

Вредоносное ПО и средства защиты

Выполнил: Студент гр. 3-2п9

Виноградов Виталий

Вредоносная программа

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

Виды вредоносных программ

- ◆ Компьютерный вирус;
- ◆ Троян, или троянская программа;
- ◆ Шпион;
- ◆ Сетевой червь;
- ◆ Руткит

Компьютерный вирус

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

Троян

Троян, или *тройанская 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;
- ◆ устанавливать 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.

Выделяют черви, которые могут инфицировать работающую программу и находиться в оперативном запоминающем устройстве (ОЗУ), не затрагивая жесткие диски. От них можно избавиться перезапуском компьютера. Специфика ОЗУ-резидентных червей заключается в том, что они сами не загружаются, а попадают в ОЗУ, используя динамические библиотеки, которые уже были загружены в память другими программами.

Существуют черви, которые после «успешного» инфицирования памяти сохраняют код в реестре Windows на жестком диске. От таких червей можно избавиться только с помощью антивируса.

Руткит

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

Различают руткиты, работающие в режиме пользователя (user-mode) и работающие в режиме ядра (kernel-mode). Первая категория основана на перехвате функций библиотек пользовательского режима, вторая — на установке в систему драйвера, осуществляющего перехват функций уровня ядра.

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 основании 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.