АНТИВИРУСЫ

Средство обнаружения вредоносных программ

МЕТОДЫ ЗАЩИТЫ ОТ ВИРУСОВ

- *Для защиты от вирусов используют три группы методов:*
- *Методы, основанные на анализе содержимого файлов (как файлов данных, так и файлов с кодами команд). К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд.*
- *Методы, основанные на отслеживании поведения программ при их выполнении. Эти методы заключаются в протоколировании всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, либо при его программной эмуляции.*
- *Методы регламентации порядка работы с файлами и программами. Эти методы относятся к административным мерам обеспечения безопасности*
- *Метод сканирования сигнатур (сигнатурный анализ, сигнатурный метод) основан на поиске в файлах уникальной последовательности байтов - сигнатуры, характерной для определенного вируса. Для каждого вновь обнаруженного вируса специалистами антивирусной лаборатории выполняется анализ кода, на основании которого определяется его сигнатура. Полученный кодовый фрагмент помещают в специальную базу данных вирусных сигнатур, с которой работает антивирусная программа. Достоинством данного метода является относительно низкая доля ложных срабатываний, а главным недостатком - принципиальная невозможность обнаружения в системе нового вируса, для которого отсутствует сигнатура в базе данных антивирусной программы, поэтому требуется своевременная актуализация базы данных сигнатур.*

АНТИВИРУСЫ

Первые антивирусные программы появились еще зимой 1984 года (первый вирус для персональных компьютеров Apple появился в 1977 году, и только в 1981 году появились вирусы, представляющие какую-либо угрозу) под названиями CHK4BOMB и BOMBSQAD. И х написал американский программист Энди Хопкинс (Andy Hopkins).

- ***Антивирусная программа*** –специализированная программа для обнаружения компьютерных вирусов ,а так же не желательных вредоносных программ и восстановления заражённых такими файлов ,а так же для профилактики приложений .

МЕТОДЫ ЗАЩИТЫ ОТ ВИРУСОВ

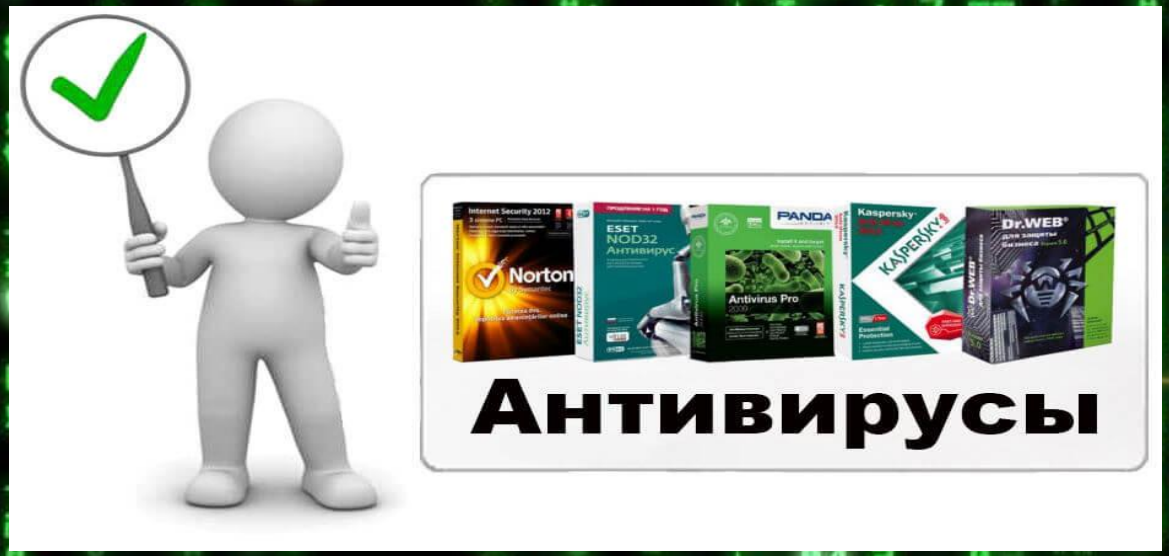
- *Метод контроля целостности основывается на том, что любое неожиданное и беспричинное изменение данных на диске является подозрительным событием, требующим особого внимания антивирусной системы. Вирус обязательно оставляет свидетельства своего пребывания (изменение данных существующих (особенно системных или исполняемых) файлов, появление новых исполняемых файлов и т.д.). Факт изменения данных - нарушение целостности - легко устанавливается путем сравнения контрольной суммы (дайджеста), заранее подсчитанной для исходного состояния тестируемого кода, и контрольной суммы (дайджеста) текущего состояния тестируемого кода. Если они не совпадают, значит, целостность нарушена и имеются все основания провести для этого кода дополнительную проверку, например, путем сканирования вирусных сигнатур. Указанный метод работает быстрее метода сканирования сигнатур, поскольку подсчет контрольных сумм требует меньше вычислений, чем операции побайтового сравнения кодовых фрагментов, кроме того он позволяет обнаруживать следы деятельности любых, в том числе неизвестных, вирусов, для которых в базе данных еще нет сигнатур .*
- *Метод сканирования подозрительных команд (эвристическое сканирование, эвристический метод) основан на выявлении в сканируемом файле некоторого числа подозрительных команд и(или) признаков подозрительных кодовых последовательностей (например команда форматирования жесткого диска или функция внедрения в выполняющийся процесс или исполняемый код). После этого делается предположение о вредоносной сущности файла и предпринимаются дополнительные действия по его проверке. Этот метод обладает хорошим быстродействием, но довольно часто он не способен выявлять новые вирусы.*

