Вирусы и антивирусные программы

Коляда Татьяна Александровна

Компьютерный вирус -

Ко – это целена озданная програ атически припис другим програ еняющая или ун

Первый вирус

Первая «эпидемия» компьютерного вируса произошла в 1986 году, когда вирус по имени Brain (англ. «мозг») заражал 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 флоппи-диск Record (MBR) винчестера. ирусов основан на алгоритма при включении или перезаг одимых тестов установленно исков и т.д.). Программа вает первый физический или CD-ROM в зависимости BIOS Setup) и передает управление.
- При зараже "подставляют" свой код , получающей управление с "заставляет" систему при мять и отдать управление не оригинальному коду загрузчика, а коду вируса.

Файловые вирусы

- К данной группе относятся вирусы, которы нии тем или ользуют файло ОС.
- Могут файлы различ , BAT, SYS, и
- Практи ные и файловые вирусы резидентные

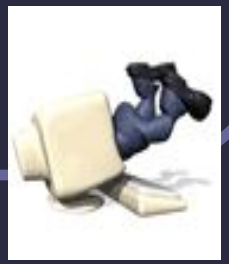
Макро-вирусы

- Макро-вирусы (macro viruses) являются программами на языках (макро-языках), встроенных в некоторые системы обработк… …электронные таблицы … …акие вирусы использу… … их помощи перенося… … (документа или табл…
- На сего… …истемы, для которых … …l, Excel, MS Office и… …ы получают управлен… …зараженного файла, г… …е функции и затем за… …бо образом идет … … макро-вирусов [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 уничтожающая информацию систему и т.п.

Большинство программами, которые "по бо полезные программы, утилит или дополнения аются по BBS-станциям или По сравнению с вирусами " ают широкого распростране ричинам - 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 в русами, но не способны ок. Например, вирус, ко стить в начало файлов д вируса, либо записыва о кода, либо неправил ехватываемого прерыван чстве случаев завешива

К катего ы, которые по приведен олько один раз - из "авто айл, они теряют способность к дальнейшему размножению.

Другие вредоносные программы

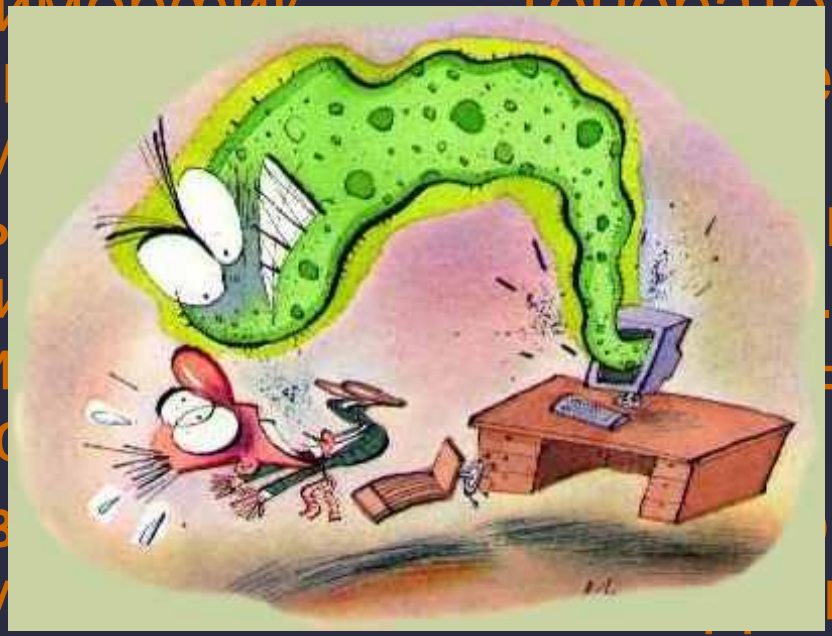
Конструкторы вирусов

Конструкто это утилита, предназначен овления новых компьютерных . Известны конструкторы OS, Windows и макро-вирусов позволяют генерировать екты вирусов (ASM-файлы), объектные модули, и/или непосредственно зараженные файлы.

Другие вредоносные программы

Полиморфные генераторы

Полиморфик генераторы, как и конструк е являются вирусам этого слова, поскольк кладываются функции открытия, закрыти ы, чтения и записи



Глав бного рода програм вание тела вируса и генерация соответствующего расшифровщика.

