

Распространенные векторы угроз

Вектор угрозы — это метод, который злоумышленник использует для получения доступа к вашим системам. Иногда его называют вектором атаки. Злоумышленники постоянно ищут новые способы получить доступ к вашим системам. Поэтому они тратят всё своё время на поиск или создание новых векторов угроз.

Например, весьма вероятно, что у вас есть адрес электронной почты, которым вы пользуетесь. И это идеальное место для злоумышленника, чтобы отправить вам информацию, которую он может использовать против вас. Например, он может разместить вредоносные ссылки в электронном письме и побудить вас перейти по ним. После этого он может установить вредоносное ПО или попытаться получить доступ к одной из ваших систем, создав фишинговую страницу.

Фишинговые атаки особенно эффективны при использовании сообщений, потому что они позволяют напрямую связаться с вами и побудить вас перейти по ссылкам, по которым вы обычно не переходите. А когда вы переходите по ссылке и попадаете на сайт, он может показать вам главную страницу, которая выглядит в точности как страница входа в ваш банк. Но на самом деле это не ваш банк. И именно здесь фишинг может воспользоваться вашим доверием к системе обмена сообщениями.

Злоумышленники также могут использовать это сообщение, чтобы внедрить вредоносное ПО в само сообщение или предоставить вам ссылку, которая ведет на сайт, где загружается вредоносное ПО. Это также отличная отправная точка для злоумышленников, поскольку они могут использовать различные методы социальной инженерии. Например, злоумышленник может отправить вам по электронной почте счет с просьбой произвести оплату. Но на самом деле это оплата за услугу, которая так и не была оказана. Или, возможно, они пытаются использовать криптовалютную аферу, чтобы либо получить доступ к вашему существующему криптовалютному кошельку, либо продать вам криптовалюту, которой на самом деле не существует.

Вот пример спама, который я получил в виде текстовых сообщений. Это сообщение было отправлено с адреса электронной почты onmicrosoft.com. Как видите, оно пришло от Почтовой службы США. «Сообщение: у вас есть посылка, которую необходимо доставить, но доставка приостановлена из-за неправильного адреса». Теперь они ждут, что вы перейдёте по ссылке, встроенной в текстовое сообщение.

Наши системы обмена сообщениями могут использоваться не только в качестве вектора атаки. Изображения, которые мы видим на экране, также могут использоваться в качестве вектора атаки. Хорошим примером может служить формат изображений SVG. Это формат масштабируемой векторной графики. Он поддерживается большинством браузеров.

На самом деле это не просто изображение. Это XML-файл, который описывает изображение и позволяет встраивать в XML-код другую информацию. Это значит, что злоумышленник может поместить в описание изображения информацию, которая будет выполняться в вашем браузере. Например, он может внедрить HTML-код. Или в XML-коде, описывающем изображение SVG, может содержаться JavaScript. Некоторые браузеры позволяют включать и отключать определенные типы изображений. Или в них может быть реализован процесс проверки входных данных для этих описаний SVG.

Бот XML-файл, содержащий описание SVG-изображения и код, который потенциально может быть использован в качестве вектора атаки. И всё это умещается в

нескольких строках программного кода. Если запустить его в браузере, отобразится изображение. Это описание треугольника, которое вы видите в XML.

Но поскольку он выводит это изображение на экран, он также запускает любой JavaScript, который вы встроили в XML. В данном случае это относительно безобидное сообщение, в котором просто говорится: «Это атака с использованием межсайтового скрипtinga». И когда вы запустите его, на экране появится именно такое сообщение.

Большинство браузеров отслеживают межсайтовый скрипting и предотвращают запуск таких скриптов. Но если в вашем браузере есть уязвимость или JavaScript, который он пытается запустить, не обязательно является межсайтовым скрипtingом, то с помощью этого встраивания XML его можно запустить.

Вполне очевидно, что файлы, которые мы запускаем в наших системах, могут представлять потенциальную угрозу. Это, безусловно, относится к исполняемым файлам, поскольку это программное обеспечение, которое активно работает в памяти вашей системы. Но исполняемый файл — не единственный тип угрозы, которую можно встретить в файловом формате.

Например, Adobe PDF — очень удобное место для размещения вредоносного ПО, потому что это своего рода хранилище, в которое можно помещать другие типы объектов. Открыв PDF-файл, вы увидите текст, изображения, а в некоторых случаях даже скрипты. И это идеальное место для начала атаки.

Или, возможно, злоумышленник просто скрывает угрозу в существующем наборе сжатых файлов, которые могут быть сжаты с помощью zip, rar или любого другого типа сжатия. Во многих случаях это затрудняет обнаружение атаки, поскольку вы видите только формат сжатого файла, например zip. Но внутри zip-файла могут находиться сотни или тысячи файлов. И один из них может содержать вредоносное ПО.

Наши документы, электронные таблицы и другие офисные файлы также могут стать источником угрозы. Например, Microsoft Office позволяет добавлять в документы макросы. И хотя большинство этих макросов, скорее всего, очень полезны и относительно безопасны, злоумышленник может написать макрос, который будет собирать личную информацию с вашего компьютера и отправлять её злоумышленнику.

