Антивирусная программа

Материал из Википедии — свободной энциклопедии

(Перенаправлено с Антивирус)

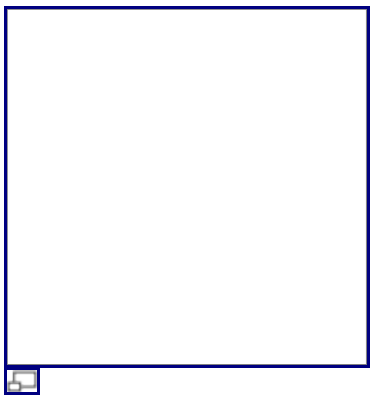
Перейти к: навигация, поиск

Антивирусная программа (**антивирус**) — программа для обнаружения и лечения программ, заражённых компьютерным вирусом, а также для предотвращения заражения файла вирусом (например, с помощью вакцинации).

Первые, наиболее простые антивирусные программы появились почти сразу после появления вирусов. Сейчас разработкой антивирусов занимаются крупные компании. Как и у создателей вирусов, в этой сфере также сформировались оригинальные приёмы — но уже для поиска и борьбы с вирусами. Современные антивирусные программы могут обнаруживать десятки тысяч вирусов.

К сожалению, конкуренция между антивирусными компаниями привела к тому, что развитие идёт в сторону увеличения количества обнаруживаемых вирусов (прежде всего для рекламы), а не в сторону улучшения их детектирования (идеал — 100%-е детектирование) и алгоритмов лечения заражённых файлов.

Антивирусное программное обеспечение состоит из компьютерных программ которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы.



Скриншот антивирусной программы

Методы обнаружения вирусов

Антивирусное программное обеспечение обычно использует два отличных друг от друга метода для выполнения своих задач:

- Сканирование файлов для поиска известных вирусов, соответствующих определению в антивирусных базах
- Обнаружение подозрительного поведения любой из программ, похожего на поведение заражённой программы.

Метод соответствия определению вирусов в словаре

Основная статья: ***Обнаружение, основанное на сигнатурах***

Это метод, когда антивирусная программа, просматривая файл, обращается к антивирусным базам, которые составлены производителем программы-антивируса. В случае соответствия какого либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в базах, программа антивирус может по запросу выполнить одно из следующих действий:

1. Удалить инфицированный файл.
2. Заблокировать доступ к инфицированному файлу.
3. Отправить файл в карантин (то есть сделать его недоступным для выполнения, с целью недопущения дальнейшего распространения вируса).
4. Попытаться восстановить файл, удалив сам вирус из тела файла.
5. В случае невозможности лечения/удаления, выполнить эту процедуру при перезагрузке

Хотя антивирусные программы, созданные на основе поиска соответствия определению вируса в словаре, при обычных обстоятельствах, могут достаточно эффективно препятствовать вспышкам заражения компьютеров, авторы вирусов стараются держаться на полшага впереди таких программ-антивирусов, создавая «олигоморфические», «полиморфические» и, самые новые, «метаморфические» вирусы, в которых некоторые части шифруются или искажаются так, чтобы невозможно было обнаружить совпадение с определением в словаре вирусов.

Метод обнаружения странного поведения программ

Основная статья: ***Обнаружение аномалий***

Антивирусы, использующие метод обнаружения подозрительного поведения программ не пытаются идентифицировать известные вирусы, вместо этого они прослеживают поведение всех программ. Если программа пытается записать какие-то данные в исполняемый файл (exe-файл), программа-антивирус может пометить этот файл, предупредить пользователя и спросить что следует сделать. В настоящее время, подобные превентивные медоды обнаружения вредоносного кода, в том или ином виде, широко применяются в качестве модуля антивирусной программы, а не отдельного продукта.

Другие названия: Проактивная защита, Поведенческий блокиратор, Host Intrusion Prevention System (HIPS), В отличие от метода поиска соответствия определению вируса в антивирусных базах, метод обнаружения подозрительного поведения даёт защиту от новых вирусов, которых ещё нет в антивирусных базах. Однако следует учитывать, что программы или модули, построенные на этом методе, выдают также большое количество предупреждений (в некоторых режимах работы), что делает пользователя мало восприимчивым ко всем предупреждениям. В последнее время эта проблема ещё более ухудшилась, так как стало появляться всё больше невредоносных программ, модифицирующих другие exe-файлы, несмотря на существующую проблему ошибочных предупреждений. Не смотря на наличие большого количества предупреждающих диалогов, в современном антивирусном программном обеспечении этот метод используется всё больше и больше. Так, в 2006 году вышло несколько продуктов, впервые реализовавших этот метод: Kaspersky Internet Security, Kaspersky Antivirus, Safe'n'Sec, F-Secure Internet Security, Outpost Firewall Pro, DefenceWall. Многие программы класса файрволл издавна имели в своем составе модуль обнаружения странного поведения программ.

