"РТКомм": "Защита от DDoS - это всегда совместная работа с клиентом"

Услуга по защите от DDoS все больше интересует не только операторов связи, финансовые корпорации и банки, но и страховые компании, государственные структуры и другие предприятия и учреждения, бизнес которых критичен к непрерывности функционирования Интернет-ресурсов. О специфике тарификации таких услуг, параметрах SLA, взаимодействии с клиентами нам рассказал Руководитель группы управления продуктами ОАО "РТКомм.РУ" Иван Мирошниченко.

Сочетание решений

["РТКомм": "Защита от DDoS - это всегда совместная работа с клиентом"]Проект защиты от DDoS в "РТКомм" стартовал почти 4 года назад - "нас очень "взбодрила" давняя ситуация с ЮТК, когда противостоять мощной DDoS-атаке не смогли никакие имевшиеся на тот момент средства. Поскольку повторения совсем не хотелось, да и "на носу" был нацпроект "Образование", мы серьезно занялись этим направлением", - говорит Иван Мирошниченко.

Для сети образовательных учреждений защита от DDoS в то время была достаточно актуальной. "Поскольку у нас был госзаказчик, то его требование было однозначным: единая сеть должна была быть защищена единым и весьма надежным решением, - продолжает он. - И на момент завершения проекта все так и было. Это сейчас конкурсы на обслуживание школ играются на местах: каждая школа самостоятельно выбирает своего поставщика услуг, поэтому мы уже физически не можем защитить те образовательные ресурсы, которые расположены в других ЦОДах или потребляют Интернет у других провайдеров".

Изначально основным решением у "РТКомм" был выбран аппаратно-программный комплекс от Arbor Networks. "4 года назад, возможно, это было не самое эффективное решение на рынке, оно было немного "сыроватым", но с большим потенциалом развития: производитель продемонстрировал нам road map и нас устроила та идеология, которая в него закладывалась. Чуть позже мы интегрировали к этой системе решение Cisco Guard, которое у нас уже было внедрено на момент закупки Arbor. Не скажу, что эти два комплекса прямые конкуренты, скорее они работают в одной нише. На первом этапе их сочетание было нам нужно для решения одной задачи - мы хотели и сумели создать эшелонированную систему анализа трафика для защиты в первую очередь собственной магистральной сети, а также иметь надежные инструменты для качественного анализа трафика. Вторым этапом было решение задачи оказания услуг нашим клиентам", - говорит Иван Мирошниченко.

Схема реализации защиты зависит от специфики инфраструктуры оператора и с учётом того, что необходимо защищать. «Например, можно очищать трафик на узлах пиринга или на границы сети. Плюсом данного подхода является то, что оно позволяет очистить паразитный трафик как можно ближе к источнику атаки. Но у него также есть и недостаток, невозможно очищать трафик внутри сети и атака может проходить от одного клиента к другому. Можно установить выделенное устройство очистки, которое будет защищать определенную инфраструктуру или клиента – например, поместить в дата-центре и гарантировать его защиту из любой точки сети. Но тогда мы “откроем” других клиентов. Третий вариант - использование центра очистки. Такое решение позволяет контролировать весь трафик клиентов услуги защиты от DDoS, обеспечивая возможность очистки его от атак вне зависимости от источника. При таком подходе не имеет значение, где и в каком месте сети подключается клиент. И последний вариант - это комбинированная схема. В этом случае на узлах пиринга мы защищаем магистраль и обеспечиваем фильтрацию атаки на входе в сеть. Центр очистки будет подавлять оставшуюся часть атаки, попадающую в сеть от собственных же клиентов, - говорит г-н Мирошниченко».

В нашей схеме Arbor Networks выдвинут на первую линию обороны, он же в постоянном режиме проверяет трафик с помощью своих анализаторов. А Cisco Guard выполняет роль укрепленных оборонных центров внутри сети и защищает вполне определенные объекты инфраструктуры и клиентские серверы. В основном, это решение используется для защиты нескольких крупных государственных клиентов, которые потребляют наши услуги ЦОД в столице", - отмечает он.

Г-н Мирошниченко уверен, что суммарная мощь двух решений вполне способна "перемолоть" практически все типы атак. Явным плюсом от такого сочетания он считает высокую защиту внутрисетевого трафика: оба центра очистки подключены параллельно к ядру сети и их можно вводить в строй в зависимости от типа и мощности атаки. В настоящий момент суммарная мощность решения от Arbor Networks составляет 9-10 Гбит/с, а Cisco Guard - 5 Гбит/с. "Но, в среднем, производительность нашего комплекса в 3-4 раза перекрывает пиковую мощность тех атак, которые случались на наши собственные и клиентские ресурсы до сих пор", - уверен Иван Мирошниченко.

