Отчет за 2017 год компании Qrator Labs

2017

При информационной
поддержке компании Валарм

Москва, 2018

1

Введение

Интенсивный поток разнообразных атак и нападений с оружием массового поражения, влияющий на значительные части интернета, прекратился — наступило время точных ударов с использованием тактического оружия.

Мы полагаем, что нынешнее прекращение огня представляет собой лишь небольшую передышку перед очередным сражением. Интернет становится все более сложным, а злоумышленники находят все больше векторов для потенциальных атак.

Компании Qrator Labs и Wallarm отметили растущую диверсификацию угроз из-за увеличивающегося множества возможных векторов атаки. Диапазон критических уязвимостей современной глобальной сети настолько широк, что злоумышленники могут выбирать из различные способы создания проблем для практически любой организации. И все большее количество инструментов может работать автоматически, делая централизованное управление излишним.

Узнаваемость проблематики DDoS растет одновременно с увеличением агрессии интернета и изменения его здорового состояния. DDoS-атаки похожи на акул в океане — вы знаете, что они есть, даже не видя плавников над водой. Эта картина в полной мере описывает происходящее в современном интернете, где атаки происходят каждую минуту, становясь новой нормальностью. Те, кто продает защиту и доступность, адаптируются соответствующим образом. В 2017 году интернет-бизнес без защиты от DDoS и без WAF прекратил свое существование.

При растущем количестве инструментов и методов для проведения различных атак, а также различных архивов, распространяющихся со скоростью полезного исходного кода, глубокая интеграция с решениями безопасности приобретает решающее значение для любого цифрового бизнеса. В противном случае практически невозможно построить и поддерживать устойчивую систему и обеспечивать ее защиту.

Если 2016 год можно назвать годом ботнетов и терабитных атак, то 2017 год был годом сетей и маршрутизации. Такие инциденты как спровоцированная Google утечка маршрутов сетей Японии, перехват чужого трафика Level3 в Соединенных Штатах и «Ростелекомом» в России, как и многие другие, демонстрируют устойчивые и высокие риски, связанные с человеческими факторами, основанные на бесхозяйственности и недостаточной автоматизации процессов. Храбрый инженер, уверенно останавливающий важный автоматический сценарий, может создать серьезные проблемы в доступности сетевых ресурсов.

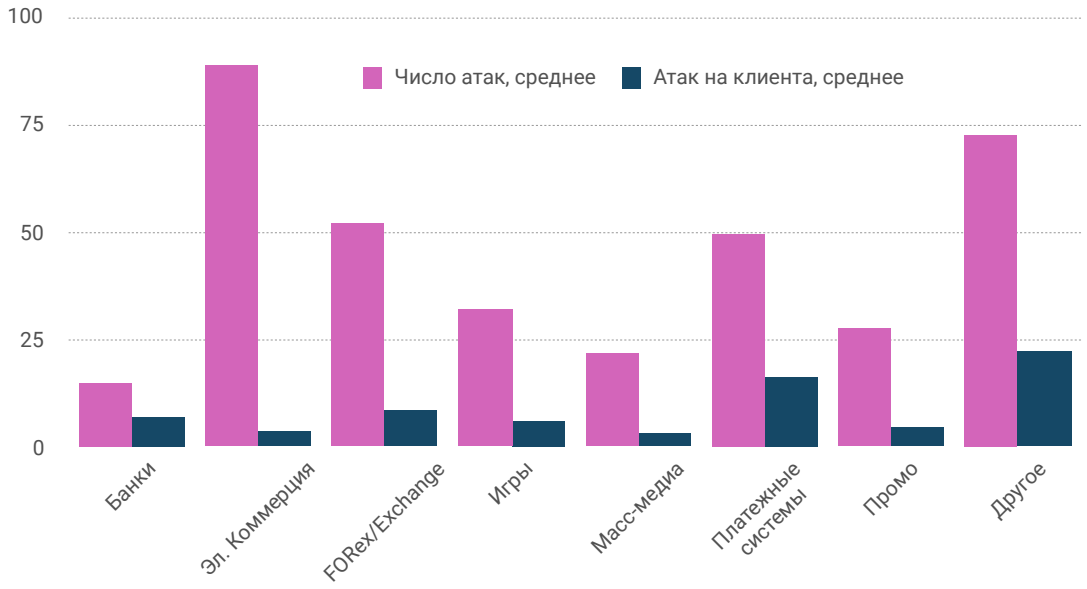
В 2017 году инциденты маршрутизации стали такими же печально известными, как и ботнеты в 2016 г. Успешная DDoS-атака всегда могла сделать один, отдельно взятый ресурс или приложение недоступными. В случае популярных социальных сетей или библиотек, которые разработчики используют для создания и поддержки нормальной работы интернет-сервисов, атака может угрожать целым экосистемам, использующим взаимосвязанные части инфраструктуры (включая хостинг и общего интернет-провайдера). Как мы видели, инциденты маршрутизации могут быть не менее масштабными и опасными, чем атаки рекордного ботнета, оставляя без доступа к популярным ре-

сурсам почти целую страну. Что произойдет, если в один прекрасный день вы вообще не сможете открыть ни одной веб-страницы? Это делает невозможной электронную коммуникацию в том виде, в каком мы ее знаем
и которую считаем саму собой разумеющейся.

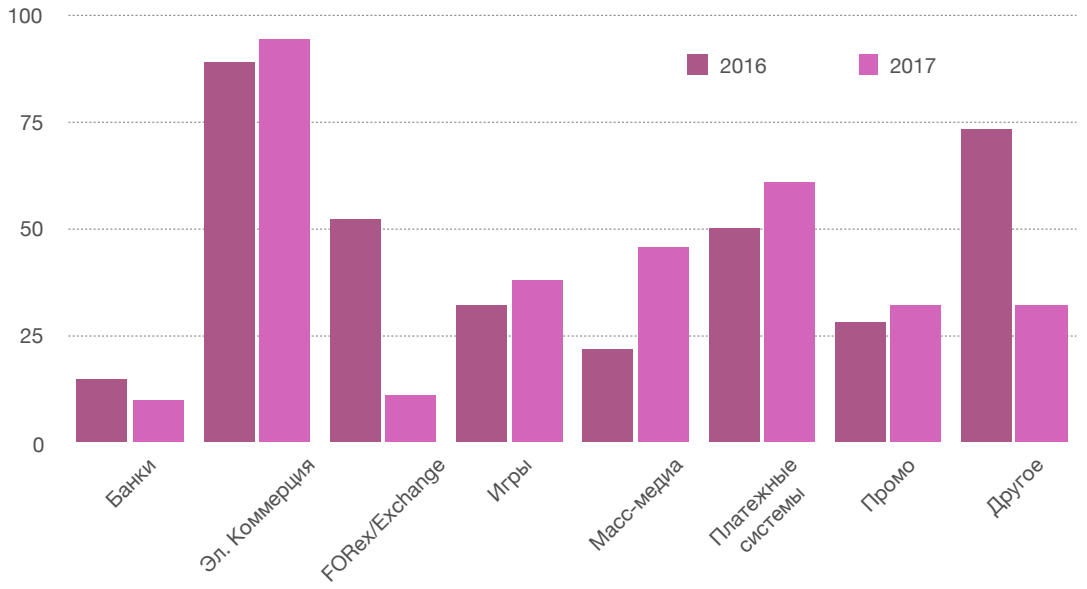
Сейчас 2018 год, и вы просто не можете отказаться от автоматизации и вспомогательных скриптов, не испытав последствий.

Угроза взлома стала в последние годы чрезмерной, часто в отсутствие адекватных технических доказательств и свидетельств произошедшего, просто для поддержания уровня или провокации внимания. По нашему мнению, это привело лишь к заблуждению общественности относительно и осложнению делового климата во всем мире.

Среднее количество атак в определенных потребительских сегментах



Динамика количества атак за 2016–2017 гг



2

Интернет вещей

Ботнеты основываются на нескольких опорных точках. Если такая сеть использует некоторую уязвимость — она умрет, как только уязвимость будет закрыта. Если ботнет существует на уровне троянского приложения, которое распространяется по электронной почте или любым другим способом в виде вредоносного файла, — ничто не ограничивает его существование. Люди, вероятно, никогда не перестанут загружать и открывать вложения из своих электронных почтовых ящиков.

Многие IoT устройства все еще взламываются с использованием тривиальных способов, таких как уязвимости в веб-интерфейсе. Почти все такие уязвимости критичны, но у производителя крайне ограниченные возможности по быстрому созданию патча и доставке его в виде обновления.

Основное различие между 2016 годом и прошлым заключается в том, что злоумышленники переключили собственное внимание со взлома отдельных устройств на атаки на облака и IoT платформы. Интернет вещей предоставляет злоумышленникам доступ к тысячам полностью работоспособных устройств одновременно, часто подобные проникновения остаются незамеченными. Экономическая эффективность — причина, по которой мы ожидаем увеличения частоты подобных атак на целые облака и платформы в 2018 году.

Взломы IoT устройств участились с тех пор, как инструментарий Mirai стал базовым фреймворком для создания ботнета в 2017 году. Однако стали известны и более ранние инкарнации ботнет-фреймворков, откуда Mirai черпал вдохновение для собственного кода, например Hajime.

Исполнение DDoS и других атак — это бизнес. А бизнесу не нужны заголовки New York Times и расследования ФБР. Атаки IoT ботнетов уже показали, на что они способны и нет никакого смысла учить этот урок заново лишь для того, чтобы избежать гласности. Сейчас для преступников наступает время молчаливых попыток получить отдачу от сделанных ранее инвестиций.

Короткое погружение в то, как работает эта экономика, может быть сделано с помощью некоторых слухов 2017 года, в частности, сообщений директора по стратегии безопасности компании Anomali. Криптографическое вымогательство стало главной угрозой 2017 года и вынудило все стороны конфликта, включая правительства, но, как всегда, исключая рядового пользователя, уделять внимание информационной безопасности, осуществляя мониторинг и пуская в ход инструменты и политики раннего обнару-

The conscience that never awakens
DRWEB

Конфликт между людьми, пытающимися контролировать IP-камеры и другие подключенные устройства, привел к фрагментации оригинального ботнета Mirai, в результате чего в 2018 году дюжина небольших ботнетов контролирует меньшие сети скомпрометированных устройств. Критические уязвимости остаются, как и угроза того, что уязвимые устройства вновь объединятся под одной крышей.

жения. Как следствие, мы видим, что среди blackhat специалистов вымогательство за счет шифрования имеет крайне плохую репутацию. Мы уже видели подобное в прошлом на рынке заказного DDoS.

Эволюция интернета вещей происходила быстро в течение всего 2017 года, что не помешало модемам Zyxel быть захваченными одной из разновидностей Mirai с помощью логинов и паролей по умолчанию.

Интернет уже является основным средством коммуникации для всех, как легитимных, так и пытающихся скрыться участников, и ни у одной из сторон нет заинтересованности в уничтожении всей системы.

Глядя на BlueBorne можно с легкостью предсказать появление куда больших по количеству и масштабу задействованных устройств и, конечно, гораздо более опасных ботнетов с точки зрения возможностей.

Мы ожидаем активное появление еще более крупных ботнетов, чем Mirai, способных к flood-атакам даже без использования amplification-протоколов. Их уже можно воспринимать как спящих драконов, существующих, но по каким-то причинам пока не задействованных в бою. Возможно, подобные ботнеты уже используются в настоящее время, однако мы не видим признаков такой активности. Альтернатива лишь одна — отсутствие возможности для 100% утилизации всей мощности такой сети.

Несомненно, взаимодействие между инженерными и сетевыми сообществами, государственными и около учреждениями может предотвратить появление проблем, вызванных как интернетом вещей, так и устаревающими протоколами. Хотя мы все еще не можем назвать яркие примеры успехов в этой области, это по-прежнему задача каждого — защищаться и искать ответы на связанные с этим вопросы.

The Attack Vector «BlueBorne» Exposes Almost Every Connected Device
ARMIS

САМЫЙ БОЛЬШОЙ БОТНЕТ В 2017 ГОДУ

124 000

УСТРОЙСТВ ПОД ЕДИНЫМ УПРАВЛЕНИЕМ

3

Криптомания

Криптовалюты, как и интернет вещей, – настолько горячая тема в настоящее время, что взрыв грязной бомбы в каждой из этих областей становится неизбежным.

Биткойн в 2017 году доказал, что является хорошей реализацией концепции hyperledger — децентрализованной базы транзакций, являясь наиболее известным на данный момент продуктом, основанным на цепочке блоков. Сама же технология все еще ищет свою цель и смысл существования. Каждое ответвление цепи блоков конкретного проекта (то, что случилось в результате Etherium DAO и Bitcoin Cash) является проблемой базы данных с технической точки зрения.

Новый и большой рынок ICO стал настоящим откровением для хакеров в 2017 году. Тенденция нападения в наиболее стрессовый для организации момент (сбор средств, рекламные кампании) сохраняется, и с растущим количеством криптовалютных проектов атаки на взлом комбинируются с DDoS. Если рынок эмитирования криптовалютных токенов продолжит свой рост — данная тенденция лишь усилится.

Рынок ICO на сегодняшний день больше связан с новостями, чем с технологиями. До того как плохие сны стали реальностью для Etherium, его знаменитый основатель г-н Виталий Бутерин, похоже, готовился стать лидером этой индустрии. Однако к началу 2018 года этого так и не случилось. Когда сойдет пена и мы увидим поверхность — тогда и найдутся по-настоящему увлекательные применения для такой технологии, как блокчейн.