Мы также часто сталкиваемся с этим при работе с дополнительными файлами или расширениями, которые могут быть установлены в вашем браузере и содержать вредоносное ПО. Просто добавив такое расширение в браузер, вы подвергаете риску всю свою систему.

Наши мобильные телефоны и системы голосовой связи представляют собой ещё один ценный вектор угрозы для злоумышленников. Это вишинг, или голосовой фишинг, когда вам звонят, чтобы вы сообщили данные своей кредитной карты или другие личные данные. Мы также сталкивались со спамом по IP, когда злоумышленники используют системы передачи голоса по IP для автоматической рассылки спам-сообщений.

Я работал с компаниями, которые потратили миллионы долларов на установку новейших межсетевых экранов, систем предотвращения вторжений и средств сетевой фильтрации. Но злоумышленник может обойти эти системы безопасности, потратив всего 10 долларов на USB-накопитель. Это может быть особенно полезно, если злоумышленнику нужно проникнуть в изолированную сеть, то есть в сеть, не имеющую прямого подключения к внутренней сети.

Вместо этого злоумышленник придёт на парковку этой компании, бросит на землю несколько USB-накопителей и будет надеяться, что кто-нибудь поднимет их, занесёт в здание и подключит. Конечно, на USB-накопителе будет вредоносное ПО, которое может нарушить работу или предоставить возможность получить данные из этих сетей.

Многие клавиатуры, которые мы используем сегодня на наших компьютерах, подключаются через USB. А специально модифицированные USB-накопители могут выступать в качестве клавиатуры для вашего компьютера. И когда вы подключаете USB-накопитель, ваша система внезапно начинает автоматически вводить текст на экране. И всё это благодаря тому, что USB-накопитель выступает в роли клавиатуры.

И, конечно же, если кто-то может подключить USB-накопитель даже к изолированной сети, то ему не составит труда передать большой объём данных, отключить накопитель, и теперь вся эта информация у него на USB-накопителе. Он может положить его в карман и выйти за дверь.

Одна из задач специалиста по безопасности — следить за тем, чтобы всё программное обеспечение было обновлено до последней версии. Это связано с тем, что в существующих версиях программного обеспечения часто встречаются проблемы с безопасностью и уязвимости, которые требуют обновления. Например, в приложении может быть заражённый исполняемый файл. Запустив такое приложение, вы фактически заразите свой локальный компьютер.

Но если это неизвестная уязвимость и злоумышленники первыми обнаружат её, у них может появиться преимущество для проникновения в ваши системы. Именно поэтому мы постоянно обновляем программное обеспечение в наших системах. Мы не только ежемесячно обновляем программное обеспечение Microsoft, но и обновляем всё остальное программное обеспечение при выходе каждого нового патча безопасности.

Но как быть с программным обеспечением, которое не установлено на вашем компьютере? Что, если это безагентная система, для работы с которой вам нужно подключиться к отдельной системе? Это очень распространено, например, в случае с веб-приложениями, когда вам не нужно ничего устанавливать на свой компьютер. Вы просто используете браузер для подключения к внешней системе.

Это означает, что если злоумышленник найдёт способ заразить центральный сервер, он потенциально сможет заразить и всех подключающихся клиентов. Злоумышленнику будет очень легко распространять вирус, поскольку он знает, что каждый человек, который входит в систему в течение дня, запускает новый экземпляр этого программного обеспечения, поскольку всё хранится на сервере.

Как мы уже упоминали, установка исправлений — отличный способ предотвратить получение злоумышленником доступа к известной уязвимости. Мы тратим много времени и сил на то, чтобы поддерживать все наши системы в актуальном состоянии и обновлять их до последней версии программного обеспечения. Однако в вашей сети или центре обработки данных могут быть системы, которые не поддерживаются производителем и для которых он больше не выпускает исправления. В этом случае у вас может не быть возможности установить новое программное обеспечение.

Это очень распространённая проблема, например, в неподдерживаемых версиях операционных систем. Со временем производитель перестаёт поддерживать операционную систему. И это создаёт огромную угрозу безопасности. Если нет

обновлений безопасности, то такая система может представлять угрозу для вашей организации.

Как выяснили многие компании, необходимо убедиться, что все эти неподдерживаемые системы идентифицированы. Были случаи, когда кто-то использовал более старую версию операционной системы на старом компьютере, который стоял под чьим-то столом. А ИТ-отдел даже не подозревал о существовании этой системы.

Вот почему так важно всегда иметь актуальный список всех систем и иметь доступ ко всем отдельным устройствам в сети. Это позволит вам периодически сканировать сеть, чтобы убедиться, что все неподдерживаемые системы исправны и могут быть должным образом защищены вашим ИТ-отделом.

