Компьютерные вирусы

Выполнил: студент группы МДИ-108
Котькин Максим

Компьютерные вирусы и антивирусные программы

Персональный компьютер играет в жизни современного человека важную роль, поскольку он помогает ему почти во всех областях его деятельности. Современное общество все больше вовлекается в виртуальный мир Интернета. Но с активным развитием глобальных сетей актуальным является вопрос информационной безопасности, так как проникающие их сети вирусы могут нарушить целостность и сохранность вашей информации. Защита компьютера от вирусов – это та задача, решать которую приходится всем пользователям, и особенно тем, кто активно пользуется Интернетом или работает в локальной сети.

Что же такое вирус? И чем биологический вирус отличается от компьютерного?

Обратимся к вирусной энциклопедии «Лаборатории Касперского», электронной энциклопедии Кирилла и Мефодия и к толковому словарю русского языка С.И. Ожегова и Н.Ю. Шведовой

Вирус – мельчайшая неклеточная частица, размножающаяся в живых клетках, возбудитель инфекционного заболевания.

Толковый словарь русского языка С. И. Ожегова и Н. Ю. Шведовой

Компьютерный вирус – специально созданная небольшая программа, способная к саморазмножению, засорению компьютера и выполнению других нежелательных действий.

Энциклопедия вирусов
«Лаборатории Касперского
http://www.viruslist.com/ru/viruses/encyclopedia

История вирусов

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. Зимой 1984 года появились первые антивирусные утилиты — CHK4BOMB и BOMBSQAD авторства Анди Хопкинса (англ. *Andy Hopkins*). В начале 1985 года Ги Вонг (англ. *Gee Wong*) написал программу DPROTECT — первый резидентный антивирус.

Первые вирусные эпидемии относятся к 1987-1989 годам: Brain (более 18 тысяч зараженных компьютеров, по данным McAfee), Jerusalem (проявился в пятницу 13 мая 1988 г., уничтожая программы при их запуске), червь Морриса (свыше 6200 компьютеров, большинство сетей вышло из строя на срок до пяти суток), DATACRIME (около 100 тысяч зараженных ПЭВМ только в Нидерландах).

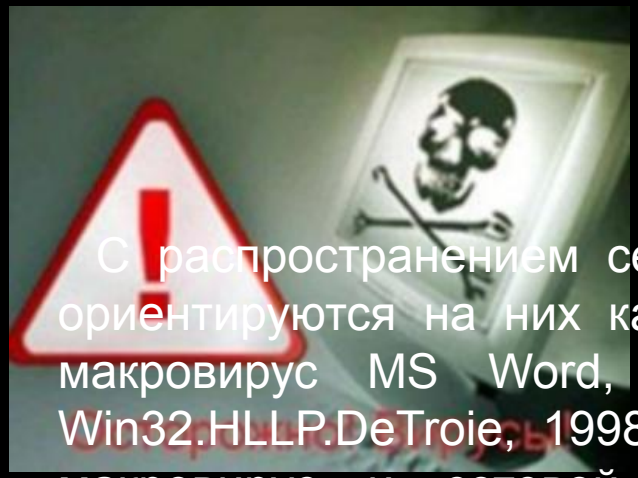
Тогда же оформились основные классы двоичных вирусов: сетевые черви (червь Морриса, 1987), «троянские кони» (AIDS, 1989), полиморфные вирусы (Chameleon, 1990), стелс-вирусы (Frodo, Whale, 2-я половина 1990).

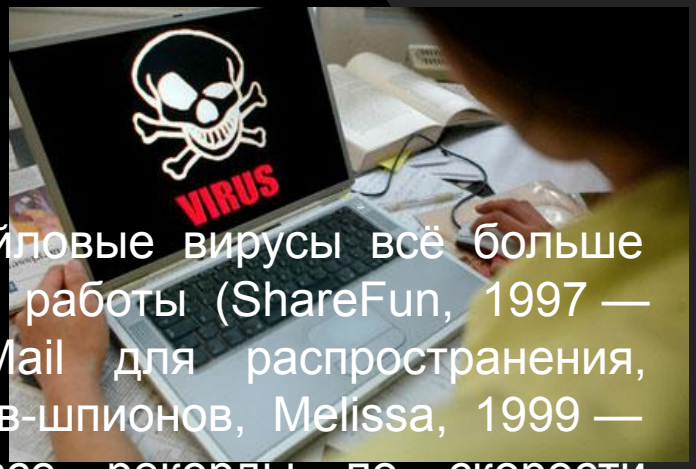
Параллельно оформляются огранизованные движения как про-, так и антивирусной направленности: в 1990 году появляются специализированная BBS Virus Exchange, «Маленькая чёрная книжка о компьютерных вирусах» Марка Людвига, первый коммерческий антивирус Symantec Norton Antivirus.

