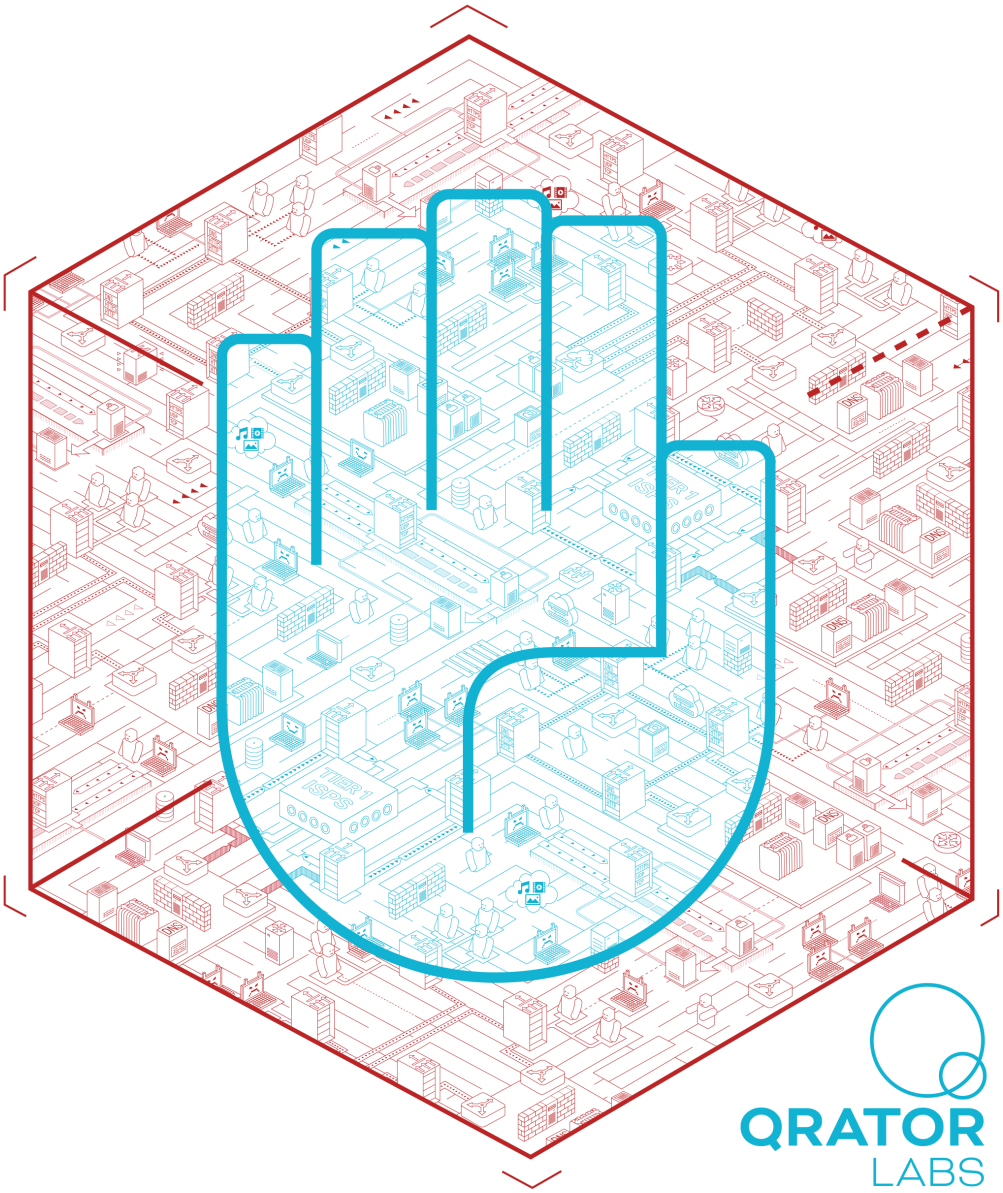
Отчёт о проблемах и доступности Интернета в 2018-2019 годах от Qrator Labs

QRATOR LABS



QRATOR LABS

3 Резюме 2018 года
7 Ключевые наблюдения 2018 года
8 *Профиль атаки с амплификацией memcached*
9 Retrospective
15 *Чемпионат Мира по футболу 2018*
16 Об улучшениях Qrator
21 *Mellanox*
25 Протоколы и опенсорс
28 *Инструменты измерения сетевой задержки RIPE Atlas*
29 Radar
32 *Значительные инциденты BGP*
33 Улучшения Радара в 2018 году:
36 *Устойчивость национальных сегментов интернета*
38 Глубокое погружение с ботами
43 *Clickhouse*
45 Интернет Вещей
46 Заключение

Резюме 2018 года

2018 год начался рекордными по интенсивности атаки с memcached амплификацией, ознаменовавшими начало новой эры DDoS-атак, противостоять которой предстояло всей отрасли кибербезопасности. Удивительной стала и реакция отрасли: отключение львиной доли уязвимых серверов в течение месяца. Кажется впечатляющим, если не задумываться об отсутствии профилактических мер позволяющих избежать подобных событий еще до их начала. 2018 год также продемонстрировал, что, помимо манипуляций с BGP, терабитные DDoS-атаки способны нокаутировать интернет провайдеров среднего уровня, если не самых крупных. Мало кто не согласится с утверждением, что количество амплификаторов и рефлекторов не упадет в обозримом будущем, из чего следует, что риск обновления рекордов в 2019 году достаточно высок.

Атаки, сосредоточенные внутри отдельных регионов, происходят со все более высокой частотой и пропускной способностью. Угрозы глобально распределенных ботнетов стали контролируемыми, но что если такое же количество атакующих устройств будет сконцентрировано внутри одного города? Для нейтрализации подобных атак требуется дополнительный опыт в управлении сетью, моделировании возможностей и дополнительных мощностях, равно как и готовность добавить сетевую задержку в обслуживание запросов потребителей.

Высокоинтенсивные DDoS-атаки сосредоточенные в одном регионе представляют собой смертельную угрозу. Мы не утверждаем, что эта угроза нова - всегда было очевидно, что в определенный момент внутри одной страны будет достаточно атакующей силы для отключения любого интернет-бизнеса, мы лишь не были уверены в прохождении данного порога в 2018 году. Однако он пройден, в виде DDoS-атак интенсивностью в 500 Гбит/сек, сгенерированных на 100% внутри одного региона. Такая сила может нанести множественные ранения даже хорошо подготовленным игрокам. Мы не просто ожидаем повторения подобных событий — они будут случаться все чаще и во многих других странах и регионах, чьи сети выросли и стали быстрыми, и эффективными. Европа, Россия, Китай, обе Америки, Индия - все эти огромные территории уже

обладают устойчивыми сетями, готовыми к тому, чтобы быть нацеленными на выведение из строя региональные цели.

Число зашифрованных атак значительно выросло, оправдывая всеобщие ожидания - Qrator Labs направляет огромные усилия на постоянную модернизацию сервиса фильтрации зашифрованного трафика без раскрытия ключей шифрования, в первую очередь его качества ввиду изменяющейся структуры рыночного спроса. В предыдущие годы подобные атаки были редки, а самые крупные рыбы мира DDoS-атак использовали в первую очередь старый вектор HTTP. Сегодня же, способные к использованию шифров боты представляют собой первостепенную опасность, ибо обладают широкими способностями к обучению.

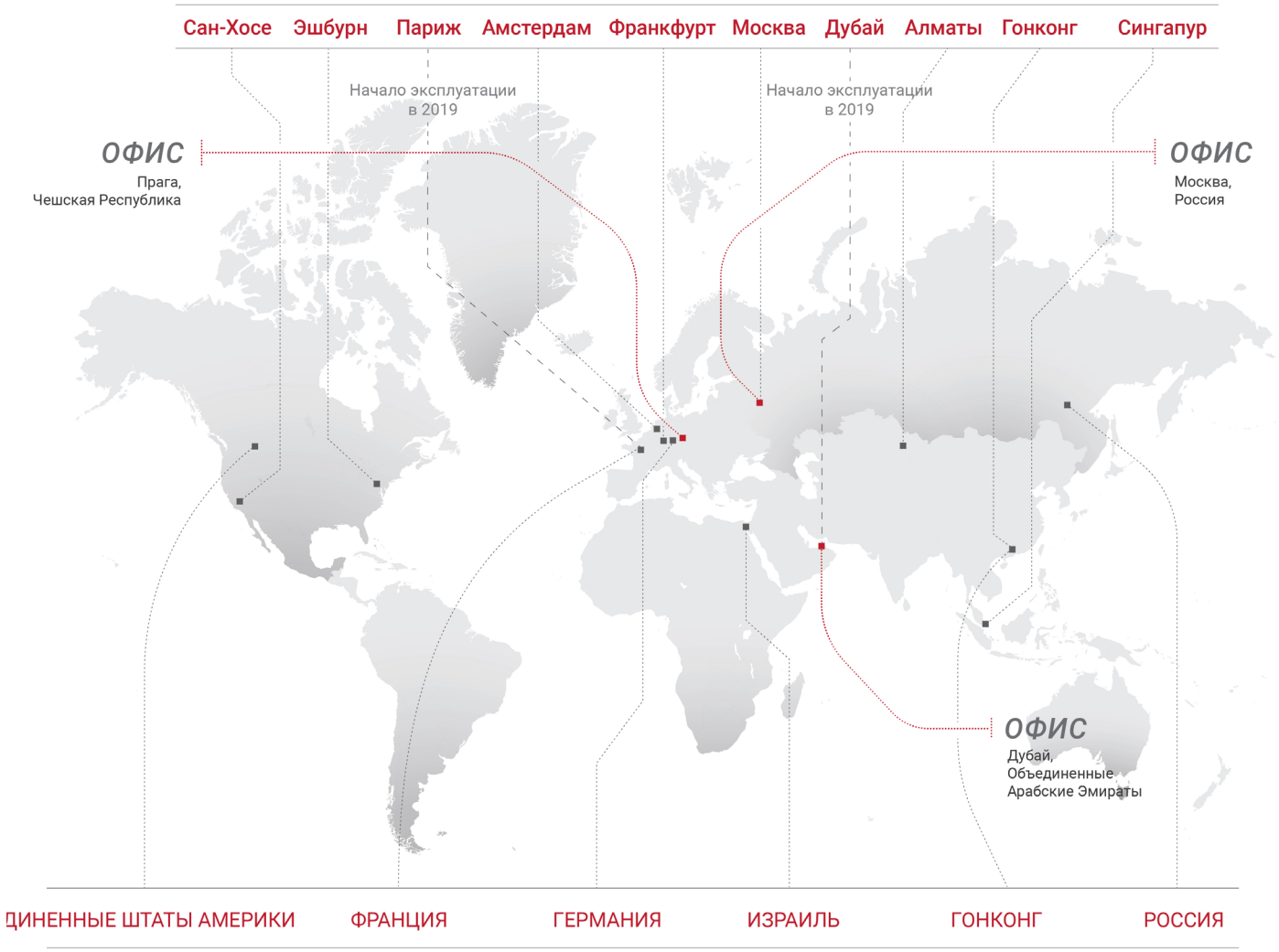
Риски, связанные с сетью, выросли на порядок за прошедшие три года и всем пришлось адаптироваться к растущей сложности и интенсивности DDoS-атак. Два параметра остаются фундаментальными в вопросе построения отказоустойчивой сети фильтрации, также, как и любой другой сети: масштабируемая архитектура с близкими к источникам трафика, а не к потребителям, точками присутствия и избыток пропускной способности. Нам приходится поспевать за ростом средних и максимальных значений интенсивности и сложности атак для предоставления максимально высокого, возможного, уровня связности потребителей, в первую очередь в стрессовых ситуациях во время атак.

В этом смысле 2018 год был крайне важен с точки зрения безопасности протокола BGP. Расширение BGPSec наконец приобрело законченный, тем не менее никто не ожидает его полной имплементации на большинстве сетей вследствие сложности поддержки.

Однако, BGP становится востребован у атакующих, все чаще использующих его для перехвата трафика и перенаправления ничего не подозревающих пользователей на фальшивые фишинговые страницы. В ростом количества жертв подобных манипуляций одним из корневых протоколов интернета, в 2018 году наконец была достигнута точка в которой стало ясно наличие проблемы и необходимость агрессивного ответа. Здесь также важно повторить тот факт, что шифрование не защитит пользователей от обмана, так как злоумышленники научились подписывать SSL сертификаты, а потому такие страницы не вызы-

вают подозрения у рядового посетителя ввиду отсутствия наглядной разницы между настоящей, легитимной веб-страницей и фальшивой.