Уровни волнения слишком высоки среди представителей проектов проводящих ICO, криптовалютных и других финтех проектов. На этих рынках уже много денег, но что отличает традиционное и неспешное банковское дело от этой новой индустрии — это краткосрочное, высокоскоростное движение от планов к исполнению и конкретным действиям поколения считающих себя опытными молодых людей, стремящихся заработать. Конечно, подобные экосистемы привлекают жуликов всех видов, а криптовалюты страдают в первую очередь от взломов и атак на отказ в обслуживании.

Майнинг-пулы атакуются в последние секунды подписи каждого блока с целью получения вознаграждения за подпись блока конкурирующим пулом. Облачные криптовалютные кошельки постоянно под атакой — в течение 2017 года мы видели крупные взломы таких сервисов с потерей всех криптовалют их создателями. Даже майнинг с помощью скриптов в браузере может быть прибыльным, не говоря о заражении большого количества старых компьютеров, серверов или игровых консолей вредоносным ПО, осуществляющих вычисления за счет жертв.

Эта конкретная, криптовалютная, цепочка блоков — лишь один из видов применения блокчейна, растет. Но до сих пор не ясно какая экономика (спрос/предложение) и мотивация стоит за ней, помимо невероятного потребления электроэнергии. Серьезные игроки смотрят на криптовалюты лишь потому, что они не лицензированы, демонстрируют фантастические процентные колебания как вверх, так и вниз, при этом сопровождаясь хором молодых и активных голосов. **Если это пузырь — он может взорваться, но никто не может**

сказать наверняка, ведь традиционные представления об экономике здесь уже не работают.

ICO представляют особый интерес для всех рыночных сторон. Из-за криптовалют и ICO на наших глазах выросла новая индустрия взломов. В этом рынке уже задействованы огромные объемы средств, а техническая сторона реализации многих проектов откровенно слабая, о чем мы говорили в 2017 году. Они постоянно взламываются.

В 2018 мы увидим последствия всех незавершившихся в 2017 событий, тем более что биткойн, как и многие другие криптовалюты, стал дорогостоящим товаром, получающим все более широкое распространение.

Атаки на вычислительные пулы также очень популярны — они предоставляют злоумышленникам еще один способ манипуляции сетями, генерирующими криптовалюты и большой вычислительной мощностью. Станет еще хуже: никто не знает, когда рост криптовалютных проектов остановится и чем дороже становится каждый из них в отдельности, тем больше попыток взломов будет суммарно.

Некоторые люди опасались, что биткоин сам по себе или вкупе с другими криптовалютами может потерпеть серьезную неудачу из-за некоторой технической ошибки в коде. До сих пор этого не случилось, что хорошо, однако, откладывать такую вероятность в будущем по-прежнему нельзя.

Майнинг криптовалют в браузерах — это то, что мы должны учитывать в будущем, так как сама идея замены рекламы на легитимный майнер одновременно захватывает дух и раздражает. Когда отдельный компьютер попадает в вычислительный пул, игнорировать это невозможно вследствие замедления работы компьютера, а ведь некоторые люди испытывают рекламную слепоту, не раздражаясь из-за баннеров. Опять же, некоторые не любят рекламу и, вполне возможно, что для них майнер на определенном сайте является меньшим из двух зол.

Майнинг криптовалют в браузере с помощью Javascript неэффективен, даже в большей степени, чем на компьютере без выделенного для этой подзадачи GPU. Однако это не имеет значения, так как подобные действия дополнительно увеличивают коэффициент монетизации трафика. Это может иметь место в случае взлома сайтов и последующего внедрения в них вредоносного кода майнера. Уже сейчас некоторые выходные ноды TOR подменяют HTTP, добавляя JS-майнер всем, кто получает доступ к ресурсам с этой точки. Не стоит забывать, что далеко не все блокируют выполнение всех скриптов в браузере.

Сетевые атаки на hyperledger-инфраструктуру (такие как DDoS-атаки по майнинг-пулам в конце вычисления каждого блока) будут расти в количестве пропорционально росту криптовалютных проектов. У каждой сложной технологии есть фундамент. Найдя в нем трещины, можно разрушить дом любого размера.

4 Инфраструктурное наследие

Основные проблемы веб-сервисов остаются такими же, как и на рассвете интернета: либо каналы слишком узкие, не позволяющие данным течь естественным образом, либо приложения плохо спроектированы и разработаны, содержат слишком много ошибок или работают используя методы, не соответствующие общепринятым подходам.

2017 год продемонстрировал, насколько разнообразные виды оборудования могут быть уязвимы к различным типам кибератак. В будущем мы увидим еще больше инцидентов, связанных с устаревшим программным и аппаратным обеспечением.

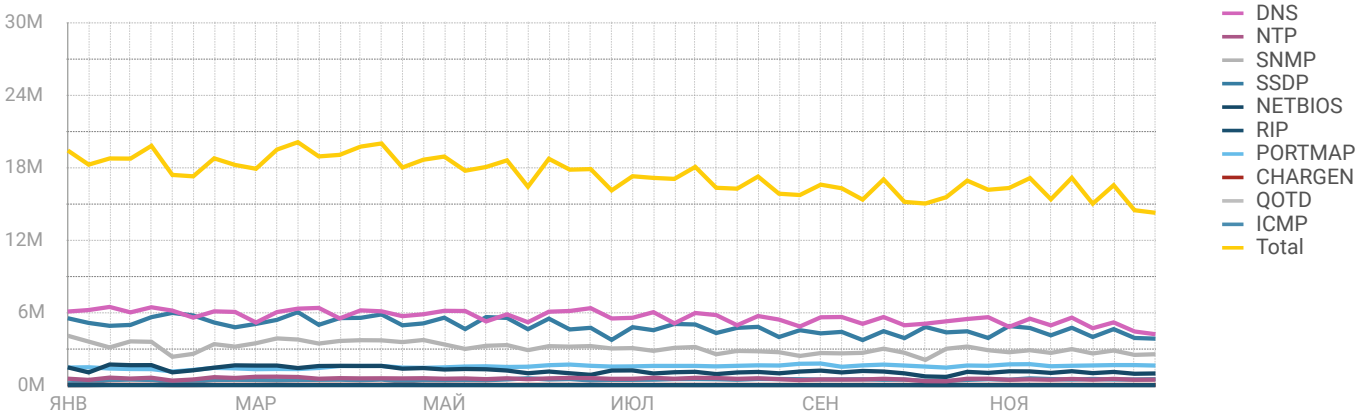
Атаки с использованием смартфонов могут производится как на основе заражения вредоносными приложениями, даже в случае их установки из официальных магазинов, так и с помощью подобных BlueBorne уязвимостей. Браузерные расширения и плагины, сетевые устройства (которые уже достаточно пострадали в течение последних трех лет), любое оборудование на стыках провайдеров — все может быть протестировано на устойчивость к атакам снова и снова и, вероятно, в конечном счете не устоит.

Атакующие прекрасно понимают сложившиеся реалии после стольких лет успешных нападений. Всем остальным также понятно, что практически любой сайт, приложение или канал связи будет иметь те или иные слабые места, доступные для атаки. В то время как атаки по полосе (максимальной пропускной способности подключенных каналов) в настоящее время не представляют собой наиболее вероятную угрозу и в большинстве сценариев могут быть нейтрализованы даже при подключении к сервису защиты находясь под атакой, удары по L7 (прикладному уровню) уже сейчас куда более разрушительны. С ними также на порядок сложнее бороться.

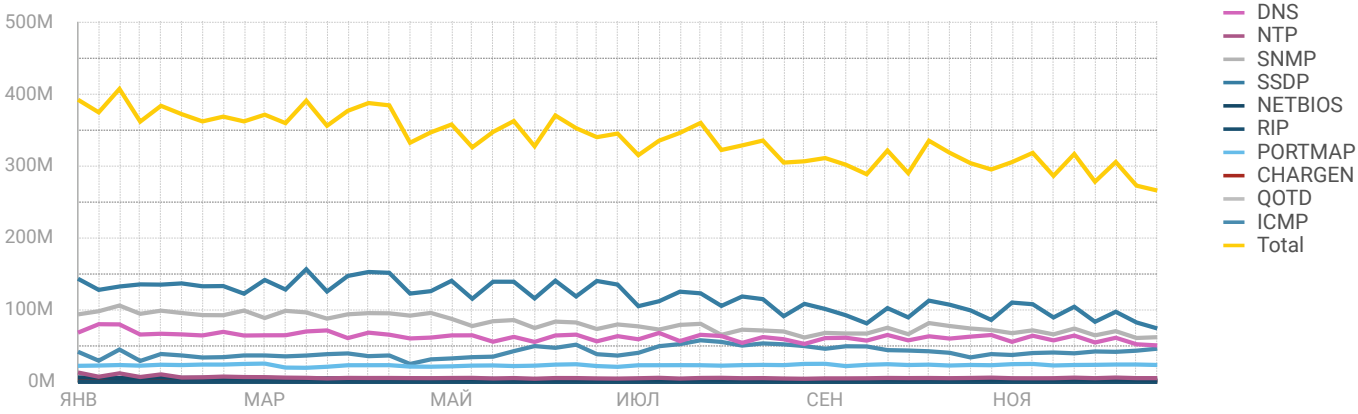
В последнее время мы также наблюдали сценарий, в котором каналы и соединения функционируют нормально, равно как не наблюдается никаких проблем и с дизайном приложения, однако в спецификации одного из используемых протоколов, на который опирается все ваше приложение, находится серьезная проблема безопасности или даже уязвимость нулевого дня. Это проблема и угроза совершенного иного порядка. В наши дни вы не можете заставить всех фронтенд и бэкенд разработчиков читать RFC — подобное замедлило бы темп разработки для большинства компаний, кроме самых крупных, непосредственно участвующих в создании протоколов.

Как правило, люди не склонны подвергать сомнению масштабируемость своих приложений при большой нагрузке. Мы могли бы даже сказать, что в 2017 году технологии воспринимаются большинством разработчиков как «хорошо масштабируемые» именно благодаря облаку, обеспечивающему высокую мощность конечного сервера, выполняющего изменяющийся по требованию объем вычислений. В зависимости от того, кто создал приложение, одна из двух слабых сторон будет превалировать: злоумышленник может попытаться найти либо конкретный запрос, приближающий его к цели, либо может залить все приложение вредоносным трафиком (что особенно актуально для служб и приложений) так,

Количество амплификаторов



Фактор амплификации протоколов



С одной стороны, человеческие факторы всегда были, являются и будут оставаться наиболее уязвимыми точками для любой компании или интернет-сервиса. С другой стороны, человеческий элемент является также и самой сильной защитой, поскольку люди выполняют свою работу, полностью контролируя обстоятельства, в которых находятся. Технологические проблемы сильно связаны между собой, поскольку весь код был написан человеком.

что приложения, и без того обладающие высокой нагрузкой, просто перестанут справляться со своими обычными задачами. В результате, подобные цели все чаще атакуются flood-атаками, поскольку бороться с отдельными нелегитимными запросами гораздо проще, зная нормальное поведение собственных пользователей, получающих доступ к странице или приложению. Другими словами, если есть хоть одна страница, которую можно запросить без какой-либо авторизации — она должна быть полностью закэширована.

События 2017 года ярко выявили критичность человеческого фактора и подчеркнули его важность. Методы найма сотрудников и внутренние политики помогают четче сформулировать, что люди думают о своей работы и ценностях компании. Чем больше выручка отдельно взятого бизнеса, тем лучше он может финансировать собственные операции и тем больше может потратить на покупку решений существующих проблем. Но некоторые вещи нельзя купить: в первую очередь моральный дух сотрудников и их внимание к деталям при выполнении рутинных задач. Это может быть как слабость, так и сила. Архитектура сама по себе может быть масштабной точкой отказа любого приложения, и строят ее люди — вот

почему нормальная коммуникация так важна для эффективной нейтрализации и защиты от атак.

Внутренняя сеть

Утечки маршрутов происходят каждый день. Мы всерьез озабочены повторением проблемы низкой квалификации технических специалистов в сетевой области. Это не должно быть проблемой, однако, по-прежнему является ею. Иногда кажется, что интернет-провайдеры не понимают, что они делают, и Бразилия — прекрасная страна — также иллюстрирует проблему с количеством сетевых инцидентов, которых там происходит больше, чем в любом другом месте.

Постоянное улучшение модели отношений автономных систем позволило нам построить отчетность о происшествиях и инцидентах в 2017 году.

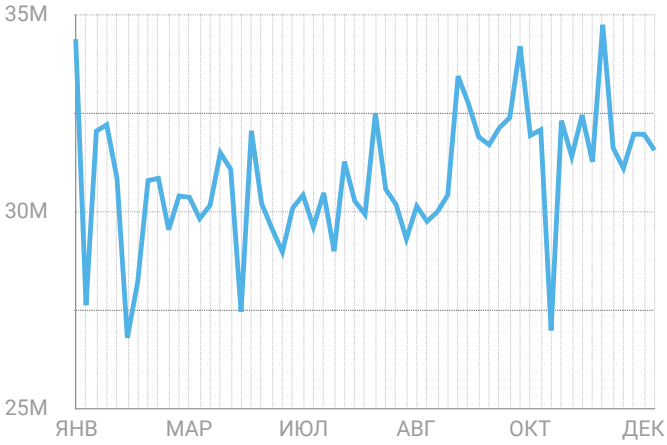
Было пугающе легко создать проблемы всему сетевому сообществу в 2017 году. Все внимание было приковано к инцидентам маршрутизации, а способность успешно перехватывать трафик для будущих или текущих злоупотреблений вновь выводит проблематику безопасности BGP на передний план.

