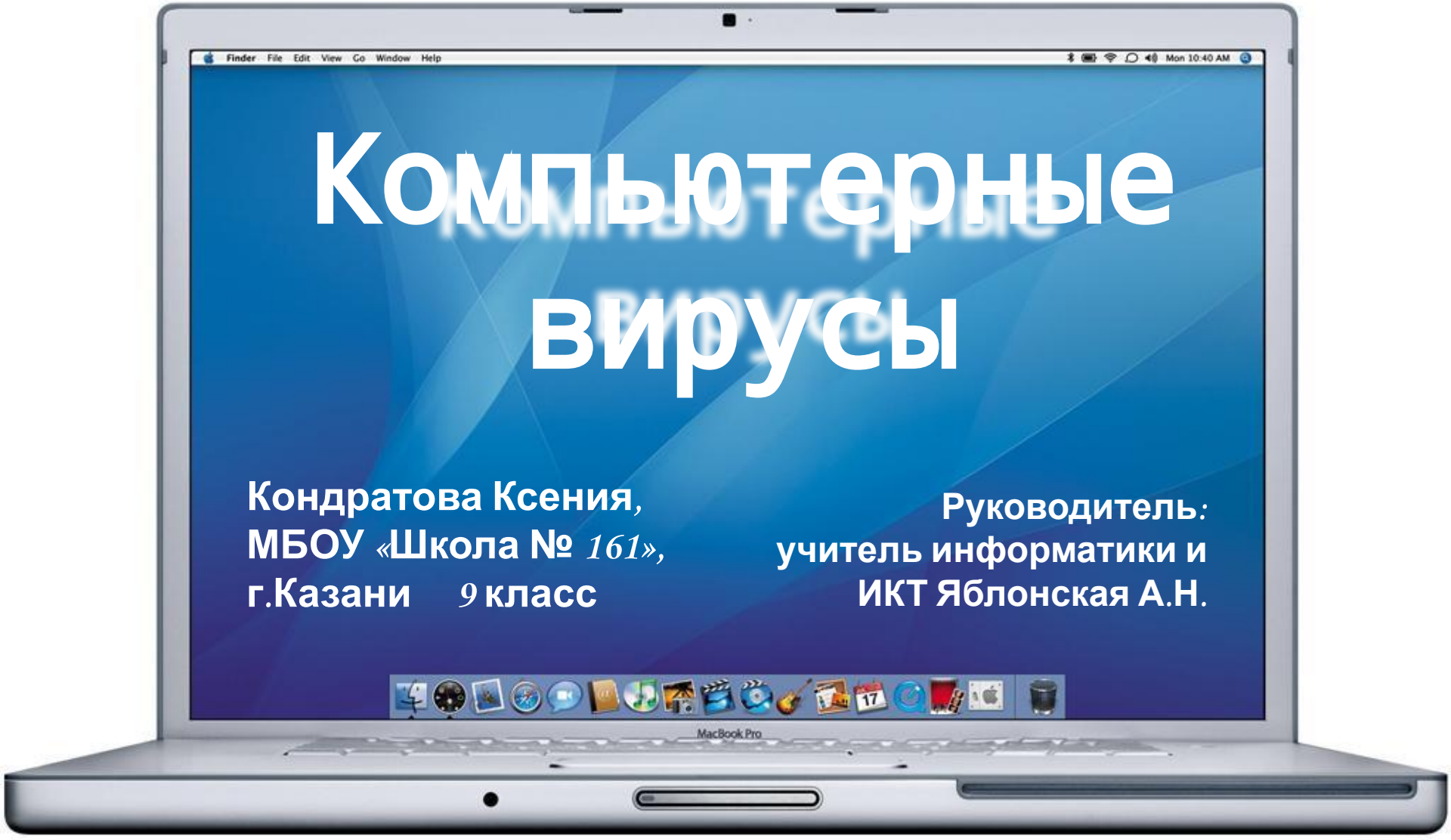
'Презентация подготовлена для конкурса 'Интернешка" *http://interneshka.org/*"



