ВИРУСЫ

Классификация вирусов

Известные программные вирусы 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;
- файлово-загрузочные.

Сетевые вирусы распространяются по различным компьютерным сетям. К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Сетевые вирусы прошлого распространялись в компьютерной сети и, как правило, так же как и компаньон-вирусы, не изменяли файлы или сектора на дисках. Они проникали в память компьютера из компьютерной сети, вычисляли сетевые адреса других компьютеров и рассылали по этим адресам свои копии. Эти вирусы иногда также 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, а «задние двери» закрыты. В результате за последние десять лет не было зафиксировано ни одного случая заражения сетевым вирусом, как, впрочем, не появилось и ни одного нового сетевого вируса.

«Macro.Word.ShareFun» - использует возможности электронной почты Microsoft Mail - он создает новое письмо, содержащее зараженный файл-документ («ShareFun» является макро-вирусом), затем выбирает из списка адресов MS-Mail три случайных адреса и рассылает по ним зараженное письмо. Поскольку многие пользователи устанавливают параметры MS-Mail таким образом, что при получении письма автоматически запускается MS Word, то вирус «автоматически» внедряется в компьютер адресата зараженного письма.

Второй вирус («Homer») использует для своего распространения протокол FTP (File Trabsfer Protocol) и передает свою копию на удаленный ftp-сервер в каталог Incoming. Поскольку сетевой протокол FTP исключает возможность запуска файла на удаленнов сервере, этот вирус можно охарактеризовать как «полу-сетевой», однако это реальный пример возможностей вирусов по использованию современных сетевых протоколов и поражению глобальных сетей.

Файловые вирусы внедряются главным образом в исполняемые модули, т. е. в файлы, имеющие расширения COM и EXE. Они 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. В отличие от загрузочных вирусов, которые практически всегда резидентны, файловые вирусы не обязательно резидентны. Областью обитания файловых вирусов являются файлы. Если файловый вирус не резидентный, то при запуске инфицированного исполняемого файла вирус записывает свой код в тело программного файла таким образом, что при запуске программы вирус первым получает управление. Произведя некоторые действия, вирус передает управление зараженной программе.

При запуске вирус сканирует локальные диски компьютера и сетевые каталоги в поисках нового объекта для заражения. После того как подходящий программный файл будет найден, вирус записывает в него свой код, чтобы получить управление при запуске этого файла.

Если файловый вирус резидентный, то он установится в память и получит возможность заражать файлы и проявлять прочие способности не только во время работы зараженного файла.

Относительно новой разновидностью файлового вируса является макрокомандный вирус, распространяющийся с документами офисных приложений, таких как Microsoft Word for Windows или Microsoft Excel for Windows.

Механизм распространения макрокомандных вирусов основан на том, что существуют макрокоманды, которые запускаются при открывании документа для редактирования или при выполнении других операций. При этом вирус получит управление и может заразить другие документы, хранящиеся на дисках. Если вирусная макрокоманда имеет имя File Save As, то распространение вируса будет происходить при сохранении документа.

Для предотвращения заражения макрокомандными вирусами необходимо перед просмотром или редактированием проверять новые файлы документов с помощью антивирусных программ, способных искать такие вирусы.

Загрузочные вирусы.

Вторая большая группа вирусов - это так называемые загрузочные вирусы. Распространение и активизация этих вирусов происходит в момент загрузки операционной системы, еще до того, как пользователь успел запустить какую-либо антивирусную программу.

Сразу после включения электропитания компьютера начинает работать программа инициализации, записанная в ПЗУ базовой системы ввода/вывода BIOS. Эта программа проверяет оперативную память и другие устройства компьютера, а затем передает управление программе начальной загрузки, которая также находится в BIOS.

Загрузка операционной системы является многоступенчатым процессом, ход которого зависит от разных обстоятельств. В этом процессе задействовано три программы, которые служат объектом нападения загрузочных вирусов:

главная загрузочная запись;

загрузочная запись на логическом диске;

загрузочная запись на дискете.

