QRATOR LABS

Эволюция DDoS-атак и средств противодействия данной угрозе

I. Введение

В области DDoS-атак, как и во всех других сферах кибербезопасности, не прекращается борьба щита и меча. Злоумышленники используют всё более изощрённые методы. Поставщики решений следуют за ними, выпуская всё новые продукты для того, чтобы помешать злому умыслу. Старые средства перестают работать, требуются новые подходы и инструменты для того, чтобы не стать жертвой киберпреступников. В данном документе рассматривается путь развития, который проходят инструменты противодействия DDoS-атакам, под влиянием меняющихся подходов киберпреступников.

Информация в данном документе будет полезной компаниям, которые хотят быть уверены, что их интернет-ресурсы защищены современными средствами противодействия, а не решениями, основанными на устаревших неэффективных более технологиях, которые всё ещё предлагаются на рынке. Также, документ предназначен для специалистов в области информационной безопасности и широкого круга людей, интересующихся данной темой.

II. Некоторые определения

DDoS-атака (Distributed Denial of Service)
Распределенная (то есть идущая из разных источников) атака на интернет-ресурс с целью добиться его отказа. То есть привести его в такое состояние, когда пользователи не могут получить к нему доступ.

Классификация DDoS-атак
Один из подходов к классификации DDoS-атак основан на том, на какой уровень сети нацелены злоумышленники:
L2 – атаки на исчерпание канальной емкости, так называемые “volumetric attacks”;
L3 – атаки на сетевую инфраструктуру и оборудование;
L4 – атаки, нацеленные на стек интернет-протоколов TCP/IP;
L5-L6 – атаки на механизмы шифрования (TLS/SSL);
L7 – атаки на протоколы сетевых приложений (HTTP, DNS, XMLGate)

Полоса DDoS-атаки
Данный термин используется Qrator Labs, чтобы дать количественную характеристику атаке и иметь возможность сравнивать атаки между собой по этому признаку. Полоса трафика атаки измеряется в количестве «мусорных» данных, обрушиваемых на ресурс в единицу времени: Мб/сек, Гб/сек. Другие характеристики, которые часто можно встретить в прессе (мощность, сила), инженеры Qrator Labs считают неточными, т.к. эти слова не отражают сути происходящего во время атаки.

Успешная DDoS-атака
Атака, которая привела к тому, что веб-ресурс оказался недоступен в течение заметного времени. Этот промежуток времени называют **downtime или даунтайм**.

Атаки вида Amplification
Атака, использующая механизм 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 и другие.

False positive, false negative
Ситуация, когда средство фильтрации трафика, используемое для противодействия DDoS-атакам, срабатывает ошибочно: задерживает «хороший» запрос (то есть обращение реального пользователя к веб-ресурсу) либо пропускает «мусорный» запрос от бота.

III. Эволюция DDoS-атак и средств противодействия данной угрозе

1995-2000гг. – Затишье перед бурей

Типы атак

На первом этапе развития интернета злоумышленники в основном атакуют веб-приложения. Цель: вывести из строя конкретное веб-приложение или операционную систему. Наиболее распространенные типы атак в этот период: SYN-flood и HTTP-flood. В обоих случаях зловредная программа отправляет массовые запросы. В первом случае генерируются «мусорные» запросы к операционной системе на установку TCP-соединения. Во втором – к приложению, например, к форме на веб-странице. Ресурс исчерпывается довольно быстро, т.к. широкие каналы и мощные сервера – редкость в это время. Большинство пользователей подключаются к интернету через dial-up.
Атаки редко бывают коммерческими, основной мотив -- хулиганство, хактивизм. Информация о взломанных хостах и спецсредства для атак распространяются через хакерские каналы IRC. Web в это время – все еще маленький мир, в котором мало ресурсов и легко отследить источник атаки.

Методы противодействия

В большинстве случаев проблема решается правильной настройкой приложений и операционной системы. Специальные средства противодействия не нужны.

2001-2005гг. – Время CPE

Типы атак

К интернету уже подключено на порядок больше ПК и серверов. Распространяется ШПД (широкополосный доступ в интернет). Основная операционная система в это время -- Windows 98, которая крайне уязвима. Ее легко взломать и установить на чужой компьютер зловредную программу. Это создает предпосылки для активного распространения ботнетов.
Большинство известных атак производятся на уровне L7 посредством эксплуатации большого количества уязвимостей веб-ресурсов и в окружающей инфраструктуре.