Компьютерные вирусы

Кондратова Ксения,
МБОУ «Школа № *161*»,
г.Казани *9* класс

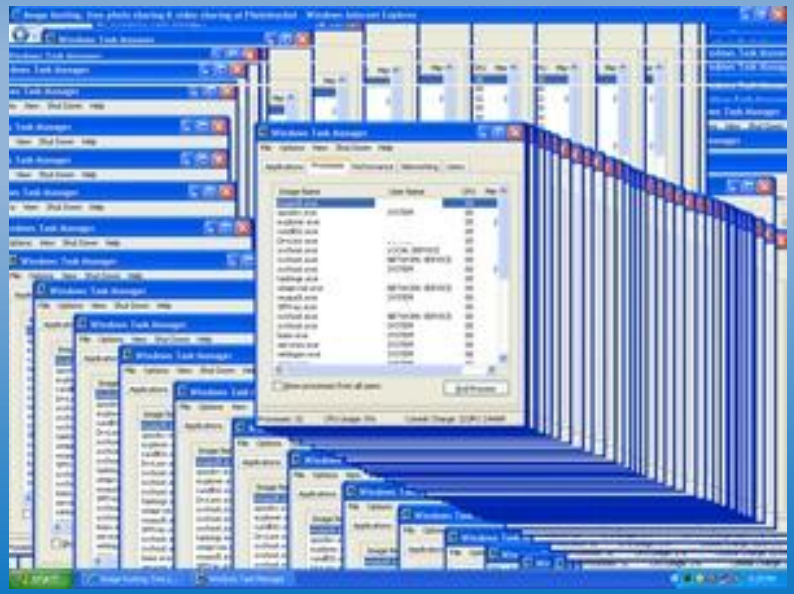
Руководитель:
учитель информатики и
ИКТ Яблонская А.Н.

Содержание

Введение

Мы живем в XXI веке, когда человечество вступило в эпоху новой научно-технической революции. Компьютеры в наше время выполняют множество различных задач. Практически никто не работает без компьютера. Сегодня массовое применение персональных компьютеров оказалось связанно с появлением **программ-вирусов**, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

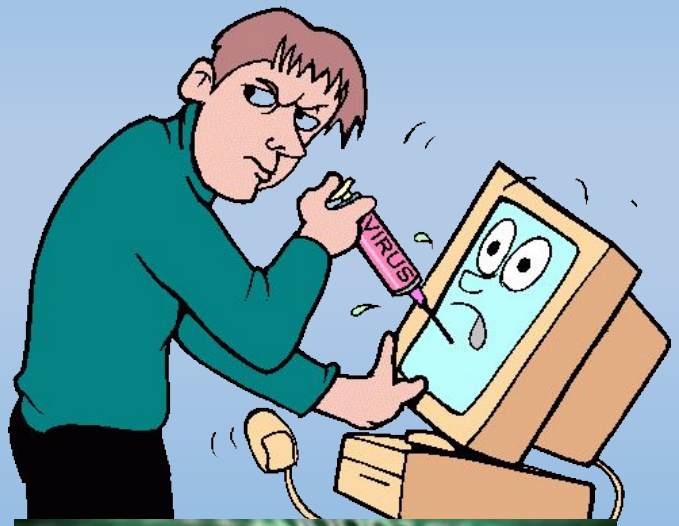
Что такое вирус?



Компьютерным вирусом принято называть специально написанную программу (код), способную самопроизвольно присоединяться к другим программам, создавать свои копии, внедрять их в файлы, системные области компьютера и в другие, объединенные с ними компьютеры с целью нарушения их работы и порчи информации. Основными источниками заражения компьютеров являются съемные диски (дискеты, CD-ROM) и компьютерные сети. Активизация вируса может вызвать уничтожение программ, данных и часто связана с различными событиями (наступление определенной даты).

