QRATOR LABS

wallarm

Тренды 2015 года в области интернет-безопасности в России и в мире

Основные угрозы:

DDoS-атаки и взлом веб-приложений

Январь 2016

Отчет описывает основные тенденции и проблемы за 2015 год в области доступности и безопасности корпоративных сайтов, связанные с угрозами DDoS и “взлома”. Отчёт подготовлен специалистами компаний Qrator Labs и Wallarm на основе мониторинга ситуации в отрасли (как в России, так и в мире), а также на основе статистики, собранной по своим клиентам в 2015 году. Также использованы данные исследований независимых компаний, сделанных по заказу Qrator Labs.

В числе клиентов Qrator Labs и Wallarm — значительное количество компаний из различных отраслей, что позволяет делать выводы о состоянии в сфере интернет-безопасности в целом.

Также в отчете использована информация сервиса компании Qrator Labs — Radar.Qrator.net. Это уникальная система глобального мониторинга интернета, данные которой поставляются как сервис провайдерам и телеком-специалистам. Эксперты Qrator Labs и Wallarm являются постоянными участниками отраслевых международных конференций, их выступления и компетенции высоко оцениваются профессионалами рынка ИТ и телекоммуникаций во всем мире.

ОГЛАВЛЕНИЕ

КЛЮЧЕВЫЕ НАБЛЮДЕНИЯ 2015 ГОДА

1. Сложность атак растет. Хакеры комбинируют различные подходы, прибегая одновременно к DDoS-атакам и атакам на уязвимости приложений.

Главное наблюдение 2015 года — понижение пиковых скоростей DDoS-атак, что, впрочем, не придает оптимизма — поскольку компенсируется ростом их сложности.
Если ранее злоумышленники, как правило, ограничивались одним видом DDoS, то сегодня атаки носят мультивекторный характер (то есть могут быть направлены сразу на несколько сетевых уровней и элементов инфраструктуры), становятся комплексными.
Хакеры наращивают сложность и объединяют DDoS с “взломом”, т.е. атаками на уязвимости приложения. В 84% случаев атака DDoS сопровождается попытками взлома сайта. Таким образом, средства, обеспечивающие только защиту от DDoS, сегодня оказываются недостаточными для обеспечения доступности интернет-ресурса.
Тем не менее, компаниям с комплексным подходом к организации системы противодействия атакам повышенной сложности удается нейтрализовать данные риски вполне успешно (см. кейс платёжного сервиса QIWI ниже в главе “Комбинированные атаки”).

2. Минимальная стоимость и простота реализации атак.

Устроить DDoS атаку еще никогда не было так дешево: это мероприятие сегодня стоит от $5 в час. Как результат — по сравнению с 2014 годом среднее количество атак на один сайт в 2015 году увеличилось в два раза. Злоумышленники активно используют облачных провайдеров для быстрого получения ресурсов, в том числе бесплатно, с использованием бонусных и триальных программ.
Схожая картина с хакерскими атаками. Благодаря доступности инструментов для поиска и эксплуатации уязвимостей, успешные атаки во многих случаях уже не требуют серьезной экспертизы: за атаками все чаще стоят не профессиональные хакеры, а “середнячки”, которые ищут и эксплуатируют известные уязвимости готовыми инструментами, руководствуясь статьями и видео инструкциями.

3. Основным вызовом с точки зрения защиты от DDoS стали атаки на уровне приложений (L7).

В 2015 году участились атаки на уровень приложений (L7), которые часто сопровождают DDoS-атаки на канальный уровень (L2). Защита от DDoS-атак на уровне приложений — наиболее сложный случай, требующий максимальной экспертизы и скорости реакции на изменение вектора атаки. При этом хакеры используют интеллектуальные автоматизированные средства, которые исключают возможность противодействия отдельным специалистом на стороне обороны. Сегодня можно говорить о том, что эффективно противостоят DDoS только системы, работающие на основе алгоритмов машинного обучения. Системы, работающие под контролем человека-оператора не в состоянии справиться с современными многовекторными атаками в режиме реального времени без существенных перерывов в обслуживании пользовательского трафика.

4. Наиболее частым вектором хакерских атак, направленных на “взлом” сайта по-прежнему являются уязвимости типа “SQL-инъекции”. Массовые атаки перебора стали новым вызовом.

Наиболее популярными атаками по-прежнему являются атаки на уязвимости типа SQL-инъекций (37,75% от общего числа атак), когда из-за специальным образом сформированного запроса можно выполнить произвольный запрос к базе данных приложения. Простые в реализации за счет автоматизированных инструментов, они открывают злоумышленникам прямой доступ к базам данных ресурса. Для обхода защитных решений все чаще используют различные способы обфускации (маскировки) вредоносных запросов, что оказывается эффективным в случае WAF’ов, не учитывающих структуру и специфику приложений.

В прошедшем году серьезно увеличилось количество атак перебора, в том числе направленных на перебор паролей (21,85%). В России это особенно коснулось интернет-ритейлеров, где злоумышленники в массовых количествах получали доступ к учетным записям, используя базы “логин-пароль”, утекшие из других ресурсов.

5. Различные группы используют техники массового сканирования интернета.

Массовые сканирования всего интернета перестали быть уделом Google и других поисковых гигантов, и теперь с различными целями осуществляются разными группами людей. Злоумышленники пытаются найти веб-ресурсы, маршрутизаторы, устройства IoT с известными уязвимостями для быстрого и автоматизированного захвата контроля. Эти ресурсы в дальнейшем активно используются для реализации мощных DDoS-атак, анонимизации, майнинга криптовалют и т.д.
“Главный итог 2015 года заключается в том, что в отрасли созрело понимание — сегодня стала невозможной защита собственными средствами. Для противодействия сложным комплексным DDoS-атакам и взломам необходимо использовать профессиональные решения, которые постоянно обновляются и используют алгоритмы машинного обучения”, — комментирует Александр Лямин, глава Qrator Labs.

