

Вирусы и антивирусные программы



Коляда Татьяна Александровна

Компьютерный вирус -

Копия
целенаправленная
программа
приписанная
программе
или устройству



— это
созданная
автоматически
другим
устройством

Первый вирус

Первая «эпидемия» компьютерного вируса произошла в 1986 году, когда вирус по имени Brain (англ. «мозг») заразил дискеты персональных компьютеров.



Россия вышла в мировые лидеры по распространению компьютерных вирусов



Аналитики PC Tools уверяют, что по масштабам распространения компьютерных вирусов, вредоносного и шпионского программного обеспечения Россия давно опередила таких "гигантов" в этой области, как Китай и США. По оценкам аналитиков PC Tools - американского производителя средств защиты от нежелательного ПО – на долю РФ приходится **27,89%** вредоносных программ в мире, Китая - **26,52%**, США - **9,98%**

Классификация вирусов по среде обитания

- Загрузочные вирусы
- Файловые вирусы
- Макро - вирусы
- Сетевые вирусы



Загрузочные вирусы

- Загрузочные вирусы заражают загрузочный (boot) сектор флорпи-дисков, жестких дисков и винчестера. Их распространение основано на алгоритмах, которые выполняются при включении компьютера (например, тестирование оборудования, проверка жестких дисков и т.д.). Программа, заражающая загрузочный сектор, получает первый контроль над компьютером (например, при загрузке с CD-ROM в BIOS Setup) и управляет процессом загрузки.
- При заражении вирус "подставляет" свой код, получая управление системой при загрузке. В результате компьютер "заставляет" загрузиться не оригинальному коду загрузчика, а коду вируса.



Файловые вирусы

- К данной группе относятся вирусы, которые используют для размножения файлы или папки. Они используют файлы с расширениями .COM, .EXE, .SYS, и т.д.
- Могут распространяться по локальной сети и через интернет. Файлы с расширениями .COM, .EXE, .SYS, и т.д.
- Практически все файлы с расширениями .COM, .EXE, .SYS, и т.д. являются файловыми вирусами резидентные



Макро-вирусы

- Макро-вирусы (macro viruses) являются программами на языках (макро-языках), встроенных в некоторые системы обработки электронных таблицы. Такие вирусы используют их возможности для переноса (документа) или табл.
- На сегодняшний день, для систем, для которых Excel, MS Office и другие программы получают управление зараженного файла, где вирус выполняет функцию и затем заходит в образ резидентные.



Сетевые вирусы

К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей.

Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. "Полноценные" сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, "подтолкнуть" пользователя к запуску зараженного файла.



По особенностям алгоритма вирусы имеют большое разнообразие

Простейшие вирусы – не изменяют содержимое файлов, могут быть легко обнаружены и уничтожены

Черви – распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и рассылают свои копии по этим адресам

Вирусы – невидимки – трудно обнаружить и обезвредить, подставляют вместо своего тела незараженные участки диска

Вирусы-мутанты – содержат алгоритмы шифровки / расшифровки, наиболее трудно обнаружить

Трояны – маскируются под полезную программу, разрушают загрузочный сектор и файловую систему

Другие вредоносные программы

Троянские кони (логические бомбы)

К троянским коням относятся программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от каких-либо условий выполняющие уничтожающую систему и т.п. информацию.

Большинство троянских коней являются программами, которые "под видом" полезных программ, дополнения к станциям или вирусам распространяются по BBS-сетям. По сравнению с вирусами они имеют широкий спектр причин - они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем.



Другие вредоносные программы

Intended-вирусы

К таким вирусам относятся программы, которые на первый взгляд являются полезными, но не являются таковыми. Например, вирус, который копирует файлы и записывает их в неправильном формате, прерывает работу и закрывает программы.



К категории Intended-вирусов относятся вирусы, которые по своей природе являются полезными, но только один раз - из "авторского" экземпляра. Если файл, они теряют способность к дальнейшему размножению.