Методы противодействия

Интернет становится пространством для ведения бизнеса. Большинство компаний сталкиваются с хакерскими и DDoS-атаками, но не могут справиться с проблемой старыми методами.
Самый популярный способ защиты -- фильтрация трафика внутри клиентской сети с помощью тех или иных средств. Как правило, это вендорские аппаратные решения.
Владельцы веб-ресурсов массово покупают «железо» и вендорскую техподдержку. Формирует рынок аппаратных средств защиты от DDoS класса CPE (Customer Premises Equipment – оборудование, устанавливаемое у клиента). На этой волне вырастает несколько крупных компаний, некоторые из них следующих этапах свернут свой бизнес.

2006 – 2010гг. – Операторские решения спасают от DDoS

Типы атак

Интернет развивается: каналы становятся шире, количество веб-ресурсов растет на десятки процентов в год, появляется рынок массового хостинга. Как правило, хостеры используют небезопасные и незрелые платформы, которые легко взломать.
Это создает предпосылки для распространения крупных ботнетов и проведения первых высокоскоростных атак. DDoS-атаки становятся системной деятельностью, превращаются в теневой бизнес, на котором специализируются как

Методы противодействия

Методы защиты на стороне клиента становятся неэффективными, т.к. атаки устраиваются с помощью огромных ботнетов, их скорость велика и позволяет очень быстро забить канал жертвы мусорным трафиком (пропускная способность канала оператора, к которому она подключена, это также позволяет).
Сетевое оборудование, осуществляющее фильтрацию трафика для противодействия DDoS-атакам, начинают использовать транзитные операторы, канальных

отдельные исполнители, так и группы киберпреступников.
Растет популярность атак типа Flood, прежде всего Syn Flood, рассчитанных на выведение из строя входящих каналов связи клиента. Возникают первые единичные атаки полосой до 100 Гб/с.
Устроить атаку средней скорости на потребительскую инфраструктуру становится просто и дешево. Это позволяет делать существенная разница в пропускной способности каналов сетевых операторов и тех каналов, к которым подключена инфраструктура их клиентов.

ресурсов которых достаточно, чтобы пропускать атаки такой величины до этого оборудования.
Рынок CPE-решений для противодействия DDoS-атакам начинает сжиматься. Уходят из бизнеса успешные в прошлом поставщики «железок» данного типа.

2011-н.вр. – Операторы теряют контроль

Типы атак

Злоумышленники открывают для себя технику Amplification. Атаки с использованием этой техники рассчитаны на эксплуатацию особенностей ряда сетевых протоколов (NTP, DNS, SNMP, Chargen, SSDP и прочие), которые позволяют путем направления определенного вида трафика на сетевой ресурс (амплификатор), использующий данный механизм, получить от него трафик в многократно увеличенном объеме.
Используя серию проходов трафика между амплификаторами и агрегировав ответный трафик в направлении выбанной жертвы, злоумышленник может, обладая скромным по современным меркам ботнетом, создать атаку, которая причинит немалый ущерб даже крупной сети с лучшим на рынке сетевым оборудованием. К 2015 году средний амплификатор дорастает до сотни.
DDoS-атаки бьют рекорды один за другим:

Методы противодействия

К этому моменту рынок операторских услуг, в число которых входит также противодействие DDoS-атакам, становится зрелым. Число клиентских подключений к операторам растет. Но вместе с тем обостряется угроза DDoS-атак. Ситуация начинает выходить из-под контроля, когда из-за растущей скорости атак даже высокопроизводительное оборудование на стороне сетевого оператора перестает быть надежным средством. Крупная атака может перекрыть всю имеющуюся канальную емкость оператора, что не только нанесет урон ему, но и выведет из строя большинство клиентов его сервиса. В итоге это грозит многократно возросшими экономическими и репутационными потерями.
Операторские решения перестали быть эффективными по следующим причинам:

100Гб/сек становится обычным делом, в 2014 году фиксируется первая атака в 500Гб/сек.
Средний размер DDoS-атак также неуклонно растет. Полоса клиентских соединений становится шире, это значит, что злоумышленникам требуется генерировать больше мусорного трафика, чтобы «уложить» веб-ресурс заказанной жертвы. Данная «гонка вооружений» развивается не в пользу сетевых операторов, которые начинают реально ощущать проблему на себе – емкости их каналов иногда уже просто не хватает. Начиная с 2014 года с возрастающей частотой случаются инциденты, когда атака на клиента попутно выводит из строя инфраструктуру его сетевого провайдера, в итоге от даунтайма страдают все остальные его клиенты. А в отдельных случаях переполняется даже upstream-канал провайдера более высокого уровня, у которого попавший в передрягу оператор покупает трафик.
С 2014 года происходит бурное созревание теневого коммерческого рынка услуг по организации DDoS-атак: услуга пользуется спросом (это дешевый и эффективный способ конкурентной борьбы), киберпреступники объединяются в коалиции, обозначаются лидеры рынка, которые предоставляют «взрослые» коммерческие услуги, нанимают субподрядчиков. Раньше исполнителям приходилось самостоятельно разрабатывать средства организации атак. Теперь в сети можно скачать пакеты инструментов “ready-to-use”, которыми может воспользоваться даже школьник. Можно купить или арендовать специальные инструменты для создания собственного ботнета, взять в аренду готовую зомби-