“Главный итог 2015 года заключается в том, что в отрасли созрело понимание — сегодня стала невозможной защита собственными средствами. Для противодействия сложным комплексным DDoS-атакам и взломам необходимо использовать профессиональные решения, которые постоянно обновляются и используют алгоритмы машинного обучения”

ГЛАВА I. АНАЛИТИКА ПО DDOS-АТАКАМ

DDoS-атаки по-прежнему применяются, как средство нечестной конкурентной борьбы. Их популярность растёт с каждым годом. 2015-й год не стал исключением – и без того пессимистичный прогноз Qrator Labs был превзойдён. Компания прогнозировала, что рост числа атак составит 25%, но на практике показатель увеличился на 100%.

+ 100% ЗА ГОД

СРЕДНЕЕ ЧИСЛО АТАК НА ОДИН САЙТ
ВЫРОСЛО В ДВА РАЗА

Никогда ещё не было так просто и дёшево устроить DDoS – это мероприятие сегодня стоит от $5 в час. Это примерная стоимость аренды инфраструктуры, необходимой для организации нападения.

Как и раньше, главная мишень злоумышленников — компании из e-commerce, банки, социальные сети. Также в 2015 году в ряду самых частых целей оказались туристические компании и агентства недвижимости, что связано с политическими причинами и экономическим давлением.

По данным исследования, проведённого аналитическим агентством 42Future по заказу Qrator Labs, в конце 2015 года, 25% крупнейших ритейлеров сталкивались с DDoS за последний год. Количество атак на сайты ритейлеров возросло примерно на 70% по сравнению с 2014 годом.

Как сообщили 80% опрошенных, по их мнению атаки в первую очередь заказывают конкуренты. Вторая причина организации атак – вымогательство путём шантажа; так ответили 45% опрошенных.

СРЕДНЕЕ КОЛИЧЕСТВО АТАК DDOS НА КЛИЕНТА В МЕСЯЦ ЗА 2014 - 2015

	Amplified DDoS	All DDoS
Интернет-магазины	25%	70%
Социальные сети	73%	159%
Купоны	-25%	-10%
Forex	-53%	-62%
Платежные системы	74%	37%
Игры	42%	110%
Торговые площадки	-15%	-18%
Банки	121%	61%
СМИ	-29%	17%
Агрегаторы контента	-43%	-28%

	Amplified DDoS	All DDoS
Промо сайты:		
Агентства недвижимости	113%	144%
Рекламные агентства	-40%	-16%
Микрофинансы	-30%	-36%
Турфирмы	-1%	145%
Такси	116%	108%
Медицина	-20%	-54%
Остальные промо-сайты	-58%	-34%

ТРЕНД 1. АТАКИ ТИПА AMPLIFICATION

В 2015 году заявила о себе группировка Armada, которая шантажировала компании, требуя выкуп в биткоинах под угрозой DDoS-атаки. Множество таких инцидентов произошло в разных странах мира, и они получили широкое освещение в прессе. Злоумышленников не удалось задержать, и группировка проявляла активность вплоть до декабря 2015 года.
Но осталось невыясненным: во всех ли известных случаях шантажа действовала одна и та же группа злоумышленников? Часто письма с угрозами приходили одновременно в несколько компаний из разных стран.

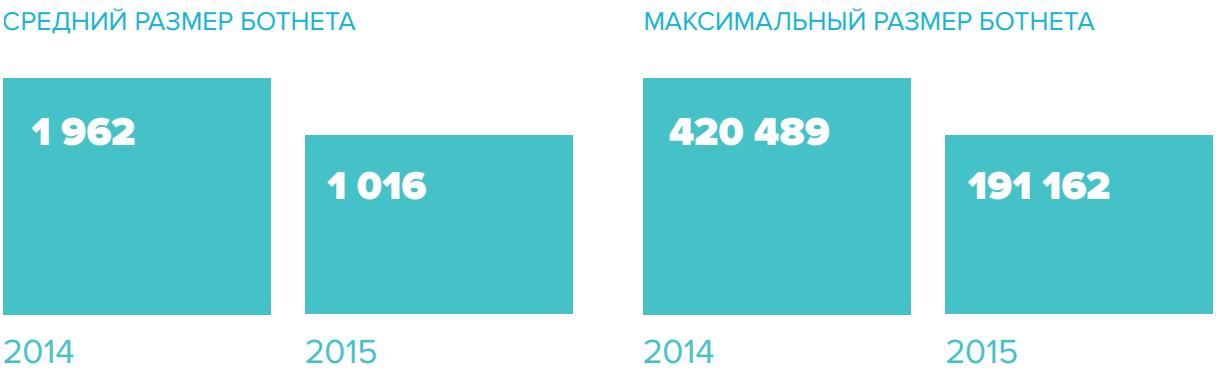
Высока вероятность того, что у первой Armada появились подражатели, действующие по тому же сценарию и использующие то же имя. Armada превратилась в явление.
Это означает, что даже если одну группу киберпреступников удастся взять под стражу, само явление и угроза, которую оно порождает, не исчезнут.

Схема работает: есть компании, которые решаются заплатить шантажистам. О некоторых подобных случаях сообщала пресса, но многие остались «за кадром» — однако о них известно в профессиональном сообществе.

К сожалению, в таких случаях даже выплата выкупа не снимает рисков – известны случаи, когда после получения денег сайт всё равно подвергался атаке.
Те же компании, которые решились заплатить вымогателям, фактически инвестируют в их инфраструктуру, используемую для последующих нападений. То есть напрямую поддерживают бизнес злоумышленников.

Противодействовать данной угрозе можно только лишь с помощью средств, которые специально разработаны для этих целей и постоянно совершенствуются, поскольку методы злоумышленников также постоянно меняются.

