ph St Ta
W32/Mapson.A-mm		7/03	Ao Ay Jg Oz Ph Sf So St Xc Zy
W32/Melare-mm		6/03	Ac Sj St Ta
W32/Mimail.A-mm		9/03	Al Ay Dp Fp Is Jg Jp Jw Jy Kd Mo Ms Mt Pb Ph Pm Rz Sg Sj Sk So Ss St Ta Zv Zy Zz
W32/Mimail.C-mm		10/03	Al Fp Is Jg Mo Mt Oz Pb Ph Pm Sk So Sr Ss St Wl Xc Zy
W32/Mimail.E-mm		11/03	Al Ao As Fp Oz Pb Ph So

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
W32/Mimail.F-mm		11/03	Ao As Fp Mt Oz Pb Ph So Sr Zy
W32/Mimail.G-mm		10/03	Al Ao As Ay Fp Jg Jp Mo Mt Oz Pb Ph Pm Sk So Sr Ss Wl Zy
W32/Mimail.H-mm		11/03	Al Ao As Fp Is Jg Jp Oz Pb Ph Sj So Ss
W32/Mimail.I-mm		11/03	Al Ao Ay Is Jg Mo Mt Ph So Sr Ss Ta Wl Zy
W32/Mimail.J-mm		11/03	Al Ao As Is Jg Jp Mo Oz Ph Pm So Sr Wl Zy
+W32/Mimail.L-mm		1/04	Ao As Sr Ta
W32/Mimail.M-mm		12/03	Ao As Jg Mt Sj Sr Ta
+W32/Mimail.P-mm		1/04	As Is So
+W32/Mimail.Q-mm		1/04	As Sj Ta
+W32/Mimail.S-mm		1/04	So Ta
W32/Mofei.A		6/03	Ay Jw Sj Sk So St Tm Zz
W32/MTX-m	Apology, Matrix	9/00	Ao As Ei Ew Fp Is Jd Mo Ph Sk Sm So Zz
+W32/Mydoom		1/04	Am As Is Jg Jy Mo So Ta Xc Zy

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
.A-mm			
+W32/Mydoom .B-mm		1/04	As Jg Sj So Ta
W32/MyLife.A -mm	30720	4/02	As Zz
W32/MyLife.B-mm	7680	4/02	Ao As
W32/MyLife.M -mm		7/03	Ao Ay Ph Sr Tm Zy
W32/MyParty. A-mm		2/02	Ao Jd Ms Ph Sk So Zz
W32/Nachi		9/03	Al Ay Dp Ei Ew Jg Jw Jy Kd Mt Oz Ph Pm Rz Sj Sk So St Xc Zy Zz
W32/Navidad. A-m	Navidad	11/00	Ao As Ei Ew Sj
W32/Navidad.B -m	Emanuel	1/01	Ei Ew
W32/Navidad.E -m		5/03	As Sk
W32/Nicehello-mm		4/03	Ac Ay Rz Xc
W32/Nimda.A-mm		10/01	Am Ao As Ei Fp Gr Jd Jw Jy Kd Mo Ms Oz Pb Ph Pr Rv Sk Sm So St Wl Za Zz

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
W32/Nimda.E-mm		11/01	Ao As Ei Ek Fp Jm Kd Mo Oz Pb Ph Sg Sj Sk So Ta Tm
W32/Onamu.A-mm		5/02	As Ph Zz
W32/Opaserv.A		10/02	Am Ay Ek Jg Jw Kd Mo Ms Mt Oz Pb Ph Sj Sk Sm So St Tc Xc
W32/Opaserv.AA		10/03	Kd Mo Sj Ss
W32/Opaserv.AC		10/03	Ay Jg Mo Ss
W32/Opaserv.AD		10/03	Ay Mo
W32/Opaserv.AE		10/03	Ay Mo
W32/Opaserv.AH		12/03	Jg Mo Ta
W32/Opaserv.B		10/02	Am Ay Kd Mo Ms Ph Sj Sk So Ss St
W32/Opaserv.C		3/03	Jg Mo Mt So St
W32/Opaserv.D		10/02	Ay Kd Mo Mt Oz Ph Sj Sk So Ss St
W32/Opaserv.E		11/02	Am Ay Jg Kd Mo Mt Oz Ph Sj Sk So St Xc
W32/Opaserv.F		1/03	Am Fp Mo Mt Sk So St Tm
W32/Opaserv.G		3/03	Am Mo Sj Sk St
W32/Opaserv.H		11/03	Mo St

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
W32/Opaserv.I		11/02	Am Ay Fp Mo Mt Sk So St Tm
W32/Opaserv.K		12/02	Am Ay Fp Jg Kd Mo Mt Oz Pm Sj Sk So Sr Ta Tm
W32/Opaserv.L		4/03	Mo So St
W32/Opaserv.M		1/03	Mo Sj Sk St
W32/Opaserv.P		9/03	Mo Ph Pm So
W32/Opaserv.Q		2/03	Mo So St
W32/Opaserv.U		6/03	Mo St
W32/Opaserv.W		5/03	Mo So
W32/Oror.B-mm		12/02	As Ph Sj Sr St
W32/Oror.Y-mm		3/03	Jw Mt Sj St
W32/Parite.A		12/02	Is Mo Mt Ph Sf Sj Sk So St Zy
W32/Parite.B		3/03	Fp Is Jg Jp Kd Ms Mt Ph Sf Sk So St Xc Zy Zz
W32/PrettyPark.37376-mm		6/99	As Ph Zz
W32/Purol.B		7/03	St Ta
W32/Qaz		9/00	Am Ao Ew Jg Mt Rv So
W32/Randex.E		9/03	Pm Rz Sj So
+W32/Scold-		1/04	Ao As

