2в1: книга+видеокурс

ВИДЕОСАМОУЧИТЕЛЬ

Сергей Яремчук

Защита вашего компьютера

ПИТЕР

Сергей Акимович Яремчук

Защита вашего компьютера

Серия «Видеосамоучитель»

Текст предоставлен издательством
http://www.litres.ru/pages/biblio_book/?art=183737
Защита вашего компьютера: Питер; Санкт-Петербург; 2008
ISBN 978-5-388-00236-5

Аннотация

С помощью компьютера мы общаемся с людьми, получаем нужные сведения, ведем деловую переписку, храним финансовую и личную информацию – доверяем компьютеру то, к чему хотелось бы ограничить доступ. В то же время сегодня только и говорят о вирусных эпидемиях, хакерских атаках, воровстве личных данных. И вы должны уметь защищать свои данные.

Прочитав эту книгу и просмотрев прилагающийся к ней видеокурс, вы узнаете о приемах, используемых хакерами, вирусописателями и сетевыми мошенниками, научитесь защищаться от вирусов и прочих вредоносных программ, распознавать и отражать хакерские атаки, уловки интернет-мошенников, защищаться от спама, контролировать доступ к тем ресурсам, которые не должен посещать ваш ребенок. Книга расскажет, а видеокурс покажет, как прятать ценную информацию от чужих глаз, подбирать пароли, восстанавливать потерянную информацию.

На прилагаемом к книге диске, кроме видеокурса, вы найдете программы, которые помогут надежно защитить ваш компьютер.

Видеокурс прилагается только к печатному изданию книги.

Содержание

Сергей Акимович Яремчук
Защита вашего компьютера

Вместо введения

Трудно сказать, что устроено сложнее: современный автомобиль, способный мчаться со скоростью сотен километров в час, или небольшой ящик, стоящий под столом и весело подмигивающий разноцветными лампочками. Чтобы управлять машиной, человек должен пройти подготовку и сдать экзамены, после чего получить заветные права, подтверждающие его знания и умения. При покупке же персонального компьютера никто и не подумает поинтересоваться, умеете ли вы на нем работать. Вероятно, такое различие связано с тем, что, выезжая на дорогу, неподготовленный водитель может представлять угрозу для жизни людей, и лучшее тому доказательство – автомобиль, летящий на красный свет.

Все, что происходит в виртуальном мире, неосязаемо. Следовательно, и опасности, которые могут подстерегать вас здесь, трудно понять и тем более ощутить. Но они есть. Каждый день появляются сообщения о проделках неуловимых хакеров, вирусных атаках, краже банковской и персональной информации и прочих опасностях.

Компьютер давно перестал быть чем-то диковинным и

недоступным – сегодня его можно встретить практически в каждом доме. Однако если на входной двери привычно видеть замок, охраняющий хозяев от непрошеных гостей, то виртуальный вход часто бывает совсем не защищен. Конечно, с современным компьютером сможет справиться каждая домохозяйка, но события последних лет показывают, что для безопасной работы умения двигать мышью явно недостаточно.

В отчете, недавно опубликованном корпорацией Microsoft, сообщается, что более 60 % всех компьютеров заражены вирусами или находятся под контролем злоумышленников. Вдумайтесь в эту цифру: получается, что почти каждый второй компьютер вышел из-под контроля хозяина и представляет опасность для остальных. В некоторых странах уже действуют законы, позволяющие отдать под суд владельца компьютера, с которого рассылались вирусы или спам. Однако проблема в том, что пользователь, возможно, и не догадывается о «тайной жизни» своей машины.

Цифры, опубликованные Microsoft, наверняка приблизительны, и узнать точное количество зараженных компьютеров вряд ли возможно. Но приведенная статистика явно указывает на то, что современному пользователю необходимо обладать знаниями, позволяющими отличить реальную угрозу от рекламных трюков и главное – надежно защитить компьютер от непрошеных гостей.

От издательства

Ваши замечания, предложения и вопросы отправляйте по адресу электронной почты **dgurski@minsk.piter.com** (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На сайте издательства **http://www.piter.com** вы найдете подробную информацию о наших книгах.

Глава 1
Защищенность компьютеров: мифы и реальность

История возникновения компьютерных вирусов
Что такое вирус
Разновидности компьютерных вирусов
Вирусные мистификации
Что за зверь – троянский конь?
Новаторские подходы хакеров – руткиты (rootkits)
Уязвимости программ и хакерские технологии

1.1. История возникновения компьютерных вирусов

Если бы разработчики первых компьютеров, сетей и сетевых протоколов могли заглянуть в будущее, то, вполне вероятно, проблем с защищенностью информации сегодня было бы меньше. Первоначально компьютеры занимали целые здания, стоили дорого и были доступны только крупным государственным и частным компаниям. Со временем возникла необходимость обмениваться информацией – так появились первые сети. В то время компьютеры были закрытыми системами и управлялись серьезными, увлеченными своим делом людьми в белых халатах, поэтому тогда никто не помышлял о хулиганстве и разрушениях.

К сожалению, история умалчивает о многих фактах, связанных с зарождением компьютерного вредительства, но кое-что все-таки дошло до наших дней. Декабрь 1949 года можно считать началом возникновения компьютерных вирусов. Именно тогда в Илинойсском университете Джон фон Нейман читал серию лекций «Теория и организация сложных автоматов», которая и легла в основу теории самовоспроизводящихся автоматов. Однако это была теория. Первым действующим вирусом можно назвать игру Darwin (**http://www.cs.dartmouth.edu/~doug/darwin.pdf**), которую изобрели в 1961 году сотрудники компании Bell Telephone

Laboratories В. А. Высотский, Х. Д. Макилрой и Р. Моррис.

Программы, написанные на ассемблере (языков высокого уровня еще не было) и называемые «организмами», загружались в память компьютера и сражались за ресурсы. Они захватывали жизненное пространство, пытаясь уничтожить противника. За этим процессом наблюдало приложение-«судья», определявшее правила и порядок борьбы соперников. Программист, разработка которого захватывала всю память компьютера, побеждал. Все это было не более чем экспериментом: участников интересовал сам процесс.

