

Итак, AV, как правило, не очень хорошо справляется с поиском информации. Теперь мы немного понимаем, почему это так. Но даже плохая AV-технология может быть полезной, потому что защита, скажем, от 30% всех угроз все равно намного лучше, чем защита от 0% всех угроз. Однако, помимо плохой защиты, в AV-технологиях старой школы есть еще много того, что может не нравиться. Обычный человек может не знать, действительно ли его защищает программное обеспечение, но, как правило, он знает, что оно работает медленно. Это, безусловно, самая распространенная жалоба, которую я слышу об этой технологии от обычных потребителей. Итак, почему большинство AV-систем работают так медленно? Давайте начнем с того, что люди чаще всего замечают это при запуске своих компьютеров.

Да, любое программное обеспечение, которое должно обеспечить вам активную защиту, должно загружаться при запуске компьютера, а это может занять некоторое время. Но, похоже, AV-продукты считают необходимым проверять файлы на вашем компьютере на наличие признаков неисправностей, и это часто отнимает время. Идея сканирования вашего компьютера на наличие неисправностей при загрузке заключается в том, что на вашем компьютере могут быть файлы, которые были недавно определены как неисправные. Итак, возможно, неделю назад вы скачали скринсейвер, но только сегодня ваша компания, производящая AV, решила, что он неисправен. Или, в некоторых случаях, вы могли получить некорректную информацию на компьютере, когда программное обеспечение для AV не было запущено.

Например, у вас может быть компьютер с двойной загрузкой, что означает, что на компьютере установлена вторая операционная система, которая может записывать данные на один и тот же диск. Возможно, вы используете Windows и Linux и загрузили какой-либо Windows-вирус во время работы с Linux (где вы вряд ли используете AV). Типичная задача AV-программного обеспечения - просмотреть каждый файл в вашей файловой системе, определяя, плохой он или нет.

В большинстве AV-программ этот процесс оценки одного файла просто неэффективен. Например, многие поставщики в значительной степени полагаются на технологию, называемую сопоставлением криптографических подписей, но делают это неразумно. Сначала давайте рассмотрим, что такое сопоставление криптографических подписей. Производители AV хотели бы провести точное сопоставление и сказать: "Этот файл, на который мы смотрим, является точной цифровой копией того плохого файла, который мы видели вчера". Однако они не хотят размещать на компьютерах клиентов все вредоносные программы, которые когда-либо были замечены, - это заняло бы слишком много места и дало бы еще больше возможностей злоумышленникам.

Вместо этого они используют некоторую криптографию, которая принимает файл в качестве входных данных и выдает число фиксированного размера. Интересно то, что число, которое получается, кажется чисто случайным, но каждый раз, когда они вводят одни и те же входные данные, появляется один и тот же результат. Числа, которые выводятся из этого алгоритма, являются большими числами — настолько большими, что они никогда не увидят двух разных входных данных, которые выдают один и тот же результат. Этот алгоритм позволяет производителям AV говорить: "Если криптографическая подпись файла равна 267 947 292 070 674 700 781 823 225 417 604 638 969, значит, он неисправен". Теперь им нужно хранить только это число, а не весь файл целиком. Плохой парень может захотеть создать плохое программное обеспечение, которое дает те же результаты, что и популярное хорошее программное обеспечение.

Например, он может попытаться создать программное обеспечение, использующее ту же криптографическую подпись, что и какая-либо версия Microsoft Word, в надежде, что это

затруднит поставщикам разработку подписи, поскольку криптографическая подпись дала бы много ложных срабатываний. Но криптография - это особый соус, делающий это невозможным. Число, которое выскакивает, на самом деле почти случайно, поэтому самое вероятное, что может сделать злоумышленник, - это написать много новых вредоносных программ, пока одна из них, наконец, не даст тот же результат, что и какой-нибудь законный файл. И, как вы можете догадаться, даже если бы все плохие парни в мире объединились для решения этой проблемы, потребовалось бы слишком много попыток, чтобы это стало практичным.