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
mm			
W32/SirCam.A-mm		7/01	Al Ao As Ay Dp Ei Ew Fp Gr Jd Jw Jy Mo Ms Mt Oz Pb Ph Pr Rv Sf Sj Sk Sm So Sr Ss St Tc Zv Zz
W32/Ska.A-m	HAPPY99	3/99	Al Ao As Fp Ph Zy Zz
W32/Sober.A-mm		10/03	As Jg Mo Mt Oz Pb Ph Rz Sk Sm Sr St Zy Zz
+W32/Sober.B-mm		1/04	Ao As Sr Ta
W32/Sober.C-mm		12/03	Am Ao As Fp Is Jg Ls Mo Mt Ph Pm Sj Sr Ta Zy
W32/Sobig.A-mm		1/03	Al As Ay Dp Ei Ek Ew Fp Jd Jg Jj Jk Jp Jw Kd Mo Ms Mt Oz Pb Ph Pm Pr Rv Sf Sh Sj Sk Sm So Ss St Tc Tm Xc Zv Zy Zz
W32/Sobig.B-mm		6/03	Al Ek Jk Jp Kd Mo Ms Ph Pm Rz Sh Sk So Sr Ss St Ta Tm Zv
W32/Sobig.C-mm		6/03	Al Ay Ek Is Jk Jp Kd Mo Oz Ph Pm Rz Sf Sh So Sr Ta Tm Zv Zy
W32/Sobig.D-mm		6/03	Am Ay Ph Rz Sf So St Ta Tm Zv Zy
W32/Sobig.E-mm		7/03	Ay Ei Ew Fp Jk Jw Kd Mo Oz Ph Rz Sf Sj So Sr St Ta Tm Xc Zv Zy Zz
W32/Sobig.F-		9/03	Al As Ay Dp Ei Ew Fp Is Jg Jp Jw Mo

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
mm			Oz Pb Ph Pm Rz Sg Sj Sk So Ss St Xc Zy Zz
W32/Stator.A		9/02	Ao Ms
W32/Surnova.A	Supova	9/02	Ms Sk So
W32/Swen-mm		9/03	Al As Ay Ei Ew Fp Is Jg Jk Mo Ms Mt Oz Pb Ph Pm Rz Sg Sj Sk Sm So Sr Ss Wl Xc Zv Zy Zz
W32/Torvil-mm		10/03	As Fp Is Jg Mt Sj Sk So Zy
W32/Valla.B		6/03	Am Ay Jg Jp Mo Ph Sh Sk So Tm Zz
W32/Warpigs.B		9/03	Ao So St
W32/Winevar.A-mm		12/02	Ek Ms Sk So
W32/Winur.C		7/03	So St
W32/Yaha.A-mm	Lentin.A	4/02	Ao As Ek Jd So St
W32/Yaha.D-mm	Lentin.B	5/02	As Ms Zy
W32/Yaha.E-mm	Lentin.D	7/02	Al Am Ao As Dp Fp Jw Mo Oz Pb Ph Pr Rz Sf Ss St Zz
W32/Yaha.G-mm	Lentin.F	7/02	Al Ay Fp Gr Is Jd Jj Jp Jw Mo Mt Ph Rz Sm So Wl Zv Zy Zz
W32/Yaha.J-mm		1/03	So Zv

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
W32/Yaha.K-mm		1/03	Al Ay Ei Ew Fp Gr Is Kd Mo Mt Oz Ph Pr Rz Sh Sj Sk So Sr Ss St Xc Zv Zy Zz
W32/Yaha.L-mm		2/03	Oz Ph Sk So Sr St Tm Zv Zz
W32/Yaha.P-mm		4/03	Ac Ay Dp Fp Ms Mt Pb Ph Rz Sk Sr Ss St Zv Zz
W32/Yaha.Q-mm		4/03	Am Ph Sk Ss St
W32/Yaha.T-mm		7/03	Pb Rz Ta
W32/Yaha.U-mm		6/03	Ac Ay Ph Tm Zy
W95/Bodgy		2/03	Mo So Sr
W95/CIH.1003	CIH.A	8/98	Am Ay Ek Fp Jd Jg Jp Kd Mo Ms Mt Oz Pb Ph Sf Sk Sm So Sr Zz
W95/CIH.1019.A	1019, CIH.C	7/98	Ao Sj
W95/CIH.1049		1/03	As Dp Kd Ph So
W95/Dupator.1503		12/02	Ay Jg Jm Kd Mo Ms Mt Ph Pm Sj Sk Sm So Sr St Xc Zy
W95/Fono	El_Inca.17152	1/03	Mo Sk So
W95/Lorez.176		1/03	Kd Mo Ph Sk So

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
6			
W95/Lovesong.998		7/02	Mo Sk So
W95/Spaces.1445	Busm.1445	12/00	Ao As Ay Dp Fp Is Jg Jy Kd Mo Ms Ph Sj Sk Sm So Sr Ss St Zv Zy Zz
W95/TenRobot.B		6/03	Kd Mo Ph Sj So
W95/Weird.10240	Kuang.GR	7/00	Ao As Kd Mo Sk So
W95/Whog.878.B		1/03	Mo Ph Sj So
W97M/Chack.B		3/00	As Jw
W97M/Class.B		2/99	As Jw
W97M/Class.D		12/98	As Dp Ei Ew Jw Ph Zv Zy Zz
W97M/Class.Q		12/98	As Zv
W97M/ColdApe.A		12/98	As Fp Ph
W97M/Eight941.D	Eight	5/00	As Zv
W97M/Ekiam.A		3/03	Am Rz Zy
W97M/Ethan.A		2/99	Al As Ek Ew Fp Jw Ph Sm St Zv Zy Zz

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
W97M/Ethan.BE		3/00	Ao As
W97M/Groov.A		7/98	As Jw Zz
W97M/Groov.B		10/99	Ao As Jw
W97M/Hope.A		8/01	As Dp
W97M/Locale.A		9/99	As Zy
W97M/Marker.C	Spooky.C	4/99	Al Ao As Dp Ei Ew Fp Jd Jw Ph Sj St Zy
W97M/Marker.D		5/99	As Ph Sm Zy
W97M/Marker.O		8/99	Ao As Zy Zz
W97M/Melissa.A-mm	Maillissa	4/99	Ao As Fp Jw Ph Zv Zz
W97M/Myna.B		1/00	As Zz
W97M/Myna.C		3/00	As Jw
W97M/Odious.A		10/03	Ao As
W97M/Opey.A		3/00	As Sj
W97M/Panther.A		11/99	Ao As Ph Zv Zz

