Защита информации от вредоносных программ

Работу выполнила:
Ястребова
Анастасия

Введение

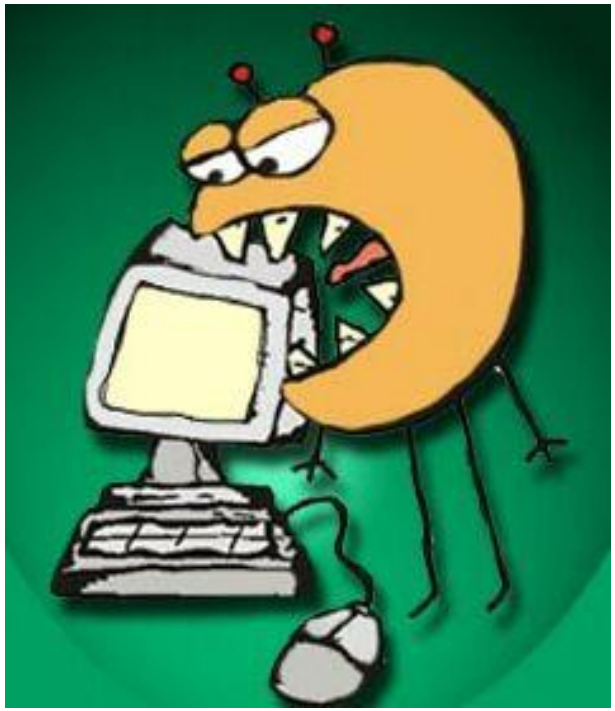
Как происходит заражение компьютера ?

На этот вопрос можно дать очень простой ответ:
"Всему виной Интернет".

ПРИЗНАКИ ЗАРАЖЕНИЯ КОМПЬЮТЕРА

- Вывод на экран непредусмотренных сообщений или изображений
- Подача непредусмотренных звуковых сигналов
- Неожиданное открытие и закрытие лотка CD/DVD дисковода
- Произвольный запуск на компьютере каких-либо программ
- Частые «зависания» и сбои в работе компьютера
- Медленная работа компьютера при запуске программ
- Исчезновение или изменение файлов и папок
- Частое обращение к жесткому диску
- «Зависание» или неожиданное поведение браузера

Вредоносные программы



Вредоносные программы – это программы, наносящие вред данным и программам , хранящимся на компьютере.

Какие бывают вредоносные программы?

Компьютерные вирусы

Название «вирус» по отношению к компьютерным программам пришло из биологии именно по признаку способности к саморазмножению

Вирус «Brain» являлся первым вирусом-невидимкой,обнаружен в 1986 году.

Вирусы можно разделить на:

Неопасные

влияние ограничивается уменьшением свободной памяти на диске, графическими, звуковыми и другими внешними эффектами

Опасные

могут привести к сбоям и «зависаниям» при работе компьютера

Очень опасные

активизация может привести к потере программ и данных (изменению или удалению файлов и каталогов), форматированию винчестера и т. д.

Защита от компьютерных вирусов

Одним из основных способов борьбы с компьютерными вирусами является своевременная профилактика.

1.Необходимо проверять все внешние диски на наличие вирусов, прежде чем копировать или открывать содержащиеся на них файлы или выполнять загрузку компьютера с таких дисков

2.Основным средством защиты информации – это резервное копирование ценных данных, которые хранятся на жестких дисках

1.проникают на компьютер, используя сервисы компьютерных сетей.

2.могут вызывать уничтожение программ и данных

3.похищают персональные данные пользователя.

В сентябре 2001 года началась стремительное «расползание» сетевого червя «Nimda»

Сетевые черви

почтовые

для своего распространения используют электронную почту.

Использующие «уязвимости» ПО

ищет в сети компьютеры, на которых используются ОС и приложения, содержащие критические уязвимости.

Использующие файлообменные сети

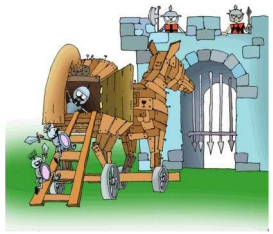
для внедрения в файлообменную сеть червю достаточно скопировать себя в папку обмена файлами на одном из компьютеров

Защита от сетевых червей

Профилактическая защита от почтовых червей состоит в том, что не рекомендуется открывать вложенные в почтовые сообщения файлы, полученные из сомнительных источников.

Профилактическая защита от таких червей, использующих «уязвимость» ПО состоит в том, что рекомендуется своевременно скачивать из Интернета и устанавливать обновления системы безопасности операционной системы и приложений.

Троянские программы



Вредоносные программы ,распространяемые людьми, в отличие от вирусов и червей, которые распространяются самопроизвольно.

Считается, что первым этот термин в контексте компьютерной безопасности употребил в своём отчёте «Computer Security Technology Planning Study» Дэниел Эдвардс

Некоторые виды

для кражи пользовательской информации, относящейся к банковским системам, системам электронных денег и пластиковых карт

для кражи пользовательской информации, относящейся к сетевым играм.

