"Акадо Телеком": "В начале года мы обучались на "живых" клиентах"

Защита от DDoS - явный тренд сезона, причем не в теоретическом, а уже в практическом плане. С запросами о такой услуге к сервис-провайдерам обращаются не только крупные корпоративные клиенты - это интересует компании любого уровня, которые зарабатывают деньги в Сети. Репутация и финансы - это то, что предпочитают защищать от атак злоумышленников российские компании в настоящий момент. Правда, далеко не все сервис-провайдеры могут представить заказчикам более-менее сформулированное тарифное и "товарное" предложение в этом направлении. Одной из компаний, которая об этом подумала является "Акадо-Телеком" - в коммерческий режиме услуга "Защита от DDoS" будет представлена в конце августа, но нам удалось побеседовать об этом с первым заместителем генерального директора, техническим директором компании Юрием Скобелевым.

Специфика внедрения

Основной двигатель для запуска услуги по защите от DDoS - уже не желание сервис-провайдеров казаться инновационными и современными: деньги инвестируются только под конкретный запрос. Поэтому, желание заниматься подобными услугами возникает как только конкретная компания получает если не массовый, то достаточно значимый поток информационных запросов по вполне определенному направлению. "Так и с защитой от DDoS, - говорит Юрий Скобелев - это не отдельная услуга, а дополнительный сервис, в основном, для тех клиентов, которые и так уже заказывают у нас услугу доступа в сеть Интернет или находятся на хостинге в нашем ЦОДе".

Типичный запрос от клиентов - это возможность предоставления услуги защиты от DDoS-атак как локальных серверов клиентов, так и серверов, установленных в ЦОДе. Причем, согласно внутренней статистике, половина обращающихся компаний заявляет о своем желании получить эту услугу до начала атаки. Остальных приходится "спасать" уже во время возникшей проблемы.

В основном, большая часть обращений приходится на финансово-кредитные учреждения и всех тех, компаний, которые как-либо связаны с торговлей в Сети интернет. Кроме того, определенное количество запросов поступает от клиентов, которые ощущают атаку на свои системы авторизации - это компании, которые оказывают локальные услуги для третьих сторон: к примеру, электронные процессионговые системы и платежные системы, работающие с "электронными деньгами", виртуальные обменные пункты. Пик обращений, по информации Юрия Скобелева, был в ноябре прошлого года - причем, не просто информационных, а запросов на предоставление услуг поступало 5-7 в месяц. С тех пор количество обращений находится примерно на аналогичном уровне. Кроме того, "помогло" сервис-провайдерам и письмо ЦБ РФ для коммерческих банков, где настойчиво предлагалось запрашивать у поставщиков ИТ-услуг защиту от DDoS для безопасности, в основном, веб-сайтов с интернет-банками.

Внедрять решение по защите от DDoS в "Акадо Телеком" решили в два этапа. Самый первый - использование "старых запасов" в виде Cisco Guard: это было "промежуточное решение", - признается Юрий Скобелев, - но надо было, с одной стороны, показать клиентам как это примерно будет работать, с другой - протестировать конкретное решение. На нем проработали всю осень 2009 года, до тех пор пока не было принято решение о закупке продукта от Arbor Networks.

Формально в "Акадо Телеком" заявляют, что выбор поставщика для анти-DDoS системы был проведен "после тестирования оборудования различных вендоров".



Юрий Скобелев

Но на самом деле, даже если такое мероприятие и имело место, то выбор конечного поставщика был обусловлен, в том числе и некоторой безысходность - крупных игроков на этом рынке пока нет и решение это было практически безальтернативным. "Данное оборудование, на наш взгляд, - уверен Юрий Скобелев, - предоставляет необходимые возможности по наблюдению за профилем трафика клиента, позволяя формировать требуемое количество отчетов для детального анализа трафика и, как следствие, понимать профиль атаки".