["РТКомм": "Защита от DDoS - это всегда совместная работа с клиентом"]

["РТКомм": "Защита от DDoS - это всегда совместная работа с клиентом"]

Тактика нападения

Типология DDoS-атак достаточно сильно зависит от того, на какого клиента ориентируются операторы и сервис-провайдеры. К примеру, в РТКомм наиболее интересными считают банковский сектор, платежные системы, крупный бизнес. Поэтому, компании приходится сталкиваться с атаками, которые характерны именно для таких клиентов. "В основном это управляемые, мощные и изощренные атаки, которые ставят себе целью наглухо "положить" инфраструктуру провайдера и "выбить" сервисы клиента. Баловство школьников ИТ-отделы этих компаний могут отсечь и без нас. Но в текущей ситуации те атаки, которым они подвержены, достаточно мощные - обычно они длятся 2-3 дня, причем наращивая свою мощность в случае обнаружения противодействия. В зависимости от защитных мероприятий атака "перестраивается на ходу" - меняется ее характер в части используемых протоколов и приложений.

В основном, атаке подвергаются, конечно, коммерческие компании – «если чей-то сайт приносит деньги, либо оперирует с деньгами, то всегда найдется тот, кто захочет эти деньги забрать, - уверен г-н Мирошниченко. - Так что, лучше, наверное, “подстелить соломку” заранее». Но бывают и достаточно серьезные атаки на государственные органы власти. Правда, здесь совсем другая мотивация - отобрать бизнес или нанести серьезный экономический ущерб там цели нет. Поэтому большая часть именно таких атак - это хулиганские действия. Присутствует и баловство: начинающие DDOSеры хотят показать свою значимость на этом рынке, записать "в портфолио" несколько "громких завалов". Но такие атаки, как правило, автоматически подавляются нашей системой и особой угрозы не представляют.

Частота значимых DDoS-атак достаточно велика - "с серьезной управляемой атакой мы сталкиваемся уже пару раз в месяц. Сначала идет "разведка боем" - атакующий хочет проверить систему защиты, чтобы оптимально сформировать свое наступление, подтянуть резервы. На основании полученных данных проводится уточнение планов и, возможно, разрабатываются новые варианты развития атаки: как в настоящем бою противник подтягивает к линии нашей обороны резервы, формирует эшелон развития атаки и прикрывает себя с флангов. Правда, в роли солдат и артиллерии - ботсети. Очень часто DDoS-атака служит для целей сокрытия других злонамеренных действий: кража денег, данных, попытка получить полномочия высшего уровня и т.д. По сути - это не само преступление ради того, чтобы "выключить" ресурс из Сети, а инструмент сокрытия преступления. Далеко не всегда атаки начинаются в выходные – зачастую большего успеха в стремлении к поставленной цели можно достигнуть, атакуя в будни. Был случай, когда в течение рабочего дня шла атака, на ночь останавливалась и на следующий день мы наблюдали продолжение по тому же сценарию. Конечно, злоумышленники знают, что самые квалифицированные сотрудники оператора ночью спят - иногда в это время они и начинают. В данном случае многое зависит от желаемого результата атакующих – заблокировать доступ к ресурсу легитимным пользователям, или “замести следы” другой неправомерной деятельности с сайтом жертвы. Кстати, атак с мощностью более 2-3 Гбит/с мы пока не наблюдали, это был наш пик. А вот средний уровень - 500-1024 Мбит/с - мы видим практически постоянно", рассказывает г-н Мирошниченко.

Цена за безопасность

В настоящий момент у "РТКомм" до сотни клиентов купили и используют услугу "защита от DDoS" и это при том, что сама услуга стартовала как отдельное приложение, отдельный сервис только в декабре 2009 года. "Правда, у нас и до этого были клиенты, которых мы защищали таким образом, - отмечает г-н Мирошниченко, - потребность была достаточно значительная: некоторые сервисы под атакой находятся практически постоянно. До запуска около полутора лет мы "обкатывали" всю технологию, разрабатывали процедуры внутри компании, приводили наши системы в порядок для нужного уровня SLA- надо было понять как мы будем его обеспечивать".