Примеры вирусов

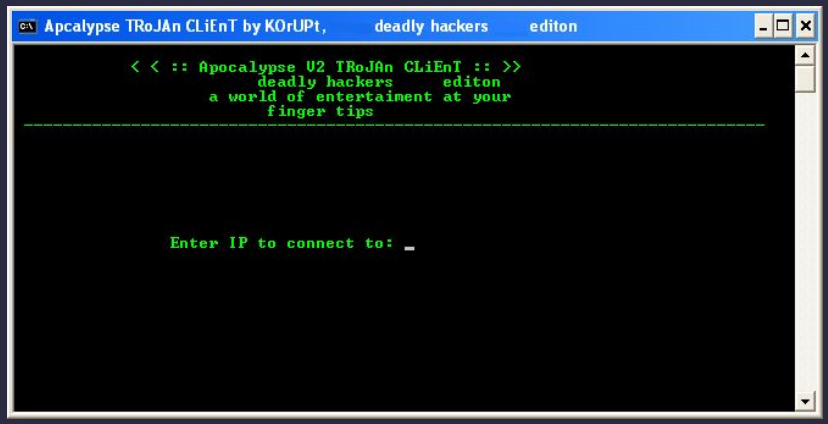
KeyKut 4.0 (Trojan-Spy.Win32.Banker.ckl)

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

Примеры вирусов

Apocalypse Trojan v2

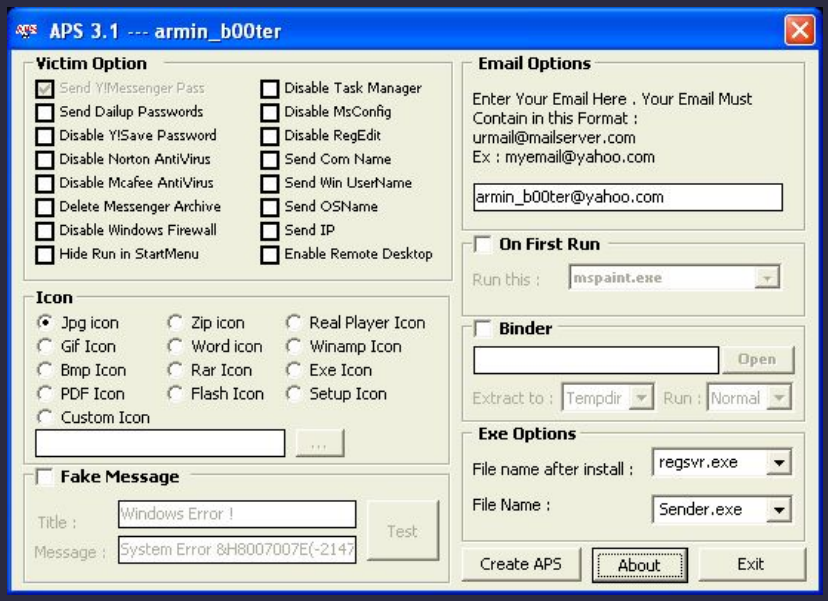
Троян-бекдор, не обнаруживаемый антивирусами. Состоит из одного файла c:\WINDOWS\system32\ntoskrnl32.exe размером 534 кб.



Примеры вирусов

APS 3.1 (Trojan.Win32.VB.akr)

Многофункциональный иранский троян, способный отключать различные средста 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.*

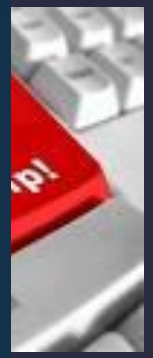
Антивирусные программы

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.

