Резидентные

Такие вирусы, получив управление, так или иначе остаются в памяти и производят поиск жертв непрерывно, до завершения работы среды, в которой он выполняется. С переходом на Windows проблема остаться в памяти перестала быть актуальной: практически все вирусы, исполняемые в среде Windows, равно как и в среде приложений Microsoft Office, являются резидентными вирусами. Соответственно, атрибут резидентный применим только к файловым DOS вирусам.

Нерезидентные

Получив управление, такой вирус производит разовый поиск жертв, после чего передает управление ассоциированному с ним объекту (зараженному объекту). К такому типу вирусов можно отнести скрипт-вирусы.

Классификация вирусов по степени воздействия

Безвредные

Это вирусы никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения).

Неопасные

Это вирусы 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

Это вирусы, которые могут привести к различным нарушениям в работе компьютера.

Очень опасные

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

Классификация вирусов по способу маскировки

Шифрованный вирус

Это вирус, использующий простое шифрование со случайным ключом и неизменный шифратор. Такие вирусы легко обнаруживаются по сигнатуре шифратора.

Вирус-шифровальщик

В большинстве случаев вирус-шифровальщик приходит по электронной почте в виде вложения от незнакомого пользователю человека, а возможно, и от имени известного банка или действующей крупной организации.

Вложения вредоносных писем чаще всего бывают в архивах .zip, .rar, .7z. И если в настройках системы компьютера отключена функция отображения расширения файлов, то пользователь (получатель письма) увидит лишь файлы вида «Документ.doc», «Акт.xls» и тому подобные.

Другими словами, файлы будут казаться совершенно безобидными. Но если включить отображение расширения файлов, то сразу станет видно, что это не документы, а исполняемые программы или скрипты, имена файлов приобретут иной вид, например, «Документ.doc.exe» или «Акт.xls.js». При открытии таких файлов происходит не открытие документа, а запуск вируса-шифровальщика.

На практике встречаются случаи получения по электронной почте обычного “вордовского” файла, внутри которого, помимо текста, есть изображение, гиперссылка (на неизвестный сайт в Интернете) или встроенный OLE-объект. При нажатии на такой объект происходит незамедлительное заражение.

Полиморфный вирус

Это вирус, использующий метаморфный шифратор для шифрования основного тела вируса со случайным ключом. При этом часть информации, используемой для получения новых копий шифратора также может быть зашифрована. Например, вирус может реализовывать несколько алгоритмов шифрования и при создании новой копии менять не только команды шифратора, но и сам алгоритм.

Классификация вирусов по среде обитания

Под “средой обитания” понимаются системные области компьютера, операционные системы или приложения, в компоненты (файлы) которых внедряется код вируса.

Файловые вирусы

Файловые вирусы при своем размножении тем или иным способом используют файловую систему какой-либо (или каких-либо) ОС. Они:

- различными способами внедряются в исполняемые файлы (наиболее распространенный тип вирусов);
- создают файлы-двойники (компаньон-вирусы);
- создают свои копии в различных каталогах;
- используют особенности организации файловой системы (link-вирусы).

Все, что подключено к Интернету – нуждается в антивирусной защите: 82% обнаруженных вирусов находятся в файлах с расширением PHP, HTML и EXE. Это говорит о том, что выбор хакеров – это Интернет, а не атаки с использованием уязвимостей программного обеспечения. Угрозы имеют полиморфный характер, это означает, что вредоносные программы могут быть эффективно перекодированы удаленно, что делает их трудно обнаруживаемыми. Поэтому высокая вероятность заражения связана, в том числе, и с посещениями сайтов.

Загрузочные вирусы

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор. Данный тип вирусов был достаточно распространён в 1990-х, но практически исчез с переходом на 32-битные операционные системы и отказом от использования дискет как основного способа обмена информацией.

Макро-вирусы

Многие табличные и графические редакторы, системы проектирования, текстовые процессоры имеют свои макро-языки для автоматизации выполнения повторяющихся действий. Эти макро-языки часто имеют сложную структуру и развитый набор команд. Макро-вирусы являются программами на макро-языках, встроенных в такие системы обработки данных. Для своего размножения вирусы этого класса используют возможности макро-языков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Скрипт-вирусы

Скрипт-вирусы, также как и макро-вирусы, являются подгруппой файловых вирусов. Данные вирусы, написаны на различных скрипт-языках (VBS, JS, BAT, PHP и т.д.). Они либо заражают другие скрипт-программы, либо являются частями многокомпонентных вирусов.

Классификация вирусов по способу заражения файлов

Перезаписывающие

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.

Паразитические

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

Вирусы-компаньоны

К ним 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.

К вирусам данного типа относятся те из них, 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.

Вирусы-ссылки

Вирусы-ссылки или link-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.

Файловые черви

Файловые черви 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.

OBJ-, LIB-вирусы и вирусы в исходных текстах

Это 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.