А вот по поводу того, что лучше «коробочные» решения или самописные в "Акадо Телеком" уверены: только «коробочные», т.к. разработкой этого решения занимается команда подготовленных специалистов, и этот продукт будет поддерживаться в течение заявленного времени, так что возможное негативное действие «человеческого фактора» при таком подходе минимально". Заказ решения был проведен - в декабре 2009 года, поставка - в мае, монтаж - в июне. В течение полугода система работала в demo-режиме: мы тестировали решение на применимость к нашим условиям работы. практически все ограничения были сняты. Единственное отличие - это, наверное, мощность "порта очистки": он был 1 Гбит/с, а не 10, как в боевой версии.

Без сомнения, борьба с DDoS - процесс творческий, с этим специалисты "Акадо Телеком" согласны: "дело в том, что при отражении атаки ее профиль меняется в течение времени. И команда специалистов, которые управляют системой защиты, должна проанализировать этот профиль и адекватно изменить ее настройки оборудования . От уровня их подготовки зависит, насколько наши клиенты смогут «спать спокойно»", - говорит Юрий Скобелев.

Правда, что за команда находится "за пультом" на стороне сервис-провайдера, нам так и не рассказали, отделавшись стандартным замечанием о том, что "команда подобрана из молодых энергичных специалистов, ранее занимавшихся вопросами сетевой безопасности". И все. Убеждает? Меня - как-то не очень. "Утешает" в данном случае тот факт, что по мнению Юрия Скобелева, все подобные специалисты пройдут несколько авторизованных курсов обучения с обязательной сертификацией от производителя до запуска услуги в коммерческую эксплуатацию.

Правда, "в начале года мы обучались на «живых» клиентах, - с улыбкой отметил он, - но своим давним партнерам мы предложили бесплатно протестировать эту услугу».

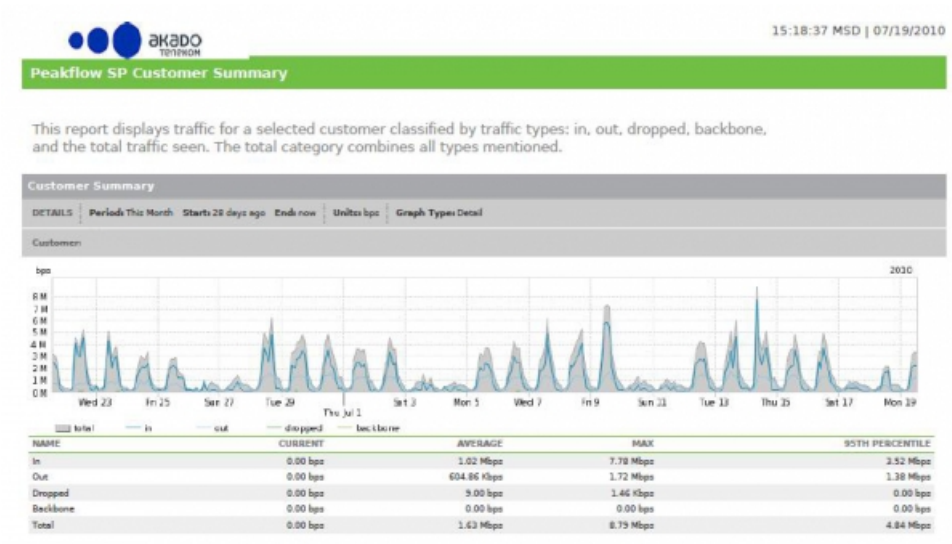
Типология решения

В настоящий момент решение для защиты от DDoS представляет собой территориально-распределенный комплекс. Причем, "основным условием эффективности подобной системы является необходимость расположить «центр очистки» как можно «выше» в структуре сети, на уровне пограничных маршрутизаторов, - говорит Юрий Скобелев. - Вызвано это тем, чтобы при возникновении атаки очистить легитимный трафик на входе в сеть, тем самым не допуская дополнительную нагрузку на оборудование, маршрутизирующее трафик к клиентам". Центр анализа данных у "Акадо Телеком" находится в телекоммуникационном центре на Варшавском шоссе, а два центра очистки - на площадке "Акадо Телеком" в РАН и на узле "Владимирский" - все внутри МКАД. Отметим, что решение от Arbor установлено не только в "Акадо Телеком", но и у "Комстар-ОТС", а также у ТТК.

