Антивирусная защита

БГА, РТФ
Кафедра ИБ

Зензин Александр Степанович, к.т.н.

Обзор

1. Антивирусная защита
2. Сканирование сигнатур
3. Метод контроля целостности
4. Сканирование подозрительных команд
5. Отслеживание поведения программ

Антивирусная защита

Антивирусная защита используется для профилактики и диагностики вирусного заражения, а также для восстановления работоспособности пораженных вирусами информационных систем.

Термин «вирусы» толкуется здесь расширенно — это не только собственно вирусы, но и другие разновидности вредоносных программ, такие как черви, троянские и шпионские программы.

Профилактика заключается в проверке файлов на присутствие вирусов перед их загрузкой на защищаемый компьютер и тем более перед их выполнением на этом компьютере. Диагностический характер носит процедура проверки файлов уже находящихся в памяти компьютера. После констатации вирусного заражения наступает этап восстановления «здоровья» вычислительной системы, который может потребовать как весьма жестких мер, когда из системы удаляются все зараженные файлы, так и не столь жестких, когда файлы исправляют, удаляя из них вредоносный код.
Большинство антивирусных программ в той или иной степени расходуют ресурсы тестируемой системы. Иногда это может вызвать заметное снижение скорости выполнения пользовательских приложений. Однако это не должно быть причиной отключения антивирусных проверок, так как ущерб от «работы» вирусов, как правило, с лихвой превышает затраты вычислительных ресурсов и времени пользователя (администратора) на борьбу с вирусами.

Антивирусная защита

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. Один из наиболее распространенных методов этой группы состоит в том, что в системе (компьютере или корпоративной сети) выполняются только те программы, запись о которых присутствует в списке программ, разрешенных к выполнению в данной системе. Этот список формируется администратором сети из проверенного программного обеспечения.

Сканирование сигнатур

Сигнатура вируса — это уникальная последовательность байтов, которая всегда присутствует в определенном виде вирусов и по которой этот вид вируса можно с большой вероятностью опознать.

Из этого определения следует основная идея метода сканирования сигнатур. Для каждого вновь обнаруженного вируса специалистами выполняется анализ кода, на основании которого определяется сигнатура. Полученный кодовый фрагмент помещают в специальную **базу данных вирусных сигнатур**, с которой работает антивирусная программа.

К размеру сигнатуры предъявляются противоречивые требования. С одной стороны, для того чтобы повысить вероятность правильной диагностики вируса, сигнатура должна быть достаточно длиной — как минимум 8-12 байт, а еще лучше 64 байта. С другой стороны, учитывая огромное число существующих к настоящему моменту вирусов (сотни тысяч), увеличение длины сигнатуры увеличит и без того большой объем базы данных сигнатур.

Система сканирования сигнатур работает следующим образом. Содержимое тестируемого файла сравнивается с каждой из заданных в базе данных этой системы сигнатур. Обнаружив совпадение, система автоматически ставит подозрительный файл на карантин, то есть блокирует файл от возможного использования. Одним из надежных способов такого блокирования является временное шифрование зараженного файла.

ПРИМЕЧАНИЕ

Различные методы шифрования и упаковки вредоносных программ используют и хакеры. После шифрования или архивирования даже известный вирус становится «невидимым» для обычного сканера сигнатур.

Сканирование сигнатур

Затем система сканирования оповещает своего пользователя об обнаружении зараженных файлов и о своих действиях, предпринятых по отношению к ним, а также предлагает пользователю выбрать тот или иной вариант дальнейших действий. В частности, она может предложить удалить файл или попытаться восстановить файл путем удаления вредоносного кода и, возможно, реконструкции его исходной структуры.

Процедура сканирования может выполняться как для отдельных файлов, так и для содержимого всего диска, как регулярно, в соответствии с заранее заданным расписанием, так и время от времени по инициативе пользователя. Некоторые антивирусные системы выполняют сканирование файлов синхронно с выполнением тех или иных операций с файлами: открытием, закрытием файлов или отправкой их в виде почтовых вложений; иногда такая тактика помогает быстрее обнаружить появление вируса.

К достоинствам данного метода относят относительно низкую долю ложных срабатываний. Главным же недостатком является принципиальная невозможность обнаружить присутствие в системе нового вируса, для которого еще нет сигнатуры в базе данных антивирусной программы. Кроме того, создание базы данных сигнатур является делом очень трудоемким, а ее эксплуатация требует постоянного оперативного обновления, что может представлять проблему как для производителей, так и для пользователей антивирусных средств.