Связанные с BGP риски перехвата трафика распространены шире, чем кажется. Существует вероятность перехвата SMTP в подобном стиле, что может привести к атакам на инфраструктуру DNS в случае, если жертва не поддерживает DNSSec. Прокси-сервер считывающий такой трафик может создать множество разнообразных проблем. За последнее десятилетие мы уже убедились в том, что подобные «уязвимости», или альтернативные методы манипуляции протоколами, могут быть найдены в широком их спектре. Уязвимости BGP были известны в течение минимум 10 лет до того момента, как мы увидели первые атаки нацеленные на крупных игроков рынка интернета.



ПРЕДСТАВИТЕЛИ И ПАРТНЕРЫ

Манипуляции DNS, такие как cache poisoning, очень часто сопровождают попытки перехвата с помощью BGP. В 2018 году мы стали свидетелями грабежа разнообразных криптовалют, организованных с использованием связки именно этих двух протоколов.

Предположение, что атакующие знают мало, или ничего, о топологии интернета более неприменимо. Развитие событий подобным образом очень важно со многих точек зрения, включая конкурентную и прагматическую. На наш взгляд, индустрия достаточно долго наслаждалась комфортом и преимуществом убежденности, что только хорошие парни знают, как работает дорогостоящее сетевое оборудование на каждой промежуточной точке по пути сетевого пакета.

Атаки 2018 года показали наличие длительной, возможно месяцы и более, предварительной подготовки атакующих. Пока кто-то может повторить "ничего нового", мы должны распознать и категоризировать каждую из развивающихся угроз, избегая отвлекающих факторов легкомыслия и чрезмерной самоуверенности.

Злодеи обучаются не хуже других и возможно делают домашнюю работу. От исследования старых форумов, сторонних выступлений на конференциях и изучения спецификаций протоколов по прежнему возможно узнать о малоизвестных и не закрытых уязвимостях, точно так же, как это случилось с memcached год назад, весной 2018 года, обновив рекорд и наше представление о возможном.

Самое худшее заключается в том, что атакующим часто даже не нужно обладать собственной дорогостоящей инфраструктурой для организации атак - все доступно, только руку протяни.

Ключевые наблюдения 2018 года:

- *Средняя длительность DDoS-атак упала до 2,5 часов;*
- *2018 год показал наличие вычислительной силы, способной генерировать атаки интенсивностью сотни гигабит в секунду внутри одной страны или региона, подводя нас к краю «квантовой теории относительности пропускной способности»;*
- *Интенсивность DDoS-атак продолжает расти;*
- *Вместе с одновременным ростом доли атак с использованием HTTPS (SSL);*
- *Персональные компьютеры мертвы — большая часть современного трафика генерируется на мобильных устройствах, представляя собой задачу для организаторов DDoS и следующий вызов для компаний, занимающихся защитой сетей;*
- *BGP наконец стал вектором атаки, на 2 года позже ожидаемого нами срока; Манипуляции DNS по прежнему являются наиболее разрушительным вектором атаки;*
- *Мы ожидаем появления новых амплификаторов в будущем, таких как memcached и CoAP.*
- *«Тихих гаваней» в интернете больше не существует и все отрасли одинаково уязвимы перед кибератаки любого рода.*

Профиль атаки с амплификацией memcached

0020:										00	01	00	00	00	01	
0030:	00	00	67	65	74	73	20	61–20	62	20	63	20	64	20	65	..gets a b c d e
0040:	20	66	20	67	20	68	20	6A–20	6B	20	6C	20	6D	20	6E	f g h j k l m n
0050:	20	6F	20	70	20	71	20	72–20	73	20	74	20	77	20	76	o p q r s t w v
0060:	20	75	20	78	20	79	20	61—0D	0A	00	00	00	00	00	00	u x y a.....
0070:	00	00	00	00	00	00	00	00–00	00	00	00	00	00	00	00	.....
0080:	00	00	00	00	00	00	00	00–00	00	00	00	00	00			.....

В 2017 году группа китайских исследователей кибербезопасности из команды 0Kee указала на вектор амплификации memcached — и всего через пару месяцев рекордные DDoS-атаки обрушились на интернет, пользуясь беззащитностью memcached серверов с настройками по умолчанию.

Будучи свободно распространяемым ПО, доступным в любом Linux-дистрибутиве, Memcached, способный предоставить фактор амплификации, превышающий 10000 (Akamai заявил о факторе выше 50000), стал мощнейшим инструментом разрушения.

И хотя исследователи обнаружили этот потенциал лишь совсем недавно, представлен в коде он был далеких 10 лет назад, когда поддержка UDP была добавлена в memcached — никто, включая автора, в то время не думал об амплификаторах. Только сейчас, в условиях высокоскоростных и эффективных сетей, это стало серьезной проблемой.

Основная идея амплификатора (умножителя/отражателя) трафика в свою очередь совсем не изменилась. Сначала, фальшивые (IP-spoofing) запросы отправляются на уязвимый (открытый на порту 11211) memcached-сервер, подготавливающий UDP-ответ и, с помощью атакующего, посылающий его многократно в цель, исчерпывая пропускную способность сетевого канала таким потоком. Большие количества доставленных пакетов в секунду и битов в секунду не могут быть смягчены или отброшены без специализированного решения, в первую очередь

по причине быстрого выведения из строя пограничных маршрутизаторов.

Текущий рекорд интенсивности DDoS-атаки — удар силой 1,7 Терабит в секунду по одному из потребителей услуги Arbor Networks в 2018, за которым последовал другой — в 1,3 Тбит/сек. по GitHub, находившемся под защитой Akamai. Эти числа подводят нас к границе того, что сегодня может быть названо «квантовой теорией относительности пропускной способности»: интенсивность подобной атаки может быть обнаружена только наблюдателем — другими словами, одна и та же атака может быть увидена одной сетью как 1 Тбит/сек, другой же как 2 Тбит/сек. Так или иначе ни та, ни другая нагрузка попросту не могут быть выдержаны типичной сетью с единственной точкой присутствия где угодно в мире.

И хотя количество уязвимых серверов в интернете уменьшается, атакующие находятся в постоянном поиске новых, серьезных уязвимостей. Сетевые администраторы, ответственные за оставшиеся незакрытые memcached серверы кажутся либо необразованными, либо безразличными — это касается длинного хвоста абсолютно всех уязвимых сервисов, используемых злоумышленниками в качестве амплификаторов. Вот почему очень важно найти рабочий способ бороться с проблемой амплификаторов в сети на уровне оператора сети.

Ретроспектива

В 2018 году наша компания «отметила» две рекордных атаки на собственную сеть. Атаки с амплификацией memcached, которые мы подробно описывали в конце февраля 2018 года, ударили по платежной системе Qiwi с интенсивностью 500 Гбит/сек, но были успешно нейтрализованы сетью фильтрации. В конце октября мы увидели другую знаковую атаку - DNS амплификацию с источниками, локализованными внутри одной-единственной страны, но невиданной ранее мощности.

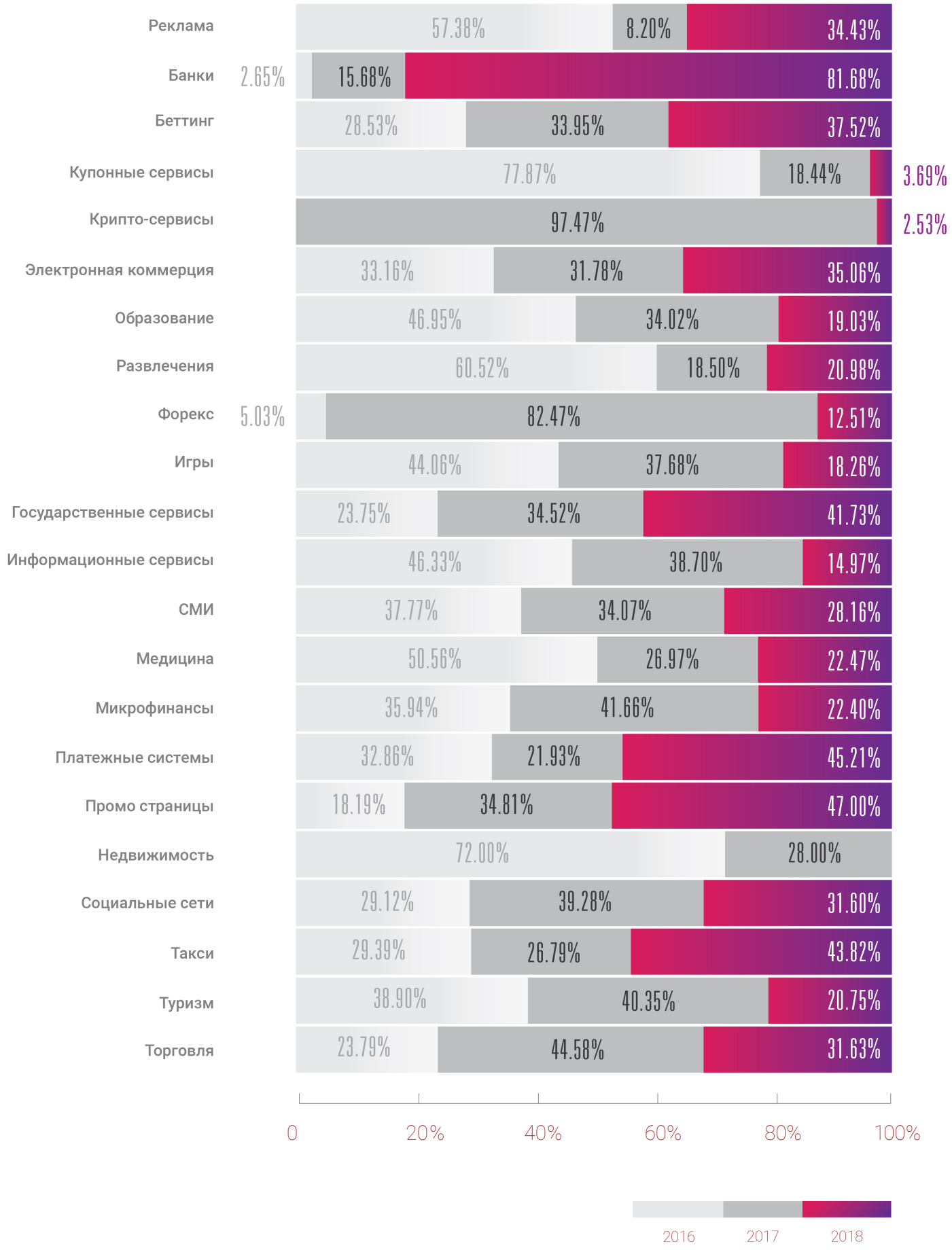
DNS амплификация была и остается одним из самых известных векторов DDoS-атак канального уровня и до сих пор поднимает два острых вопроса. В случае атаки интенсивностью в сотни гигабит в секунду существует немалая вероятность перегрузки подключения к вышестоящему провайдеру. Как с этим бороться? Очевидно, необходимо распределить такую нагрузку по как можно большему количеству каналов — что приводит нас ко второй проблеме — добавленной сетевой задержке в результате изменения путей движения трафика до мест его обработки. К счастью, мы справились и со второй атакой благодаря гибким опциям балансировки нагрузки внутри сети Qrator.

Именно таким образом балансировка продемонстрировала нам свою высочайшую ценность — так как Qrator Labs управляет anycast BGP-сетью, наш Radar моделирует распределение трафика по сети после изменения модели балансировки. BGP - это дистанционно-векторный протокол и мы хорошо понимаем состояния, ведь граф дистанций остается почти статичным. Анализируя эти дистанции с учётом LCP и Equal-Cost Multipath мы можем заранее оценить AS_path из точки А в точку Б с высокой степенью точности.

Это не значит, что амплификация является наиболее серьезной угрозой — нет, атаки прикладного уровня остаются наиболее успешными, невидимыми и эффективными, так как большая часть из них совершаются на низкой интенсивности используемой полосы.

Это основная причина, по которой Qrator Labs бескомпромиссно улучшает соединения с операторами на точках присутствия, одновременно увеличивая их количество. Такой шаг является логичным для любого сетевого оператора в настоящее время, при условии, что бизнес растет. Но мы продолжаем считать, что большинство атакующих сначала

3-ЛЕТНЯЯ ДИНАМИКА АТАК ПО ПОТРЕБИТЕЛЬСКИМ СЕКТОРАМ



собирает ботнет и лишь после начинает выбирать среди широчайшего списка доступных амплификаторов, по которым можно ударить из всех возможных орудий, на максимальной скорости перезарядки. Такие гибридные атаки происходят уже давно, но лишь недавно их интенсивность, как с точки зрения количества пакетов в секунду, так и задействованной сетевой полосы, начала расти.