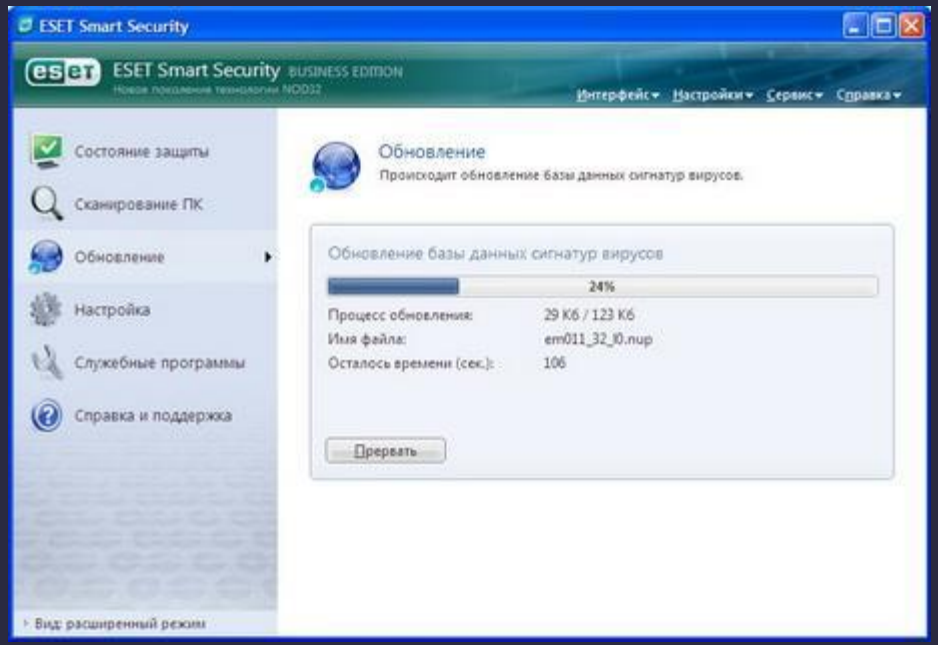
Антивирусное программное обеспечение состоит из подпрограмм, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другое вредоносное программное обеспечение.