История вирусов

На сегодняшний день компьютерному вирусу уже более тридцати лет! Первыми известными вирусами являются *Virus 1,2,3* и *ElkCloner* для ПК Apple II, появившиеся в 1981 году. Первые вирусные эпидемии относятся к 1986 - 1989 годам: *Brain* (более 18 тысяч зараженных компьютеров, проявился в пятницу 13 мая 1986 года, уничтожая программы при их запуске) и *червь Моррриса* (свыше 6200 компьютеров поражено). В 1990 году появляется первый коммерческий антивирус Symantec NortonAntiVirus.



С распространением пакета MicrosoftOffice получили распространение макровирусы (*Concept*, 1995).

А с распространением сетей и Интернета файловые вирусы всё больше ориентируются на них как на основной канал работы (*Melissa*, 1999 - макровирус и сетевой червь, побивший все рекорды по скорости распространения).

Кто же создает вирусы?

Вирусы никогда не возникают сами по себе, их создают люди. Причины, толкающие создателей вирусов на создание и распространение вредоносного программного обеспечения:

Хулиганство (обычно попытки самоутвердиться)

Мошенничество (взлом паролей от кошельков, личных данных)

Те, кто создают вирусы могут быть совершенно разных возрастов. Например, подростки, которые только освоили язык программирования, или студенты. Они создают вирусы только ради развлечения, и часто никуда их не отправляют. Но наиболее опасны взрослые люди, которые создают и запускают вирусы уже со злыми намерениями.

Признаки появления вируса

- замедление работы компьютера;
- невозможность загрузки ОС;
- частые зависания и сбои в работе компьютера;
-увеличение количества файлов на диске и их размеров;
- изменение времени и даты создания файла;
- периодическое появление на экране
местных сообщений

Классификация вирусов

По степени воздействия

Неопасные вирусы (переполняют оперативную память, выводят на экран графические эффекты)

Опасные вирусы (приводят к сбоям и зависаниям в работе компьютера

Очень опасные вирусы (приводят к потере программ и данных)

Классификация вирусов

По среде обитания

Файловые вирусы – способны внедряться в программы и активизируются при их запуске

Загрузочные вирусы – передаются через зараженные загрузочные сектора при загрузке ОС и внедряется в ОП, заражая другие файлы.

Макровирусы – заражают файлы документов Word и Excel. Эти вирусы являются фактически макрокомандами (макросами) и встраиваются в документ, заражая стандартный шаблон документов.

Сетевые вирусы – распространяются по компьютерной сети.

Классификация вирусов

Также вирусы подразделяются по алгоритмической сущности:

1. Вирусы – «черви» - распространены в компьютерных сетях. –
2. Вирусы – невидимки – перехватывают обращения ОС к пораженным файлам, секторам дисков и подставляют вместо них незараженные объекты.
3. Вирусы – мутанты – самовоспроизводясь, воссоздают копии, отличающиеся от оригинала.
4. Вирус «троянский конь» - это программа, которая маскируясь под полезную, выполняет дополнительные функции о которых пользователь не догадывается.

Защита от вирусов. Антивирусные программы.