- Атак стало слишком много, изменился их профиль. Средства, которые используют операторы, умеют анализировать только «слепок» с трафика (откуда он идет, есть ли нетипичные IP-адреса, наблюдается ли несвойственный всплеск активности и т.д.). Но этого недостаточно, чтобы «отловить» атаки уровня L7, т.к. в этом случае требуется анализировать поведение пользователей. По этой причине все чаще возникает ситуация, когда оператор, по его мнению, успешно фильтрует DDoS-атаку, но веб-ресурс клиента все равно «лежит».
- Операторские решения не способны на глубокий анализ трафика в том числе и потому что через них проходят слишком большие объемы данных. Подробно анализировать все пакеты было бы слишком долго и накладно.
- Как правило центр очистки трафика (ЦОТ) оператора сконцентрирован -- находится в одном ЦОД, куда направляется зеркальная копия всего клиентского трафика.
- Обычно реакция на DDoS-атаку производится вручную (это обозначено в типичных операторских SLA) – при возникновении подозрительной ситуации администратор получает оповещение, и должен отреагировать на происходящее, например, заблокировав группу IP-адресов. Время реакции может составлять 15-30 минут, что для некоторых веб-ресурсов может быть критичным (например, для банковских систем ДБО или

сеть со всеми необходимыми средствами управления.
Нападения на веб-ресурсы становятся гибридными и сложносоставными: DDoS-атаки на переполнение канальной емкости комбинируются с атаками L7, сопровождаются взломом.

интернет-магазинов в горячий сезон).

- Операторы не могут себе позволить включить автоматическую отработку подозрительных ситуаций, т.к. их ЦОТ видит только статистику запросов, а значит может часто ошибаться (приводить к false positive, false negative).

IV. Облачные распределенные специализированные решения – ответ на изменившийся профиль угроз

Начиная с 2010 года наряду с операторскими решениями на рынке появились и получают все большее распространение специализированные инструменты противодействия DDoS-атакам – облачные сети фильтрации трафика от внешних поставщиков. Такие решения лишены недостатков, которые присущи операторским сетям и решениям фильтрации трафика на стороне оператора в силу специфики бизнеса телеком-компаний:

- Операторская бизнес-модель требует от него строить стыки с другими операторами там, где трафик дешевле. Это позволяет получать больше прибыли. Но вместе с тем это повышает риски для его клиентов стать жертвой успешной DDoS-атаки – самыми дешевыми источниками трафика являются публичные точки обмена трафиком (Internet Exchange), являющиеся по своей структуре огромными Ethernet-матрицами, в которых невозможно контролировать происхождение трафика и гарантировать SLA.
- Эффективная сеть фильтрации трафика должна строиться на основе другой логики – узлы необходимо располагать как можно ближе к источникам атак. В частности, сеть Qrator спроектирована с учетом этого принципа.
- Чтобы правильно спроектировать сеть фильтрации трафика, то есть обеспечить эффективное противодействие DDoS-атакам, необходимо вести постоянную исследовательскую работу: наблюдать за тем, откуда идут атаки, понимать логику связности интернета, следить за изменениями ситуации в глобальной сети, за прогрессом подходов злоумышленников. Это отдельное направление деятельности, которое требует инвестиций, наличия команды высокооплачиваемых специалистов с глубокой экспертизой по данному вопросу. Для операторов это, фактически, означает необходимость дополнительных расходов на неспецифическое для себя направление.

- В отличие от операторских решений, специализированные облачные средства противодействия DDoS-атакам анализируют не только статистические данные о трафике, они проводят глубокий анализ содержимого пакетов (как в зашифрованном виде, так и с передачей SSL-ключа поставщику услуги), поведения пользователей. Такие системы самосовершенствуются, благодаря встроенным алгоритмам машинного обучения. Они могут настраиваться под конкретных клиентов, чтобы учитывать особенности бизнеса, что невозможно в случае с операторскими решениями.
- Наиболее эффективное решение защиты от интернет-угроз на сегодняшний день – это интеграция двух средств: распределенной сети фильтрации трафика для противодействия DDoS и инструментов защиты от хакерских атак.

