Московский Физико-Технический Институт
Факультет Радиотехники и Кибернетики

Классификация вирусов. Методы обнаружения.

Предмет: Защита информации
Автор: Аксёнова О.Ю., студентка 016 гр.

2004 г.

Введение

В настоящее время в связи с массовым применением компьютеров в самых различных областях появилось огромное количество компьютерных вирусов, то есть программ, способных исказить или уничтожить информацию, хранящуюся в компьютере, разрушить файловую структуру дисков или просто попортить нервы пользователю. Известно больше 5000 компьютерных вирусов, и их число постоянно растет. Известны случаи, когда вирусы блокировали работу целых организаций. Сейчас существуют аппаратные и программные средства защиты от вирусов, но, к сожалению, они не дают полной защиты. Очень часто знания пользователей (иногда и программистов) о вирусах очень поверхностны, а необходимые навыки полностью отсутствуют.

Основным свойством вируса является его способность к самовоспроизведению. Но кроме вирусов такой особенностью обладают многие вполне мирные программы (например, операционная система). Кроме того, вирус должен каким-либо образом обеспечить передачу управления себе для того, чтобы выполнить свою основную задачу.

Что такое «компьютерный вирус»

Попробуем дать определение компьютерного вируса. Если сказать, что вирус – это скрытая программа, способная к самовоспроизведению, внедрению в другие объекты, самораспространению и потенциально опасная, то для каждого из перечисленных свойств (пожалуй, кроме последнего) можно найти контрпример (либо мирную программу, обладающую таким свойством, либо вирус без него).

Например, способность самовоспроизведения характерна для многих операционных систем. Кроме вирусов файлы могут быть удалены многими обычными программами, а некоторые вирусы в принципе не занимаются ничем подобным.

Получается, что точно определить характерные особенности вирусов невозможно.

Необходимым свойством вируса можно назвать его способность к самовоспроизведению, то есть способность создавать жизнеспособные копии себя самого, возможно, не имеющие совпадающих участков кода. Но следует помнить, что кроме вирусов таким свойством обладают хотя бы те же операционные системы. Правда, в отличие от них, вирус не является самодостаточным, для «жизни» ему необходимо использовать информацию о файловой структуре дисков, сами файлы, программы или хотя бы их имена.

Классификация вирусов

Вирусы можно разделить на классы по следующим признакам:

- среда обитания;
- операционная система (ОС);
- особенности алгоритма работы;
- деструктивные возможности.

Рассмотрим классификацию по первому признаку – среде обитания:

- *сетевые вирусы* распространяются через электронную почту или команды и протоколы компьютерных сетей
- *файловые вирусы* чаще всего "живут" в выполняемых файлах
- *загрузочные вирусы* заражают загрузочный сектор либо меняют указатель на активный boot-сектор
- *макро-вирусы* внедряются в документы и редакторы

Некоторые сложные вирусы, использующие, например, полиморфик-технологии, могут "обитать" в нескольких типах сред. Примером может служить макро-вирус. Он распространяется по электронной почте и заражает редактируемые документы.

Так как вирус должен «жить» в какой-либо определенной операционной системе, то можно выделить вирусы, заражающие файлы и программы одной (или нескольких) из существующих ОС – DOS, Windows, Linux, OS/2 и т.д. Например, макро-вирусы под Windows заражают файлы Word, Excel, Office97. Загрузочные вирусы тоже ориентированы на конкретное расположение системных данных в загрузочных секторах. Теоретически возможна ОС, совершенно защищенная от вирусов (например, ОС, в которой запрещены какие-либо изменения исполняемых файлов), но такой ОС пока не создано.

По особенностям алгоритма работы можно выделить следующие разделы:

- способ заражения;
- использование стелс-алгоритмов;
- самошифрование и полиморфичность;
- использование нестандартных приемов.

По способу заражения вирусы можно разделить на резидентные и нерезидентные.

Резидентный вирус после проникновения в компьютер записывает в оперативную память специальную программу (резидентная часть). Это программа-перехватчик для обращений операционной системы к каким-то определенным объектам (загрузочным секторам дисков, редактируемым документам и т. п.). После получения такого обращения программа внедряется в данный объект. Удалить резидентные вирусы из оперативной памяти можно только с помощью перезагрузки компьютера. К резидентным также следует отнести, например, макро-вирусы, поскольку они активны, пока работает редактор, и удаляются из памяти после выхода из него. Если вирус оставляет в памяти резидентную программу, но эта программа его не распространяет, его считают нерезидентным.