Armada использует атаки с использованием техники амплификации (атаки типа Amplification) – это яркая иллюстрация тренда 2015 года. Именно такие нападения стали наиболее распространенным явлением в 2014 и продолжают этот тренд в 2015 году. Атака типа Amplification осуществляется следующим образом: на сервер, содержащий уязвимость, отправляется запрос, который этим сервером многократно тиражируется и направляется на веб-ресурс жертвы. В качестве серверов, поневоле участвующих в таких атаках, могут использоваться DNS-, NTP-, SSDP-серверы и другие.



Данная инфографика демонстрирует, что в 2015 году размер ботнетов, задействованных в DDoS-атаках уменьшился. Вместе с тем увеличилось число атак класса Spoofed, в категорию которых попадают атаки типа Amplification.

При атаках типа Amplification ботнеты для генерации первой волны мусорного трафика используются редко. Обычно для этих целей арендуются серверы, либо используется чужие взломанные. Даже в случае аренды организация атаки обходится недорого – ведь злоумышленнику достаточно генерировать запросы со скоростью в несколько Гбит/сек и направлять их на сервер с уязвимостью, который увеличит эту скорость на несколько порядков.

100

СРЕДНЯЯ ВЕЛИЧИНА МУЛЬТИПЛИКАТОРА ПРИ АТАКАХ ТИПА AMPLIFICATION

30-40 ГБИТ/СЕК

МИНИМАЛЬНАЯ СКОРОСТЬ АТАК ТИПА AMPLIFICATION В 2015 ГОДУ

Противодействовать такого рода атакам «вручную» уже невозможно, их слишком много и это дорого. Фактические затраты злоумышленника на инфраструктуру, необходимую для организации атаки в несколько десятков раз меньше, чем требуются компании-жертве, чтобы самостоятельно нейтрализовать такую атаку.

ТРЕНД 2. КОМБИНИРОВАННЫЕ АТАКИ

L2 и L7: канальный уровень и уровень приложений

Наиболее распространенный сценарий, которому следовали компании для защиты от DDoS в 2013-2014 годах заключается в следующем:

- в случае атак на канальный уровень (когда “мусорным” трафиком исчерпывают канальную ёмкость) компании надеются на защиту, предоставляемую провайдером;
- для атак на инфраструктуру используют “самописные” или локальные решения, внедряемые на собственных серверах.

Постепенно уходят в прошлое попытки самостоятельно справиться с атаками канального уровня (L2). Ведь для этого необходимо организовать и содержать дорогой канал связи и распределенную инфраструктуру (в нескольких дата-центрах). Поэтому компании предпочитают полагаться на своих интернет-провайдеров или начинают использовать профессиональные облачные сервисы противодействия, подобные Qrator.
Но стоит ли полностью полагаться на интернет-провайдера? Летом 2015 года произошел инцидент, в результате которого от интернета было отключено пять городов в США. Сервер по конкретному IP подвергся DDoS-атаке, которая легко “забила” канал локального интернет-провайдера, который предоставлял доступ в интернет жителям и компаниям нескольких населённых пунктов.

«Уверен, что мы услышим ещё немало подобных историй. Атаки набирают скорость и становятся все более изощрёнными. Небольшие интернет-провайдеры, работающие на «последней миле» часто неспособны справиться даже с атакой средней руки. В данном случае пять городов обслуживались через канал связи ёмкостью всего лишь 10Гбит/сек. То есть канальной емкости на порядок меньше, чем типичная DDoS-атака 2015 года, хватило, чтобы полностью забить канал. Кроме того, сеть была организована с нарушением минимальных норм отказоустойчивости, так что специалисты собственной техподдержки провайдера не могли дозвониться к своему магистральному провайдеру, чтобы тот заблокировал атакуемый IP — телефония техподдержки была развёрнута на том же самом канале», — комментирует Александр Лямин, руководитель Qrator Labs.

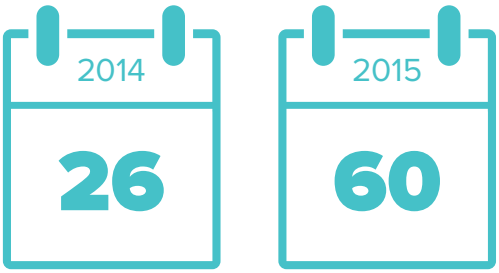
Большинство крупных и наиболее прогрессивных компаний также прекратили экспериментировать с самописными средствами и локально-инсталлированными решениями для противодействия атакам уровня приложений (L7). Атак становится слишком много и средства защиты, требующие ручного вмешательства, неэффективны. Противодействие DDoS должно происходить автоматически.

Платёжный сервис QIWI может служить хорошим примером того, как организовать эффективную систему противодействия атакам нарастающей сложности.
В 2015 году на интернет-ресурсы QIWI было произведено около 25 атак. Максимальная скорость достигала 16 Гб/сек. Почти все атаки были направлены на HTTPS-сервисы, обслуживающие зашифрованные транзакции пользователей сервиса.

15% атак сопровождались попытками взлома.

Компания использует сеть фильтрации трафика Qrator и защиту от взлома WAF от Wallarm. Специалисты QIWI отказались от организации системы противодействия собственными силами. И вот почему:

“Когда через платежную систему проходят миллионы транзакций в день, доступность ресурсов становится критической частью бизнеса. В сегодняшних реалиях, когда новой нормой стали атаки в несколько сот гигабит в секунду, для защиты от DDoS нужны правильные инструменты. Компания Qrator Labs стала надежным партнером, который помог обеспечить нужный бизнесу SLA, проявив гибкость в работе с нашей непростой веб-инфраструктурой. Wallarm мы отдельно используем для защиты веб-приложений и наших многочисленных API. Особенно радует, что мы смогли интегрировать оба решения с нашим центром реагирования на инциденты и системой мониторинга.”, — говорит Кирилл Ермаков, CISO QIWI.



СРЕДНЕЕ КОЛИЧЕСТВО DDOS- АТАК В СУТКИ, НЕЙТРАЛИЗУЕМЫХ СЕТЬЮ QRATOR LABS

Появились способы многократно увеличить плечо атаки L7 за счет использования рефлекторов — серверов с «дырами» в защите, которые умножают и направляют трафик на сайт жертвы в виде полностью корректных запросов к приложению.