Ботнеты значительно развились за 2018 год, а их владельцы придумали новое занятие — кликфрод. С улучшением технологий машинного обучения и получением в руки headless-браузеров, работающих без сетевых заголовков, занятие кликфродом значительно упростилось и удешевилось — всего за два года.

Сегодня среднестатистический веб сайт получает от 50% до 65% трафика от мобильных устройств, их браузеров и приложений. Для некоторых сетевых сервисов, эта доля может доходить до 90% или даже 100%, в то время как исключительно «десктопных» веб сайтов уже практически не существует, разве что внутри корпоративных окружений, либо в виде узкоспециализированных случаев.

Персональные компьютеры, фактически, исчезли с пика сетевого ландшафта к 2019 году, делая некоторые в прошлом успешные техники, такие как слежение за положением мыши, абсолютно нерабочими для целей фильтрации трафика и защиты от ботов. Фактически, не только персональные компьютеры, но и большинство ноутбуков и все-в-одном коробок редко когда являются источником значительной доли посещений страниц, при этом легко становясь оружием. В свое время, простого отказа в доступе чему угодно, некорректно представляющим мобильный браузером еще недавно было вполне достаточно для нейтрализации атак с ботнетов почти полностью, нивелируя отрицательный эффект для ключевых бизнес метрик до нуля.

Создатели и управляющие ботнетами уже привыкли к внедрению практик, имитирующих поведение реальных посетителей страниц в собственный вредоносный код, точно так же, как владельцы веб страниц привыкли к тому, что браузеры на персональных компьютерах имеют

значение. Впрочем, и то и другое видоизменяется, последнее, правда, гораздо медленнее первого.

Мы уже заявили, что ничего не изменилось в 2018 году, но прогресс и сами изменения претерпели значительную эволюцию. Один из наиболее ярких примеров — машинное обучение, где улучшения и прогресс были хорошо заметны, особенно в области генеративно-состязательных сетей. Медленно, но верно, ML достигает массового рынка. Машинное обучение уже стало вполне доступным и, как показала граница 2018-2019 годов, уже не является ограниченной до академиков отраслью.

И хотя мы ожидали появления первых, основанных на ML-алгоритмах, DDoS-атак уже к началу 2019 года — до сих пор подобного не случилось. Тем не менее, это не меняет наших ожиданий, но лишь подогревает их, особенно учитывая снижающуюся стоимость управления нейросетями и постоянно повышающуюся точность их аналитики.

С другой стороны, если рассмотреть текущее состояние индустрии «автоматизированных человеческих особей», то становится ясно, что имплементация нейросети в эту конструкцию является потенциально прорывной идеей. Подобная сеть может учиться на поведении реальных людей в контексте управления веб страницами. Подобную вещь назовут «пользовательский опыт искусственного интеллекта» и, конечно же, подобная сеть, вооруженная веб браузером, может расширить арсенал обеих сторон: атакующей и защищающейся.

Обучение нейросети дорогостоящий процесс, но распространение и аутсорсинг подобной системы мог бы быть дешев, эффективен и, потенциально, даже бесплатен — в случае, когда вредоносный код прячется внутри взломанных приложений, расширений и много чего другого. Потенциально, подобная перемена могла бы изменить всю индустрию так же, как генеративно-состязательные сети трансформировали наше понимание «визуальной реальности» и «достоверности».

Учитывая продолжающуюся гонку между поисковыми движками — в первую очередь Google и всеми остальными, кто пытается осуществлять их реверс-инжиниринг, дело может дойти до, пока, совсем фан-

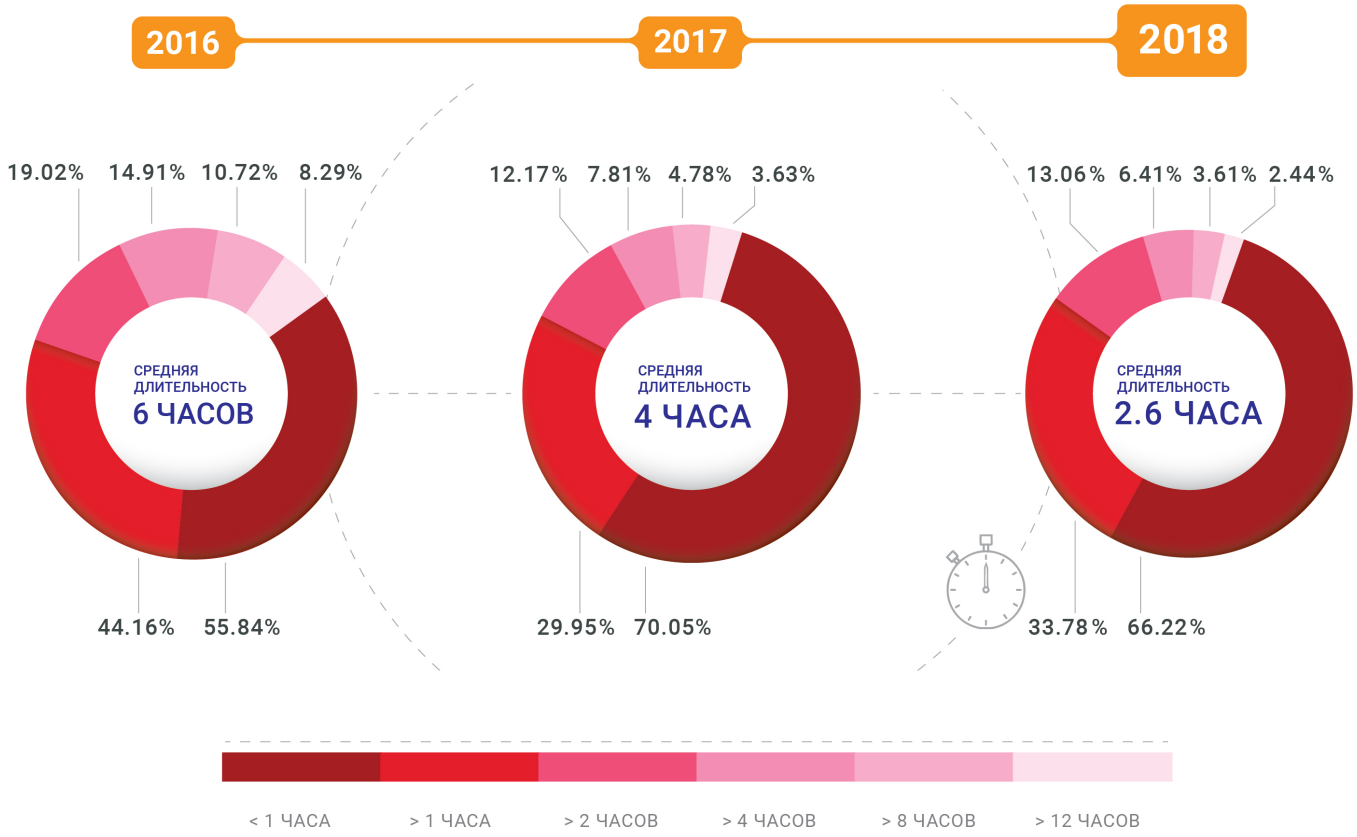
тастических вещей — таких как имитация ботом одного-единственного, конкретного, человека. Как правило сидящего за уязвимым компьютером. Версии проекта Captcha и ReCaptcha могут служить примером того, как быстро и сильно атакующая сторона развивает и улучшает собственные инструменты и техники нападения.

После memcached было много разговоров о вероятности (или невероятности) появления совершенно нового класса вооружения для DDoS — уязвимости, бота, некорректно настроенного сервиса или чего-то еще, что будет бесконечно посылать данные по специфической цели, выбранной атакующим. Одна команда от атакующего вызывает непрерывный поток трафика, такого как любой из флудов, или отправка syslog. На текущий момент — это теория. Мы по прежнему не можем сказать, существуют ли подобные серверы, устройства, но если ответ на такой вопрос утвердителен — будет недооценкой ситуации сказать, что подобная вещь может стать невероятно опасным оружием в злых руках.

В 2018 году мы также увидели нарастающий интерес в том, что называется «управлением интернетом» и связанными с ним сервисами со стороны государств и некоммерческих организаций по всему миру. Мы относимся нейтрально к подобному развитию событий до того момента, когда начинается подавление фундаментальных гражданских и индивидуальных свобод, чего мы надеемся не случится в развитых странах.

Наконец, спустя годы сбора и анализа трафика атак по всему миру, Qrator Labs готова к имплементации блокировки по первому сетевому запросу. Модели, которые мы используем для предсказания злонамеренного поведения позволяют нам с высокой точностью определять легитимность пользователя для каждой конкретной страницы. Мы продолжаем настаивать на собственной философии безбарьерного входа для пользователя и неразрывного пользовательского опыта, без JavaScript-проверок или капчи, которая с 2019 года начнет работать еще быстрее, обеспечивая высочайший уровень доступности защищаемых сервисов.

3-Х ЛЕТНЯЯ ДИНАМИКА ПРОДОЛЖИТЕЛЬНОСТИ АТАК



Чемпионат мира по футболу 2018 года

Как компания, чья деятельность началась в России, мы пристально следили за проведением Чемпионата мира по футболу 2018 года. Статистика, собранная нами за это время, выглядит следующим образом.

За время проведения чемпионата трафик онлайн магазинов упал на 46%, в то время как посещаемость трейдинговых платформ, включая форекс, снизилась на треть. Онлайн игры на промежуток чемпионата потеряли 14% постоянных посетителей.

В дни игр сборной России по футболу изменения в трафике были более заметны: посещаемость онлайн игр падала на 38%, а трейдинговых платформ — на 28%. Тем не менее, большинство пользователей вернулись на ресурсы по окончанию игр.

Наиболее драматично, за все время проведения чемпионата, возрос трафик онлайн касс в ретейл-магазинах, отелях и ресторанах — в шесть раз.

И наоборот, в дни игр национальной сборной России, он падал же падал на 1.4x — почти в полтора раза.

Вызовы такси онлайн росли на 50% в общем, но падали на 12,5% в дни игр сборной России.

Похожее происходило и с онлайн банками — общий подъем в трафике на 27% и падение на 38% в дни игр сборной России.

Популярность беттинговых ресурсов роста в соответствии с ожиданиями. Трафик же крупных медиа ресурсов, освещавших подробности хода Чемпионата мира по футболу, удвоился, в то время как на специализированные спортивные ресурсы пришло в четыре раза больше посетителей, нежели обычно.

Об улучшениях Qrator

В 2018 году Qrator Labs внедрила Single Page Application подход в закрытой, внутренней части веб сайта, где потребители основной услуги фильтрации управляют сервисом. Прежде всего, теперь секции бэкенда главной панели управления Qrator, сообщающиеся с фронтендом, где работает пользователь, настраиваются и управляются в виде контейнеров с оркестрацией, подключенных исключительно к API. Мы отка-

зались от тяжелого HTML — простое javascript-приложение отображает все пользователю, статические же данные лежат в идеальных для них условиях, а API обеспечивает гладкое взаимодействие.

Говоря об оркестрации контейнеров важно отметить, что данный тренд не может быть обойден стороной. С Docker и Kubernetes меняется и мониторинг, сдвигаясь в сторону наблюдения за сервисами и их показателями, вместо оборудования. И хотя мы до сих пор осуществляем мониторинг эффективности железа, эти числа, в реальной жизни, теряют свое значение рядом с более высокоуровневыми метриками, такими как «доступность сервиса» или «деградация сервиса».