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
W97M/Pri.A		6/99	As Jw Zv
W97M/Proverb.A		5/00	As Ph
W97M/Smac.D	BDOC2X	5/00	Ao As Fp Zy
W97M/Story.A	Jack_Box	8/99	As Fp Jw Ph Zv
W97M/Thus.A	Thursday.A	9/99	Ao As Ek Ph Sj Zv Zz
W97M/Thus.C	Thursday	6/00	As Jw Zv
W97M/Thus.K		6/03	As Zy
W97M/Titch.D		9/00	Ao As Dp Fp
W97M/Title.A		6/03	As Fp
W97M/Twopey.H		7/03	As Rz
W97M/Verlor.A		1/00	Al As Fp Ph Zy
W97M/VMPCK1.BY		8/99	As Fp Ph Zy
W97M/VMPCK1.DD		2/01	As Fp Ph Zz
W97M/Wrench.E		7/00	Ao As Jw
WM/CAP.A		5/97	Ao As Fp Jw Ph Sj Zv Zz
WM/Concept.A	Prank Macro	12/96	As Jw Ph Zz
WM/CopyCap.	WM.Pac.A	7/98	Jw Zz

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
A			
WM/Npad.A	Jakarta	10/96	As Fp
WM/Wazzu.A	Wazzu	12/96	Jw Zv Zz
Wyx	Preboot	11/01	Fp Jg Kd Sj So Zz
X97M/Barisada.A		8/00	As Sk
X97M/Barisada.AG		6/03	Sk St
X97M/Barisada.B	X97M/HJB.B	9/00	As So
X97M/Divi.A	BASE5874	12/99	As Sk So
X97M/Divi.D		7/00	As Kd Sk So
X97M/Laroux.A		7/97	As Jw So Zv Zz
X97M/Laroux.DX		12/98	As So
X97M/Laroux.E		12/98	As Jw Sk Zz
X97M/Yawn.A		7/00	As Sk So
XF/Sic.L		10/03	As Ay
XM/Laroux.A		2/97	Sm So Zz
Итого вирусов в списке: 261			

Как уже говорилось, компьютерный вирус включается в приведённый ниже «Дополнительный список», если сообщение о его существовании поступило от одного респондента. Причём составляющие дополнительный список вирусы, как правило, попадают затем в основной список. Необходимо также подчеркнуть, что «Дополнительный список» больше тяготеет к отражению ситуации на региональном уровне. Например, компьютерный вирус часто появляющийся в отчётах одного из респондентов в качестве очень распространённого, тем не менее, не обнаруживается больше нигде в мире.

Удалённые в отчётном месяце из основного списка вирусы помечаются символом минус (–). Вирусы, впервые включённые в дополнительный список в отчётном месяце, помечаются символом плюс (+). После исключения вируса из дополнительного списка он, иногда, вновь включается в него. Такие компьютерные вирусы помечаются символом «***».

ДОПОЛНИТЕЛЬНЫЙ СПИСОК

Название вируса	**Другое (ие) имя (имена)**	**Дата**	**Код участника**	**Название вируса**	**Другое (ие) имя (имена)**	**Дата**	**Код участника**
Backformat.2000.A	Backform	3/03	Mt	W32/Tzet		10/03	Ao
BAT/Arica.B-mm		7/03	Ta	W32/Upering		10/03	Ao
Dodgy		11/97	So	W32/Veedna.C		6/03	Ta
Empire.Monkey.B	Monkey2	11/03	So	W32/Veedna.E		6/03	Ta
Hare.mp.7		5/02	So	W32/Vote.		5/03	So

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
786.A				D-mm			
+JS/Flea.B-m		1/04	Sj	W32/Warpigs.A		10/03	Ao
JS/Kak.AB-m		11/01	As	W32/Wohar		6/03	Ta
JS/Messenger		2/02	Ao	W32/Wukill.B-mm		11/03	Ao
Natas.mp.4744		5/02	So	+W32/Yaha.AA-mm		1/04	Fp
Neuroquila.mp.4544.A	Havoc, Wedding	6/02	Ao	W32/Yaha.AF-mm		11/03	Ao
NRLG.700.A		6/02	Ao	W32/Yaha.B-mm	Lentin.B	5/03	As
O97M/Tristate.I		7/00	As	W32/Yaha.C-mm	Lentin.C	4/03	As
One_Half.mp.3544.A	Dis, Free Love	10/95	Mt	W32/Yaha.M-mm		4/03	Sj
Sampo	Turbo, Wllop	1/95	Zz	+W32/Yaha.V-mm		1/04	Ta
VBS/Freelink-mm		10/99	Jd	+W32/Zezer-mm		1/04	So
VBS/Gaggl		5/03	Jd	W32/Zoher.	Sheer.	1/02	Ao

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
e-mm				A-mm	A		
VBS/Haptime.F-mm		1/03	As	W95/Bumble.1736		11/02	Mo
VBS/Love Letter.BJ-mm	7/01	Ao		W95/Ilmx		1/03	Mo
VBS/Love Letter.CI		6/02	Ao	W95/Marburg.8590	Marburg.A	2/03	Mo
VBS/Lubus.A-mm		1/02	Jm	W95/Plage-m	HLLW	7/00	As
+VBS/Redlof.C		1/04	Jy	W97M/Antimarc.A-mm		11/99	As
VBS/Sorry.C	Mcon.B, Pica	3/01	Ao	W97M/Assilem.G		3/02	As
VBS/Spam Brief-mm		6/03	Ta	W97M/Assilem.G		7/00	As
VBS/Sysnom-mm		6/03	Ta	W97M/Astia.C		1/00	As
VBS/Tiltel-mm		6/03	Ta	W97M/Astia.L		3/00	As
VBS/Zsyang-mm		6/03	Ta	W97M/Astia.U		5/00	As
W32/Agobot.F		3/03	So	W97M/Bablas.A		11/03	As

