Мы живем в веке компьютерных технологий. Компьютеры стали неотъемлемой частью нашей жизни.

И самая опасная угроза для наших компьютеров являются – компьютерные вирусы.


VIRUS

Определение:

Компьютерные вирусы — 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.

```
text    segment   'code'
        assume cs:text,ds:text
        org     100h     main

main    proc
        jmp     VirStart            ;Переход на вирус
        db      'A'                 ;Маркер заражённости
        mov     ax,4C00h            ;Штатное завершение
        int     21h

VirStart:
        call    $+3                 ;Определение адреса
FindIP: pop     bp                  ;начала вируса
        sub     bp,offset FindIP

        mov     di,100h             ;Восстановление
        lea     si,[bp+OldBytes]    ;оригинального начала
        movsw                       ;заражённого файла
        movsw

        mov     ax,2524h            ;Переопределение int 24h
        lea     dx,[bp+New_24h]
        int     21h

        call    FindVictimFiles     ;Подпрограмма поиска и заражения
                                    ;жертв

        mov     ah,1Ah              ;Восстановление int 24h
        mov     dx,80h
        int     21h
```

Как правило, целью вируса является нарушение работы программно-аппаратных комплексов.

История:

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 вирусами являются Virus 1,2,3 и Elk Cloner для ПК Apple II, появившиеся в 1981 году.

Классификация:

Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности.

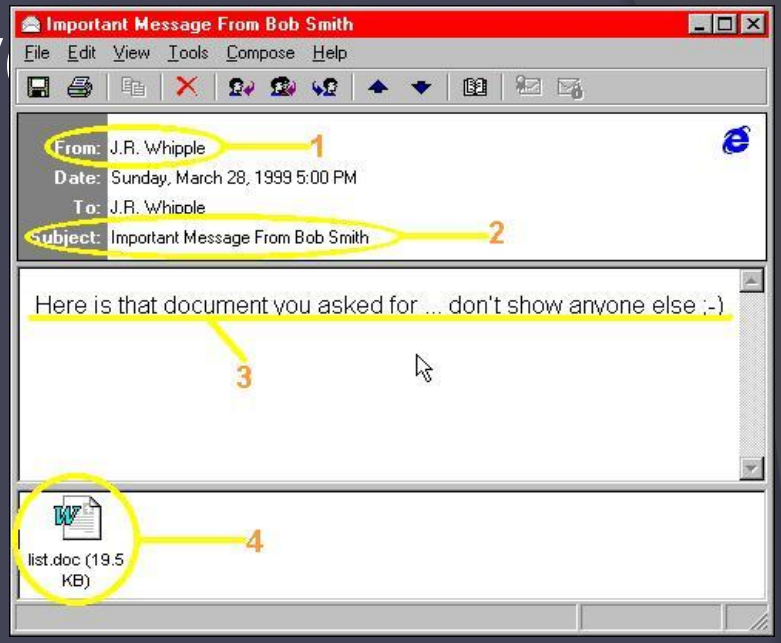
Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

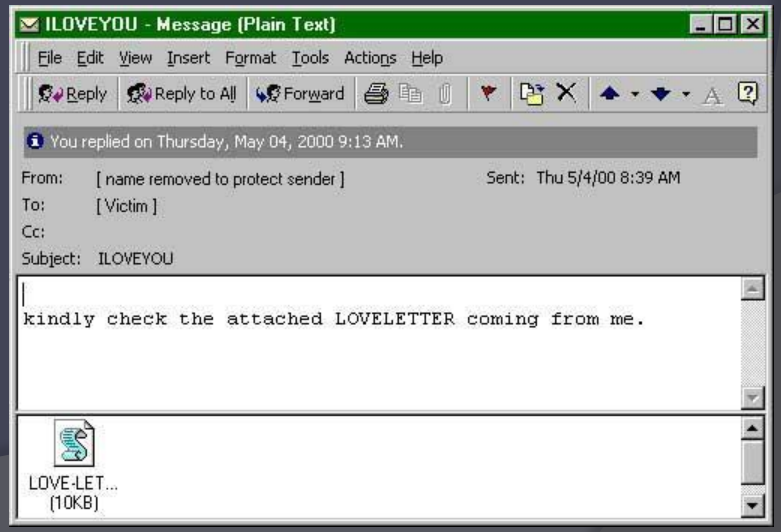
В настоящее время не существует единой системы классификации и именования вирусов (хотя попытка создать стандарт была предпринята на встрече CARO в 1991 году). Принято разделять вирусы:

- по поражаемым объектам (файловые , загрузочные вирусы, сценарные вирусы, макровирусы , вирусы, поражающие исходный код);
- файловые вирусы делят по механизму заражения: паразитирующие добавляют себя в исполняемый файл, перезаписывающие невосстановимо портят заражённый файл, «спутники» идут отдельным файлом.
- по поражаемым операционным системам и платформам (DOS,Microsoft Windows , Unix, Linux);
- по технологиям, используемым вирусом (полиформные вир стелс-вирусы , руткиты);
- по языку, на котором написан вирус (ассемблер, высокоуровневый язык программирования, сценарный язы др.);
- по дополнительной вредоносной функциональности (бэкдоры, кейлоггеры , шпионы, ботнеты и др.).