Метод контроля целостности

Метод контроля целостности основывается на том, что любое неожиданное и беспричинное изменение данных на диске является подозрительным событием, требующим особого внимания антивирусной системы. Действительно, любой вирус обязательно оставляет свидетельства своего пребывания на диске. Такими «следами» может быть искажение данных в уже существующих файлах или появление новых исполняемых файлов.

Факт изменения данных — нарушение целостности — легко устанавливается путем сравнения контрольной суммы (или 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 сканирование вирусных сигнатур.

В отличие от сканирования сигнатур метод контроля целостности позволяет обнаруживать следы деятельности любых, в том числе неизвестных, вирусов, для которых в базе данных еще нет сигнатур. Кроме того, он работает быстрее, поскольку операции подсчета контрольных сумм требуют меньше вычислений, чем операции сравнения кодовых фрагментов.

Сканирование подозрительных команд

В арсенале вирусных программ есть особенно опасные средства. Примером такого грозного оружия может служить код, вызывающий форматирование жесткого диска. Каждый случай обнаружения такого кода должен переводить систему в состояние тревоги, или, по крайней мере, система должна уведомить пользователя об этом событии и попросить подтверждения, прежде чем выполнить операцию, которая может привести к катастрофическим последствиям.

Известно, что вирусные программы разных видов могут содержать функционально подобные (но программно не идентичные) блоки. Например, многие виды вирусов содержат функцию внедрения в исполняемый код. Для этого они сначала отыскивают файлы с расширениями exe, а затем выполняют для них операции открытия и записи. И хотя совокупность этих действий может быть реализована разными кодовыми последовательностями, ее все же можно характеризовать некоторыми общими признаками, которые могут стать опознавательным знаком для функции внедрения вируса.

Если в результате сканирования в файле обнаруживают некоторое число подозрительных команд и/или признаков подозрительных кодовых последовательностей, то 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.

Отслеживание поведения программы

Принципиально другим подходом по сравнению с методами сканирования содержимого файлов являются методы, основанные на анализе поведения программ во время их выполнения. Этот метод обнаружения вирусов можно сравнить с поимкой преступника «за руку» на месте преступления. Тестируемую программу запускают на выполнение, инструкцию за инструкцией, но все ее подозрительные действия контролируются и протоколируются антивирусной системой. Если программа пытается выполнить какую-либо потенциально опасную команду, например записать данные в исполняемый файл другой программы, то ее работа приостанавливается, и антивирусная система запрашивает пользователя о том, какие действия ей надо предпринять.

Антивирусные средства данного типа часто требуют активного участия в тестировании пользователя, призванного реагировать на многочисленные предупреждения системы, значительная часть которых может оказаться впоследствии ложными тревогами.

ПРИМЕЧАНИЕ

Важной характеристикой любого антивирусного средства является частота ложных положительных («Да, это вирус») и ложных отрицательных («Нет, вирус отсутствует») заключений. Если система слишком часто бьет ложную тревогу, то пользователь этой системы может вообще перестать реагировать на эти сигналы, однако если она слишком часто объявляет зараженный файл «чистым», то возникает вопрос о качестве антивирусного средства.

Отслеживание поведения программы

При использовании антивирусных систем, анализирующих поведение программ, всегда существует риск «пропустить удар» от вируса, в результате которого по ошибке будет выполнена команда вирусного кода, способная нанести ущерб защищаемому компьютеру или сети.

Для устранения этого недостатка был разработан другой метод, который тоже строит работу по распознаванию вирусов на основе анализа выполнения программ, однако тестируемая программа выполняется в искусственно созданной (виртуальной) вычислительной среде, которую иногда называют песочницей (sandbox). Такой способ называют эмуляцией. При эмуляции так же, как и при реальном выполнении, фиксируются все подозрительные действия программы, однако в этом случае отсутствует риск повреждения информационного окружения.

Принцип работы антивирусных средств, построенных на основе анализа поведения программ, показывает, что эти средства могут использоваться для обнаружения не только известных, но и не известных вредоносных программ.

Дополнительные материалы для изучения

- Смотри лекцию 8а «Средства противодействия атакам».