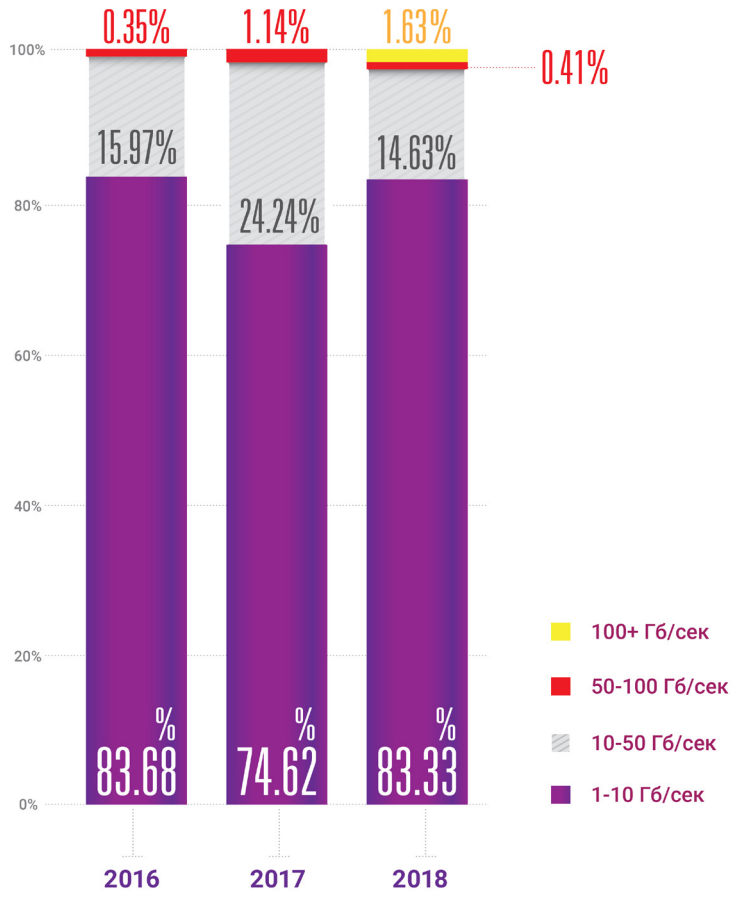
В 2018 году Qrator Labs произвела значительное улучшение статистического аппарата со следующими изменениями:

- *Вводом новых, гибких и масштабируемых метрик, которые мы готовы видоизменять по требованию потребителей;*
- *Отдельным отказоустойчивым кластером для сбора и обработки статистических данных;*
- *Все точки присутствия отправляют статистику в аппарат независимо друг от друга — данные не запрашиваются;*
- *Внутренний протокол синхронизации сети претерпел модернизацию, что позволило нам в три раза улучшить показатель точности по времени;*

Предложение услуг нашей компании расширяется горизонтально, одновременно с расширением фокуса работы внутри каждой проблемы потребителя как единство верное направление развития, которое задают постоянно эволюционирующие угрозы. Мы планируем расширять поддержку протоколов стратегически, так как включение IPv6, HTTP/2,

DNSSec, DoH и других вещей требует гораздо большего, нежели написания всего лишь дополнительных строк кода. Требуется взгляд в далекое будущее рынка для того, чтобы совместить эффективную защиту от DDoS-атак с требованиями потребителя и реальностью сетевой архитектуры.

3-ЛЕТНЯЯ ДИНАМИКА ИНТЕНСИВНОСТИ DDOS АТАК



Как будет выглядеть сеть фильтрации в 2022 году?
Всегда проще сказать, как она не должна будет выглядеть, вместо голословных предположений о ее будущей архитектуре.

Без глубокой кастомизации, решения по фильтрации трафика никогда не смогут полностью интегрироваться со специфическими ресурсами, требующими защиты. Попытка применить стандартную систему нейтрализации DDoS там, где присутствует специфический трафик, приложение или архитектура, редко смогут обеспечить приемлемый уровень качества. Так происходит с любым решением в отсутствие значительных усилий по его отладке и индивидуализации, что особенно заметно именно в области безопасности.

Это основная причина, по которой Qrator Labs вкладывает значительные усилия в улучшение и обучение сервиса фильтрации, добавляя новые возможности и новые данные для анализа. Развивая сеть наилучшим возможным способом, мы внимательно прислушиваемся к требованиям потребителей, ведь именно их бесценные сетевые ресурсы мы и защищаем.

В 2018 году мы проапгрейдили все соединения с вышестоящими поставщиками на точках собственного присутствия, так как текущий уровень угроз уже не позволяет обходится 40G, не говоря о 10G, соединениями для адекватного уровня качества услуги, называющейся «непрерывная доступность».

Flowspec там, где он доступен, отлично помогает блокировать мусорный трафик на уровне вышестоящего провайдера, но далеко не все Tier-1 и Tier-2 интернет-провайдеры поддерживают такую возможность. Это объяснимо, ведь flowspec предоставляет нижестоящему соединению возможность управления вышестоящим, что дает пространство для злоупотребления. Однако, при помощи BGP communities возможно изолировать отдельные потоки трафика от всего клиентского трафика крупного международного Tier-1 провайдера, позволяя безопасно управлять необходимой его частью.

Внутренний сервисный протокол Qrator Labs, обеспечивающий синхронизацию данных между точками присутствия претерпел значительные улучшения, а также объединил все внутренние инструменты и сервисы компании, постоянно использующиеся нашими сетевыми инженерами при нейтрализации различных DDoS-атак.

Долгие годы коды состояний HTTP и рост их количества на стороне потребителя и клиента были признаком беды и, буквально, лучшей метрикой для мониторинга. В 2018 году Qrator Labs поставляет потребителю услуги почти такое же количество метрик, связанных с бизнес показателями приложения под защитой, а не просто коды состояний HTTP. Измеряя ежедневное самочувствие приложения, его статус и потоки трафика гораздо проще предсказывать флуктуации, включая те, что связаны с атаками. Метрики могут быть также заданы пользователем, ведь в конечном счете именно он знает все уголки собственного приложения.

Увлечение безопасностью необходимо всем участникам растущего пространства объединенных, однако децентрализованных, сетей, называемых интернетом. В качестве публичного пространства, интернет включает в себя одновременно добросовестных и злонамеренных участников, ждущих момента и возможности эксплуатации уязвимостей. И поскольку интернет является публичным пространством, важно создавать правила одинаково эффективные для всех его участников, обеспечивая всех и каждого ресурсом и возможностью.

Сети доставки контента, файрволы веб приложений, защита серверов системы доменных имен и хостинг доменных зон - все это оказывается включено внутрь сети фильтрации Qrator, что оказалось самым удобным для нашего потребителя способом пользоваться услугой, без отвлечения важных ресурсов от ключевого направления бизнеса.

В 2019 году наши планы включают в себя предоставление в законченном виде услуг защиты для сетей доставки контента (CDN) от атак сквозь них же (origin error), а также нововведение услуги защиты офисных сетей крупных предприятий.

В ушедшем году нашу компанию часто называли MSSP — сокращением от «поставщика управляемой услуги безопасности». Конкретные названия и сокращения могут меняться время от времени, вне зависимости от нашей главной цели — предоставления потребителю постоянной доступности и реальной нейтрализации DDoS-атак.

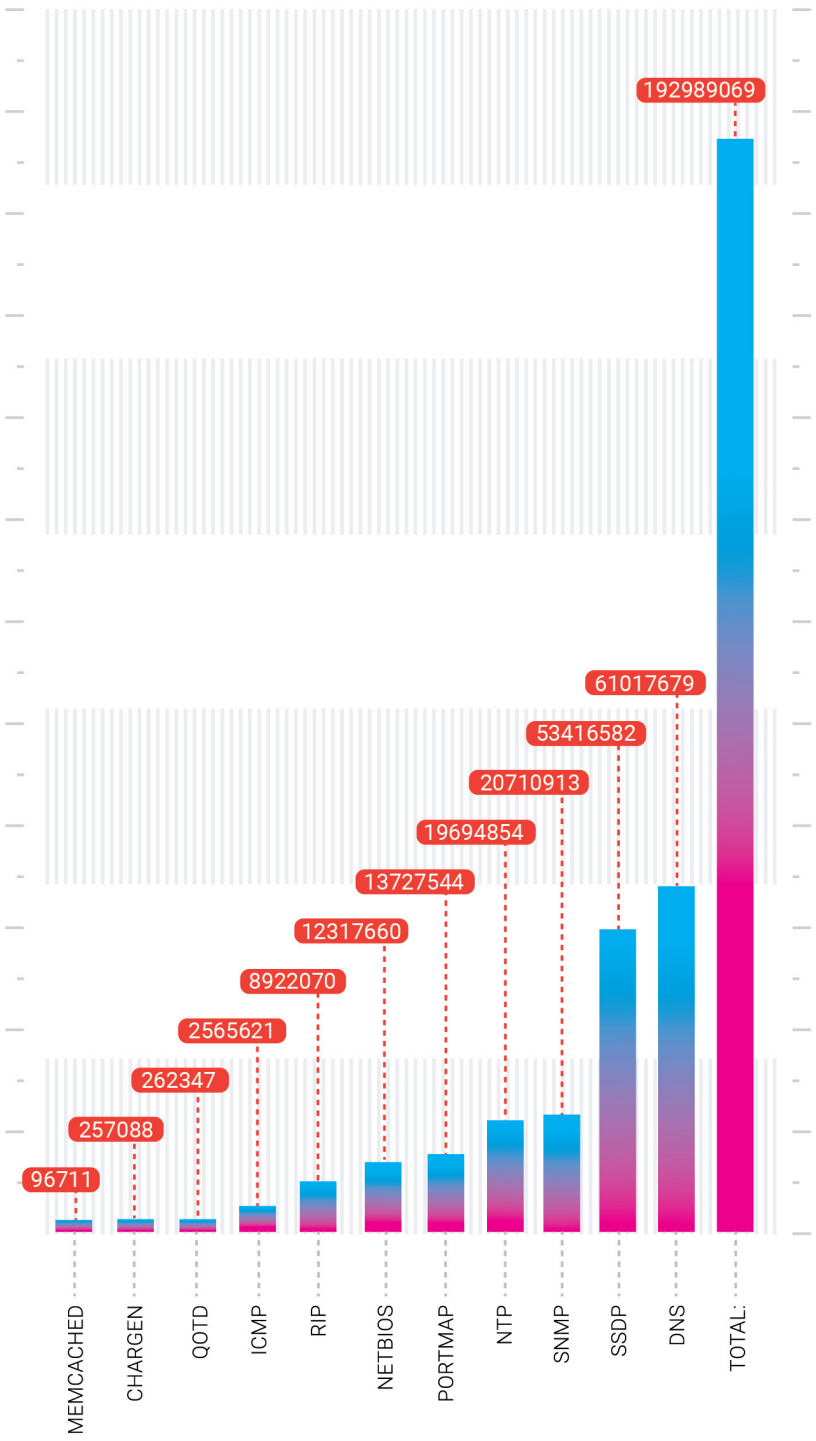
Тем не менее, мы не можем поставить все современные сервисы одновременно под именем и гарантией работоспособности Qrator Labs. Это причина по которой мы постоянно ищем новых и надежных партнеров, способных дать потребителю узкоспециализированные и эффективные сервисы, как, например, Web Application Firewall, безусловно требуемый для защиты от кибератак, с поддержкой на всех языках и во всех часовых поясах.

Mellanox

Наша компания выбрала 100G свитчи Mellanox в результате внутреннего тестирования, проводившегося в течение нескольких лет. Мы по прежнему отбираем то оборудование, которое лучше всего выполняет наши достаточно специфические требования в определенных условиях наилучшим образом. Например, свитч не должен сбрасывать маленькие пакеты на line rate — предельной скорости, неприемлема даже минимальная деградация. К тому же, свитчи Mellanox обладают приятной ценой. Однако это не все - справедливость цены подтверждается тем, как тот или иной вендор реагирует на ваши запросы.

