Отчет

Маленькая грязная тайна отрасли безопасности

Дискуссия вокруг динамических техник обхода (AET)

Содержание

Введение

В последние годы центральное место в обсуждении вопросов сетевой безопасности занимают постоянные угрозы повышенной сложности (advanced persistent threats — APTs). Многие организации внедряют новые решения для защиты от вредоносных программ этого типа. Тем не менее киберпреступникам по-прежнему удается преодолевать даже самые мощные системы защиты сети, в том числе защитные системы очень крупных предприятий.

Одним из грязных приемов, который хакеры используют для обхода систем защиты и проникновения в наиболее защищенные сети, являются динамические техники обхода (advanced evasion techniques — AETs). Такие техники широко известны в хакерском сообществе и активно распространяются и используются в течение последних лет, однако среди специалистов, ответственных за блокировку этих техник, наблюдается непонимание, неверная интерпретация и использование неэффективных средств защиты.

Для того чтобы оценить отношение ИТ-специалистов к проблеме динамических техник обхода, а также определить, какие средства используются для борьбы с этой проблемой, в январе 2014 г. компания McAfee заказала компании Vanson Bourne соответствующее исследование, в ходе которого были опрошены 800 управляющих информационными службами и менеджеров, отвечающих за безопасность и работающих в различных странах — США, Великобритании, Германии, Франции, Австралии, Бразилии и ЮАР. Результаты исследования показали, что у большинства респондентов нет полного понимания проблемы, и вследствие этого на предприятиях отсутствуют средства защиты, необходимые для блокировки техник AET.

В ходе исследования были получены следующие важные результаты:

- Как минимум один из пяти опрошенных признал, что в его сети были случаи утечки данных (22 %), причем около 40 % специалистов, подтвердивших утечку данных, считают, что основную роль в этом сыграли динамические техники обхода.
- Целых 39 % ИТ-специалистов, ответственных за принятие решений, считают, что в их организации нет средств обнаружения и отслеживания динамических техник обхода.
- Почти две трети респондентов (63 %) в качестве самой трудной проблемы при внедрении технологий по борьбе с техниками AET называют необходимость убедить руководство в том, что подобные атаки действительно представляют серьезную угрозу.

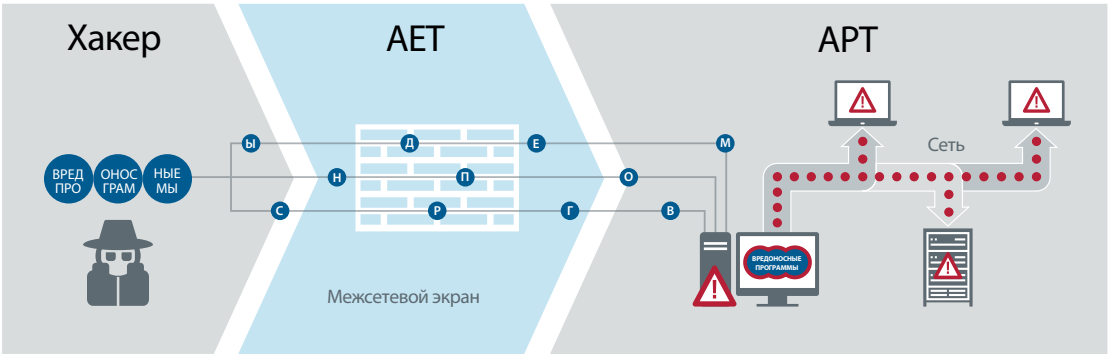
В то время как среди специалистов разгораются ожесточенные дискуссии по поводу самого существования динамических техник обхода, хакеры продолжают успешно использовать эти техники для кражи информации. Такая ситуация позволяет хакерам использовать дополнительные средства для дальнейшего совершенствования сетевых атак и при этом еще дольше оставаться незамеченными, что в конечном итоге ведет к ущербу для компаний и дорогостоящим утечкам информации. Чем дольше продолжаются споры о существовании динамических техник обхода, тем дольше предприятия будут уязвимы для атак такого типа.

Отличия динамических техник обхода (AET) от постоянных угроз повышенной сложности (APT)

Постоянные угрозы повышенной сложности привлекли внимание специалистов по обеспечению безопасности тем, что могут неделями, а то и месяцами оставаться скрытыми, постепенно вытягивая конфиденциальные данные из информационной системы организации. В погоне за прибылью хакеры применяют комплексы APT, которые сочетают в себе различные способы взлома, средства использования уязвимостей, а также вредоносные программы, и способны оставаться незамеченными в сети в течение периода времени, нужного киберпреступникам.

