Классификация компьютерных вирусов

Вирусы можно разделить на классы по следующим основным признакам:

среда обитания;

особенности алгоритма работы

деструктивные возможности.

В зависимости от **среды обитания** вирусы можно разделить на:

файловые;

загрузочные;

макровирусы;

сетевые.

Исходя из особенностей алгоритма работы:

Резидентный вирус

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

Полиморфик-вирус

трудно поддаются обнаружению, не содержат ни одного постоянного участка кода. Часто два образца одного и того же полиморфик-вируса не имеют ни одного совпадения. Происходит шифрование основного тела вируса и модификация программы-расшифровщика.

«Стелс» - вирусы

теми или иными способами скрывают факт своего присутствия в системе.

Классификация компьютерных вирусов

По деструктивным возможностям вирусы можно разделить на:

безвредные, 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 и графическим, звуковым и прочими эффектами;

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

очень опасные – в алгоритм их работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию.

троянские – осуществляющие различные несанкционированные пользователем действия: сбор информации, ее передачу злоумышленнику, или использование ресурсов компьютера в неблаговидных целях

Файловые вирусы

По способу заражения делятся на:

- Overwriting – вирусы;
- Link - вирусы;
- Parasitic – вирусы;
- Companion – вирусы;
- Файловые черви.

Overwriting-вирусы

Вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Такие вирусы очень быстро обнаруживают себя, так как операционная система и приложения довольно быстро перестают работать.

Link-вирусы

Не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют операционную систему выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

Parasitic-вирусы

Вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сами файлы при этом полностью или частично работоспособными.

Файловые вирусы

Companion-вирусы

Вирусы, не изменяющие заражаемых файлов. Для заражаемого файла создаётся файл-двойник, причём при запуске зараженного файла управление получает именно этот двойник, т.е. вирус.

Файловые черви

Не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют операционную систему выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.

Загрузочные вирусы

Загрузочный вирус (Boot-вирус), записывается в первый сектор гибкого или жёсткого диска и выполняется при загрузке компьютера или при обращении к диску.
Вирус заменяет собой загрузочный код и получает управление, размещая в памяти своё тело, которое хранит в неиспользованных секторах, идущих после главной загрузочной записи (MBR), но до первого загрузочного сектора раздела. Размножается вирус записью в загрузочную область других накопителей компьютера.

Макровирусы

Это разновидность компьютерных вирусов, разработанных на макроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office. Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносятся из одного зараженного файла в другие.

Сетевые вирусы

Сетевые вирусы для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию.

Троянские программы

Программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.
Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера.

Backdoor — троянские утилиты удаленного администрирования

Троянские программы этого класса являются утилитами удаленного администрирования компьютеров в сети.

Trojan-PSW — воровство паролей

Данное семейство объединяет троянские программы, «ворующие» различную информацию с зараженного компьютера.

Trojan-Clicker — интернет-кликеры

Семейство троянских программ, основная функция которых — организация несанкционированных обращений к интернет-ресурсам (обычно к веб-страницам).

Троянские программы

Trojan-Downloader — доставка прочих вредоносных программ

Троянские программы этого класса предназначены для загрузки и установки на компьютер-жертву новых версий вредоносных программ, установки «троянцев» или рекламных систем.

Trojan-Dropper — инсталляторы прочих вредоносных программ

Троянские программы этого класса написаны в целях скрытной инсталляции других программ и практически всегда используются для распространения на компьютер-жертву вирусов или других троянских программ.

Trojan-Proxy — троянские прокси-сервера

Семейство троянских программ, скрытно осуществляющих анонимный доступ к различным интернет-ресурсам. Обычно используются для рассылки спама.

Trojan — прочие троянские программы

К данным троянцам относятся те из них, которые осуществляют прочие действия, попадающие под определение троянских программ, т. е. разрушение или злонамеренная модификация данных, нарушение работоспособности компьютера и прочее.

Сетевые черви

Основным признаком, по которому типы червей различаются между собой, является способ распространения червя — каким способом он передает свою копию на удаленные компьютеры. Другими признаками различия являются: способы запуска копии червя на заражаемом компьютере, методы внедрения в систему, а также полиморфизм, «стелс» и прочие характеристики, присущие и другим типам вредоносного программного обеспечения (вирусам и троянским программам).

Email-Worm — почтовые черви

К данной категории червей относятся те из них, которые для своего распространения используют электронную почту.

IM-Worm — черви, использующие интернет-пейджеры

Известные компьютерные черви данного типа используют единственный способ распространения — рассылку на обнаруженные контакты сообщений, содержащих URL на файл, расположенный на каком-либо веб-сервере.

IRC-Worm — черви в IRC-каналах

Существуют два способа распространения червя по IRC-каналам. Первый заключается в отсылке URL-ссылки на копию червя. Второй способ — отсылка зараженного файла какому-либо пользователю сети. При этом атакуемый пользователь должен подтвердить прием файла, затем сохранить его на диск и открыть (запустить на выполнение).

Сетевые черви

Net-Worm — прочие сетевые черви

Существуют способы заражения удаленных компьютеров:

- копирование червя на сетевые ресурсы;
- проникновение червя на компьютер через уязвимости в операционных системах и приложениях;

проникновение в сетевые ресурсы публичного использования; паразитирование на других вредоносных программах.

P2P-Worm — черви для файлообменных сетей

Механизм работы большинства подобных червей достаточно прост — для внедрения в P2P-сеть червю достаточно скопировать себя в каталог обмена файлами, который обычно расположен на локальной машине.