Вирусы и антивирусные программы

Компьютерный вирус -

Компьют ses) - это
программ много кода,
которые, опреки воле
пользова ции на этом
компьюте ь объекты,
модифиц программные
файлы, обственному
распрост льным сетям
или по программных
файлов, ых секторов
дисков та и становятся
носителя ередь могут
осуществ операции,
называет) и является
важнейш ов.

Первый вирус

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

Классификация компьютерных вирусов

- по среде обитания
- по способу заражения
- по воздействию
- по особенностям алгоритма

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 М, BAT, SYS, и
- Практи ные и файловые вирусы резидентные

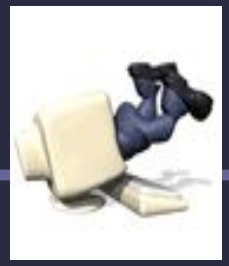
Макро-вирусы

- 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, п… …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 способу заражения

- **Резидентные** – при заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения
- **Нерезидентные** – не заражают оперативную память и активны ограниченное время

По воздействию

- **Неопасные** – не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках
- **Опасные** – приводят к различным нарушениям в работе компьютера
- **Очень опасные** – могут приводить к потере программ, данных, стиранию информации в системных областях дисков

По особенностям алгоритма

- **Паразиты** – изменяют содержимое файлов и секторов, легко обнаруживаются
- **Черви** –вычисляют адреса сетевых компьютеров и отправляют по ним свои копии
- **Стелсы** – перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области
- **Мутанты** – содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую
- **Трояны** – не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему

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.

Вредоносные программы

Intended-вирусы

К таким вирусам относятся программы, которые на первый взгляд яв о не способны размножа вирус, который при зара ачало файлов команду вируса, либо записыва о кода, либо неправил ехватываемого прерыван нстве случаев завешива

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

Вредоносные программы

Конструкторы вирусов

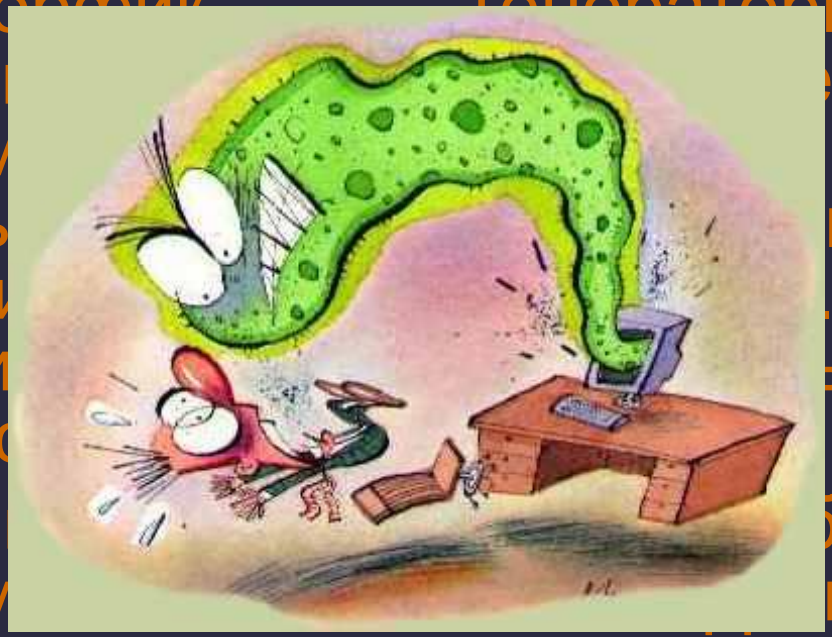
Конструктор это утилита, предназначен овления новых компьютерных . Известны конструкторы OS, Windows и макро-вирусов позволяют генерировать екты вирусов (ASM-файлы), объектные модули, и/или непосредственно зараженные файлы.

Вредоносные программы

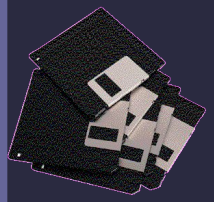
Полиморфные генераторы

Полимо генераторы, как и конструк являются вирусам этого слова, посколь кладываются функции открытия, закрыти ы, чтения и записи

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



Каналы распространения



- ***Дискеты***

Самый распространённый канал заражения в 1980-90 годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов.