Хорошо оснащенные и замотивированные хакеры используют динамические техники обхода для выполнения атак с применением постоянных угроз повышенной сложности. Сами по себе техники AET не являются атакой: фрагменты кода, используемого в таких техниках, не обязательно вредоносны. Именно поэтому такие техники используются для маскировки атаки. Опасность заключается в том, что динамические техники обхода предоставляют инициаторам атаки доступ к сети, который невозможно обнаружить. Разработка набора техник AET позволяет хакеру создать «универсальную отмычку» для проникновения в любую защищенную сеть, использования ее уязвимых мест и нанесения ущерба объектам атаки.

Для того чтобы обойти элементы управления безопасностью сети, такие как межсетевые экраны и системы предотвращения вторжений (intrusion prevention system — IPS), в динамических техниках обхода используется сочетание различных средств, например фрагментации и скрытых файлов. Техники AET работают за счет разбиения вредоносного содержимого на более мелкие фрагменты, которые маскируются и одновременно отправляются в сеть через различные редко используемые протоколы. Попадая в сеть, фрагменты снова собираются в первоначальный вид для распространения и продолжения атаки с использованием постоянных угроз повышенной сложности.



Хакеры используют **динамические техники обхода (АЕТ)** для маскировки своих атак. К таким техникам относится в том числе разбиение вредоносного содержимого на фрагменты и отправка таких фрагментов в сеть через различные редко используемые протоколы.

Техника АЕТ позволяет успешно преодолеть защиту выбранной сети и остаться незамеченным. Попадая в сеть, фрагменты снова собираются в первоначальный вид для распространения и продолжения атаки с использованием **угроз повышенной сложности (APT)**.

Целью **атак с использованием APT** являются коммерческие или политические организации, поэтому успешность атаки зависит от ее способности оставаться незамеченной в течение продолжительного периода времени.

Рис. 1. Элементы атаки.

Одним из примеров проникновения в сеть с помощью постоянных угроз повышенной сложности, получившим широкую огласку, является кибершпионаж «Операция „Троя"» в Южной Корее. В ходе этой кампании использовались динамические техники обхода и многочисленные специальные средства, которые позволили скрывать факт кибершпионажа в течение четырех лет. Эксперты полагают, что благодаря методам обхода защиты в сеть был запущен замаскированный «троянский конь», который остался необнаруженным и быстро распространился по организации. Эта успешная атака говорит о том, что хакерам хорошо известно о существовании динамических техник обхода и о том, как их использовать.

Разногласия на рынке

Согласно результатам исследования, сотрудники, ответственные за безопасность, могут путать постоянные угрозы повышенной сложности с динамическими техниками обхода и поэтому не обеспечивают полную защиту от последних. Например, среди тех организаций, которые в ходе опроса подтвердили случаи утечки данных в течение последних 12 месяцев, 17 % заявили о том, что перед атакой в их сети были внедрены средства для борьбы с динамическими техниками обхода. Но в то же время оказалось, что большинство респондентов не могут с уверенностью сказать, что же на самом деле представляют собой эти методы обхода. Отсутствие должного понимания привело к появлению ложного чувства защищенности. Явным показателем путаницы является то, что 70 % опрошенных считают, что знают, что такое АЕТ (в Великобритании этот процент ниже — 50 %), в то же время 37 % из них дали неверное определение термину «динамические техники обхода (АЕТ)». Это означает, что дать верное определение АЕТ смогли меньше половины всех участников опроса.

Более половины участников опроса не смогли дать верное определение техникам АЕТ.

Рис. 2. Анализ географического распределения респондентов, правильно ответивших на вопрос об определении АЕТ (из числа 800 опрошенных).

На сегодняшний день были выявлены миллионы комбинаций и модификаций техник AET, основанных на строении сети, и эти техники способны динамично изменяться даже во время атаки. Участники опроса дали неверную оценку количества динамических техник обхода, известных на данный момент — 329 246. На самом деле на сегодняшний день количество протестированных техник AET составляет **более 800 миллионов**. Это еще один показатель того, что сотрудники, отвечающие за безопасность, неверно представляют себе эту угрозу.