Следующий этап – самоперемещающаяся программа Creeper, созданная в начале 1970-х годов сотрудником компании BBN Бобом Томасом для подсистемы RSEXEC с целью продемонстрировать возможность самопроизвольного перемещения программ между компьютерами. Creeper не приносил вреда: предыдущая копия уничтожалась, а вирус перемещался на следующий компьютер.

В это время была разработана еще одна программа – Reaper, которую можно считать первым антивирусом. Перемещаясь по сети, Reaper отыскивал действующие копии Creeper и прекращал их работу.

В 1970 году произошло еще одно знаковое событие. В мае в журнале Venture был опубликован фантастический рассказ Грегори Бенфорда, в котором было приведено одно из первых описаний вирусных и антивирусных программ – Virus и Vaccine. Через два года в фантастическом романе «Когда

Харли был год» Дэвида Герролда были описаны программы, захватывающие системы подобно червям. Сам термин «червь» был впервые использован в романе Джона Браннера «На шоковой волне», опубликованном в 1975 году.

Термин «компьютерный вирус» был впервые использован в 1973 году в фантастическом фильме Westworld. Данное словосочетание употреблялось в значении, привычном для современного человека, – «вредоносная программа, внедрившаяся в компьютерную систему».

Наконец, 20 апреля 1977 года был выпущен компьютер, предназначенный для массового использования. Условия для реализации самовоспроизводящихся программ заметно улучшились.

В 1980-х годах компьютеры значительно подешевели и их количество увеличилось. Кроме того, машины стали более производительными, а энтузиастов, получивших к ним доступ, стало намного больше.

Неудивительно, что это десятилетие стало более богатым на события в компьютерном мире. Были проведены эксперименты по созданию самовоспроизводящихся программ и программ-червей; появились программы Elk Cloner и Virus, которые считаются первыми компьютерными вирусами. Если раньше экспериментальные образцы никогда не покидали компьютеры, на которых они запускались, то новые программы были обнаружены «на свободе» – на компьютерах вне лаборатории.

Дальнейшее развитие событий напоминало лавину. В 1987 году появился первый вирус, заражающий IBM PC-совместимые компьютеры под управлением MS-DOS, – Brain. Этот вирус был достаточно безвредным: его действие заключалось в изменении метки на дискетах в 360 Кбайт. Brain был написан двумя пакистанскими программистами, владельцами компании Brain Computer Services (отсюда и название вируса), исключительно в рекламных целях, но на его основе были созданы менее миролюбивые особи. В том же 1987 году появился Jerusalem («иерусалимский вирус»), запрограммированный на удаление зараженных файлов по пятницам 13-го. Первые его версии содержали ошибку, благодаря которой он повторно действовал на уже зараженные файлы. В последующих версиях ошибка была исправлена.

Хотя к тому времени уже появились материалы, посвященные безопасности информации, все это воспринималось не более чем игрушкой, экспериментом. Прозрение наступило неожиданно, когда эта «игрушка» перестала повиноваться и повела себя как разумный организм, заражающий все на своем пути. Это произошло 2 ноября 1988 года, когда студент Корнельского университета Роберт Моррис-младший запустил программу-червь, которая сохранилась в истории под именем своего разработчика. Червь Морриса стал первым сетевым червем, успешно распространившимся «на свободе», и одной из первых известных программ, эксплуатирующих такую уязвимость, как переполнение буфера.

За каких-то полтора часа вредителю удалось заразить около 6 тыс. машин. Произошедшее повергло общественность в шок: вирусы гуляли по Сети и ранее, но заразить каждый десятый компьютер до сих пор не удавалось никому. Срочно были пересмотрены требования к безопасности систем и созданы институты вроде CERT (Computer Emergency Response Team – команда по ответам на непредвиденные компьютерные ситуации), которые стали заниматься безопасностью компьютеров и давать рекомендации по устранению вирусов.

Компьютеры становились все доступнее. Со временем большинство платформ и операционных систем унифицировалось, на рынке стали преобладать Intel-совместимые компьютеры, которые работали под управлением операционной системы, разработанной компанией Microsoft. Дальнейшие события развивались с огромной скоростью. В 1991 году появился *полиморфный* вирус, видоизменявший свое тело. Операционная система Windows 95 была практически готова, и ее beta-версию разослали 160 тестерам. Все диски оказались зараженными загрузочным вирусом Form, и только один тестер не поленился проверить диск антивирусом. В пресс-релизе, посвященном выходу принципиально новой операционной системы, было сказано, что она полностью защищена от вирусов всех типов. Через несколько месяцев эти заявления были разнесены в пух и прах неожиданным подарком – первым *макровирусом*, представлявшим собой не

привычный исполняемый файл, а сценарий, который заражал документы Microsoft Word. В течение месяца макровирус Concept облетел вокруг земного шара, внедрился в компьютеры пользователей Microsoft Word и парализовал работу десятков компаний по всему миру.

Примечание

На сегодняшний момент известно около 100 модификаций вируса Concept.

В январе 1996 года появился первый вирус для операционной системы Windows 95 – Win95.Boza, а резидентный вирус Win95.Punch, появившийся позже, окончательно подорвал доверие пользователей к Windows 95. В марте этого же года началась первая эпидемия вируса Win.Tentacle, написанного для Windows 3.0/3.1. Он заразил компьютерную сеть в нескольких учреждениях Франции. До этого все Windows-вирусы хранились только в коллекциях и электронных журналах вирусописателей, на свободе гуляли лишь написанные для MS-DOS загрузочные и макровирусы. В этом же году был пойман макровирус Laroux, написанный для Microsoft Excel.

В 1997 году на свет появились новые виды вирусов – FTP– и mIRC-черви, в июне 1998 года – вирус Win95.CIH. Этот вирус активизировался 26 апреля (впервые – в 1999 году) и уничтожал информацию на жестком диске, записывая на него мусор. Кроме того, он перезаписывал Flash BIOS, если переключатель находился в положении, разрешающем запись, и выводил из строя материнскую плату.

Примечание

Эпидемия вируса Win95.CIH, также известного как «Чернобыль» и поразившего компьютеры 26 апреля 1999 года, была на тот момент самой разрушительной.