- ***Флеш-накопители (флешки)***

В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны. Использование этого канала преимущественно обусловлено возможностью создания на накопителе специального файла ***autorun.inf***, в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. Флешки — основной источник заражения для компьютеров, не подключённых к сети Интернет.

- ***Электронная почта***

Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты.

- ***Системы обмена мгновенными сообщениями***

Так же распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

- ***Веб-страницы***

Возможно также заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов

- ***Интернет и локальные сети (черви)***

Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер.

Примеры вирусов

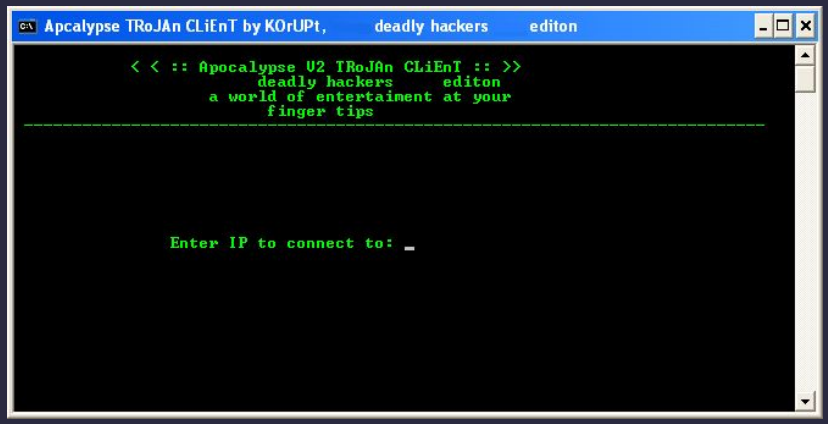
KeyKut 4.0 (Trojan-Spy.Win32.Banker.ckl)

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

Примеры вирусов

Apocalypse Trojan v2

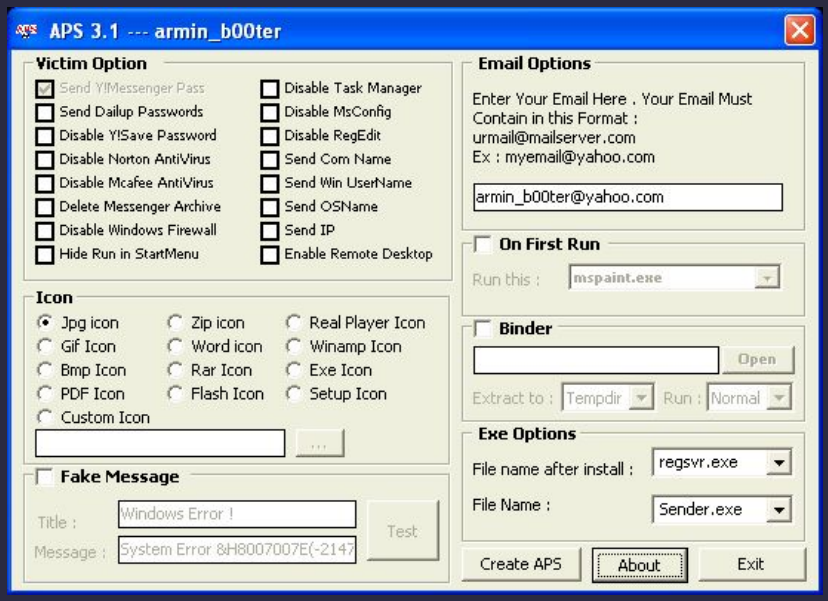
Троян-бекдор, не обнаруживаемый антивирусами. Состоит из одного файла c:\WINDOWS\system32\ntoskrnl32.exe размером 534 кб.



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.*

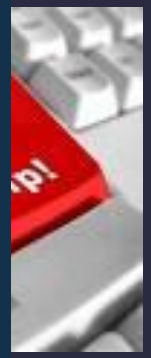
Антивирусные программы

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.