Свитчи Mellanox работают на Switchdev, что превращает их порты в простые интерфейсы внутри Linux. Будучи частью основного ядра Linux, Switchdev предоставляет удобный способ управления устройством с помощью понятных и привычных интерфейсов, под одним API, к которому абсолютно привычен любой современный программист, разработчик и сетевой инженер. Любая программа, использующая стандартный сетевой API Linux, может быть запущена на свитче. Весь мониторинг сетевой

КОЛИЧЕСТВО УНИКАЛЬНЫХ АМПЛИФИКАТОРОВ В 2018



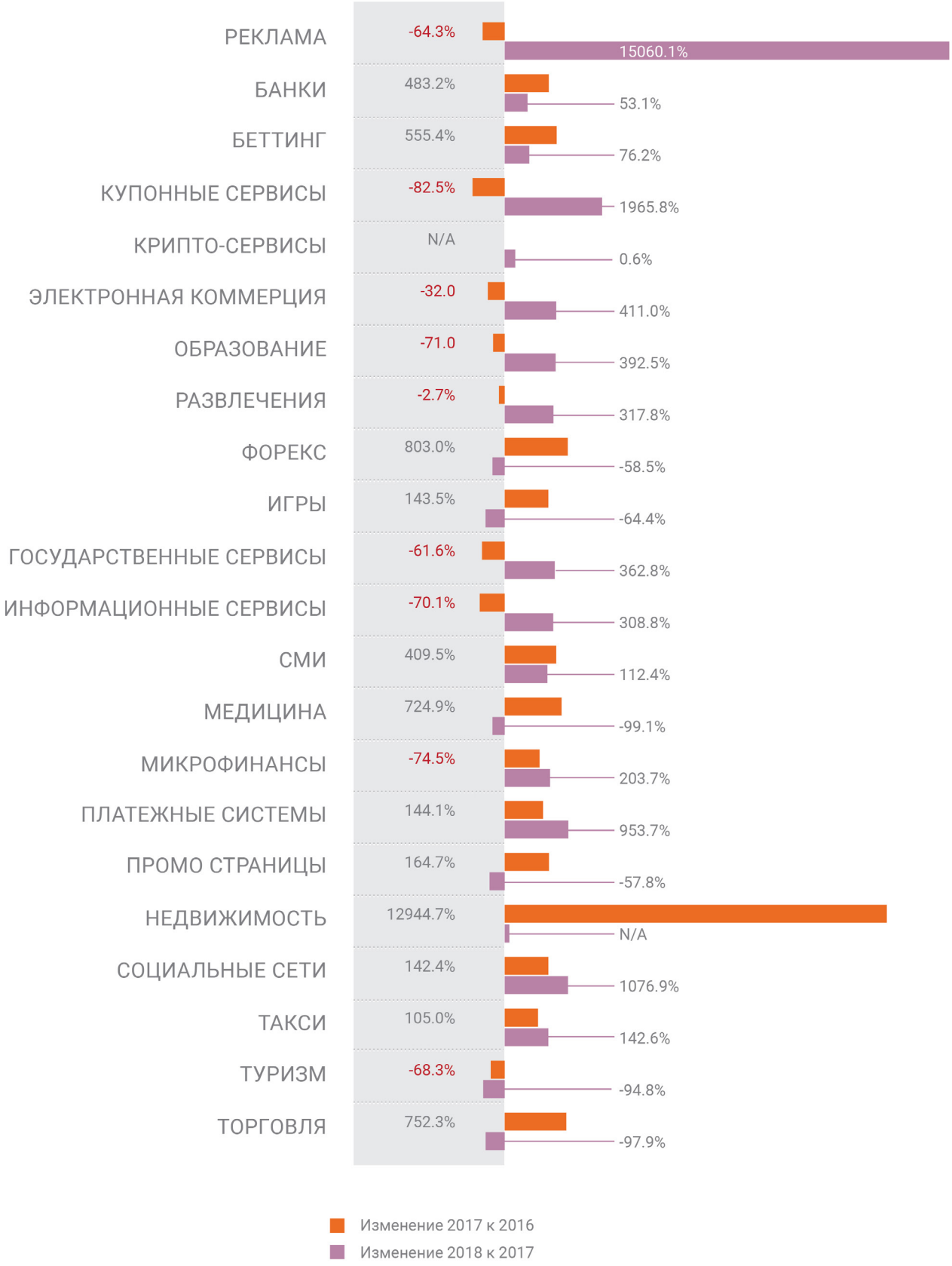
активности и управление им, созданное для серверов на Linux, включая возможные собственные решения, легко доступны. Для иллюстрации изменений, произошедших с активным развитием Switchdev отметим, что модификация таблиц маршрутизации стала в разы быстрее и удобнее со Switchdev. До самого уровня сетевого чипа весь код виден и прозрачен, что позволяет учиться и делать вносить модификации до того момента, когда вам потребуется знать, как именно построен сам чип или, как минимум, внешний интерфейс к нему.

Устройство Mellanox под управлением Switchdev оказалось долгожданной комбинацией, которой так долго ждали в Qrator Labs, но что еще лучше — компания-производитель оправдала все ожидания и требования, не только в вопросе полной поддержки свободной операционной системы из коробки.

Тестируя оборудование перед запуском в эксплуатацию, мы выяснили что часть перенаправленного трафика теряется. Наше расследование показало, что это было вызвано тем, что трафик на один из интерфейсов направлялся с помощью контрольного процессора, который не мог справится с высоким его объемом. Не будучи в состоянии определить точную причину такого поведения, мы, однако, предположили что это связано с обработкой ICMP-редиректов. Mellanox подтвердил источник проблемы, а потому мы попросили что-то сделать с таким поведением устройства, на что компания отреагировала мгновенно, предоставив рабочее решение за короткий срок.

Отличная работа, Mellanox!

3-ЛЕТНЯЯ ДИНАМИКА МАКСИМАЛЬНОЙ ИНТЕНСИВНОСТИ DDOS-АТАК



Протоколы и опенсорс

DNS-over-HTTPS представляет собой более комплексную технологию, нежели DNS-over-TLS. Мы наблюдаем, как первый процветает, в то время как о втором медленно забывают. Данный пример хорош тем, что в этом конкретном случае «сложность» означает «эффективность», так как трафик DoH неразличим от любого другого HTTPS. Мы уже видели то же самое с интеграцией данных RPKI, изначально позиционировавшемся как решение для анти-перехвата и, в итоге, с ним не случилось ничего хорошего. Спустя некоторое время RPKI вновь появился на сцене, как мощный инструмент против таких аномалий, как утечка маршрутов и некорректные настройки маршрутизации. И вот шум трансформировался в сигнал, а RPKI начал поддерживаться на крупнейших точках обмена трафиком, что является отличной новостью.

Прибыл и TLS 1.3. Qrator Labs, как и вся индустрия информационных технологий, пристально следила за процессом разработки нового стандарта шифрования на каждом этапе, от первоначального черновика в IETF до понятного и управляемого протокола, который мы готовы поддерживать начиная с 2019 года. Рынок отреагировал аналогично, обещая скорейшее внедрение заслужившего доверие протокола безопасности. Возможно, что не все производители решений по нейтрализации DDoS смогут одинаково быстро адаптироваться к изменившейся реальности, ведь из-за технической сложности поддержки протокола в железе могут возникнуть объяснимые задержки.

Мы также следим за продолжающимся развитием HTTP/2. На текущий момент, Qrator Labs не поддерживает новую версию протокола HTTP, в первую очередь из-за несовершенства актуальной кодовой базы. Баги и уязвимости все еще слишком часто обнаруживаются в новом коде; как поставщик решения безопасности, мы еще не готовы поддерживать данный протокол под SLA, с которым согласились наши потребители.

В 2018 году мы часто задавали себе вопрос: «Почему люди так сильно хотят HTTP/2?», что являлось причиной многочисленных ожесточенных дебатов. Люди все еще склонны думать о вещах с приставкой «2», как о «более лучших» версиях чего угодно, что особенно верно конкретно в случае некоторых аспектов реализации данного протокола. Тем не менее, DoH рекомендует использование именно HTTP/2 и, вполне возможно, из этой синергии родится высокая степень принятия рынком обоих протоколов.

Одним из переживаний при рассмотрении разработки протоколов следующего поколения и их планируемых возможностей является тот факт, что очень часто разработки не выходят за чисто академический уровень, не говоря о рассмотрении таких крайних по-мнению создателей протоколов случаев, как нейтрализация DDoS-атак. Возможно, это является причиной, по которой и занимающиеся кибер и инфобезопасностью компании прикладывают мало усилий в разработке таких стандартов. Секция 4.4 черновика IETF под названием «QUIC manageability», являющегося частью будущего пакета протокола QUIC, является просто идеальным примером такого подхода: в ней утверждается, что «текущие практики в детектировании и нейтрализации [DDoS-атак] в большинстве своем задействуют пассивное измерение с использованием данных сетевого уровня». Последнее крайне редко используется на деле, за исключением разве что сетей интернет-провайдеров и вряд ли является «общим случаем» на практике. Однако в академической исследовательской бумаге «общие случаи» формируются именно так, в результате чего финальные стандарты протоколов оказываются просто-напросто неприменимы в продакшене, после совершения таких простых манипуляций перед вводом в эксплуатацию, как тестирование под нагрузкой и имитация атак прикладного уровня на приложение, их использующее. Принимая во внимание продолжающийся процесс внедрения TLS в глобальную инфраструктуру интернета, утверждение о каком либо пассивном мониторинге вообще подвергается серьезному сомнению. Выстраивание корректных академических исследований — еще одно испытание для поставщиков решений безопасности в 2019 году.

В то же время, Switchdev полностью оправдал ожидания, которые были заложены в него год назад. Мы надеемся, что непрестанная работа над Switchdev приведет сообщество и общий плод труда к отличным результатам уже в ближайшем будущем.

Дальнейшее развитие и внедрение Linux XDP поможет индустрии добиться высоких значений эффективности обработки сетевых пакетов. Отгрузка некоторых паттернов фильтрации нелегитимного трафика с центрального процессора на сетевой процессор, а в некоторых случаях даже на свитч, уже выглядит многообещающе и наша компания продолжает собственные исследования и разработку в данной области.

УСТРОЙСТВ
ПРИНИМАЮЩИХ УЧАСТИЕ
В ОДНОЙ АТАКЕ
В 2018

671652

Инструменты измерения сетевой задержки RIPE Atlas

Исторически сервисы по нейтрализации DDoS-атак создавались как услуги или оборудование, включающееся в работу непосредственно в момент атаки. Однако, для многих высокорисковых и высокомаржинальных сервисов постоянное включение-выключение такой услуги или оборудования все равно ведет к временной недоступности. В итоге ради избежания даунтайма сервисы постепенно переходят от модели включения под атакой в модель постоянной и непрерывной фильтрации трафика. Но это накладывает на сервисы, предоставляющие услуги фильтрации, дополнительные требования по низким задержкам. Согласно недавнему исследованию Akamai, удовлетворенность людей падает пропорционально падению качества просматриваемого видео и наличию проблем с буферизацией, неразрывно связанных с сетевыми задержками. Пинг крайне критичен для онлайн-игр и игроков, делая невозможной соревновательную игру в случае высоких задержек. Сетевые задержки влияют даже на то, как мы ищем информацию в интернете и принимаем связанные с этим решения. Миллисекунды оказывают огромное, порой невидимое, влияние.

Год назад, в начале 2018 года мы выпустили набор инструментов для проведения нескольких типичных экспериментов, фокусирующихся на визуализации сетевых задержек на карте, а также выдачи DNS. Нашей целью было создание инструмента, способного получать интересные результаты и обойти некоторые ограничения, такие как задействование не более тысячи проб за замер. На текущий момент инструментарий включает в себя следующие компоненты:

RIPE ATLAS HEAT MAP:

Рисует тепловую карту сетевых задержек до заданной цели;

RIPE ATLAS NSLOOKUP MAP:

Визуализация вывода DNS;

RIPE ATLAS COUNTRY MAP:

Рисует среднюю сетевую задержку для определенной области из заданных стран;

RIPE ATLAS REACHABILITY:

Диагностический инструмент, измеряющий доступность специфической цели, дополнительно собирая traceroute от проб не получивших echo-ответ.

Есть также несколько дополнительных флагов, ознакомиться с которыми можно в исходном коде, находящемся в репозитории GitHub. Инструмент прост в установке и использовании - все что вам нужно это кредиты RIPE Atlas.

Radar

Теперь, когда джинн манипуляции BGP выпущен из бутылки, сетевое сообщество должно действовать решительно. Поэтому мы считаем единственным возможным форматом работы взаимодействие внутри Инженерного Совета Интернета (IETF).

В предыдущие годы, мы целились в улучшения протоколов, направленные на снижение уровня ошибок, а в 2018 году сконцентрировались на борьбе со злонамеренной активностью и, в особенности, перехватами BGP. Данный вектор мощен и атакующие не преминут возможностью воспользоваться им снова в попытке вывести интернет сервис из строя или украсть пользовательские данные. Основная же проблема по преж-

нему заключается в том, что помимо мониторинга нет хороших способов предотвратить перехваты трафика в самом протоколе. Как мы уже писали, BGPSec не изменит реальность до тех пор, пока не будет поддержан большинством крупнейших сетей и их операторов, что вполне возможно уже произошло бы в ситуации, когда расширение протокола годилось для скорейшего внедрения и эксплуатации.

