В предыдущей главе я доказывал, что брандмауэр Windows помогает защитить пользователей от интернет-угроз, особенно если пользователь не предпринимает ничего рискованного. В этой главе я собираюсь пожаловаться на брандмауэры, но не только на брандмауэры любого типа. Я собираюсь пожаловаться на персональные брандмауэры, которые немного отличаются от брандмауэра, поставляемого с Windows, и брандмауэра, который вы можете запустить в сети. Что такое персональный брандмауэр?

Предполагается, что брандмауэр отслеживает трафик, поступающий в сеть или выходящий из нее (если брандмауэр подключен к сети), или с компьютера (если он подключен к вашей машине). Он разрешает или блокирует трафик на основе политики. Как правило, операционные системы имеют встроенный брандмауэр, который довольно эффективен. Они останавливают весь трафик, поступающий на компьютер, за исключением случаев, когда это происходит в ответ на какие-либо действия пользователя (хотя вы можете разрешить исключения, например, если хотите запустить свой собственный веб-сервер на своем компьютере).

Но если сетевой трафик инициируется с вашего компьютера, брандмауэр операционной системы, как правило, ничего не делает. Предположим, вы случайно загрузили банковский троян, который будет отслеживать все ваши банковские операции в Интернете, а затем тайно отправлять информацию о вашем аккаунте злоумышленникам на другом конце света. Поскольку вы заражены, ваш AV-сервер уже не смог обнаружить вредоносное программное обеспечение, которое продолжит сбор вашей информации.

Но даже если ваши личные данные будут собраны, что, если вы сможете предотвратить передачу этих данных злоумышленникам? Встроенные брандмауэры, такие как брандмауэр Windows, на самом деле не могут этого сделать. Если вы хотите, чтобы брандмауэр останавливал нежелательный исходящий трафик, вам необходимо предоставить ему информацию о том, какие приложения пытаются взаимодействовать, что является основной идеей персонального брандмауэра (иногда называемого брандмауэром приложений). Это может позволить вам сказать: “Только Internet Explorer может взаимодействовать с устройствами на порту 80” или “Пусть Skype использует все, что ему нравится”. Однако управление политиками - это огромная проблема. Если вы хотите остановить вредоносные программы-трояны, вам нужно начать с политики, которая запрещает все, если вы специально этого не разрешите.

Перечисление используемых вами приложений - это большая работа, и ужасно не забывать настраивать свой персональный брандмауэр каждый раз, когда вы устанавливаете новое программное обеспечение, которое может использовать Интернет. Способ, которым персональные брандмауэры решают эту проблему, заключается в том, что они предоставляют вам всплывающие окна, которые заставляют вас принимать политические решения. Например, когда вы устанавливаете Skype, у вас может появиться всплывающее окно с надписью: “Хотите ли вы skype.exe чтобы получить доступ к Интернету?” И, как правило, вы предлагаете брандмауэру “запомнить ваше решение”, чтобы больше не получать неприятное приглашение. Большинство пользователей терпеть не могут множество приглашений. Ситуация усугубляется тем фактом, что во многих приложениях есть несколько программ, которые будут обрабатываться отдельно.

Например, у большинства приложений есть основной исполняемый файл, который, когда приходит время проверять наличие обновлений программного обеспечения, запускает вторую программу. Вам нужно предоставить доступ к этой программе отдельно. Некоторые приложения устанавливают множество отдельных исполняемых файлов. Например, программа iTunes от Apple устанавливает десятки различных исполняемых файлов с множеством

различных функций. Если вы действительно использовали все функции, которые входят в комплект поставки, то в конечном итоге можете получать множество запросов.

Эти подсказки - единственный способ заставить персональный брандмауэр работать достаточно хорошо, но я бы сказал, что они недостаточно разумны. Дело не только в том, что диалоговые окна неприятны. Дело в том, что они пытаются заставить пользователей принимать решения, к принятию которых они не готовы. Обычно случается так, что люди в конечном итоге видят программу, которую они не узнают. Например, вы можете увидеть приглашение, в котором говорится: “GCONSYNC.EXE хотели бы воспользоваться Интернетом. Хотите ли вы разрешить это?”

Вы могли бы сказать себе: “Что, черт возьми, происходит GCONSYNC.EXE ?!?”, и вы можете отказаться от этого, просто на случай, если это что-то плохое. Что ж, если вы это сделаете, то заблокируете один из многочисленных компонентов iTunes. Как только вы блокируете что-то, что вам знакомо, и программа выходит из строя, если вы похожи на большинство людей, вы будете считать, что у каждой программы, которую вы не узнаете, есть действительная цель, и просто начнете разрешать все. Конечно, некоторые люди могут искать информацию о каждом разрешенном ими исполняемом файле, но для обычного пользователя это заняло бы слишком много времени. Я просто отключаю свой персональный брандмауэр. Если мне придется нажимать, чтобы разрешить все, что он мне показывает, зачем беспокоиться о раздражающих всплывающих окнах? Если бы я оставил его включенным, то, вероятно, просто чувствовал бы себя в большей безопасности, чем есть на самом деле.

