Вредоносное ПО и средства защиты

Выполнил: Студент гр. 3-2п9

Дзугаев Георгий

Вредоносная программа

Вредоносная программа — это компьютерная программа или внедренный код, пред назначенный для реализации угроз информации, хранящейся в компьютерной системе, ли бо для скрытого нецелевого использования ресурсов системы, либо иного воздействия, препятствующего нормальному функционированию компьютерной системы.

Виды вредоносных программ

Виды вредоносных программ. Проблема вредоносных программ, называемых далее просто «вирусами», — рекламных и шпионских — заслуживает повышенного внимания, поскольку: во-первых, они появляются без ведома получателя; во-вторых, даже при обна ружении вредоносных программ от них трудно избавиться. Последствиями внедрения ви русов являются снижение производительности ПЭВМ, беспорядочная смена пользо вательских настроек, появление новых сомнительных панелей инструментов (аддонов). Ви русы могут глубоко внедряться в сложные механизмы работы ОС так, чтобы в значительной степени осложнить их обнаружение и уничтожение.

КОМПЬЮТЕРНЫЙ ВИРУС

Компьютерный вирус — это разновидность компьютерных программ, обладающих способностью к размножению (самореплицирующихся).

Троян

Троян, или ***троянская программа*** (троян, троянец, троянский конь, трой), — это вирус, проникающий на компьютер под видом безвредной программы.

Вирус не имеет собственного механизма распространения, и этим отличается от вирусов, которые распространяются, прикрепляя себя к обычной программе, и от «червей», которые копируют себя по сети. Если же троян несет вирусное тело, то он становится очагом «заразы».

Трояны крайне просты в написании: простейшие из них состоят из нескольких десятков строк кода языка C++. Троян, запущенный на ПЭВМ, может мешать работе пользователя, шпионить за ним, использовать ресурсы компьютера для целей запустившего его злоумышленника (хакера).

Шпион

Шпион — это вирус, скрытно устанавливающийся на ПЭВМ в целях полного или частичного контроля за работой компьютера и пользователя без согласия последнего.

Существуют и другие определения шпионов. Шпионы способны:

- собирать информацию о наиболее часто посещаемых сайтах;
- запоминать нажатия клавиш на клавиатуре, записывать скриншоты экрана и отправлять информацию хакерам;
- несанкционированно и удаленно управлять компьютером;
- инсталлировать на компьютер пользователя дополнительные программы;
- сканировать порты, пароли и др.;
- изменять параметры ОС (руткиты, перехватчики управления);
- перенаправлять активность браузеров, что влечет за собой посещение веб-сайтов вслепую с риском заражения вирусами.

Сетевой червь

Сетевой червь- это разновидность самовоспроизводящихся вирусов- программ, распространяющихся в локальных и глобальных сетях.

Черви являются самостоятельными программами, которые могут использовать раз личные механизмы распространения. Одни — требуют определенного действия пользовате ля для распространения, например, открытия инфицированного сообщения в клиенте элек тронной почты. Другие — могут распространяться автономно, выбирая и атакуя компьюте ры в полностью автоматическом режиме.

Руткит

Руткит — это вирусная программа или набор программ, использующих технологии сокрытия системных объектов (файлов, процессов, драйверов и др.) посредством обхода механизмов системы.

Руткит позволяет хакеру закрепиться во взломанной системе и скрыть следы своей де ятельности. В системе Windows под термином «руткит» принято понимать программу, ко торая внедряется в систему и перехватывает системные функции или производит замену сис темных библиотек.

Основные признаки заражения

- вывод на экран непредусмотренных сообщений или изображений;
- подача непредусмотренных звуковых сигналов;
- неожиданное открытие и закрытие лотка CD-ROM-устройства;
- самопроизвольный запуск на компьютере каких-либо программ;
- при наличии на ПЭВМ межсетевого экрана появление предупреждений о попытке программы выйти в Интернет, хотя вы это никак не инициировали;
- друзьям или знакомым идут от вас сообщения, которые вы не отправляли;
- наличие в почте массы сообщений без обратного адреса и заголовка.

Косвенные признаки заражения

- частые зависания и сбои в работе компьютера;
- медленная работа компьютера при запуске программ;
- невозможность загрузки ОС;
- исчезновение файлов и каталогов или искажение их содержимого;
- частое несанкционированное обращение к жесткому диску;
- зависание интернет-браузера.

Действия при обнаружении вирусов

- отключить компьютер от локальной сети;
- установить (если не установлен) антивирус;
- получить последние обновления антивирусных баз;
- запустить полную проверку компьютера.

Методы защиты от вредоносных программ

Чтобы снизить риск потерь от воздействия вредоносных программ, рекомендуется:

- использовать современные ОС;
- включать режим автоматического обновления ОС;
- постоянно работать на ПЭВМ исключительно под правами пользователя;
- использовать антивирусы известных производителей с автоматическим обновлением сигнатурных баз;
- использовать персональный Firewall, контролирующий выход в Интернет с персонального компьютера на ос новании политик, которые устанавливает сам пользователь;
- ограничивать физический доступ к компьютеру посторонних лиц;
- использовать внешние носители информации от проверенных источников;
- не открывать компьютерные файлы, полученные от ненадежных источников;
- отключать автозапуск со сменных носителей.

СПАСИБО ЗА ВНИМАНИЕ