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.

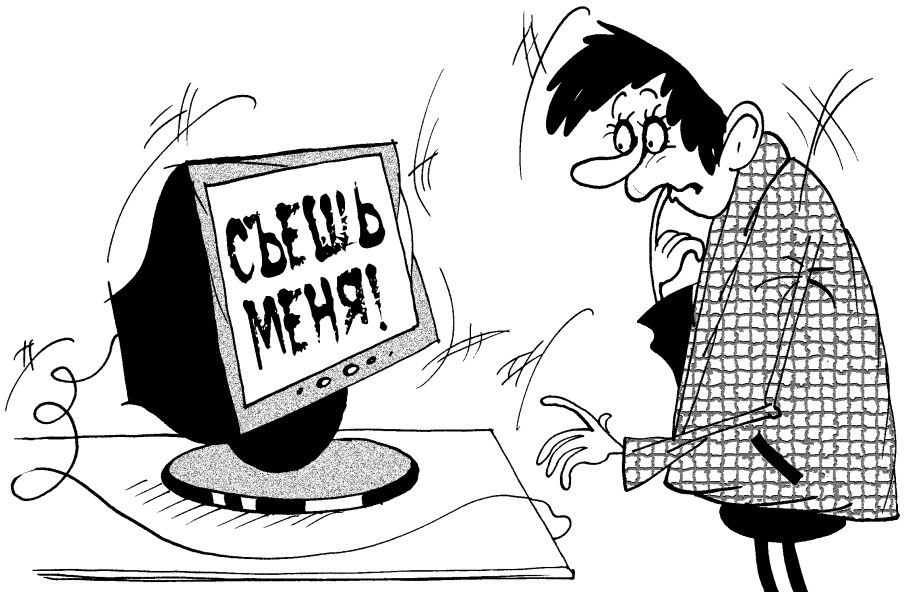
Компьютеры становились все доступнее. Со временем большинство платформ и операционных систем унифицировалось, на рынке стали преобладать Intel-совместимые компьютеры, которые работали под управлением операционной системы, разработанной компанией Microsoft. Дальнейшие события развивались с огромной скоростью. 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.

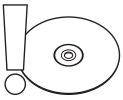
Сегодня общие годовые потери всех коммерческих организаций от действий вирусов могут сравниться с бюджетом небольшой страны, и эта сумма каждый год удваивается. Заявления некоторых специалистов по безопасности свидетельствуют о серьезности проблемы. По сведениям главы технологического департамента компании 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 Санкт-Петербургской 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 программированию. 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 вроде: «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.

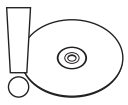
По среде обитания. Первая классификация относится к среде, в которой «живет» вирус.

- 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 различ-

ными 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.



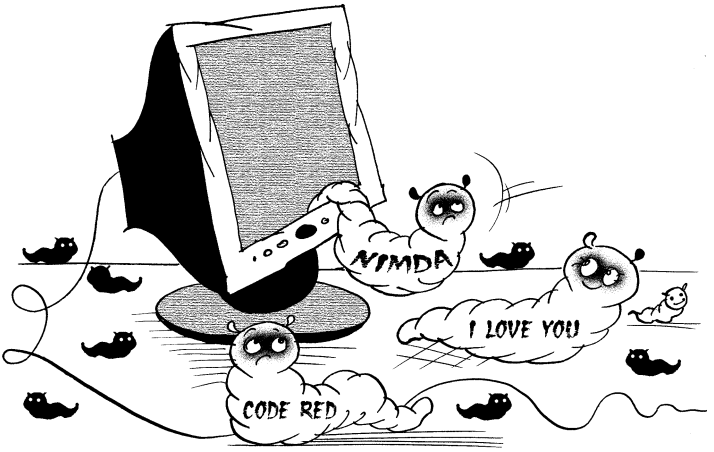
ВНИМАНИЕ

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.