В этой главе мы более подробно рассмотрим основу индустрии — антивирусы (AV). Я остановлюсь на том, почему у них плохая репутация и почему эта репутация вполне заслуженная. В следующей главе мы рассмотрим, почему AV работает медленно. Обратите внимание, что многие компании пытаются устранить эти проблемы, но у большинства поставщиков это получается медленно. Я расскажу о сроках улучшения ближе к концу этой книги. Почти все используют AV или, по крайней мере, думают, что используют. В Windows более 90% всех пользователей используют AV, а число людей, которые думают, что это так, еще больше.

Она гораздо более распространена, чем любая другая технология для конечных пользователей, и гораздо чаще встречается в жизни людей, чем единственная другая технология безопасности, имеющая довольно широкое распространение, — брандмауэр. Многих людей удивляет, что AV-технологии настолько распространены, потому что их так широко поносят. Технические специалисты часто заявляют, что AV не работает и что это приводит к проблемам со стабильностью. И почти все утверждают, что это замедляет работу вашего компьютера. Я не могу спорить. Когда я только пришел в McAfee (я некоторое время отсутствовал в McAfee и с тех пор вернулся), я отвечал за разработку ядра AV engine (а не продуктов, в которых использовался этот движок). Я унаследовал его. Я узнал об этом все и изучил всех конкурентов. Во многих AV-компаниях по всему миру было много блестящих людей. Тем не менее, я могу без обиняков сказать, что большинство AV-продуктов оправдывают свою плохую репутацию.

Даже антивирусная программа McAfee была не слишком хороша, когда я унаследовал эту технологию, хотя она быстро совершенствуется и по сей день. Например, в недавнем независимом сравнительном тестировании McAfee была отмечена на первом месте в области обнаружения вредоносных программ, что вполне правдоподобно. Сначала давайте разберемся, что такое AV и как работает типичная технология, а затем рассмотрим, в чем заключаются огромные трудности и почему возникают эти проблемы. Я отложу обсуждение того, как, по моему мнению, все “должно” делаться, до главы 39.

Возможно, вы ожидаете, что я сначала дам определение слову "вирус" как ключевому для понимания AV. Но AV—технологии, как правило, выходят за рамки вирусов, а также пытаются обнаружить червей, программное обеспечение для ботнетов, троянские программы и даже шпионское ПО, рекламное ПО и средства атаки, хотя вопрос о том, являются ли большинство из последних трех категорий вредоносными, может оказаться щекотливым. Например, McAfee (и другие) всегда считали программу nmap плохой, поскольку ее можно использовать в качестве средства атаки, хотя многие, очень многие хорошие парни используют этот инструмент (он просто помогает определить, какие службы видны в сети — название происходит от “карта сети”)..

Логика в основном заключается в том, что среднестатистический пользователь AV не должен иметь его на своем компьютере, и жалобы на программное обеспечение AV на это не помешают законному специалисту использовать этот инструмент. В этом есть заслуга обеих сторон, и во многих случаях все становится плохо, когда решение явно находится в серой зоне. В любом случае, все эти термины на данный момент неуместны. Достаточно сказать, что существует масса плохого программного обеспечения, которое вы, вероятно, не хотели бы использовать на своем компьютере. В отрасли распространенное вредоносное программное обеспечение часто называют вредоносным ПО, и мы будем использовать этот термин.

Шпионское и рекламное ПО иногда находятся в серой зоне, где они не являются намеренно вредоносными и не могут называться вредоносными программами, но вы должны понимать основную идею. Антивирусное программное обеспечение - это программа, которая пытается

идентифицировать вредоносное ПО и либо вообще помешать вам установить или запустить его, либо удалить, если оно уже установлено. Существует два способа запуска антивирусного программного обеспечения: сканирование при доступе и сканирование по требованию. Сканирование при доступе означает, что вот-вот будет запущена какая-то программа или будет использован какой-то другой файл, и AV сначала проверяет его, чтобы определить, может ли он быть неисправен. Сканирование по требованию означает, что файлы проверяются, даже если они не используются. Обычно это происходит при полной проверке системы, которую многие AV-продукты выполняют при загрузке компьютера.

Как правило, когда файл сканируется и обнаруживается, что он поврежден, пользователь получает уведомление и предпринимаются соответствующие действия, такие как удаление файла или (особенно на некоторых предприятиях) помещение его в зону карантина, где он не будет запущен, но кто-нибудь сможет просмотреть его позже. Антивирусный продукт, работающий на настольном компьютере, обычно не слишком хорошо разбирается в том, что является вредоносным ПО, а что нет. В этом заключается работа того, что в отрасли называется DAT (файлами данных) или файлами сигнатур. AV-продукт содержит механизм, который знает, как выбрать файл, который вы хотите отсканировать, а затем запросить один или несколько файлов сигнатур, чтобы выяснить, может ли что-то быть опасным.

