**Вредоносное ПО**

В настоящее время известно более 5000 программных вирусов, их можно классифицировать по следующим признакам:

* среде обитания
* способу заражения среды обитания
* воздействию
* особенностям алгоритма

В зависимости от среды обитания вирусы можно разделить на сетевые, файловые, загрузочные и файлово-загрузочные. Сетевые вирусы распространяются по различным компьютерным сетям. Файловые вирусы внедряются главным образом в исполняемые модули, т. е. В файлы, имеющие расширения COM и EXE. Файловые вирусы могут внедряться и в другие типы файлов, но, как правило, записанные в таких файлах, они никогда не получают управление и, следовательно, теряют способность к размножению. Загрузочные вирусы внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record). Файлово-загрузочные вирусы заражают как файлы, так и загрузочные сектора дисков.

По способу заражения вирусы делятся на резидентные и нерезидентные. Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера. Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

неопасные, не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах

опасные вирусы, которые могут привести к различным нарушениям в работе компьютера

очень опасные, воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.

По особенностям алгоритма вирусы трудно классифицировать из-за большого разнообразия. Простейшие вирусы - паразитические, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены. Можно отметить вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии. Известны вирусы-невидимки, называемые стелс-вирусами, которые очень трудно обнаружить и обезвредить, так как они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Наиболее трудно обнаружить вирусы-мутанты, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов. Имеются и так называемые квазивирусные или «троянские» программы, которые хотя и не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Среди всего разнообразия вирусов можно выделить следующие основные группы:

* загрузочные
* файловые
* файлово-загрузочные

**Сетевые черви**  
В последнее время сетевые черви, пожалуй, потеряли свою популярность среди вирусописателей. Да и можно ли вообще активистов данного "движения" назвать настоящими создателями вирусов? Я думаю, что нет. Большинство этих людей — школьники или студенты, к которым в руки тем или иным путем попадают конструкторы троянских программ. А случаи появления по-настоящему достойных экземпляров червей, которые действительно исправно выполняли бы свои вредоносные функции, сведены к минимуму. Взять хотя бы бюллетень безопасности Лаборатории Касперского за первое полугодие 2006 г. (см. рис. 1). Из диаграммы хорошо видно, какая из групп вредоносного ПО преобладает. Ну да ладно, речь идет о сетевых червях. Сетевой червь — это вредоносный программный код, распространяющий свои копии по локальным или/и глобальным сетям с целью проникновения на компьютер-жертву, запуска своей копии на этом компьютере и дальнейшего распространения. Для распространения черви используют электронную почту, ISQ, P2P- и IRC-сети, LAN, сети обмена данными между мобильными устройствами. Большинство червей распространяются в файлах (вложение в письмо, ссылка на файл и т.д.). Но существуют и черви, которые распространяются в виде сетевых пакетов. Такие разновидности проникают непосредственно в память компьютера и сразу начинают действовать резидентно. Для проникновения на компьютер-жертву используются несколько путей: самостоятельный (пакетные черви), пользовательский (социальный инжиниринг), а также различные бреши в системах безопасности операционной системы и приложений. Некоторые черви обладают свойствами других типов вредоносного программного обеспечения (чаще всего это троянские программы). Теперь, пожалуй, поподробней на классах сетевых червей:

**Почтовые черви (Email-Worm).**Данный класс сетевых червей использует для распространения электронную почту. При этом червь отправляет жертве письмо с прикрепленным телом кода либо в письме присутствует ссылка на ресурс (естественно, зараженный). Для отправки сообщений червями используются следующие способы: прямое подключение к SMTP-серверу, используя встроенную в код червя почтовую библиотеку;  
использование сервисов MS Outlook;  
использование функций Windows MAPI.  
  
Для поиска адресов жертв чаще всего используется адресная книга MS Outlook, но может использоваться также адресная база WAB. Червь может просканировать файлы, хранящиеся на дисках, и выделить из них строки, относящиеся к адресам электронной почты. Черви могут отсылать свои копии по всем адресам, обнаруженным в почтовом ящике (некоторые обладают способностью отвечать на письма в ящике). Встречаются экземпляры, которые могут комбинировать способы.  
  
