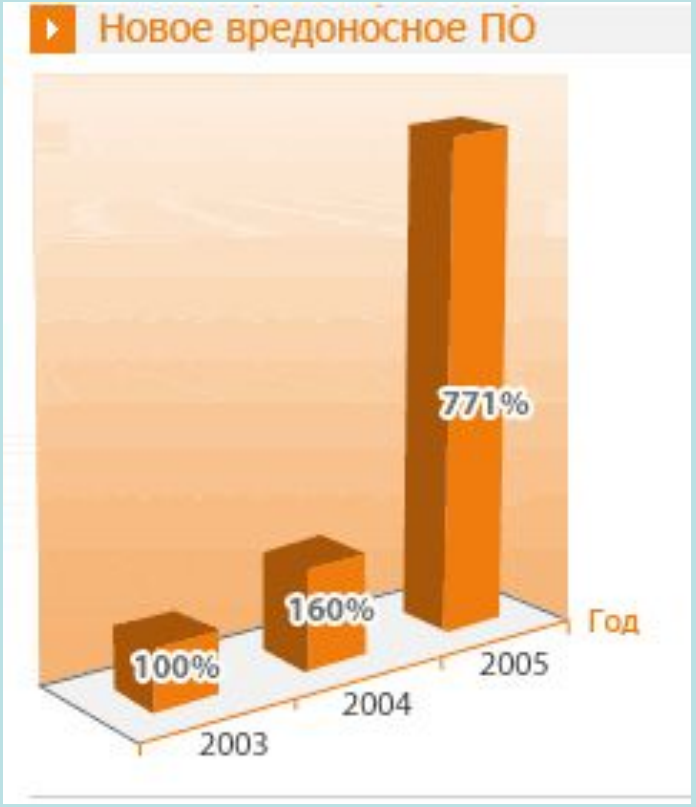
Вредоносные программы и антивирусные программы

ВРЕДОНОСНЫЕ ПРОГРАММЫ

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

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



ПЕРВЫЕ ВРЕДОНОСНЫЕ И АНТИВИРУСНЫЕ ПРОГРАММЫ

Первый вирус, появившийся в июле 1982 г., был написан 15-летним школьником Ричем Скрента (Rich Skrenta) для платформы Apple II и относился к категории загрузочных. Он распространялся, заражая код загрузочных секторов дискет для операционной системы Apple II. При загрузке компьютера вирус оставался в памяти и заражал все дискеты, которые вставлялись в дисковод.

Жертвами вируса стали компьютеры друзей и знакомых автора, а также его учитель математики.

Как многие старые вирусы, Elk Cloner отличался визуальными проявлениями: при каждой 50-й загрузке он показывал короткое стихотворение («Elk Cloner - это уникальная программа. Она проникнет на все ваши диски, профильтрует ваши чипы. О да, это Cloner. Она приклеится к Вам, как клей. Программа способна изменить и RAM. Пустите к себе Cloner»).

```
Elk Cloner:
The program with a personality

     It will get on all your disks
       It will infiltrate your chips
         Yes it's Cloner!

     It will stick to you like glue
       It will modify ram too
         Send in the Cloner!
```