Файлы сигнатур часто также содержат информацию о том, как при необходимости предотвратить заражение. Как правило, AV-продукт загружает новые файлы подписей раз в день (если вы постоянно находитесь в Сети). Некоторые продукты проверяются дважды в день или даже ежечасно (а McAfee теперь обновляет их в режиме реального времени). AV-движки, как правило, невероятно универсальны. Они настроены на сопоставление шаблонов с файлами произвольных типов. Они должны понимать любой тип файлов, который потенциально может вызвать проблемы, что является огромной проблемой, особенно если вы собираетесь попытаться обнаружить произвольные файлы данных, такие как изображения, которые могут повредить ваш компьютер, если они будут загружены не в ту программу просмотра фотографий.

В качестве примера того, какими универсальными могут быть AV-движки, можно привести McAfee AV engine, в котором реализовано несколько языков программирования. Файлы сигнатур содержат множество небольших программ, которые AV-движок запускает каждый раз, когда просматривает файл, чтобы определить, является ли этот файл некорректным. Один из языков программирования, используемых McAfee, предназначен для быстрого определения шаблонов в двоичных файлах, а другой - для решения сложных проблем, для решения которых другой язык слишком прост, таких как ремонт. Первый язык специально разработан для того, чтобы люди, пишущие на нем отдельную программу, случайно не стали причиной зависания вашего компьютера.

Второй язык следует использовать с осторожностью и тщательно протестировать перед его внедрением для пользователей. За любой технологией AV обычно стоит обширная работа. Поставщик должен знать достаточно, чтобы быть в состоянии сказать: “Эй, этот файл - вредоносное ПО”, поэтому у него либо должен быть какой-то секретный код, позволяющий ему определять вредоносное ПО с помощью алгоритма, либо ему нужно изучить отдельные программы и принять решение.

Обычно поставщики анализируют вредоносное ПО и пытаются выявить закономерности, а затем создают сигнатуры, которые являются достаточно универсальными, чтобы выявлять как можно больше вредоносных программ, не помечая как плохие то, что на самом деле является хорошим. Затем сотрудники поставщика анализируют файлы, используя некоторую автоматизацию, но, как правило, также прибегая к ручным усилиям. Должен быть разработан

рабочий процесс для отслеживания отправлений и общения с людьми, которые отправляют вредоносные программы. Как только поставщик анализирует файлы, он, при необходимости, создает подпись. Сигнатура может быть достаточно универсальной, чтобы обнаружить и устранить целый класс вредоносных программ, или же она может просто обнаружить одну вредоносную программу, возможно, не устраняя саму причину заражения.

После создания подписей поставщику, как правило, необходимо тщательно протестировать их, чтобы убедиться, что они не вызовут проблем при развертывании. Самая большая проблема заключается в том, что сигнатура может объявить вредоносным ПО то, чего на самом деле нет, и в этом случае считается, что сигнатура дала ложноположительный результат или была поддельной. Поставщику не нравятся ложные срабатывания, особенно потому, что это мешает пользователям запускать программное обеспечение, которое они, возможно, захотят запустить, и, возможно, даже удаляет программное обеспечение. В средствах массовой информации сообщалось о нескольких ложных срабатываниях, но, вероятно, самый серьезный инцидент произошел в марте 2006 года, когда McAfee выпустила обновление сигнатуры, которое обнаружило Microsoft Excel (среди прочего) как вирус и удалило его с компьютеров.

У каждого крупного поставщика есть похожие истории, и у большинства поставщиков есть более свежие истории. В случае с McAfee этот инцидент действительно помог ускорить работу компании по кардинальному совершенствованию ее технологии. Компании, занимающиеся рекламой, тратят много ресурсов на предотвращение ложных срабатываний. Они, как правило, проводят тщательное тестирование сигнатур, в том числе прогоняют их по огромным базам данных известных надежных программ, чтобы убедиться, что ни одна из этих программ не помечена. И в большинстве компаний несколько человек проверяют каждую сигнатуру, чтобы убедиться, что это не окажет негативного влияния. Тем не менее, ложные срабатывания все еще случаются, и довольно часто (хотя обычно в приложениях, которые обычно не используются). После тестирования рекламная компания может опубликовать подписи. Процесс публикации может быть сложным, но часто бывает так, что подписи публикуются примерно в одно и то же время каждый день.