**Черви, использующие интернет-пейджеры (IM-Worm).**

Известные компьютерные черви данного типа используют единственный способ распространения — рассылку на обнаруженные контакты (из контакт-листа) сообщений, содержащих URL на файл, расположенный на каком-либо веб- сервере. Данный прием практически полностью повторяет аналогичный способ рассылки, использующийся почтовыми червями.  
  
**Черви в IRC-каналах (IRC-Worm).**

Черви этого класса используют два вида распространения: посылание пользователю URL-ссылки на файл-тело; отсылку пользователю файла (при этом пользователь должен подтвердить прием).  
  
**Черви для файлообменных сетей (P2P-Worm).**

Механизм работы большинства подобных червей достаточно прост: для внедрения в P2P-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине. Всю остальную работу по его распространению P2P-сеть берет на себя — при поиске файлов в сети она сообщит удаленным пользователям о данном файле и предоставит весь необходимый сервис для его скачивания с зараженного компьютера.  
  
Существуют более сложные P2P-черви, которые имитируют сетевой протокол конкретной файлообменной системы и положительно отвечают на поисковые запросы (при этом червь предлагает для скачивания свою копию).

**Прочие сетевые черви (NET-Worm).**

Существуют прочие способы заражения удаленных компьютеров — например:

* копирование червя на сетевые ресурсы;
* проникновение червя на компьютер через уязвимости в операционных системах и приложениях;
* проникновение в сетевые ресурсы публичного использования;
* паразитирование на других вредоносных программах.

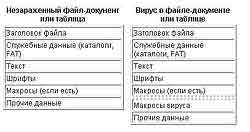
Используя первый способ, червь ищет в сети машины с ресурсами, открытыми на запись, и копирует. При этом он может случайным образом находить компьютеры и пытаться открыть доступ к ресурсам. Для проникновения вторым способом червь ищет компьютеры с установленным программным обеспечением, в котором имеются критические уязвимости. Таким образом, червь отсылает специально сформированный пакет (запрос), и часть червя проникает на компьютер, после чего загружает полный файл-тело и запускает на исполнение.  
  
**Классические вирусы**  
Когда профессионал говорит "вирус", он имеет в виду именно этот тип вредоносных программ. Вирусы, в отличие от червей, не пользуются сетевыми сервисами для распространения своих копий. Компьютерный вирус, как правило, попадает на компьютер-жертву по причинам, не зависящим от функционала кода. Обычно виноват пользователь, который не проверяет антивирусной программой информацию, попадающую на компьютер, в результате чего, собственно, и происходит заражение. Способов "подцепить" классический вирус довольно много:

* внешние носители информации;
* интернет ресурсы;
* файлы, распространяющиеся по сети (LAN, Internet).

Классический компьютерный вирус может иметь свойства других типов вредоносного ПО (например, троянскую процедуру удаления информации на диске). Вирусы делятся на классы по среде обитания, а эти классы, в свою очередь, делятся на подклассы по способу заражения. Итак, по среде обитания вирусы делятся на файловые, загрузочные, макро- и скриптовые. Файловые вирусы для заражения пользуются файловой системой ОС. Они различными способами внедряются в исполняемые файлы, создают файлы-двойники и т.д.  
  
**Перезаписывающие вирусы (Overwriting).**

Самый распространенный способ заражения. Вирус переписывает код программы (заменяет его своим), после чего, естественно, файл перестает работать. Файл, зараженный данным способом, восстановлению не подлежит. Перезаписывающий вирус быстро обнаруживает себя, так как зараженная система (или программа) перестает функционировать.  
  