Сетевой инцидент, вызванный Google в Японии был, пожалуй, самым ярким примером того, что может произойти при неправильной настройке BGP большим, тем не менее — единственным поставщиком контента.

Глобальные утечки маршрутов и перехваты адресного пространства снова появились в новостных заголовках, но они и так происходили постоянно, о чем явно говорит статистика перехватов в мобильных и контент сетях, создавая увеличенные сетевые задержки.

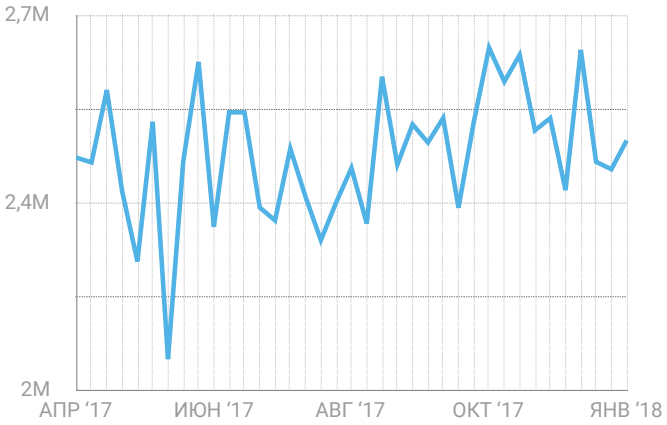
Против MiTM-атак (man-in-the-middle, атака посредника) шифрование более не является панацеей. Уязвимая инфраструктура провоцирует все новые атаки на центры сертификации, количество фальшивых прокси растет,
в популярных операционных системах находятся уязвимости реализации DNS. После всего этого отправка plain text почтовым клиентом Outlook

Статические циклы в 2017 году



Лучше не становится — в среднем постоянно активны 30 миллионов статических циклов. 0,7% адресного пространства IPv4 на ежедневной основе попадает в статические циклы.

Открытые порты BGP



Открытые порты BGP совсем недавно стали уязвимостью. Команда Qrator.Radar считает подобную ситуацию опасной, так как открытые порты BGP оставляют злоумышленнику потенциальную возможность нарушения нормальной работы автономной системы.

Man-in-the-middle attack
WIKIPEDIA

вместе с шифрованным сообщением уже не кажется такой серьезной проблемой.

BGP, DNS и те, кто осуществляет локальную настройку этих протоколов по-прежнему относятся нами к числу наиболее значительных сетевых уязвимостей. Многие испытывают

В случае BGP необходимо быть предельно осторожными, так как потенциальный урон может быть колоссален. Поскольку BGP управляет передачей всего трафика от одной AS к другой, мы говорим не только об увеличенных задержках в доступе к ресурсам для пользователей, но, что более важно, о появлении вероятности MiTM-атаки на шифрованный трафик. Подобные инциденты могут затронуть миллионы пользователей в разных странах.

ложную надежду относительно безопасности того, что построено на этом шатком основании. Но в сеть проникает все большее количество угроз: амплификаторы и фактор амплификации находятся в падении с 2016 года, оставляя возможность сетевым атакам быстро достичь пропускной способности в 1 Тбит/с, так как количество незащищенных сетей все еще велико. Однако поскольку амлификация является давней и хорошо известной, а также легко обнаруживаемой проблемой, их использование становится все менее широким. Старое оборудование, ответственное за атаки с использованием протоколов амплификации в прошлом, к настоящему моменту либо выведено из эксплуатации, либо обновлено.

Сетевые операторы со своими автономными системами должны полностью осознать все, что происходит внутри периметра. Уязвимости все еще могут появляться, но тем не менее должны закрываться. Если природа сетевого инцидента понятна, всегда найдется способ борьбы с ним.

Базовое правило маршрутизации гласит, что more specific (более узкие) префиксы всегда предпочтительны. И при настройке BGP даже небольшая ошибка в IP-адресе может привести к плохим последствиям. Тем не менее, сообщество, занимающееся развитием BGP, все еще сохраняет доверительные рабочие отношения. Но скорость внедрения новых или обновленных технологий, таких как DNSSEC (15% внедрения в 2017 году) и RPKI (7%) низка и мы считаем, что это связано с удовлетворением операторов автономных систем текущими решениями. Недостаточно мотивации для выполнения обновлений из-за рисков несовместимости и увеличения расходов, ведь для обеспечения надлежащего уровня клиентского сервиса необходимы капиталовложения, не всегда приводящие к пропорциональному росту доходов.

Конечно, новые инструменты призваны помочь владельцам AS, но мы не видим, чтобы это происходило. В дополнение к протоколу, испытывающему проблемы, есть программное обеспечение с дополнительным слоем уязвимостей. Внутреннее противоречие хорошо видно на примере продуктов с открытым исходным кодом, где у популярного и свободно распространяемого программного маршрутизатора может быть гораздо больше полезных функций, равно как и уязвимостей и проблем, нежели у устаревшего и разрабатываемого маленькой группой людей проприетарного продукта.

Развитие сети характеризуется вялотекущими процессами внутри таких организаций, как ICANN, IETF и IEEE, а также отсутствием воли сильных корпоративных игроков, таких как Amazon, Microsoft, Google и других, которым пришлось бы взаимодействовать с операторами связи всех

Контент — новый король, а те интернет компании, которые поставляют в основном контент, генерируемый пользователями внутри платформы, такие как Google, Amazon, Facebook и многие другие, начинают строить собственные сети. Ярким примером 2017 года была компания Microsoft, проложившая первый трансатлантический кабель для собственного облака Azure. Во многом это связано с тем, что и до отмены Net Neutrality сети не были бесплатными для использования — кто-то всегда брал деньги за глобальную доставку контента до пользователя. Сетевое сообщество хорошо помнит пиринговые войны, которые имеют сильное сходство с сегодняшним ограничением свободного течения трафика и эксклюзивным доступом к основным контент-провайдерам или сетям. Существует четкий усиливающийся тренд в желании обладать собственными сетями среди контент-провайдеров, и уже сегодня многие Tier-1 операторы остаются не у дел.

размеров для внедрения требуемых улучшений. Вместо этого мы видим отмену закона о Net Neutrality в Соединенных Штатах и углубляющуюся изоляцию каждого из сетевых игроков.

Мы все еще живем в мире открытой сети, но чем дальше, тем больше это воспринимается как роскошь, а не как должное. В 2017 году тот факт, что любая организация все еще может получить статус LIR и овладеть автономной системой, становясь тем самым оператором связи, заслуживает отдельных слов благодарности.

В 2017 году мы по прежнему видели IPv6 провайдеров связи в отсутствие глобальной связности просто потому, что всем «без разницы». С технической точки зрения ни одна автономная система не обязана общаться и обмениваться трафиком с другими автономными системами. Пример такого токсичного поведения может вновь вернуться в мир IPv4, особенно учитывая все, что связано с текущим обсуждением отмены сетевого нейтралитета в стране, где сконцентрированы основные сетевые ресурсы с многомиллионными пользовательскими аудиториями.

Кто контролирует трафик?

MiTM, или атака посредника — это пример перехвата трафика между клиентом и сервером. Данная практика хорошо известна с самых ранних дней существования корреспонденции и сообщения, когда переписка могла быть перехвачена для получения секретов во время войн, переговоров или коммерческой конкуренции. За это время многое изменилось… но только не цели организации подобных атак. В настоящее время перехват трафика происходит в первую очередь тогда, когда кто-то преследует такие цели, как кража учетных данных или слежка.

Большинству кажется, что перехват трафика — это удаленная физическая операция, происходящая где-то на глубине колодца, на уровне расщепления оптоволоконных кабелей. Хотя подобный сценарий и возможен, это далеко не самая частая практика. Откровения, раскрытые Эдвардом Сноуденом, подняли интерес к вопросам конфиденциальности и безопасности переписки и хранения данных, не только с точки зрения государственного надзора и контроля населения. Распространение Let's Encrypt с его бесплатными

Атаки (без атак перебора) по типам

SQL-инъекции	21%
Удаленное выполнение команд	36%
XSS	38%
Обход каталога	2%
Другие	3%

Атаки перебора

Брутфорс и перебор учетных записей	97%
Перебор ресурсов	2,5%

Распределение атак на типам

Распределение приводится по количеству вредоносных запросов. Чтобы данные были более показательны, они разделены на две категории: атаки на уязвимости приложений (SQL инъекции, XSS и т.д.) и атаки перебора, на которые приходится большая часть вредоносных запросов.

Что на самом деле представляет из себя протокол HTTPS? «S» означает «security» или «безопасность», обозначающую аутентификацию и шифрование. Аутентификация означает, что центр сертификации подтвердил личность и легитимность владельцев данного веб-сайта.

SSL сертификатами — лишь один из примеров реакции рынка на данную конкретную тенденцию. Без общественного интереса мы бы не увидели уровня принятия протокола HTTPS на уровне 62,1% от общего количества ресурсов в интернете, согласно статистике SSL Labs за 2017 год.

В 2017 году мы видели сразу несколько уязвимостей, делающих атаку посредника возможной. В их числе:

— Атака переустановки ключей WPA2

— Уязвимость DNS клиента Windows, позволяющая подделывать запросы и компрометировать выполнение кода
— Outlook 2016, отправляющий текстовые сообщения вместе с их зашифрованным эквивалентом

HTTPS уязвим для атак посредника. Многие люди склонны думать, что HTTPS из-за наличия аутентификации и шифрования неуязвим для любых атак, если центр сертификации работает корректно, включая невозможность перехвата трафика посреди HTTPS-сессии.

Но часто эти же люди забывают о том, что MiTM-атаки на центр сертификации могут производиться так, что злоумышленник свяжется с центром сертификации вместо легитимного владельца сайта, на другом конце поддерживая обычную HTTP-сессию с жертвой. Атакующий заставляет центр сертификации думать, что он и является владельцем сайта, к которому жертва пытается получить доступ. Таким образом, именно он подписывает сертификат, позволяющий ему и далее заниматься своими грязными делами с жертвой.

Утечка маршрута представляет собой наиболее распространенное последствие ситуации, когда злоумышленники обнаруживают уязвимость, вызванную человеческой ошибкой, и это может значительно повлиять на доступность веб-ресурсов для большого количества пользователей. Так как почти любой маршрут может быть анонсирован любой автономной системой, то количество таких инцидентов в 2017 году зашкаливало, так как число автономных систем уже больше 60000. «Более точные» маршруты приводят к ситуации, когда маршрутизаторы выбирают потенциально вредоносные пути, где, в конце концов, данные могут быть в лучшем случае удалены.

Как перехватывается трафик на больших масштабах?

DNS и BGP представляют собой два основных протокола управления потоками трафика. Никогда не следует забывать о том, что интернет был создан на основе модели доверия, часто нарушаемой сегодня.

Спуфинг DNS (или отравление кэша DNS) — это метод, основной задачей которого является перенаправление пользователей на скомпрометированный веб-сайт вместо реального путем подделки (отравления) IP-адреса за доменным именем, хранящего в кэше DNS-сервера, к которому обращается пользователь (резолвер).

BGP, в свою очередь, является стандартным протоколом междоменной маршрутизации и он очень проблематичен. Так как в BGP буквально все основано на доверии, любая автономная система может быть введена в заблуждение с двумя последствиями: перехватом трафика или утечкой маршрута.

Мы надеемся, что BGPSec, получивший наконец статус RFC в 2017 году будет принят индустрией намного быстрее, чем DNSSec, интегрированный лишь в 15% интернет-ресурсов с 2005 года.

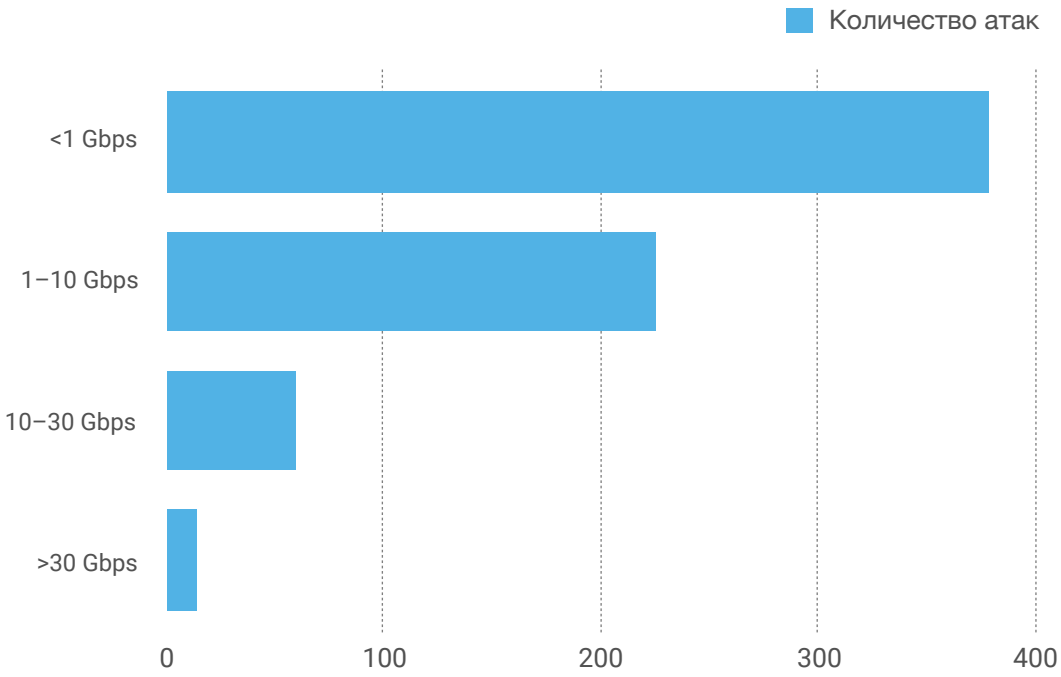
В настоящее время каждый двадцатый префикс испытывает проблемы ежедневно. Инцидент Google-Verizon в Японии произошел лишь в результате неправильной конфигурации оборудования и привел к ужасным последствиям в виде отсутствия доступа к основной массе популярных ресурсов для японских интернет-пользователей.