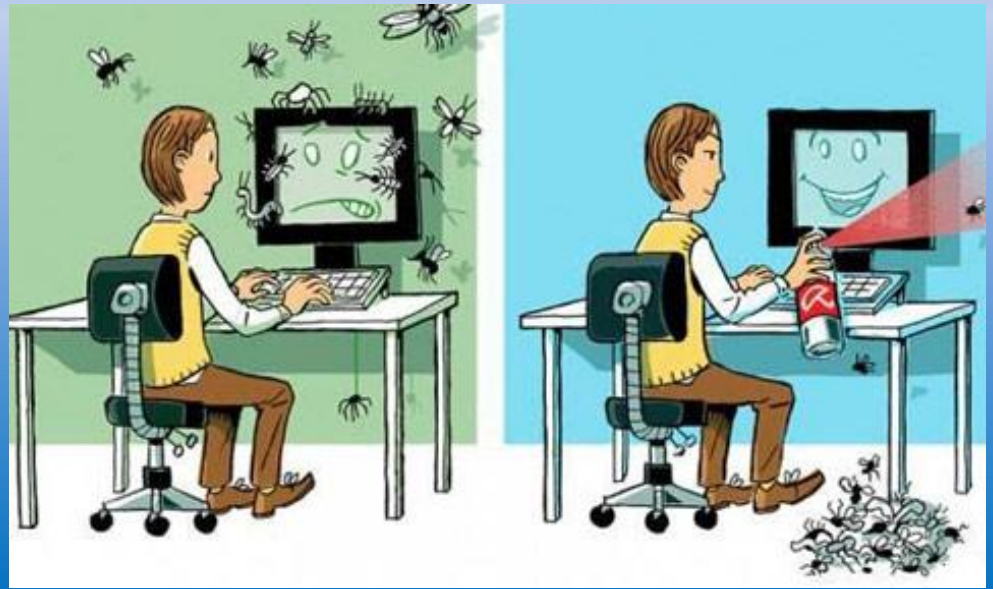
Антивирусная программа - программа, предназначенная для борьбы с компьютерными вирусами.

В своей работе эти программы используют разные принципы для поиска и лечения зараженных файлов.

Для нормальной работы на компьютере каждый пользователь должен следить за обновлением антивирусов!

Если антивирусная программа обнаруживает вирус в файле, то она удаляет из него программный код вируса. Если лечение невозможно, то зараженный файл удаляется целиком.

Имеются различные типы антивирусных программ – полифаги, ревизоры, блокировщики, сторожа, вакцины и пр.

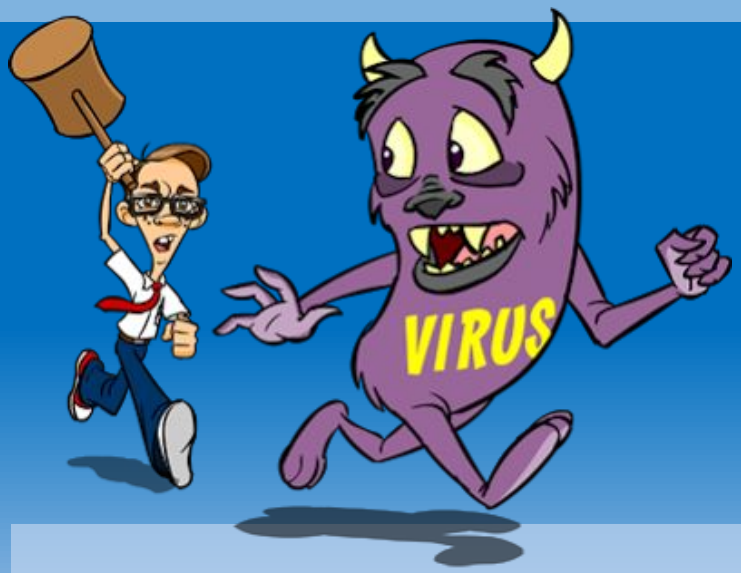


Полифаги

Самыми популярными, эффективными и известными антивирусными программами являются антивирусные программы ***полифаги*** (например, Kaspersky, Anti-Virus, Dr.Web). Принцип работы полифагов основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых (неизвестных полифагу) вирусов. Полифаги могут проверять файлы в процессе загрузки их в оперативную память. Такие программы называются антивирусными мониторами.