Теперь, когда мы разобрались с криптографическими сигнатурами, давайте посмотрим, как производители AV могут применить их для решения этой проблемы. При просмотре файла они хотели бы определить его криптографическую подпись, а затем посмотреть подпись в базе данных, чтобы убедиться, что она неверна. И, надеюсь, поиск в базе данных будет невероятно быстрым. На самом деле, существуют хорошо известные алгоритмы, в которых такой поиск действительно должен быть практически мгновенным. Поиск должен быть намного быстрее, чем вычисление криптографической подписи.

Давайте на мгновение предположим, что это то, что происходит на самом деле (часто это не так). Сколько времени требуется для вычисления криптографической подписи? Что ж, стоимость определяется главным образом количеством времени, которое требуется для чтения файла с вашего жесткого диска. Все остальное, что происходит, практически не имеет значения. Самые быстрые жесткие диски на сегодняшний день способны считывать около 125 мегабайт в секунду. Если ваше AV-программное обеспечение собирается просканировать, скажем, 40 гигабайт файлов, вы потратите не менее 5 минут физического времени на ожидание, пока диск будет занят передачей данных в AV-систему, что является абсолютно идеальным решением.

В то же время, когда другие программы пытаются получить доступ к диску, все замедляется. Другие ваши приложения ожидают паузы в рабочей нагрузке AV, а затем происходит снижение производительности, когда диск приходится перемещать для различных приложений. Если вы проводите сканирование всей системы, где вам необходимо выполнить криптографическую подпись каждого файла, то в результате вы можете ожидать, что все будет происходить очень медленно. Но для некоторых AV-систем ситуация гораздо хуже, потому что для каждого сканируемого файла требуется много дополнительной работы. Вместо того, чтобы просто спросить: "Теперь, когда я обработал этот файл, есть ли его подпись в базе данных?" и получить немедленный ответ, обычно происходит что-то вроде этого:

Я только что обработал файл.

Его подпись - 267,947,292,070,674,700,781,823,225,417,604,638,969.

Давайте назовем эту подпись S.

Равен ли S 221,813,778,319,841,458,802,559,260,686,979,204,948?

Если это так, то файл является вредоносным ПО.

Равен ли S 251,101,867,517,644,804,202,829,601,749,226,265,414?

Если это так, то файл является вредоносным ПО.

Равен ли S 311,677,264,076,308,212,862,459,632,720,079,837,243?

Если это так, то файл является вредоносным ПО.

...

Равен ли S 11,701,885,383,227,023,807,765,753,397,431,618,256?

Если это так, то файл является вредоносным ПО.

В одной из таких проблемных систем вопрос задается один раз для каждой вредоносной программы, имеющей криптографическую подпись. Этот подход не очень хорошо подходит для решения сегодняшней проблемы вредоносных программ. Давайте разберемся, почему. Каждый день создается около 10 000 новых вредоносных программ (большинство из них автоматически генерируются из других вредоносных программ, чтобы избежать обнаружения). Давайте предположим, что AV-компания может отловить их все. Давайте также предположим, что компания добавляла по 10 000 подписей в день всего за год. Это 3 650 000 подписей.

Если на обработку одной подписи уходит миллионная доля секунды (а это, вероятно, займет несколько миллионных долей), то на обработку всех этих подписей потребуется 3,65 секунды. На самом деле у AV-компаний есть другие методы, которые они предпочитают использовать, если им не нужно использовать криптографические подписи. Они хотели бы иметь возможность перехватывать как можно больше вредоносных программ с помощью одной подписи, и поскольку они, как правило, не видят все 10 000 новых вредоносных программ в день, они собираются сосредоточить свои подписи на “наиболее важных” вредоносных программах.