Увеличение сетевых задержек — это «лучшее» возможное последствие как перехвата трафика, так и утечки маршрута, с полным выходом из строя автономной системы как «наихудший» результат.

3 масштабных инцидента маршрутизации, произошедших в 2017 году и рассказанных командой Qrator.Radar:
1. Что происходит, когда банк

When Bank Plays in IP-transit Games
QRATOR LABS. RADAR

Количество атак по используемой полосе



решает сыграть в оператора связи? Недоступность для всех вовлеченных сторон.

2. Каждый день в мире появляются новые провайдеры интернет-услуг, но время от времени в дикой природе появляется один, рожденный перехватывать трафик.
3. В конце августа 2017 года разразился колоссальный инцидент маршрутизации. Его последствия были настолько серьезны, что Министерство внутренних дел и Министерство связи Японии начали расследование причин, вызвавших настолько масштабный отказ работы сетей. То, что произошло накануне, было утечкой префиксов партнеров Google в сторону провайдера Verizon, где он был распространен уже глобально на операторов всех размеров.Поскольку Google анонсировал сразу множество более специфичных маршрутов, которые не видны в глобальной таблице маршрутизации BGP, некоторые сети вполне могли испытать значительное увеличение сетевых задержек или даже потери пакетов данных. Например, серьезное воздействие инцидента почувствовала AS4713 (NTT OCN) — крупнейший поставщик электронных услуг в Японии. Этот конкретный пример показал, насколько серьезными и масштабными могут быть последствия инцидентов, связанных с утечкой маршрутов и перехватом трафика.

Born to Hijack
QRATOR LABS. RADAR

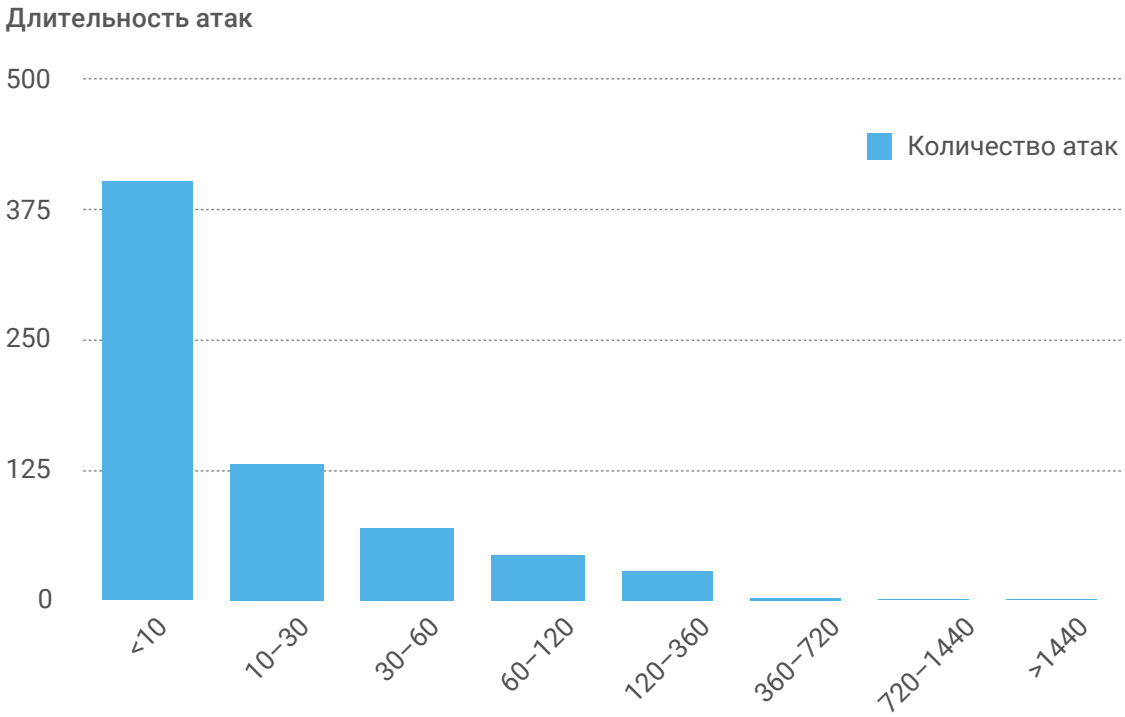
Когда программное обеспечение становится критической инфраструктурой Масштабирование DNS

Еще до эпохи глобальной сети система доменных имен была представлена файлом хоста, содержащим перевод доменного имени в адрес сервера. В конце 2017 года DNS выполняет различные формы балансировки нагрузки (round-robin, geolocation-based и другие), являясь, помимо всего прочего, основой функционирования глобального интернета с необходимостью поддержки корневых серверов имен, которыми управляет ICANN.

Как DNS подсистема должна управляться?

Существует два наиболее распространенных варианта:

1. Ее можно купить в виде облачного сервиса
2. Ее можно построить и управлять ею на основе внутреннего ресурса компании.



Существует сразу несколько причин, по которым лучше не заниматься внутренней разработкой системы управления DNS.

Прежде всего, не существует стандартного и масштабируемого решения, которое было бы принято всей индустрией для управления подсистемой DNS. Управление системой доменных имен выросло в отдельную рыночную нишу, где разными компаниями были выделены значительные ресурсы для разработки коммерческих решений и инструментов.

В 2017 году Qrator Labs провела внутреннее тестирование различных сервисов с открытым исходным кодом, помогающим в управлении подсистемой DNS, и результаты были разочаровывающими. Поскольку запросы и ответы DNS редки и не объемны, мы всерьез не ожидаем высокой нагрузки на DNS. По этой причине DNS-серверы никогда не строились как нагруженные решения. Но еще в конце 2016 года это стало уязвимостью, как показали атаки Mirai на DNS-провайдера Dyn с использованием flood-атаки (DNS water torture). И хотя скорость ответа от сервера DNS на конкретный запрос определяет скорость загрузки страницы для конечного пользователя, общая неэффективность DNS — истина, с которой мы существуем уже десятилетия.

Еще одна проблема DNS кроется в том, что геолокационные базы, содержащие, казалось бы, точные данные о местоположении и, как ожидается, призванные помогать в построении надежной подсистемы управления DNS, фактически делают обратное. Информация присутствующая в таких базах данных, как MaxMind, не является на 100% верной. В 2017 году мы провели отдельное исследование, основанное на инструментарии RIPE Atlas и обнаружили, что частота ошибок MaxMind достигает 4,6% — и это лучший результат. Почти 5% пользователей были перенаправлены системой DNS «куда-то еще» на основе некорректных данных о местоположении.

В 2018 году DNS представляет собой высоко динамичную систему, что само по себе является некоторой проблемой. Система управления конфигурацией DNS на основе API является жизненно важной необходимостью, позволяющей обеспечить быструю проверку конфигурации, управление политиками и обзор статистики работы всей системы.

С теми TTL, что присутствуют в мире DNS-подсистем, проблема переноса конкретного ресурса с одной подсистемы на другую, обеспечивающую его нормальную работу, приобретает

актуальность. Так как чем ниже выставленный TTL, тем выше загрузка на всю подсистему, и, как уже упоминалось ранее, DNS не предназначен для обработки большого количества запросов под нагрузкой. И последнее, но не по важности: полный комплект инфраструктурных решений, частью которого является DNS , имеет решающее значение для поддержания стабильной работы интернет-бизнеса любого рода.

Существует множество крупных поставщиков облачных DNS-решений и, будучи одним из таких поставщиков, Qrator Labs рекомендует всем, кто пытается получить больше контроля над подсистемой доменных имен, принять на вооружение стандартную тактику диверсификации. С помощью SRTT (Smooth Round Trip Time) можно легко иметь двух или трех независимых поставщиков услуги DNS, что само по себе обеспечивает как должный уровень резервирования, но, помимо этого, также улучшает задержки для конечного пользователя, пытающегося получить доступ к вашим сетевым ресурсам.

Прикладной уровень

API становятся все более важными для крупных клиентов — они профессиональны и хотят иметь максимум контроля над процессами очистки и фильтрации трафика.

Наиболее заметным фактом в этой области являются даже не сами атаки, а тот прогресс, который сделали все поставщики решений безопасности в процессе обучения, коммуникации и сотрудничества, а не только конкуренции, с целью нахождения ответов на наиболее серьезные вопросы современности, как, например, противодействие ботнетам. Когда появляются подобные масштабные угрозы, ставящие под вопрос существование уже не отдельных веб-сервисов, но всей индустрии как таковой, происходит объединение компаний сразу на нескольких уровнях: формальном, неформальном, B2G и B2C. Мы уже видели успехи, связанные с такой кооперацией, по противодействию крупным ботнетам в 2017 году среди крупнейших компаний, работающих в области информационной безопасности.

Атаки прикладного уровня крайне опасны, как и раньше. Если ваше предприятие подключено выделенным L2 каналом к поставщику связи, то

В 2017 году мы явно осознали, насколько критическая ответственность прячется в API цифрового продукта. В настоящее время большинству потребителей электронного сервиса требуется рабочий и полностью функциональный API, и этот факт невозможно недооценивать. API является жизненно важной частью сети фильтрации Qrator, однако разные разработчики и инженеры рассматривают API сквозь разные призмы, выдвигая различные требования. Отключение API или выведение его из строя может быть равноценно полному отсутствию доступа к сервису. Поскольку интеграция клиентов в сервис фильтрации трафика требует больших усилий и эта система работает в реальном времени, с синхронизацией сразу в нескольких точках, в случае чрезвычайной ситуации ее настройка значительно осложняется.

это лишь вопрос времени, когда против вас будет использована уязвимость в отдельно взятом незащищенном оборудовании или сторонней услуге, используемой для поддержания работоспособности. Коммерческие DDoS-атаки значительно усложнились в 2017 году: тут обойти, там взломать, в конечном итоге — найти способ нанести ущерб. 2017 год также продемонстрировал, что ботнеты основанные на зараженных Windows-машинах, никуда не делись. Эффекты и последствия от эпидемий шифровальщиков, таких как WannaCry, Petya и NotPetya, могут быть воссозданы в форме DDoS-атаки, когда незаметное пользователю ПО будет командовать генерацией трафика с каждой отдельной зараженной машиной в рамках сколько-нибудь масштабной сети. По нашим наблюдениям, ботнеты растут в размерах — недалека точка, в которой вредоносное ПО нового поколения наберет достаточный масштаб для атак на крупные соединенные куски интернета и отдельных сетей крупных провайдеров.

Высокоскоростные атаки на базе Windows-ботнетов превратили прошлогоднюю шутку про атаки в 1 Тбит/сек. на прикладной уровень в печальную реальность, видимую все чаще. Не за горами тот день, когда сотни Гбит/сек, бьющие по тому же L7 (прикладной уровень), войдут в нашу

Цензурирование или, как мы это называем, «блокада» иностранных интернет-ресурсов на определенных территориях будет повторяться все в большем количестве стран по всему миру. История человечества демонстрирует, что интеграция и сотрудничество, как правило, более выгодно использовать в качестве элементов развития международных отношений. Комплексное решение выигрывает от многообразия создающих его участников.

повседневную жизнь. Скорее всего, это произойдет в 2018 году, ведь уже сейчас все, что может быть сломано с помощью такой атаки, отключается гораздо быстрее, чем атака достигает предельных уровней канальной емкости.

Подключенные устройства уже давно концентрируются в IoT платформы — данный процесс, как мы ожидаем, ускорится в 2018 году ради облегчения управления устройствами, их коллективного контроля и обновления. Подобные устройства не станут более защищенными, будучи объединены под одной крышей — скорее наоборот, вместо сбора миллионов устройств по отдельности, в случае успешного взлома злоумышленник получит доступ сразу к миллионам полнофункциональных и уже скомпрометированных устройств.

Существует серьезная вероятность того, что сквозное шифрование будет принято 100% интернет игроков, проектов, ресурсов, услуг. Это и позитивно, и негативно, так как уже сегодня мы видим серьезные попытки различных правительств получить «ключи шифрования» в борьбе за контроль над коммуникацией граждан.