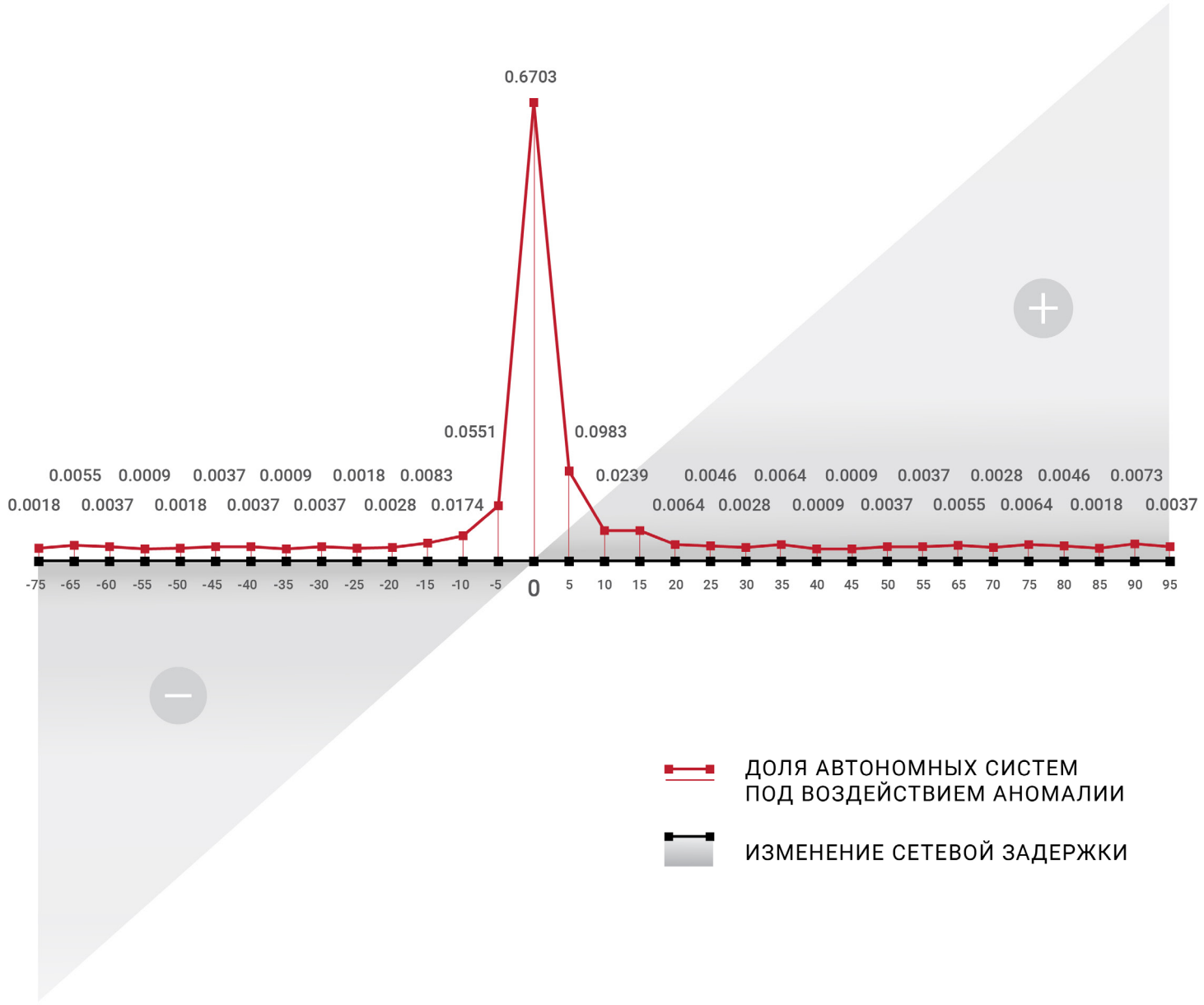
Наш ответ заключается в правильном хакерском подходе — ASPA, где уже существующий инструментарий задействуется для одной из серьезнейших проблем мира BGP маршрутизации. Его внедрение легко и безболезненно, в то же время снимая большую часть связанных рисков. Тот факт, что не требуется полного принятия протокола большинством участников рынка для получения эффекта доказывает, почему нашей инициативе требуется общественная поддержка.

В 2018 году мы видели колоссальные по объему утечки маршрутов, серьезные перехваты трафика и множество других инцидентов, задействующих BGP, что является основной причиной по которой нужно искать решение данной проблемы в ближайшие месяцы, а не десять лет, потребовавшиеся на внедрение BGPSec в текущем виде.

Предлагаемое нами под названием Autonomous System Path Authorization улучшение к протоколу BGP, над которыми наши сетевые инженеры работали в профессиональной группе коллег, может эффективно, но что еще более важно — быстро решить глобальную проблему перехвата трафика. Хотя над решением меньших проблем уровня региональных аномалий все еще придется поработать и в будущем.

Общая сложность управления автономной системой с помощью BGP протокола не снижается со временем и приложенными усилиями. Операторы в развивающихся рынках, где ниши интернет-провайдеров и операторов связи растут огромными темпами каждый год, плохо оценивают возможные последствия некорректно настроенных AS. Никакая система безопасности не защитит от возможной внутренней ошибки. Отсутствие автоматизации BGP делает корректную настройку автономных систем новыми игроками практически невозможной, не говоря о стрессовых ситуациях, таких как перехват трафика или случайное создание утечки трафика.

ВЛИЯНИЕ УТЕЧЕК ТРАФИКА НА СЕТЕВУЮ ЗАДЕРЖКУ



Значительные инциденты BGP

Заметные BGP-инциденты, происходившие в короткий двухнедельный промежуток в конце апреля и начале мая 2018 года могут служить отличным примером того, что происходит, на деле, ежедневно:

24 апреля: ENET, AS10297, США:

злонамеренный перехват одновременно BGP и DNS с успешной кражей криптовалют;

26 апреля: DPSTL, AS267286, Бразилия:

мега-перехват. Бразильский интернет-провайдер анонсировал 16 /8 префиксов, плюс несколько меньших, представляющих в общей сложности ~5% всего адресного пространства IPv4;

4 мая: ELCAT, AS8449, Кыргызстан:

гигантская утечка трафика между Китаем и Россией

21 мая: еще один бразильский интернет-провайдер

совершил утечку маршрутов по более чем 5000 сетевых префиксов.

Если аномалия маршрутизации ударяет по региону, она может быть очень быстро замечена обычными пользователями и масс медиа в наши дни. Тем не менее, большинство аномалий, связанных с BGP, остаются совершенно необнаружимыми в первое время их существования и могут жить по несколько суток, прежде чем ответственный за ее создание оператор предпримет меры по устранению.

Улучшения Радара в 2018 году:

- *Качество детектирования перехватов трафиков значительно улучшилось благодаря интеграции внутрь Радара данных RPKI и IRR;*

- *Наиболее популярная, с точки зрения обращений потребителей, возможность которую мы внедрили связана с приданием разного веса инцидентам. Сама природа BGP инцидентов напрямую зависит от того, насколько далеко сумела распространиться каждая утечка маршрута — как много автономных систем приняли ее. Теперь Радар предоставляет потребителям информацию о каждой отдельной аномалии, задевающей определенный регион. Подобная опция позволяет BGP оператору приоритезировать те инциденты, в разрешении которых он наиболее заинтересован. В 2019 году данная функция также появится для бесплатных пользователей Радара;*

- *До 2018 года Радар не рассматривал проблематику манипуляции AS_PATH вглубь. В течение 2019 года мы собираемся сделать определенные*

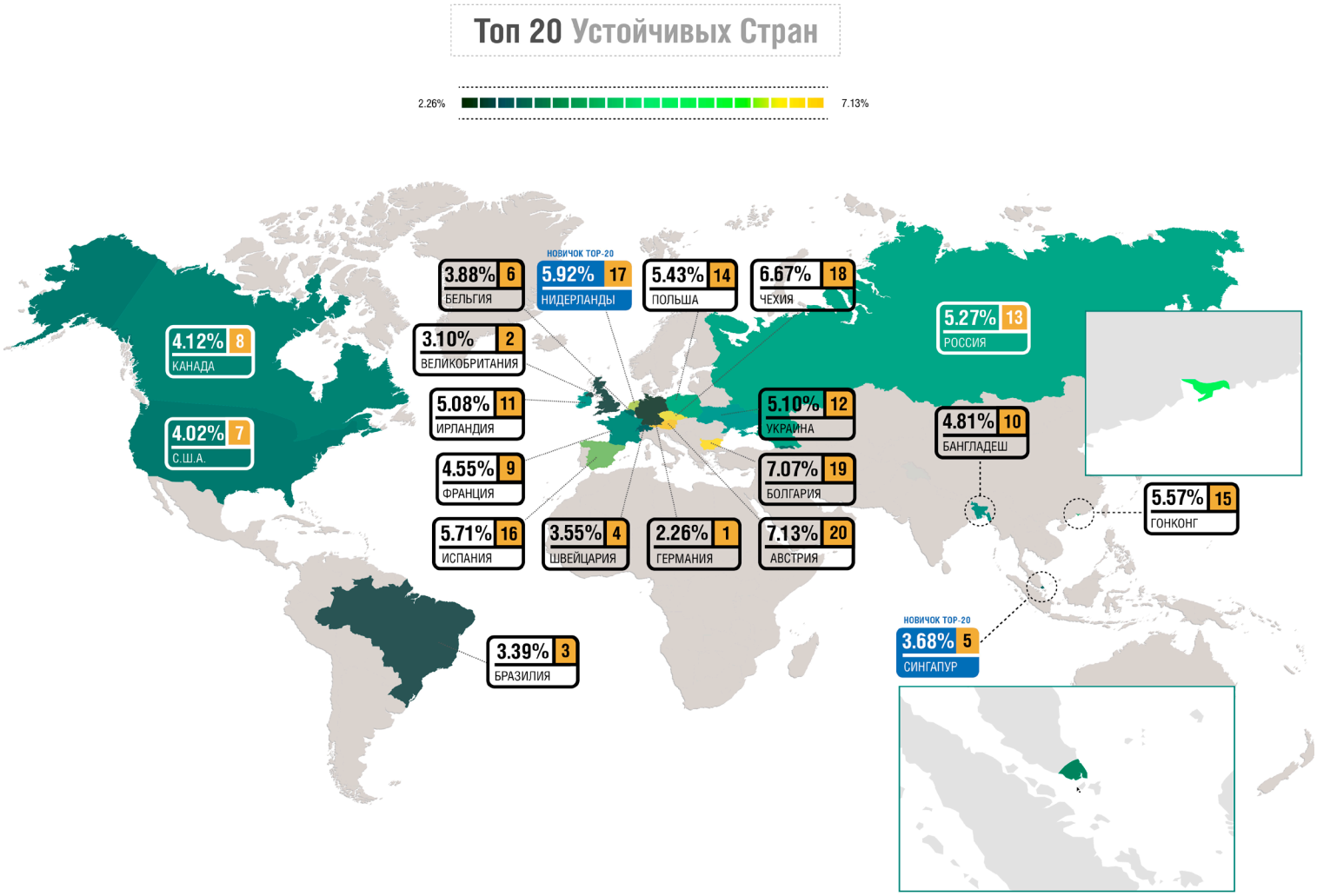
улучшения и обновления в системе мониторинга Радара для того чтобы быстрее анализировать перехваты трафика, а если точнее — именно инциденты, связанные с манипуляцией AS_PATH. Это позволит нам эффективнее отделять инциденты, связанные со злонамеренными атаками на маршрутизацию от ошибок конфигурации. Частота совершения подобных атак растет и нам необходимо снарядить пользователей Радара специфическими инструментами, позволяющими лучше понимать каждый отдельный инцидент перехвата трафика с помощью BGP для лучшей защиты;

- *Так как Радар наблюдает исходящие анонсы с тем же успехом, что и входящие, мы улучшаем детектирование аномалий с помощью «Принятых перехватов» в качестве новой аналитической метрики, делая симметричным анализ как входящих, так и исходящих BGP аномалий.*

Есть и еще одно дополнительное улучшение, насчет которого мы до сих пор не уверены, является ли оно «фичей», так как подобных возможностей в прошлом мы не наблюдали. В течение 2018 года мы осознали, что в определенных ситуациях оператор автономной системы должен быть в состоянии активно противодействовать манипуляции AS_PATH со стороны упорного атакующего. Это достаточно сложный, в том числе и этический, вопрос, ведь определенные шаги могут быть предприняты для обращения любого доброго начинания во вред но, в некоторых ситуациях, просто нет способа остановить потерю данных и растущую угрозу раскрытия конфиденциальности персональных данных пользователей, в лучшем случае. Мы до сих пор оцениваем как именно, кому конкретно и основываясь на каких требованиях мы готовы давать такую возможность, возможно в ближайшем будущем предоставив подтвержденным пользователям Радара доступ на специальную страницу, закрытую авторизацией от посторонних людей и доступную только проверенным владельцам соответствующих автономных систем.