Вирусы могут заменять некоторые или все перечисленные выше объекты, встраивая в них свое тело и сохраняя содержимое оригинального загрузочного сектора в каком-либо более или менее подходящем для этого месте на диске компьютера.

В результате при включении компьютера программа загрузки, расположенная в BIOS, загружает в память вирусный код и передает ему управление. Дальнейшая загрузка операционной системы происходит под контролем вируса, что затрудняет, а в некоторых случаях и исключает его обнаружение антивирусными программами. Загрузочные вирусы заражают загрузочный (boot) сектор флоппи-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.

Файлово–загрузочные вирусы.

Существует большое количество сочетаний - например, файлово-загрузочные вирусы, заражающие как файлы, так и загрузочные сектора дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют стелс и полиморфик-технологии

По способу заражения среды обитания вирусы делятся на две группы:

- резидентные
- нерезидентные.

Под термином "***резидентность***" (DOS'овский термин TSR - Terminate and Stay Resident) понимается способность вирусов оставлять свои копии в системной памяти, перехватывать некоторые события (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов). Таким образом, резидентные вирусы активны не только в момент работы зараженной программы, но и после того, как программа закончила свою работу. Резидентные копии таких вирусов остаются жизнеспособными вплоть до очередной перезагрузки, даже если на диске уничтожены все зараженные файлы. Часто от таких вирусов невозможно избавиться восстановлением всех копий файлов с дистрибутивных дисков или backup-копий. Резидентная копия вируса остается активной и заражает вновь создаваемые файлы. То же верно и для загрузочных вирусов — форматирование диска при наличии в памяти резидентного вируса не всегда вылечивает диск, поскольку многие резидентные вирусы заражает диск повторно после того, как он отформатирован.

Нерезидентные вирусы, напротив, активны довольно непродолжительное время — только в момент запуска зараженной программы. Для своего распространения они ищут на диске незараженные файлы и записываются в них. После того, как код вируса передает управление программе-носителю, влияние вируса на работу операционной системы сводится к нулю вплоть до очередного запуска какой-либо зараженной программы. Поэтому файлы, зараженные нерезидентными вирусами значительно проще удалить с диска и при этом не позволить вирусу заразить их повторно.

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.
- Вирусы-репликаторы, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.
- 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 (полиморфные вирусы), 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.

Макровирусы.

Весьма оригинальный класс вирусов (хотя вирусами в полном смысле этого слова их даже нельзя назвать), заражающий документы, в которых предусмотрено выполнение макрокоманд. При открытии таких документов вначале исполняются макрокоманды (специальные программы высокого уровня), содержащиеся в этом документе, - макровирус как раз и представляет собой такую макрокоманду. Таким образом, как только будет открыт зараженный документ, вирус получит управление и совершит все вредные действия (в частности, найдет и заразит еще не зараженные документы).

Полиморфные вирусы.

Этот вид компьютерных вирусов представляется на сегодняшний день наиболее опасным.

Полиморфные вирусы - вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

Такие вирусы не только шифруют свой код, используя различные пути шифрования, но и содержат код генерации шифровщика и расшифровщика, что отличает их от обычных шифровальных вирусов, которые также могут шифровать участки своего кода, но имеют при этом постоянный код шифровальщика и расшифровщика.

Полиморфные вирусы - это вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: сделать невозможным проанализировать код вируса с помощью обычного дизассемблирования, даже имея зараженный и оригинальный файлы. Этот код зашифрован и представляет собой бессмысленный набор команд. Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку в ходе работы, может вновь шифровать уже отработавшие участки. Все это делается ради затруднения анализа кода вируса.

Стелс-вирусы.

В ходе проверки компьютера антивирусные программы считывают данные - файлы и системные области с жестких дисков и дискет, пользуясь средствами операционной системы и базовой системы ввода/вывода BIOS. Ряд вирусов, после запуска оставляют в оперативной памяти компьютера специальные модули, перехватывающие обращение программ к дисковой подсистеме компьютера. Если такой модуль обнаруживает, что программа пытается прочитать зараженный файл или системную область диска, он на ходу подменяет читаемые данные, как будто вируса на диске нет.