Злоумышленники знают, что ваша собственная сеть создаёт цифровой канал, который позволяет им беспрепятственно перемещаться между всеми системами в вашей сети. Они пользуются уязвимостями, встроенными в эту сетевую инфраструктуру. Например, если у вас есть беспроводная инфраструктура, вам нужно убедиться, что вы используете все новейшие протоколы безопасности. Если вы используете WEP, WPA или WPA2, возможно, вам стоит перейти на новейший протокол WPA3.

Многие организации периодически сканируют свою сеть, чтобы выявить открытые или несанкционированные точки беспроводного доступа, которые могут обеспечить злоумышленнику лёгкий доступ к остальной части сети. Как для проводных, так и для беспроводных сетей рекомендуется включить протокол 802.1X. Это протокол аутентификации, который не позволяет получить доступ к сети без предоставления соответствующих учётных данных.

Даже беспроводные протоколы, такие как Bluetooth, могут быть использованы злоумышленниками в качестве вектора угрозы. Например, они могут использовать их для разведки, чтобы выяснить, где находится конкретная система. Или же реализация Bluetooth в системе может иметь ограничения или недостаточный уровень безопасности, что станет отличной отправной точкой для злоумышленника.

Когда вы устанавливаете веб-сервер в центре обработки данных, для предоставления этих услуг в сети открывается ряд портов. Например, веб-сервер может использовать TCP-порт 80 и TCP-порт 443. Если вы откроете эти порты на устройстве, третья сторона сможет получить доступ по крайней мере к части этой системы. Обычно мы обеспечиваем безопасность, которая предотвращает несанкционированный доступ. Но если злоумышленник знает об уязвимости в программном обеспечении веб-сервера, он может использовать эти открытые порты для проникновения на компьютер.

Это ещё одна причина, по которой мы постоянно обновляем программное обеспечение этих сервисов, чтобы всегда иметь возможность устранить уязвимости, которые могут быть связаны с нашими веб-сервисами или другими приложениями. И, конечно, очень легко неправильно настроить одно из этих сложных приложений. Иногда простая ошибка в конфигурации может привести к несанкционированному доступу к системе.

Каждый раз, когда вы устанавливаете на этот компьютер новую службу, ей требуется собственный номер порта для предоставления доступа извне. Таким образом, чем больше служб вы устанавливаете, тем больше открытых портов и тем менее безопасной может быть система. Это одна из причин, по которой мы используем

брандмауэры на основе портов или брандмауэры с поддержкой приложений для обеспечения дополнительной безопасности систем с открытыми портами. Например, если мы установили на компьютер пять или шесть различных сервисов, мы можем ограничить доступ извне только к одному из них, что, безусловно, сократит количество возможных атак на эту систему.

Давайте посмотрим, смогу ли я угадать учётные данные для вашего кабельного модема или беспроводного маршрутизатора, который вы используете дома. Допустим, вы используете имя пользователя admin и пароль admin. В конце концов, это учётные данные по умолчанию, которые используются во многих точках доступа и маршрутизаторах. Это хороший пример использования учётных данных по умолчанию.

И если вы знаете учётные данные по умолчанию для устройства и кто-то не обновил их, то теперь у вас есть полный доступ к этой системе. К счастью, на многих устройствах, которыми мы пользуемся сегодня, требуется сменить пароль при первом входе в систему. Это означает, что административный доступ, который обычно предоставляется при использовании учётных данных по умолчанию, будет недоступен после первого входа в систему.

Найти учётные данные по умолчанию для этих устройств очень просто. Есть даже такие сайты, как routerpasswords.com, на которых собраны все учётные данные по умолчанию для тысяч различных устройств. После просмотра этого видео вы можете проверить устройства в своей сети и убедиться, что вы не используете ни одну из этих настроек по умолчанию.

Иногда эти векторы угроз проникают в вашу сеть через «парадный вход» — цепочку поставок. Это позволяет третьей стороне получить доступ к вашей инфраструктуре, внедрившись в существующее оборудование, которое вы устанавливаете. Это может произойти в процессе производства. Производитель может даже не подозревать, что происходит. Или это может произойти после производства, когда третья сторона захочет получить доступ к вашим системам.

Иногда эти векторы угроз возникают из-за того, что вы работаете со сторонним поставщиком, который является частью вашей цепочки поставок. Например, вашей сетью может управлять MSP. Это поставщик управляемых услуг. Возможно, вы платите этой сторонней организации за мониторинг ваших систем и получение информации о том, нужно ли что-то обновить или изменить в вашей инфраструктуре. Это также идеальное место для начала атаки, поскольку, получив доступ к MSP, злоумышленник получит доступ и к вашим системам.

Именно этот вектор угрозы использовали злоумышленники, которые в 2013 году получили доступ к сети Target и смогли установить вредоносное ПО на все системы торговых точек, чтобы похитить номера кредитных карт. Злоумышленники получили доступ к системам, которые контролировались подрядчиками по системам отопления, вентиляции и кондиционирования, нанятыми Target, и поэтому смогли перейти из сети HVAC в сеть Target, а затем во все магазины, подключённые к системам Target.

вредоносное ПО, которое позволяло злоумышленникам получать контроль над этими коммутаторами.