Червь I love you, выпущенный на Филиппинах в мае 2000 года, нанес владельцам компьютеров ущерб на сумму, по

некоторым оценкам превышающую $10 млрд. Следующий червь, вошедший в историю как Code Red, за 14 часов сумел заразить более 300 тыс. компьютеров, подключенных к Интернету. После них были и другие, часто – первые в определенной категории. Например, Nimda (слово admin, прочитанное наоборот), многовекторный червь, распространялся сразу несколькими способами, включая «черные ходы», оставленные другими червями. MyDoom был признан самым быстрым червем, распространяющимся по электронной почте.

До этого большая часть вирусов была написана на языке низкого уровня – ассемблере, позволявшем создать небольшой оптимизированный вирус. Автором червя AnnaKournikova, который поразил Интернет в феврале 2001 года, оказался голландский студент, который вообще не умел программировать, даже на таком простом языке, как Basic.

Сегодня общие годовые потери всех коммерческих организаций от действий вирусов могут сравниться с бюджетом небольшой страны, и эта сумма каждый год удваивается. Заявления некоторых специалистов по безопасности свидетельствуют о серьезности проблемы. По сведениям главы технологического департамента компании MessgeLabs (**http://www.messagelabs.com/**) Алекса Шипа, в 1999 году фиксировалось в среднем по одному новому вирусу в час, в 2000 году эта цифра составляла уже по одной программе каждые три минуты, а в 2004 году это время сократилось до

нескольких секунд. По данным СанктПетербургской антивирусной лаборатории И. Данилова (ООО «СалД»), только за март 2007 года в антивирусную базу добавлено более 7 тыс. записей.

Игра Darwin продолжается…

1.2. Что такое вирус

Как бы странно это ни звучало, *компьютерный вирус* – программа и, как правило, небольшая по размеру. Все дело в назначении и способе распространения. Обычная программа выполняет полезную работу, стараясь не нарушить функционирование операционной системы. Чаще всего пользователь устанавливает ее самостоятельно. В случае с вирусом все наоборот. Задача, которую ставит его создатель, состоит в том, чтобы нарушить работоспособность компьютера, удалить, повредить, а иногда и зашифровать важную информацию с целью получения выкупа. Вирусы распространяются между компьютерами по сети, замедляя их работу, перегружая каналы и блокируя работу сервисов.

> **Внимание!**
>
> Главная особенность любого вируса – умение самопроизвольно размножаться и распространяться без участия пользователя.

Размножение вируса происходит за счет того, что он «дописывает» собственный код к другим файлам либо по сети передает свое тело другому компьютеру.

Главная задача вируса – заразить максимальное количество компьютеров. Сегодня написать вирус может любой, было бы желание и наличие специальных конструкторов, не требующих особых знаний, в том числе и по программиро-

ванию. Однако долго такой вирус не протянет (хотя бывают и исключения: вспомним AnnaKournikova). Реализациям алгоритмов выживания и заражения посвящены целые журналы, причем некоторые подходы вызывают восхищение.

Для маскировки вирус может заражать другие программы и наносить вред компьютеру не всегда, а только при определенных условиях. Он сканирует диск в поисках исполняемых файлов (обычно такая чрезмерная активность выдает присутствие вируса) либо, находясь в оперативной памяти, отслеживает обращения к таким файлам. Выполнив нужные действия, вирус передает управление программе, в теле которой находится, и она начинает работать как обычно.

Вирус старается заразить максимальное количество файлов, отдавая предпочтение сменным носителям и сетевым ресурсам. Почему? А все потому, что ему нужно выжить: ведь всегда есть вероятность, что в сетевую папку зайдет пользователь с другого компьютера. Именно поэтому, попав на компьютер, многие вирусы не сразу занимались разрушением (зачем же уничтожать себя, любимого?), а прежде всего устанавливали счетчик успешно зараженных файлов. Пока в компьютере было заражено относительно мало программ, наличие вируса могло оставаться незамеченным. Система работала быстро, на экране не появлялось никаких сообщений, и пользователь редко замечал что-то необычное. Однако когда показатель на счетчике вируса достигал нужного значения, вредитель начинал действовать.

В начальный период существования вредоносных программ были популярны вирусы-шутки, которые мешали работе пользователей. Деструктивные особи практически не встречались. Например, такие программы просили дополнительной памяти («пирожка» и т. п.), и экран блокировался, пока пользователь не вводил с клавиатуры нужное слово (иногда его нужно было угадать). Лично я сталкивался с вирусом, который при обнулении счетчика не давал запустить приложение Microsoft Word с 18:00 до 09:00, мотивируя это тем, что работать нужно в рабочее время. Были и курьезы. Например, вирус, который выводил на экран сообщение вро-

де: «Нажмите одновременно **L + A + M + E + R + F1 + Alt**». Пользователь нажимал, после чего появлялось сообщение о том, что таблица разделов стерта с жесткого диска и загружена в оперативную память и если пользователь отпустит хотя бы одну клавишу, то со своей информацией он может проститься, а если просидит так ровно час, то все будет в порядке. Через час оказывалось, что это была шутка. Ничего себе шуточки…

Массовое распространение персональных компьютеров привело к появлению людей, которых интересовал не сам процесс создания вируса, а результат, наносимый вредоносной программой. Изменились и шутки: вирусы начали реально форматировать диски, стирать или кодировать важную информацию. Некоторые приложения использовали недостатки оборудования и портили его, например выстраивали лучи монитора в одну точку, прожигая его (надежность устройств в то время оставляла желать лучшего), или ломали жесткие диски, гоняя считывающую головку по определенному алгоритму.

На сегодня в мире вирусов наметилась явная коммерциализация: данные в большинстве случаев не уничтожают, а пытаются украсть. Например, популярность онлайн-игр привела к появлению вирусов, специализирующихся на краже паролей к учетным записям игроков, так как виртуальные ценности, заработанные в игре, можно продать за реальные деньги.

1.3. Разновидности компьютерных вирусов

Пришло время ознакомиться с особенностями работы некоторых вирусов – хотя бы для того, чтобы, узнав о начале очередной эпидемии, не спешить отключать кабель, ведущий к модему.

