Классификация вирусов

В настоящее время известно более 70 000 программных вирусов, их можно классифицировать по следующим признакам:

— среда обитания;

— способ заражения среды обитания;

— воздействие;

— особенности алгоритма.

Среда обитания

В зависимости от среды обитания вирусы можно разделить на:

- Сетевые - распространяются по различным компьютерным сетям.
- Файловые -внедряются чаще всего в исполняемые модули, файлы (COM и EXE). 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.
- Загрузочные - внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Record).
- файлово-загрузочные - заражают как файлы, так и загрузочные сектора дисков.

Способ заражения среды обитания

Резидентные и нерезидентные.

- Резидентный вирус при заражении (инфицировании) компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется и них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера.

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

Воздействие

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,

Особенности алгоритма

- 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.
- Известны 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, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки бантов.
- Имеются и так называемые квазивирусные («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.

Загрузочные вирусы

В загрузочных вирусах выделяют две части — голову и хвост. Хвост может быть пустым.
Этот вирус является активным резидентным.

При заражении нового съемного диска не закрытого от записи, вирус производит следующие действия:

- выделяет некоторую область диска и помечает ее как недоступную операционной системе. Это можно сделать по разному (традиционно занятые вирусом секторы помечаются как сбойные);
- копирует в выделенную область диска свой хвост и оригинальный (здоровый) загрузочный сектор;
- замещает программу начальной загрузки в загрузочном секторе (настоящем) своей головой;
- организует цепочку передачи управления через себя.

Таким образом, голова вируса первой получает управление, вирус устанавливается в память и передает управление оригинальному загрузочному сектору.

При загрузке компьютера с жесткого диска первой берет на себя управление программа начальной загрузки в MBR (Master Boot Record). Программа начальной загрузки в MBR находит загрузочный раздел, и передает управление на программу начальной загрузки этого раздела. Код последней совпадает с кодом программы начальной загрузки, содержащейся на обычных дискетах, а соответствующие загрузочные секторы отличаются только таблицами параметров.

Таким образом, на жестком диске имеются два объекта атаки загрузочных вирусов программа начальной загрузки в MBR и программа начальной загрузки в бут-секторе загрузочного диска.

Файловые вирусы

При запуске инфицированного исполняемого файла вирус получает управление, производит некоторые действия и передает управление «хозяину !!!!???? »

Действия выполняемые вирусом:

Поиск нового объекта для заражения — подходящий по типу файл, который еще не заражен. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла.

Кроме своей основной функции (размножение), вирус может что-нибудь сделать.

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.

Заражая исполняемый файл, вирус всегда изменяет его код, следовательно, заражение исполняемого файла всегда можно обнаружить. Но, изменяя код файла, вирус не обязательно вносит другие изменения:

- — он не обязан менять длину файла;
- — неиспользуемые участки кода
- — не обязан менять начало файла.

Загрузочно-файловые вирусы

- Пример загрузочного вируса OneHalf, заражающий главный загрузочный сектор (MBR) и исполняемые файлы.

- Основное разрушительное действие — шифрование секторов винчестера.
- При каждом запуске вирус шифрует очередную порцию секторов, а зашифровав половину жесткого диска, сообщает об этом.
- Основная проблема при лечении данного вируса состоит в том, что недостаточно просто удалить вирус из MBR и файлов, надо расшифровать зашифрованную им информацию.
- Наиболее «смертельное» действие — просто переписать ног вый здоровый MBR.

Макровирусы

- Приложения, которые поддерживают макросы, подвержены риску заражения макровирусами.

- Макровирусы — это команды, встроенные в файлы вместе с данными. Примерами таких приложений являются Word, Excel и интерпретаторы Postscripts. Когда они открывают файлы данных, то происходит заражение макровирусом. Наиболее распространены макровирусы для Microsoft Word в силу его широкой распространенности и наличия в нем средств автоматизации.

Полиморфные вирусы

- Полиморфные вирусы - вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совладать 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 - имея зараженный и оригинальный файлы невозможно проанализировать его код с помощью обычного дизассемблирования.

- Расшифровка производится самим вирусом уже непосредственно во время выполнения. При этом возможны варианты: он может расшифровать себя всего сразу, а может выполнить такую расшифровку по факт, а уже отработавшие участки зашифровать. Все это делается ради затруднения анализа кода вируса.