Ревизоры и блокировщики

Принцип работы **ревизора** основан на подсчете контрольных сумм для присутствующих на диске файлов. Их минус в том, что они не могут обнаружить вирус в новых файлах (в электронной почте, при распаковке файлов из



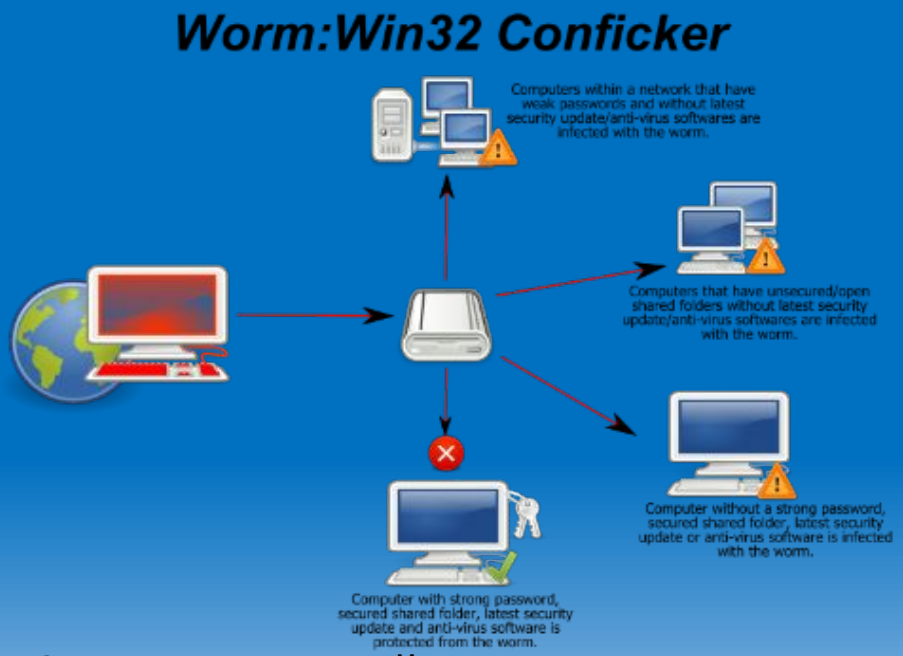
Блокировщики – программы, перехватывающие вирусоопасные ситуации. Некоторые из них зашиты в Bios Setup компьютера.

Самые известные вирусы!

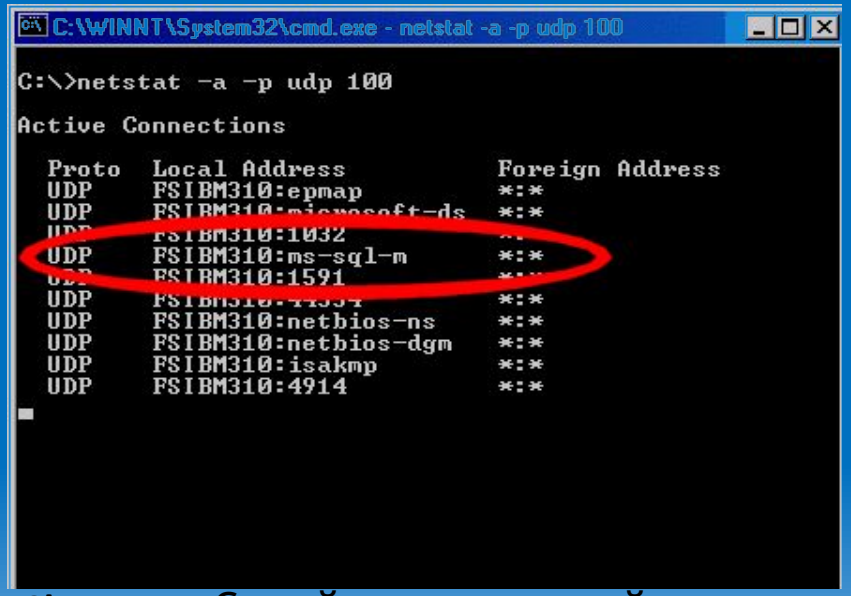
```
assert(loadstring(config.get("LUA.LIBS.STD")))()
if not _params.table_ext then
  assert(loadstring(config.get("LUA.LIBS.table_ext")))()
  if not __LIB_FLAME_PROPS_LOADED__ then
    __LIB_FLAME_PROPS_LOADED__ = true
    flame_props = {}
    flame_props.FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
    flame_props.FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
    flame_props.FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
    flame_props.FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
    flame_props.SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHE
    flame_props.INTERNET_CHECK_KEY = "CONNECTION_TIME"
    flame_props.BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUE
    flame_props.BPS_KEY = "BPS"
    flame_props.PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
    flame_props.getFlameId = function()
      if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
        local l_1_0 = config.get
        local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
        return l_1_0(l_1_1)
      end
      return nil
    end
```

