«Синтерра»: "Качественный DDoS - угроза национальной безопасности

Защитой от DDoS занимается множество разных компаний - от локальных ЦОДов, распределенных систем под управлением авторского ПО, до магистральных операторов связи, защищающих своих клиентов на всей территории страны. Причем, число клиентов, которым требуются такие услуги, постепенно растет. Оно и понятно - если репутация или бизнес-процессы компаний каким-то образом зависят от работоспособности веб-ресурсов, размещенных в Сети, то необходима защита от этого достаточно эффективно оружия, имеющего весьма избирательное действие. О своем подходе к защите компаний, сроках взятия их "под зонтик" безопасности, типологии DDoS-атак нам рассказал ***Андрей Бугаенко, директор по информационным технологиям компании «Синтерра», недавно перешедшей под контроль «МегаФона».***

Собственная разработка

Выработкой стратегии по комплексной защите от DDoS в "Синтерре" приступили еще в 2007 году, когда Южная телекоммуникационная компания стала жертвой одной из самых мощных и длительных сетевых атак в рунете - общий объем "мусорного" трафика достигал 10 Гбит/с, причем атака длилась более полутора месяцев. "Это была четко спланированная и эффективно управляемая акция, - вспоминает Андрей Бугаенко, - причем невольно пострадали и мы - через тогда принадлежавший «Синтерре» РТКомм.Ру, сетями которого, среди прочих магистральных провайдеров, пользовалась «ЮТК». Бот-сети злоумышленников тогда постоянно адаптировались к попыткам противодействия - на сеть ЮТК и его магистральных поставщиков были установлены несколько решений по защите, но все они с нагрузкой фактически не справились. Достаточно быстро отказало решение Cisco Guard: не помогла даже архитектура Cisco Multi-Verification Process (MVP) с многоуровневой защитой, Arbor Networks, установленный в сети РТКОММ тоже справлялся с трудом. Временная передышка была достигнута только после того, как предприняли кардинальные меры со стороны технических служб компаний, участвовавших в подавлении атаки, но потом все началось снова. Победы не было - атака закончилась сама собой. Но оставила явное беспокойство государственных чиновников, да и бизнеса, по поводу незащищенности инфраструктуры операторов, которые обеспечивают функционирование сайтов госструктур и крупных корпоративных сетей связи перед этой угрозой. В современном цифровом мире концепция защиты ресурсов изменилась, образно говоря, основной задачей информационной безопасности в Сети сейчас является не ограничение доступа к информации, а обеспечение непрерывности функционирования значимых ИТ-сервисов и максимальной доступности информационных ресурсов. Учитывая тот факт, что на наших ресурсах обслуживается существенное количество госзаказчиков и крупных корпоративных клиентов и контент-провайдеров с весьма высокими требованиями по надежности функционирования и доступности критических бизнес-приложений, было принято решение не только внедрить на сети «Синтерры» решение мирового лидера по защите сетей операторского класса Arbor Networks, но и создать собственное решение для защиты от DDoS операторского класса".