Топ 10 самых опасных компьютерных виру

1. STORM WORM
2. OOMPA-LOOMPA
3. SASSER
4. MYDOOM
5. SQL SLAMMER
6. NIMDA
7. CODE RED И CODE RED II
8. KLEZ
9. I LOVEYOU
10. MELISSA





Раз вирусы такие опасные, так что может их остановить? Против вирусов есть специализированные программы , и они называются – антивирусы.

Антивирус — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

История:

Первые антивирусные утилиты появились зимой 1984. Анди Хопкинс (Andy Hopkins) написал программы CHK4BOMB и BOMBSQAD. CHK4BOMB позволяла проанализировать текст загрузочного модуля и выявляла все текстовые сообщения и «подозрительные» участки кода (команды прямой записи на диск и др.). Благодаря своей простоте (фактически использовался только контекстный поиск) и эффективности CHK4BOMB получила значительную популярность. Программа BOMBSQAD.COM перехватывает операции записи и форматирования, выполняемые через BIOS. При выявлении запрещенной операции можно разрешить её выполнение.

Анди Хопкинс

Первый резидентный антивирус.
В начале 1985 Ги Вонг (Gee Wong) написал программу DPROTECT — резидентную программу, перехватывающую попытки записи на дискеты и винчестер. Она блокировала все операции (запись, форматирование), выполняемые через BIOS. В случае выявления такой операции программа требовала рестарта системы.

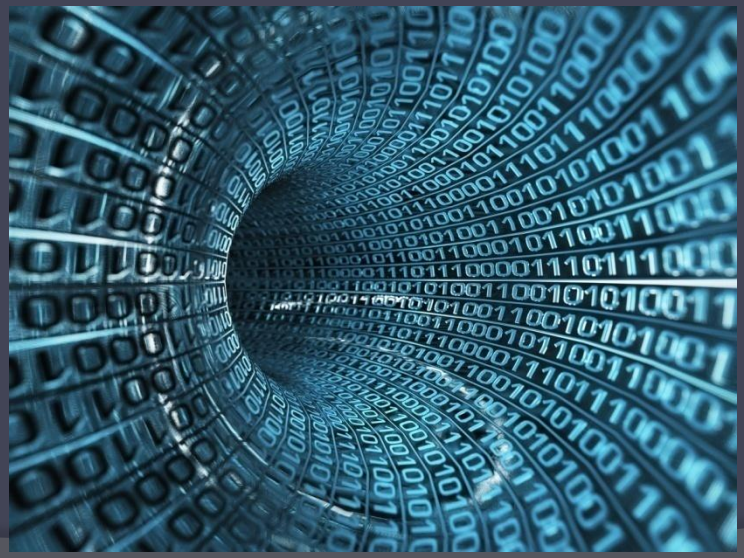
Ги Вонг

Классификация антивирусных продуктов.

- По используемым технологиям антивирусной защиты:
- Классические антивирусные продукты (продукты, применяющие только сигнатурный метод детектирования, продукты, применяющие только проактивные технологии антивирусной защиты);

- Комбинированные продукты (продукты, применяющие как сигнатурные методы защиты, так и проактивные)
- По функционалу продуктов:
- Антивирусные продукты (продукты, обеспечивающие только антивирусную защиту)
- Комбинированные продукты (продукты, обеспечивающие не только защиту от вредоносных программ, но и фильтрацию спама, шифрование и резервное копирование данных и другие функции)

- По целевым платформам:
- Антивирусные продукты для ОС семейства Windows
- Антивирусные продукты для ОС семейства *NIX (к данному семейству относятся ОС BSD, Linux и др.)
- Антивирусные продукты для ОС семейства MacOS
- Антивирусные продукты для мобильных платформ (Windows Mobile, Symbian, iOS, BlackBerry, Android, Windows Phone 7 и др.)
- Антивирусные продукты для корпоративных пользователей можно также классифицировать по объектам защиты:
- Антивирусные продукты для защиты рабочих станций
- Антивирусные продукты для защиты файловых и терминальных серверов
- Антивирусные продукты для защиты почтовых и Интернет-шлюзов
- Антивирусные продукты для защиты серверов виртуализации
- и т.д.



Итоги:

На данный момент существует множество компьютерных вирусов, и не каждый антивирус может гарантировать полную защиту вашего компьютера.

Нужно постоянно проводить проверку вашей системы и не качать с непроверенных сайтов. Ухаживайте за вашими компьютерами, ведь они тоже хотят быть здоровыми☺