Настольный AV-клиент пытается загрузить эти подписи, когда считает, что они могут быть опубликованы, и продолжает попытки довольно часто, если что-то не так (например, компьютер может быть отключен от сети или подписи могут быть опубликованы с опозданием). Более или менее так работает индустрия аудио-видео в течение последних 20 лет или около того. Технологии на самом деле не сильно улучшились, и они не так эффективны, как должны были бы быть. Давайте рассмотрим проблемы. Наиболее очевидной проблемой является масштабируемость. Каждый день появляются тысячи новых вредоносных программ.

В наши дни большинство из них появляются на довольно небольшом количестве компьютеров (скажем, на десятках), прежде чем они автоматически “мутируют” в несколько другие программы, которые выполняют то же самое. В AV-компаниях, как правило, до 100 человек работают над этой проблемой полный рабочий день, но каждый из этих людей вряд ли сможет справиться с более чем несколькими вредоносными программами в день. Привлечь большое количество людей, обладающих необходимыми навыками для понимания и обнаружения вредоносных программ, чрезвычайно сложно, особенно из-за обширных технических знаний, необходимых для того, чтобы выяснить, какие действия предприняли умные злоумышленники, чтобы помешать индустрии безопасности выполнять свою работу.

Нехватка людей, способных справиться с потоком вредоносных программ, является основной причиной того, что уровень обнаружения AV-технологий настолько низок (некоторые люди говорят, что на практике он достигает 30%). Индустрия пытается справиться с этим, создавая сигнатуры для отдельных частей вредоносного ПО, а затем пытаясь создать сигнатуры,

которые были бы достаточно универсальными, чтобы обнаружить как можно больше вредоносных программ. Но злоумышленники довольно хорошо научились усложнять задачу. На практике лучшее обнаружение, как правило, происходит поэтапно, поскольку хорошие ребята из AV-компании усердно работают над анализом тенденций в отношении большого количества вредоносных программ и пишут код для общего обнаружения как можно большего количества вредоносных программ.

К сожалению, это происходит недостаточно быстро и, как правило, оставляет людей незащищенными от отдельных угроз на длительный период времени. Существует множество других причин, по которым происходит длительная задержка в обнаружении (большое окно уязвимости). Одна из причин заключается в том, что производители видеоигр, как правило, не видят достаточного количества вредоносных программ. Они используют несколько способов получения своих вредоносных программ:

• Многие производители ежедневно обмениваются вредоносными программами друг с другом.

• Многие поставщики имеют свои собственные системы для обхода темных уголков Интернета в поисках вредоносных программ и оставляют уязвимые системы в надежде, что люди взломают их и оставят вредоносное ПО.

• Для крупнейших поставщиков основным источником вредоносного ПО является клиентская база. Клиенты отправляют поставщику вредоносное ПО, которое продукт не смог обнаружить. Часто это крупные корпоративные клиенты, а не частные лица, и на самом деле можно поспорить, что крупные компании уделяют своим проблемам больше внимания, чем мелкие компании. Все это может звучать убедительно, но если десять лет назад эта стратегия хорошо работала (когда одна вредоносная программа, как правило, заражала тысячи пользователей), то сейчас, когда вредоносных программ стало намного больше и они заражают всего несколько десятков пользователей одновременно, она работает не очень хорошо. Еще одна причина, по которой существует большое количество уязвимостей, заключается в том, что производители мультимедийных систем не хотят, чтобы их технология давала ложные срабатывания, как в случае с Microsoft Excel, о котором мы говорили ранее. Но, как я уже говорил, ложные срабатывания легко создать.

Поскольку файлы AV-сигнатур представляют собой код, а в код легко добавлять ошибки, вполне естественно, что в конечном итоге это может привести к ложным срабатываниям. Чтобы решить эту проблему, компаниям, производящим AV-сигнатуры, приходится проводить тестирование, которое требует времени. Если вы объедините это с ежедневной проверкой сигнатур, то разумно ожидать, что между началом распространения вредоносного ПО и его обнаружением AV-продуктом пройдет от 24 до 48 часов. Однако на самом деле это в среднем занимает от одной до трех недель.

Например, в 2007 году Yankee Group опубликовала отчет, в котором обсуждался вирус, известный как руткит Hearse. Компания под названием Prevx обнаружила этот руткит и более или менее незамедлительно предложила защиту. McAfee потребовалось еще 10 дней, чтобы получить подпись, а Symantec - 13 дней. Многие люди думают, что проблема AV-технологий в том, что это простая утилита для подбора шаблонов, замаскированная под что-то более мощное. Возможно, в некоторых случаях это было правдой.