Обычно *нерезидентным* называют вирус, который оперативную память не заражает и активен только в течение некоторого ограниченного времени после появления.

При использовании стелс-алгоритмов вирус может полностью или частично скрыть себя в системе. Такие вирусы очень трудно обнаружить, так как они перехватывают обращения ОС к зараженным объектам и подставляют вместо себя незараженные участки диска. Один из первых файловых стелс-вирусов – вирус «Frodo», первый загрузочный стелс-вирус – «Brain».

Очень многими вирусами используются самошифрование и полиморфичность. Это делается для усложнения процедуры детектирования вируса. Эти вирусы довольно трудно обнаружить, так как они содержат алгоритмы шифровки-расшифровки, вследствие чего копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов.

Кроме того, для проникновения в ОС, защиты обнаружения и затруднения лечения в вирусах используются различные нестандартные приемы.

По деструктивным возможностям вирусы можно разделить на:

- *безвредные*, т.е. совершенно не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске);
- *неопасные*, влияние которых ограничивается уменьшением свободной памяти на диске и различными эффектами (графическими, звуковыми и т.д.);
- *опасные*, которые способны привести к серьезным сбоям в работе компьютера;
- *очень опасные*, в алгоритм работы которых заведомо заложены процедуры, приводящие к потере программ, уничтожению различных данных и т.д..

Даже если вирус не имеет опасных процедур, он является программой, следовательно, может содержать непредсказуемые и порой катастрофические ошибки. Например, до сих пор попадаются вирусы, определяющие «COM или EXE» не по внутреннему формату файла, а по его расширению. Разумеется, при несовпадении формата и расширения имени зараженный файл становится неработоспособным. На новой версии операционной системы вирус может просто «заклинить». И так далее.

Способы противодействия

Основные способы противодействия:

- *профилактика заражения*
- *обезвреживание известного вируса*
- *обезвреживание неизвестного вируса*

Очень часто для этой цели используются различные антивирусные программы.

Кто-то написал вирус, и он пошел гулять по сети. Через некоторое время кто-то заподозрит что-нибудь неладное. Чаще всего это обычный пользователь, который заметил какие-то странности в поведении компьютера. Потом вирус попадает к специалистам. Они изучат его, соберут о нем всю необходимую информацию (способ распространения и заражения, сигнатура – характерные участки кода, заражаемые объекты и т.д.). Эта информация позволяет выяснить способы обнаружения и обезвреживания вируса (если это возможно).

Признаки появления вирусов

Необходимо знать основные признаки проявления вирусов:

- прекращение работы или неправильная работа программ, которые раньше нормально работали
- медленная работа компьютера
- невозможность загрузки ОС
- исчезновение или искажение файлов и каталогов
- 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

Эти явления не обязательно вызываются вирусом, а могут быть следствием других причин. Поэтому правильная диагностика состояния компьютера всегда затруднена.

Обнаружение вирусов и меры по защите и профилактике

Во-первых, не стоит паниковать. Это не приведет ни к чему хорошему. Вирус не способен нанести столько ущерба, сколько перепуганный пользователь. К тому же вирусное заражение не самое плохое, что может случиться с компьютером.

Если есть подозрение, что в системе "поработал" вирус, но не удается обнаружить какие-либо очевидные изменения файлов или загрузочных секторов дисков, то с большой вероятностью можно сказать, что в компьютер попал стелс-вирус. Чтобы избавиться от него, нужно загрузить DOS с незараженной дискеты и лечить нерезидентный вирус. Если же такой возможности нет, то следует нейтрализовать его резидентную часть.

Обнаружение загрузочного вируса

Обычно в загрузочных секторах дисков расположены небольшие программы, определяющие размеры и границы логических дисков или загружающие операционную систему.

Чтобы обнаружить загрузочный вирус, который "поработал" с этими программами, надо для начала прочитать содержимое подозреваемого сектора. Для этого можно использовать DISKEDIT из «Нортоновских утилит» или AVPUTIL из профессионального комплекта AVP.

Некоторые вирусы загрузочного типа дописывают или удаляют характерные текстовые строки, например, имена системных файлов или сообщения об ошибках.