В 2015 году Qrator Labs наблюдал множество атак L7, построенных на эксплуатации уязвимости WordPress Pingback. В интернете функционируют сотни тысяч серверов с этой «дырой», которые могут стать рефлекторами фейковых запросов на веб-приложения жертвы.

В конце декабря на крупную российскую транспортную компанию была инициирована атака, в которой участвовало 3,5 тысячи серверов на WordPress. Они генерировали вредоносный трафик со скоростью 7,5 Гбит/сек в пике.

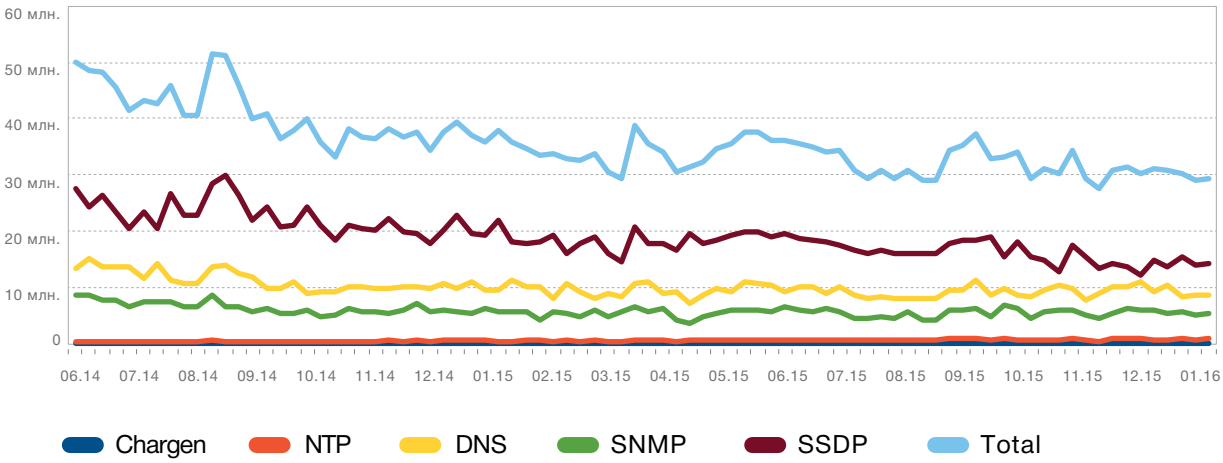
Атаки L7 теперь легко и дёшево организуются, появились способы увеличить их «плечо». От L7 больше нельзя защититься с помощью простых “доморощенных” средств. “Самолечение” в данном случае – это дорого и неэффективно.

Всё большее число веб-ресурсов используют защищённый протокол HTTPS, который подразумевает шифрацию трафика. Это действенное средство для защиты пользовательских данных от кражи. Но в случае атаки, L7 сервер, работающий на HTTPS делает зашифрованными абсолютно все запросы к приложениям, в том числе те, которые приходят от ботов. Распознать бота при L7 можно лишь по его поведению. Это значит, что в данном случае необходимо использовать средства противодействия DDoS, умеющие работать с зашифрованным трафиком. При этом зачастую обязательным требованием к провайдеру защиты является неиспользование ключей шифрования интернет-ресурса.

Комбинации амплификаторов и атак разных уровней

Согласно статистике, собранной в 2015 году, число амплификаторов медленно уменьшается. Но их всё ещё около 30 млн. Это значит, что данный тип атак будет использоваться ещё долго. К тому же появляются новые амплификаторы, которые могут использоваться для эксплуатации уязвимостей старых протоколов. Свежие примеры – RIP и QotD.

КОЛИЧЕСТВО АМПЛИФИКАТОРОВ



В стандартной атаке типа Amplification обычно используется сразу несколько амплификаторов. В 2015 году отчётливо обозначился также тренд организации комбинированных нападений: за Amplification-атакой может следовать атака на приложения (L7). Это означает, что выстраивать защиту от DDoS следует сразу на всех уровнях.

DDoS-атаки, комбинированные со взломом

Громкое освещение в прессе в 2015 году получила деятельность группировки DD4BC. Злоумышленники в погоне за наживой использовали (и продолжают это делать) самые разные средства: от DDoS до распространения троянов, взлома веб-приложений и смартфонов. Часто атаки типа DDoS киберпреступники комбинировали с хакерскими атаками на сайты. От их рук пострадало несколько финансовых организаций по всему миру. Подход DD4BC — комбинирование атак различных классов, — набирает популярность и может быть назван ярким трендом 2015 года.

Согласно подсчётам Wallarm, в 84% случаев наблюдается чередование DDoS-атак с попытками взломов сайтов.

ТРЕНД 3. ИНЦИДЕНТЫ BGP

Проблемы протокола маршрутизации BGP, на котором построен весь Интернет, известны уже несколько лет. Но ошибки, которые в нём имеются, в последние годы начинают всё чаще приводить к серьезным негативным последствиям.

Нештатные ситуации, связанные с маршрутизацией на междоменном сетевом уровне, способны повлиять на большое число хостов, сетей и даже на глобальную связность и доступность в Интернете.

Наиболее типичным видом сетевой аномалии является утечка маршрута или RouteLeak. Проблема возникает в результате анонсирования маршрута в неправильном направлении. Например, если AS (автономная система,—основная система, делающая оператора оператором) подключена к двум провайдерам, и при этом анонсирует префиксы этих провайдеров (то есть объявляет себя источником этого префикса), то весь трафик от обоих провайдеров перетечёт в сеть этой AS. Это скорее всего приведет к недоступности самой AS, а также к частичной недоступности всех сетей, оказавшихся в данном RouteLeak.

Например, в 2008 году автономная система AS36561, относящаяся к национальной сети Пакистана, присвоила себе префикс, принадлежащий Youtube и начала сбрасывать трафик, относящийся к этому префиксу. Это привело к временной недоступности YouTube.