Антивирусные программы

- NOD 3
- Dr. We
- Kaspe
- Avast!
- Nortor
- Panda

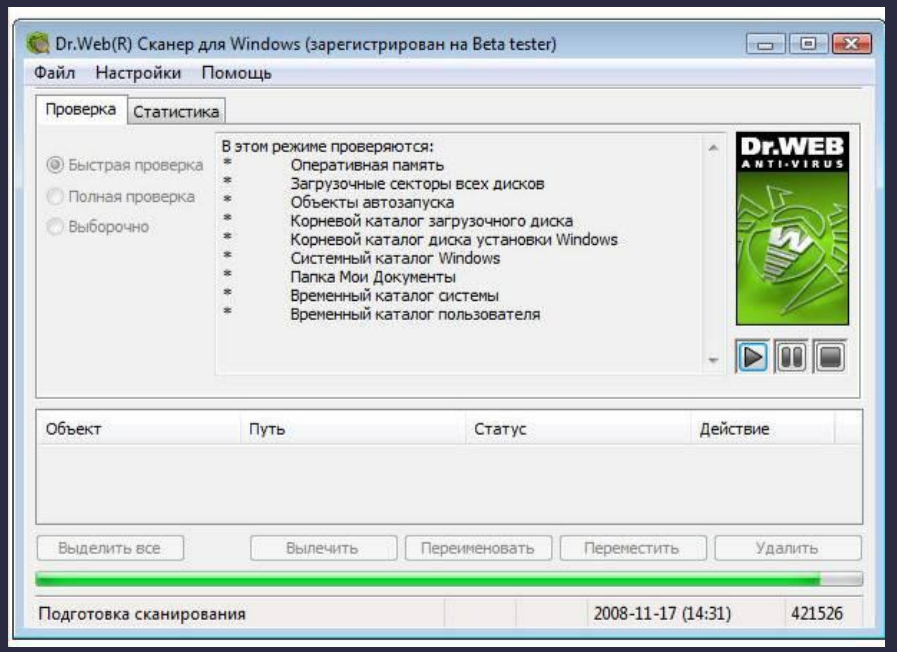


NOD 32



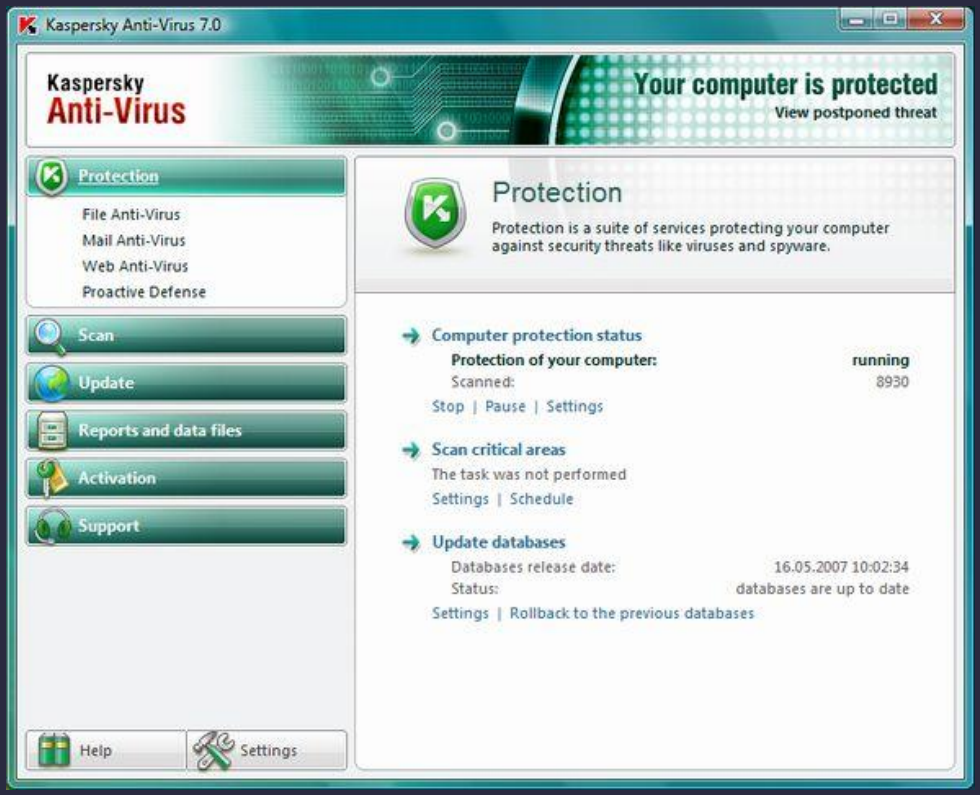
http://www.esetnod32.ru/

Dr. Web



http://www.drweb.com/

Kaspersky Antivirus



http://www.kaspersky.ru/

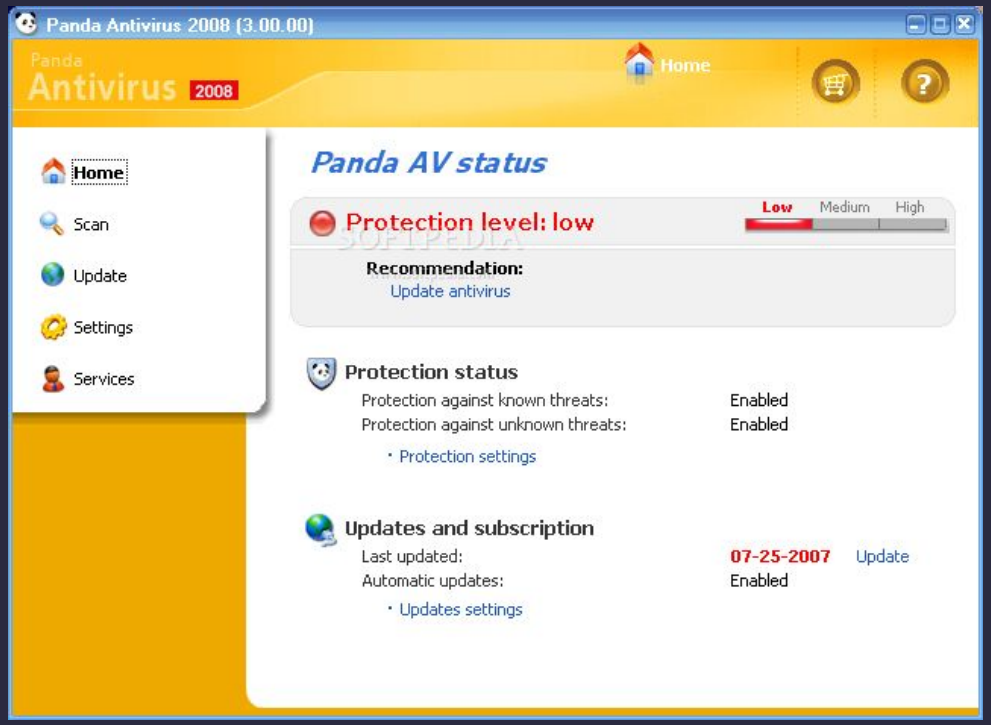
Avast!

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

Norton AntiVirus

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 заражает диск повторно после того, как он отформатирован.