Стелс-вирусы обманывают антивирусные программы и в результате остаются незамеченными. Тем не менее, существует простой способ отключить механизм маскировки стелс-вирусов. Достаточно загрузить компьютер с не зараженной системной дискеты и сразу, не запуская других программ с диска компьютера (которые также могут оказаться зараженными), проверить компьютер антивирусной программой.

При загрузке с системной дискеты вирус не может получить управление и установить в оперативной памяти резидентный модуль, реализующий стелс-механизм. Антивирусная программа сможет прочитать информацию, действительно записанную на диске, и легко обнаружит вирус.

Вирусы-призраки.

Вирусы-призраки маскируются с помощью другого механизма. Эти вирусы постоянно модифицируют себя таким образом, что не содержат одинаковых фрагментов. Такие вирусы хранят свое тело в закодированном виде и постоянно меняют параметры этой кодировки. Стартовая же часть, занимающаяся декодированием непосредственно самого тела, может генерироваться весьма сложным способом. При переносе вируса данного типа с компьютера на компьютер код вируса изменяется таким образом, что уже не имеет ничего общего со своим предыдущим вариантом.

А часть вирусов может самомодифицироваться и в пределах одного компьютера. Обнаружение таких вирусов весьма затруднено, хотя часть антивирусных программ пытается находить их по участкам кода, характерным для стартовой части.

Компаньон – вирусы.

Компаньон - вирусы (companion) - это вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для EXE-файлов файлы-спутники, имеющие то же самое имя, но с расширением .COM, например, для файла XCOPY.EXE создается файл XCOPY.COM. Вирус записывается в COM-файл и никак не изменяет EXE-файл. При запуске такого файла DOS первым обнаружит и выполнит COM-файл, т.е. вирус, который затем запустит и EXE-файл.

Вирусы-«черви».

Вирусы–«черви» (worm) - вирусы, которые распространяются в компьютерной сети и, так же как и компаньон - вирусы, не изменяют файлы или сектора на дисках. Они проникают в память компьютера из компьютерной сети, вычисляют сетевые адреса других компьютеров и рассылают по этим адресам свои копии. Такие вирусы иногда создают рабочие файлы на дисках системы, но могут вообще не обращаться к ресурсам компьютера (за исключением оперативной памяти).

Студенческие вирусы.

Студенческие вирусы являются самыми примитивными и элементарными, потому что эти вирусы пишутся ради забавы или от нечего делать студентами, которые только что научились их писать и решили попробовать свои силы. Но также есть исключения, например такой вирус как «Чернобыль» написан самым обычным студентом. Но такие исключения очень редки.

Троянские кони, программные закладки и сетевые черви.

Троянский конь – это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания. Обычно такие программы маскируются под какие-нибудь полезные утилиты. Вирусы могут нести в себе троянских коней или "троянизировать" другие программы – вносить в них разрушающие функции.

«Троянские кони» представляют собой программы, реализующие помимо функций, описанных в документации, и некоторые другие функции, связанные с нарушением безопасности и деструктивными действиями. Отмечены случаи создания таких программ с целью облегчения распространения вирусов. Списки таких программ широко публикуются в зарубежной печати. Обычно они маскируются под игровые или развлекательные программы и наносят вред под красивые картинки или музыку.

В качестве примера приведем возможные деструктивные функции, реализуемые «троянскими конями» и программными закладками:

1. Уничтожение информации. Конкретный выбор объектов и способов уничтожения зависит только от фантазии автора такой программы и возможностей ОС. Эта функция является общей для троянских коней и закладок.

2. Перехват и передача информации. В качестве примера можно привести реализацию закладки для выделения паролей, набираемых на клавиатуре.

3. Целенаправленная модификация кода программы, интересующей нарушителя. Как правило, это программы, реализующие функции безопасности и защиты.