В основном подобные инциденты возникают от невнимательности администраторов и банальных ошибок в сетевых настройках. Пока уязвимости BGP редко используются умышленно. Организовать атаку, эксплуатирующую ошибки BGP, сложно и дорого. Но в последние годы значительно возросли масштабы организованных преступных группировок (в том числе политизированных), действующих в киберпространстве. К тому же одна таргетированная успешная атака на крупный банк может окупить целый год подготовки к ней.

Поэтому в будущем могут происходить громкие инциденты безопасности, связанные с проблемами BGP.

В прошлом году был документально зафиксирован случай умышленного использования уязвимостей BGP. В августе 2015 года кибергруппа Hacking Team, сотрудничающая с правительствами разных стран, помогающая им бороться с киберпреступностью, инициировала “угон” IP-адресов (hijacking), которые ей не принадлежали. Хакеры сделали это, чтобы помочь итальянской полиции взять под контроль несколько компьютеров, за которыми велось наблюдение в рамках расследования.

Возможно, злоумышленники также используют подобные методы, но жертвы об этом не подозревают. Атаки, организованные на уровне протокола маршрутизации и сетевой инфраструктуры в целом, довольно сложно выявить.

Масштабы таких действий могут быть огромными, а разнообразие последствий весьма широким. Манипулирование BGP может позволить украсть трафик и данные, устроить DDoS, незаметно перевести пользователей на фейковый сайт популярного сервиса, чтобы получить их логины и пароли и так далее.

Ещё один свежий пример: в прошлом году оператор Telecom Malaysia по ошибке перенаправил на себя весь мировой трафик Фейсбука, с которым, конечно же, не смог справиться. Проблема возникла из-за неправильно настроенной маршрутизации. В итоге пользователи социальной сети в течение двух часов испытывали проблемы с доступом к ней.

Telecom Malaysia, фактически (хотя и не специально), устроил DoS на Фейсбук по типу “prefix hijacking” – в этом случае служебный префикс сети одного оператора начинает использоваться в сети совершенно другого оператора. В результате возникает путаница и часть пользовательских запросов может направляться по некорректному маршруту и приземляться на другой сервер. Telecom Malaysia ошибся в анонсировании 179 000 префиксов, заставив провайдеров третьего уровня проложить неправильные маршруты.

«Мы наблюдали в 2015 году перехваты сетей с помощью утечек маршрутов BGP (hijacking leaks) и множество случаев обычных утечек маршрутов, но не знаем наверняка, использовались ли они для преступных целей. Риски, связанные с уязвимостью BGP довольно высокие. Эта проблема может использоваться для реально серьёзных атак, в том числе применимых в качестве кибероружия», — говорит Александр Лямин, глава Qrator Labs.

По наблюдениям Qrator.Radar (уникальная и единственная в своём роде система глобального мониторинга интернета, инновационный облачный сервис для операторов и телеком-специалистов), число префиксов, подверженных route leaks, насчитывает десятки тысяч. А количество префиксов, замеченных в MOAS-конфликтах к концу 2015 года приблизилось к 150 тысячам. MOAS-конфликты (multiple origin AS) – анонсирование одинаковых префиксов разными источниками.

51 527

УНИКАЛЬНЫЕ ПРЕФИКСЫ AC В ROUTELEAK

144 424

УНИКАЛЬНЫЕ ПРЕФИКСЫ В MOAS (MULTIPLE ORIGIN AS) КОНФЛИКТАХ

ВЫВОДЫ И ПРОГНОЗЫ ПО DDOS НА 2016 ГОД

L7-атаки снова набирают популярность

В 2015 году мощность ботнетов упала в связи с тем, что злоумышленники переключились на атаки типа Amplification. К концу 2016 года конкуренция за амплификаторы может возрасти. Также, по мере внедрения средств противодействия данному типу атак, они будут всё чаще заменяться атаками L7 (на приложения). Именно этот тип атак станет главным трендом 2016 года. Рекомендация – подготовиться заранее и начать использовать комбинированные средства противодействия на базе технологий машинного интеллекта, поставляемые удалённо.

Всё большее количество компаний из разных отраслей переводит свои сайты на защищенную передачу данных по протоколу HTTPS. Вслед за этим хакеры уделяют всё больше внимания атакам на приложения, работающие по этому протоколу. Общее увеличение количества DDoS и стабильный ежегодный рост зашифрованного трафика (в 2015-м году он вырос в мире примерно в 2 раза) сигнализируют о том, что в 2016 году число DDoS-атак на HTTPS-сервисы вырастет соответственно.

Атаки на DNS

Прогноз Qrator Labs, сделанный в 2014 году, продолжает сбываться – атаки на инфраструктуру всё ещё редки, но их число растёт. К ним относятся в частности, атаки на DNS-серверы. Ситуации, в которых атаке подвергается сетевая инфраструктура, обычно несут разрушительные последствия, причём заметные на глобальном уровне. Так, 30 ноября и 1 декабря 2015 года были проведены атаки на корневые серверы системы DNS, причем часть из них злоумышленникам удалось вывести из строя. 14 декабря 2015 года перестали работать DNS-серверы турецкого домена верхнего уровня .tr

В январе 2016 аналогичные атаки продолжились. Целью в этот раз были DNS-серверы европейского регистратора RIPE, при этом часть атак была успешной. Число подобных инцидентов, связанных с атаками на сетевую инфраструктуру (на сервера DNS, а также атаки, связанные с ошибками BGP), будет расти в ближайшие несколько лет.

Инциденты BGP

Все более актуальной становится тема угроз доступности сайтов, которая возникает вследствие умышленных или случайных ошибок маршрутизации BGP — основополагающего протокола сети интернет. Мы прогнозируем, что в 2016 году (как и в 2015), порядка 5-10% Автономных систем (AS) провайдеров доступа в интернет будет испытывать проблемы с доступностью своих сервисов. То есть этот показатель не будет расти. Однако само число AS увеличится. Также возрастёт количество значимых инцидентов BGP, приводящих к недоступности сотен и даже тысяч сетей.

