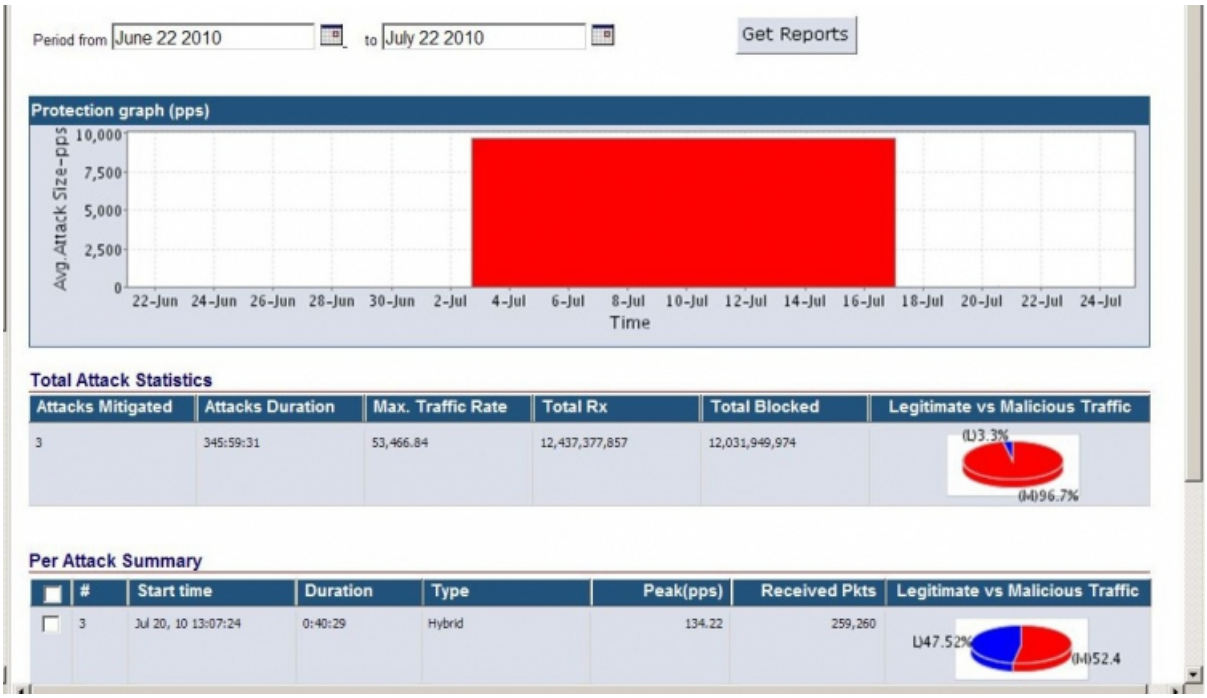
Orange: "Мы работаем на уровне индивидуальной настройки"