Точную классификацию вирусов и других вредоносных программ до сих пор никто не придумал. Вирус часто нельзя отнести ни к одной из категорий. Кроме этого, антивирусные компании вводят свою терминологию, по-разному обозначая новый вирус. Однако по некоторым общим признакам вредоносные программы можно разделить на группы.

По среде обитания. Первая классификация относится к среде, в которой «живет» вирус.

• Первые вирусы, которые были популярны до массового распространения Интернета, – *файловые*. Их еще называют *традиционными*. Сегодня известны программы, заражающие все типы исполняемых файлов в любой операционной системе. Например, в Windows опасности подвергаются в первую очередь исполняемые файлы с расширениями EXE, COM и MSI, драйверы (SYS), командные файлы (BAT) и динамические библиотеки (DLL). С механизмом заражения такими вирусами и их распространением вы познакомились в предыдущем разделе.

• *Загрузочные* вирусы также появились одними из первых. Как видно из названия, такие вирусы заражают не файлы, а загрузочные секторы дискет и жестких дисков.

• С массовым развитием Интернета появились *сетевые* вирусы. По данным антивирусных компаний, именно различные виды сетевых червей представляют сегодня основную угрозу. Главная их особенность – работа с различными сетевыми протоколами и использование возможностей глобальных и локальных сетей, позволяющих им передавать свой код на удаленные системы.

Классическим примером сетевого вируса является червь Морриса, рассмотренный в разделе 1.1.

Наибольшую распространенность получили сетевые черви, использующие электронную почту, интернет-пейджеры, локальные и файлообменные (P2P) сети, IRC-сети и сети обмена данными между мобильными устройствами. Некоторые сетевые черви, например W32.Slammer или Sapphire, использующий уязвимость Microsoft SQL Server 2000, могут не оставлять на жестком диске никаких следов, хранясь только в оперативной памяти. Благодаря способности активно распространяться и работать на зараженных компьютерах без использования файлов подобные вирусы наиболее опасны. Они существуют исключительно в системной памяти, а на другие компьютеры передаются в виде пакетов данных. Первое время антивирусное программное обеспечение не было способно бороться с такими бестелесными вредителями.

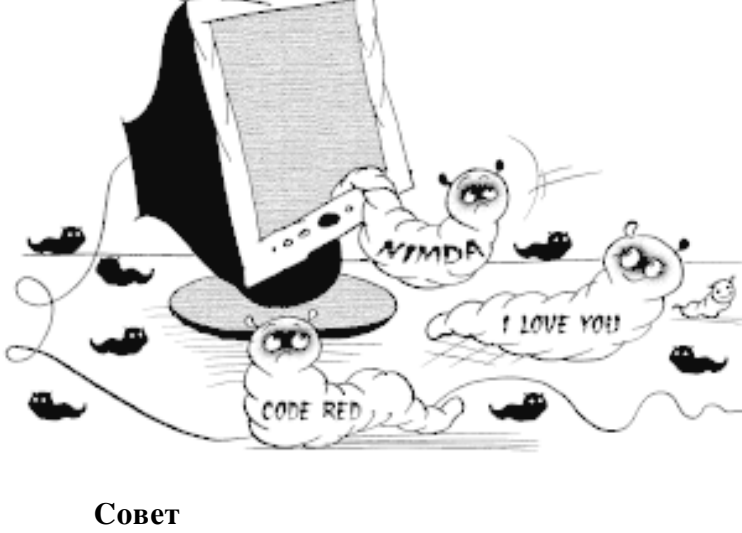
Внимание!

Сетевые и почтовые вирусы наиболее опасны, так как способны за короткое время заразить большое количество систем.

• Сегодня наиболее популярны сетевые вирусы, распространяющиеся посредством электронной почты, поэтому их часто выделяют в отдельную категорию – *почтовые* черви. Так, три из четырех крупнейших эпидемий 2005 года были вызваны именно почтовыми червями. Такие вирусы чаще всего распространяются через электронную почту: они рассылают по адресам, имеющимся в адресной книге, письма с прикреплениями в виде самих себя. Для передачи могут использоваться средства операционной системы или небольшой встроенный почтовый сервер (функция такого сервера – отправка писем).

Например, червь Melissa отсылал себя сразу после активизации только по первым 50 адресам, а I Love You использовал все записанные в адресной книге почтовые адреса, что обеспечило ему высокую скорость распространения. Другой тип червя – сценарий KakWorm, который после прочтения зараженного письма не рассылался, а прикреплялся к каждому посланию, отправляемому пользователем. При этом на новом компьютере вредоносное приложение либо выполнялось автоматически, используя уязвимости в почтовой программе, либо различными способами подталкивало пользователя к своему запуску. Зараженное письмо может прийти

со знакомого адреса, и пользователь, скорее всего, откроет его. Могут применяться различные ухищрения. Например, вирус AnnaKournikova приглашал посмотреть фотографии известной теннисистки Анны Курниковой: любопытство чаще всего брало верх над осторожностью, и пользователи запускали прикрепленный к письму исполняемый файл.



Совет

Будьте осторожны с письмами, полученными от неизвестных людей. Открывайте файлы, прикрепленные к таким письмам, только после проверки антивирусом.

• Очень часто встречаются вирусы смешанного типа – *почтово-сетевые*. В таком случае их обычно называют просто

сетевыми. Яркий пример – сетевой червь Mytob.c, который в марте 2005 года пересылался в виде вложений в электронные письма и использовал для своего распространения уязвимость в сервисе LSASS Microsoft Windows.

Черви – наиболее опасный тип вирусов. Они распространяются очень быстро и способны поражать файлы, диски и оперативную память. Правильно написанный червь может парализовать работу Интернета либо перегрузив каналы, либо заразив серверы. Например, Slammer сумел поразить почти четверть Интернета. В этом случае поражает беспечность фирмы-разработчика, так как об уязвимости, которая была использована автором Slammer, было известно еще за полгода до атаки. Интересно, что не один год до этого почтовые черви с успехом использовали уязвимость Microsoft Internet Explorer, позволяющую запускать любой исполняемый файл, пришедший вместе с электронным письмом, без согласия пользователя.

