

## Файловые вирусы

К данной группе относятся вирусы, которые при своем размножении тем или иным способом используют файловую систему какой-либо (или каких-либо) ОС.

Внедрение файлового вируса возможно практически во все исполняемые файлы всех популярных ОС. На сегодняшний день известны вирусы, поражающие все типы выполняемых объектов стандартной DOS: командные файлы (BAT), загружаемые драйверы (SYS, в том числе специальные файлы IO.SYS и MSDOS.SYS) и выполняемые двоичные файлы (EXE, COM). Существуют вирусы, поражающие исполняемые файлы других операционных систем - Windows 3.x, Windows95/NT, OS/2, Macintosh, UNIX, включая VxD-драйвера Windows 3.x и Windows95.

Существуют вирусы, заражающие файлы, которые содержат исходные тексты программ, библиотечные или объектные модули. Возможна запись вируса и в файлы данных, но это случается либо в результате ошибки вируса, либо при проявлении его агрессивных свойств. Макро-вирусы также записывают свой код в файлы данных - документы или электронные таблицы, - однако эти вирусы настолько специфичны, что вынесены в отдельную группу.

### 1. Способы заражения

По способу заражения файлов вирусы делятся на

- паразитические ("parasitic"),
- "overwriting",
- вирусы без точки входа
- компаньон-вирусы ("companion"),
- вирусы-черви
- "link"-вирусы,
- вирусы, заражающие объектные модули (OBJ), библиотеки компиляторов (LIB) и исходные тексты программ.

#### • *Parasitic*

К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сии файлы при этом полностью или частично работоспособными. 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).

#### *Внедрение вируса в начало файла*

Известны два способа внедрения паразитического файлового вируса в начало файла. Первый способ заключается в том, что вирус переписывает начало заражаемого файла в его конец, а сам копируется в освободившееся место. При заражении файла вторым способом вирус создает в оперативной памяти свою копию, дописывает к ней заражаемый файл и сохраняет полученную конкатенацию на диск. Некоторые вирусы при этом дописывают в конец файла блок дополнительной информации (например, вирус "Jerusalem" по этому блоку отличает зараженные файлы от незараженных).

Внедрение вируса в начало файла применяется в подавляющем большинстве случаев при заражении DOS'овских BAT- и COM-файлов. Известно несколько вирусов, записывающих себя в начало EXE-файлов операционных систем DOS, Windows и даже Linux. При этом вирусы, чтобы сохранить работоспособность программы, либо лечат зараженный файл, повторно запускают его, ждут окончания его работы и снова записываются в его начало (иногда для этого используется временный файл, в который записывается обезвреженный файл), либо восстанавливают код программы в памяти компьютера и настраивают необходимые адреса в ее теле (т.е. дублируют работу ОС).

### **Внедрение вируса в конец файла**

Наиболее распространенным способом внедрения вируса в файл является дописывание вируса в его конец. При этом вирус изменяет начало файла таким образом, что первыми выполняемыми командами программы, содержащейся в файле, являются команды вируса.

В DOS COM-файле в большинстве случаев это достигается изменением его первых трех (или более) байтов на коды инструкции JMP Loc\_Virus (или в более общем случае - на коды программы, передающей управление на тело вируса). DOS EXE-файл переводится в формат COM-файла и затем заражается как COM-файл либо модифицируется заголовок файла. В заголовке DOS EXE-файла изменяются значения стартового адреса (CS:IP) и длина выполняемого модуля (файла), реже - регистры-указатели на стек (SS:SP), контрольная сумма файла и т.д. В исполняемых файлах Windows и OS/2 (NewEXE - NE,PE,LE,LX) изменяются поля в NewEXE-заголовке. Структура этого заголовка значительно сложнее заголовка DOS EXE-файлов, поэтому изменению подлежит большее число полей - значение стартового адреса, количество секций в файле, характеристики секций и т.д. Дополнительно к этому длины файлов перед заражением могут увеличиваться до значения, кратного параграфу (16 байт) в DOS или секции в Windows и OS/2 (размер секции зависит от параметров заголовка EXE-файла).