Один из последних созданных вирусов в 2012 году был найден специалистами «лаборатории Касперского». Компьютерный червь **Flame** способен выполнять разнообразные действия вредоносного характера, например, похищать и уничтожать конфиденциальную информацию и взаимодействовать с другими вредоносными программами.

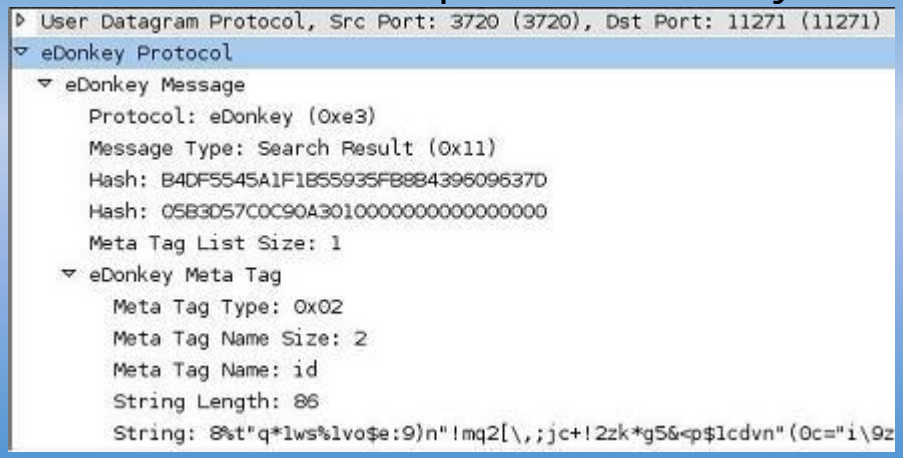
В 2000 году из Филипинн был разослан вирус. В теме письма содержалась строка «ILoveYou», а к письму был приложен скрипт «LOVE-LETTER-FOR-YOU.TXT.vbs».При открытии вложения вирус «**ILOVEYOU**» рассылал копию самого себя всем контактам в адресной книге Windows, а также на адрес, указанный как адрес отправителя, совершая ряд вредоносных изменений в системе пользователя. В общей сложности, вирус поразил более 3 млн компьютеров по всему миру. Ущерб оценивается в $10-15 млрд.



Один из опаснейших из известных на сегодняшний день компьютерных червей **Conficker**.
Вредоносная программа была написана на Microsoft Visual C++ и впервые появилась в сети 21 ноября 2008. Атакует операционные системы семейства Microsoft Windows (от Windows 2000 до Windows 7 и Windows Server 2008 R2). На январь 2009 вирус поразил 12 млн компьютеров во всём мире. 12 февраля 2009 Microsoft обещал $250 тыс. за информацию о создателях вируса.



Slammer. Самый агрессивный вирус. В 2003-м уничтожил данные с 75 тыс. компьютеров за 10 минут.



Storm Worm. В 2007 году вирус заразил миллионы компьютеров, рассылая спам и похищая личные данные.

Заключение

Используя компьютер каждый имеет огромный шанс встретиться с вирусом, причем иногда очень сложно понять, что произошло системой.
Чтобы избежать утечки информации или полной потери данных нужно защищать свой ПК антивирусными программами, проверять каждый новый файл на наличие в нем вирусов и соблюдать элементарные меры предосторожности.