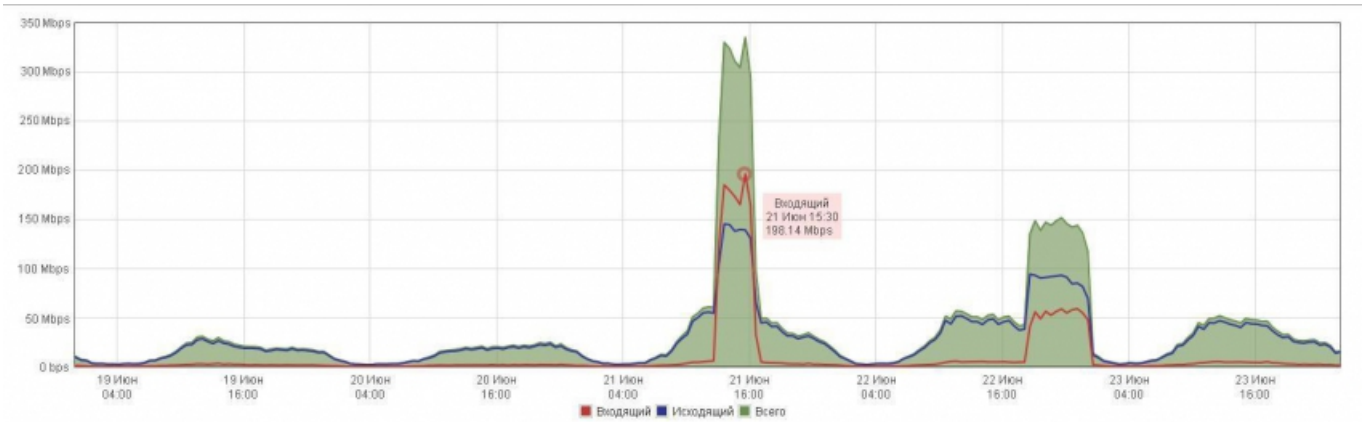
За последние полтора года на "проект А", как с улыбкой его называют в "Синтерре" (кодовое имя проекта мне так и не сказали) было израсходовано более 70 млн. руб. – работа проводилась в несколько этапов. На первом этапе сформирована группа серьезных экспертов из числа представителей ведущих научных школ РФ, госорганов, представителей телекома. Они обозначили цели и задачи, масштабы проблемы и в итоге представили формализованное техническое задание. Следующим этапом стало уточнение и детализация технического задания экспертами и практиками из мира телекоммуникаций и ИТ. Реализовать техническое задание было поручено "МФИ-Софт". "В России есть великолепные "мозги" - специалисты, которые глубоко понимают все особенности сетевых атак, структуру трафика на магистральных сетях, умеют программировать уникальные алгоритмы для высокоскоростных вычислений. Важно грамотно поставить задачу на создание эшелонированных оборонительных рубежей, выбрать исполнителя, который наиболее полно отвечает решаемой задаче", - говорит Андрей Бугаенко.

Кстати, выбор исполнителя не предполагал никакого конкурса или тендера. "Мы исходили из ситуации, что на российском рынке есть только две спецслужбы и три-четыре коммерческие компании, специалисты которых способны создать по нашему заказу необходимое решение. С компаниями получилось следующее: нам нужно было российское предприятие, обладающее опытом

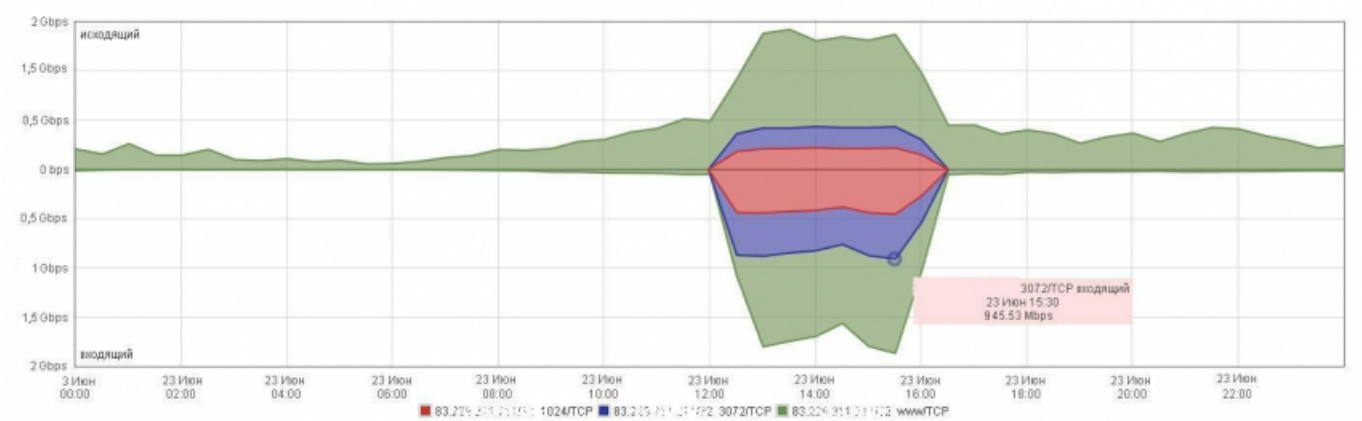
промышленного аутсорсингового программирования и глубокими знаниями сетевых технологий в их магистральном аспекте. Хорошие специалисты есть, например, в "Лаборатории Касперского", но компания нацелена, в первую очередь, на создание продуктов для себя. Качественная экспертиза была в CBOSS и еще ряде компаний, но риск был примерно аналогичным. Поэтому мы выбрали "МФИ-Софт", которая на постоянной основе работает по аутсорсинговым схемам. Они разрабатывали продукты для крупнейших производителей телекоммуникационного оборудования (например, Nortel и Siemens), их софтсвичи работают не только в российских операторских сетях, но и у зарубежных операторов, а разработанный МФИ-Софтом российский телефонный узел получил высокую оценку руководителями государства и операторским сообществом, поэтому специфика отрасли связи им вполне понятна, что такое операторский магистральный трафик они представляют очень хорошо".