Если вирусы и «троянские кони» наносят ущерб посредством лавинообразного саморазмножения или явного разрушения, то основная функция вирусов типа «червь», действующих в компьютерных сетях, – взлом атакуемой системы, т.е. преодоление защиты с целью нарушения безопасности и целостности.

В более 80% компьютерных преступлений, расследуемых ФБР, "взломщики" проникают в атакуемую систему через глобальную сеть Internet. Когда такая попытка удается, будущее компании, на создание которой ушли годы, может быть поставлено под угрозу за какие-то секунды.

Этот процесс может быть автоматизирован с помощью вируса, называемого сетевой червь.

Червями называют вирусы, которые распространяются по глобальным сетям, поражая целые системы, а не отдельные программы. Это самый опасный вид вирусов, так как объектами нападения в этом случае становятся информационные системы государственного масштаба. С появлением глобальной сети Internet этот вид нарушения безопасности представляет наибольшую угрозу, т. к. ему в любой момент может подвергнуться любой из 40 миллионов компьютеров, подключенных к этой сети.

Признаки появления вирусов.

При заражении компьютера вирусом важно его обнаружить. Для этого следует знать об основных признаках проявления вирусов. К ним можно отнести следующие:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размеров файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;
- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- частые зависания и сбои в работе компьютера.

Следует отметить, что вышеперечисленные явления необязательно вызываются присутствием вируса, а могут быть следствием других причин. Поэтому всегда затруднена правильная диагностика состояния компьютера.

Антивирусные программы

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать вирусы. Такие программы называются антивирусными. Различают следующие виды антивирусных программ:

- программы-детекторы;
- программы-доктора или фаги;
- программы-ревизоры;
- программы-фильтры;
- программы-вакцины или иммунизаторы.

Программы-детекторы осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

Программы-доктора или фаги, а также программы-вакцины не только находят зараженные вирусами файлы, но и «лечат» их, т.е. удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние. В начале своей работы фаги ищут вирусы в оперативной памяти, уничтожая их, и только затем переходят к «лечению» файлов. Среди фагов выделяют полифаги, т.е. программы-доктора, предназначенные для поиска и уничтожения большого количества вирусов. Наиболее известные из них: AVP, Aidstest, Scan, Norton AntiVirus, Doctor Web.

Программы-ревизоры относятся к самым надежным средствам защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов и системных областей диска тогда, когда компьютер не заражен вирусом, а затем периодически или по желанию пользователя сравнивают текущее состояние с исходным. Обнаруженные изменения выводятся на экран монитора. Как правило, сравнение состояний производят сразу после загрузки операционной системы. При сравнении проверяются длина файла, код циклического контроля (контрольная сумма файла), дата и время модификации, другие параметры. Программы-ревизоры имеют достаточно развитые алгоритмы, обнаруживают стелс-вирусы и могут даже очистить изменения версии проверяемой программы от изменений, внесенных вирусом. К числу программ-ревизоров относится широко распространенная в России программа Adinf.

Программы-фильтры или «сторожа» представляют собой небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов. Такими действиями могут являться:

- попытки коррекции файлов с расширениями COM, EXE;
- изменение атрибутов файла;
- прямая запись на диск по абсолютному адресу;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

При попытке какой-либо программы произвести указанные действия «сторож» посылает пользователю сообщение и предлагает запретить или разрешить соответствующее действие. Программы-фильтры весьма полезны, так как способны обнаружить вирус на самой ранней стадии его существования до размножения. Однако, они не «лечат» файлы и диски. Для уничтожения вирусов требуется применить другие программы, например фаги.

Вакцины или иммунизаторы - это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, «лечащие» этот вирус. Вакцинация возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится. В настоящее время программы-вакцины имеют ограниченное применение.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на каждом компьютере позволяют избежать распространения вирусной эпидемии на другие компьютеры.

Главным оружием в борьбе с вирусами являются антивирусные программы. Они позволяют не только обнаружить вирусы, в том числе вирусы, использующие различные методы маскировки, но и удалить их из компьютера.

