Классификация компьютерных вирусов

СРЕДА ОБИТАНИЯ

По среде обитания вирусы можно разделить на сетевые, файловые и загрузочные. Сетевые вирусы распространяются по компьютерной сети, файловые внедряются в выполняемые файлы, загрузочные - в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий системный загрузчик винчестера (Master Boot record). Существуют сочетания, например, файлово-загрузочные вирусы.

СПОСОБЫ ЗАРАЖЕНИЯ

Способы заражения делятся на резидентный и нерезидентный.

Резидентный вирус при при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них.

Нерезидентные вирусы не заражают память компьютера и являются активными ограниченное время.

ДЕСТРУКТИВНЫЕ ВОЗМОЖНОСТИ

Подеструктивным возможностям вирусы можно разделить на:

безвредные, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);

неопасные, влияние которых ограничивается уменьшением свободной памяти на диске, графическим,звуковыми и прочими эффектами;

опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;

очень опасные, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях.

ОСОБЕННОСТИ АЛГОРИТМА

По особенностям алгоритма можно выделить следующие группы вирусов:

вирусы-"спутники" (companion) - это вирусы, не изменяющие файлы. Алгоритм работы этих вирусов состоит в том, что они создают для ЕХЕ-файлов файлы-спутники, имеющие то же самое имя, но с расширением СОМ. При запуске система ищет сначала файл с расширением СОМ, запускает его, вирус выполняет все свои действия, а затем запускает настоящую прогамму, у которой расширение ЕХЕ;

вирусы-"черви" (worm) - вирусы, которые распространяются в компьютерной сети. Они проникают в память компьютера по сети, вычисляют адреса других компьютеров и рассылаются по этим адресам;

"паразитические" - все вирусы, которые при распространении своих копий изменяют содержимое дисковых секторов и файлов. В эту группу входят все вирусы, которые н являются "спутниками" и "червями";

"студенческие" - крайне примитивные вирусы, часто нерезидентные и содержащие большое число ошибок;

"стелс"-вирусы (вирусы-невидимки, stealsh) - это очень совершенные программы, которые перехватывают обращения DOS к пораженным файлам или секторам диска и "подставляют" вместо себя незараженные участки;

вирусы-"призраки" - достаточно труднообнаружимые вирусы, не имеющие ни одного постоянного участка кода. Вирус шифрует свой код. При шифровке каждый раз используются разные ключи. Кроме того, модифицируется и программа-расшифровщик. Таким образом, код вируса в разных случаях заражения будет разный.