Решение, которое установлено у "Акадо Телеком" базовое - не начального, а среднего уровня для мощного сервис-провайдера, обладающего собственной опорной сетью. У него, разумеется, есть

возможность масштабирования - оно может отбивать атаки до 10 Гбит/с на один порт. "Более мощное решение понадобится не ранее, чем через год, - отмечает Юрий Скобелев, - это уже будет кластерное решение с совершенно другой производительностью. Возможности по масштабированию существующего решения позволяют это сделать оперативно и с минимальными затратами".





"Система защиты классифицирует атаки в автоматическом режиме - низкий, средний и высокий, а в связи с тем, что профили атак индивидуальны для каждого объекта защиты и могут меняться в течение времени мы создаем индивидуальные профили защиты для наших клиентов, также мы получаем обновления ПО от производителя аппаратно-программного комплекса. Низкие и средние атаки отбиваются в автоматическом режиме, а вот высокие - это уже ручное управление. Дело в том, что необходимо гибко настраивать оборону, выставлять новые фильтры и т.д., поскольку атакующая сторона регулярно меняет тактику", - говорит Юрий Скобелев.

Хотя, некоторые клиенты не хотят, чтобы система работала полностью в автоматическом режиме - им требуется подтверждение атаки со стороны оператора и только после этого можно включать систему для очистки нелигитимных запросов. Обычно, такие заказчики переживают из-за того, что их рекламные компании, которые дают взрывообразное посещение веб-ресурсов, могут посчитать за DDoS-атаку и "отсечь" множество полезных и целевых клиентов.

"Чаще всего мы наблюдаем атаки мощностью 200-300 Мбит/с, причем на клиентов, у которых канал в Сеть составляет от 2 до 10-20 Мбит/с: их пытаются атаковать с большим запасом. Редко у какой компании есть канал со скоростью выше 100 Мбит/с - это уже крупный корпоративный клиент с

сотнями сотрудников и разветвленной филиальной сетью. Ну а атаки мощностью в гигабиты пока на нашей сети не отмечались - с их помощью пытаются "нападать" только на операторов связи", - отмечает г-н Скобелев.

Надо отметить, что современные DDoS-атаки далеко не всегда работают "в лоб": к примеру, обрушение ресурса может использоваться только как "дымовая завеса" для того, чтобы злоумышленники начали атаку по похищению ЭЦП пользователей или могли добраться до данных кредитных карт. То есть недоступность ресурса уже не единственная цель мошенников - главное для них получить конфиденциальную информацию, которую можно реализовать впоследствии. Понятно, что это заказные атаки - и здесь легко ошибиться для ИТ-специалистов компании: они бросают все силы для защиты доступности своего веб-ресурса, "оголяя" другие рубежи обороны. Часто банки считают, что способны с такими атаками справиться сами - но часто самоуверенность ИТ-специалистов "на зарплате" совершенно не обоснованна: ресурсов и знаний для этого не хватает. Учитывая тот факт, что атаки на финансово-кредитные компании идут практически круглосуточно, в "Акадо Телеком" считают, что им точно пора привлекать специалистов для помощи в такой борьбе. "Многие клиенты считают, что могут справиться с ddos-атакой сами, - но это совсем не так", - уверен Юрий Скобелев.

Практика перевода

В настоящий момент прайс-лист у "Акадо Телеком" уже сформирован. Деньги берутся с клиентов за два основных действия. Первое - это т.н. инсталляционный платеж за настройку системы и создание "образа" нормальной нагрузки на тот или иной ресурс, стоить это будет порядка 200 долл. И второе - это абонентская плата за защиту, стоимость которой будет варьироваться от мощности канала, который потребляет клиент: нижняя граница за 2 Мбит/с будет составлять от 250 долл.: это дополнительный платеж именно за эту услугу. За эти деньги в "Акадо Телеком" обещают отбивать все атаки любой мощности, которые могут "положить" ресурсы клиентов надолго: до 1-10 Гбит/с. "Дело в том, что атака "на входе" может быть гораздо больше, чем суммарная пропускная способность каналов клента - важно настроить защиту так, чтобы доступность ресурсов не пострадала", - отмечает Юрий Скобелев.