Инциденты TCP

Инфраструктура интернета активно обновляется, чтобы поддерживать постоянный рост скоростей. После 10Гб/сек становится новым стандартом скорость в 100Гб/сек. Но вместе с этим возникают проблемы с устаревшим, придуманным на заре интернета, протоколом TCP, который совершенно не рассчитан на такие скорости.

В связи с этим может возникать множество проблем, связанных с возможностью подделать пакеты, взломав поле Sequence Number и Acknowledge Number, с помощью которых стороны, обменивающиеся пакетами, различают свои TCP-соединения.

К примеру, становится возможной атака типа TCP Hijacking, когда злоумышленник превращается в “man-in-the-middle” (“человека посередине”) и пропускает через себя все пакеты, которыми обмениваются два узла. Соответственно, он может просматривать пакеты, отправлять ложные, включать в них команду сброса соединения и так далее.

“На сегодня, уязвимости в TCP вновь возвращаются в фокус интересов исследователей. Думаю что громкие случаи с их эксплуатацией мы будем наблюдать уже скоро. Возможно, уже в 2016 году. — Комментирует Александр Лямин, глава Qrator Labs. — Проблемы с TCP, базовым протоколом глобальной Сети, настолько серьёзны, если злоумышленники активно за них возьмутся, то весь Интернет затрещит по швам. Это заденет всех”.

Проблемы IoT

Серьёзную угрозу представляет собой зарождающийся мир “интернета вещей” (Internet of Things, IoT). Все устройства, подключённые к интернету, потенциально могут стать частью инфраструктуры злоумышленников и быть задействованы в DDoS-атках.

В 2015 году Qrator Labs наблюдал множество атак с ботнетов, организованных на Android-устройствах. Число открытых злоумышленниками уязвимостей этой и других ОС будет расти, и вместе с этим – размеры ботнетов.

Распространение IoT несёт в себе ещё более масштабную угрозу – производители всевозможных подключённых устройств (чайники, ТВ, автомобили, мультиварки, весы, «умные» розетки и т.д.) далеко не всегда заботятся о должном уровне защиты. Часто такие устройства также используют старые версии популярных операционных систем (в частности, тот же Android), и не заботятся о регулярном их обновлении на новые версии, в которых устранены уязвимости.

Предвестники проблемы IoT уже прозвучали в 2015 году. В частности, была обнаружена ботсеть, построенная на сетевых маршрутизаторах, в которых не поменяли стандартные пароли. «Казалось бы, сетевое оборудование настраивается специалистами, и в последнюю очередь должно оказаться под угрозой взлома. Но практика показывает обратное. Что уж говорить об уязвимости пользовательских устройств. Мы прогнозируем, что очень скоро все смартфоны на старых версиях Android будут состоять как минимум в одном ботнете. За ними последуют все «умные» розетки, холодильники и прочая бытовая техника. Уже через пару лет нас ждут ботнеты из чайников, радионянь и мультварок. Интернет вещей принесёт нам не только удобство и дополнительные возможности, но и много проблем. К этому следует готовиться уже сейчас», — говорит Александр Лямин, глава Qrator Labs.

Иллюстрацией того, насколько уязвимы совершенно неожиданные гаджеты может служить недавняя история, приключившаяся в Калифорнии. Маленький ребёнок пожаловался родителям, что слышит мужской голос по ночам. Выяснилось, что хакер взломал радионяню и пугал мальчика, общаясь с ним дистанционно.

ГЛАВА II. ХАКЕРСКИЕ АТАКИ НА ВЕБ-РЕСУРСЫ

Угроза взлома веб-приложений остаётся одной из самых серьёзных проблем для веб-ресурсов любой направленности. Почувствовать себя хакером сегодня может даже человек, слабо подготовленный технически – методиы взлома и необходимые инструменты доступны в открытом виде и легко могут быть найдены с помощью обычных поисковиков. В 2015 году в этой сфере наблюдались следующие тренды.

КЛЮЧЕВЫЕ НАБЛЮДЕНИЯ 2015

В 84% случаев наблюдается чередование DDoS атак с попытками взломов сайтов. Можно с большой долей вероятностью быть уверенным, что вслед за прекратившейся DDoS-атакой будет проведена попытка взлома сайта и наоборот.

Массовые сканирования всего интернета в поисках ресурсов с известными уязвимостями касаются любого сайта. Так, сканирования на предмет уязвимости ShellShock, обнаруженной еще в 2014 и позволяющей удаленно выполнять произвольный код, по-прежнему фиксируются практически для каждого клиента Wallarm.

31% сайтов содержат критические уязвимости, описания которых доступны публично. То есть каждый третий сайт может быть взломан даже не высококвалифицированным специалистом, потратившим немного времени. Амплитуда атак увеличивается в момент появления информации о публичной уязвимости в популярных фреймворках или продуктах (CMS, форумах и т.д.). Причем время от появления публичного эксплоита до массовых сканирований редко превышает 24 часа.

Увеличивается количество атак на облачные инфраструктуры (AWS, Azure и т.п.). Злоумышленники пользуются частыми ошибками в администрировании облачных ресурсов, для которых еще не сложились лучшие практики использования.

Наиболее популярными атаками по-прежнему являются атаки на SQL-инъекции (37,75%). Возможность получения прямого доступа к базе данных, что часто и является целью атаки, и относительная простота реализации атаки с помощью автоматизированных инструментов делает этот вид атак абсолютным лидером.

