Антивирусная защита

Антивирус

Определение

Антивирус — программное средство, предназначенное для борьбы с вирусами

- Как следует из определения, основными задачами антивируса является:
  - Препятствование проникновению вирусов в компьютерную систему
  - Обнаружение наличия вирусов в компьютерной системе
  - Устранение вирусов из компьютерной системы без нанесения повреждений другим объектам системы
  - Минимизация ущерба от действий вирусов

Технологии обнаружения вирусов

Технологии, применяемые в антивирусах, можно разбить на две группы:

- Технологии сигнатурного анализа
- Технологии вероятностного анализа

Сигнатурный анализ

— метод обнаружения вирусов, заключающийся в проверке наличия в файлах сигнатур вирусов

- Сигнатурный анализ является наиболее известным методом обнаружения вирусов и используется практически во всех современных антивирусах. Для проведения проверки антивирусу необходим набор вирусных сигнатур, который хранится в антивирусной базе.

Антивирусная база

— база данных, в которой хранятся сигнатуры вирусов

- Ввиду того, что сигнатурный анализ предполагает проверку файлов на наличие сигнатур вирусов, антивирусная база нуждается в периодическом обновлении для поддержания актуальности антивируса. Сам принцип работы сигнатурного анализа также определяет границы его функциональности — возможность обнаруживать лишь уже известные вирусы — **против новых вирусов сигнатурный сканер бессилен.**
- С другой стороны, наличие сигнатур вирусов предполагает возможность лечения инфицированных файлов, обнаруженных при помощи сигнатурного анализа. Однако, лечение допустимо не для всех вирусов — трояны и большинство червей не поддаются лечению по своим конструктивным особенностям, поскольку являются цельными модулями, созданными для нанесения ущерба.

Технологии вероятностного анализа

подразделяются на три категории:

- Эвристический анализ
- Поведенческий анализ
- Анализ контрольных сумм

Эвристический анализ

— технология, основанная на вероятностных алгоритмах, результатом работы которых является выявление подозрительных объектов

- В процессе эвристического анализа проверяется структура файла, его соответствие вирусным шаблонам. Наиболее популярной эвристической технологией является проверка содержимого файла на предмет наличия модификаций уже известных сигнатур вирусов и их комбинаций. Это помогает определять гибриды и новые версии ранее известных вирусов без дополнительного обновления антивирусной базы.
- Эвристический анализ применяется для обнаружения неизвестных вирусов, и, как следствие, не предполагает лечения.
- Данная технология не способна на 100% определить вирус перед ней или нет, и как любой вероятностный алгоритм грешит ложными срабатываниями.

Поведенческий анализ

— технология, в которой решение о характере проверяемого объекта принимается на основе анализа выполняемых им операций

- Поведенческий анализ весьма узко применим на практике, так как большинство действий, характерных для вирусов, могут выполняться и обычными приложениями. Наибольшую известность получили поведенческие анализаторы скриптов и макросов, поскольку соответствующие вирусы практически всегда выполняют ряд однотипных действий. Например, для внедрения в систему, почти каждый макровирус использует один и тот же алгоритм: в какой-нибудь стандартный макрос, автоматически запускаемый средой Microsoft Office при выполнении стандартных команд (например, « Save », « Save As», «Open», и т.д.), записывается код, заражающий основной файл шаблонов normal.dot и каждый вновь открываемый документ.
- Средства защиты, вшиваемые в BIOS, также можно отнести к поведенческим анализаторам. При попытке внести изменения в MBR компьютера, анализатор блокирует действие и выводит соответствующее уведомление пользователю.
- Помимо этого поведенческие анализаторы могут отслеживать попытки прямого доступа к файлам, внесение изменений в загрузочную запись дискет, форматирование жестких дисков и т.д.
- Поведенческие анализаторы не используют для работы дополнительных объектов, подобных вирусным базам и, как следствие, неспособны различать известные и неизвестные вирусы — все подозрительные программы априори считаются неизвестными вирусами. Аналогично, особенности работы средств, реализующих технологии поведенческого анализа, не предполагают лечения.

Анализ контрольных сумм

— это способ отслеживания изменений в объектах компьютерной системы. На основании анализа характера изменений — одновременность, массовость, идентичные изменения длин файлов — можно делать вывод о заражении системы

- Анализаторы контрольных сумм (также используется название «ревизоры изменений») как и поведенческие анализаторы не используют в работе дополнительные объекты и выдают вердикт о наличии вируса в системе исключительно методом экспертной оценки. Большая популярность анализа контрольных сумм связана с воспоминаниями об однозадачных операционных системах, когда количество вирусов было относительно небольшим, файлов было немного и менялись они редко.
- Сегодня ревизоры изменений утратили свои позиции и используются в антивирусах достаточно редко.
- Чаще подобные технологии применяются в сканерах при доступе — при первой проверке с файла снимается контрольная сумма и помещается в кэше, перед следующей проверкой того же файла сумма снимается еще раз, сравнивается, и в случае отсутствия изменений файл считается незараженным.

Категории антивирусов

- Таким образом, антивирусы можно разделить на две большие категории:
- **Предназначенные для непрерывной работы** — к этой категории относятся средства проверки при доступе, почтовые фильтры, системы сканирования проходящего трафика Интернет, другие средства, сканирующие потоки данных
- **Предназначенные для периодического запуска** — различного рода средства проверки по запросу, предназначенные для однократного сканирования определенных объектов. К таким средствам можно отнести сканер по требованию файловой системы в антивирусном комплексе для рабочей станции, сканер по требованию почтовых ящиков и общих папок в антивирусном комплексе для почтовой системы (в частности, для Microsoft Exchange)

Спасибо за внимание!