Подозрение на вирус должно вызывать изменение или отсутствие строки-заголовка boot-сектора – строки, содержащей номер версии DOS или название фирмы-производителя программного обеспечения, например, "MSDOS5.0" или "MSWIN4.0". Систем Windows95/NT это не касается: они записывают в заголовок загрузочных секторов дискет случайные строки текста. Многие вирусы дописывают достаточное количество информации, что можно обнаружить по увеличению длины кода. К примеру, известно, что загрузчик MS-DOS, расположенный в MBR, должен занимать меньше половины сектора. Эта информация дает возможность обнаружить заражение MBR винчестера.

Вирусы не всегда изменяют тесктовые строки загрузочного сектора. Обнаружить его можно с помощью дискеты, на которую в виде файла на незараженном компьютере записан ее boot-сектор. Наличие изменений в этом файле после работы с файлами на предположительно зараженном компьютере подтвердит присутствие вируса.

Чтобы "поймать" вирусы с еще более сложными алгоритмами, может понадобиться детальное исследование кода загрузочного сектора и анализ его работы. Сложность состоит в том, что вирус может изменить, например, всего лишь 3 байта Disk Partition Table – адрес активного загрузочного сектора.

Обнаружение файлового вируса

Сначала рассмотрим поражение системы нерезидентным вирусом (это более простой случай). Такой вирус начинает свою работу при запуске зараженной программы, а по завершении своих действий передает управление ей, и потом совершенно на нее не влияет. Чтобы обнаружить такой вирус, надо сравнить длины файлов в дистрибутиве и на диске, либо сравнить эти файлы побайтно. Во многих вирусах есть характерные строки: ".COM", "*.COM", ".EXE", "*.EXE", "*.*", "MZ", "COMMAND" и т.д. Эти строки часто встречаются в начале или в конце зараженных файлов и помогают обнаружить вирус. Кроме того, многие типы файлов имеют вполне определенную структуру, отступления от которой также позволяют обнаружить заражение. Например, в выполняемых файлах Windows и OS/2 сначала идут сегменты кода, потом сегменты данных. Если за сегментом данных идет еще один сегмент кода, то это может служить сигналом о наличии вируса.

Тем, кто знаком с Ассемблером, можно попробовать разобраться в кодах подозрительных программ. Для быстрого просмотра лучше всего подходит HIEW (Hacker's View) или AVPUTIL. Для более подробного изучения потребуется дизассемблер – Sourcer или IDA.

Для обнаружения некоторых резидентных вирусов можно запустить какой-нибудь блокировщик и отслеживать с его помощью все подозрительные действия (например, запись в COM- или EXE-файлы, запись на диск по абсолютному адресу и т.п.). Есть блокировщики, которые не только перехватывают такие действия, но и сообщают адрес поступления подозрительного вызова. После обнаружения такого действия надо узнать, какая программа собирается его выполнить, после чего проанализировать ее код с помощью резидентного дизассемблера (например, AVPUTIL.COM).

У DOS-блокировщиков есть большой недостаток: при работе в DOS-окне под Windows95/NT, они не срабатывают, потому что в этих ОС вирус может работать «в обход» блокировщика (как, впрочем, и всех остальных резидентных программ). Кроме того, DOS-блокировщики не способны остановить распространение Windows-вирусов.

Описанные методы обнаружения файловых и загрузочных вирусов подходят для большей части резидентных и нерезидентных вирусов. Эти методы не работают, если вирус выполнен по технологии «стелс».

Обнаружение макро-вируса

Характерные проявления макро-вирусов:

- Word: невозможность конвертирования зараженного документа Word в другой формат.
- Word: зараженные файлы имеют формат Template (шаблон), поскольку при заражении Word-вирусы конвертируют файлы из формата Word Document в Template.
- Word: невозможность записи документа в другой каталог/на другой диск по команде "Save As".
- Excel/Word: в STARTUP-каталоге присутствуют посторонние файлы.
- Excel: наличие в Книге (Book) лишних и скрытых Листов (Sheets).

Проверить систему на вирусы можно с помощью Tools/Macro. Посторонние макросы могут принадлежать вирусу. Если этот пункт меню не работает, то, возможно, в системе находится стелс-вирус. Вообще, если не работают различные пункты меню Tools/Options, это может быть следствием действий вируса.

Вирус – программа, и тоже имеет ошибки. В таком случае редактор выдаст сообщение, например:

WordBasic Err = номер ошибки

Если такое сообщение появляется при редактировании нового документа, не содержащего макросы, то, скорее всего, система заражена.