В 1992 году появились первый конструктор вирусов для PC — VCL (для Amiga конструкторы существовали и ранее), а также готовые полиморфные модули (MtE, DAME и TPE) и модули шифрования для встраивания в новые вирусы.

В несколько последующих лет были окончательно отточены стелс- и полиморфные технологии (SMEG.Pathogen, SMEG.Queeg, OneHalf, 1994; NightFall, Nostradamus, Nutcracker, 1995), а также испробованы самые необычные способы проникновения в систему и заражения файлов (Dir II — 1991, PMBS, Shadowgard, Cruncher — 1993). Кроме того, появились вирусы, заражающие объектные файлы (Shifter, 1994) и исходные тексты программ (SrcVir, 1994). С распространением пакета Microsoft Office получили распространение макровирусы (Concept, 1995).

В 1996 году появился первый вирус для Windows 95 — Win95.Boza, а в декабре того же года — первый резидентный вирус для нее — Win95.Punch.





С распространением сетей и Интернета файловые вирусы всё больше ориентируются на них как на основной канал работы (ShareFun, 1997 — макровирус MS Word, использующий MS-Mail для распространения, Win32.HLLP.DeTroie, 1998 — семейство вирусов-шпионов, Melissa, 1999 — макровирус и сетевой червь, побивший все рекорды по скорости распространения). Эру расцвета «троянских коней» открывает утилита скрытого удаленного администрирования BackOrifice (1998) и последовавшие за ней аналоги (NetBus, Phase).

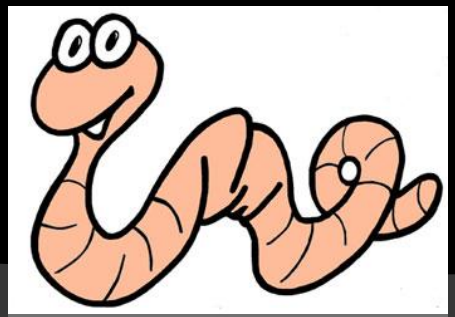
Вирус Win95.CIH достиг апогея в применении необычных методов, перезаписывая Flash Bios зараженных машин (эпидемия в июне 1998 считается самой разрушительной за предшествующие годы).

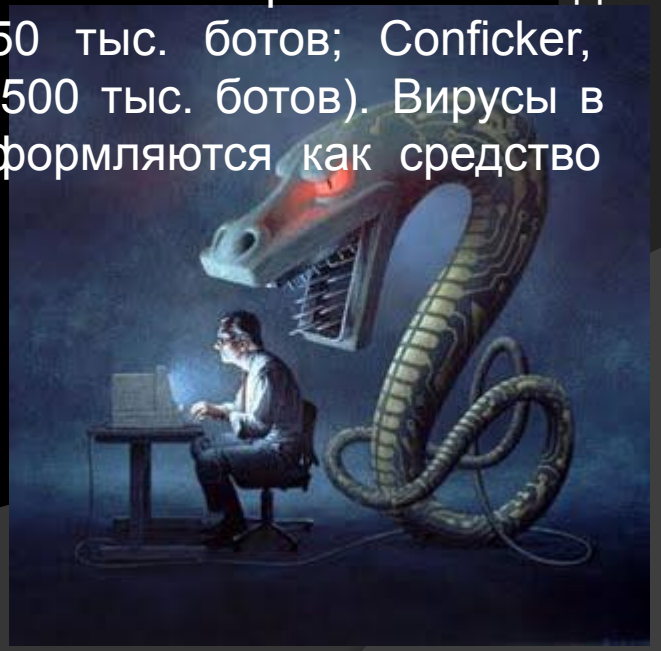
В конце 1990-х — начале 2000-х с усложнением ПО и системного окружения, массовым переходом на сравнительно защищенные Windows семейства NT, закреплением сетей как основного канала обмена данными, а также успехами антивирусных технологий в обнаружении вирусов, построенных по сложным алгоритмам, последние стали всё больше заменять внедрение в файлы на внедрение в операционную систему (необычный автозапуск, руткиты) и подменять полиморфизм огромным количеством видов (число известных вирусов растет экспоненциально).