Другие вредоносные программы

Конструкторы вирусов

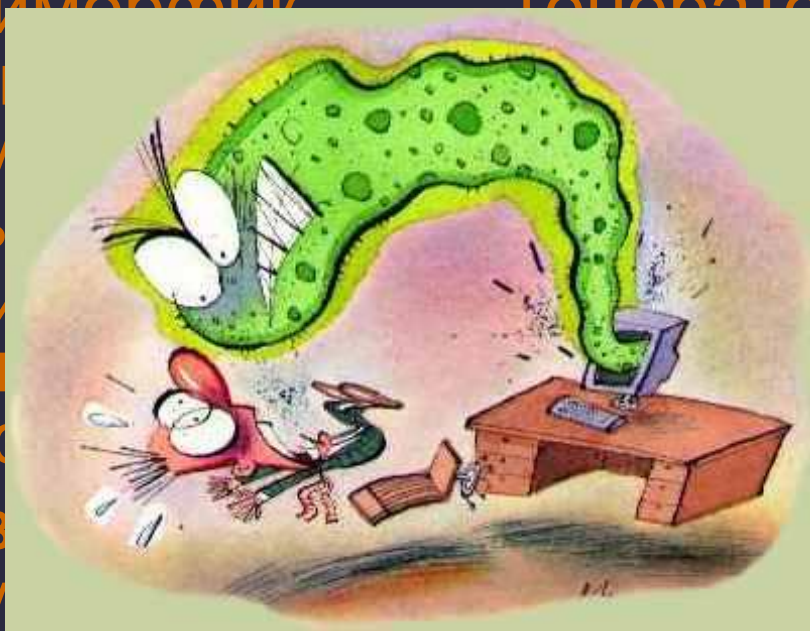
Конструкторы вирусов — это утилита, предназначенная для управления новыми компьютерными вирусами. Известны такие конструкторы вирусов, как DOS, Windows и макро-вирусов. Они позволяют генерировать тексты вирусов (ASM-файлы), объектные модули, и/или непосредственно зараженные файлы.



Другие вредоносные программы

Полиморфные генераторы

Полиморфные генераторы, как и вирусы, являются вредоносными программами. Это слово, происходящее от греческого слова, означающего «разнообразие», описывает способность этих программ изменять свой код при каждом запуске. Это позволяет им избежать обнаружения антивирусными программами. Они используют различные методы для скрытия своего присутствия, такие как маскировка, изменение имени файла, использование случайных имен переменных и функций, а также изменение структуры кода. Это делает их очень опасными, так как они могут легко избежать обнаружения антивирусными программами. Главной функцией полиморфных генераторов является генерация соответствующего вредоносного кода. Они могут генерировать код для различных целей, таких как кража информации, повреждение данных и уничтожение файлов. Кроме того, они могут использоваться для создания ботнетов, которые могут использоваться для проведения DDoS-атак и других вредоносных действий.



Примеры вирусов

KeyKut 4.0 (Trojan-Spy.Win32.Banker.ckl)

Бразильский троян для кражи персональной информации, написан на Delphi. Имеет размер более 2Мб.



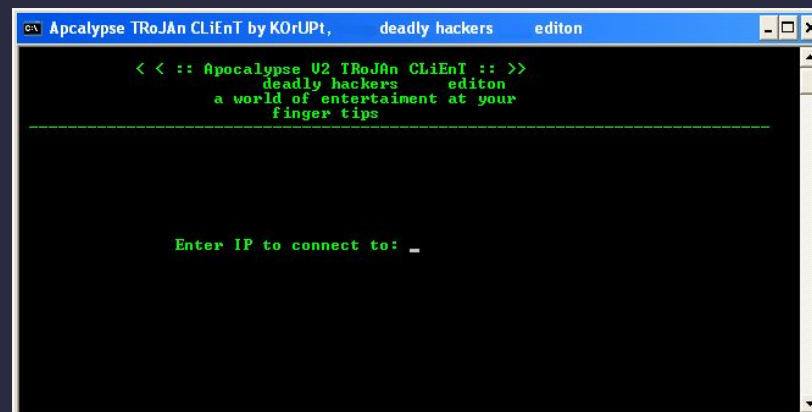
Примеры вирусов

Аpocalypse Trojan v2

Троян-бекдор, не обнаруживаемый антивирусами.