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
W32/Aimven		4/03	Ac	W97M/Bablas.BH		4/01	As
W32/Alcaul.G-mm		6/03	Ta	+W97M/Bablas.E		1/04	Jy
W32/Alcaul.I-mm		6/03	Ta	W97M/Bablas.K		3/00	As
W32/Anset.A-mm		11/01	As	W97M/Bablas.S		12/00	As
W32/Antiqfx.B		7/03	Tm	W97M/Bobo.B		7/02	As
+W32/Ardurk.G-mm		7/03	Ta	W97M/Bottra.C		12/02	As
W32/Axam.A-mm		3/03	St	W97M/Caligula.A		11/00	As
W32/Babybear-mm		10/03	Ao	W97M/Chack.CO		5/03	Rz
W32/BackZat.I-mm		7/03	Ta	W97M/Chack.G		7/02	As
W32/BackZat.J-mm		7/03	Ta	W97M/Class.AY		5/01	As
W32/BackZat.K-mm		7/03	Ta	W97M/Class.BV		11/99	As
W32/Bacterra		10/03	So	W97M/Class.ED		2/00	As

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
W32/Bandie		11/03	Ao	W97M/Class.EQ		4/01	As
W32/Benatic.B		6/03	Ta	W97M/Class.FT		6/03	Sk
W32/Bereb		11/03	Ao	W97M/Claud.A		3/00	As
W32/Bibrog.B-mm		4/03	Ac	W97M/Coke.22231.A		12/00	As
W32/Bibrog.D-mm		4/03	St	W97M/ColdApe.B		3/99	As
W32/Blare		11/03	As	W97M/Crono.C		6/03	Sk
W32/Blaxe		10/03	So	W97M/DB.A		5/00	As
W32/BleBla.A-mm	Verona.A	12/00	Kd	W97M/Ded.A		10/99	As
W32/Blueball.4147		5/03	Mo	W97M/Ded.B		1/00	As
W32/Cabanas		1/03	Mo	W97M/Ded.C		7/02	As
W32/Capside		11/03	Sj	W97M/Dest.J		12/02	As
+W32/Cayam-mm		1/04	Ta	W97M/Dimbed		6/03	Sk

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
W32/Chir.A-mm		10/02	Sj	W97M/Eight941.E		3/00	As
W32/Conut-mm		10/03	Ao	W97M/Eight941.F		12/00	As
W32/CTX	6886, 6886	2/02	Am	W97M/Eight941.U		3/02	As
W32/Cult		3/03	Ay	W97M/Eight941.Y		7/02	As
W32/Cult.C-mm		6/03	Zy	W97M/Ethan.AJ		6/03	As
W32/Cydog.C-mm		6/03	Ta	W97M/Ethan.AK		12/01	As
W32/Dammit.1537		6/03	So	W97M/Ethan.AT		10/99	As
W32/Danvee-mm		7/03	Ta	W97M/Ethan.BI	Ethan.D	3/00	As
W32/Darby.B-mm		11/03	As	W97M/Ethan.BR		2/00	As
W32/Darby.C-mm		11/03	As	W97M/Ethan.BW		2/00	As
W32/Darby.G-mm		11/03	As	W97M/Ethan.CC		5/00	As
W32/Deborm.Y		7/03	Rz	W97M/Ethan.CR		11/00	As

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
W32/Demig.16354		10/03	Mo	W97M/Ethan.D		6/00	As
W32/Demiurg		5/03	As	W97M/Ethan.ER		6/03	Tc
W32/Druagz		6/03	Ta	W97M/Ethan.P		2/00	As
W32/Duksten.H-mm		1/03	As	W97M/Ethan.Q		9/99	As
W32/Duksten.M-mm		3/03	Jw	W97M/FF.A	Lys.H	7/02	As
W32/Dumaru.E-mm		10/03	So	W97M/FF.E		11/00	As
W32/Dumaru.G-mm		11/03	Sj	W97M/Flop.A		8/01	As
W32/Duni.A		8/02	Fp	W97M/Footer.A		12/99	As
W32/Duni.C-mm		6/03	Ta	W97M/Groov.C		11/99	As
+W32/Eggsa-mm		1/04	Ao	W97M/Hopper.AJ		6/03	So
W32/Enegg-mm		10/03	Ao	W97M/IIS.A		11/00	As
W32/Estrella.A		1/02	Jm	W97M/IIS.D		10/03	As

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
– W32/ExploreZip.L-mm		1/03	Sk	W97M/IIS.E		6/00	As
– W32/FBound.C-mm		4/02	Ao	W97M/Ipid.G		10/01	As
W32/Fix2001-m	Admin.12288	11/03	As	W97M/Jerk.A		7/02	As
W32/Flopcopy		11/03	Ao	W97M/Killfound		6/03	Jw
+W32/Franriv		1/04	So	W97M/Kingpawn		6/03	Sk
W32/Frethem.S-mm		5/03	Mt	W97M/Lakko		6/03	Sk
W32/Gant.A-mm		6/03	Ta	W97M/Lexar.A		10/03	Sk
W32/Gant.C-mm		7/03	Ta	W97M/Macroble.A		7/02	As
+W32/Gluber.A-mm		1/04	Sj	W97M/Marker.AD		12/00	As
+W32/Gluber.B-mm		1/04	Ta	W97M/Marker.AE		9/99	As
W32/Gnu		4/01	Ao	W97M/Mar		2/01	As

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
man				ker.AY			
W32/Graps		7/03	Tm	W97M/Marker.AZ		2/00	As
W32/Gruel-mm		10/03	Ao	W97M/Marker.DG		3/01	As
W32/HLLP.DeTroie.A		6/02	Ao	W97M/Marker.EL		8/00	As
W32/Holar.A-mm		7/03	St	W97M/Marker.GO		10/01	As
–W32/Holar.C-mm		12/02	Fp	W97M/Marker.J		3/00	As
W32/Holar.G-mm		10/03	Mo	W97M/Marker.N		2/00	As
W32/Horo-mm		6/03	So	W97M/Marker.Q		11/03	As
W32/Hybris.E-mm		6/03	Sh	W97M/Marker.R		6/03	As
W32/Indor.E-mm		10/03	Ao	W97M/Marker.T		3/01	As
W32/Jantic.B-mm		10/03	Ao	W97M/Marker.X		9/99	As
+W32/Jubo		1/04	Ta	W97M/MD		7/99	As