**Паразитические вирусы (Parasitic).**

К таковым относятся все вирусы, которые изменяют содержимое файла, но при этом оставляют его работоспособным. Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (prepending), в конец файлов (appending) и в середину файлов (inserting). В свою очередь, внедрение вирусов в середину файлов происходит различными методами — путем переноса части файла в его конец или копирования своего кода в заведомо неиспользуемые данные файла (cavity-вирусы). При записывании кода в начало файла вирус может воспользоваться двумя способами. Первый — это перенос начала файла в конец и дописывание собственного кода в освободившееся место. Второй — дописывание кода файла к своему коду. В обоих случаях при запуске файла управление получает вирус, а потом во избежание подозрений управление передается обратно файлу-жертве. При внедрении кода вируса в конец файла используется способ дописывания. Код вируса дописывается в конец файла- жертвы, при этом головная часть файла изменяется таким образом, что управление, опять же, первым получает вирус, ну, а потом файл. При внедрении в середину файла вирус может воспользоваться несколькими вариантами. Первый — перенос части файла, вместо которой предполагается расположить код вируса, в конец. Второй — так называемое "раздвижение" кода файла. Третий — замещение неисполняемых областей файла кодом вируса. Но каким бы из способов вирус ни воспользовался, ему опять придется изменять головную часть файла-жертвы. Изменение головной части кода файла происходит двумя способами. Наиболее распространен способ, при котором вирус точку входа, "перенося" ее на принадлежащий ему участок. Но некоторые могут просто добавить команду передачи управления — таким образом, файл стартует с оригинальной точки входа, а потом (по дописанной команде) передает управление коду вируса.  
  
**Вирусы-компаньоны (Companion).**

Данный способ подразумевает создание файла-двойника, при этом код файла-жертвы не изменяется. Обычно вирус изменяет расширение файла (например, с .exe на .com), потом создает свою копию с именем, идентичным имени файла-жертвы, и дает ему расширение, тоже идентичное. Ничего не подозревающий пользователь запускает любимую программу и не подозревает, что это вирус. Вирус, в свою очередь, заражает еще несколько файлов и запускает программу, затребованную пользователем.  
  
Существуют и еще способы заражения, но они настолько редко встречаются, что мы остановимся только на их перечислении: вирусы, заражающие объектные модули (OBJ); вирусы, заражающие библиотеки компиляторов (LIB); вирусы, заражающие исходные тексты программ. Известные на текущий момент загрузочные вирусы заражают загрузочный сектор гибкого диска и boot-сектор или Master Boot Record (MBR) винчестера. Принцип действия загрузочных вирусов основан на алгоритмах запуска операционной системы при включении или перезагрузке компьютера — после необходимых тестов установленного оборудования (памяти, дисков и т.д.) программа системной загрузки считывает первый физический сектор загрузочного диска (A:, C: или CD-ROM в зависимости от параметров, установленных в BIOS Setup) и передает на него управление. При заражении дисков загрузочные вирусы "подставляют" свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков во всех вышеописанных способах: вирус "заставляет" систему при ее перезапуске считать в память и отдать управление не оригинальному коду загрузчика, а коду вируса. Заражение дискет производится единственным известным способом — вирус записывает свой код вместо оригинального кода boot-сектора дискеты. Винчестер заражается тремя возможными способами: вирус записывается либо вместо кода MBR, либо вместо кода boot-сектора загрузочного диска (обычно диска C:), либо модифицирует адрес активного boot-сектора в таблице разделов диска (Disk Partition Table), расположенной в MBR винчестера. При инфицировании диска вирус в большинстве случаев переносит оригинальный boot-сектор (или MBR) в какой-либо другой сектор диска (например, в первый свободный). Если длина вируса больше длины сектора, то в заражаемый сектор помещается первая часть вируса, остальные части размещаются в других секторах (например, в первых свободных). Макровирусы в основном заражают документы MS Office. При этом вирус добавляет свой код в область макросов документа. Расположение кода вируса в документах разных приложений вышеописанного пакета разное, поэтому представить его можно только лишь схематично (см. рис. 2). Скрипт-вирусы — это вирусы, написанные на скрипт-языках (VBS, JS, BAT, PHP и т.д.). Заражают они файлы довольно большого диапазона расширений: от .exe до .html.