• *Макровирусы* являются программами, написанными на макросах – последовательностях команд, используемых в некоторых системах обработки данных, например текстовых редакторах и электронных таблицах. Возможности макроязыков в таких системах позволяют вирусу переносить свой код в другие файлы, заражая их. Наибольшее распространение получили макровирусы для Microsoft Word и Excel. Такой вирус активизируется при открытии зараженного документа и переносится на компьютер, как правило, внедряясь в

шаблон **Обычный** (файл **Normal.dot**). После этого каждый сохраняемый документ заражается вирусом, а когда другие пользователи открывают его, их компьютеры также инфицируются. Существуют также макровирусы, заражающие базы данных Microsoft Access.

Традиционные и макровирусы сегодня практически вымерли, так как скорость их распространения значительно ниже, чем скорость распространения сетевых вирусов, и у антивирусных компаний достаточно времени, чтобы создавать вакцину против таких вредителей. Однако это совсем не значит, что угроза миновала и такие вирусы не стоит брать в расчет.

По алгоритму работы. Например, существуют резидентные и нерезидентные вирусы.

• *Резидентный* вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, чтобы перехватывать все обращения операционной системы к объектам, пригодным для заражения. Это наиболее распространенный тип вирусов: они активны не только во время работы зараженной программы, но и – что наиболее важно – когда приложение закрыто. Резидентные вирусы постоянно находятся в памяти компьютера и остаются активными вплоть до его выключения или перезагрузки.

• *Нерезидентные* вирусы не заражают память компьютера и сохраняют активность лишь ограниченное время, хотя возможны варианты. Однако нерезидентные вирусы сегодня

практически не встречаются, они не способны к быстрому размножению. Можно сказать, что они не выдержали конкуренции своих более активных собратьев.

Примечание

Хочется еще раз обратить внимание на понятия «резидентность» и «файловый вирус». Несколько раз мне приходилось наблюдать настоящую панику, вызванную тем, что файл, который кто-то принес на дискете, заражен вирусом. Несмотря на то что некоторые вирусы могут спокойно размножаться без участия пользователя, файловые, загрузочные и макровирусы (резидентные и нерезидентные) не способны распространяться без помощи человека. Чтобы такой вирус начал разрушительную работу, его необходимо активизировать. Находясь на дискете или жестком диске, он разве что будет вызывать раздражение антивирусной программы, и, если пользователь сам не запустит его, нерезидентный вирус не принесет вреда.

Десятки вирусов этого типа хранятся у меня в отдельной папке для тестирования и изучения антивирусных программ, и за несколько лет ни одному из них не пришло в голову активизироваться самостоятельно, поэтому дискета с зараженным файлом не должна вызывать панику, следует оценить ситуацию и принять правильное решение – удалить потенциально опасный файл или попробовать вылечить его с помощью антивируса.

• Первые антивирусные программы очень быстро находили вирус по его уникальной сигнатуре. Чтобы затруднить подобный поиск, создатели вредоносных программ стали шифровать тела вирусов. В результате появились вирусы, названные *полиморфными*.

• В литературе часто упоминаются *стелс-вирусы* (stealth – невидимка), которые были распространены во времена MS-DOS. Они применяют множество средств, чтобы скрыть свое присутствие в системе. Определить наличие таких вирусов без соответствующего инструментария практически невозможно.

Сегодня для маскировки своего присутствия в системе вирусы используют руткит-технологии (о них будет рассказано позже). Вирусы можно подразделить также по следующим критериям:

• по методу заражения (вирусы-паразиты, компаньоны и др.);

• типу операционной системы (Windows, Unix, Linux, MS-DOS, Java);

• деструктивной возможности (от безвредных, просто мешающих работе, до крайне опасных);

• языку, на котором написан вирус (ассемблер, язык сценариев и др.).

Вирусы могут использовать различные упаковщики, позволяющие превратить известный код в практически неузнаваемый.

Каждый вирус имеет собственное имя. Вы слышите его, когда узнаете об очередной эпидемии. Откуда берется имя? Обнаружив новый вирус, антивирусные компании дают ему имена в соответствии с классификациями, принятыми в каждой конкретной компании, причем классификация у каждой фирмы своя. Посмотрите сами: например, Worm.Win32.Nuf – это то же самое, что NetWorm.Win32.Mytob.c. Часто название дается по некоторым внешним признакам:

- по месту обнаружения вируса (Jerusalem);
- содержащимся в теле вируса текстовым строкам (I Love You);
- методу подачи пользователю (AnnaKournikova);
- эффекту (Black Friday).

Бывает так, что вирус несколько раз переименовывают. Например, это касается «иерусалимского вируса». Изначально его назвали по месту обнаружения – Israeli, затем решили, что это название слишком антисемитское, и заменили его на «1813» (по размеру вируса), при этом параллельно использовалось другое имя – IDF (Israeli Defence Forces), и только через некоторое время вирус назвали Jerusalem.

Кстати

Самым маленьким по размеру вирусом считается Repus (Win95.c) – всего 156 байт (существуют, однако, и более тяжеловесные модификации, вплоть до 256 байт). Для уменьшения размера этого вируса используются

различные программные хитрости и уловки; вреда он не приносит, и все программы работают без проблем. При этом есть как резидентные, так и нерезидентные представители Repus (Win95.c). Помимо малого размера, Repus стал первым вирусом, использующим для своего размножения кэш-память Windows. Он ищет в кэш-блоках заголовки файлов, записывается в них и устанавливает для блоков атрибут dirty, который дает системе команду сохранить его на диск. Подобная методика позволяет даже нерезидентному варианту распространяться со скоростью резидентного вируса.

Одним из самых интересных является вирус I-Worm.Hybris (Vecna), получивший в июле 2002 года четвертую категорию опасности. Он распространяется посредством электронной почты. В первую очередь этот вирус заражает системный файл **wsock32.dll**, получая доступ ко всему интернет-трафику, а затем рассылает себя по полученным таким образом почтовым адресам. Самое интересное, что этот вирус может самостоятельно обновляться через Интернет, скачивая с новостной конференции **alt.comp.virus** плагины, дающие ему новые возможности.

Количество сигнатур в антивирусных базах многих производителей уже перевалило 400-тысячную отметку и постоянно растет.