Вирусы, внедряющиеся в DOS SYS-файлы, приписывают свои коды к телу файла и модифицируют адреса программ стратегии (Strategy) и прерывания (Interrupt) заражаемого драйвера (встречаются вирусы, изменяющие адрес только одной из этих программ). При инициализации зараженного драйвера вирус перехватывает соответствующий запрос операционной системы,

передает его драйверу, ждет ответа на этот запрос, корректирует его и остается вместе с драйвером в одном блоке оперативной памяти. Такой вирус может быть чрезвычайно опасным и живучим, так как он внедряется в оперативную память при загрузке DOS раньше любой антивирусной программы, если она, конечно, тоже не является драйвером.

Существуют также вирусы, заражающие системные драйвера другим способом: вирус модифицирует его заголовок так, что DOS рассматривает инфицированный файл как цепочку из двух (или более) драйверов.

Аналогично вирус может записать свои коды в начало драйвера, а если в файле содержится несколько драйверов, то и в середину файла.

### **Внедрение вируса в середину файла**

Существует несколько методов внедрения вируса в середину файла. В наиболее простом из них вирус переносит часть файла в его конец или "раздвигает" файл и записывает свой код в освободившееся пространство. Этот способ во многом аналогичен методам, перечисленным выше. Некоторые вирусы при этом компрессируют переносимый блок файла так, что длина файла при заражении не изменяется (см. "Mutant").

Вторым является метод "cavity", при котором вирус записывается в заведомо неиспользуемые области файла. Вирус может быть скопирован в незадействованные области таблицы настройки адресов DOS EXE-файла (см. "BootExe") или заголовок NewEXE-файла ("Win95.Murkry"), в область стека файла COMMAND.COM ("Lehigh") или в область текстовых сообщений популярных компиляторов ("NMSG"). Существуют вирусы, заражающие только те файлы, которые содержат блоки, заполненные каким-либо постоянным байтом, при этом вирус записывает свой код вместо такого блока.

Кроме того, копирование вируса в середину файла может произойти в результате ошибки вируса, в этом случае файл может быть необратимо испорчен.

- ***Overwriting***

Данный метод заражения является наиболее простым: вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать. Мне не известно ни одного случая, когда подобного типа вирусы были бы обнаружены "в живом виде" и стали причиной эпидемии.

К разновидности overwriting-вирусов относятся вирусы, которые записываются вместо DOS-заголовка NewEXE-файлов. Основная часть файла при этом остается без изменений и продолжает нормально работать в соответствующей операционной системе, однако DOS-заголовок оказывается испорченным.

- **Вирусы без точки входа**

Отдельно следует отметить довольно незначительную группу вирусов, не имеющих "точки входа" (ЕРО-вирусы - Entry Point Obscuring viruses). К ним относятся вирусы, не записывающие команд передачи управления в заголовок СОМ-файлов (JMP) и не изменяющие адрес точки старта в заголовке ЕХЕ-файлов. Такие вирусы записывают команду перехода на свой код в какое-либо место в середину файла и получают управление не непосредственно при запуске зараженного файла, а при вызове процедуры, содержащей код передачи управления на тело вируса. Причем выполняться эта процедура может крайне редко (например, при выводе сообщения о какой-либо специфической ошибке). В результате вирус может долгие годы "спать" внутри файла и выскочить на свободу только при некоторых ограниченных условиях.

Перед тем, как записать в середину файла команду перехода на свой код, вирусу необходимо выбрать "правильный" адрес в файле - иначе зараженный файл может оказаться испорченным. Известны несколько способов, с помощью которых вирусы определяют такие адреса внутри файлов.