МЕТОДЫ ЗАЩИТЫ ОТ ВИРУСОВ

- Метод отслеживания поведения программ принципиально отличается от методов сканирования содержимого файлов, упомянутых ранее. Этот метод основан на анализе поведения запущенных программ, сравнимый с поимкой преступника «за руку» на месте преступления. Антивирусные средства данного типа часто требуют активного участия пользователя, призванного принимать решения в ответ на многочисленные предупреждения системы, значительная часть которых может оказаться впоследствии ложными тревогами. Частота ложных срабатываний (подозрение на вирус для безвредного файла или пропуск вредоносного файла) при превышении определенного порога делает этот метод неэффективным, а пользователь может перестать реагировать на предупреждения или выбрать оптимистическую стратегию (разрешать все действия всем запускаемым программам или отключить данную функцию антивирусного средства). При использовании антивирусных систем, анализирующих поведение программ, всегда существует риск выполнения команд вирусного кода, способных нанести ущерб защищаемому компьютеру или сети. Для устранения подобного недостатка позднее был разработан метод эмуляции (имитации), позволяющий запускать тестируемую программу в искусственно созданной (виртуальной) среде, которую часто называют песочницей (sandbox), без опасности повреждения информационного окружения. Использование методов анализа поведения программ показало их высокую эффективность при обнаружении как известных, так и неизвестных вредоносных программ

ЛЖЕАНТИВИРУСЫ

- В 2009 началось активное распространение лжеантивирусов — программного обеспечения, не являющегося антивирусным (то есть не имеющего реальной функциональности для противодействия вредоносным программам), но выдающим себя за таковое. По сути, лжеантивирусы могут являться как программами для обмана пользователей и получения прибыли в виде платежей за «лечение системы от вирусов», так и обычным вредоносным программным обеспечением.



ЭФФЕКТИВНОСТЬ АНТИВИРУСОВ

- *Аналитическая компания Imperva в рамках проекта Hacker Intelligence Initiative опубликовала интересное исследование, которое показывает малую эффективность большинства антивирусов в реальных условиях.*
- *По итогам различных синтетических тестов антивирусы показывают среднюю эффективность в районе 97 %, но эти тесты проводятся на базах из сотен тысяч образцов, абсолютное большинство которых (может быть, около 97 %) уже не используются для проведения атак.*
- *Вопрос в том, насколько эффективными являются антивирусы против самых актуальных угроз. Чтобы ответить на этот вопрос, компания Imperva и студенты Тель-Авивского университета раздобыли на российских подпольных форумах 82 образца самого свежего вредоносного ПО — и проверили его по базе VirusTotal, то есть против 42 антивирусных движков. Результат оказался плачевным.*
- *Эффективность антивирусов против только что скомпилированных зловредов оказалась менее 5 %. Это вполне логичный результат, поскольку создатели вирусов обязательно тестируют их по базе VirusTotal.*

ЭФФЕКТИВНОСТЬ АНТИВИРУСОВ

- *От появления вируса до начала его распознавания антивирусами проходит до четырёх недель — это у «элитных» антивирусов, а у остальных срок может доходить до 9-12 месяцев. Например, в начале исследования 9 февраля 2012 года был проверен свежей образец фальшивого инсталлятора Google Chrome. После окончания исследования 17 ноября 2012 года его определяли только 23 из 42 антивирусов.*
- *У антивирусов с самым высоким процентом определения зловредов присутствует также высокий процент ложных срабатываний.*
- *Хотя исследование сложно назвать объективным, ибо выборка зловредов была слишком маленькой, но можно предположить, что антивирусы совершенно непригодны против свежих киберугроз.*

КЛАССИФИКАЦИЯ

- Антивирусные программы подразделяются по исполнению (средствам блокирования) на:
- программные;
- программно-аппаратные.
- По признаку размещения в оперативной памяти выделяют:
- резидентные (начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов);
- нерезидентные (запускаются по требованию пользователя или в соответствии с заданным для них расписанием).
- По виду (способу) защиты от вирусов различают:
- Программы-детекторы, или сканеры, находят вирусы в оперативной памяти, на внутренних и(или) внешних носителях, выводя сообщение при обнаружении вируса.
- Программы-доктора, фаги, полифаги находят зараженные файлы и "лечат" их. Среди этого вида программ существуют полифаги, которые способны удалять разнообразные виды вирусов, самые известные из антивирусов-полифагов Norton AntiVirus, Doctor Web, Kaspersky Antivirus.

КЛАССИФИКАЦИЯ

- Программы-вакцины (иммунизаторы) выполняют иммунизацию системы (файлов, каталогов) блокируя действие вирусов.
- Программы-ревизоры являются наиболее надежными в плане защиты от вирусов. Ревизоры запоминают исходное состояние программ, каталогов, системных областей диска до момента инфицирования компьютера (как правило, на основе подсчета контрольных сумм), затем сравнивают текущее состояние с первоначальным, выводя найденные изменения на дисплей.
- Программы-мониторы начинают свою работу при запуске операционной системы, постоянно находятся в памяти компьютера и осуществляют автоматическую проверку файлов по принципу "здесь и сейчас".
- Программы-фильтры (сторожа) обнаруживают вирус на ранней стадии, пока он не начал размножаться. Программы-сторожа - небольшие резидентные программы, целью которых является обнаружение действий, характерных для вирусов.