Следующей проблемой, которая нас серьезно беспокоит, является протекающий в настоящий момент политический конфликт за «всемирный сетевой контроль», и этот конфликт не утихает — наоборот. Слишком многие страны хотят свой «суверенный, чистый и бесплатный» интернет. Чего они никак не ожидают, так это необходимости нести полную тяжесть расходов, связанных с разработкой новых протоколов, обеспечением совместимости. Это сложно, дорого и непонятно, зачем кому-то ломать то, что работает в попытках получить то, что обречено на поломку.

Появились большие данные и машинное обучение в форме нейронных сетей, с помощью которых мы получаем много новых и полезных методов для своей работы. Однако все еще многое необходимо сделать, поскольку текущие нейросетевые приложения и алгоритмы, обрабатывающие большие объемы неструктурированных данных, в основном используются в развлекательной и рекламной деятельности. Нам же необходимо строить надежную сеть и искать возможности применения новых технологий для решения задач с большим количеством переменных и потоков данных в режиме реального времени, таких как управление и фильтрация трафика. И здесь мы сами изобретаем подходы и технологии.

Квантовые вычисления также представляют собой определенный интерес в 2018 году и развиваются очень динамично. О них также часто говорят в ключе «конец криптографии», но на наш взгляд пока — это лишь догадки и досужие разговоры.

Сетевое обновление

BGPSec уже стал стандартом, и это хорошая новость для всей отрасли. Пишите и звоните своим поставщикам, интернет-провайдерам, родственникам и убедите их в том, что они должны изучить спецификации данного протокола чем раньше, тем лучше.

Будучи ведущими участниками проекта по разработке спецификации ролей BGP в IETF,

Не только HTTP, но и DNS может быть зашифрован уже в ближайшее время.

- A **Шифрование (DNS over TLS)**
- B **DNSSEC**
- C **В 2018 году мы ожидаем увидеть примеры локальной реализации обновленных протоколов DNS**

Вероятно, дополнительно понадобится 5 лет на то, чтобы очистить «кладбище», которое DNS оставил за собой в течение собственного жизненного цикла.

Qrator Labs планирует интегрироваться с BGPSec с целью обеспечения полной защиты от манипуляций с метриками и утечек маршрутов. Мы ждали BGPSec в течение пяти лет и, несмотря на то что он по-прежнему нуждается в некоторых модификациях, его наличие жизненно важно для всех пользователей BGP.

BGP и DNS останутся ключевыми и фундаментальными технологиями для интернет-архитектуры в ближайшем будущем. DNSSEC также приближается к адаптации индустрией, поскольку в текущей реализации системы доменных имен существует огромное множество проблем стабильности и безопасности, нашедших все подтверждения еще в 2016 году. DNS не является на 100% надежной системой — ответы DNS-сервера могут быть подделаны, сами серверы могут находится в руках неизвестных людей и правительств, поэтому интернет, построенный на DNS как камне основания, не может считаться и рассматриваться пространством свободы, в том числе свободы слова.

Постоянная технологическая модернизация и обновление является единственным способом улучшения ситуации для поддержания общего благосостояния и нормальной работоспособности глобальной сети.

Мы рады видеть, что Atlas RIPE, наконец, нашел свое применение в реальной жизни. Платформы обмена трафиком (internet exchange — биржа трафика) начинают пристально наблюдать за сетевыми параметрами, будучи наконец заинтересованными в том, что происходит за пределами их собственных сетей. В первую очередь мы обязаны изменению данной ситуации новостным заголовкам, рассказывающим про сетевые инциденты.

Модели и моделирование интернета является очень горячей темой. Недавно мы увидели некоторые поглощения (BGPmon, Dyn), указывающие в первую очередь на потенциально внутреннее использование таких инструментов в рамках построения крупных сетей. Те, кто управляют большими BGP Anycast сетями, вероятно, уже имеют (если не имели до 2017 года) свои собственные модели, архитектурные инструменты, позволяющие анализировать сети. Google, Microsoft, Amazon — все эти компании при своем масштабе просто обязаны иметь инструменты моделирования для адекватного прогнозирования поведения сети в режиме реального времени либо максимально к нему приближенно.

Однако мы не видим большого числа новых игроков на рынке мониторинга BGP. Radar на сегодняшний день анализирует данные самого большого количества BGP-сессий, получаемых от более чем 400 источников по всему миру.

Нет никакой альтернативы мониторингу в случае, когда вы хотите знать, что происходит с анонсируемым адресным пространством и что может повлиять на него. Чем быстрее мы реагируем на инцидент, тем слабее он распространяется, что означает меньшее количество перенаправленного трафика на поврежденный, или скомпрометированный, ресурс или сеть. Конечно, интеграция систем мониторинга с системами автоматизации — текущая тенденция. Благодаря коммодитизации услуг хостинга и доступа в сеть все больше людей понятия не имеет, как сетевые протоколы могут повлиять на то, что они контролируют (или думают, что контролируют).

Сетевой рынок состоит из трех крупных групп: поставщиков аппаратного, программного обеспечения и их клиентов. Такие производители, как Mellanox, отлично справляются с поддержкой активно развивающегося Switchdev. Ограничение вендором (vendor-lock) было грехом сетевой индустрии, и мы надеемся, что с приходом универсального программного обеспечения, такого как Switchdev, производители оборудования поддержат его совместимость с собственным железом. Благодаря 100-гигабитным интерфейсам скорость и количество данных значительно возрастут, а задержки и издержки, наоборот, снизятся.

Другие протоколы

Отдельные лица и компании в основном разрабатывают новые инструменты и протоколы для собственного, внутреннего, использования. В IETF существует множество рабочих групп, которые практически не взаимодействуют между

собой. Поэтому усилия по разработке, созданию и внедрению нового интернета, в широком смысле, фрагментированы. Новый транспорт — QUIC, в основном решает проблемы Google. Facebook открыла свою платформу маршрутизации и строит проприетарное оборудование, как например DWDM и платы маршрутизаторов. Некоторые компании вознаграждают собственных инженеров за каждый документ, принятый инженерной организацией, что также далеко не всегда хорошо, особенно когда начинается гонка за количеством таких документов. IETF — это организация, в которую приходят интернет-провайдеры, поставщики ПО и оборудования решать проблемы, работающие на благо всего сетевого сообщества, но это не значит, что там можно расслабляться. Мы уже увидели, что бывает, когда уязвимость закрадывается в спецификации протокола еще на уровне его проектирования — подобное никогда не должно повториться. IETF как организация также меняется со временем, сменив поставщиков на инженеров в качестве основных участников сообщества, привлекая все больше людей с разными взглядами к работе на одну цель.

Старые протоколы, на которые мы полагаемся, исключительно масштабируемы, но почти не защищены. Это то, что мы и называем наследием, которое, вероятно, никуда не денется в ближайшее десятилетие. Люди всегда хотят быстрого удовлетворения, поэтому шанс принятия определенных вещей, работающих на общее благо даже в случае частичной интеграции, все же сохраняется. Нереально ожидать, что 100% сетей одновременно примут обновление до одной версии в случае каждого отдельно взятого протокола, продукта или сервиса.

Как невыполненное обещание может доставить множество проблем тому, кто его дал, так и сложные современные технологии разрабатываются поверх других технологий в отсутствие глубокого понимания всех зависимостей и макро картины происходящего. «Извините» здесь не поможет избежать проблем и последствий.

Черновик BGP-стандарта и IETF

Мы надеемся, что уже в 2018 году наш черновик по ролям в BGP получит статус RFC. Команда Qrator.Radar инвестирует значительные усилия и ресурсы в создание расширения BGP, подходящего всей индустрии поставщиков связи.

Сеть Google также представляет собой SDN (software defined network), использующей BGP для внутреннего взаимодействия всех ее частей. Другие компании строят уникальные комбинации услуг с использованием уже давно известных протоколов. Смотря на три года в будущее, мы ожидаем, что два черных ящика смогут сообщаться через некоторую надежную транспортную IP-систему, но мы не знаем, что будет внутри самих ящиков. Существуют и другие интересные разработки: LPWAN — захватывающий пример технологии, не полагающейся на V4 адресацию. Давайте также не забывать о том, что MPLS является транспортно-агностическим. OpenFlow увеличивает свое присутствие на рынке. HTTP/2, за пределами всех возможных противоречий, быстро внедряется или, по меньшей мере, так часто говорят. Мы желаем, чтобы тенденция закрытия экосистем внутрь самих себя прекратилась. То, что точно не вызывает никаких сомнений, так это положительные новости для всех в виде стандарта BGPSec.

5

Инфраструктурное наследие и интранет

2017 стал настоящим годом взломов. От эпидемий шифровальщиков до открытий архивов Vault7 и Shadow Brokers, в дополнение к заметным утечкам вследствие человеческих ошибок, где Uber и Equifax представляют собой два наиболее громких примера.

Это производит впечатление уличной банды, получившей контроль над арсеналом самой передовой армии мира. Мы всерьез предполагаем, что эпидемии шифровальщиков служили лишь прикрытием, и небольшое количество уплаченных в качестве откупа биткойнов является тому доказательством. Скорее всего, мы видели первые побеги нового класса эксплойтов, но для того, чтобы узнать наверняка, требуется время.

Интернет становится все более распределенным каналом доставки «заразы». Как и в толпе, где каждый болен опасной и заразной болезнью, присоединиться — значит подвергнуть себя риску.

В 2017 году было много атак, со временем они становятся все опаснее. В правильной комбинации, с миллионами предварительно просканированных IP-адресов и доменных имен при выпуске каждого эксплойта возникает волна взломов. В случае open-source решений это происходит постоянно, особенно учитывая, что логи обновлений публично доступны. Как только важные патчи готовы, преступникам требуется всего несколько дней для подготовки эксплойтов и начала атак. При этом совсем необязательно, что именно большое количество приложений будет под ударом — существует 3 миллиарда Wordpress страниц, и только 100 000 могут быть задействованы. Но даже это число значительно, и ущерб будет заметен. IPv6 способствует распространению атак с бесконечными прокси и огромной вычислительной мощностью сети. Все происходит так быстро, что большинство средств защиты просто не может опережать плохих парней.

Множество ошибок при настройке доступа к резервным копиям и базам данных — вот что приводит к утечкам данных. Bruteforce (грубая сила) атаки также растут, поскольку пользователи, устанавливающие тривиальные пароли, не уменьшаются в количестве.

Эпидемии шифровальщиков — текущая тенденция, но важно понимать, что одни и те же уязвимости могут быть использованы как для взломов, так и для DDoS-атак. Последнее будет означать войну на прикладном уровне во всем интернете.

Никто не обновляется, хотя новые неприятные истории громогласно звучат почти каждый день. Вредоносное ПО, шифрующее все данные в бизнес-сетях, на домашних компьютерах, в больницах и правительственных учреждениях, может прервать работу тысяч людей.

Конечно, антивирусные программы общепринятые, но, как ни странно, они не предотвращают подобные эпидемии. Более умелые компании пытаются контролировать все внутри своего сетевого периметра, но, оказывается, что у них нет возможности достичь своей цели.

Эсплойты ShadowBrokers сработали как вакцина для всех устаревших устройств, подключенных к интернету. Мы должны заботиться о старых ПК, так как многие из них до сих пор работают в

Несмотря на сильную мотивацию в отношении безопасности, инвестиции в обучение и продвинутые продукты и все другие меры, направленные на улучшений общей осведомленности, фактический уровень безопасности в любой компании сводится к конкретному человеку и степени, в которой все уроки были выучены в прошлом. Именно человеческий фактор является основной причиной возникновения инцидентов, которые мы наблюдали в 2017 году.

самых удивительных местах, где от них зависят люди. Что еще более важно — они очень уязвимы. Vault7 сделал то же самое и, надеемся, в будущем подобные утечки будут оканчиваться так же хорошо.

Уязвимости в приложениях всегда были вызваны ошибками при планировании архитектуры и логики их работы, оркестрации или администрирования.

Компании, разрабатывающие современные браузеры, прилагают большие усилия для того, чтобы информировать общественность о незащищенных страницах, блокируют всплывающие окна, не дают осуществить автоматическую загрузку файла — все то, что долгие годы служило эпицентром распространения эпидемий. Значительный объем трафика в интернете зашифрован HTTPS, и теперь люди, стараниями все тех же разработчиков, обращают внимание на отсутствие сертификата благодаря предупреждениям.

Уязвимости

Все уязвимо. Так что разговор стоит вести не о том, «что наиболее уязвимо», но «где уязвимость может быть найдена раньше». Там, где есть уязвимости, существуют и атаки. Более того, есть ряд широко распространенных технологий, воспроизводящих уязвимости — когда исправляется одно, а ломается другое. Злоумышленники пристально следят за подобной деятельностью — они знают, что чем более крупный перед ними поставщик, тем больше времени ему понадобится для разработки и доставки обновления до своих потребителей.

Облако также переходит в статус наследия со всеми проблемами, которые унаследованы новыми поколениями устройств и технологий. Утечки Uber и

Распределение по уязвимостям

Межсайтовый скриптинг	50,24%
Раскрытие данных	40,82%
SQL-инъекции	2,78%
Межсайтовая подделка запроса	2,12%
Удаленное выполнение кода	1,62%
Небезопасное перенаправление	1,23%
Обход каталога	0,66%
XXE (XML eXternal Entity)	0,41%
CRLF-инъекции	0,12%

Оценка уязвимостей

Распределение по найденным уязвимостей приложений мало чем отличается от привычной картины год от года. Уязвимости межсайтового скриптинга традиционно занимают первое место. Раскрытие конфиденциальных данных (ошибочно GIT-репозитории с открытым доступом, базы данных без авторизации и т.д.) занимают второе место. Разные типы инъекции (прежде всего SQL-инъекции) занимают третье место.