Первый способ - поиск в файле последовательности стандартного кода С/Pascal (вирусы "Lucretia", "Zhengxi"). Эти вирусы ищут в заражаемых файлах стандартные заголовки процедур С/Pascal и записывают вместо них свой код.

Второй способ - трассировка или дизассемблирование кода файла ("CNTV", "MidInfector", "NexivDer"). Такие вирусы загружают файл в память, затем трассируют или дизассемблируют его и в зависимости от различных условий выбирают команду (или команды), вместо которых записывается код перехода на тело вируса.

Третий способ применяется только резидентными вирусами - при запуске файла они контролируют какое-либо прерывание (чаще - INT 21h). Как только заражаемый файл вызывает это прерывание, вирус записывает свой код вместо команды вызова прерывания (см. "Avatar.Positron", "Markiz").

- **Компаньон-вирусы**

К категории "компаньон" относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.

Наиболее распространены компаньон-вирусы, использующие особенность DOS первым выполнять .СОМ-файл, если в одном каталоге присутствуют два файла с одним и тем же именем, но различными расширениями имени - .СОМ и .ЕХЕ. Такие вирусы создают для ЕХЕ-файлов файлы-спутники, имеющие то же самое имя, но с расширением .СОМ, например, для файла ХСОРУ.ЕХЕ создается файл ХСОРУ.СОМ. Вирус записывается в СОМ-файл и никак не изменяет ЕХЕ-файл. При запуске такого файла DOS первым обнаружит и выполнит СОМ-файл, т.е. вирус, который затем запустит и

EXE-файл. Некоторые вирусы используют не только вариант COM-EXE, но также и BAT-COM-EXE.

Вторую группу составляют вирусы, которые при заражении переименовывают файл в какое-либо другое имя, запоминают его (для последующего запуска файла-хозяина) и записывают свой код на диск под именем заражаемого файла. Например, файл XCOPY.EXE переименовывается в XCOPY.EXD, а вирус записывается под именем XCOPY.EXE. При запуске управление получает код вируса, который затем запускает оригинальный XCOPY, хранящийся под именем XCOPY.EXD. Интересен тот факт, что данный метод работает, наверное, во всех операционных системах - подобного типа вирусы были обнаружены не только в DOS, но в Windows и OS/2.

В третью группу входят так называемые "Path-companion" вирусы, которые "играют" на особенностях DOS PATH. Они либо записывают свой код под именем заражаемого файла, но "выше" на один уровень PATH (DOS, таким образом, первым обнаружит и запустит файл-вирус), либо переносят файл-жертву на один подкаталог выше и т.д.

Возможно существование и других типов компаньон-вирусов, использующих иные оригинальные идеи или особенности других операционных систем.

- **Файловые черви**

Файловые черви (worms) являются, в некотором смысле, разновидностью компаньон-вирусов, но при этом никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям "специальные" имена, чтобы подтолкнуть пользователя на запуск своей копии - например, INSTALL.EXE или WINSTART.BAT.

Существуют вирусы-черви, использующие довольно необычные приемы, например, записывающие свои копии в архивы (ARJ, ZIP и прочие). К таким вирусам относятся "ArjVirus" и "Winstart". Некоторые вирусы записывают команду запуска зараженного файла в BAT-файлы (см. например, "Worm.Info").

Не следует путать файловые вирусы-черви с сетевыми червями. Первые используют только файловые функции какой-либо операционной системы, вторые же при своем размножении пользуются сетевыми протоколами.

- **Link-вирусы**

Link-вирусы, как и компаньон-вирусы не изменяют физического содержимого файлов, однако при запуске зараженного файла "заставляют" ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

На сегодняшний день известен единственный тип Link-вирусов - вирусы семейства "Dir\_II". При заражении системы они записывают свое тело в последний кластер логического диска. При заражении файла вирусы корректируют лишь номер первого кластера файла, расположенный в

соответствующем секторе каталога. Новый начальный кластер файла будет указывать на кластер, содержащий тело вируса. Таким образом, при заражении файлов их длины и содержимое кластеров диска, содержащих эти файлы, не изменяется, а на все зараженные файлы на одном логическом диске будет приходиться только одна копия вируса.