Я действительно считаю, что можно установить персональный брандмауэр, который не будет мешать вам, за исключением очень редких случаев. Возьмем, к примеру, GCONSYNC.EXE. Эта программа подписана Apple, что означает, что мы можем быть уверены в ее законности. Apple - уважаемый поставщик, так почему кто-то должен спрашивать об этом? Просто ознакомьтесь с этим. Конечно, не каждая программа имеет цифровую подпись — многие из них таковыми не являются. Мы не будем вдаваться в технические подробности, но мы должны ожидать, что поставщики систем безопасности смогут составить большой список хорошего программного обеспечения, используя всевозможные методы. Затем предупредите нас только о том, что может оказаться вредным, и это должен быть очень короткий список. Каталогизация всего программного обеспечения в мире может показаться безнадежной задачей, но производители начинают делать это довольно успешно.

Теперь у вас есть возможность использовать персональный брандмауэр, который не так уж и плох, потому что вам почти никогда не придется его видеть. Если все сделано правильно, вы просто получите уведомление о том, что программа блокируется, потому что она, вероятно, неисправна. Вам не пришлось бы ничего делать, если бы система не была неисправна и вам не нужно было бы ее переопределить. Когда этот день настанет, технология станет настолько незаметной, что станет просто частью вашего AV. Не нужно будет даже думать о ней как о персональном брандмауэре. Это хорошо, потому что большинство потребителей в любом случае не знают или не хотят знать, что такое брандмауэр. Даже когда этот день настанет, не ждите, что персональный брандмауэр исчезнет. Поставщики аудио- и видеотехники продолжат предоставлять персональные брандмауэры, потому что многие их клиенты ожидают их появления.

Ограничения традиционных брандмауэров

Когда данные передаются между двумя компьютерами в Интернете, базовая инфраструктура Интернета должна знать, как передавать эти данные туда и обратно. На самом простом уровне это та же проблема, с которой сталкивается почтовое отделение при маршрутизации обычной

почты. Почтовое отделение решает свою проблему, предоставляя вам адрес. В Интернете у компьютеров тоже есть адреса. В отличие от почтовых адресов, интернет-адреса имеют смысл только для компьютеров (они представляют собой просто последовательности чисел, например, 157.166.224.25, это единственный адрес, по которому вы сможете добраться до cnn.com).

Допустим, вы хотите запустить сервер электронной почты и веб-сервер на одном компьютере. Когда кто-то подключается, вам нужен способ определить, к какой службе этот пользователь хочет получить доступ. Для этого вы добавляете номер порта, который напоминает номер почтового ящика (их может быть много, и все они находятся по одному адресу). Как правило, приложения имеют “стандартные” порты. Например, веб-серверы часто подключаются к порту 80 (порт 443, если они подключены безопасно). Но это всего лишь условность — вы можете подключить свой веб-сервер к любому порту, который вам нравится, и люди все равно смогут его найти.

Традиционный брандмауэр позволяет вам устанавливать политику на основе сетевой информации, в первую очередь адресной (хотя есть и другие низкоуровневые параметры, которые вы можете фильтровать). Брандмауэр может легко сказать: “Не разрешайте новые входящие подключения ни к одному порту на этом компьютере”. Это простая и эффективная политика, если только вы не хотите запускать свои собственные службы. Если вам необходимо запустить веб-сервер, который доступен в Интернете, вы можете сделать исключение для этого. Вы также можете настроить брандмауэр таким образом, чтобы он разрешал доступ к веб-серверу, но только с локальных компьютеров. Хотя брандмауэры позволяют легко защитить себя от внешнего мира, вы также можете использовать их для блокирования подключений, которые вы устанавливаете, если эти подключения могут быть установлены вредоносным программным обеспечением.

Например, если вы знаете, что злоумышленники хранят свои данные на одном конкретном компьютере (и вам известен его сетевой адрес), вы можете запретить брандмауэру передавать данные на адрес этого компьютера. Или, если вы знаете, что одно семейство вредоносных программ отправляет данные на множество разных компьютеров, но всегда использует порт 3l337, вы можете отключить весь трафик, направленный на порт 31337, независимо от того, на какой адрес он был направлен. Или, что более реалистично, вы можете решить, что будете пользоваться только Интернетом и электронной почтой, а все остальное, что вы, возможно, захотите использовать, должно быть заблокировано. В этом случае вы могли бы просто заблокировать брандмауэр, который обычно не используется с помощью электронной почты или Интернета.

Многие компании настроили свои брандмауэры таким образом, но, как оказалось, это работает не очень хорошо. Проблема в том, что злоумышленники не хотят, чтобы их данные были заблокированы. Чтобы избежать блокировки, они будут обмениваться данными через порт 80, чтобы их трафик на брандмауэре выглядел как веб-трафик. Даже легальные программы, такие как Skype и онлайн-игры, часто решают отправлять весь свой трафик через порт 80, чтобы брандмауэры их не блокировали. Для них это разумная стратегия, поскольку она облегчает жизнь их пользователей. Часто у пользователей нет возможности изменить политику брандмауэра (особенно на работе), и они злятся на производителей программного обеспечения, а не на своих работодателей. Поскольку злоумышленники могут легко отправлять исходящий трафик через веб—порты, который выглядит точно так же, как законный веб-трафик, традиционные брандмауэры не подходят для остановки исходящего трафика - они хороши только для предотвращения поступления информации.