Как и следовало ожидать, крупные компании обычно отдают предпочтение тому, что им присылают их крупные корпоративные клиенты, а не тому, что они получают от небольших компаний, и частные лица, скорее всего, будут проигнорированы — даже в крупнейших компаниях в любой момент времени всего несколько десятков аналитиков занимаются подобными вопросами. При таком большом количестве вредоносных программ криптографические контрольные суммы становятся действительно важным методом. Их легко создать (автоматизированные серверные системы могут легко создавать подписи), и эти подписи легко устранить, если они окажутся неправильными. Безусловно, при правильном проектировании криптографические подписи могут повысить эффективность. Глупый способ их обработки, как правило, является артефактом того, как подписи создавались всегда, - это представление о том, что одно правило следует за другим, следует за другим.

Это хорошо работало, когда в общей сложности было всего несколько десятков тысяч вредоносных программ, но сейчас это не так. Производители AV начинают переходить на более разумные способы работы с криптографическими сигнатурами. Но даже когда они это делают, у них все равно остаются все некриптографические сигнатуры. Опять же, в случае с традиционным AV-движком производители надеются, что их обычные сигнатуры будут устранять большинство вредоносных программ. Поскольку существует множество вредоносных программ, которые обходят стороной AV-движки, они хотели бы получить сигнатуры, которые будут обнаруживать множество вредоносных программ, и, надеюсь, даже те, которые еще не были созданы. До тех пор, пока большое внимание уделяется традиционным подписям для защиты, будет существовать множество подписей, выполнение которых может занять много времени, даже если поставщики лучше справляются с криптографическими подписями.

Еще одна причина, по которой количество сигнатур увеличивается, а производительность снижается по мере роста вредоносного ПО, заключается в том, что поставщики антивирусных программ, как правило, не могут легко удалить старые сигнатуры. Поставщики обычно не хранят достаточно данных, чтобы определить, являются ли старые сигнатуры ненужными из-за появления новых сигнатур. Они также не собирают достаточно информации, чтобы узнать,

когда сигнатура может быть удалена, поскольку обнаруженное вредоносное ПО больше не распространяется. Это может показаться рискованным, но есть вредоносные программы, которые не сработали бы даже в том случае, если бы вам удалось установить их на свой компьютер, просто из-за того, что системы развивались со времен старой доброй операционной системы DOS. Теперь, когда мы знаем немного больше о том, почему AV - это проблема, возникает вопрос о том, что может с этим сделать конечный пользователь.

Вы можете выбрать свой AV-продукт, основываясь на исходных показателях производительности, но производительность - это еще не все. И большинство продуктов работают достаточно хорошо, если выполнять сканирование только по запросу. Чаше всего пользователи обращают внимание на сканирование по требованию, и я рекомендую отключить эту функцию. Как правило, нет веских причин выполнять сканирование всей вашей системы, особенно если это приведет к снижению производительности. Вы можете опасаться, что вы вообще не защищены, но программное обеспечение AV наиболее эффективно работает при сканировании в режиме onaccess, а это означает, что AV engine сканирует файлы непосредственно перед тем, как вы начнете их использовать.

Вредоносная программа не может повредить вашей системе, если вы ее не запустите, так кого волнует, что она бездействует на вашем диске? Единственным существенным преимуществом полного сканирования системы является то, что вы можете найти вредоносные файлы до того, как случайно передадите их кому-то другому.

Однако в наши дни почти ни одно вредоносное ПО не распространяется таким образом, и даже если бы это было так, можно было бы надеяться, что у человека, которому вы его передали, также установлена какая-то эффективная защита хоста. В целом, я не думаю, что в этом случае стоит замедлять работу вашего компьютера больше, чем необходимо. Также обратите внимание, что полное сканирование системы обычно выполняется не реже одного раза в день — всякий раз, когда AV-система загружает новые сигнатуры. Однако для большинства людей, которые оставляют компьютер включенным на весь день, это может не иметь значения, поскольку обычно это происходит в середине ночи. В любом случае, многие из этих проблем связаны с тем, что большинство AV-технологий не были созданы для масштабирования. Масштабирование безопасности хостинга - сложная проблема, которую мы рассмотрим в главе 39.

<http://tl.rulate.ru/book/118738/4765017>