2016-2020гг. – Прогноз

Типы атак

По прогнозу Qrator Labs, основной интернет-угрозой станут комбинированные сложные атаки. Теневая индустрия услуг по организации DDoS-атак будет расти и дальше. Сегодня ботнет – массовый инструмент, и он по-прежнему будет использоваться. Также будут появляться новые типы угроз, в частности, усилится давление на сетевую инфраструктуру. Атаки на DNS уже стали реальной проблемой, как и прогнозировала в отчете за 2015 год Qrator Labs. Так, в конце прошлого года два корневых DNS-сервера (по сути главные инфраструктурные элементы глобального интернета) вывели из строя в результате целевой атаки на ресурсы RIPE NCC (глобальный координационный центр интернета). До того считалось, что мощности серверов достаточно, чтобы выдержать любое нападение, но их удалось «положить». Атаки на глобальную инфраструктуру интернета продолжатся. Qrator Labs ожидает, что подобного масштаба

Методы противодействия

Для противодействия новым угрозам необходимо использовать распределенные сети фильтрации трафика с узлами, расположенными как можно ближе к источникам атак.
Для того, чтобы сеть поставщика услуги была максимально эффективной, он должен постоянно проводить исследования связности интернета и адаптировать архитектуру своей сети в соответствии с меняющимися условиями.
Такие специализированные решения должны использовать элементы искусственного интеллекта, чтобы быстро адаптироваться под меняющиеся условия и автоматически подстраиваться под новые методы, используемые злоумышленниками.

Для противодействия атакам на BGP требуется разработка специальных средств. На сегодняшний день существует возможность выявлять такие атаки и изолировать источник, но нет инструментов их предотвращения. На уровне атакуемого

достигнет угроза атак на глобальную систему маршрутизации – манипуляций с протоколом BGP.
Злоумышленники могут начать использовать уязвимости BGP-протокола для искажения или добавления ложной информации о маршрутах, перехвата трафика или перенаправления его третьей стороне.

оператора обнаружить утечку маршрута обычно невозможно, т.к. манипуляции производятся вне зоны его видимости. Для обнаружения инцидентов BGP требуется следить за множеством узлов одновременно. То есть, очевидно, необходимо создание специализированных сервисов для борьбы с данной угрозой.
Противодействие атакам на BGP возможно только при сотрудничестве разных игроков рынка.
Ещё в 2010 году Qrator Labs прогнозировала риски, связанные с уязвимостью BGP и начала исследования в данной области. В частности, компания создала сервис Qrator.Radar, с помощью которого можно выявлять утечки маршрутов.

V. Выводы

- Атаки сегодня стали сложными и многоуровневыми: DDoS-атака на канальную емкость L2 нередко сопровождается атакой на уровень веб-приложений L7, а также может отвлекать внимание от взлома. Сложность атак и их системность будут расти – злоумышленники выбирают конкретную цель и могут долго готовиться к нападению, чтобы ударить именно в наиболее уязвимые элементы.
- Эволюция интернет-угроз закономерно повлияла и на развитие средства противодействия им. Сегодня наиболее эффективный инструмент защиты интернет-ресурсов от внешних атак из сети – это облачная распределенная сеть фильтрации трафика с элементами машинного обучения, интегрированная со средствами защиты от взлома (WAF – Web Application Firewall).
- Теневой рынок киберпреступлений очень быстро реагирует на появляющиеся уязвимости новыми атаками. На нечестные средства конкурентной борьбы есть спрос, который рождает предложение. Поэтому компании, использующие устаревшие средства защиты, серьезно рискуют. Важно, чтобы поставщик комбинированной услуги (фильтрация трафика + WAF) следил за тем, как меняются угрозы и адаптировал свое решение в соответствии с этим.
- Ответа на новые угрозы, связанные с уязвимостями протокола маршрутизации BGP, пока нет. Инструменты предотвращения атак данного типа могут быть

созданы лишь в сотрудничестве множества игроков рынка интернет-телекоммуникаций. На данный момент система глобального мониторинга Qrator.Radar, ведущая наблюдения за связностью интернета, способна выявлять утечки маршрутов и оповещать о них.

- Помимо тактических решений для борьбы с атаками на глобальную маршрутизацию следует обратить внимание на стратегические инициативы, которые направлены на развитие самого протокола и повышение его безопасности. К числу таких инициатив относятся недавние драфты, посвященные методикам обнаружения инцидентов и расширениям протокола BGP:
  https://tools.ietf.org/html/draft-ietf-idr-route-leak-detection-mitigation-03
  https://tools.ietf.org/html/draft-ymbk-idr-bgp-open-policy-00
  https://tools.ietf.org/html/draft-ietf-sidr-bgpsec-overview-07