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
n				MA.K			
W32/Kickin.D-mm		11/03	As	W97M/Melissa.M-mm		12/99	As
W32/Kindal-mm		3/03	Mt	W97M/Melissa.O-mm	Empirical	2/00	As
W32/Kitro-mm		3/03	So	W97M/Model.A		7/02	As
W32/Klez.B-mm		11/01	Jg	W97M/Murke.A		10/00	As
W32/Kriz.3863		1/03	Mo	W97M/Myna.BG		6/03	As
W32/Kriz.4029		1/00	Mo	W97M/Nagem.A		1/01	As
W32/Kwbot.C		6/03	Zy	W97M/Nagem.B		7/02	As
W32/Kwbot.D		6/03	Tm	W97M/Nid.A		3/00	As
W32/Kwbot.F		7/03	Ta	W97M/Nono.A		2/99	As
W32/Lanet-mm		4/03	Am	W97M/Nosf.B		6/03	Sk
W32/Lazi		11/03	As	W97M/Notfam.A-mm		6/03	Sk
W32/Libid.		10/0	Jm	W97M/Nott		6/03	Sk

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
A		1		ice.D			
– W32/Liote n		1/03	So	W97M/Nott ice.D		6/03	As
W32/Lirva. B-mm		7/03	St	W97M/Oca rd.A		7/00	As
+W32/Log pole.A		1/04	Ta	W97M/One x.A		4/01	As
W32/Logp ole.B		11/0 3	Ao	W97M/One x.E		12/00	As
W32/Lolol. E		3/03	So	W97M/Ope y.C		10/03	As
+W32/Lov gate.d-m		1/04	Ta	W97M/Ope y.J		6/03	As
W32/Maax .B-mm		6/03	Ac	– W97M/Ope y.M		10/00	As
W32/Mago ld.B-mm		7/03	Ta	W97M/Ostr ich.A		6/02	As
W32/Mago ld.C-mm		7/03	Ta	W97M/Ostr ich.B		7/01	As
W32/Mald al.C-mm	Keyluc, Reezak	12/0 1	Ph	W97M/Piec e.A-mm		3/01	As
W32/Many		6/03	Ta	W97M/Pin		6/03	Tc

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
x-m				g.W			
W32/Mapson.C-mm		7/03	Zy	W97M/Pri.B	Prilissa.A	3/99	As
W32/Mario.45056.A		7/01	Jm	W97M/Pri.Q-mm		11/99	As
W32/Marque		10/03	Mt	W97M/Proverb.C		8/00	As
W32/Merkur.D-mm		7/03	Ta	W97M/Replog.A		11/00	St
+W32/Mertian-mm		1/04	Ao	W97M/Replog.F		3/03	As
W32/Mimail.B-mm		11/03	So	W97M/RV.A		10/03	As
W32/Mimail.D-mm		11/03	So	W97M/Seliuq.A		11/00	Sk
W32/Mimail.L-mm		11/03	Sj	W97M/Seliuq.E		6/03	Fp
W32/MoFei.B		7/03	Oz	W97M/Service.A-mm		11/03	As
W32/Mofei.B		11/03	So	W97M/Sting.A		5/02	As
W32/Morbex-mm		5/03	So	W97M/Story.E		10/03	As
W32/MSIn	Bymer.	11/0	Ao	W97M/Surr		7/00	As

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
it.A	A	0		ound.A			
– W32/MyLife.J-mm		5/02	Ao	W97M/Surround.B		10/02	As
W32/Naco.B-mm		6/03	Ta	W97M/Temple.A		3/02	As
W32/Naco.D-mm		7/03	Ta	W97M/Thus.AP		12/00	As
W32/Naco.E-mm		6/03	Ta	W97M/Thus.AW		12/00	As
W32/Naco.F-mm		7/03	Ta	W97M/Thus.B		10/03	As
W32/Naco-mm		5/03	Sj	W97M/Thus.BH		4/01	As
W32/Niden		10/03	Ao	W97M/Thus.BX		3/02	As
W32/Niklas.N		10/03	So	W97M/Thus.CD		10/03	As
W32/Nofear.A-mm		7/03	Ta	W97M/Thus.CQ		5/01	As
W32/Nofear.B-mm		7/03	Ta	W97M/Thus.E		3/00	As
W32/Nofear.C-mm		7/03	Ta	W97M/Thus.G	THUS.G	6/03	As

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
W32/Onamu.B-mm		5/03	As	W97M/Thus.H		3/00	As
+W32/Opaserv.Aj		1/04	Mo	W97M/Thus.I		8/00	As
W32/Opaserv.J		3/03	Mo	W97M/Thus.M		7/00	As
– W32/Opaserv.N		1/03	Mo	W97M/Thus.O		11/00	As
W32/Opaserv.O		1/03	Mo	W97M/Thus.P		12/00	As
– W32/Opaserv.R		1/03	Mo	W97M/Thus.Q		6/00	As
W32/Opaserv.T		3/03	Mo	W97M/Thus.R		12/00	As
W32/Opaserv.V		3/03	Mo	W97M/Thus.U		10/03	As
W32/Opex.B		7/03	Ta	W97M/Thus.X	Bethlem	6/00	As
W32/Oror.AC-mm		4/03	Zy	W97M/Timret		4/03	Ac
+W32/Oror.AD-mm		1/04	Zy	W97M/Titch.A		1/00	As