Использование устаревших версий ПО

В 2017 году у 78% пользователей WAF были обнаружены уязвимости, связанные с устаревшими версиями ПО. Среднее время устранения таких уязвимостей составило 15 дней.

Так как уязвимо все устаревшее (не обновляющееся) оборудование — совершенно неясно, что с этим можно сделать. Это проблема, потому что подобное железо не способно к поддержке новых протоколов, не говоря о том, что в какой-то момент поддержка многих работающих устройств просто останавливается. Это беспорядок, которым пользуются злоумышленники.

Lessons Learned from the Equifax Disaster
WALLARM

93 ДНЯ

СРЕДНЕЕ ВРЕМЯ, НЕОБХОДИМОЕ ДЛЯ УСТРАНЕНИЯ УЯЗВИМОСТИ

OneLogin начались с того, что ключи от хранилища Amazon были опубликованы на GitHub или в другом месте — возможно, что на стикере, прилепленном к монитору.

Другой серьезной проблемой является ситуация с MongoDB, Cassandra, Memcache и другими популярными базами данных. Когда их администраторы забывают установить соответствующий уровень безопасности, атакующим не представляет труда найти лазейки.

В случае Uber, утечка ключа от контейнера была, вероятно, наиболее серьезным инцидентом из аналогичного ряда. Petya и WannaCry показали, насколько пористы границы интернета, а вредоносные программы, появляющиеся в одной стране, быстро находят пути в другую.

Следует также отметить, что некоторые уязвимые части браузеров, наконец, отключаются у пользователей по умолчанию: технология Flash — наиболее известный пример. Это касается и разработчиков — мы видели множество таких изменений в PHP и MySQL. Это помогает, поскольку часто разработчикам не хватает времени для правильного управления настройками. Если другие создатели ПО поддержат эту полезную практику, то в результате многие приложения станут гораздо безопаснее.

Одновременно продолжают появляться эксплойты Apache Struts, в 2017 году вышел уже четвертый. Так как Struts достаточно популярен, он получает много лишнего внимания. То, что случилось с Equifax, пожалуй, лучше всего иллюстрирует возможные последствия, ведь именно этот Java-фреймворк оказался повинен.

Платформы, такие как фреймворк Struts, упомянутый выше, или Rails, входят в фокус исследований сразу нескольких заинтересованных сторон. Так как на этих технологиях основывается большое количество приложений, всегда выгоднее сфокусироваться именно на широком спектре возможностей. Когда выполняется вредоносный код, целые рынки и индустрии могут быть выведены из строя на часы или даже дни. Для защиты клиентов от известных и еще не обнаруженных уязвимостей в различных фреймворках Wallarm использует виртуальные патчи и наблюдение за периметром приложения в реальном времени.

6

Обход систем защиты

Обход систем защиты и безопасности уже стал новым трендом среди атакующих. Вопрос заключается в том, как свести к минимуму вероятность подобного события, когда дорогостоящая система внезапно становится неэффективной. Это может касаться таких систем, как WAF, нейтрализация DDoS, IDS и DPI. Почти все сложные технологии сегодня можно обойти. Только глубокая интеграция систем защиты в цифровой бизнес, как броня, плотно сидящая на воине, может защитить от атак.

Не продавать услугу при потенциально плохой интеграции может быть хорошей идеей в некоторых случаях, ведь пропущенная атака может повредить более, чем одному клиенту и заказчику. Она в первую очередь заставляет узнавших о ней задаваться вопросом о работоспособности самой технологии.

Публичный инструментарий, доступный для обхода таких популярных решений, как Cloudflare и Incapsula, проверяет их эффективность и способность компании тесно общаться с клиентом, поскольку устранение подобных угроз является, прежде всего, вопросом сотрудничества. Использование PDNS/SSL-cert-scan на решениях диктует необходимость подключения L2 MPLS соединения для корпоративных клиентов.

Обход систем защиты в целом, а также доступные в уголках интернета интерфейсы по обходу различных систем являются еще одной угрозой для отрасли.

Атаки 2017 года были быстрыми, безжалостными. Злоумышленники предварительно сканировали и анализировали системы, а затем выжидали верный момент — и лишь тогда били со всей силы. Как уже было написано, ничто, кроме общения между поставщиком защитного решения и его потребителем, не поможет избежать подобного сценария.

Случаются и хорошие вещи, однако, как всегда, позитивные изменения в интернете происходят медленно и с трудом.

Мы уже упоминали, насколько нападающие умны и настойчивы — у них также в распоряжении богатый арсенал. Они изучают историю DNS, просматривают RIPE DB, пути к цели, наблюдая за жертвой в реальном времени. Времена, когда решение по защите от чего угодно могло быть куплено и включено в строй в начале атаки,

Что вообще происходит? Раньше мы точно знали, где «наша сеть», ориентируясь на точные контуры периметра сети. В 2017 году все претерпело значительные изменения, быстро распространяется и уменьшается в размерах. Во многих компаниях почти невозможно одновременно учесть все ресурсы, действия, подключения и зависимости в сети и на отдельных устройствах. Более того, возможное отключение крупной интернет-компании, такой как Amazon или Google, может запустить цепную реакцию для гораздо большего количества важных интернет-сервисов. В эпоху интеграции это реальный и значительный риск — стоит лучше учитывать сложность собственной инфраструктуры.

при этом выполнив свою функцию, бесследно прошли. В настоящее время худший сценарий, который происходит все чаще, — это переезд цифрового бизнеса из одного дата-центра в совершенно другой из-за невозможности защититься.

Возможность обхода систем защиты — то, о чем должна знать каждая компания, поскольку многие аппаратные решения и программные средства можно легко обойти.

Внешний IP-адрес или порт, о котором вы «забыли», или периферийное оборудование, о работе которого вы имеете достаточно смутное представление, — вот лишь пара причин, по которым вы можете потерять множество времени и нервов.

7

Предсказания сбылись

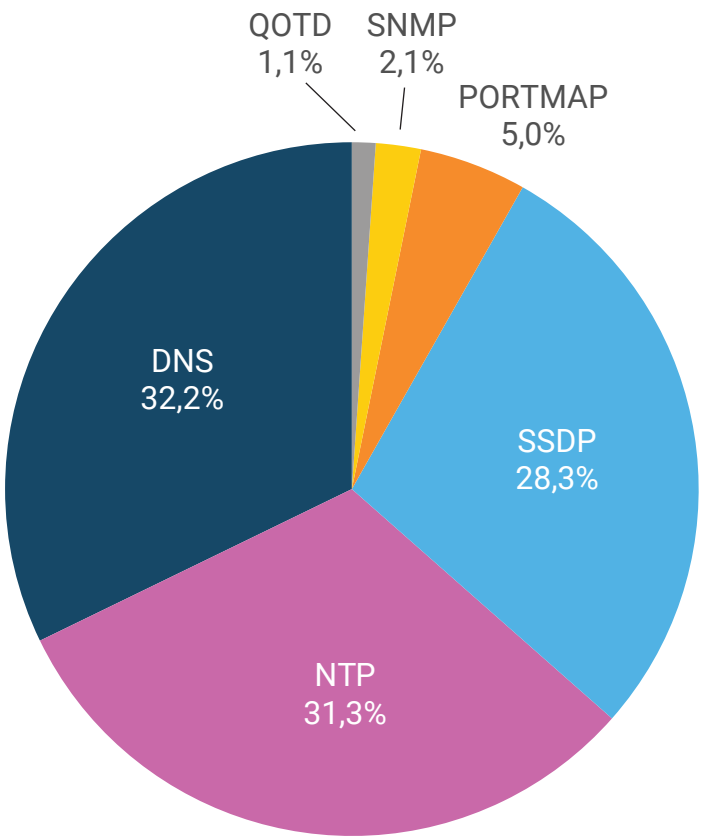
Отношение по модели «у меня все хорошо» остается распространенным во многим частях мира информационных технологий. Это иллюзия, с которой мы продолжаем бороться, но эта битва не окончится никогда.

Повышение уровня информированности всего вовлеченного в интернет сообщества, пожалуй, лучший способ для всех справиться с тем, что мы видели в 2017 году. Qrator.Radar выполняет эту почетную миссию, не только предоставляя инструмент мониторинга автономной системы в реальном времени, но и являясь активным участником IETF, всячески способствуя принятию черновика по ролям BGP в статусе протокола (RFC). Помимо этого, мы стараемся следить за популярными маршрутизационными движками — Quagga и Bird, вкладываясь в исходный код данных решений в случае необходимости улучшений. В 2018 году мы сделаем Radar более визуальным, добавив возможности автоматизации.

Ложные срабатывания возникают, когда клиент сообщает об атаке или недоступности ресурса, но после некоторого расследования становится ясно, что никакой атаки не было — сервер испытывал проблемы по другой причине. Подобные инциденты случаются постоянно.

Численность растет: сетей, автономных систем, интернет-провайдеров. В то время как интернет-компании входят на сетевой рынок, все масштабируется, ведь все больше игроков хотят контролировать трафик. Конечно, в будущем это грозит большим количеством инцидентов, поскольку никаких иных предпосылок нет. Мониторинг — единственный возможный способ предотвращения сетевых аномалий.

Распределение атак по протоколам



Удивительным образом, нагрузочное тестирование может также стать проблемой, так как система нейтрализации DDoS-атак, как и WAF и любой другой сетевой экран, представляет собой разумную систему, от которой требуется научиться нормальному поведению пользователя, как и поведению атаки, чтобы отделить одно от другого. Нагрузочные тесты, как правило, умнее — их исполнители ищут наиболее уязвимое место для

	Average amount of IPs within 1 attack	Single attack average requests amount	Single attack average duration (minutes)
SQL-инъекции	26	60	37
Удаленное выполнение кода	26	2	25
Межсайтовый скриптинг	26	3	19
XXE (XML eXternal Entity)	20	8	46
NoSQL-инъекции	12	5	14
Обход каталога	26	3	10
Атаки перебора	11	93	110
Перебор ресурсов	25	164	327

Детальная статистика по атакам по сегменту электронной коммерции

Чтобы проиллюстрировать типичный срез атак и дать более детальные характеристики, был выбран срез электронной коммерции. В этом сегменте атакующие традиционно активны, и системой Валарм отслеживаются как атаки на эксплуатацию разных типов уязвимостей, так и атаки перебора (в основном перебор учетных записей со взломанных ресурсов)

демонстрации возможности пройти решение по защите. Когда мы знаем о готовящемся тестировании, это позволяет следить за происходящим и реагировать в случае необходимости, но нагрузочное тестирование без объявления — это атака, которая будет отфильтрована, что понимают не все технические специалисты.

Еще один пример — это автоматическое тестирование, широко распространившееся к текущему моменту. Чтобы эффективно выполнять подобные тесты, их источники, как правило, заносятся в белый список на стороне решения по безопасности. Однако иногда тесты могут помешать доступности сервисов, а включение в белый список означает, что с данного IP отправляется любое количество запросов, и мы ничего не можем с этим поделать. В течение 2017 года мы имели дело сразу с несколькими атаками из источников в белых списках потребителей.

По-сравнению с феноменальным 2016 годом с точки зрения DDoS-атак, ушедший 2017 был спокойным, без атак огромного масштаба. За этим изменением стоят сразу несколько факторов, в том числе:

— Концентрированная мощь ботнетов, которые питают камеры, DVR-приставки и роутеры, спрятанные за NAT'ом, была захвачена, разделена и снова захвачена несколько раз. Со временем количество устройств утекало из рук их новых операторов, как песок. Конкуренция за эту власть среди желающих ею обладать, попробовать новый код и посмотреть, что произойдет, привела нас к частым, но слабым атакам. Это не означает, что в один день не может появится новый суперботнет, уничтожающий любые цели.
— IPv6 распространяется все шире, означая меньшее количество устройств, скрытых с помощью NAT. Но поскольку среди конечных пользователей подобных устройств не существует адек-

ватных мер безопасности, включая сетевые, мы ожидаем увидеть еще больше зараженных устройств: телевизоры, смартфоны, все, что подключается к интернету.

— Судебное преследование создателей Mirai показало нам драматический образ молодых людей, который поступили противозаконно, а началось все с игровых серверов. Любой интернет-сервис, приносящий минимум дохода, может привлечь любопытных людей, которые легко влезают в проблемы и легко манимы неправильным путем. Это главная причина всех атак Mirai — доказать чью-то неправоту, и вот почему это были атаки по пропускной полосе. Профессиональный рынок DDoS предпочитает атаки прикладного уровня — они, как правило, куда более эффективны с точки зрения стоимости и временных затрат.

Старые уязвимости тоже исправляются — не стоит обесценивать данный факт. В 2016 мы видели множество атак на Wordpress, но в 2017 Pingback более не является проблемой вследствие уменьшения количества уязвимых установок.

