Компьютерные вирусы

Введение

- **Компью́терный ви́рус** — разновидность компьютерных программ, отличительной особенностью которых является способность к размножению (самореплицирование). В дополнение к этому вирусы могут без ведома пользователя выполнять прочие произвольные действия, в том числе наносящие вред пользователю и/или компьютеру. По этой причине вирусы относят к вредоносным программам.
- 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.

История развития

- Основы теории самовоспроизводящихся механизмов заложил американец венгерского происхождения Джон фон Нейман, который в **1951** году предложил метод создания таких механизмов. С **1961** года известны рабочие примеры таких программ.

- Первыми известными собственно вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году.
- Первые вирусные эпидемии относятся к **1987-1989 годам**: Brain, Jerusalem, червь Морриса , DATACRIME.

- **в 1990** году появляются специализированная BBS Virus Exchange, «Маленькая чёрная книжка о компьютерных вирусах» Марка Людвига, первый коммерческий антивирус Symantec Norton Antivirus.
- В **1992 г**оду появились первый конструктор вирусов для PC — VCL
- В **1996 году** появился первый вирус для Windows 95 — **Win95.Boza**, а в декабре того же года — первый резидентный вирус для нее — Win95.Punch.

- . **В 2004** г. беспрецедентные по масштабам эпидемии вызывают MsBlast , Sasser и Mydoom
- Набирает обороты самый современный вид вирусов — черви-ботнеты

Классификации:

- **Загрузочные:**

ПНЗ (ПЗУ) - ВИРУС - ПНЗ (диск) -СИСТЕМА

- **Файловые:**

При запуске вирус получает управление, производит некоторые действия и передает управление «хозяину».

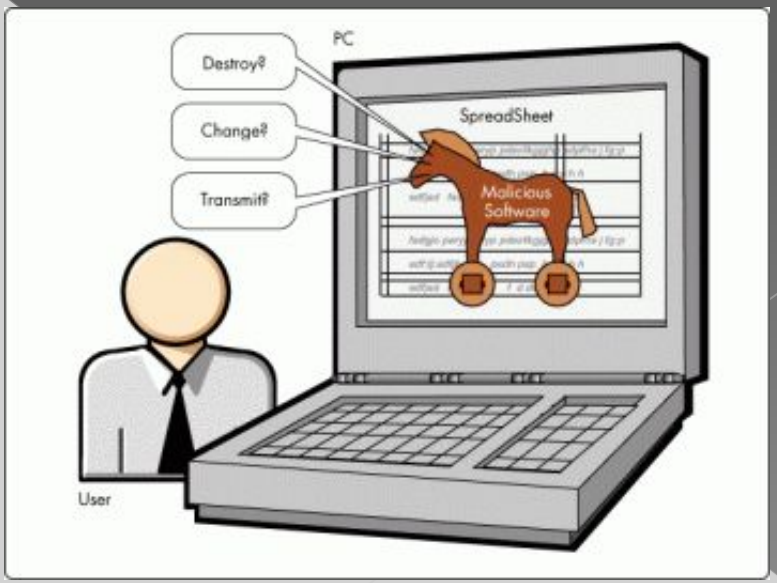
- **Файлово-загрузочные:**

Основное разрушительное действие - шифрование секторов винчестера.

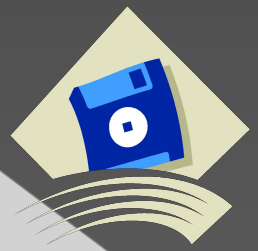
Виды компьютерных вирусов

- Рекламные программы
- Бэкдоры (Backdoor)
- Bot-сеть
- Эксплойт
- Hoax (дословно шутка, ложь)
- Ловушки
- Макровирусы
- Фарминг

- Фишинг
- Программные вирусы
- Руткит
- Скрипт-вирусы и черви
- Шпионское ПО
- Троянские программы
- Зомби



Каналы распространения



- Дискеты
- Флеш-накопители

- Электронная почта
- Системы обмена мгновенными сообщениями

- Веб-страницы
- Интернет и локальные сети (черви)

Троянские программы

- **Май Sender** - тип Троянов, работающих на основе отправки информации "хозяину". На данный момент это очень распространенный вид Троянов. С помощью такого типа "коней" люди, настроившие их, могут получать по почте аккаунты Интернета, пароли ICQ, почтовые пароли. MailSender никак не зависит от "хозяина"

Троянские программы

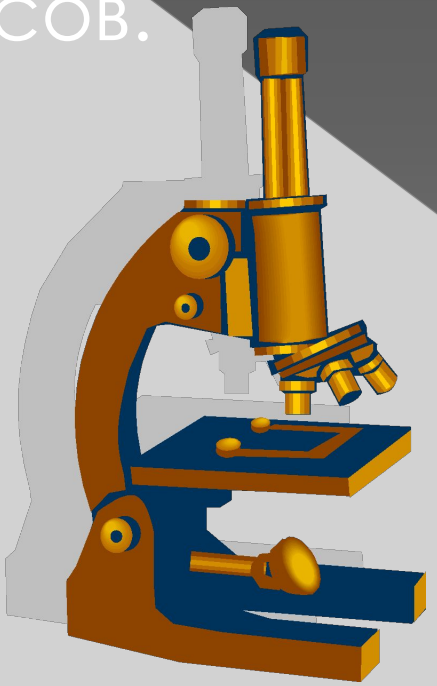
- **BackDoor -** тип Трояна, функции которого включают в себя все, на что способен Троян типа Mail Sender, плюс еще десяток-другой функций удаленного администрирования. Трояны такого типа дают кому угодно полный доступ к компьютеру.

Троянские программы

- **Log Writer** - это последний тип Троянов (из основных), копирующий всю информацию, вводимую с клавы, и записывающий ее в файл, который впоследствии будет либо отправлен на определенный E-Mail адрес, либо просмотрен через FTP

Антивирусы

- 1) программы-детекторы: предназначены для нахождения зараженных файлов одним из известных вирусов.



Антивирусы

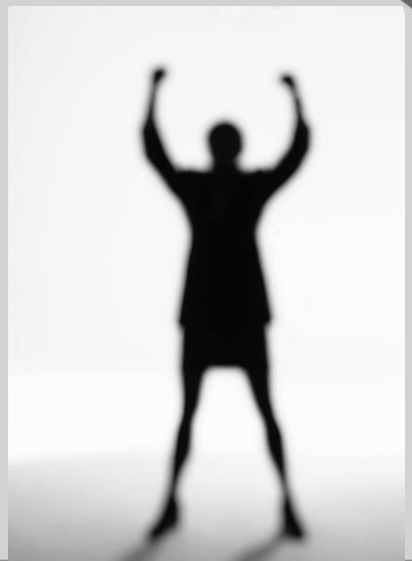
- 2) программы-лекари: предназначены для лечения зараженных дисков и программ.
- 3) программы-ревизоры: предназначены для выявления заражения вирусом файлов, а также нахождение поврежденных файлов.

Антивирусы

- 4) лекари-ревизоры: предназначены для выявления изменений в файлах и системных областях дисков и, в случае изменений, возвращают их в начальное состояние.

Антивирусы

- 5) программы-фильтры: предназначены для перехвата обращений к операционной системе, которые используются вирусами для размножения и сообщают об этом пользователя.



Антивирусы

- 6) программы-вакцины: используются для обработки файлов и boot-секторов с целью предупреждения заражения известными вирусами.
- Одни из самых известных антивирусов:
- **DRWEB, Касперский,AVG, AVP и другие.**