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
W32/Oror.AG-mm		4/03	Ac	W97M/Titch.H		3/01	As
W32/Oror.AR-mm		7/03	Ta	W97M/Titch.M		3/03	St
W32/Oror.J-mm		3/03	St	W97M/Toler.D		6/03	Sk
W32/Oror.L-mm		5/03	Sh	W97M/Turn.A		12/99	As
W32/Oror.N-mm		3/03	St	W97M/Twotraps.A		5/03	Tm
+W32/Oror.Q-mm		1/04	Is	W97M/Van		6/03	Sk
W32/Parite.C		5/03	So	W97M/VMPCK1.E1		6/03	Sk
W32/Pesin.B		11/03	As	W97M/Walker.D		6/99	Fp
W32/Petch.B		11/03	Ao	W97M/Walker.E		6/99	As
+W32/PetTick-mm		1/04	Ta	W97M/Wazzu.X		5/01	As
W32/Poopoo		6/03	Ta	W97M/Wisefool		6/03	Sk
W32/Porkis-mm		1/03	As	W97M/Wrench.I	Egerton	5/01	As

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
W32/Pretty Park.51433-mm		5/00	Ao	W97M/Xaler.B		7/03	Zy
W32/Pretty Park.60928-mm		3/01	As	W97M/Xthree.A		5/01	As
W32/Prolin.A-mm	Creative.A	12/00	As	W97M/Yozak.B		10/03	Ao
W32/Randex.C		7/03	Ta	WM/MDMA.A	Sticky Keys	12/01	Zz
W32/Randex.D		7/03	Ta	WM/Wazzu.DO		11/01	Fp
+W32/Reur.E		1/04	Ta	WM97/Tolu.D		3/03	St
W32/Ronoper.T		11/03	Al	X97M/AND.D		6/03	So
+W32/Rosya.I		1/04	Mt	X97M/Anis.A		3/03	So
W32/Rutern.5244		11/03	Ao	X97M/Barisada.D		12/00	As
W32/Sachiel.C		7/03	Tm	X97M/Divi.AB		7/03	As
W32/Sahay.A		3/03	St	X97M/Divi.B		9/00	Sm

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
W32/Savior		7/03	Tm	X97M/Divi.F		8/00	As
+W32/Scold.B-mm		1/04	Ta	X97M/Divi.H		10/03	As
W32/Sddrop.C		6/03	Ta	X97M/Divi.Q		12/00	As
W32/Sddrop.C		7/03	St	X97M/Jini.A1		11/00	As
W32/Shower		3/03	So	X97M/Laroux.AE		5/00	As
W32/Shynet		6/03	Ac	X97M/Laroux.CF		7/99	As
+W32/Slideshow		1/04	Ao	X97M/Laroux.D		3/01	As
W32/Sluter		7/03	Tm	X97M/Laroux.FC		10/03	As
W32/Sober.B-mm		11/03	Am	X97M/Laroux.HO		5/99	As
W32/Spex		10/03	Ao	X97M/Laroux.IH		3/01	As
W32/Spybot.AB		7/03	Ta	X97M/Laroux.MG		5/03	As
W32/STD.B		6/03	Ta	X97M/Laroux.ML		5/03	Rz

Название вируса	Другое (ие) имя (имена)	Дата	Код участника	Название вируса	Другое (ие) имя (имена)	Дата	Код участника
W32/Systemp		4/03	Ac	X97M/Laroux.OQ		5/03	Rz
W32/Taripox.A		6/03	Ta	X97M/Linik.C		6/03	Sk
W32/Taripox.C		6/03	Ta	X97M/Phoneman		6/03	Sk
W32/Tariprox.B-mm		5/03	So	X97M/Squared.A		4/01	As
W32/Tarit		6/03	Ta	X97M/Squared.A		4/02	So
W32/Tinit.A		6/01	Mo	XM/Laroux.G		2/01	As
Итого вирусов в списке: 390							

Всего вирусов в основном и дополнительном списках: 651

В настоящее время в качестве дополнения к приведённому выше «Основному списку» вирусов в «The WildList» включается таблица «плотности распределения вирусов».

Эта таблица не претендует на роль инструмента, который однозначно показывает уровень распространённости каждого вируса из числа включаемых в «The WildList». Она содержит названия – основное и дополнительные (или так называемые «клички») наиболее часто встречающихся в сообщениях респондентов компьютерных вирусов. Условием-ограничением для включения конкретного вируса в таблицу

является требование, в соответствии с которым он должен быть упомянут в сообщениях, поступивших в Международную организацию WildList по крайней мере от 15 респондентов. Указанная таблица ранжируется исходя из критерия частоты упоминания вируса в сообщениях респондентов.

ОСНОВНОЙ СПИСОК «THE WILDLIST»

УПОРЯДОЧЕННЫЙ ПО ЧАСТОТЕ УПОМИНАНИЯ ВИРУСОВ

Частота упоминания	Название	Другое название	Частота упоминания	Название	Другое название
46	W32/Klez.H-mm	–	20	W32/BadTrans.B-mm	29020
38	W32/Sobig.A-mm	–	20	W32/Sobig.C-mm	–
37	W32/BugBear.A-mm	–	20	W95/CIH.1003	CIH.A, Spacefiller
33	W32/BugBear.B-mm	–	19	W32/Blaster.A	–
31	W32/Funlove.4099	–	19	W32/Mimail.G-mm	–
31	W32/Ganda-mm	–	19	W32/Opaserv.A	–
31	W32/SirCam.A-mm	–	19	W32/Sobig.B-mm	–
29	W32/Swen-mm	–	19	W32/Yaha.G-mm	Lentin.F

Частота упоминания	Название	Другое название	Частота упоминания	Название	Другое название
28	W32/Klez.E-mm	–	18	W32/Braid.A-mm	–
27	W32/Fizzer-mm	–	18	W32/Mimail.C-mm	–
27	W32/Lirva.A-mm	–	17	W32/Gibe.B-mm	–
27	W32/Mimail.A-mm	–	17	W32/Lovgate.F-m	–
26	VBS/Redlof.A-m	–	17	W32/Nimda.E-mm	–
26	W32/Magistr.B-mm	–	17	W32/Yaha.E-mm	Lentin.D
26	W32/Sobig.F-mm	–	17	W95/Dupator.1503	–
25	W32/Magistr.A-mm	Disembowler	16	W32/Lirva.C-mm	–
25	W32/Yaha.K-mm	–	15	VBS/Haptime.A-mm	Help
24	W32/Dumaru.A-mm	–	15	W32/BadTrans.A-mm	13312
24	W32/Nimda.A-mm	–	15	W32/Gibe.A-mm	–