есть некоторые нюансы, но сегодня это, конечно, не так. Поскольку в AV-движках, как правило, используются настоящие языки программирования, они могут выполнять произвольные действия. То, что автограф-разработчики могут делать практически все, еще не означает, что они это делают. Как правило, совершенно новые подходы, которые могли бы существенно

изменить ситуацию, нелегко реализовать с использованием технологий, уже существующих в AV-продуктах, и новые технологии могут легко оказать значительное влияние на конечных пользователей, поскольку неизбежно возникнет множество ошибок и проблем с производительностью. Таким образом, в результате AV-компании, как правило, выполняют четыре действия в своих файлах сигнатур (и часто что-то из этого помещается в “движок”):

• Простое сопоставление шаблонов для отдельных приложений. Это часто сводится к следующему: “Если файл идентичен той вредоносной программе, которую мы видели ранее, значит, он неисправен”. В этом есть некоторые технические хитрости, но он эффективно выполняет поиск точного соответствия без необходимости включать весь файл для каждой вредоносной программы целиком.

• Простое сопоставление с шаблоном для группы похожих приложений. Это называется “общим” обнаружением, и мы надеемся, что шаблон однозначно идентифицирует класс вредоносных программ, а не какое-либо законное программное обеспечение. Если повезет, это поможет избавить AV-компании от необходимости создавать множество индивидуальных сигнатур для других вредоносных программ этого семейства. В некоторых случаях этот тип обнаружения может обнаруживать только один файл, но в наши дни это редко используется, поскольку простые сигнатуры делают то же самое и не рискуют случайно пометить хороший файл как плохой.

• Обратите внимание на внешние факторы (например, на возможное подозрительное поведение при запуске программного обеспечения), чтобы определить, является ли оно вредоносным ПО. Это называется эвристическим обнаружением, что означает, что код основан на наилучшем предположении, даже если компания, производящая аудио-видео, вероятно, раньше не сталкивалась с этой конкретной программой. Это та область, где крупнейшие AV-компании действуют очень осторожно, потому что если они допустят ошибку, то в конечном итоге расстроят клиентов ложными срабатываниями.

• Попытайтесь восстановить систему от заражения. Однако ни один из этих типов сигнатурного содержимого не позволяет в достаточной степени устранить основную проблему масштабирования. Решение проблем масштабирования потребует существенно иного подхода. Конечно, AV-компании пробуют что-то новое, чтобы добиться большего успеха, но это медленный, экспериментальный процесс.

Другая фундаментальная проблема, связанная с точностью воспроизведения видео, заключается в том, что плохие парни тоже могут запускать видео-продукты. Допустим, злой Билл пишет некачественное программное обеспечение. Видео-продукты могут обнаружить это сразу, но Билл сразу же узнает об этом, просто запустив их. Он может продолжать настраивать свое вредоносное ПО до тех пор, пока программы не перестанут жаловаться, а затем распространить его по всему миру и гарантированно получить некоторое время до того, как кто-либо остановит его (как мы видели, это может занять недели). Что еще хуже, если Злому Биллу все-таки удастся установить свою вредоносную программу на ваш компьютер, от нее будет трудно избавиться.

Программное обеспечение Билла почти наверняка выведет из строя ваше аудио-видео программное обеспечение, сделав его неработоспособным. Эти проблемы кажутся непреодолимыми, но некоторые технологии на самом деле обещают решить большинство из них с минимальными затратами. Вопрос в том, почему мы до сих пор не используем более совершенные технологии? Большинству существующих AV-технологий около 20 лет. Большую часть этого времени они работали достаточно хорошо, чтобы достичь и поддерживать почти 100%-ное проникновение на рынок. Таким образом, в некотором смысле, пока деньги

продолжают поступать, у крупных компаний, которые уже вложили значительные средства в создание своей технологии, нет большого экономического стимула вкладывать гораздо больше в ее переосмысление.

Вместо этого деньги на новые разработки, как правило, направляются на создание новых продуктовых линеек, которые потенциально могут принести больше денег. Для крупных компаний с экономической точки зрения может оказаться более разумным позволить кому-то другому (скажем, стартапу) создать более совершенную технологию, а затем приобрести ее, когда в этом возникнет необходимость. В долгосрочной перспективе существуют многообещающие технологии (например, технология коллективного разума, о которой я расскажу в главе 39). Эти технологии могли бы значительно облегчить работу AV-компании, но для этого требуются значительные затраты времени и денег. Я вижу, что индустрия начинает двигаться в этом направлении, но пройдет еще некоторое время, прежде чем мы добьемся этого.