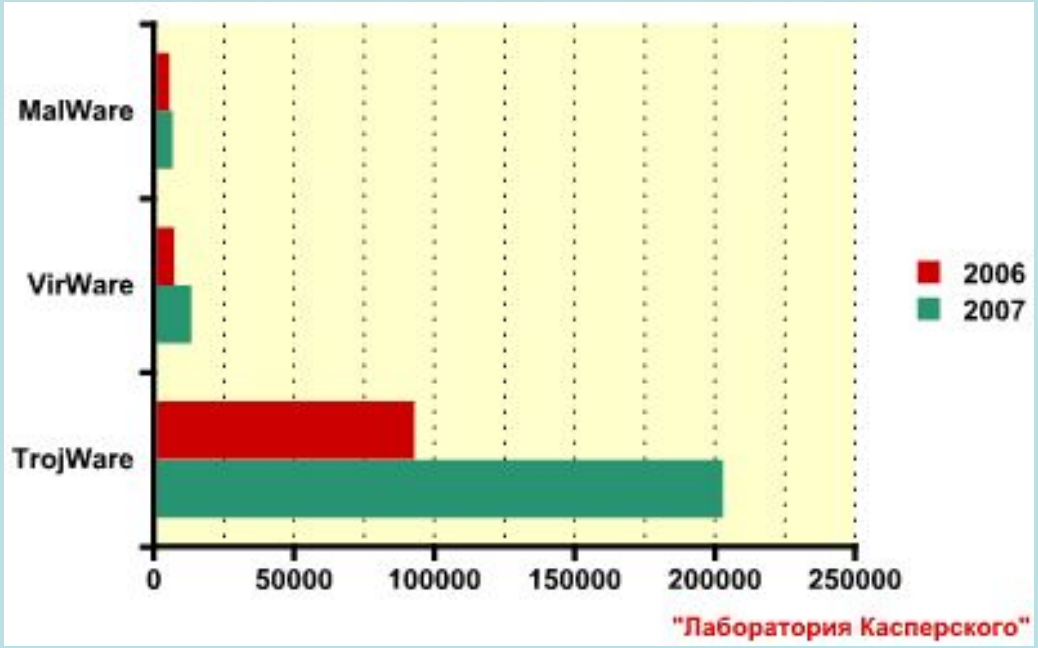
Первый антивирус всего лишь на два года младше своего врага. В 1984 г. программист Анди Хопкинс (Andy Hopkins) написал утилиты, позволяющие перехватывать некоторые операции, выполняемые через BIOS, а также анализировать загрузочный модуль, что давало возможность бороться с некоторыми типами вирусов того времени.

ТИПЫ ВРЕДОНОСНЫХ ПРОГРАММ

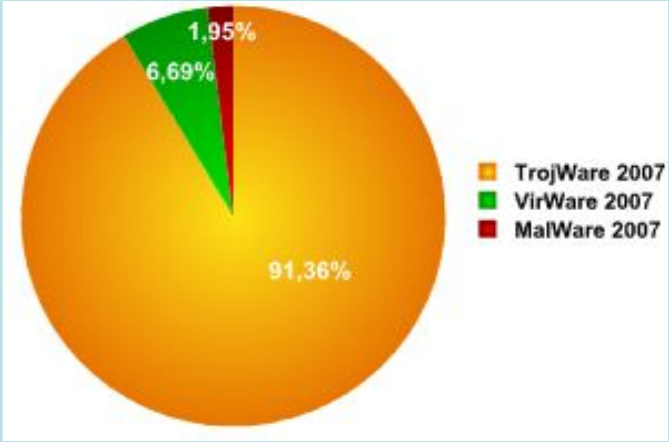
- КОМПЬЮТЕРНЫЕ ВИРУСЫ
- СЕТЕВЫЕ ЧЕРВИ
- ТРОЯНСКИЕ ПРОГРАММЫ
- ПРОГРАММЫ ПОКАЗА РЕКЛАМЫ (ADWARE)
- ПРОГРАММЫ-ШПИОНЫ (SPYWARE)
- ХАКЕРСКИЕ УТИЛИТЫ

ТИПЫ ВРЕДОНОСНЫХ ПРОГРАММ

Количество новых вредоносных программ, обнаруженных аналитиками «Лаборатории Касперского» в 2007 году



Распределение классов вредоносных программ (первое полугодие 2007 г.)



Согласно классификации «Лаборатории Касперского»:
TrojWare: различные троянские программы без возможности самостоятельного размножения (backdoor, rootkit и всевозможные trojan);
VirWare: саморазмножающиеся вредоносные программы (вирусы и черви);
Other MalWare: программное обеспечение, интенсивно используемое злоумышленниками при создании вредоносных программ и организации атак.

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).

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

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