До заражения данные каталога хранят адрес первого кластера файла. После заражения данные каталога указывают на вирус, т.е. при запуске файла управление получают не файлы, а вирус.

- ***OBJ-, LIB-вирусы и вирусы в исходных текстах***

Вирусы, заражающие библиотеки компиляторов, объектные модули и исходные тексты программ, достаточно экзотичны и практически не распространены. Всего их около десятка. Вирусы, заражающие OBJ- и LIB-файлы, записывают в них свой код в формате объектного модуля или библиотеки. Зараженный файл, таким образом, не является выполняемым и неспособен на дальнейшее распространение вируса в своем текущем состоянии. Носителем же "живого" вируса становится COM- или EXE-файл, получаемый в процессе линковки зараженного OBJ/LIB-файла с другими объектными модулями и библиотеками. Таким образом, вирус распространяется в два этапа: на первом заражаются OBJ/LIB-файлы, на втором этапе (линковка) получается работоспособный вирус.

Заражение исходных текстов программ является логическим продолжением предыдущего метода размножения. При этом вирус добавляет к исходным текстам свой исходный код (в этом случае вирус должен содержать его в своем теле) или свой шестнадцатеричный дамп (что технически легче). Зараженный файл способен на дальнейшее распространение вируса только после компиляции и линковки (см. например, вирусы "SrcVir", "Urphin").

- ***2. Внедрение вируса в DOS COM- и EXE-файлы***

Выполняемые двоичные файлы DOS имеют форматы COM или EXE, различающиеся заголовком и способом запуска программ на выполнение. Расширение имени файла (".COM" или ".EXE") не всегда соответствует действительному формату файла, что, правда, никак не влияет на работу программы. Файлы COM и EXE заражаются по-разному, следовательно вирус должен отличать файлы одного формата от другого. Вирусы решают эту задачу двумя способами: одни анализируют расширение имени файла (".COM", ".EXE"), другие - заголовок файла. Первый способ далее будет называться заражением .COM- (или .EXE-) файлов, второй - заражением COM- (или EXE-) файлов.

В большинстве случаев вирус инфицирует файл корректно, т.е. по информации, содержащейся в теле вируса, можно полностью восстановить зараженный файл. Но вирусы, как и большинство программ, часто содержат незаметные с первого взгляда ошибки. Из-за этого даже вполне корректно написанный вирус может необратимо испортить файл при его заражении. Например, вирусы, различающие типы файлов по расширению имени (.COM, .EXE), очень опасны, так как портят файлы, у которых расширение имени не соответствует внутреннему формату.

Один из наиболее часто встречающихся примеров некорректного заражения файла - COMMAND.COM от Windows95. Этот файл по сути является EXE-файлом, более того имеет размер более 90К, что невозможно для COM-файла. Поэтому вирусы, которые различают COM/EXE файлы по расширению имени и не проверяют длины заражаемых COM-файлов (например, "Junkie"), портят такой COMMAND.COM, и он становится неработоспособным.

- **3.Примитивная маскировка**

При инфицировании файла вирус может производить ряд действий, маскирующих и ускоряющих его распространение. К подобным действиям можно отнести обработку атрибута read-only, снятие его перед заражением и восстановление после. Многие файловые вирусы считывают дату последней модификации файла и восстанавливают ее после заражения. Для маскировки своего распространения некоторые вирусы перехватывают прерывание DOS, возникающее при обращении к защищенному от записи диску (INT 24h), и самостоятельно обрабатывают его.