Вместе с тем, обнаружение в Windows и другом распространенном ПО многочисленных уязвимостей открыло дорогу червям-эксплоитам. В 2004 г. беспрецедентные по масштабам эпидемии вызывают MsBlast (более 16 млн систем по данным Microsoft), Sasser и Mydoom (оценочные ущербы 500 млн долл. и 4 млрд долл. соответственно).

Кроме того, монолитные вирусы в значительной мере уступают место комплексам вредоносного ПО с разделением ролей и вспомогательными средствами (троянские программы, загрузчики/дропперы, фишинговые сайты, спам-боты и пауки). Также расцветают социальные технологии — спам и фишинг — как средство заражения в обход механизмов защиты ПО.

Вначале на основе троянских программ, а с развитием технологий p2p-сетей — и самостоятельно — набирает обороты самый современный вид вирусов — черви-ботнеты (Rustock, 2006, ок. 150 тыс. ботов; Conficker, 2008—2009, более 7 млн ботов; Kraken, 2009, ок. 500 тыс. ботов). Вирусы в числе прочего вредоносного ПО окончательно оформляются как средство киберпреступности.





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 ОСОБЕННОСТЯМ АЛГОРИТМА:

паразитические

полиморфные

черви

троянские

невидимки

и т. д.

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.

Стелс-вирусы

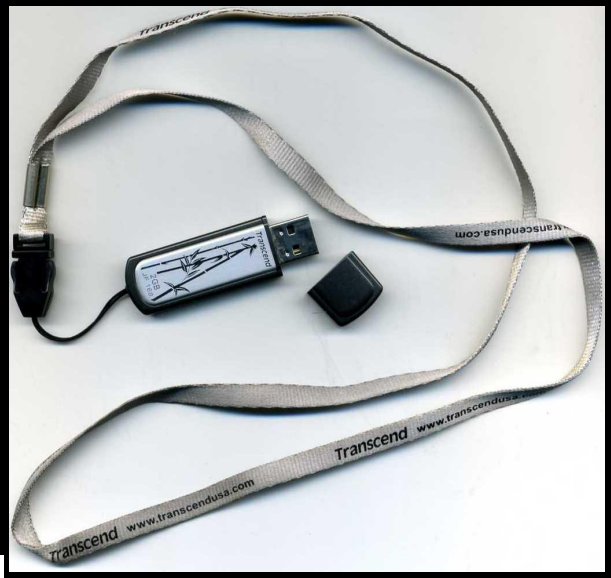
Некоторые вирусы после запуска оставляют в оперативной памяти компьютера специальные модули. Они перехватывают обращение программ к дисковой подсистеме компьютера. Если такой модуль обнаруживает, что программа пытается прочитать зараженный файл или системную область диска, он подменяет читаемые данные.

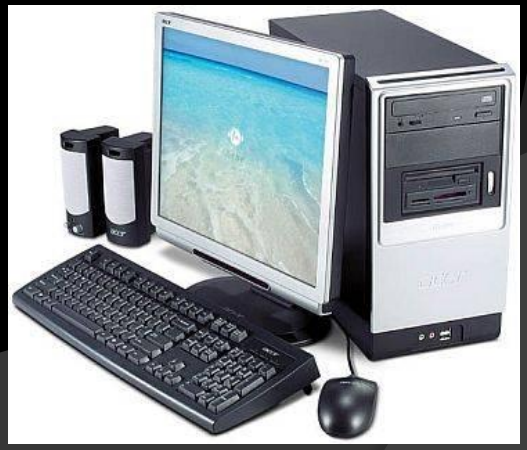
Троянский конь – это программа, содержащая в себе некоторую разрушающую функцию, которая активизируется при наступлении некоторого условия срабатывания.

