Вредоносные программы

Вредоносные программы делятся на:

Вирусы

Черви

Троянские программы

Вирусы

- **Компьютерный вирус —** разновидность компьютерных программ или вредоносный код, отличительным признаком которых является способность к размножению.

Виды вирусов:

- ***Вирус VIENNA (Вена)***

Другие названия вируса: 648, Restart (перезагрузка), Time Bomb (часовая бомба) и др..

Одна из первых наиболее примитивных вирусов. Найден сначала в Вене, затем заполонил весь мир. При загрузке в память компьютера просматривает все COM-программы в текущем каталоге и в доступных через PATH. Первоначальный вариант этого вируса увеличивал длину жертвы на 648 байт. Первую найденную еще не зараженную программу или заражает, или, с вероятностью 1 / 8 , портит таким образом, что она при запуске приводит к перезагрузке системы. В последнем случае в начале жертвы записывается код EAFoFFooFo, который на машинном языке означает теплый рестарт (эквивалентно действию клавиш Ctrl + Alt + Del). Если испорчена таким образом программа вызывается из AUTOEXEC.BAT, процедура начальной загрузки операционной системы зацикливается.

- ***Вирус BLACK FRIDAY (Черная пятница)***

Другие названия вируса: Israeli Virus (израильский вирус), Ierusalem (Иерусалим), Black Hole (черная дыра) и др..

Он заражает EXE-и COM-файлы, увеличивая их размеры на 1813 байт, и остается резидентным в памяти ПК. При этом заражение может происходить неоднократно, что приводит к невероятному разрастанию зараженных файлов. Инфицированный данным вирусом ПК замедляет свою работу в несколько тысяч раз. При выводе информации на дисплей в нижнем левом углу экрана появляется черный прямоугольник . Если время работы приходится на пятницу 13-го числа, то зараженные файлы уничтожаются.

- ***Вирус DARK AVENGER (Черный мститель)***

  Другие названия вируса: Eddie, Sofia.

  Вирус заражает EXE-и COM-файлы, есть резидентным, его длина в байтах 1800. Вирус очень опасен, поскольку на инфицированном компьютере файлы заражаются не только при исполнении, но и во время их просмотра и копирования. Он также уничтожает COM-файлы, длина которых лежит в пределах от 64К1800байт до 64К. Периодически уничтожает информацию в одном из секторов винчестера.

Сетевые черви

Сетевые черви — черви, использующие для распространения протоколы Интернет и локальных сетей.

Почтовые черви — черви, распространяющиеся в формате сообщений электронной почты

IRC-черви — черви, распространяющиеся по каналам IRC (Internet Relay Chat)

P2P-черви — черви, распространяющиеся при помощи пиринговых (peer-to-peer) файлообменных сетей

IM-черви — черви, использующие для распространения системы мгновенного обмена сообщениями

- Классическими ***сетевыми червями*** являются представители семейства Net-Worm.Win32.Sasser. Эти черви используют уязвимость в службе LSASS Microsoft Windows. При размножении, червь запускает FTP-службу на TCP-порту 5554, после чего выбирает IP-адрес для атаки и отсылает запрос на порт 445 по этому адресу, проверяя, запущена ли служба LSASS. Если атакуемый компьютер отвечает на запрос, червь посылает на этот же порт эксплойт уязвимости в службе LSASS, в результате успешного выполнения которого на удаленном компьютере запускается командная оболочка на TCP-порту 9996. Через эту оболочку червь удаленно выполняет загрузку копии червя по протоколу FTP с запущенного ранее сервера и удаленно же запускает себя, завершая процесс проникновения и активации.

- В качестве примера ***почтового червя*** можно рассмотреть Email-Worm.Win32.Zafi.d. Зараженное сообщение включает в себя выбираемые из некоторого списка тему и текст, содержанием которых является поздравление с праздником и предложение ознакомиться с поздравительной открыткой во вложении. Поздравления могут быть на разных языках. Имя находящегося во вложении файла червя состоит из слова postcard на языке, соответствующем поздравлению, и произвольного набора символов. Расширение файла червя случайным образом выбирается из списка .BAT, .COM, .EXE, .PIF, .ZIP. Для рассылки червь использует адреса электронной почты, найденные на зараженном компьютере. Чтобы получить управление, червь должен быть запущен пользователем.

- ***IRC-Worm.*** Win32.Golember.a является, как следует из названия IRC-червем. При запуске он сохраняет себя в каталоге Windows под именем trlmsn.exe и добавляет в раздел автозапуска реестра Windows параметр со строкой запуска этого файла. Кроме этого червь сохраняет на диск свою копию в виде архива Janey2002.zip и файл-изображение Janey.jpg. Затем червь подключается к произвольным IRC-каналам под различными именами и начинает слать определенные текстовые строки, имитируя активность обычного пользователя. Параллельно всем пользователям этих каналов отсылается заархивированная копия червя.

- Функциональностью распространения через ***P2P-каналы*** обладают многие сетевые и почтовые черви. Например, Email-Worm.Win32.Netsky.q для размножения через файлообменные сети ищет на локальном диске каталоги, содержащие названия наиболее популярных сетей или же слово «shared», после чего кладет в эти каталоги свои копии под различными названиями.

- ***IM-черви*** редко пересылают зараженные файлы непосредственно между клиентами. Вместо этого они рассылают ссылки на зараженные веб-страницы. Так червь IM-Worm.Win32.Kelvir.k посылает через MSN Messenger сообщения, содержащие текст «its you» и ссылку «http://www.malignancy.us/[removed]/pictures.php?email=[email]», по указанному в которой адресу расположен файл червя.

Троянские программы