1.4. Вирусные мистификации

Уважаемый получатель, Вы только что получили вирус «ТАЛИБАН».

Поскольку мы в Афганистане не так уж и продвинуты в технологиях, этот вирус следует исполнять вручную. Пожалуйста, перешлите это письмо всем, кого знаете, и уничтожьте все файлы на Вашем жестком диске собственноручно. Большое спасибо за помощь.

Абдулла, хакер из Талибана

Историю развития компьютерных систем нельзя назвать веселой. В первые годы антивирусы были несовершенны, а пользователи еще не владели достаточной информацией, но уже представляли, какую угрозу несут компьютерные вирусы. Вероятно, поэтому каждое сообщение о появлении нового вируса вызывало панику. Со временем у пользователей появился другой, не менее опасный синдром – вирусные мистификации. Хотя первые вирусные мистификации начали появляться приблизительно в 1988 году, а расцвет пришелся на конец 1990-х, рассказать об этом явлении стоит, так как мы не застрахованы от него и сегодня, когда скорость распространения любой информации на порядок выше.

Выглядит это приблизительно так. Злоумышленник либо случайный человек пишет предупреждение о том, что он обнаружил опасный вирус либо подозрительный файл, и поме-

щает это сообщение в конференцию или рассылает по электронной почте максимальному количеству людей. На самом деле никакого вируса нет. Прочитавший такое письмо пользователь спешит предупредить своих товарищей (часто такой совет присутствует в самом послании). Дальнейшее развитие событий подобно вирусной эпидемии: поток корреспонденции увеличивался лавинообразно, так как напуганные пользователи из лучших побуждений спешат предупредить об «опасности» коллег и партнеров по бизнесу. Результатом является вирусная истерика, которая систематически сотрясает компьютерный мир, принося напрасное беспокойство тысячам людей.

Первой действительно удачной мистификацией следует считать вирус Good Times, появившийся в 1994 году в сети AOL. Все началось с того, что кто-то разослал сообщение с предупреждением: ни в коем случае нельзя было читать электронное письмо с заголовком Good Times. Это письмо якобы содержало страшный вирус, стирающий информацию на жестком диске. В послании говорилось, что о новом вирусе следует предупредить всех знакомых и сослуживцев. Затем шло подробное описание принципа действия вируса и способа избавиться от него. Стоит ли говорить о том, что такого вируса не существовало и в помине! Кстати, само письмо-предупреждение также имело заголовок Good Times.

Основные идеи Good Times используются и сегодня.

Другая мистификация, появившаяся в том же году, бы-

ла запущена из меркантильных соображений. Некий Майк Рошенл отправил на несколько BBS-станций сообщения, в которых рассказал о появлении нового вируса, заражающего модемы, работающие на скорости 2400 бод. Народ поверил. В результате спрос и соответственно цены на более медленные модемы – 1200 бод – резко увеличились, а на более быстрые упали.

Следует, однако, отметить, что часто истерика возникала действительно из-за того, что кто-то находил вирус. Например, в 2001 году один из пользователей обнаружил, что файл **sulfnbk.exe**, лежащий в системной области, заражен вирусом – имеет подозрительное название и странный значок. Когда страсти утихли, выяснилось, что данный файл – это системная утилита, отвечающая за создание резервных копий файлов с длинными именами (название – от System Utility for Long FileName Backup – системная утилита для резервного копирования с сохранением длинных имен файлов), и у конкретного пользователя она действительно была заражена вирусом. Подобная история повторилась через год. Начавшись среди испаноговорящих пользователей Интернета в начале апреля 2002 года, мистификация быстро распространилась на англоговорящих к середине апреля. Под подозрение попал файл **jdbgmgr.exe**, принадлежавший пакету Visual J++ 1.1. И опять – сомнительный значок, непонятное название и действительно зараженный файл. Однако в данном случае, если пользователь не работал с пакетом Visual J++, работо-

способность системы при удалении этого файла не нарушалась.

К чести вирусописателей, эта история не была забыта, и через некоторое время действительно появился вирус, имеющий именно такое имя файла.

В 2002 году появился новый вирус – Perrun (W32/Perrun-A, PE_PERRUN.A, Win32.Perrun, W32/Perrun, W32/Perrun.A), который неизвестные часто присылали на сайты антивирусных компаний, очевидно, как предупреждение: мол, мы и так можем. Этот вирус мог заражать графические файлы и текстовые файлы с расширением TXT. Новость подхватили информационные агентства, и народ, естественно, начал волноваться. При ближайшем рассмотрении оказалось, что для заражения файла и его последующего распространения необходима программа-кодировщик, которая фактически является вирусом и без которой данный вирус можно считать разве что шуткой.

Самая интересная и известная мистификация произошла в 1991 году. Ее автор Роберт Моррис сообщил, что стал жертвой нового вируса, распространяющегося по обычной электрической сети, и рассказал о мерах, которые необходимо принять для защиты от него. По словам Морриса, нельзя было делать следующие вещи:

- включать что-либо в электрические розетки;
- использовать батарейки (поскольку вирус пробрался на заводы по производству батареек и заразил все положитель-

ные клеммы готовой продукции);

• передавать друг другу файлы любыми способами;

• читать на компьютере текст, причем совершенно любой, даже сообщение самого Морриса;

• использовать последовательные порты, модемы, телефонные линии, процессоры, системную память, сетевое оборудование, принтеры, мониторы и клавиатуры;

• пользоваться электроприборами, газовыми плитами, водопроводом, огнем и колесным транспортом.

Хорошо, что многие сразу понимали, что это просто шутка.

Как видите, мистификации появляются от недостаточной компьютерной грамотности при огромном желании показать свои знания. Преклонение перед неизвестным часто порождает множество мифов. Чего стоят рассказы о том, что кактус способен защитить от компьютерного (а почему не мониторного?) излучения. Эта шутка появилась в каком-то журнале в номере за 1 апреля. Автор статьи подробно описал размер иголок кактуса, расстояние между ними, высоту и рекомендуемый вид колючего растения, а также наилучшее место для его расположения. Конечно, кактус на мониторе способен разве что улучшить настроение, но никак не остановить излучение.