Пользователи также запросили опцию активного контр-перехвата внутри нашего сервиса фильтрации, почти одновременно с теми, кто пользуется инструментом мониторинга BGP под названием Qrator.Radar. Основная причина, по которой большинство разработчиков никогда не думало и продолжает игнорировать проблемы подобные DDoS, а теперь и перехваты трафика, спуфы и прочее заключается в окончании «эры доверия». Прямо сейчас мы находимся в самом её центре, и нам необходимо приложить значительные усилия к тому, чтоб умные люди наконец начали задумываться и о том, как отдельный протокол поведет себя в ситуации стресса и напряжения, а также о том, что на каждое доброе намерение найдется как минимум несколько злых. Повторим, в попытке «исправить вещи» важно не создать новых проблем, вот почему наша компания продолжает участвовать в IETF — мы считаем, что только широкая дискуссия внутри профессионального сообщества может помочь решить проблемы, один в этом поле — не воин.

Устойчивость национальных сегментов интернета



В то время как отдельные страны могут перемещаться вверх и вниз по рейтингу, общая картина не претерпела существенных изменений с 2017 года. В прошлом году среднее значение отказа по миру составляло 41%, в 2018 оно снизилось на 3% до 38% с небольшим. Количество стран, снизивших зависимость от одной AS до менее 10% (что является признаком высокой отказоустойчивости) увеличилось на единицу до 30.

Еще одним заметным изменением стало значительное повышение надежности интернета в небольших странах Южной Азии и Африки. Эти

регионы по-прежнему развиваются, но значительное улучшение разнообразия на рынке IP-транзита является признаком ускорения прогресса.

Повышение надежности связности Сингапура объясняется его позицией среди азиатских тигров — наиболее быстрорастущих экономик региона. Гонконг и Сингапур поменялись местами на основе 2%-го изменения индекса.

Это соревнование ожесточено в верхней части рейтинга устойчивости, где позиции расположены достаточно плотно в процентном соотношении.

Считается, что если технология хорошо работает в IPv4, её можно легко портировать в IPv6. Это ошибочное предположение может быть структурной проблемой всего процесса разработки IPv6.

Измерение глобальной надежности между двумя версиями протокола не так легко как может показаться. Для поддержания глобальной связности в IPv4, любой и единственный путь до Tier-1 провайдера будет достаточен. Но в IPv6 это может быть не так. Из-за продолжающихся пиринговых войн между несколькими провайдерами верхнего уровня в IPv6 они не все связаны друг с другом. По-меньшей мере две пары провайдеров решили разорвать пиринговые отношения (“de-peer”) в IPv6: Cogent (AS174) и Hurricane Electric (AS6939), Deutsche Telekom (AS3320) и Verizon US (AS701). Эти телекоммуникационные компании могут иметь разнообразные причины для своих конфликтов, но если сеть подключена только к одной их стороне, она не будет иметь полноценной связности в IPv6. Это также влияет на надежность интернет-провайдера с несколькими апстримами — отказ одного может привести к проблемам со связностью.

Общее сравнение IPv4 и IPv6 в случае единственного отказа показывает, что у 86% национальных сегментов IPv4 связность намного выше.

Важным открытием в мире IPv6 является то, что многие интернет-провайдеры не имеют надлежащей связности даже в нормальных условиях — без каких-либо сбоев. Например, в США это относится к примерно

10% всех AS, поддерживающих IPv6, а в Китае ситуация еще хуже, так как China Telecom (AS4134) получает глобальную связность только от одного провайдера — Hurricane Electric.

Глубокое погружение с ботами

ЧЕМ РАЗЛИЧАЮТСЯ БОТЫ

DDOS БОТЫ		СКАНИРУЮЩИЕ / КЛИКАЮЩИЕ / КОММЕНТИРУЮЩИЕ БОТЫ
Косвенные Нематериальные	**ВЫГОДЫ АТАКУЮЩИХ:**	Прямая прибыль Девальвация данных Девальвация вклада пользователей
Исчерпание ресурса центрального процессора Оперативной памяти Канальной емкости сетевого подключения Диска	**ЦЕЛИ:**	Сканирование / копирование данных Ввод данных Совершение действий (кликов/нажатий) Формирование некорректных статистических данных
Нулевая/низкая стоимость Уровень расходов 0-30%	**ОПЕРАЦИОННЫЕ ИЗДЕРЖКИ:**	Средняя/высокая стоимость Уровень расходов 30-100%
Высокая частота запросов Атакуют болевые места	**ПОВЕДЕНИЕ:**	Низкая частота запросов Мимикрия под пути легитимных пользователей

Многие компании стремятся получить защиту от ботов и, что неудивительно, мы увидели большое количество разнообразных групп профессионалов работающих над различными областями данной проблематики в 2018 году. Что нам кажется отдельно интересным, так это то, что большая часть компаний, формирующих подобный спрос, никогда не испытывала целенаправленной DDoS-атаки, по-меньшей мере типичной, направленной на исчерпание конечных ресурсов, таких как память, процессор или канал сетевого подключения. Они боятся ботов, но не могут отличить их от легитимных пользователей или определить, что же именно они делают. Большинство источников таких обращений хотят избавиться от ощущения, что к ним на страницы приходят не живые люди.

Проблематика ботов-сканеров и многих других подвидов заключается в очень важной экономической компоненте. Если 30% трафика нелегитимны и происходят от нежелательных источников, то 30% затрат на поддержку такого трафика оказываются выброшены в мусор, по логике расходов. Сегодня можно рассматривать подобное как неизбежный «налог интернета» на бизнес. Это число практически невозможности свести к нулю, но владельцы бизнеса по возможности хотят видеть данный процент как можно меньшим.

Идентификация становится крайне серьезной проблемой и задачей в современном интернете, так как самые продвинутые боты даже не пытаются изображать человека — они им управляют и находятся в одном с ним пространстве, похожим на паразитов образом. Мы повторяли в течение уже длительного времени что любая информация, доступная публично, без аутентификации и авторизации есть и, в конечном итоге, закончит свое существование в виде общественного достояния — никто не может предотвратить это.

Рассматривая данную проблематику, мы сконцентрировались на вопросах идентификации и управления ботами. Однако, на наш взгляд широкий спектр работы куда более интересен — мы живем в эпоху, когда

уже невозможно узнать, почему тот или иной клиент запрашивает что-то у сервера. Вы все верно прочитали — в конечном итоге любой бизнес хочет знать, что потребитель пришел за покупкой, ведь это цель его, бизнеса, существования. Поэтому некоторые компании хотят взглянуть вглубь того, кто и что запрашивает у их серверов — есть ли за запросом реальный человек.

Неудивительно, в итоге, что часто владельцы бизнеса узнают о том, что значительная доля трафика их веб сайта сгенерирована роботами, а никакими не покупателями.

Автоматизированные человеческий особи, которых мы уже упоминали в ином контексте, могут быть нацелены на куда более специфические сетевые ресурсы пользуясь вещами почти незаметными, такими как расширения для браузера. Мы уже знаем, что очень многие расширения, которые пока сложно назвать «вредоносными» существуют исключительно с целью сбора и анализа поведения реального пользователя. А ведь есть и совсем другие вещи — там, где автоматика не может пройти выставленное перед ней заграждение, появляются люди с модификациями браузеров и совершают все те же простые действия, возможно, лишь чуть дороже для организаторов. К тому же ряд задач, таких как манипуляции рекламой и кликфрод гораздо эффективнее выполняются с реальным человеком перед экраном. Только представьте, что может произойти, если кто-то найдет хороший способ усилить все еще и машинным обучением, в нужном участке данной цепи.

Парсеры и сканеры, являющиеся частью широкой проблематики ботов, вышли на наш горизонт только в 2018 году и, в первую очередь, благодаря нашим потребителям, сообщившим нам о собственном опыте и предоставивших возможность глубже изучить и проанализировать то, что происходило на их сетевых ресурсах. Такие боты могут быть даже не видны на уровне стандартных метрик, таких как средняя используемая сетевая полоса или загрузка центрального процессора сервера. В настоящий момент Qrator Labs тестирует разнообразные подходы,

но очевидно одно — наши потребители хотят, чтобы вредоносные по их мнению боты были заблокированы на первом же запросе к серверу.

Во время эпидемии парсинга, которую мы наблюдали в России и СНГ всю вторую половину 2018 года, стало очевидно, что боты далеко продвинулись в вопросах шифрования. Один запрос в минуту — это вполне нормальная интенсивность для бота, которую очень сложно заметить без анализа запросов и исходящего трафика ответов. По нашему скромному мнению, только потребитель вправе решать, что делать с любым нежелательным источником запросов после анализа и маркировки трафика. Блокировать, пропустить или обмануть — решать не нам.

Тем не менее, у чисто автоматических решений, или как мы их привыкли называть — «ботов», существуют определенные трудности во взаимодействии. Если вы уверены, что именно бот сгенерировал нежелательный и вполне специфический запрос, первая вещь, которую захочет сделать большинство - заблокировать его, не отвечая от сервера. Тем не менее, мы пришли к выводу, что подобный подход бессмысленен, ибо дает слишком много обратной связи как самому боту, так и его создателю и стимулирует искать обходной путь. Если боты не пытаются вывести сервис из рабочего состояния, в общем и целом мы советуем не проповедовать такой подход - в результате игры в кошки-мышки достаточно целеустремленный злоумышленник почти всегда обойдет вас в погоне за целью, какой бы она ни была.

Это же является причиной, по которой Qrator Labs приняла подход маркировки вредоносного, равно как и всего трафика в общем, для того чтобы предоставить владельцу приложения максимум данных и возможностей для принятия взвешенного решения, рассмотрев возможные последствия для пользователей и бизнес-целей. Одним из хороших примеров, иллюстрирующих возможные последствия, являются блокировщики рекламы. Большая часть современной рекламы в интернете представлена именно в форме скриптов, блокируя которые вы совершенно не обязательно заблокируете именно рекламу, а не, допустим, javascript-проверку сервиса защиты от DDoS. Легко представить, куда

может завести эта тропа, в конечном итоге выливаясь в снижение прибыли интернет бизнеса.

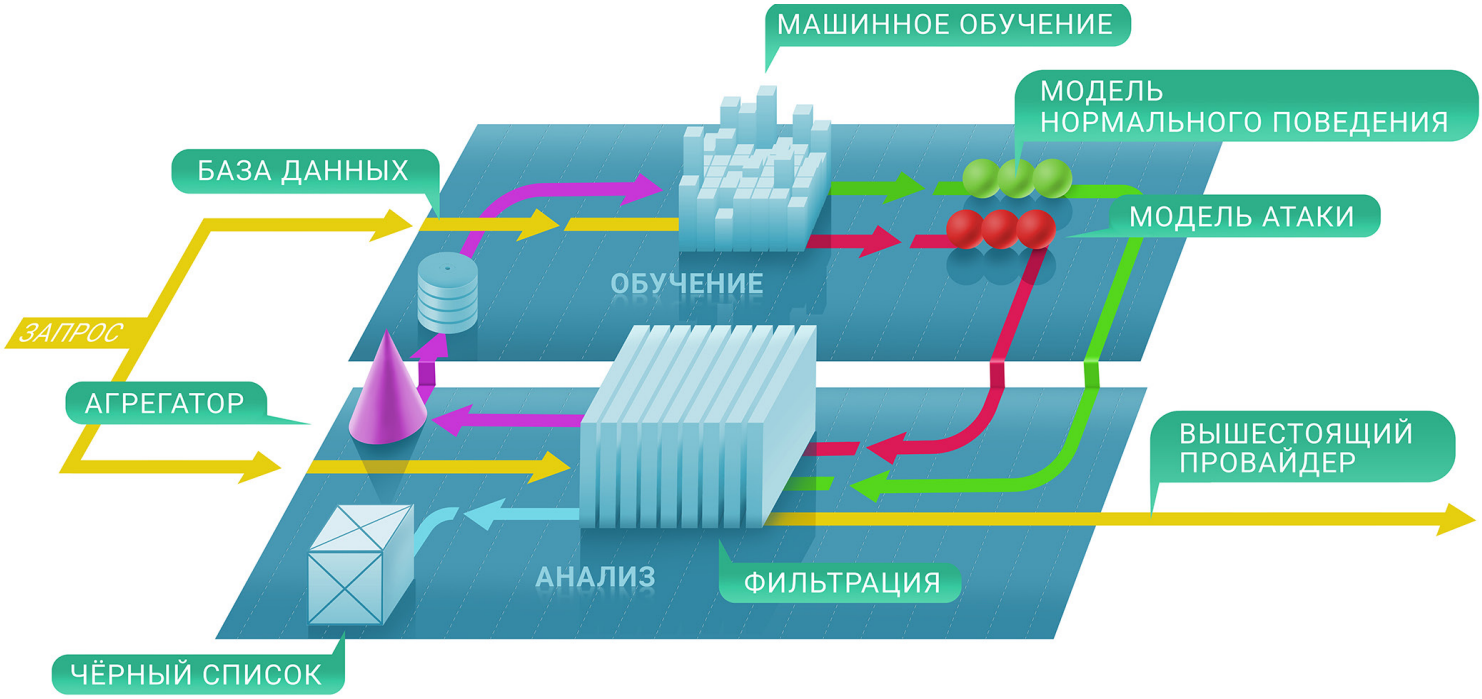
Когда атакующие блокируются и получаются необходимую им обратную связь, ничто не мешает им адаптироваться, учиться и атаковать снова. Технологии Qrator Labs построены вокруг простой философии того, что предоставлять роботам обратную связь не обязательно - нужно ни блокировать, ни пропускать их, но просто детектировать и маркировать. После того, как подобная маркировка сделана и мы уверены в ее точности, правильно задать следующий вопрос: «Что им нужно?» и «Почему они заинтересованы именно в этом?» Возможно, достаточно лишь слегка изменить контент веб страницы так, что ни один живой человек не почувствует разницы, но реальность бота перевернется с ног на голову? Если это парсеры — то возможно, что определенный процент данных окажется некорректным и фальшивым, но это в любом случае выведет защиту из поиска бинарных нуля или единицы и даст то, что действительно необходимо — время.