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.

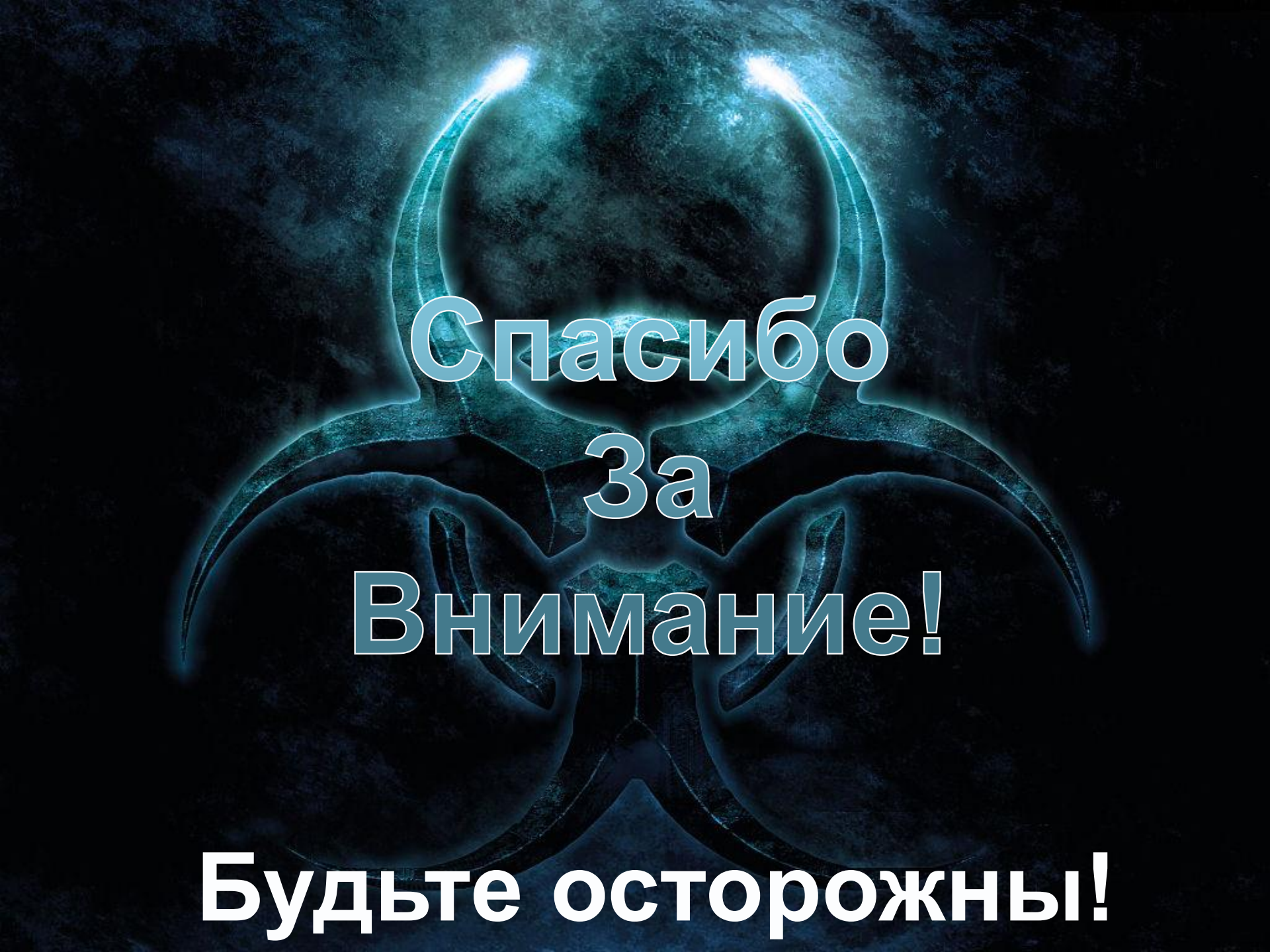
Пути проникновения





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


Спасибо
За
Внимание!
Будьте осторожны!