Мистификации могут принести немалый вред. Перегружаются почтовые серверы, пользователи в панике удаляют системные файлы. Вера в мистификацию может нанести се-

рьезный удар репутации человека или по крайней мере сделать его объектом насмешек: как же, мнил себя суперхакером, а оказался чайником, попавшимся на такую шутку. Кроме того, письма часто приходят с заполненными полями **Копия** и **Кому**, поэтому спамеры могут получить подарки в виде реально существующих адресов. Вирусные мистификации могут отвлечь внимание от принятия необходимых мер безопасности, так как после нескольких ложных предупреждений пользователи могут недооценить опасность реальных вирусов.

Как отличить мистификацию от реального вируса?

• Необходимо относиться с большим подозрением к письмам, полученным от неизвестных людей, с какими бы благими намерениями они ни обращались. Откуда у отправителя ваш электронный адрес? Может быть, из базы данных спама?

• Никогда не открывайте вложения к письмам от незнакомых отправителей, иначе у вас появится возможность на себе почувствовать то, о чем вы прочитали в предыдущем разделе.

• Если вы никогда не оставляли свои данные на специализированных сайтах и не регистрировали свою версию антивируса или подобной программы, то к любому письму, полученному от антивирусной лаборатории компании Microsoft или даже лично Била Гейтса, следует относиться с подозрением. С чего это они вдруг написали вам?

• Если письмо содержит подробную техническую инфор-

мацию, отнеситесь к нему скептически. В описании Good Times говорилось, что процессор будет выведен из строя бесконечным циклом *n*-й сложности… Если вас просят удалить или запустить какой-то файл, без сомнений удаляйте письмо.

Большие компании дорожат временем, поэтому вместо описания проблемы они, скорее, ограничатся ссылкой на соответствующий сайт. Пусть вас не смущает, что в послании упоминаются известные антивирусные или правительственные организации. Если вы думаете, что вам действительно сообщают о чем-то важном, то, перед тем как начать паниковать, зайдите на сайт данной компании: среди новостей вы обязательно увидите предупреждение об опасности.

В Интернете есть несколько ресурсов, посвященных мистификациям. Самые популярные из них – сайт Роба Розенбергера (**http://www.vmyths.com/hoax.cfm**) и сайт охотников за мистификациями Hoaxbusters (**http://hoaxbusters.ciac.org/**).

Все ведущие антивирусные компании имеют собственные страницы, посвященные мистификациям. И информацию можно найти на сайте **Вирусной энциклопедии** (**http://www.viruslist.com/**), Symantec (**http://www.symantec.com/avcenter/index.html**) и McAfee (**http://vil.mcafee.com/hoax.asp**).

И, конечно же, не забывайте о Google – на то он и поисковик, чтобы все знать!

1.5. Что за зверь – троянский конь?

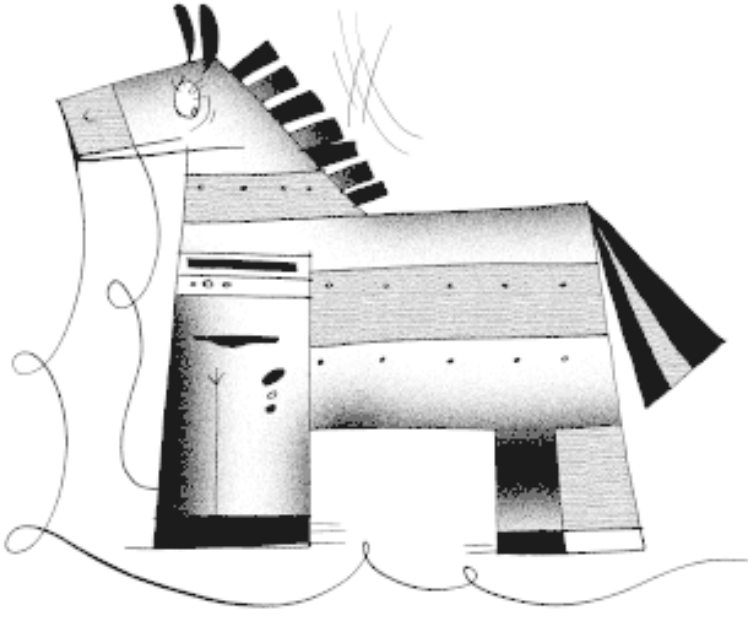
Практически ни один разговор о компьютерных вирусах не обходится без термина «троянская программа», или «троянец». Чем это приложение отличается от вируса, каково его назначение и чем оно опасно? К этой категории относятся программы, выполняющие несанкционированные действия без ведома пользователя. По характеру действия троянец напоминает вирус: он может красть персональную информацию (прежде всего файлы паролей и почтовые базы), перехватывать данные, введенные с клавиатуры, реже – уничтожать важную информацию или нарушать работоспособность компьютера. Троянская программа может применяться для использования ресурсов компьютера, на котором она запущена, в неблаговидных или преступных целях: рассылки вирусов и спама, проведения DDOS-атак (Distributed Denial of Service – распределенных атак, направленных на нарушение работы сетевых сервисов).

Это могут делать и вирусы. Отличие заключается в том, что часто внешне троянец выглядит как вполне нормальная программа, выполняющая полезные функции. Однако у нее есть и «вторая жизнь», о которой пользователь не догадывается, так как часть функций приложения скрыты. Троянская программа отличается от вируса неспособностью к самораспространению: она не может сама копироваться на

другие компьютеры, ничего не уничтожает и не изменяет в компьютере пользователя (кроме функций, которые нужны для ее запуска). Троян может прокрасться к ничего не подозревающему пользователю под видом ускорителя Интернета, очистителя дискового пространства, видеокодека, плагина к проигрывателю Winamp или исполняемого файла, имеющего двойное расширение.

> **Примечание**
>
> Хотя, в отличие от вируса, троянец не способен к саморазмножению, от этого он не становится менее опасным.