Более того, похоже что 2017 год принес с собой логическую эволюцию угроз в интернете и за его пределами. Без примечательных DDoS-атак мы видели значительные эпидемии зараженного ПО. В течение года их было несколько, плюс утечки данных, затрагивающие, как в случае Equifax, целые страны. Само понятие «конфиденциальности» должно быть переопределено, чтобы включить факт постоянного взлома все увеличивающегося количества подключенных устройств, в итоге используемых в качестве прокси, коллекторов и шпионов. Это уже не антиутопическая фантазия.

Компании, занимающиеся нейтрализацией DDoS, порой могут принести вреда больше, чем пользы, разрушая сложившиеся связи между группами пользователей во имя безопасности и прибыли. Чем больше расстояние между пользователем и сервером — тем хуже. Политика и политики приводят к ухудшению доступности определенных ресурсов у пользователей, и их список растет. В совокупности это ведет нас к изолированному интернету, который уже не может называться таковым словом, ведь «internet» значит «interconnected networks» — объединённые сети. Сегрегированная, разъединенная сеть, с разным уровнем доступа для всех — не лучший ориентир.

Прозрачность сети должна быть священна. Под этим инженеры, как правило, понимают равную обработку сетевых пакетов без какой либо приоритезации. К сожалению, управление трафиком — это реальность, едва ли делающая современный интернет более прозрачным.

Мы также разочарованы практиками, несовместимыми с предсказуемостью и прозрачностью. Если определенные виды трафика, такие как видео или голос, получают приоритет в определенных сетях, то это должно происходить согласно понятному описанию протокола (RFC), что часто бывает иначе.

Вдобавок интернет-провайдеры, продающие услуги по подключению новых клиентов, имеют множество разнообразного оборудования на периферии сетей: DPI, межсетевые экраны и прочее. Такое оборудование может внедрять рекламу, фильтровать и анализировать трафик, внедрять вредоносный код. Поскольку интернет-провайдеры стремятся к увеличению добавленной стоимости, вряд ли данная ситуация изменится в обозримом будущем.

Сети принадлежат главным образом коммерческим структурам и, как ни странно, мы продолжаем верить что они должны обслуживать всех одинаково. В реальной жизни провайдер всегда отдаст предпочтение более маржинальному потребителю.

Черный рынок

Конечные пользователи всегда страдают сильнее всех и, вероятно, это не прекратится. В 2017 году стало известно, что самой популярной ОС в мире является Minix — свободно распространяемое ПО, установленное на -3 уровне платы Intel для управления всеми системными ресурсами. Взлом, активированный и распространяемый через сетевой уровень глобальной сети может нанести

Множество личностей и организаций: разведка, правоохранительные органы, индивидуальные преступники, порой просто любопытные дети — все вкладывают собственные усилия. Серый рынок уже сформирован с помощью эксплойтов, ботнетов, продажи уязвимостей нулевого дня и другими «нишами». В 2017 году мы увидели архивы кибероружия и эпидемии невиданной силы.

непоправимые последствия. Уязвимости есть везде, в том числе в упомянутой ОС, так что перед нами джинн в бутылке — и пробки уже нет.

Экономика вредоносного ПО не нова, но продолжает увеличиваться. Она следует своим собственным законам. Совсем недавно RAND Corporation выпустила важный отчет об уязвимостях нулевого дня, сообщающий, что это рынок объемом меньше оборонного, и он сокращается. Это тем не менее не означает, что теневая экономика умрет — она адаптируется путем поиска новых источников дохода. Люди, зарабатывающие этим на жизнь, определенно не поменяют работу — лишь переключат внимание.

Дальнейшее развитие коммерческих DDoS-сервисов — стрессеров (stresser, booter) — все больше приближает злоумышленников к рядовым пользователями. Такие ресурсы предоставляют удобные интерфейсы и низкую цену. Часто тестовые атаки вообще бесплатны — потребителю показывают товар лицом.

Доминирование CDN

Дело не в концепции CDN (content delivery network) — суть успеха этой модели в интернет потреблении и конечном подключении потребителя. Если мы посмотрим на цены и прибыль операторов CDN и сравним их с теми же параметрами интернет-провайдеров, то станет ясно, что цены снижаются гораздо быстрее, чем растет подключение пользователей к глобальной сети, в любой стране мира. Уже сейчас в интернете более 4 миллиардов пользователей, а в большинстве развитых и развивающихся стран не наблюдается недостатка в возможностях подключения. Люди оказались в изоляции именно там, где отсутствует классическая инфраструктура: дороги, кабели. Предоставление им связи с внешним миром — ближайший вызов, и уже начинают появляться компании, предлагающие хорошие решения в этой области.

Zero Days, Thousands of Nights
RAND

В настоящее время контент, как и транзитные модели, претерпевает значительные изменения. Более того, в конце 2017 года мы можем представить себе ситуацию, в которой интернет-провайдер будет платить пользователям за транзит их данных. На самом деле операторы CDN очень похожи на интернет-провайдеров, так что появление «сетей доставки» вполне возможно в будущем. Тем более в том случае, если контент-провайдеры (крупнейшие сервисы и сети, накапливающие пользовательские данные) начнут продавать услуги доступа в интернет.

8

Предсказания на 2018

Когда мы делали прогноз на 2017 год около года назад, то предполагали, что индустрия будет поддерживать набранный импульс, особенно в отношении DDoS-атак. В прошлом году интернет взорвался другими вещами: блокчейном, криптошифровальщиками, утечками и т.д.

Громкие инциденты воспринимаются как угроза, заслуживающая внимания. Утечка данных Uber, Equifax, эпидемии WannaCry и NotPetya — все это произошло в 2017 году и привлекло внимание к самой концепции информационной безопасности.

Процессы информационной безопасности плохо совместимы с существующими тенденциями гибкости, непрерывности и ориентации на микросервисы. Безопасность по-прежнему воспринимается, как работа периферийных устройств и сервисов, а не отношение к разработке продукта.

Развиваются системы защиты — в настоящее время безопасность основана на воспринимаемых угрозах, а потому существуют межсетевые экраны, защита от DDoS, системы предотвращения утечки данных (DLP). Одновременно с этим развивается и угроза. Рынок уязвимостей нулевого дня умирает, потому что осталось мало исследователей, брокеров и компаний, готовых платить за подобные «продукты». Серые хакеры работают на программы bug bounty (охота на баги/уязвимости), а исследователи — напрямую с компаниями. Атаки на взлом все еще часто сочетаются с DDoS-атаками, так как именно в этом случае легче получить то, что хотел, когда жертва вернется в сознание, а все оборудование заработает. Это же касается и уязвимостей нулевого дня — одна может и не нанести вреда, но комбинация двух или четырех, скорее всего, будет способна это сделать. Если злоумышленники имеют хоть какое-то представление о внутренних процессах внутри целей, они найдут подходящую комбинацию инструментов, которые окажутся наиболее эффективными.

Относительно новая, но уже стойкая тенденция — это использование искусственного интеллекта (ИИ). Однако, в некоторых случаях за использованием модного термина скрывается неспособность базовых продуктов выполнять основные задачи. ИИ-методики могут помочь в решении многих задач, как, например, обнаружение аномалий, что реализовано в Wallarm, или помощь в автоматизации. В любом случае пока ИИ не может принимать решения. DLP, где в основе лежит некоторый искусственный интеллект, просто не работает. В SOC (security operations center — центр управлению безопасностью) ИИ еще может быть применим, но только после хорошей подготовки и под наблюдением. Намного эффективнее ИИ работает уже сегодня в области атак и их автоматизации, что легко может стать проблемой.

Все вышеперечисленное является ответом на увеличивающуюся технологическую сложность. Сегодня растущему бизнесу сложно быть одновременно рациональным и экономным. Поэтому так важна автоматизация — лучше часто выполнять задачу в отлаженном автоматическом режиме, чем вручную углубляться в настройку элементов управления дорогого оборудования либо сложного ПО.

9

Эпилог

Мы уже видели, насколько быстро мир в прошлом году перешел из одного состояния в другой. Электронные письма, с помощью которых злоумышленники вымогают криптовалюту угрозами организации DDoS-атак, могут посеять панику среди сотрудников. Паническое состояние не способствует ни долгосрочному планированию, ни активной защите ресурса в настоящем времени. Угрозы следует рассматривать издалека, выискивая время для ознакомления и предварительной подготовки.

Основной целью создания решения по нейтрализации DDoS является в конечном итоге установление защиты, чья поддержка дешевле организации атак. Только отобрав экономическое преимущество у злоумышленников, можно начать бороться на одних условиях. И это сложная задача, в первую очередь по двум факторам:

- **A Безрассудный подход к основам информационной безопасности и анализу угроз**
- **B Страх новостей и публичности, попытки скрыть информацию в случае проблем**

У каждой услуги есть компоненты, ответственные за успех. Мы выбрали несколько историй для того, чтобы проиллюстрировать весь спектр задач, которые должна решить современная IT-компания для того, чтобы доставить свой продукт или услугу.

Железо и ПО 2017 года

Нам очень нравится ситуация, в которой мы находимся в настоящий момент. Рынок предоставляет широкий выбор специализированного оборудования, такого как процессоры для свитчей, коммутаторов. Еще в 2016 году подобный выбор был бы ограничен двумя производителями: Mellanox и Broadcom. Нам требовалось больше альтернатив, и в 2017 году конкуренция между производителями чипов в коммутаторах 100G-400G разогрелась до рабочей температуры. Помимо упомянутых компаний, появились Cavium, Barefoot, Innovium, и в целом чувствуется динамика данного рынка. В 2017 году мы уже получаем отличное оборудование по достаточно скромной цене — это в первую очередь результат конкуренции.

AMD представила новое процессорное ядро в 2017 году, но мы пока не тестировали его. В целом процессоры Intel кажутся нам более эффективными, но мы рады любой конкуренции на рынке центральных процессоров — в долгосрочной перспективе они толкают цены вниз. Серверные процессоры семейства Skylake отсутствовали долгое время, но Intel представила и их. Многоядерный процессор с шестью каналами памяти и значительно расширенными кэшами L2 и L3 — это существенное улучшение. NVRAM — пример еще одной стремительно развивающейся технологии, за которой мы пристально наблюдаем, ведь хранилище, работающее на скорости памяти, может быть очень полезно в ряде задач.

XDP
PROTOTYPE KERNEL

eXpress Data Path (XDP) марширует сквозь сетевое сообщество Linux, позволяя управлять трафиком и обработкой пакетов на низшем и наиболее эффективном уровне. В 2017 мы увидели поддержку XDP многими производителями как оборудования, так и ПО. Это хорошие новости. XDP дает увеличенную производительность на том же самом железе, оптимизированном под ваши нужды.

Switchdev представляет собой еще одно отличное решение — операционную систему для сетевых коммутаторов. Производители оборудования наконец начали поддерживать его в 2017 году, и мы ожидаем взрывного развития в этой области.

Эти разработки означают лишь одно — то что мы можем отвязать собственные продукты и сервисы от проприетарных операционных систем. Эта возможность в сочетании с более мощными центральными процессорами позволяет нашим компаниям строить эффективную защиту при низких эксплуатационных расходах.

100 гигабитные интерфейсы — отличная новость для Qrator Labs. В 2018 году мы планируем использовать такое соединение в большем количестве наших точек присутствия. В наши дни успевать за всеми вновь появляющимися опциями улучшения производительности — непростая задача. Но повсеместный, десятикратный рост скорости подключения к сетевым интерфейсам — это то, чего инженеры нашей компании с нетерпением ждут.

В 2017 году утверждение, что интернет-провайдеры могут быстро внедрить и предоставить клиентам 100 Гбит/с интерфейсы, оказалось правдивым. Qrator Labs обновляет подключение до новых интерфейсов там, где это возможно, не только по причине финансовой целесообразности, но и ради получения контроля над всей входящей полосой. Ранее нам приходилось полагаться на то, как конкретные операторы распределяют трафик между каналами 10 Гбит/с. Теперь в большинстве случаев мы контролируем весь поток трафика целиком, что куда лучше подходит для задач нейтрализации DDoS.

Атаки становятся все более сложными и своевременными. Хуже того, даже с самыми надежными сервисами нельзя до конца быть уверенным в их способности нейтрализовать все нападения. Статистика отдельных клиентов наших компаний демонстрирует порой чрезвычайно устойчивые и долговременные намерения по выведению из строя ресурсов компаний, на которые нацелились злоумышленники.

switchdev.txt
GITHUB

Что нам на самом деле нужно — так это новый транспортный протокол, полностью поддерживающий мобильные сети и все устройства. Если протокол содержит какой-то криптоидентификатор объекта, с которым мы взаимодействуем. Приложение ли это, смартфон или пользователь — неважно. Если он принят, становится возможной фильтрация на основе cookie на транспортном уровне. Мобильная сеть является болью для традиционного набора протоколов TCP-IP, так как при смене базовой станции нарушается связь между уровнем приложения и всеми нижележащими.

Клиентоориентированность

Часто значительным препятствием для нашей компании является то, что мы вынуждены проверять и перепроверять каждого потенциального потребителя. На рынке нейтрализации DDoS, где репутация компании является основой большинства продаж, в наших интересах — удостовериться в том, что в защите будущего клиента нет технологических отверстий. Подробные руководства по подключению, рекомендации безопасности, и списки «как сделать» не работают в компаниях с десятками инженеров, одновременно пытающихся общаться с представителями компании, предоставляющий им сервис или оборудования для защиты. Мы достигли той точки, когда всего один неверный шаг может открыть настоящий проход для злоумышленников, делая бессмысленным само наличие такого сервиса. Поэтому вместо обновления инструкций, хотя они и есть, мы пересмотрели собственные внутренние процедуры в попытке улучшить методы и практики, которые мы используем для мониторинга нужд и потребностей наших клиентов.

