Компьютерные вирусы и антивирусные программы

Презентация подготовлена для конкурса «Интернешка»

Вирусы

Что такое компьютерный вирус?

Компьютерный вирус — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Вирусы

Компьютерные вирусы делятся на несколько видов по среде обитания

1. Загрузочные вирусы.
2. Файловые вирусы.
3. Файлово-загрузочные вирусы.
4. Сетевые вирусы.
5. Документные вирусы.

Загрузочные вирусы

Загрузочные вирусы проникают в загрузочные сектора устройств хранения данных. При загрузке операционной системы с зараженного диска происходит активация вируса. Его действия могут состоять в нарушении работы загрузчика операционной системы, что приводит к невозможности ее работы, либо изменении файловой таблицы, что делает недоступным определенные файлы.

Файловые вирусы

Файловые вирусы заражают файлы компьютера. Заражение может проводиться либо изменением кода атакуемого файла, либо созданием его модифицированной копии. Таким образом, вирус, находясь в файле, активируется при доступе к этому файлу, инициируемому пользователем или самой ОС. Файловые вирусы – наиболее распространенный вид компьютерных вирусов.

Файлово-загрузочные вирусы

Файлово-загрузочные вирусы обедняют в себе возможности двух предыдущих групп, что позволяет им представлять серьезную угрозу работе компьютера.

Сетевые вирусы

Сетевые вирусы распространяются посредством сетевых служб и протоколов. Они очень опасные, так как заражение не остается в пределах одного компьютера или даже одной локальной сети, а начинает распространятся по разнообразным каналам связи.

Документные вирусы

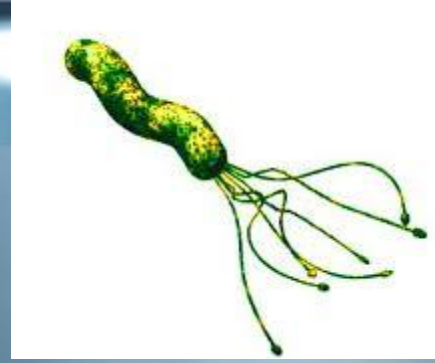
Документные вирусы заражают файлы современных офисных систем через возможность использования в этих системах макросов (заранее заданных микропрограмм).

Вирусы

Также компьютерные вирусы делятся на несколько видов по своему функционированию

1. Вирусы-паразиты
2. Вирусы-репликаторы
3. Трояны
4. Вирусы-невидимки
5. Самошифрующиеся вирусы
6. Матирующиеся вирусы
7. «Отдыхающие» вирусы

Вирусы-паразиты

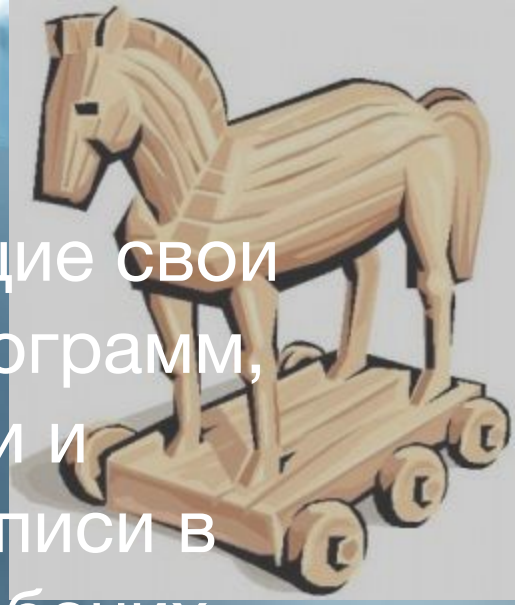


Вирусы-паразиты (Parasitic) – вирусы, работающие с файлами программ, частично выводящие их из строя. Могут быть легко выявлены и уничтожены. Однако, зачастую, файл-носитель остается не пригодным.

Вирусы-репликаторы

Вирусы-репликаторы (Worm) – вирусы, основная задача которых как можно быстрее размножится по 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) – вирусы, массирующие 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) – нзваны по имени самолета-невидимки "stealth", наиболее сложны для обнаружения, так как имеют свио 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.

Антивирусные программы

Что такое антивирус?

Антивирусная программа – специализированная программа для обнаружения компьютерных вирусов, а также нежелательных программ вообще и восстановления заражённых такими программами файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом.

Топ лучших антивирусов

1. Kaspersky Internet Security 2015
2. Bitdefender Internet Security
3. 360 Total Security (бесплатный!)
4. Avira Internet Secu
5. ESET Smart Secur

Спасибо за внимание