Состоит из одного файла

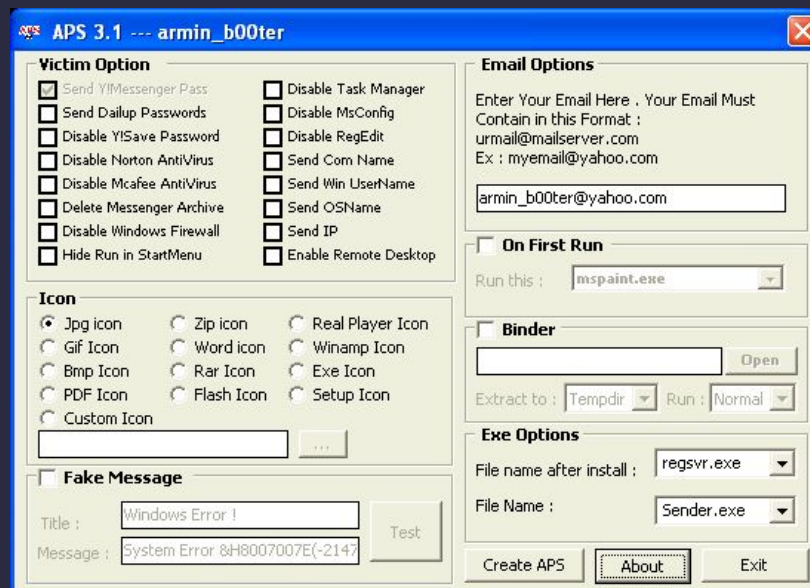
c:\WINDOWS\system32\ntoskrnl32.exe
размером 534 кб.



```
Apocalypse TRoJAn CLiEnT by KOrUP1, deadly hackers  editon
<< :: Apocalypse U2 TRoJAn CLiEnT :: >>
      deadly hackers      editon
a world of entertainment at your
      finger tips
-----
Enter IP to connect to: _
```


Примеры вирусов

APS 3.1
(Trojan.Win32.VB.akr)
Многофункциональный
иранский троян,
способный отключать
различные средства
защиты компьютера.
Серверная часть
состоит из одного
файла
c:\WINDOWS\system32\
regsvr.exe размером
23,203 байт.



Признаки, указывающие на поражение программ вирусом:

- *Неправильная работа программ*
- *Медленная работа компьютера*
- *Невозможность загрузки операционной системы*
- *Исчезновение файлов*
- *Изменение даты, времени создания файла или его размера*
- *Вывод на экран непредусмотренных сообщений или изображений*
- *Частые зависания компьютера и т.д.*

Антивирусные программы



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

Антивирусное программное обеспечение состоит из подпрограмм, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другое вредоносное программное обеспечение.