- **4.Скорость распространения**

Говоря про файловые вирусы, необходимо отметить такую их черту, как скорость распространения. Чем быстрее распространяется вирус, тем вероятнее возникновение эпидемии этого вируса. Чем медленнее распространяется вирус, тем сложнее его обнаружить (если, конечно же, этот вирус пока неизвестен антивирусным программам). Понятия "быстрого" и "медленного" вируса (Fast infector, Slow infector) являются достаточно относительными и используются только как характеристика вируса при его описании.

Нерезидентные вирусы часто являются "медленными" - большинство из них при запуске заражает один или два-три файла и не успевает заполнить компьютер до запуска антивирусной программы (или появления новой версии антивируса, настроенной на данный вирус). Существуют, конечно же, нерезидентные "быстрые" вирусы, которые при запуске ищут и заражат все выполняемые файлы, однако такие вирусы очень заметны: при запуске каждого зараженного файла компьютер некоторое (иногда достаточно долгое) время активно работает с винчестером, что демаскирует вирус.

"Скорость" резидентных вирусов обычно выше, чем у нерезидентных - они заражают файлы при каких-либо обращениях к ним. В результате на диске оказываются зараженными все или почти все файлы, которые постоянно используются в работе.

Скорость распространения резидентных файловых вирусов, заражающих файлы только при их запуске на выполнение, будет ниже, чем у вирусов, заражающих файлы и при их открытии, переименовании, изменении атрибутов файла и т.д. Многие вирусы при создании своей копии в оперативной памяти компьютера пытаются занять область памяти с самыми старшими адресами, разрушая временную часть командного интерпретатора COMMAND.COM. По окончании работы зараженной программы временная часть интерпретатора восстанавливается, при этом происходит открытие

файла COMMAND.COM и, если вирус заражает файлы при их открытии, его заражение. Таким образом, при запуске подобного вируса первым будет заражен файл COMMAND.COM

- **5. Алгоритм работы файлового вируса**

Получив управление, вирус совершает следующие действия (приведен список наиболее общих действий вируса при его выполнении; для конкретного вируса список может быть дополнен, пункты могут меняться местами и значительно расширяться):

- Резидентный вирус проверяет оперативную память на наличие своей копии и инфицирует память компьютера, если копия вируса не найдена. Нерезидентный вирус ищет незараженные файлы в текущем и (или) корневом оглавлении, в оглавлениях, отмеченных командой RATH, сканирует дерево каталогов логических дисков, а затем заражает обнаруженные файлы;
- выполняет, (если они есть), дополнительные функции: деструктивные действия, графические или звуковые эффекты и т.д. Дополнительные функции резидентного вируса могут вызываться спустя некоторое время после активизации в зависимости от текущего времени, конфигурации системы, внутренних счетчиков вируса или других условий; в этом случае вирус при активизации обрабатывает состояние системных часов, устанавливает свои счетчики и т.д.;
- возвращает управление основной программе (если она есть). Паразитические вирусы при этом либо а) лечат файл, выполняют его, а затем снова заражают, либо б) восстанавливают программу (но не файл) в исходном виде (например, у COM-программы восстанавливается несколько первых байт, у EXE-программы вычисляется истинный стартовый адрес, у драйвера восстанавливаются значения адресов программ стратегии и прерывания). Компаньон-вирусы запускают на выполнение своего "хозяина", вирусы-черви и overwriting-вирусы возвращают управление DOS.

Метод восстановления программы в первоначальном виде зависит от способа заражения файла. Если вирус внедряется в начало файла, то он либо сдвигает коды зараженной программы на число байт, равное длине вируса, либо перемещает часть кода программы из ее конца в начало, либо восстанавливает файл на диске, а затем запускает его. Если вирус записался в конец файла, то при восстановлении программы он использует информацию, сохраненную в своем теле при заражении файла. Это может быть длина файла, несколько байт начала файла в случае COM-файла или несколько байтов заголовка в случае EXE-файла. Если же вирус записывается в середину файла специальным образом, то при восстановлении файла он использует еще и специальные алгоритмы.