Тарификация по защите от DDoS у "РТКомм" возможна в двух основных вариантах: постоянный платеж в виде абонентской платы, либо небольшая "абонентка" и платеж за каждую удачно отбитую атаку (провайдер ее, конечно, сам не эмитирует :). В любом случае есть первоначальный платеж, но он не за мифическую "настройку оборудования", "скорее речь идет о небольшом технической аудите в плане информационной безопасности - мы многое рассказывает клиенту о его трафике и выдаем полезные рекомендации по защите его сети и только после этого согласовываем наши совместные действия в случае нападения", - отмечает Иван Мирошниченко. За такой аудит, в зависимости от вида отчетности, клиенту надо будет заплатить 10-20 тыс. руб. Изучение ресурса и трафика клиента, обычно, продолжается 10-14 дней и еще 48 часов на подготовку документации.

Кстати, услуга по защите включает в себя некоторые опции. К примеру, online отчетность о трафике, определенные виды информирования (не только почта, но и телефонный звонок: не обязательно в случае атаки, но и в случае потенциальной проблемы), выбор типа защиты - автоматическая реакция, либо "руками". Сама же стоимость защиты от DDoS будет у "РТКомм" варьироваться совсем не от мощности канала заказчика, а от количества объектов, которые встают под защиту. Под объектом

понимается оборудование пользователя с определенным диапазоном IP-адресов. Как минимум - один объект, но их может быть и три и пять и больше. К примеру, если клиент хостинговая компания, то он может разделить своих клиентов на категории и к каждой категории применять отдельные правила анализа трафик и методы защиты. В "РТКомм" пока спокойно относятся к тому, что их услуги перепродаются конечным пользователям с помощью ЦОДов или операторов связи второго уровня - говорят, еще не готова розничная система продаж, ее "поставят на ноги" за год, а пока такая схема вполне допустима. Самое интересное - так это тот факт, что некоторые хостеры продают эту услугу от своего имени, не упоминая, что у них не хватает оборудования и специалистов для таких действий.

За защиту одного объекта в месяц клиенту "РТКомм" надо будет заплатить 16-18 тыс. руб., если клиент выбирает постоянный платеж. Либо абонентская плата ниже 10 тыс. руб. и от 25 до 35 тыс. руб. за отбитие каждой DDoS-атаки: своеобразный антикризисный тариф для тех компаний, где DDoS все-таки редкость. Цифры, откровенно говоря, не очень большие, но это начальная стоимость, порог от которого начинается разговор. Для сравнения отметим, что стоимость, к примеру, простоя интернет-банка исчисляется уже сотнями тысяч долларов за несколько часов.

Относительно скорости канала у своих клиентов г-н Мирошниченко был достаточно откровенен. "Если честно, то мы всегда рекомендуем пользователям ее увеличивать, когда они заказывают услугу защиты от DDoS. Это облегчает работу систем защиты. Ведь при защите мы используем, в том числе, вероятностные методы, и какое-то количество паразитного трафика туда все равно попадет. А если у клиента "узкий" канал, то даже средней по мощности атакой его достаточно быстро "задавят", даже если мы очистим 99% паразитного трафика просто массой. А с широким каналом у нас будет какое-то время для более подробного анализа угрозы, прежде чем ресурсы и приложения клиента "упадут". Правда, услуги временного расширения канала на время DDoS-атаки у "РТКомм" пока нет, мотивируют это тем, что таких запросов им пока не поступало, да и оперативно увеличить полосу на последней миле не всегда удается. "Все-таки защита от DDoS - это всегда совместная работа с клиентом,- продолжает он. - К примеру, клиенту желательно информировать нас о своей предполагаемой активности - о маркетинговых акциях, ожидаемых "всплесках" посещения его ресурсов со стороны легитимных пользователей".

Показатели SLA

Самое интересное в договорах с клиентом - это формулировки. "Мы пока не стали четко формализовать понятие DDoS-атаки, как это не парадоксально звучит, - признается г-н Мирошниченко. - По сути, защита от DDoS - это динамичный адаптивный процесс и если сейчас зафиксировать типы и виды атак, то завтра появятся новые и о чем нам тогда говорить с клиентами? Правда, те компании, которые "встают под защиту" это, в основном, понимают, поэтому мы гарантируем им работу приложений, а не процент отбития какого-то вида атак. То есть мы не говорим, что отобьем 99,9% атак - это сейчас уже далеко не мерило успеха. Главное, чтобы была доступность к основному виду услуг, которые они потребляют (доступ в Интернет) и успешность работы приложений, на которых клиент, собственно говоря, зарабатывает деньги".

