О компьютерных вирусах-популярно

История вирусов

Считается, что авторов первой программы – вируса является американец Фред Коэн. В 1983 году, будучи студентом, он в рамках работы над диссертацией написал программу, которую окрестил «вирусом» за её способность к саморазмножению(созданию собственных копий). Демонстрацию своего творения Фред произвёл 10 ноября 1983 года, тогда же и был впервые официально использован термин «компьютерный вирус». По результатам демонстрации Коэну было запрещено проводить дальнейшие исследования и эксперименты в области вирусных программ.

Кратко о вирусах

Вирус – не зависящая от пользователя программа, основной целью которой является самораспространение.

Вот то определение, которым пользуется антивирусный отдел общества «Ангстрем» : *информационный вирус – Это способный к саморазмножению программный код, выполнение которого обычно нежелательно для пользователя, на чьём компьютере (или ином устройстве) он выполняется.*

Типы вирусов

1. Файловые вирусы.
2. Загрузочные вирусы.
3. Файлово - загрузочные вирусы.
4. Макровирусы.
5. Полиморфные вирусы.
6. Стелс - вирусы.
7. Самошифрующиеся вирусы.
8. Резидентные вирусы.
9. Сетевые черви различных типов.
    a) Worm.
    b) Троянские кони.
    c) Скрипт – вирусы.

Файловые вирусы

Эти вирусы записывают свой код в исполняемые файлы (наиболее часто – типа *.exe и *.com). При этом вирус может поместить своё тело без последующей корректировки вместо части данных зараженного файла, и тогда исходный файл потеряет работоспособность, равно как и возможность быть «вылеченным» при помощи антивирусной программы.

Загрузочные вирусы

Загрузочные вирусы отличаются от файловых тем, что записывают свои копии в главную загрузочную запись (Master Boot Record – MBR) и загрузочный сектор (Boot Sector – BS) дискового носителя. Заражение происходит при считывании (и выполнении) данных областей, которое происходит при включении компьютера.

Файлово - загрузочные вирусы

Файлово- загрузочные вирусы сочетают в себе возможности первых двух классов. Это позволяет им повышать как выживаемость на инфицированном компьютере, так и скорость распространения.

Макровирусы

Макровирусы инфицируют документы программ пакета Microsoft Office (Word, Excel, и др.) и их шаблоны. В отличие от простого текстового файла (plain text format) типа *.txt.

Простые текстовые файлы, например, созданные с помощью программы Блокнот, зараженными вирусом быть не могут. А вот безопасность файлов формата RTF (*Ricb* Text Format) – не более чем миф.

Полиморфные вирусы

Полиморфные вирусы способны изменять во время копирования своё тело. Поэтому копии одного вируса не совпадают друг с другом, хотя и сохраняют (как правило) свою функциональность «родительской». Алгоритмы модификации достаточно сложны и красивы с точки зрения программирования, однако создаются они не ради эстетики, а с вполне конкретной целью – затруднить выявление копий вируса.

Стелс вирусы

Стелс вирусы названы так в честь самолета «Stealth» американских ВВС – якобы невидимого на радарах. Они перехватывают системные обращения и маскируют своё присутствие в системе, успешно скрываясь от антивирусных сканеров и программ антивирусной проверки в режиме реального времени (антивирусных мониторов).

Самошифрующиеся вирусы

Самошифрующиеся вирусы динамически осуществляют шифрование/расшифровывание своего тела, что затрудняет их обнаружение (но отнюдь не исключает саму возможность этого).

Резидентные вирусы

Резидентные вирусы остаются в оперативной памяти после завершения «родительского» процесса (работы инфицированной ими программы). Поскольку оперативное запоминающее устройство – память энерго-зависимая, то после перезагрузки системы резидентные вирусы удаляются. Однако если такой вирус «прописан» на автозапуск, то перезагрузка компьютера его не инактивирует (точнее – вызовет повторное заражение).

Сетевые вирусы.

По компьютерной сети могут распространяться и заражать любые обычные вирусы. Например, при получении заражённых файлов с серверов файловых архивов. Однако существуют и специфические сетевые вирусы, которые используют для своего распространения электронную почту и Инет.

Интернет черви (worm).

Это вирусы, которые распространяются в компьютерной сети во вложенных в почтовые сообщение файлов. Автоматическая активация червя и заражение компьютера могут произойти при обычном просмотре сообщения.

Трояны.

Трояны внедряются в операционную систему. Такие вирусы «похищают» идентификатор и пароль пользователя для доступа в Интернет и передают их на определенный почтовый адрес. В результате злоумышленники получают возможность выхода в Интернет за деньги ничего не подозревающих пользователей.

Скрипт – вирусы.

Особой разновидностью вирусов является активные элементы (программы) на языках JavaSccipt или VBScript, которые могут выполнять разрушительные действия, то есть являться вирусами. Такие программы передаются по Всемирной паутине в процессе загрузки Web – страниц с серверов Интернета в браузер локального компьютера.

Помните информационные воины опасны для вашего компьютера!