Обсуждая данную проблематику на протяжении всего 2018 года мы назвали атаки, подобные описанным, атаками на бизнес-метрики. Веб сайт, приложение и сервер могут работать просто замечательно, а ни один пользователь не будет жаловаться, но вы все равно что-то чувствуете… вроде падения CPA от рекламы, которую вы берете для размещения на программатик-платформе, толкая рекламодателей в сторону ее, даже не ваших, конкурентов.

Снижение поощрения атакующего — единственный способ противодействия. Попытка остановить ботов не принесет ничего, кроме потраченных времени и средств. Если что угодно кликает на то, что дает вам прибыль — отмените эти клики; если вас парсят, вы можете включить слой «фальшивой» информации, через которую с легкостью пройдет обычный, любопытный, пользователь в поисках корректной и достоверной информации.

Clickhouse

Двухуровневый фильтр с машинным обучением



На высоком уровне сервис фильтрации Qrator состоит из двух уровней: на первом мы незамедлительно оцениваем, если определенный запрос является злонамеренным с помощью проверок с сохранением состояния и без и, на втором, принимаем решение о том, задержать ли источник в черном списке и на какой срок. Получающийся в итоге черный список может быть представлен в виде уникальной таблицы IP-адресов.

На первом этапе данного процесса мы задействуем техники машинного обучения для того, чтобы лучше понимать естественные уровни и характеристики трафика для каждого ресурса в отдельности, так как каждый параметры защиты каждого отдельного сервиса настраиваются индивидуально на базе собираемых нами метрик.

Здесь в дело вступает Clickhouse. Для того чтобы лучше понять, почему определенный IP-адрес был заблокирован от общения с ресурсом, нам нужно проследить весь путь машинного обучения вплоть до базы данных Clickhouse. Она работает очень быстро с большими кусками данных (представьте себе DDoS-атаку интенсивностью 500 Гбит/сек и продолжающуюся несколько часов чистого времени вне пауз) и хранит их в удобном виде для фреймворка машинного обучения, используемого в Qrator Labs. Больше логов и больше сохраненного трафика DDoS-атак ведут к точным результатам от наших моделей, помогающих осуществлять тонкую настройку сервиса фильтрации в реальном времени, под наиболее серьезными атаками.

Мы используем Clickhouse DB для хранения всех логов нелегитимного трафика атак и паттернов поведения ботов. Данное, специализированное, решение было выбрано нами из-за высокого потенциала хранения массивных датасетов в стиле классической базы данных с целью последующей обработки. Анализ этих данных используется в том числе для построения паттернов DDoS-атак, помогая машинному обучению постоянно улучшать наши алгоритмы фильтрации трафика.

Значительным преимуществом Clickhouse, в сравнении с другими базами данных, является то, что ей не нужно считывать целую строковую переменную данных — она может взять гораздо меньший, строго необходимый, сегмент, если вы храните все по рекомендациям. И это работает, быстро!

Интернет Вещей

IoT как индустрия не совершил значительного прогресса в сторону улучшения своей общей безопасности за прошедший год. На деле, исследователи обнаружили новый класс индустриального оборудования, которое сейчас массово подключается к сетям и обладает значительными уязвимостями. Недавние открытия относительно протокола CoAP свидетельствуют, что подобных незакрытых точек эксплуатации может быть очень много. Возможно, не в протоколе, как таковом — иногда достаточно клиентского приложения с ошибками в коде. Результатом чаще всего служит непредсказуемость и неконтролируемость.

Точность нашего прошлого предсказания относительно IoT позволяет поделиться тем, чего мы ожидаем и от будущего данной индустрии. В IoT пока нет буквы «S» для «security», что привлечет еще немало проблем и создаст новые и населенные ботнеты. Амплификаторы на базе IoT являются очевидным дальнейшим развитием идеи уязвимых сервисов. Более того, домашние подключенные устройства представляют собой лишь статистическую верхушку этого айсберга, под уровнем воды которого находятся другие группы «подключенных устройств», сообщающихся с помощью протоколов, выбранных по непредсказуемой логике и, естественно, не обеспечивающими достаточную защиту устройств.

Незакрытые уязвимости в индустриальном интернете вещей будут эксплуатироваться и дальше при условии неизменности текущего подхода к разработке, опирающегося на спешку, тоннельное зрение или жадность, за яркими исключениями в виде стандарта TLS 1.3.

Касательно TLS 1.3 — очевидно, что обновленная версия протокола уже встретила воодушевленную поддержку, так как никого в современном мире не нужно убеждать в необходимости крепкого шифрования.

Заключение

На протяжении уже длительного времени мы живем в мире мультифакторных атак, эксплуатирующих атакующие возможности сразу нескольких протоколов для выведения цели из работоспособного состояния.

Цифровая гигиена и актуальные меры безопасности должны и, на самом деле, покрывают порядка 99% существующих рисков, которые может встретить обыкновенный пользователь, за исключением лишь, пожалуй, узкоспециализированных атак на конкретные цели.

С другой стороны, в современном интернете существуют акулы, способные перекусить доступность целых государств. Это не касается BGP, где возможно погасить лишь некоторые точки на любой карте, которую злоумышленник захочет нарисовать.

Уровень знаний, касаемый сетевой безопасности продолжает расти. Тем не менее, если вы взглянете на цифры связанные с количеством амплификаторов в сетях или поищите возможности подделки запросов — количество уязвимых сервисов и серверов не падает. Ежедневный темп приобретения молодыми людьми знаний, касаемых навыков программирования и управления компьютерными сетями не соответствует времени, необходимому для получения соответствующего опыта в реальной жизни. Уверенность в том, что с новыми продуктами не выходят новые уязвимости приобретается долго, а главное - больно.

Одним из наиболее удивительных открытий прошедшего года было то, что большинство людей ожидает от новых технологий существенно больше, чем те способны предоставить. Так было не всегда, однако прямо сейчас мы наблюдаем растущую тенденцию людей «требовать большего» вне зависимости от возможностей софта и тем более, железа. Это ведет нас в мир достаточно извращенных маркетинговых кампаний. Но люди, тем не менее, продолжают «покупать обещания» а компании, в свою очередь, чувствуют себя обязанными их исполнить.

Возможно это и есть суть прогресса и эволюции. Сейчас многие расстраиваются из-за факта не получения «гарантированного» и того, за что были уплачены средства. Из невозможности «полностью» купить устройство у производителя и растут многие из современных проблем, в обратную же сторону стоимость «бесплатных» сервисов может получаться просто баснословной, если рассмотреть кумулятивную стоимость данных, которые получает от пользователя крупная социальная сеть, не требующая оплаты.

Консьюмеризм говорит нам, что если мы очень сильно чего то хотим, то, в конечном счете, заплатим собственными жизнями. Действительно ли нам нужны подобные продукты и сервисы, улучшающие себя только для того, чтобы предлагать нам «улучшенные предложения» на основе тех данных, что собрали о нас, нравится нам это или нет? Тем не менее, это судя по всему и есть ближайшее будущее, как нам показали случаи с Equifax и Cambridge Analytica совсем недавно. Неудивительно, если впереди нас ждет «большой взрыв» использования персональных и прочих, касающихся индивидуальной жизни каждого, данных.

Спустя десять лет работы мы не поменяли ключевые устои об архитектуре интернета. Это причина, по которой Qrator Labs продолжает развивать BGP anycast сеть фильтрации с возможностью обработки зашифрованного трафика именно в таком виде, избегая капчи и других неожиданных для легитимного пользователя препятствий.

Наблюдая за тем, что продолжает происходить с экспертами в области кибербезопасности, равно как и компаниями в данном поле, мы еще раз хотим повторить очевидное: наивный, простой и быстрый подход неприменим.

Поэтому у Qrator Labs нет сотен или даже десятков точек присутствия, сравнимых с CDN. Управляя меньшим количеством центров фильтрации, каждый из которых подключен к интернет-провайдерам классом не ниже Tier-1, мы добиваемся настоящей децентрализации. По этой же причине мы не пытаемся строить свой собственный файрвол, представ-

ляющий собой задачу совершенно иного уровня, нежели та, над которой мы работаем — связностью.

На протяжении многих лет мы говорили, что в конечном итоге не сработает ни капча, ни javascript-проверка и вот мы находимся в 2019 году, когда нейросети стали высокоэффективны в решении первых, а вторые вообще никогда не представляли собой проблему для атакующего с мозгом.

Хотелось бы отметить еще одно интересное изменение на границе времени: DDoS-атаки долгое время были серьезной проблемой лишь для ограниченного числа бизнес отраслей, как правило тех, где деньги покачиваются на поверхности: электронная коммерция, торговля и биржа, банкинг и платежные системы. Но с продолжающимся развитием интернета, мы наблюдаем DDoS-атаки увеличенной интенсивности и частоты в абсолютно всех частях интернета. Эпоха DDoS началась с определенного порога пропускной способности домашних роутеров и, неудивительно, что с появлением микрочипа в каждой физической вещи вокруг ландшафт атак начал стремительно меняться.

Тот, кто либо ожидает окончания развития данной тенденции, скорее всего неправ. Также, как неправы и мы, написав так много предсказаний. Никто не может утверждать наверняка, как именно интернет будет развиваться и распространять собственное влияние в ближайшие годы, но оглядываясь на то, что мы видели, понятно одно — все умножится. В 2020 году количество подключенных к сети устройств должно превысить 30 миллиардов, не говоря о том простом факте, что роботы уже давно генерируют гораздо больше трафика, чем люди. Совсем скоро нам придется решать, что делать со всем этим «интеллектом», искусственным или нет, так как мы до сих пор существуем в мире где человеческая особь ответственна за свои поступки, правильные или нет.

2018 год был годом возможностей для темной стороны. Мы увидели и рост атак, с одновременным их усложнением и увеличением как объема в сетевых терминах, так и частоты. Злодеи получили мощные инструменты и потратили немало времени на их изучение, в то время, как хорошие парни не делали ничего более, нежели наблюдали за их прогрессом. Мы искренне надеемся, что в текущем году изменится хоть что то, по меньшей мере в наиболее болезненных местах.

QRATOR LABS

www.qrator.net ООО “Эйч-Эль-Эль”

Юридический адрес:
Россия, 121205, г. Москва,
территория инновационного центра
«Сколково», Большой бульвар, д. 42,
стр. 1, этаж 4, пом. 1660

Фактический адрес:
Россия, 123290, г. Москва, 1-й
Магистральный тупик, д. 5А, блок D,
офис 304

Тех. поддержка: +7 800 333 35 22 (с
территории РФ)

mail@qrator.net
press@qrator.net