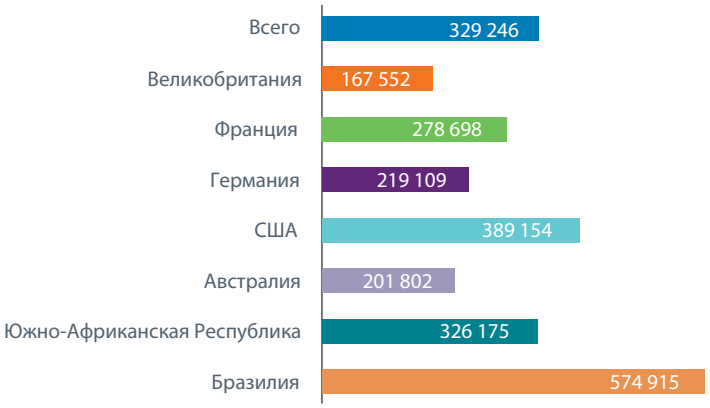


Рис. 3. Ответы на вопрос *«Сколько техник AET, по вашему мнению, обнаружено и исследовано на данный момент?»*
Этот вопрос был задан 800 специалистам. В действительности количество техник AET, о которых сейчас известно, составляет около 800 миллионов.

Результаты опроса показывают, что стандарты кибербезопасности лишь способствуют дальнейшей путанице. Более половины респондентов (63 %) отметили, что огромное количество стандартов по кибербезопасности привели к неверной оценке реальных угроз для предприятий. Этот процент еще выше в Великобритании (70 %) и Австралии (71 %). Однако 80 % опрошенных специалистов, ответственных за безопасность, сообщили, что будут приветствовать появление новых стандартов в отношении техник AET и способов защиты предприятий от них. Это говорит о том, что специалисты нуждаются в четком изложении информации по динамическим техникам обхода и средствам борьбы с такими техниками.

«В погоне за обнаружением новых вредоносных программ большинство организаций совершенно упускает из виду динамические техники обхода, которые помогают вредоносным программам преодолевать имеющуюся защиту. Техники AET — это очень серьезная угроза, так как большинство средств защиты не позволяют обнаружить или блокировать такие техники. Специалисты по обеспечению безопасности, а также руководители предприятий должны осознать всю реальность этой растущей угрозы».

Джон Олтсик (John Oltsik),
главный аналитик,
Enterprise Strategy Group

Ложное чувство защищенности

О техниках AET принято говорить как об атаках, основанных на особенностях строения сетей. Это средство маскировки, позволяющее злоумышленникам во время атаки обходить средства обнаружения. Большинство систем безопасности, представленных на рынке — системы предотвращения (IPS) и обнаружения (IDS) вторжений, системы унифицированного управления угрозами (UTM) и даже межсетевые экраны следующего поколения, — не обладают встроенными средствами для блокировки методов обхода, так как могут лишь анализировать сетевые уровни в пределах одного протокола и проверять отдельные сегменты. Обнаружение известного средства использования уязвимости является довольно простой задачей, однако обнаружение техник AET требует анализа и нормализации трафика всего стека для каждого протокола. Такая глубокая проверка требует привлечения большого количества ресурсов, что может негативно сказаться на общей производительности некоторых систем обеспечения безопасности сети.

Результаты опроса свидетельствуют о том, что отсутствие четкого понимания различий между APT и AET привели к формированию у респондентов ложного чувства защищенности сети. Большинство опрошенных (61 %) отметили, что на сегодняшний день в их сети реализованы средства для отслеживания/обнаружения техник AET. При этом половина (50 %) положительно ответивших на этот вопрос сообщили, что в их организации защита от динамических техник обхода осуществляется за счет IPS (в Бразилии — 60 %), IDS (57 % в Австралии) и (или) защиты конечных точек. На самом деле во всех этих решениях отсутствует защита от методов обхода. Половина опрошенных (50 %) ответили, что знают производителей решений для защиты от техник AET. Из них более 75 % указали производителей, которые на данный момент не предоставляют решений по борьбе с динамическими техниками обхода.

Из этого видно, что многие организации уверены в своей защищенности от техник AET, в то время как на самом деле они защищены только от вредоносных программ и средств использования уязвимости.

Из этого видно, что многие организации уверены в своей защищенности от техник AET, в то время как на самом деле они защищены только от вредоносных программ и средств использования уязвимости.

Такое ложное чувство защищенности может формироваться за счет тестов производительности по защите от техник AET, публикуемых некоторыми производителями. Производители, в свою очередь, используют при тестировании заведомо благоприятные условия, тем самым искажая результаты, что позволяет им создать ощущение, что их системы действительно способны обнаруживать обход защиты. Один из таких производителей заявляет о том, что его продукты обеспечивают защиту только от 60 техник AET, в то время как на данный момент обнаружено уже более 800 миллионов таких техник.

