Компьютерные вирусы. Антивирусные программы.

Презентация подготовлена для конкурса «Интернешка» Ученицей 9 «А» класса Батищевой Анастасией

Что такое компьютерные вирусы?

Компьютерные вирусы – это специально написанная небольшая по размерам программа, которая может «приписывать» себя к другим программам, а также выполнять различные нежелательные действия на компьютере.

Стадии функционирования вирусов

Виды вирусов по принципу функционирования

1. Вирусы-паразиты (Parasitic)
2. Вирусы-репликаторы (Worm)
3. Трояны (Trojan)
4. Вирусы-невидимки (Stealth)
5. Самошифрующиеся вирусы
6. Матирующиеся вирусы
7. "Отдыхающие" вирусы

Вирусы - паразиты

Вирусы-паразиты (Parasitic) – вирусы, работающие с файлами программ, частично выводящие их из строя. Могут быть легко выявлены и уничтожены. Однако, зачастую, файл-носитель остается не пригодным.

Вирусы - репликаторы

Вирусы-репликаторы (Worm) – вирусы, основная задача которых как можно быстрее размножится оп всем возможным местам хранения данных и коммуникациям. Зачастую сами не предпринимают никаких деструктивных действий, а являются транспортом для других видов вредоносного кода.

Трояны

Трояны (Trojan) – получили свое названия в честь “Троянского коня”, так как имеют схожий принцип действия. Этот вид вирусов массирует свои модули под модули используемых программ, создавая файлы со схожими именами и параметрами, а так же подменяют записи в системном реестре, меняя ссылки рабочих модулей программ на свои, вызывающие модули вируса. Деструктивные действия сводятся к уничтожению данных пользователя, рассылке СПАМа и слежения за действиями пользователя. Сами размножатся зачастую не могут. Выявляются достаточно сложно, так как простого сканирования файловой системы не достаточно.

Вирусы - невидимки

Вирусы-невидимки (Stealth) – названы по имени самолета-невидимки "stealth", наиболее сложны для обнаружения, так как имеют свои алгоритмы маскировки от сканирования. Маскируются путем подмены вредоносного кода полезным во время сканирования, временным выведением функциональных модулей из работы в случае обнаружения процесса сканирования, сокрытием своих процессов в памяти и т.д.

Самошифрующиеся вирусы

Самошифрующиеся вирусы – вирусы вредоносный код которых хранится и распространяется в зашифрованном виде, что позволяет им быть недоступными для большинства сканеров.

Матирующиеся вирусы

Матирующиеся вирусы – вирусы не имеющие постоянных сигнатур. Такой вирус постоянно меняет цепочки своего кода в процессе функционирования и размножения. Таким образом, становясь неуязвимым для простого антивирусного сканирования. Для их обнаружения необходимо применять эвристический анализ.

«Отдыхающие» вирусы

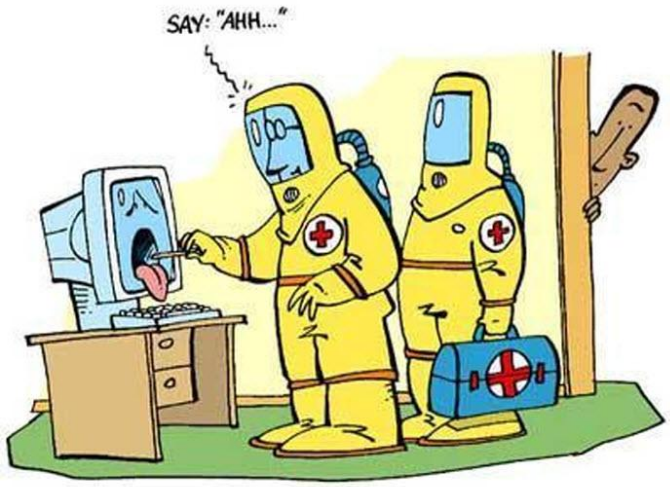
"Отдыхающие" вирусы – являются очень опасными, так как могут очень продолжительное время находится в состоянии покоя, распространяясь по компьютерным сетям. Активация вируса происходит при определенном условии, зачастую по определенной дате, что может вызвать огромные масштабы одновременного заражения. Примером такого вируса является вирус CHIH или Чернобыль, который активировался в день годовщины аварии на ЧАЭС, вызвав выход из строя тысяч компьютеров.

Антивирусные программы

Антивирусная программа (антивирус) — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Работа антивируса

1. Поиск в базе данных антивирусного ПО сигнатур вирусов.
2. Если найден инфицированный код в памяти (оперативной и/или постоянной), запускается процесс «карантина», и процесс блокируется.
3. Зарегистрированная программа обычно удаляет вирус, незарегистрированная просит регистрации и оставляет систему уязвимой.



Виды антивирусных программ

1. Детекторы
2. Доктора (фаги)
3. Ревизоры
4. Доктора-ревизоры
5. Фильтры и вакцины (иммунизаторы

Примеры антивирусных программ

Среди платных	Среди бесплатных:
· Symantec · McAfee · Dr.Web · Лаборатория Касперского · ESET Nod32 · Trend Micro · BitDefender	· AntiVir (Avira) · Avast! · AVG · Comodo

Недостатки антивирусов

Ø Ни одна из существующих антивирусных технологий не может обеспечить полной защиты от вирусов.

Ø Антивирусная программа забирает часть вычислительных ресурсов системы, нагружая центральный процессор и жёсткий диск. Особенно это может быть заметно на слабых компьютерах. Замедление в фоновом режиме работы может достигать 380 %.

Ø Антивирусные программы могут видеть угрозу там, где её нет (ложные срабатывания).

Ø Антивирусные программы загружают обновления из Интернета, тем самым расходуя трафик.

Ø Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы не обнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. Однако во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.

Спасибо за внимание!!!