Изменения в файлах и системной конфигурации Word, Excel и Windows тоже является сигналом о присутствии вируса. Некоторые вирусы при заражении файла устанавливают на него пароль, создают новые секции и/или опции в файле конфигурации Windows (WIN.INI).

К проявлениям вируса относится появление сообщений или диалогов со странным содержанием или на языке, не совпадающем с языком установленной версии редактора.

Программы обнаружения и защиты от вирусов

Для обнаружения, удаления и защиты от компьютерных вирусов разработаны различные антивирусные программы. Существуют следующие виды антивирусных программ:

- *детекторы*
- *доктора* или *фаги (полифаги)*
- *ревизоры*
- *фильтры*
- *вакцины* или *иммунизаторы*

Детекторы осуществляют поиск характерной для конкретного вируса сигнатуры в оперативной памяти и в файлах и выдают соответствующее сообщение при обнаружении. К сожалению, они могут находить только вирусы, известные разработчикам.

Доктора и *вакцины* "лечат" файловые и макровирусы: находят зараженные файлы и возвращают их в исходное состояние, удаляя из файла тело программы-вируса. Сначала такие программы ищут и уничтожают вирусы в оперативной памяти, а затем - файлов. *Полифаги* предназначены для поиска и уничтожения большого количества вирусов. Наиболее известные: Aidstest, Scan, Norton AntiVirus, Doctor Web. Поскольку постоянно возникают новые вирусы, полифаги быстро устаревают, и требуется регулярное обновление версий или баз данных.

Одно из самых надежных средств защиты от вирусов – *ревизоры*, которые запоминают исходное состояние программ, каталогов и системных областей диска незараженного компьютера. Обычно сразу после загрузки ревизоры сравнивают текущее состояние с исходным операционной системы с исходным: проверяются длины файлов, даты и время модификации, контрольные суммы и другие параметры. Сравнение можно провести и по желанию пользователя. Программы-ревизоры способны обнаружить стелс-вирусы и могут даже убрать изменения, внесенные вирусом в проверяемую программу. К программам-ревизорам относится Adinf.

Фильтры – это небольшие резидентными программы. Они могут определить характерные действия вирусов при работе компьютера, такие как:

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-нибудь программы произвести подобные действия «фильтр» посылает сообщение и предлагает запретить или разрешить соответствующее действие. Эти программы весьма полезны, так как способны обнаружить вирус на

самой ранней стадии его существования. К сожалению, они не способны лечить файлы и диски. Также их недостатки – назойливость и возможные конфликты с другими программами. *Вакцины* – резидентные программы, предотвращающие заражение файлов. Их применяют, если отсутствуют программы-доктора от данного вируса. Вакцина изменяет программу или диск так, что это не отражается на их работе, а вирус воспринимает эти изменения как зараженне и не внедряется. Вакцинация возможна только от известных вирусов.

Слабое звено

Как нетрудно догадаться, речь идет об обязательном компоненте любой рабочей системы – пользователе. Вместо того чтобы писать вирус, можно просто «уговорить» человека запустить нужный файл на своем компьютере.

Довольно часто при попытках проникновения на компьютер, почтовый ящик и т. д., используются:

- письма, присланные от лица администрации сервисов Интернета с просьбой выслать им пароль, например, из-за его утери (на самом деле им проще поменять его и выслать новый);
- файлы, присылаемые по почте, ICQ и т.д., которые часто запускаются пользователями без предварительной проверки на вирусы.

Стоит хорошенько подумать, прежде чем запускать что-то пришедшее извне, вот один из самых примитивных способов:
В ICQ, методом «социальной инженерии», «хакер» прикидывается девушкой и вступает с «жертвой» в разговор; заинтересовав разговором, он под каким-либо предлогом устраивает обмен фотографиями, только «жертва» ему пошлет нормальную фотографию, а «хакер» пошлет обыкновенный троян со стандартной иконкой от jpg файлов и кучей пробелов, но его последние символы все-таки будут запускными. Как только «жертва» попробует посмотреть «фотку», троян заразит систему и распакует из своего тела небольшую фотографию. «Жертва», скорее всего, не сразу догадается, что же произошло, а последствия могут быть очень серьезными...

Источники:

1. http://www.uinc.ru/articles/10/index.shtml
2. http://www.semsk.kz/computers/virus/
3. http://www.viruslist.com/viruslistbooks.html?id=21
4. http://www.saslib.ru/ref/arh/14/VDV-0132/index.txt