Презентация подготовленна для конкурса „интернешка”

Определение вредоносных программ:

Вредоносными программами являются программы, наносящие вред данным и программам, хранящимся в компьютере

Типы вредоносных программ:

Вирусы, черви, троянские и хакерские программы.

Эта группа объединяет наиболее распространенные и опасные категории вредоносных программ. Защита от которых обеспечивает минимально допустимый уровень безопасности

Шпионское, рекламное программное обеспечение, программы скрытого дозвона.

Данная группа объединяет в себе, потенциально опасное программное обеспечение, которое может причинить неудобство пользователю или даже нанести значительный ущерб.

Потенциально опасное программное обеспечение. Эта группа включает программы, которые не являются вредоносными или опасными, однако при некотором стечении обстоятельств могут быть использованы для нанесения вреда вашему компьютору.

Внимание!

За создание , использование и распространение вредоносных программ в России предусмотрена уголовная ответственность!

Антивирусные программы

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

Для поиска известных вредоносных программ используются сигнатуры.

Признаки заражения компьютера.

Вывод на экран непредусмотренных сообщений или изображений.

Подача непредусмотренных звуковых сигналов.

Неожиданное открытие и закрытие лотка CD/DWD дисковода

Произвольный запуск на компьютере каких-либо программ

Признаки заражения компьютера

Частые зависания и сбои в работе компьютера.

Медленная работа компьютера при запуске программ

Исчезновение или изменение файлов и папок.

Частое обращение к жесткому диску (часто моргает лампочка на системном блоке)

Первые вирусы

- Первыми известными вирусами являются Virus 1,2,3Первыми известными вирусами являются Virus 1,2,3 и Elk ClonerПервыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple IIПервыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 годуПервыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году. Зимой1984 годаПервыми известными вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году. Зимой1984

Классификация вирусов

- Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности. Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет. Растёт и функциональность вирусов, которую они перенимают от других видов программ.
- В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:
- по поражаемым объектам (файловые вирусыпо поражаемым объектам (файловые вирусы, загрузочные вирусыпо поражаемым объектам (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы, поражающие исходный код);
- файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.
- по поражаемым операционным системам и платформам (DOSпо поражаемым операционным системам и платформам (DOS, Microsoft Windowsпо поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unixпо поражаемым операционным системам и платформам (DOS, Microsoft Windows, Unix, Linux);
- по технологиям, используемым вирусом (полиморфные вирусыпо технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусыпо технологиям, используемым вирусом (полиморфные вирусы, стелс-вирусы, руткиты);
- по языку, на котором написан вирус (ассемблерпо языку, на котором написан вирус (ассемблер, высокоуровневый язык программированияпо языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язык и др.);
- по дополнительной вредоносной функциональности (бэкдорыпо дополнительной вредоносной функциональности (бэкдоры, кейлоггерыпо дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионыпо дополнительной вредоносной функциональности (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

Профилактика и лечение

- В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:
- Не работать под привилегированными учётными записями без крайней необходимости. (Учётная запись администратора в Windows)
- Не запускать незнакомые программы из сомнительных источников.
- Стараться блокировать возможность несанкционированного изменения системных файлов.
- Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
- Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
- Пользоваться только доверенными дистрибутивами.
- Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания.
- Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

Первый антивирус

Первые антивирусные утилиты появились зимой 1984 года. Анди Хопкинс (англ. Andy Hopkins) написал программы CHK4BOMB и BOMBSQAD. CHK4BOMB позволяла проанализировать текст загрузочного модуля и выявляла все текстовые сообщения и «подозрительные» участки кода (команды прямой записи на диск и др.). Благодаря своей простоте (фактически использовался только контекстный поиск) и эффективности CHK4BOMB получила значительную популярность. Программа BOMBSQAD.COM перехватывает операции записи и форматирования, выполняемые через BIOS. При выявлении запрещённой операции можно разрешить её выполнение.
[править]Первый резидентный антивирус
В начале 1985 года Ги Вонг (англ. Gee Wong) написал программу DPROTECT — резидентную программу, перехватывающую попытки записи на дискеты и винчестер. Она блокировала все операции (запись, форматирование), выполняемые через BIOS. В случае выявления такой операции программа требовала рестарта системы.