Частота упомина ния	Название	Другое название	Частота упоминан ия	Название	Другое название
23	W32/Elkern .C	WQK.C	15	W32/Opas erv.K	–
22	W32/Sobig. E-mm	–	15	W32/Parit e.B	–
22	W95/Spaces .1445	Busm.144 5	15	W32/Sobe r.C-mm	–
21	W32/Hybris .B-mm	Hybris.230 40-mm	15	W32/Yaha .P-mm	–
21	W32/Nachi	–			–

«The WildList» в целом является перечнем компьютерных вирусов «в диком виде», написанных для IBM-совместимых персональных компьютеров, но иногда его составители получают от респондентов отчёты о вредоносных компьютерных программах, которые не могут быть однозначно отнесены к категории «вирусов для PC», но привлекающих внимание пользователей и специалистов. В этом случае в «The WildList» вводится ещё один раздел под названием «Иные».

Пример такой вредоносной компьютерной программы приведён в таблице ниже.

Иные

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
Linux/OSF.875	–	5/02	Am

Название вируса	Другое(ие) имя (имена)	Дата	Код участника
9			
Итого в списке «Иные»: 1			

СПИСОК ЛИТЕРАТУРЫ

1. . 1986 U.S.Computer Fraud and Abuse Act.
2. Bontchev Vesselin. Methodology of Computer Anti-Virus Research. Doctoral Thesis. University of Hamburg, 1998.
3. Burger Ralph. Computer Viruses. The Decease of High Technologies. 1987.
4. Chess David. Private e-mail conversation.
5. Cohen F. Computer viruses, theory and experiments // Computers & Security. Vol. 6. 1987.
6. Cohen F. Computer viruses: theory and experiments // Proc. 2nd IFIP Int. Conf. on Computer Security, 1984.
7. Cohen F. Models of practical defenses against computer viruses // Computers & Security. Vol. 8. 1989.
8. Cohen F., A Formal Definition of Computer Worms and Some Related Results, IFIP-TC11 Computers and Security V11#7, November 1992.
9. Computer Viruses. ASP Press, 1986.
10. Computer viruses: a secret threat. Conference Dierstein R. Computerviren // KES, 1985. V. 1. № 3, 4. Securicom, Paris, 1986.
11. Demers A., Greene D., Hauser C., Irish W., Larson J., Shenker S., Sturgis H., Swinehart D. and Terry D. Epidemic algorithms for replicated database maintenance. Oper. Syst. Rev. Vol. 22. 1988.
12. Dewdney A. K. In the game called Core War hostile programs engage in a battle of bits // Scientific American, 1984. V. 250. № 5.
13. Dierstein R. Computer viren. Output, 1986, V. 15. № 8.

14. Dierstein R. Computerviren // KES, 1985. V. 1. № 3, 4.

15. Dr. Harold Joseph Highland. The BRAIN virus: fact and fantasy // Computers & Security. Vol. 7. 1988.

16. Electronic fund transfer systems fraud, Paladin Press, Boulder, Colorado, 1989.

17. Ferbrache. A pathology of Computer Viruses. Springer, London, 1992.

18. Fraud protection and detection series: Counterfeit Securities. Check Fraud, Letters of Credit Fraud, Account-Opening Fraud, Cheque Kiting, Advanced Fee Fraud, Money Transfer; Bank Administration Institute, Rolling Meadows, Illinois, 2002.

19. George I. Davida, Yvo G. Desmedt and Brian J. Matt. Defending systems against viruses through cryptographic authentication. Proc. 1989 Symp. on Security and Privacy, Oakland, California, May 1–3, 1989.

20. Gleissner Winfried. A mathematical theory for the spread of computer viruses // Computers & Security. Vol. 8. 1989.

21. Goffman W. and Newill V. A. Generalization of epidemic theory, an application to the transmission of ideas // Nature. Vol. 204, 1964.

22. Highland Harold J. Computer Virus Handbook. Elsevier Advanced Technology. Oxford, England, 1990.

23. J. Von Neumann and A. W. Burks. Theory of Self-Reproducing Automata. University of Illinois Press, Urbana, Illinois, 1966.

24. Jeffrey O. Kephart and Steve R. White. Measuring Computer Virus Prevalence // Proceedings of the Second International Virus Bulletin Conference. Edinburgh, Scotland, September 2–3, 1992.

25. John Shock, Jon Hepps. The «Worm» Programs – Early Experience with a Distributed Computation // Communications of the ACM.

Volume 25. 1982. P. 172–180.

26. K. R. van Wyk The Lehigh virus // C&S. 1989. V. 8. № 2.

27. Kane Pamela. Anatomy of a Virus Scare. ISP News of May/June 1992.

28. Kane Pamela. P.C. Security and Virus Protection Handbook.

29. M. W. Eichin and J. A. Rochlis. With microscope and tweezers: An analysis of the Internet virus of November 1988 // Proc. 1989 IEEE Symp. on Security and Privacy, Oakland, California, May 1–3, 1989.

30. Maria M. Pozzo and Terence E. Gray. An approach to containing computer viruses // Computers & Security. Vol. 6. 1987.

31. Marius van Oers. Digital Rivers of Babylonia // Virus Bulletin. February 2000. P. 6–7.

32. McAfee, quoting expert sources on The MacNeil / Lehrer News Hour, March 5, 1992.

33. Melissa Computer Virus Writer, David Smith, Pleads Guilty in Federal Court. ICSA, 9 December 1999.

34. Melissa virus creator pleads guilty. BBC News Online, 9 December 1999.

35. Michael W. Miller. «Michelangelo» Scare Ends In an Anticlimax // The Wall Street Journal, March 9, 1992.

36. Nachenberg Carey. Computer Parasitology // Proceedings of the Ninth International Virus Bulletin Conference, September/October 1999.

37. Nick Lai and Terrence E. Gray. Strengthening discretionary access controls to inhibit trojan horses and computer viruses // Proc. Summer 1988 USENIX Conf. San Francisco, California, June 20–24, 1988.