для кражи пользовательских аккаунтов от интернет-пейджеров

Защита от троянских программ

обнаруживаются и удаляются антивирусным и антишпионским ПО точно так же, как и остальные вредоносные программы.

Троянские программы хуже обнаруживаются контекстными методами антивирусов, потому что их распространение лучше контролируется, и экземпляры программ попадают к специалистам антивирусной индустрии с бóльшей задержкой, нежели самопроизвольно распространяемые вредоносные программы.

Шпионские программы

Программой-шпионом (альтернативные названия - Spy, SpyWare, Spy-Ware, Spy Trojan) принято называть ПО, собирающее и передающее кому-либо информацию о пользователе *без его согласия*.

В марте 2005 года под видом поисковой панели для браузера Internet Explorer начала распространяться рекламно-шпионская программа «mwsbar». Программа регистрирует себя в системном реестре и добавляет в автозагрузку, что приводит к изменению настроек браузера и перенаправлению результатов поиска в Интернете на сайт злоумышленника.

Защита от шпионских программ

- Используйте брандмауэр
- Обновляйте свое программное обеспечение
- Настройте параметры безопасности Internet Explorer
- Загрузите и установите антишпионскую защиту
- Посещайте сайты и загружайте более осторожно

Спам

Рассылка коммерческой и иной рекламы или иных видов сообщений лицам, не выражавшим желания их получать

Виды спама

реклама

Некоторые компании, занимающиеся легальным бизнесом, рекламируют свои товары или услуги с помощью спама

антиреклама

Запрещенная законодательством о рекламе информация — например, порочащая конкурентов и их продукцию, — также может распространяться с помощью спама.

фишинг

Он представляет собой попытку спамеров выманить у получателя письма номера его кредитных карточек или пароли доступа к системам онлайновых платежей

«Нигерийские письма»

Такое письмо содержит сообщение о том, что получатель письма может получить каким-либо образом большую сумму денег, а отправитель может ему в этом помочь. Затем отправитель письма просит перевести ему немного денег под предлогом, например, оформления документов или открытия счета. Выманивание этой суммы и является целью мошенников.

Защита от спама

Самый надёжный способ борьбы со спамом — не позволить спамерам узнать электронный адрес. Это трудная задача, но некоторые меры предосторожности можно предпринять.

ДЕЙСТВИЯ ПРИ НАЛИЧИИ ПРИЗНАКОВ ЗАРАЖЕНИЯ КОМПЬЮТЕРА

1. Сохранить результаты работы на внешнем носителе

2. Отключить компьютер от локальной сети и Интернета, если он к ним был подключен

3. Загрузиться в режиме защиты от сбоев или с диска аварийной загрузки Windows (если компьютер выдает ошибку, когда вы его включаете)

4. Запустить антивирусную программу

АНТИВИРУСНЫЕ ПРОГРАММЫ

Принцип работы антивирусных программы основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вирусов.

Для поиска известных вирусов используются сигнатуры, т.е. некоторые постоянные последовательности двоичного кода, специфичные для конкретного вируса.

Для поиска новых вирусов используются алгоритмы эвристического сканирования, т.е. анализ последовательности команд в проверяемом объекте.

Большинство антивирусных программ сочетает в себе функции постоянной защиты (антивирусный монитор) и функции защиты по требованию пользователя (антивирусный сканер).

Ссылки:

Как происходит заражение компьютера?

http://smolin.delnet.ru/sistemnoe-administrirovanie/137-kak-proiskhodit-zarazhenie-kompyutera-virusom

Признаки заражения компьютера

http://support.kaspersky.ru/790?el=88446

Вредоносные программы

http://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0

Компьютерные вирусы

http://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81

Шпионские программы

http://z-oleg.com/secur/articles/spyware.php

Спам

http://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B0%D0%BC

Троянские программы

http://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D1%8F%D0%BD%D1%81%D0%BA%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0

Сетевые черви

http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%87%D0%B5%D1%80%D0%B2%D1%8C

Антивирусные программы

https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0

Тест по пройденной теме

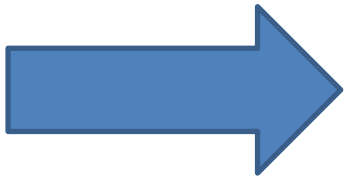
начать

программы, наносящие вред данным и программам , хранящимся на компьютере называют

Антивирусными

Вредоносными

«snaper»

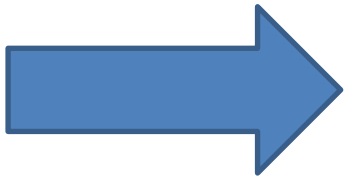


Откуда произошло название «вирус»?

Математика

биология

История

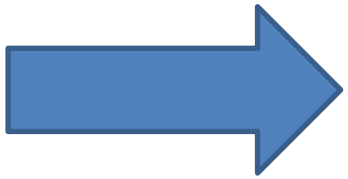


Разновидность спама

Почтовый

Опасный

Реклама



Спасибо за внимание!