Таким образом, в SLA с "РТКомм" фигурируют несколько основных показателей. Первый - это время реакции на атаку. В рабочее время активные действия начинаются в течение 15 минут после заявки пользователя об атаке (это по договору нам надо согласовать с ним свои действия), либо в случае автоматического детектирования. Второе - скорость восстановления сервиса. "К сожалению, мы не можем гарантировать, что через 20 минут мы все отобьем - все сильно зависит от типа атаки. Но в течение 2-х часов (рабочее время) или 8-ми часов (нерабочее) для самого дорогого SLA все должно работать. Для начального уровня SLA в рабочее время порог работоспособности сервиса - 4 часа. Правда, делений по уровням приложений (что должно работать в первую очередь, а что может и подождать - Прим. ред.) пока нет - это в планах".

О команде специалистов, которые занимаются защитой от DDoS нам, традиционно, говорили очень осторожно. «Есть мнение, что борьба с DDoS – процесс творческий, - говорит г-н Мирошниченко, - но часто творчество возникает там, где не хватает знаний. У нас есть большое желание превратить процесс все же в технологию. По моему мнению, правильнее было бы говорить о тандеме экспертных знаний специалистов, помноженных на опыт в данной области. Безусловно, также важен хороший “инструмент”. Мы с большой ответственностью подошли к вопросу подбора команды для реализации проекта построения защиты от DDoS. Для этого у нас создан специальный отдел “проверенных” товарищей, которые не первый год занимаются темой DDoS».

По словам г-на Мирошниченко "это специалисты высокого уровня, которые работают с клиентами индивидуально. Опыт работы - от пяти лет, обучались на спецфакультетах гражданских ВУЗов, работали до этого или в спецслужбах или крупных интеграторах, которые занимались этим вопросом. Общая численность - около 10 человек, 60-70% своего времени эти люди тратят именно на защиту от DDoS". Дежурства специалистов в центре контроля сети есть, но в нерабочее время этот персонал там не находится. Мониторинг настроен таким образом, что предпринять действия "в горячем режиме" могут и специалисты не самой высокой категории. Если есть серьезная проблема -

специалисты подключаются к сети удаленно для координации действий по защите того или иного клиента. Подобное происходит не более десяти раз в месяц - ехать для этого на работу не обязательно. Часто, к слову, клиенты сами не готовы работать ночью - по их просьбе все "боевые действия" начинаются только с утра.

Перспективные планы

В настоящий момент, имеющаяся система защиты, специалистов "РТКомм" устраивает. Во всяком случае, менять Cisco Guard в настоящий момент в "РТКомм" не намерены - во всяком случае пока такой задачи не стоит. Но, сейчас специалисты компании начинают интеграцию в систему оборудования другого крупного производителя в данной области, а также активно тестируют системы третьего - но что это за компании нам не рассказали.

Кроме того, "у нас уже существует потребность в собственной разработке дополнительных модулей, которые могли бы "закрыть" некоторые виды DDoS-атак, которые могут угрожать клиентам даже при наличии двух систем. Это не страшно и мы с ними справляемся, - говорит г-н Мирошниченко, - но приходится выполнять большой объем ручной работы и экспертных действий, а ведь его можно автоматизировать. Вот этим мы в самое ближайшее время и займемся - благо опыта и понимания, как это должно работать, у нас достаточно. В любом случае, работа той системы, которую мы построили, нас удовлетворяет на 90%, а это вполне хороший показатель".

По поводу рынка защиты от DDoS г-н Мирошниченко высказывает вполне распространенное мнение : "Он не сформирован, конкуренция есть, но очень небольшая". По поводу небольших "защитников" с самописными решениями он скептичен: "В числе конкурентов мы их не видим, поскольку мы общаемся с клиентами, которые ходили по многим таким компаниям, но не получили услугу защиты с требуемым качеством. Причем, именно такие клиенты у нас, как правило, остаются". Кроме того, он отмечает, что наибольшая конкуренция ожидается, для начала, на рынке крупных заказчиков: "Зачастую именно они "сидят" у двух-трех операторов связи своими каналами связи и стойками в ЦОДах (резерв), поэтому стараются закрывать все свои каналы доступа от DDoS".

Правда, взаимодействие между операторами в такой ситуации пока не происходит: если один канал под атакой, то "соседний" провайдер может и не знать о том, что активное противодействие DDoS уже ведется “конкурентом”. "У нас больше примеров, когда с запросом о сотрудничестве (или с просьбой о прикрытии источника атаки) к нам обращается западный оператор связи, имеющий с нами пиринг, а не российский оператор связи". Но при развитии рынка данных услуг, когда услуга защиты от DDoS станет действительно неотъемлемой частью доступа в Сеть, операторы сами придут к прямому оперативному взаимодействию без какого-либо государственного воздействия или руководящего указания. "Пара лет и рынок сам отрегулируется", - уверен Иван Мирошниченко.