Если провести параллель с автомобилестроением, сейчас "проект А" у "Синтерры" закончил технические испытания на сети, и с декабря прошлого года система работает в режиме постоянной эксплуатации на сети «Синтерры». "Система умеет анализировать трафик объемом до 250 Гбит/с, а чистить - до 9 Гбит/с. Это вполне сопоставимо с параметрами решения Arbor Networks», - с явной гордостью за сделанную работу утверждает г-н Бугаенко. Причем, он отмечает, что на рынке, конечно, существует множество хороших решений, которые внедрены в различных ЦОДах. Все они хорошо блокируют атаки до 1 Гбит/с, нацеленные на одного-двух клиентов. Если мощность бот-сети вырастает, то, по мнению г-на Бугаенко, эффективность такой защиты можно поставить под вопрос.

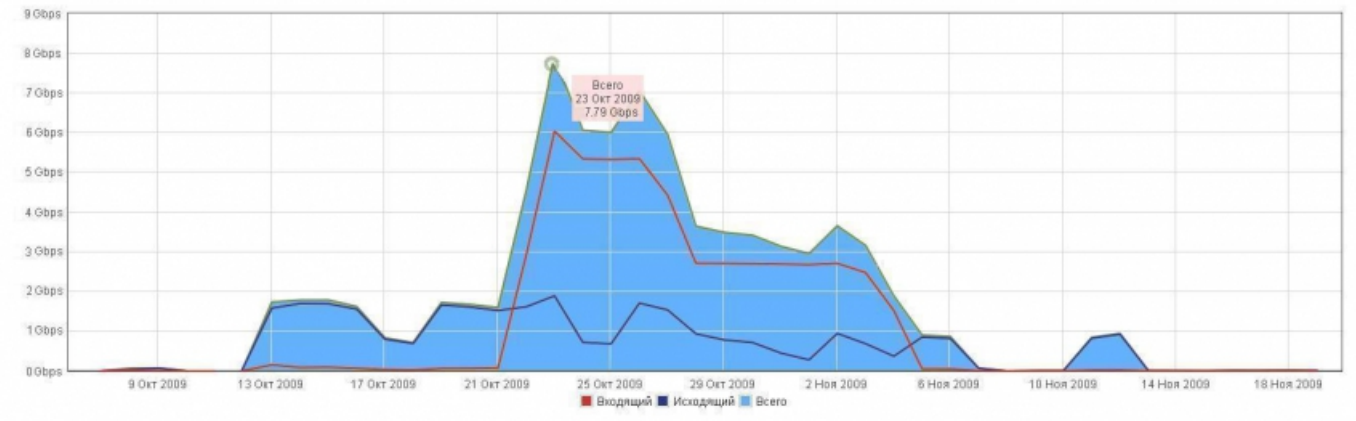
Самое время отметить, как по мнению директора по информационным технологиям "Синтерры" классифицируются наблюдаемые на сети DDoS-атаки. К первому классу относятся самые различные "пробы пера". "Дети балуются, - улыбается он. - Примерно также, как раньше это было с компьютерными вирусами. Ну что такое атака 100-150 Мбит/с на час или пару дней? Ее может парировать, не особенно напрягаясь, даже средней руки ЦОД. Ни системности в этой атаке, ни творческого подхода. Бороться с ней не особенно сложно - на такие атаки у нас приходится до 80% срабатываний наших систем защиты, они и блокируются в автоматическом режиме, поскольку идут по давно известным алгоритмам".