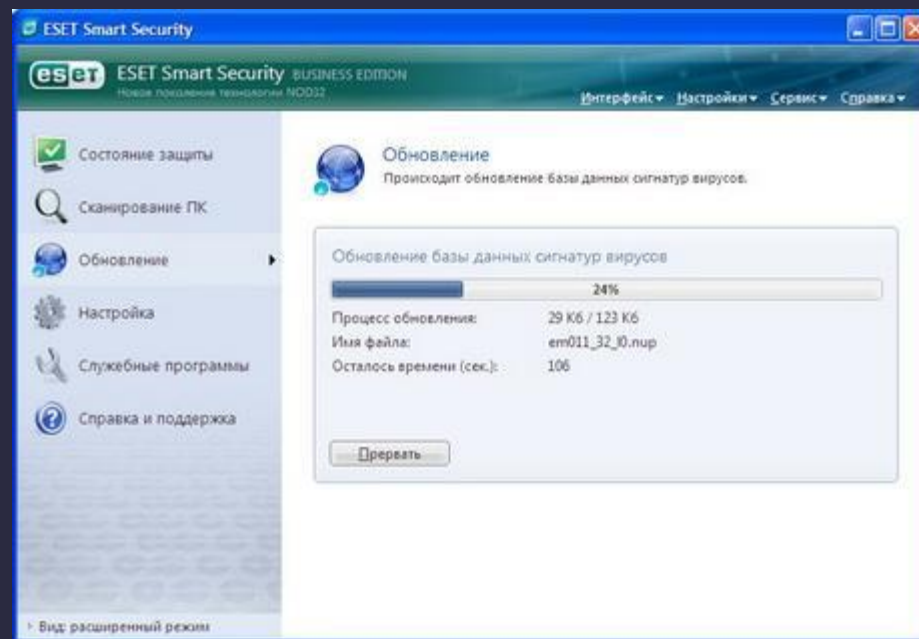


Антивирусные программы

- [NOD 32](#)
- [Dr. Web](#)
- [Kaspersky](#)
- [Avast!](#)
- [Norton](#)
- [Panda](#)



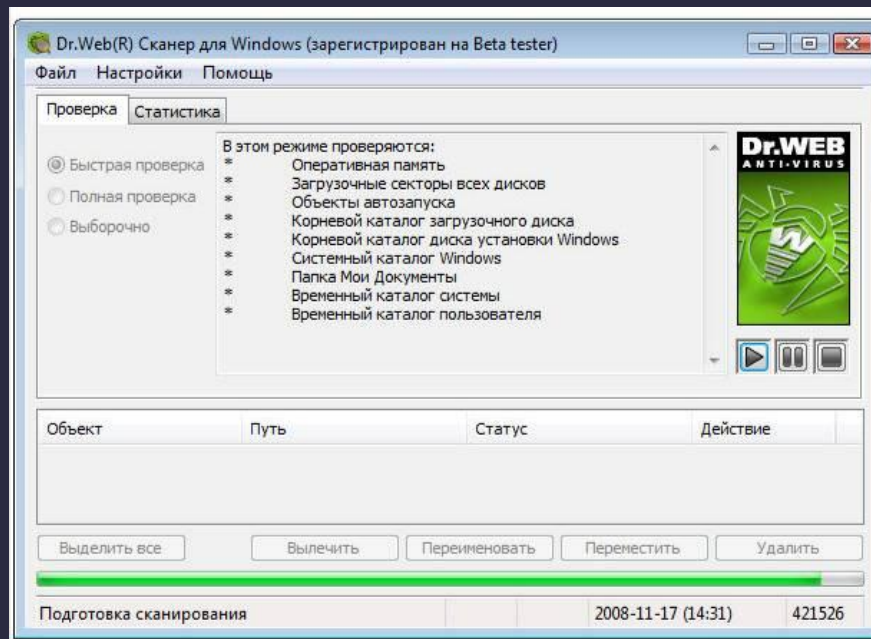
NOD 32



<http://www.esetnod32.ru/>



Dr. Web



<http://www.drweb.com/>



Kaspersky Antivirus



<http://www.kaspersky.ru/>



Avast!



<http://www.avast.com/ru-ru/index>



Norton AntiVirus

A screenshot of the Norton AntiVirus user interface. The interface is dark-themed with yellow and green accents. At the top left, there is a green checkmark icon and the word "Secure". Below this, there are performance metrics for CPU (100%) and Norton (88%). The main area is divided into "Computer" and "Network" sections. The "Computer" section shows "Insight Protection" (On), "Antivirus" (On), "Antispyware" (On), and "SONAR Protection" (On). The "Network" section shows "Intrusion Prevention" (On), "Email Protection" (On), "Browser Protection" (On), and "Download Intelligence" (On). At the bottom, there is a "Norton from symantec" logo and a trial period expiration notice. A URL "www.izone.ru" is visible in the bottom right corner of the interface.