«Существуют миллионы комбинаций и модификаций техник AET, которые способны изменяться даже во время атаки, — утверждает Пэт Калхун (Pat Calhoun), старший вице-президент по защите сетей McAfee. — Именно поэтому традиционные методы анализа сигнатур или обнаружение с помощью сопоставления шаблонов — методы, используемые в большинстве существующих на сегодняшний день решений для обеспечения сетевой безопасности, — не могут эффективно противостоять техникам AET».

Компания McAfee предлагает бесплатный инструмент Evader — средство для выявления техник обхода, которое поможет ИТ-специалистам по обеспечению сетевой безопасности определить наличие техник AET в сети предприятия. Однако ИТ-специалистам следует сохранять бдительность: некоторые производители придумали обходные пути, которые позволяют создать видимость того, что их решения способны определять и блокировать техник AET.

Цена молчания

Ошибочное понимание различий между AET и APT, а также ложное чувство защищенности обходятся предприятиям очень дорого. Почти четверть опрошенных ИТ-специалистов, ответственных за принятие решений (22 %), признали, что за последние 12 месяцев в их сети были случаи утечки данных. Кроме того, каждый двадцатый респондент (6 %) сообщил, что не знает, были ли в его организации случаи утечки данных. Эти цифры оказались еще выше в Германии (31 %) и США (29 %).

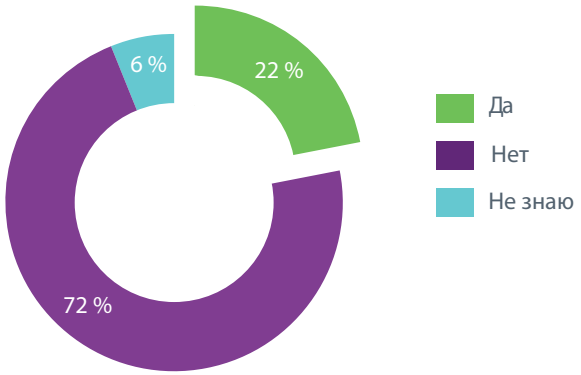


Рис. 4. Ответы на вопрос *«Сталкивалась ли ваша организация со случаями утечки данных в течение последних 12 месяцев?»*
Этот вопрос был задан 800 специалистам.

«На самом деле процент скорее всего еще выше, так как далеко не все специалисты по обеспечению безопасности готовы признать наличие случаев утечки», — говорит Пэт Калхун.

Участники опроса, в организациях которых за последние 12 месяцев наблюдалась утечка данных, в среднем оценивают ущерб в 931 006 долл. США. Согласно полученным данным, в Австралии наблюдалось меньшее количество случаев утечки данных (15 %), при этом средняя оценка нанесенного ущерба значительно выше — 1,5 млн долл. США. В среднем ущерб для американских организаций также превысил 1 млн долл. США. Наиболее серьезным оказался удар по сектору финансовых услуг: оценка ущерба от каждой утечки данных превышает 2 млн долл. США, независимо от страны.

Помимо финансового ущерба организации, утечка данных вредит также бренду и репутации компании, причем такой ущерб может оказаться невосполнимым. Законы о публичном раскрытии информации, например регламент Европейского союза о защите данных и принятый в США Закон об унификации и учете в области медицинского страхования (HIPAA), требуют от организаций отчетности и уведомления клиентов о случаях нарушения конфиденциальности данных, а также уплаты огромных штрафов в управляющие органы. Такие уведомления могут способствовать утрате доверия к компании, что может привести к тому, что клиенты и партнеры начнут искать другого поставщика услуг, и в конечном счете будет означать продолжительные убытки для компании и ущерб ее дальнейшему развитию.

Пять главных требований к системе для борьбы с динамическими техниками обхода

Обычные межсетевые экраны не обеспечивают защиту от техник AET и большинства других угроз. Предприятиям необходима система, которая будет обладать следующими функциями:

1. *Защита от угроз, сложность которых постоянно растет.* За последние 18 месяцев сложность сетевых угроз значительно возросла, особенно это касается борьбы с бот-сетями, обеспечения защищенного доступа к приложениям Веб 2.0 и работы в облачной среде.
2. *Подробная проверка в режиме реального времени.* Возросший объем трафика для приложений SaaS (программное обеспечение как услуга) и HTTP/HTTPS привел к перегрузке межсетевых экранов первого поколения. В действительности почти 85 % трафика является трафиком HTTP/HTTPS. Межсетевые экраны первого поколения оказываются неспособны проводить проверку сетевого трафика в режиме реального времени, либо не способны обеспечить должный уровень такой проверки. Для поддержки такого трафика в большинстве случаев приходится вручную настраивать межсетевые экраны, что является критическим условием обеспечения деятельности организации. В результате за счет ошибок, допущенных специалистами при ручной настройке межсетевых экранов, растет количество случаев утечки данных.
3. *Высокая надежность.* Проблема доступности сети по сей день вызывает серьезную обеспокоенность на предприятиях. Функционал межсетевых экранов первого поколения очень ограничен в отношении поддержки такой доступности. Они не поддерживают кластеризацию межсетевых экранов в режиме «активный–активный», которая позволила бы организации наращивать мощности при необходимости. Кроме того, они также не поддерживают балансировку нагрузки ISP и VPN. Поэтому для кластеризации, балансировки нагрузки и перехода на другой ресурс при сбое приходится использовать дополнительные средства.
4. *Сопоставление данных и прозрачность сети.* Неспособность межсетевых экранов первого поколения сопоставлять сетевые события в значительной степени ограничивает возможности предприятия осуществлять упреждающее управление и обнаруживать сетевые угрозы. Это является серьезным препятствием для прозрачности сети. Самое лучше, что могут позволить межсетевые экраны первого поколения — это сделать моментальный снимок сетевой активности посредством консоли управления. При этом практически отсутствует возможность детализации и изучения конкретных угроз, особенно учитывая тот факт, что в сетях современных предприятий, как правило, установлены десятки межсетевых экранов разных производителей. Например, межсетевой экран первого поколения может уведомить об угрозе, но окажется при этом неспособен определить действие конкретного межсетевого экрана. Поэтому вместо того чтобы немедленно устранить угрозу и обновить все установленные межсетевые экраны для борьбы с похожими атаками, администратору приходится тратить ценное время просто на то, чтобы обнаружить, откуда исходит эта угроза. Такая неэффективность сама по себе является угрозой.
5. *Простое использование и управление.* Каждый межсетевой экран первого поколения требует отдельного управления и ручной настройки. Современные сети состоят из устройств, объединенных сложной конфигурацией. Каждое из таких устройств требует постоянного мониторинга и обновлений. Отсутствие простого способа мониторинга сетевой активности и настройки устройств делает управление межсетевыми экранами первого поколения неупорядоченным и неэффективным. Задача становится еще более сложной из-за того, что в современные сети, как правило, входят устройства различных производителей, каждый из которых оснащает устройства собственной консолью управления. В конечном итоге в связи с растущей популярностью виртуальных сетевых устройств сложность управления растет экспоненциально со снижением прозрачности сети. Использование межсетевых экранов первого поколения не позволяет предприятиям централизованно управлять *всеми* виртуальными и физическими устройствами обеспечения безопасности.

Выводы

Жизненно важным аспектом защиты любой организации является хорошее понимание той роли, которую динамические техники обхода играют в атаках, проводимых с использованием постоянных угроз повышенной сложности. Понимание разницы между APT и AET и способность представить картину угроз способствует снижению рисков для безопасности сети и компании.

Ссылки на ресурсы с информацией о техниках AET

- *Advanced Evasion Techniques For Dummies* (Динамические техники обхода для «чайников»)
- Бесплатный инструмент Evader http://evader.mcafee.com
- Информационный бюллетень *Protect Against Advanced Evasion Techniques* (Защита от динамических техник обхода)

О решении StoneGate FW/VPN

Решение StoneGate FW/VPN использует встроенную технологию, которая декодирует и нормализует сетевой трафик для проверки на всех уровнях протокола, обеспечивая при этом отсутствие в трафике техник для обхода защиты, а также средств использования уязвимости. Компания McAfee обеспечивает самую надежную защиту от большинства известных атак. Такой уровень безопасности отвечает всем современным требованиям и является критически важным для блокировки растущего числа атак, основанных на строении сети и способных обходить обычные системы безопасности сети.

О компании McAfee

McAfee, стопроцентная дочерняя компания Intel Corporation (NASDAQ: INTC), позволяет предприятиям, организациям государственного сектора и домашним пользователям безопасно и эффективно применять Интернет-технологии. Компания поставляет проверенные решения и услуги упреждающей защиты для систем, сетей и мобильных устройств по всему миру. Благодаря своей стратегии Security Connected, новаторскому подходу к решениям безопасности, усиленным средствами аппаратного обеспечения, а также благодаря уникальной сети сбора информации об угрозах Global Threat Intelligence, компания McAfee непрерывно и целеустремленно ищет новые пути защиты своих клиентов. www.mcafee.com/ru

McAfee
An Intel Company

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной», Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.McAfee.ru

60982rpt_aet_0314_fnl_ETMG