Причем, оборудование клиента может стоять где угодно - либо в ЦОДе "Акадо Телеком", либо на его технологической площадке: главное, чтобы он был к Сети именно с помощью этого провайдера связи. Кстати, цена услуги от этого тоже не меняется: "ведь комплекс защитных мероприятий одинаков", - уверен Юрий Скобелев. "Кстати, перед заказом конкретной услуги клиент может ее протестировать в течение недели, - отмечает г-н Скобелев, - но если он не будет атакован, то никакого отчета по результатам действия системы он просто не получит. Но протестировать взаимодействие своих и наших технических специалистов вполне возможно. Настройка профиля трафика клиента может занимать минимально неделю, рекомендуемый срок - до 4 недель, после чего этот профиль добавляется в нашу базу и система начинает отслеживать различные аномалии, которые связаны с превышением средненормативных показателей для каждого конкретного клиента".

Причем, со скоростью перевода трафика на «центр очистки» для новых клиентов, которые находятся под атакой, окончательная ясность была только примерной. Да, специалисты "Акадо Телеком" подтвердили, что все услуги оказываются в кредит - то есть достаточно заключить договор на доступ в Сеть, чтобы, чисто теоретически, подключить эту услугу. Или поставить свое оборудование в ЦОД компании. Но скорость реакции будет индивидуальной в каждом случае - непонятно сколько времени у ИТ-специалистов клиента уйдет времени на решение технических вопросов. Между тем, размещать оборудование в ЦОДе в "Акадо Телеком" готовы даже ночью и в выходные дни. Но выразили легкое недоумение тем, что при "горячей" защите проблему пытаются решить с помощью дорогого решения - размещения "железа" в ЦОДе, оснащенного мощными каналами связи и специальными системами безопасности, которые работают по системе 24x7x365.

Не смотря на то, что услуга будет только запущена в коммерческую эксплуатацию, у "Акадо Телеком" уже есть уже один "боевой" договор с коммерческой компанией (это банк), а также несколько клиентов включила защиту от DDoS в тестовом режиме (время на тестирование - индивидуально). Широкая компания по привлечению абонентов начнется с осени - до конца 2010 года планируется подключить до 300 компаний из 2,5 тыс. тех клиентов, которые есть у "Акадо Телеком" в настоящее время: на самом деле, это очень оптимистично. Дело в том, что годовые бюджеты на ИТ и телекоммуникационные услуги у многих компаний уже сверстаны и добавить туда новую услугу достаточно сложно.

Наличие возможности оказать услугу по защите от DDoS полезно не только с т.з. работы с конкретным корпоративным клиентом, но и " для участия в тендерах на комплексное телекоммуникационное обслуживание клиентов", - отмечает Юрий Скобелев. - В наибольшей степени такой подход, конечно, интересует компании бизнес-сегмента, а бюджетные организации не так активны в этом вопросе.

Кстати, кроме крупных сервис-провайдеров на рынке защиты от DDoS есть интересная группа

небольших компаний, которые специализируются именно на отбитии уже идущих атак - их цены не очень велики, а самописные решения для обороны могут показывать вполне высокую эффективность. Правда, в "Акадо Телеком" к конкуренции с такими компаниями относятся спокойно. "Эти решения могут действовать хорошо, качественно и гибко, предлагая клиентам буквально вручную "отскрести" их трафик и настроить нормальное функционирование сети. Причем, вне зависимости от провайдера и от ЦОДа, где находится клиентское "железо", - говорит Юрий Скобелев. -. Но наши возможности несопоставимы - мы можем работать с десятками клиентов одновременно, они - с единичными заказами. Вряд ли у них может быть оборудование операторского класса, да и порог атак, с которыми они могут справиться, до конца не понятен". В любом случае, рынок защиты от DDoS пока слишком молод - места хватает всем и даже "локтевой" конкуренции не заметно вовсе.