КОМБИНИРОВАНИЕ DDOS-АТАК С АТАКАМИ НА ПРИЛОЖЕНИЕ

Согласно подсчётам Wallarm, в 84% случаев наблюдается чередование DDoS-атак с попытками взломов сайтов. Это свидетельствует о согласованности действий и повсеместном применении хакерами различных техник атак. «Можно с большой долей вероятностью быть уверенным, что вслед за прекратившейся DDoS атакой будет проведена попытка взлома сайта и наоборот. А внезапно прекратившаяся DDoS-атака может означать успешный взлом», — комментирует Иван Новиков, глава Wallarm. Таким образом, только одновременное использование разно профильных средств защиты (включающих защиту от DDoS и атак на приложения, а также средства мониторинга BGP), может эффективно противостоять хакерам.

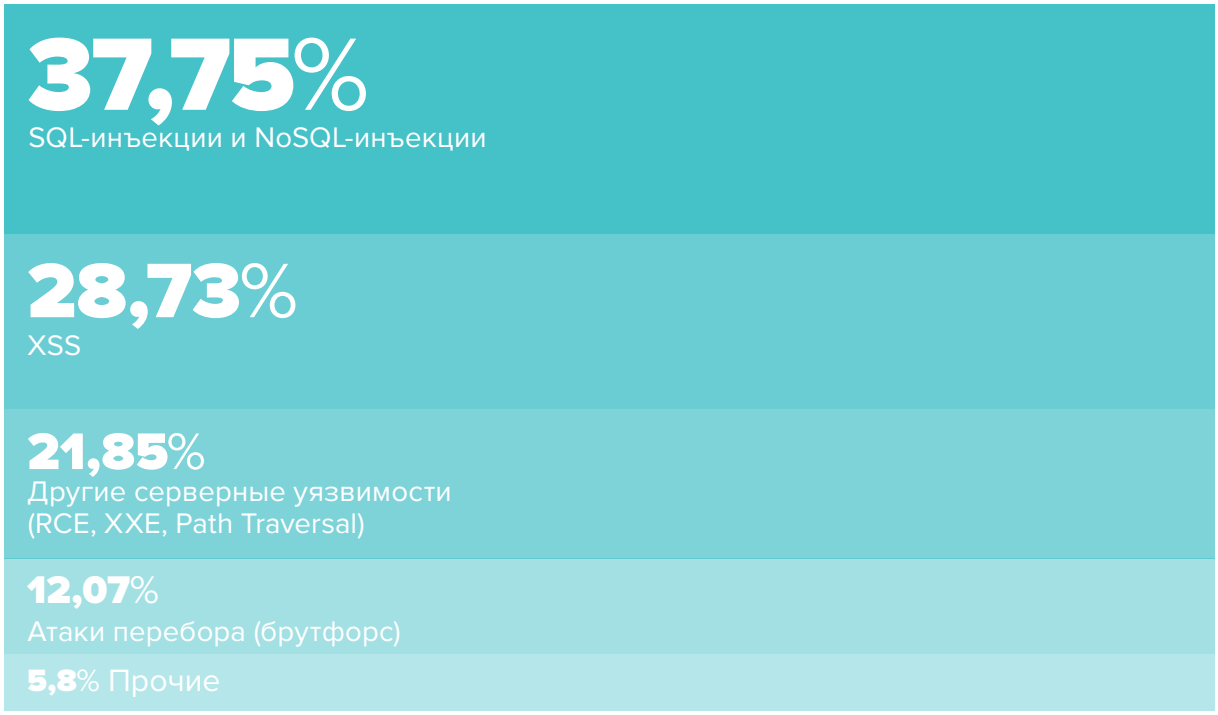
Более 30% сайтов содержат критические уязвимости, описания которых доступны публично. То есть каждый третий сайт может быть взломан даже не высококвалифицированным специалистом, потратившим немного времени.

Это означает, что защищаться от угроз безопасности следует с помощью комбинированных интегрированных решений, которые работают удалённо – то есть не находятся в атакуемой инфраструктуре.

ХАРАКТЕРИСТИКА АТАК НА ВЕБ-САЙТЫ

За 2015-й год компанией Wallarm было зафиксировано более 100 млн атак на веб-ресурсы своих клиентов.

РАСПРЕДЕЛЕНИЕ АТАК ПО ТИПАМ ЭКСПЛУАТИРУЕМЫХ УЯЗВИМОСТЕЙ:



На долю атак SQL-инъекций приходится больше всего вредоносных запросов (37,75%). Это обусловлено наличием в открытом доступе множества инструментов для автоматизированного тестирования веб-приложений на этот тип уязвимости. Кроме того, риск уязвимости крайне высок — успешная эксплуатация сразу же открывает перед злоумышленником возможность получения полного доступа к базе данных.

Второе место занимают атаки, направленные на клиентские уязвимости, так называемый межсайтовый скриптинг или “XSS” (28,73%). Успешная эксплуатация дает возможность получения несанкционированного доступа к конкретной учетной записи пользователя-жертвы или их группы. Эти уязвимости гораздо более распространены в веб-приложениях и считаются разработчиками менее критичными, так как требуют взаимодействия с браузером атакуемого пользователя.

Примечательно, что в прошедшем году серьезно увеличилось количество атак перебора, в том числе направленных на перебор паролей (21,85%). В России это, прежде всего, коснулось сайтов интернет-ритейлеров, где злоумышленники в массовых количествах получали доступ к учетным записям, используя базы “логин-пароль”, утекшие из других ресурсов. Более подробно мы это описывали в отдельном отчете о безопасности интернет-ритейла в декабре 2014 года.

ЗОНЫ РИСКА ПО ОТРАСЛЯМ

Агрессивность среды в интернете растет с каждым годом. Если еще несколько лет назад, массовые сканирования на предмет известных уязвимостей были крайне редким явлением, то сегодня практически каждый сайт ежедневно обходится проверяющим ботом. Любой ресурс, в том числе мало известный и практически не посещаемый, может быть взломан автоматизированными инструментами.

Цель злоумышленников в этом случае — вычислительные ресурсы, которые они в дальнейшем могут использовать для реализации DDoS-атак, в качестве прокси-сервера, майнинга криптовалют, и т.д.