Второй вариант - это использование хорошо организованных «аутсорсинговых» бот-сетей. "В данном случае злоумышленник, как правило, «заказывает» конкретный информационный ресурс, - говорит г-н Бугаенко. - Скорость может быть до 1-2 Гбит/с и выше, а срок атаки зависит от толщины кошелька злоумышленника. Обычно это одна-две недели. Да, это уже более серьезный уровень, но чаще всего такая атака осуществляется без особенных изысков: шаблонные схемы, заблокированные бот-сети исполнители не особенно стремятся восстанавливать, подключая дополнительные атакующие мощности. Обычно заказчику атаки хватает временной недоступности ресурса-конкурента. Хотя, в данном сегменте, временами встречаются интересные варианты реализации, но их, обычно, просто тестируют для реализации атак более высокого класса ".



И, конечно, третий вариант - мощные заказные атаки. "В данном случае все гораздо серьезнее, - отмечает Андрей Бугаенко, - привлекаются значительные ресурсы и по количеству хостов в бот-сетях, по объему трафика, меняется тактика атаки. Максимальная нагрузка, которую мы видели в рунете при атаке на ресурс одного из клиентов - 4,5 Гбит/с. При этом атака имеет хорошо прописанный сценарий. Для таких заказов у организаторов DDoS есть свои операторы, управляющие бот-сетями, которые постоянно мониторят доступность атакуемого ресурса, пытаются навязать свой сценарий. Происходит это не часто, но всегда метко - ведь перед такими "мероприятиями" ИТ-ресурсы атакуемой компании и оператора связи подвергаются разведке и анализу".



Комплексная защита

Защиту от DDoS "Синтерра" предлагает в любом из своих ЦОДов. Система состоит из нескольких компонент, основой которой является комплекс Arbor Networks и собственная разработка. Бесспорно, что система находится в распределенном виде, ее компоненты распределены по сети передачи данных в т.н. точки тяготения трафика. Во всех этих местах находятся т.н. "очистители", подключенные к каналам параллельно, а аномалии на сети оценивает специальный "анализатор". Как только детектируется DDoS-атака, происходит перенаправление того или иного трафика для очистки от паразитического трафика в "очиститель", где его «перемалывают» мощные специализированные аппаратные решения и, после этого, возвращают его в ту же самую точку, откуда он был взят. "При этом предельная задержка, которую мы отмечаем, составляет всего 0,2 мс при пике загрузки в 9 Гбит/с", - рассказывает г-н Бугаенко.

Тарифы «Синтерры» на услугу «Противодействие сетевым атакам на информационные ресурсы через сеть Интернет»

Скорость подключения клиента	**1 Мбит/с**	**10 Мбит/с**	**100 Мбит/с**	**1 Гбит/с**
Единовременные платежи	250 руб.	2,5 тыс. руб.	25 тыс. руб.	250 тыс. руб.
Ежемесячные фиксированные платежи	100 руб.	1 тыс. руб.	10 тыс. руб.	100 тыс. руб

Вся система базируется на "самых обычных серверах, конкретное наполнение каждого зависит от мощности каналов связи. "Мы не заказывали ничего суперспециального", - говорит Андрей Бугаенко. Правда, производителя "железа" представители "Синтерры" назвать категорически отказались. Сама же система, по их словам, представляет собой "облако, которое может управляться из нескольких региональных центров контроля". Мониторинг проходит в online-режиме в течение 24 часов.

В настоящее время у "Синтерры" несколько десятков клиентов, которые пользуются услугой по защите от DDoS. Обязательным условием для этого является перенос своего оборудования в один из ЦОДов оператора связи. "Здесь как с автомобилем: можно ставить на него множество различных сигнализаций и даже застраховать по КАСКО, но если не ставите его на охраняемую стоянку ночью, то шпана запросто разобьет стекла или проткнет колеса, - уверен г-н Бугаенко. - Мы не сможем обеспечить безопасность вне нашего периметра защиты. В остальном - все достаточно просто. Как

только клиент изъявляет желание воспользоваться услугой, особенно в момент атаки, он должен практически сразу начать монтировать свое оборудование у нас в ЦОДе. За рабочий день мы готовы начать с ним работать. Хотя бывали случаи, когда оборудование к нам перевозили и ночью, но к счастью сейчас таких случаев все меньше: все-таки предвидение кризисных ситуаций является работой ИТ-специалистов заказчика, сейчас у них складывается более глубокое понимание того, что защита от DDoS необходима".