Метод обнаружения при помощи эмуляции

Основная статья: ***Обнаружение, основанное на эмуляции***

Некоторые программы-антивирусы пытаются имитировать начало выполнения кода каждой новой вызываемой на исполнение программы перед тем как передать ей управление. Если программа использует самоизменяющийся код или проявляет себя как вирус (то есть немедленно начинает искать другие exe-файлы например), такая программа будет считаться вредоносной, способной заразить другие файлы. Однако этот метод тоже изобилует большим количеством ошибочных предупреждений.

Другие методы обнаружения вирусов

Ряд других методов предлагается в исследованиях и используется в антивирусных программах (см. также эвристическое сканирование).

Важные замечания

- Распространение вирусов по электронной почте (возможно наиболее многочисленных и вредоносных) можно было бы предотвратить недорогими и эффективными средствами без установки антивирусных программ, если бы были устранены дефекты программ электронной почты, которые сводятся к выполнению без ведома и разрешения пользователя исполняемого кода, содержащегося в письмах.
- Обучение пользователей может стать эффективным дополнением к антивирусному программному обеспечению. Простое обучение пользователей правилам безопасного использования компьютера (например не загружать и не запускать на выполнение неизвестные программы из Интернета) снизило бы вероятность распространения вирусов и избавило бы от надобности пользоваться многими антивирусными программами.
- Пользователи компьютеров не должны всё время работать с правами администратора. Если бы они пользовались режимом доступа обычного пользователя, то некоторые разновидности вирусов не смогли бы распространяться (или, по крайней мере, ущерб от действия вирусов был бы меньше). Это одна из причин, по которым вирусы в Unix-подобных системах относительно редкое явление.
- Метод обнаружения вирусов по поиску соответствия в словаре не всегда достаточен из-за продолжающегося создания всё новых вирусов, метод подозрительного поведения не работает достаточно хорошо из-за большого числа ошибочных решений о принадлежности к вирусам незаражённых программ. Следовательно, антивирусное программное обеспечение в его современном виде никогда не победит компьютерные вирусы.
- Различные методы шифрования и упаковки вредоносных программ делают даже известные вирусы необнаруживаемыми антивирусным программным обеспечением. Для обнаружения этих «замаскированных» вирусов требуется мощный механизм распаковки, который может дешифровать файлы перед их проверкой. К несчастью, во многих антивирусных программах эта возможность отсутствует и, в связи с этим, часто невозможно обнаружить зашифрованные вирусы.
- Постоянное появление новых вирусов даёт разработчикам антивирусного программного обеспечения хорошую финансовую перспективу.
- Некоторые антивирусные программы могут значительно понизить быстродействие. Пользователи могут запретить антивирусную защиту, чтобы предотвратить потерю быстродействия, в свою очередь, увеличивая риск заражения вирусами. Для максимальной защищённости антивирусное программное обеспечение должно быть подключено всегда, несмотря на потерю быстродействия. Некоторые антивирусные

программы (как AVG for Windows) не очень сильно влияют на быстродействие.
- Иногда приходится отключать антивирусную защиту при установке обновлений программ, таких, например, как Windows Service Packs. Антивирусная программа, работающая во время установки обновлений, может стать причиной неправильной установки модификаций или полной отмене установки модификаций. Перед обновлением Windows 98, Windows 98 Second Edition или Windows ME на Windows XP (Home или Professional), лучше отключить защиту от вирусов, в противном случае процесс обновления может завершиться неудачей.

Антивирусные компании и программы

- AOL® Virus Protection в составе AOL Safety and Security Center
- ActiveVirusShield от AOL (на базе KAV 6)
- AhnLab
- Aladdin Knowledge Systems
- Alwil
- AVG
- Avira Из Германии
- BitDefender из Румынии
- BullGuard из Дании
- Computer Associates США
- Comodo Group США
- ClamAV — GPL
- ClamWin — GPL ClamAV for Windows
- Dr.Web из России
- Eset NOD32 из Словакии
- Frisk Software из Исландии
- F-Secure из Финляндии
- GeCAD из Румынии (Microsoft купил компанию в 2003)
- GFI Software
- Grisoft (AVG)
- Hauri
- H+BEDV из Германии
- Kaspersky из России
- McAfee США
- MicroWorld Technologies из Индии
- MKS из Польши
- Norman из Норвегии
- Panda Software из Испании
- Sophos из Великобритании
- Stiller Research
- ROSE SWE
- Sybari Software (Microsoft купил компанию в начале 2005)
- Symantec США или Великобритания
- Trend Micro из Японии (номинально Тайвань-США)
- Украинский Национальный Антивирус с Украины
- VirusBuster из Венгрии
- ZoneAlarm AntiVirus (из Zone Labs)
- Quick Heal AntiVirus из Индии