С точки зрения целенаправленных атак, можно выделить следующие категории ресурсов:

1. Электронная коммерция и прежде всего интернет-ритейлеры. Фрод с бонусными баллами, охота за пользовательскими базами.
2. Платежные системы и агрегаторы, финансовые брокеры и другие финансовые учреждения. Попытка получить доступ к базе данных с возможностью изменения балансов.
3. Игровая индустрия. Фрод с внутренней экономикой игр, краха исходных кодов и т.д.
4. Рекламные сети. Мошенничество с внутренними балансами счетов и фрод с количеством показов.
5. СМИ. Нарушение доступности и работоспособности ресурсов.

При этом взлом веб-приложений нередко становится ступенькой к доступу ко внутренней инфраструктуре компании.

ОСНОВНЫЕ ПРИЧИНЫ ВЗЛОМА ВЕБ-ПРИЛОЖЕНИЙ

Порог “входа в профессию” стремительно снижается. Зачастую не нужно обладать специальными знаниями для того, чтобы реализовать успешную атаку. Для любой критической уязвимости в известных продуктах вскоре появляется публичный эксплоит — весь процесс эксплуатации в этом случае сводится к банальному указанию домена или IP-адреса уязвимого ресурса. Снижаются и требования к разработчикам, минимально необходимые для начала работы над веб-приложениями, что непременно влияет на качество кода систем.

В среднем за первый месяц подключения Wallarm система находит несколько уязвимостей, которые так или иначе могли бы быть использованы злоумышленниками для взлома. Можно также выделить несколько самых распространенных проблем, из-за которых сайты становятся легкой мишенью для злоумышленников:

1. Использование устаревшего ПО (например, WordPress или его отдельные плагины) и незащищенные второстепенные ресурсы на сетевом периметре проекта, про которые все забыли или не все знали.
2. Базовые критические уязвимости, допущенные при разработке или модификации ПО.
3. Ошибки администрирования (пароли по умолчанию, бездумная настройка сервисов по инструкциям в стиле “сделал как Хабре/stackoverflow”).
4. Таргетированные заражение ПК сотрудников компании, имеющих необходимые доступы (пароли к FTP, SSH, VPN и т. д.). Как правило, через фишинг.
5. Учетные записи по ошибке публикуются в открытом доступе (форумы разработчиков, сайты вроде Pastebin, репозитории кода на GitHub и т. д.).

Стоит отметить, что подобные причины актуальны как для небольших и средних проектов, где всегда есть недостаток экспертизы, так и для крупных проектов с масштабной инфраструктурой, динамично развивающимися веб-приложениями и меняющейся командой. В условиях кризиса турбулентность в области кадров только подталкивает этот процесс.

ПРОГНОЗЫ НА 2016

1. Упрощение взлома и продолжение смещения людей, стоящих за атаками — от профессионально понимающих предметную область к новичкам, которые ищут и эксплуатируют уязвимость, руководствуясь статьями и видео инструкциями.

2. Взлом и заражение всевозможных IoT-устройств. Веб-интерфейсов, API в бытовой технике, машинах, гаджетах построены на базе тех же технологий — и потому страдают теми же проблемами, что и многие веб-ресурсы. Не исключены массовые DDoS-атаки с использованием таких устройств.

3. Увеличение количества атак на облачные инфраструктуры (AWS, Azure). Стремительное распространение облачных сервисов и отсутствие устоявшихся практик по их управлению создает новые возможности для хакеров.

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.

www.qrator.net

Компания Wallarm разрабатывает решения для защиты веб-ресурсов, совмещающие в себе функции файровола 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.

www.wallarm.com

ПРИЛОЖЕНИЕ

КРАТКИЕ СВЕДЕНИЯ О DDOS

DDoS-атака (от англ. Distributed Denial of Service) — атака на вычислительную систему с целью довести её до отказа (то есть до состояния, при котором легитимные пользователи не могут получить доступ к системе) посредством исчерпания тех или иных вычислительных ресурсов. Зачастую DDoS-атака реализуется за счёт большого количества запросов к серверу от зараженных компьютеров, при этом каждый из запросов аналогичен тем, что генерируют легитимные пользователи. Это вызывает отказ инфраструктуры сайта, которая не выдерживает нагрузки, многократно превышающей норму.

Для генерации такого количества запросов киберпреступники используют компьютеры интернет-пользователей, которые об этом и не подозревают. Злоумышленники заражают Web-серверы и компьютеры программами-троянами, превращая их в «зомби». Тысячи “зомби” объединяются в ботнет (англ. botnet) – сеть, которой можно управлять дистанционно. Самый большой ботнет был зарегистрирован в 2009 году и объединял 1,9 млн. компьютеров из 77 стран. Для старта DDoS-атаки достаточно одной команды, которую хакер отправляет из любой точки планеты. Именно по этой причине правоохранительным органам сложно найти исполнителей и организаторов DDoS-атак.

Qrator Labs классифицирует атаки согласно тому, на какие элементы инфраструктуры они направлены:

- Канальный уровень [OSI Layer 2] — атаки на исчерпание канальной ёмкости;
- Сетевая инфраструктура [OSI Layer 3] — атаки, направленные на вывод из строя сетевого оборудования (коммутаторы и маршрутизаторы);
- Транспортный уровень и протокол TCP [OSI Layer 4] — различные манипуляции с TCP стейт-машиной: SYN-flood, некорректные инициации/закрытия соединений, переполнения буферной памяти;
- Приложение [OSI Layer 7] – атаки, реализуемые с помощью семантически осмысленных конструкций протокола атакуемого интернет-приложения, например, HTTP Flood для Web-сайтов.

Отдельно нужно выделить FBS-подкласс (Full browser stack) атак на приложение. Для таких атак используются ботнеты, имеющие в своем распоряжении полноценный веб-браузер с необходимым набором расширений и плагинов. Такого рода атаки гарантированно преодолевают решения, использующие различные “головоломки-верификаторы” для клиента — начиная от простых HTTP-редиректов до менее тривиальных верификаторов с использованием JS/AdobeFlash или Quicktime.