В последнем случае может прийти письмо с просьбой посмотреть фотографию и прикрепленным файлом вроде **superfoto.bmp.exe** (как вариант, после BMP может быть большое количество пробелов, чтобы пользователь ничего не заподозрил). В итоге получатель сам устанавливает вредоносную программу. Отсюда произошло название таких приложений: вспомните, как ахейцы захватили Трою. Город был хорошо укреплен, ахейцы долго не могли его взять и обманули защитников. Для жителей Трои конь был символом мира, и ахейцы, якобы для примирения, построили деревянную статую коня, внутрь которой посадили своих лучших воинов. Ничего не подозревающие троянцы затащили подарок в город, а ночью ахейцы вылезли из статуи, обезвредили стражу и открыли ворота, впустив основные силы.



Размножению троянской программы может способствовать сам пользователь, копируя его друзьям и коллегам. Возможен вариант, когда программа попадает на компьютер пользователя как червь, а далее работает как троян, обеспечивая создателю возможность дистанционного управления зараженным компьютером. Чаще всего такие программы все-таки относят к червям.

Запустившись, троянец располагается в памяти компьютера и отслеживает запрограммированные действия: крадет пароли для доступа в Интернет, обращается к сайтам, накру-

чивая чьи-то счетчики (за что пользователь платит лишним трафиком), звонит на платные, часто дорогие, телефонные номера, следит за действиями и привычками хозяина компьютера и читает его электронную почту.

Современные троянцы, как правило, уже не тащат все подряд. Они целенаправленно занимаются сбором конкретной информации. Например, «банковские» шпионы крадут номера кредитных карточек и других банковских данных. В связи с ростом популярности интернет-игр появился интерес к краже игровых предметов или персонажей, цена которых порой доходит до нескольких тысяч долларов, поэтому кража учетных записей для мошенников не менее привлекательна, чем кража банковских атрибутов.

Отдельно следует упомянуть Trojan-Downloader и Trojan-Dropper, которые используются для установки на компьютеры троянских, рекламных (adware) или порнографических (pornware) программ. Кроме того, троянцы часто используются для создания троянских прокси-серверов или даже целых зомбисетей для рассылки спама или вирусов.

Как определить, что в системе поселилась троянская программа? Во-первых, согласитесь, странно, когда только что установленный плагин к Winamp не обнаруживается в списке. Во-вторых, при инсталляции трояна может быть выведено сообщение, причем как об успешном окончании установки (вроде **Internet Exsplorer already patched**), так и, наоборот, говорящее о том, что утилита не установлена, потому

что системная библиотека несовместима с версией программы либо архив поврежден. Возможно, будут также выведены рекомендации по устранению ошибки. После долгих мучений пользователь вряд ли получит ожидаемый результат, скорее всего, оставит все попытки и будет пребывать в уверенности, что это полезная программа, которая просто не запустилась по непонятным причинам. Троянец тем временем пропишется в автозапуске. Например, в Windows необходимо быть внимательным к следующим веткам реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Runservices

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunservicesOnce

Возможно помещение ярлыка трояна в папку **Автозагрузка** (это встречается очень редко, так как присутствие вредоносной программы в этой папке легко обнаружить) или запись в файлы **autoexec.bat**, **win.ini**, **system.ini**. Часто разработчики принимают меры, чтобы трояна не было видно в окне **Диспетчер задач**, выводимом нажатием сочетания клавиш **Ctrl+Alt+Delete**. Наиболее сложные троянские программы умеют самостоятельно обновляться через Интернет, прятаться от антивирусов и расшифровывать файлы паро-

лей. Управлять троянцем можно несколькими способами – от прямого подключения к компьютеру до проверки определенного сетевого ресурса, на который хозяин посылает e-mail, ICQ и IRC-команды.

Часто троянец состоит из двух частей: клиентской, установленной у хозяина, и серверной, работающей на машине жертвы. Такие программы также называют backdoor (потайной ход). Запустив программу-клиент, злоумышленник проверяет, находится ли сервер в Сети: если отклик получен, то удаленным компьютером можно управлять как своим.

Учитывая неумение троянских программ распространяться самостоятельно, простым и эффективным правилом, позволяющим избежать заражения, является загрузка файлов только из надежных источников. Несмотря на то что, в отличие от вирусных эпидемий, о троянских эпидемиях пока еще никто не слышал, да и вряд ли услышит, учитывая неспособность этих программ к самостоятельному размножению, они не менее (а, возможно, даже более) опасны, чем вирусы. Ведь часто такие программы создаются для персонального использования, и поэтому сегодняшние антивирусы не могут знать обо всех них. Это означает, что пользователь может долгое время работать на зараженной машине, не подозревая об этом. Чтобы найти троянское приложение, требуются специальные утилиты и наблюдение за сетевой активностью компьютера с помощью штатных средств операционной системы и установленного брандмауэра, о чем бу-

дет подробнее рассказано в главе 4.

1.6. Новаторские подходы хакеров – руткиты (rootkits)

Если троянцы, о которых говорилось выше, можно обнаружить с помощью системных утилит, то представители этого класса вычисляются только с помощью специальных утилит.

Руткиты представляют собой более продвинутый вариант троянских коней. Некоторые антивирусные компании не разделяют руткиты и троянцы, относя их к одной категории зловредных программ. Однако троян прячется на компьютере, обычно маскируясь под известную программу (например, Spymaster выдавает себя за приложение MSN Messenger), а руткиты используют для маскировки более продвинутые методы, внедряясь глубоко в систему.

Изначально словом «руткит» обозначался набор инструментов, позволяющий злоумышленнику возвращаться во взломанную систему таким образом, чтобы системный администратор не мог его видеть, а система – регистрировать. Долгое время руткиты были привилегией Unix-систем, но, как известно, хорошие идеи просто так не пропадают, и в конце XX века стали массово появляться руткиты, предназначенные для Microsoft Windows. О руткитах заговорили, только когда на их использовании в своих продуктах была поймана фирма Sony. Сегодня эксперты предсказывают

бум этой технологии, и в ближайшие два-три года ожидается массовый рост количества руткитов – вплоть до 700 % в год. Самое печальное, что их будут использовать не только злоумышленники: руткиты станут массово применяться в коммерческих продуктах, в первую очередь для защиты от пиратства. Например, недавно было объявлено, что компания Microsoft создала руткит, обнаружить который невозможно. Не исключено, что это изобретение встретится в новых версиях Windows.

Конец ознакомительного фрагмента.