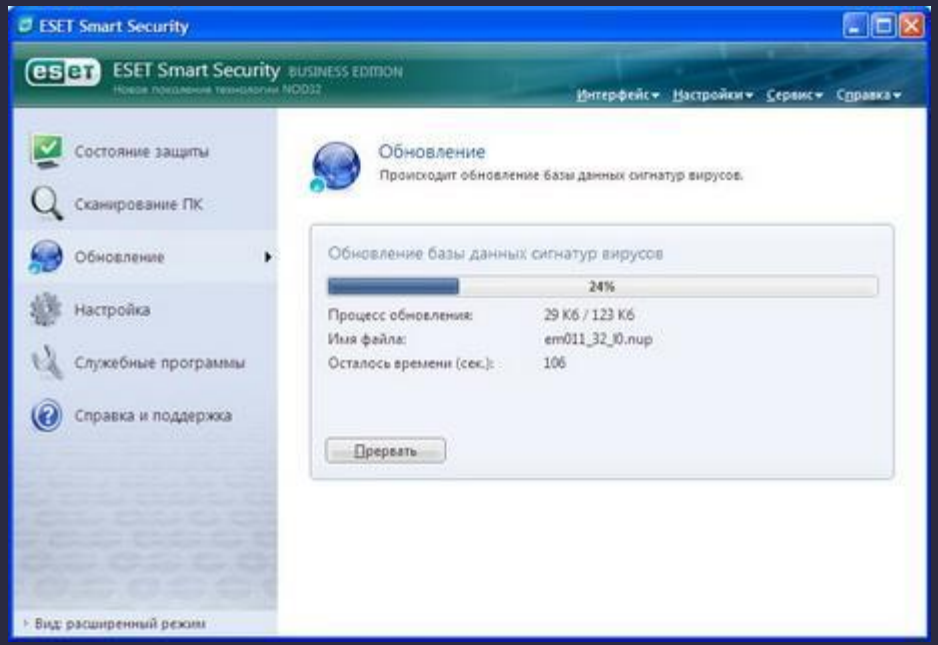
Антивирусное программное обеспечение состоит из подпрограмм, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другое вредоносное программное обеспечение.