Интеграция с клиентом, поддерживающим собственную распределенную сеть, всегда сложна. Чем сложнее инфраструктура — тем больше времени и усилий потребуется для тщательного планирования всех шагов по необходимой интеграции и тестированию. Проблемы возникают тогда, когда требуются быстрые изменения в схемах подключения таких больших систем — в рамках SLA незапланированные изменения невозможны.

КАК ИЗМЕРИТЬ ЭФФЕКТИВНОСТЬ NOC?

15 МИНУТ

СРЕДНЕЕ ВРЕМЯ РЕАКЦИИ НА ЗАЯВКУ

Может показаться удивительным, но достаточно часто мы получаем от наших клиентов просьбы, выполнение которых легко откроет двери атакующим и подвергнет угрозе DDoS-атаки или взлома. Запросы потребителей охватывают весь комплекс сложности современных компьютерных систем, и какие-то могут быть решены мгновенно, в то время как другие требуют времени для реализации. Мы всегда говорим, что вы не должны смущаться, обращаясь к нам, более того — часто мы не рекомендуем предпринимать действия, в последствиях которых вы не уверены, до получения технической помощи от наших инженеров. Нахождение под интенсивной атакой, а порой и просто настройка сложного оборудования может быть напряженной, а ошибки ведут к серьезным последствиям. Не нужно стрелять себе в ногу, пытаясь бежать как можно быстрее.

Каждый владелец бизнеса, технический или директор по безопасности должен понимать и помнить, что спешка не помогает нейтрализации и борьбе с атаками, на самом деле наоборот. Более того, в случае DDoS с обработкой HTTPS-трафика можно оказаться в крайне непростой ситуации.

Маленькие компании, естественно, чаще действуют в подобной саморазрушительной манере — там нет голоса, кричащего «Что вы делаете?!» и чаще совершаются действия, ставящие весь бизнес на грань выживания. В случае защиты этот риск действительно не оправдан.

Таким образом, на наш взгляд проверка клиента перед продажей ему сложного продукта или услуги является необходимой частью повседневной работы. Поскольку решение по нейтрализации DDoS, как и Web Application Firewall, являются сложными и глубоко интегрированными в архитектуру защищаемого сервиса, потребитель не всегда понимает, что происходит между им и нами, как все работает на нашей стороне и работает ли вообще. До атаки нет возможности почувствовать, что вы под защитой — а ведь она стоит денег. Поэтому часто возникает желание «проверить» — именно это может вызвать ужасные последствия как для самого клиента, так, иногда, и для нас. Важно, чтобы потребитель хорошо понимал, зачем он приобретает подобный сервис и как он будет работать.

Документация при этом остается неотъемлемой частью сложной системы. Отсутствие надлежащей документации — причина, создающая множество проблем как для потребителей, так и для самих производителей. Документация также должна быть понятной и, в идеале, слегка интересной — иначе ее вряд ли прочитают даже в случае поиска какой-то конкретной информации, там упомянутой.

Чеклист по проверке инфраструктуры

DDoS-атака всегда стремится вывести цель из рабочего состояния, делая его недоступным в первую очередь за счет исчерпания ограниченного ресурса на стороне той или иной сетевой сущности, которая не обязательно является фактической целью злоумышленников

— Последние апдейты и все обновления безопасности для каждого установленного аппаратного и программного обеспечения
— Виртуальные машины и контейнеры (работают, резервно скопированы, настроены на перезагрузку при ошибке)
— Нагрузочное тестирование фронтенда (ответ HTTP 200 на GET / запрос, а не что-то еще)
— DNS
— BGP
— Каналы / аплинки (параметры подключения в операторам связи или транзитным операторам)
— Базы данных: правильные политики доступа и настройки безопасности
— Установленное и используемое аппаратное и программное обеспечение (NAT, трекинг соединения, сетевые экраны, IDS/IPS, WAF, CDN)

Любой конечный ресурс может быть исчерпан, независимо от того, это деньги, время или люди. Все подобные атаки на истощение можно считать DDoS-атакой, а для их успешного отражения необходимо знать, какие ресурсы есть в вашем распоряжении и как они могут быть дополнительно зарезервированы и защищены. В мире бизнеса первым чувствуется именно финансовый убыток, поэтому нельзя исключать из рассмотрения риск ущерба от нападений на деловых партнеров, поставщиков и так далее — всех, с кем так или иначе взаимодействует ваша система.

Глобальная инфраструктура интернета — это оборудование, которое решает, где и как в конечном счете обработать пакет трафика.

Кейс **Lazada**

Когда мы выбрали Qrator Labs в качестве поставщика решения по нейтрализации DDoS, мы уже использовали решение по защите от атак. Однако наш предыдущий поставщик не всегда мог предоставить необходимый нам уровень защиты из-за того, что время реакции на атаки было слишком длительным, а уровень распознавания атаки былнеудовлетворительным, порождая слишком много ложных срабатываний. Общение со службой технической поддержки было медленным и неэффективным, так как мы не могли получить исчерпывающего ответа на все вопросы.

Мы поняли, что ситуацию необходимо менять и начали поиск решения, которое бы полностью удовлетворяло нашим требованиям. К тому моменту мы уже слышали о компании Qrator Labs и ее основателе Александре Лямине, поэтому решили рассмотреть в том числе и это решение среди прочих. После первоначальных тестов и анализа рынка стало ясно, что предложение Qrator Labs имеет лучшее соотношение цена/качество.

Lazada является самой быстрорастущей площадкой электронной коммерции в Юго-Восточной Азии и должна быть всегда доступна как для покупателей, так и для продавцов. «Доступность» означает не только то, что на сайт можно зайти, но и то, насколько быстро и беспрепятственно можно это сделать. Пути эскалации во время атак и других инцидентов являются критически важными; иногда просто необходимо иметь возможность позвонить техническому директору… однако мы ни разу этого не сделали.

Основываясь на 16 месяцах эксплуатации решения по нейтрализации DDoS компании Qrator Labs, мы можем утверждать, что техническая экспертиза службы поддержки — то, что дифференцирует данную компанию от всех остальных поставщиков схожих услуг на рынке. Комбинация столь высокого уровня сервиса, скорости решения технических вопросов, проблем и запросов от наших специалистов делает решение Qrator Labs, так же как и команду технической поддержки и сетевых операций компании, лучшими в сфере информационной безопасности. Так как к атакам и другим инцидентам практически невозможно подготовиться, крайне важно, чтобы при их возникновении коммуникация оставалась четкой, быстрой и профессиональной, удовлетворяя всем требованиям клиента. Мы не говорим о качестве работы сети фильтрации Qrator и способности нейтрализовать DDoS-атаки, так как высочайший уровень эффективности — это тот базис, с которого компания нашего размера и технической экспертизы начинает рассмотрение стороннего решения. Мы не можем позволить себе использовать сервис, принцип работы которого не понятен нам до конца, не говоря уже о любых сомнениях в его стабильности.

В среднем мы испытываем атаки средней степени опасности каждую неделю или две. Раз в два-три месяца мы фиксируем целенаправленные попытки вывести нашу систему из строя с помощью сложной DDoS-атаки. И раз или два в год происходят по-настоящему экстремальные события, имеющие своей целью выведение из строя уже не отдельно взятого сайта, но всей нашей сети и автономной системы. На подобные события мы должны реагировать молниеносно и агрессивно, нейтрализуя такие нападения совместно со специалистами Qrator Labs. Рано или поздно восприятие атак переходит в рутинную область, и мы узнаем об инциденте, только читая отчет, приходящий на следующее утро.

Решение Qrator Labs, согласно нашим замерам, также немного снизило задержки внутри нашей сети, благодаря грамотной архитектуре решения Qrator и глубокой интеграции. При том что у Lazada не так много возможностей подобного улучшения, выигрыш в несколько миллисекунд представляет собой положительное достижение.

После года совместной работы с Qrator Labs мы решили также защитить собственный DNS. У нас были некоторые, очень специфические, запросы к защите нашей системы доменных имен, и мы направили их в Qrator Labs. Через несколько недель запрошенные нами инструменты и опции управления были добавлены в решение Qrator. Иногда сложно просить компанию реализовывать какие-то решения, необходимые именно вам, но когда это происходит и вы получаете желаемое - ощущения фантастические.

Работа с такой компанией, как Qrator Labs, представляет собой замечательную возможность учиться и улучшать собственный продукт в высокопрофессиональной среде.

Кейс **SDVentures**

SOCIAL DISCOVERY VENTURES

Сравнение было выполнено компанией SDVentures в конце 2017 года со следующей методологией:

> Используя инструментарий websitepulse, из 3-х локаций в Китае проводилось по 5 замеров, 1 лучший и 1 худший из них отбрасывались, после чего брался средний результат оставшихся 3-х измерений.*

Таблица ниже иллюстрирует результат, полученный компанией SDVentures в конце тестирования в виде времени загрузки указанных страниц, в секундах.

Вся суть данного бизнес-кейса заключается в количественном подходе при тестировании продуктов и сервисов, а также при сравнении различных сервисов в ключе специфических требований к их работе, а также реальных условий. Методология может улучшаться постоянно, к ней можно бесконечно задавать вопросы. Однако, так как данное тестирование не было проведено компанией Qrator Labs, мы сочли возможным продемонстрировать данный результат в годовом отчете за 2017 год.

Подобные тесты демонстрируют корректный и практичный подход к получению исходных данных в форме индикаторов эффективности, приближенных к специфике бизнеса. Такая активность в тестировании облачных сервисов показывает высокий уровень технического профессионализма и осведомленности в компании, проводящей тесты. Не верить маркетинговым материалам и проводить собственные исследования — абсолютно нормально и даже хорошо, как мы неоднократно говорили в прошлом. Это же является причиной, по которой в прошлом году мы отдали в открытый доступ собственный набор инструментов для тестирования облачных сервисов с помощью Atlas RIPE всем заинтересованным сторонам.

Сама возможность формализации ключевых параметров, которые имеет смысл сравнивать в ходе тестирования, очень важна и далеко не всегда легка. Измеряя некорректные индикаторы, вы не сможете получить больше информации о сервисе или продукте, а также о том, какой из многих лучше подойдет вашему бизнесу. Континентальный Китай же представляет собой очень особенный случай из-за широко известного “Великого Файрволла”, влияющего на стандартную передачу и обработку сетевых пакетов.

Measurement as the key to transparency
QRATOR LABS. RADAR

Measurement tools
GITHUB

	Akamai	Incapsula	Qrator	Akamai	Incapsula	Qrator	Akamai	Incapsula	Qrator
	/texts/forms/purchase/purchase			/users?filter=photos&gender=...			/users/429790031/photos/06b15		
Beijing, China	4.909	2.370	0.910	3.083	0.502	1.133	3.955	0.612	1.135
Shanghai, China	1.523	0.546	0.400	2.711	0.692	0.321	2.640	0.954	0.320
Guangzhou, China	2.986	1.009	0.370	3.002	1.044	0.452	3.374	1.049	0.519

* Данная методология и результаты берут свое начало от нашего клиента и должны быть рассматриваемы с некоторой осторожностью.

О компаниях

Qrator Labs основана в 2009 году. Компания предоставляет услуги противодействия DDoS-атакам и является признанным экспертом в этой области.

Команда экспертов Qrator Labs занимается исследовательской деятельностью в области защиты от DDoS с 2006 года, и постоянно совершенствует алгоритмы, технологии и приемы противодействия DDoS-атакам.

В 2010 году компания запустила в эксплуатацию собственную сеть фильтрации трафика Qrator, как технологическую основу коммерческого сервиса для защиты сетевых сервисов от подобных угроз. Алгоритмы и технологии, которые используются для противодействия атакам на сетевые сервисы клиентов, являются know-how компании.

На сегодняшний день Qrator Labs – один из лидеров рынка услуг защиты от DDoS. Её клиентами являются многие крупные компании из различных отраслей: ведущие банки (банк «Тинькофф Кредитные Системы», ЮниКредит Банк, МДМ банк, Рокет банк, ОТП банк, банк Интеза, банк Национальный Расчётный Депозитарий) и платёжные системы (Qiwi, Cyberplat, Элекснет), магазины электронной коммерции (Lamoda, Юлмарт, Эльдорадо, Wildberries, Ситилинк), СМИ (МИА «Россия Сегодня», ИТАР-ТАСС, радиостанция «Эхо Москвы», Регнум, телеканалы «Звезда», ТНТ, «Дождь», НТВ-Плюс) и многие другие.

8 800 3333 522

qrator.net

press@qrator.net

Компания Wallarm разрабатывает решения для защиты веб-ресурсов, совмещающие в себе функции файрвола для веб-приложений (WAF) и активный сканер уязвимости.

Продукты широко востребовано интернет-компаниями, имеющими высоконагруженные веб-приложения и работающими на рынках электронной коммерции, онлайн-платежей, SaaS/PaaS, Big Data, СМИ и персональных коммуникаций.

В 2014 году компания стала победитем конкурса iSecurity, который проводит фонд «Сколково» среди проектов по информационной безопасности.

wallarm.com

press@onsec.ru