38. Quittner Joshua. Michelangelo Virus: No Brush With Disaster. New York Newsday, April 5, 1992.

39. Riordan Roger. Private e-mail conversation.

40. Sarah Gordon and Richard Ford. Real World Anti-Virus Reviews and Evaluations-the Current State of Affairs // Proceedings 19th National Information Systems Security Conference. Baltimore Maryland. October 1996.

41. Seeley D. A tour of the worm // Proc. Usenix Winter 1989 Conference, San Diego, California, 1989.

42. Solomon Alan. Private e-mail conversation.

43. Spafford E. H. The Internet worm program: an analysis // Computer Comm. Review 19, 1. 1989.

44. Spafford Eugene. The Internet Worm Program: an Analysis // Purdue University Technical Report CSD-TR-823.

45. Sprengelmeyer Mike. Computer virus catchy, not fatal, // The Daily Northwestern, Tuesday, November 12, 1985 (Vol 107, No. 37).

46. Steven Braggs, Richard Wang. Seek and Destroy // Virus Bulletin, August 1999.

47. Stoll Cliff. An epidemiology of viruses and network worms // 12th National Computer Security Conference, 1989.

48. Survivor's Guide to Computer Viruses / ed. Victoria Lammer. Virus Bulletin Ltd, 1993.

49. Ször Péter. Happy Gets Lucky // Virus Bulletin, April 1999.

50. Top ten viruses reported to Sophos Anti-Virus in June 2000. Sophos PLC.

51. Verborgener befehl // Der Spiegel, 1984. V. 38. № 47.

52. Webster Anne E. University of Delaware and the Pakistani computer virus // Computers & Security. Vol. 8. 1989.

53. West, Harry: «Fraud – The Growth Industry», British Institute of Management, Kogan Page Ltd., London, 1988.

54. Whalley Ian. Bursting the Bubble // Virus Bulletin, December 1999.

55. Whalley Ian. Melissa – The Little Virus That Could // Virus Bulletin, May 1999.

56. Whalley Ian. Testing Times for Trojans // Proceedings of the Ninth International Virus Bulletin Conference, September/October 1999.

57. Young Catherine L. Taxonomy of computer virus defense mechanisms // Proc. 10th National Computer Security Conference. Baltimore, Maryland, 1987.

58. Альбрехт У., Венц Дж., Уильямс Т. Мошенничество. Луч света на темные стороны бизнеса. СПб., 1996.

59. Андрианов Б. Ч., Бородин В. А. «Шпионские штучки» и устройства защиты объектов и информации. СПб., 1996.

60. Батурин Ю. М. Проблемы компьютерного права. М., 1991.

61. Батурин Ю. М., Жодзинский Н. Л. Компьютерная преступность и компьютерная безопасность. М., 1991.

62. Безруков Н. Н. Компьютерная вирусология. Киев, 1990.

63. Беляев В. С. Безопасность в распределительных системах. М., 1995.

64. Большой толковый медицинский словарь. Oxford. Том 2 (Н – Я). Oxford University Press; АСТ; Вече, 1998.

65. Вехов В. Б. Компьютерные преступления: способы совершения, методики расследования. М., 1996.

66. Волокитин А. В., Лопаткин С. В. Электронная коммерция. Учебное пособие для служащих государственных организаций и

коммерческих фирм / Под общей редакцией Л. Д. Реймана М., 2002.

67. Гасанов Р. М. Шпионаж и бизнес. М., 1992.

68. Гасанов Р. М. Шпионаж особого рода. М., 1989.

69. Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 9 сентября 2000 года № Пр–1895.

70. Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных».

71. Закон Российской Федерации «Об авторском и смежных правах».

72. Как хранят секреты в Америке // Новости разведки и контрразведки. 1994. № 13.

73. Кащеев В. И. Специальная техника контроля и защиты информации // Системы безопасности. М., 1995. № 1.

74. Корчагин А. Г. Экономическая преступность. Владивосток, 1998.

75. Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // «Российская юстиция». 1999. № 1.

76. Криминология. Учебник для юридических вузов / Под ред. В. Н. Кудрявцева, В. Е. Эминова. М., 1995.

77. Крылов В. В. Информационные компьютерные преступления. М., 1997.

78. Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность: Справочник. М., 1998.

79. Лучин И. Н., Желдаков А. А., Кузнецов Н. А. Взламывание парольной защиты методом интеллектуального перебора //

Информатизация правоохранительных систем. М., 1996.

80. Мелик Э. Компьютерные преступления. Информационно-аналитический обзор. М., 1999.

81. Мещеряков В. А. Криминалистическая классификация преступлений в сфере компьютерной информации // Конфидент. 1999. № 4–5.

82. Моисеенков И. Э. Суета вокруг Роберта или Моррис-сын и все, все, все... М., 1990/

83. Наумов В. Отечественное законодательство в борьбе с компьютерными преступлениями. М., 1997.

84. Панов В. П. Сотрудничество государств в борьбе с международными уголовными преступлениями. М., 1993.

85. Проблемы борьбы с компьютерной преступностью // Борьба с преступностью за рубежом. М., 1992. № 4.

86. Ривкин К. Преступления с кредитными карточками // Экономика и жизнь. 1997. № 2.

87. Родионов А. Компьютерные преступления и организация борьбы с ними // Научно-правовой альманах МВД России «Профессионал». 1999. 5 (31).

88. Свенссон Б. Экономическая преступность. М., 1987.

89. Современный промышленный шпионаж // Борьба с преступностью за рубежом. М., 1995. № 11.

90. Сорокин А. В. Компьютерные преступления: уголовно-правовая характеристика, методика и практика раскрытия и расследования. Курган, 1999.

91. Уголовное право России. Особенная часть: Учебник / Отв. ред. Б. В. Здравомыслов. М., 1996.

92. Уголовный кодекс Российской Федерации. М., 2002.

93. Федеральный закон «Об информации, информатизации и защите информации».

94. Шаваев А. Г. Безопасность корпораций: криминологические, уголовно-правовые и организационные проблемы. М., 1998.

95. Яковлев А. М. Социология экономической преступности. М., 1988.