Антивирусные программы

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

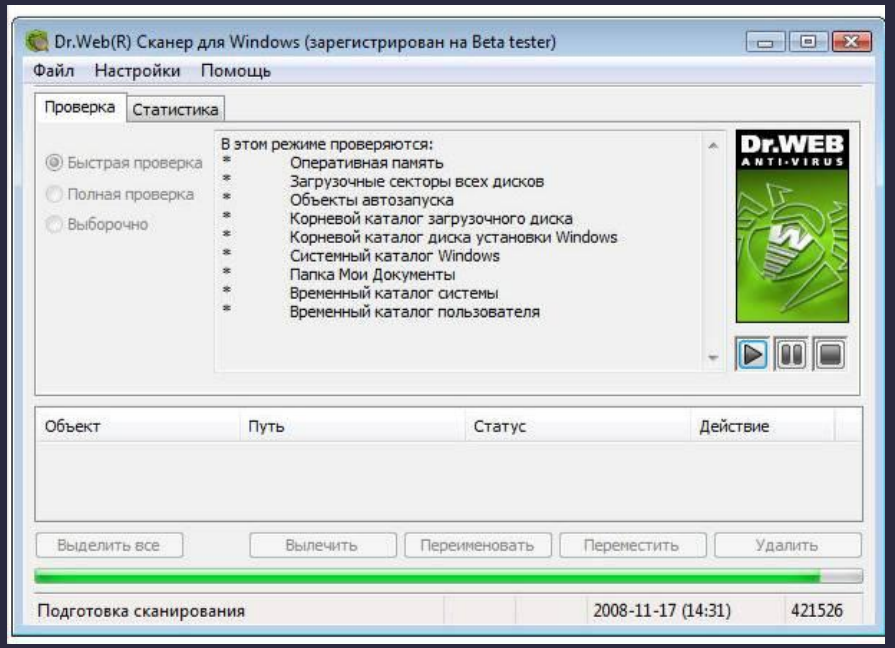


NOD 32



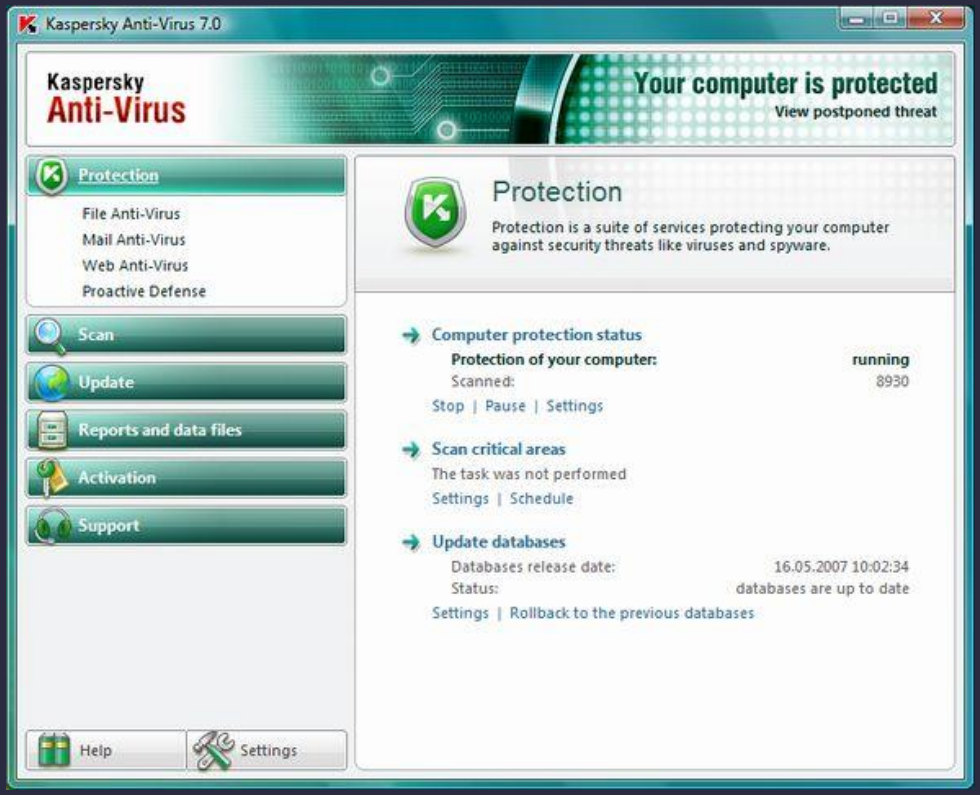
http://www.esetnod32.ru/

Dr. Web



http://www.drweb.com/

Kaspersky Antivirus



http://www.kaspersky.ru/

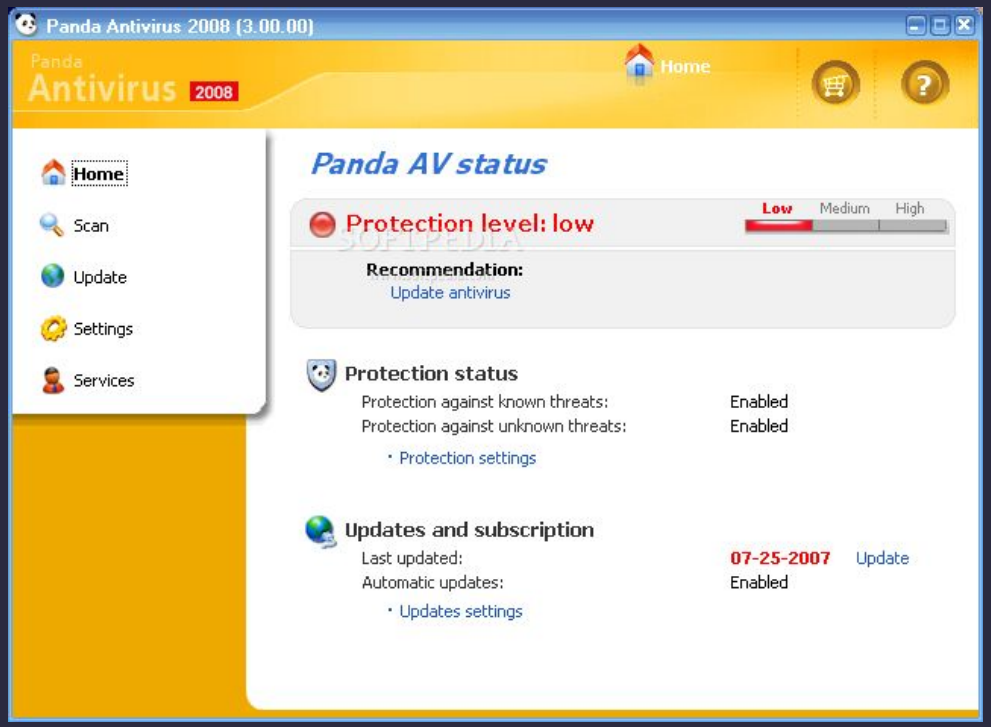
Avast!

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