Г-н Бугаенко делит клиентов «Синтерры» на "спокойных" и "беспокойных". Первых, которые заказывают защиту заранее, большинство, до 90%. "Они знают, что им необходимо, ставят вопросы достаточно четко, отлично представляют себе свою ИТ-инфраструктуру и составляют план переезда на наши площадки таким образом, чтобы сотрудники их предприятий и потребители информации ни на минуту ни чувствовали перебоев в работе сервисов", - рассказывает г-н Бугаенко. Клиенты "беспокойные" начинают волноваться после того, как их ИТ-инфраструктура перестает справляться с трафиком, генерируемым атакующими. Тогда не избежать ночных звонков, ажиотажа и экстренной работы технических специалистов. "Хотя надо понимать, - говорит г-н Бугаенко, - что «идеальный вариант», когда у компании полстойки серверов и их можно очень оперативно перевезти, случается редко. Если это, к примеру, хостинг-провайдер с тридцатью полными стойками, или компания с распределенной сетевой и ИТ-инфраструктурой по всей стране и множеством постоянно обновляемых БД, то физически они просто так не переедут - нужно обеспечить место в ЦОДе, оценивать потребности в энергетике, тепловыделение оборудование, тщательно прорабатывать архитектуру сети и ее возможные изменения и т.п.. Мы-то готовы включить свою услугу в течение часа, но те же записи в DNS будут меняться до 12 часов". Так что разумнее думать о своей безопасности до того, как что-то случилось.

Борьба с DDoS - процесс творческий, и сильно зависит от команды, управляющей работой "железа". В "Синтерре", в лучших традициях конспирации, не стали рассказывать о том, какое количество людей у них работает на этом проекте - скорее всего, их около десятка. Причем, все это уникальные эксперты, которые отлично знают не только сами решения, но и структуры различных атак, схему сети передачи данных "Синтерры", ее особенности и нагрузки, отлично разбираются в сетевых вопросах и структуре обмена трафиком между операторами связи. По словам г-на Бугаенко, некоторых специалистов в "Синтерре" воспитывали буквально с ВУЗовской скамьи, кого-то приглашали уже состоявшимися специалистами. Из ВУЗов, откуда были взяты кадры, были названы следующие - МГТУ им. Баумана, МИФИ, МГУ им. Ломоносова, Военная Инженерно-Космическая Академия им. Можайского, Институт криптографии и связи Академии ФСБ России и т.д. Сейчас из этих специалистов сформированы группы экспертов и рабочие смены, которые работают на DDoS-защитой круглосуточно, правда находятся все в Москве. В случае начала DDoS-атаки на клиента, именно они будут на связи с ответственными ИТ-сотрудниками заказчика, чтобы координировать свои действия между ним и оператором связи.

Единственное, что тревожит г-на Бугаенко - несистемность борьбы с виртуальными угрозами. "DDoS-атака, одна из самых недооцененных угроз, в том числе национальной кибербезопасности, особенно в свете развития государственных электронных услуг", - замечает он, рассуждая о том, что в идеале необходимо создавать целую Ассоциацию российских операторов связи, которые будут бороться с сетевыми атаками с помощью обмена информации об атаках. Все-таки анализаторы и проекта "Синтерры", и решений Arbor Networks, IBM и других производителей могут обмениваться информацией обо всех новых ситуациях и, подобно эвристическому анализатору антивирусных программ, самостоятельно обучаться борьбе с новыми угрозами. Заранее, пока проблемы еще не наступили. Сейчас подобный обмен информацией возможен только в рамках двухсторонних отношений технических служб, общей системы нет. "Вот у Arbor Networks есть свой единый дата-центр, куда это оборудование, установленное во всех странах мира, "сливает" информацию о поведении бот-сетей, - отмечает г-н Бугаенко. - Других аналогичных примеров пока неизвестно. Возможно, этим займутся регулирующие органы в России. Еще совсем не поздно".