Norton AntiVirus

Leave Feedback Norton Account Help & Support

Secure

Computer Settings

Scan Now
History & Quarantine

Run LiveUpdate: 5 days ago

Insight Protection Details On *i*

Antivirus On *i*

Antispyware On *i*

SONAR Protection On *i*

Network Settings

Vulnerability Protection
Network Security Map

Intrusion Prevention On *i*

Email Protection On *i*

Browser Protection On *i*

Download Intelligence On *i*

Norton
from symantec

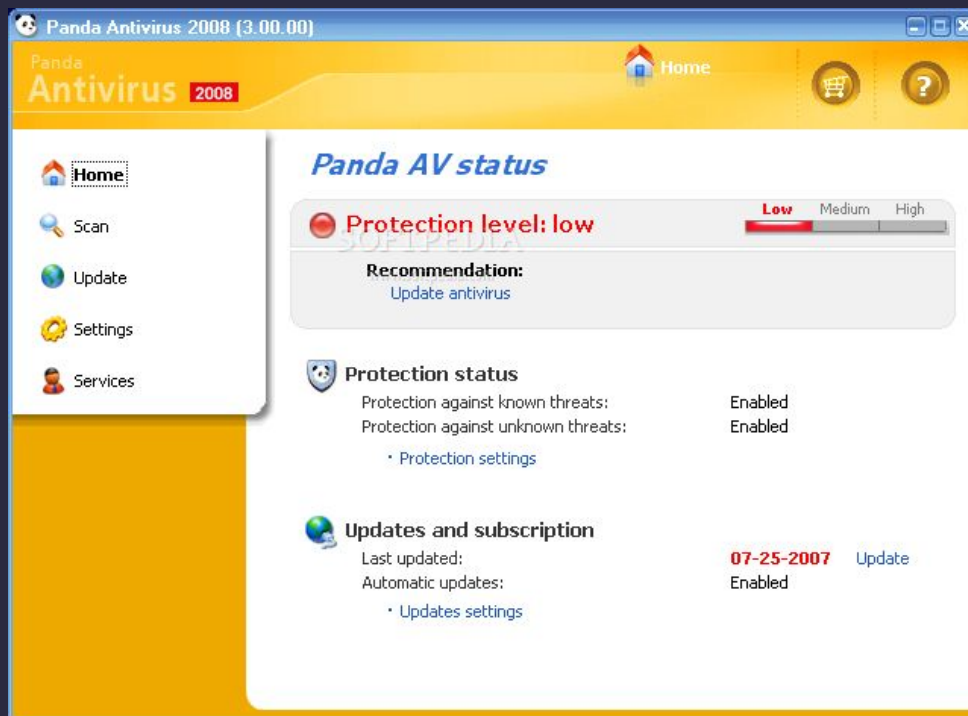
Learn About Web Protection

Your trial period expires in 1 www.izone.ru

<http://www.symantec.com/norton/antivirus>



Panda Antivirus



<http://www.pandasecurity.com/russia/>



Правила защиты от компьютерных вирусов

- Регулярно тестируйте компьютер на наличие вирусов с помощью антивирусных программ
- Перед считыванием информации со съемных носителей проверяйте их на наличие вирусов
- Всегда защищайте свои носители информации от записи при работе на других компьютерах
- Делайте архивные копии ценной для вас информации
- Не используйте программы, поведение которых непонятно
- Регулярно обновляйте антивирусные программы

Источники информации

- Компьютерные вирусы
- Компьютерный вирус
- Антивирусная программа

Резидентность

Под термином "резидентность" (DOS'овский термин TSR - Terminate and Stay Resident) понимается способность вирусов оставлять свои копии в операционной системе, перехватывать некоторые события (например, обращения к файлам или дискам) и вызывать при этом процедуры заражения обнаруженных объектов (файлов и секторов).

Таким образом, резидентные вирусы активны не только в момент работы зараженной программы, но и после того, как программа закончила свою работу. Резидентные копии таких вирусов остаются жизнеспособными вплоть до очередной перезагрузки, даже если на диске уничтожены все зараженные файлы. Часто от таких вирусов невозможно избавиться восстановлением всех копий файлов с дистрибутивных дисков или backup-копий. Резидентная копия вируса остается активной и заражает вновь создаваемые файлы.

То же верно и для загрузочных вирусов - форматирование диска при наличии в памяти резидентного вируса не всегда вылечивает диск, поскольку многие резидентные вирусы заражают диск повторно после того, как он отформатирован.