Существует несколько основополагающих **методов поиска вирусов**, которые применяются антивирусными программами:

- Сканирование;
- Эвристический анализ;
- Обнаружение изменений;
- Резидентные мониторы.

Антивирусные программы могут реализовывать все перечисленные выше методики, либо только некоторые из них.

Сканирование является наиболее традиционным методом поиска вирусов. Оно заключается в поиске сигнатур, выделенных из ранее обнаруженных вирусов. Антивирусные программы-сканеры, способные удалить обнаруженные вирусы, обычно называются полифагами.

Недостатком простых сканеров является их неспособность обнаружить полиморфные вирусы, полностью меняющие свой код. Для этого необходимо использовать более сложные алгоритмы поиска, включающие эвристический анализ проверяемых программ.

Кроме того, сканеры могут обнаружить только уже известные и предварительно изученные вирусы, для которых была определена сигнатура. Поэтому программы-сканеры не защитят ваш компьютер от проникновения новых вирусов, которых, кстати, появляется по несколько штук в день. Как результат, сканеры устаревают уже в момент выхода новой версии.

Эвристический анализ зачастую используется совместно со сканированием для поиска шифрующихся и полиморфных вирусов. В большинстве случаев эвристический анализ позволяет также обнаруживать и ранее неизвестные вирусы. В этом случае, скорее всего их лечение будет невозможно.

Если эвристический анализатор сообщает, что файл или загрузочный сектор, возможно, заражен вирусом, вы должны отнестись к этому с большим вниманием. Необходимо дополнительно проверить такие файлы с помощью самых последних версий антивирусных программ сканеров или передать их для исследования авторам антивирусных программ.

Обнаружение изменений.

Заражая компьютер, вирус делает изменения на жестком диске: дописывает свой код в заражаемый файл, изменяет системные области диска и т. д. На обнаружении таких изменений основываются работа антивирусных программ-ревизоров.

Антивирусные программы-ревизоры запоминают характеристики всех областей диска, которые могут подвергнутся нападению вируса, а затем периодически проверяют их. В случае обнаружения изменений, выдается сообщение о том, что возможно на компьютер напал вирус.

Резидентные мониторы.

Антивирусные программы, постоянно находящиеся в оперативной памяти компьютера и отслеживающие все подозрительные действия, выполняемые другими программами, носят название резидентных мониторов или сторожей. К сожалению, резидентные мониторы имеют очень много недостатков, которые делают этот класс программ малопригодными для использования. Они раздражают пользователей большим количеством сообщений, по большей части не имеющим отношения к вирусному заражению, в результате чего их отключают.

Основные меры по защите от вирусов

Для того, чтобы не подвергнуть компьютер заражению вирусами и обеспечить надежное хранение информации на дисках, необходимо соблюдать следующие правила:

- оснастить компьютер современными антивирусными программами, например AVP, Aidstest, Doctor Web, и постоянно обновлять их версии;
- перед считыванием с дискет информации, записанной на других компьютерах, всегда проверять эти дискеты на наличие вирусов, запуская антивирусные программы;
- при переносе на компьютер файлов в архивированном виде проверять их сразу же после разархивации на жестком диске, ограничивая область проверки только вновь записанными файлами;
- периодически проверять на наличие вирусов жесткие диски компьютера, запуская антивирусные программы для тестирования файлов, памяти и системных областей дисков с защищенной от записи дискеты, предварительно загрузив операционную систему с защищенной от записи системной дискеты;
- всегда защищать дискеты от записи при работе на других компьютерах, если на них не будет производится запись информации;
- обязательно делать архивные копии на дискетах ценной информации;
- не оставлять в кармане дисковода А дискеты при включении или перезагрузке операционной системы, чтобы исключить заражение компьютера загрузочными вирусами;

- использовать антивирусные программы для входного контроля всех исполняемых файлов, получаемых из компьютерных сетей;
- для обеспечения большей безопасности применения Aidstest и Doctor Web необходимо сочетать с повседневным использованием ревизора диска Adinf, либо использовать полный комплект антивируса AVP.