Компьютерные вирусы

Свойства

Вирус– это программа, обладающая способностью к самовоспроизведению.

Классификация

По среде обитания вирусы делятся на:

- загрузочные
- сетевые
- файловые
- файлово-загрузочные

По способу заражения:

резидентные

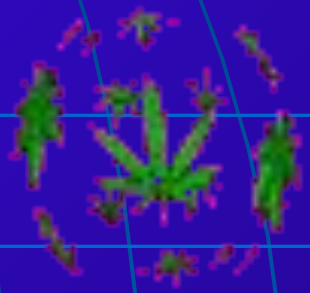
оставляют в оперативной памяти свою резидентную часть, которая потом перехватывает обращение ОС к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения или перезагрузки компьютера

нерезидентные

не заражают память компьютера и являются активными ограниченное время.

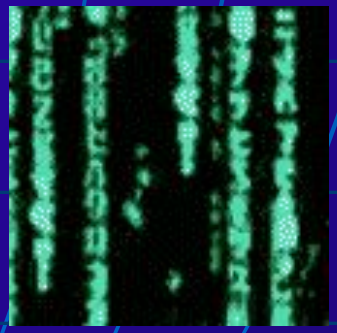
По степени воздействия:

неопасные



опасные

очень опасные

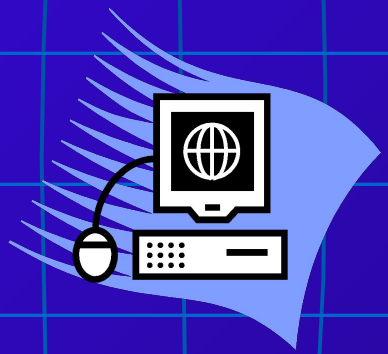


По особенностям алгоритма:

паразитические

полиморфные

черви



троянские

невидимки

и т. д.

Загрузочные вирусы

Схема функционирования загрузочного вируса

ПНЗ (ПЗУ) - ПНЗ (диск) - СИСТЕМА

вирус

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

Файловые вирусы

При запуске инфицированного файла вирус получает управление, производит некоторые действия и передает управление. Затем вирус ищет новый объект для заражения – подходящий по типу файл, который еще не заражен. Заражая файл, вирус внедряется в его код, чтобы получить управление при запуске этого файла.

Полиморфные вирусы

вирусы, модифицирующие свой код в зараженных программах таким образом, что два экземпляра одного и того же вируса могут не совпадать ни в одном бите.

вирусы с самомодифицирующимися расшифровщиками. Цель такого шифрования: имея зараженный и оригинальный файлы, вы все равно не сможете проанализировать его код.

Некоторые вирусы после запуска оставляют в оперативной памяти компьютера специальные модули. Они перехватывают обращение программ к дисковой подсистеме компьютера. Если такой модуль обнаруживает, что программа пытается прочитать зараженный файл или системную область диска, он подменяет читаемые данные.

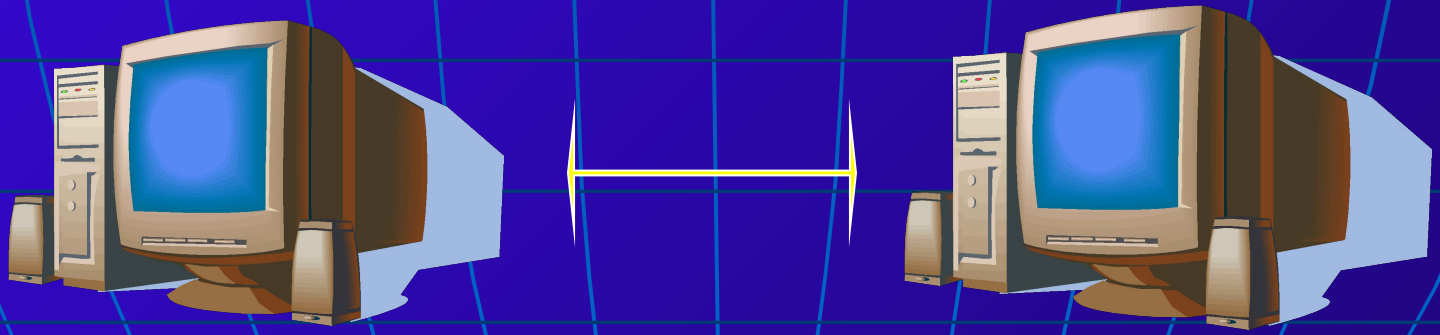
Стелс-вирусы

Троянский конь – это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания.

Программные закладки также содержат некоторую функцию, наносящую ущерб, но эта функция, наоборот, старается быть как можно незаметнее, т.к. чем дольше программа не будет вызывать подозрений, тем дольше закладка сможет работать.

Основная функция вирусов типа червь – взлом атакуемой системы. Они распространяются по глобальным сетям, поражая целые системы, а не отдельные программы.

Пути проникновения



1. прекращение работы или неправильная работа ранее успешно функционировавших программ
2. медленная работа компьютера
3. невозможность загрузки операционной системы
4. исчезновение файлов и каталогов или искажение их содержимого
5. изменение даты и времени модификации файлов
6. изменение размеров файлов
7. неожиданное значительное увеличение количества файлов на диске
8. существенное уменьшение размера свободной оперативной памяти
9. вывод на экран непредусмотренных сообщений или изображений
10. подача непредусмотренных звуковых сигналов

частые зависания и сбои в работе компьютера

Методы защиты

Чего ожидать в последующие годы?

Основными проблемами останутся:

полиморфные вирусы

макро-вирусы

сетевые вирусы