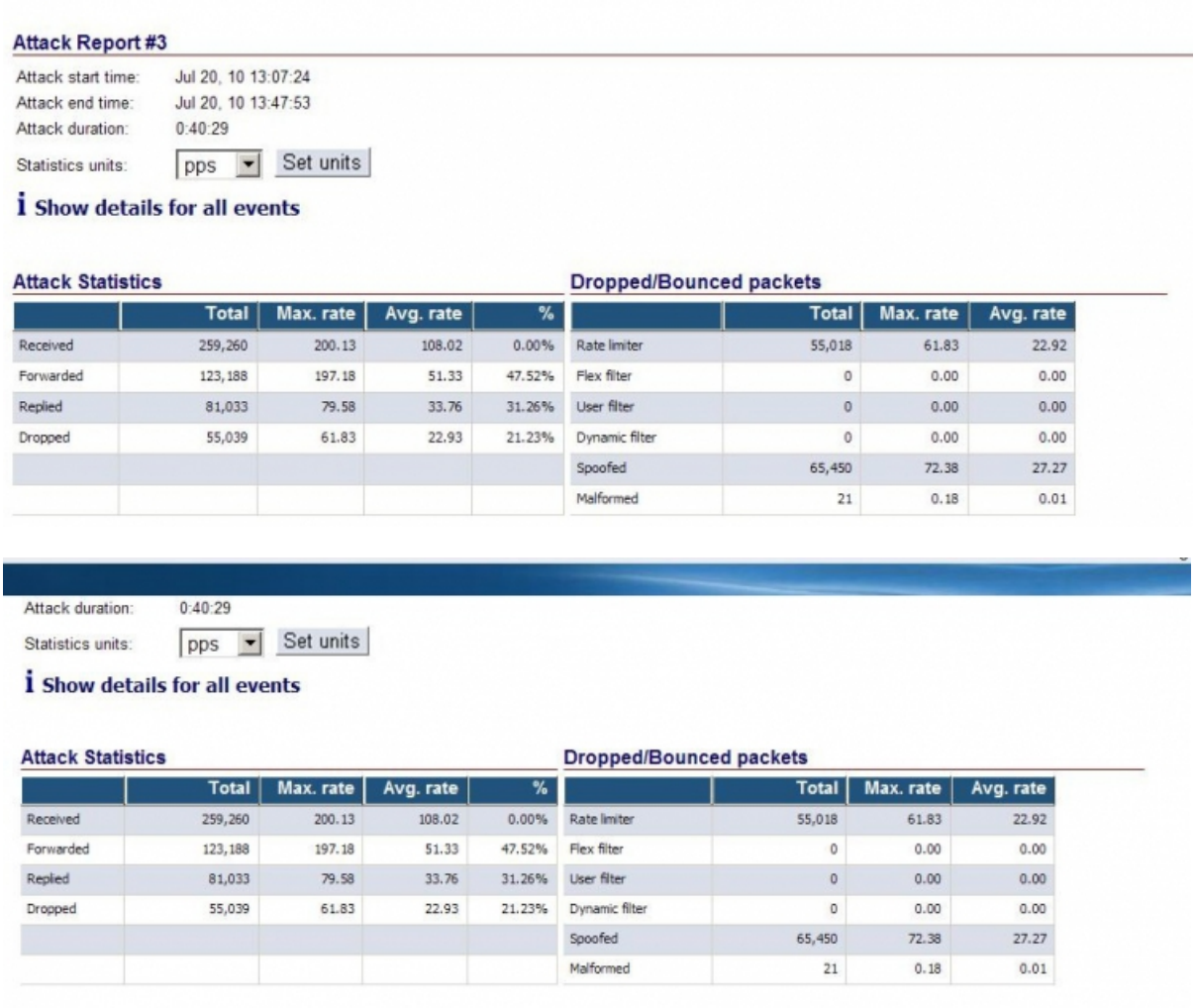


В Orange Business Service царит дух спокойствия и риски подсчитываются заранее. Во всяком случае, поговорив с Владимиром Вальковичем, руководителем Департамента технического развития и эксплуатации компании о новой услуге - Internet Umbrella, с помощью которой предполагается в режиме 24x7x365 защищать на уровне оператора связи ресурсы клиентов от DDoS-атак, у меня сложилось впечатление, что для компании это давно просчитанная, но все-таки дополнительная услуга связи. При этом, с клиентами, которые приходят «под атакой», компания не готова работать в "пожарном режиме". В принципе, «спасать и защищать» здесь готовы только тех клиентов, которые заранее позаботились о минимизации всех рисков.

ЦА для защиты

Эффективность DDoS-защиты и описание самого процесса, изложенное тезисно, можно найти на специальной веб-страничке компании, там же располагается очень приятный видеоролик с ее рекламой - все схематично "для чайников". Правда, создатели веб-страницы чуть-чуть пугают заказчиков - "за последние 7 лет мощность DDoS-атак выросла в 100 раз. В 2009 году была зафиксирована DDoS-атака мощностью 49 Гбит/сек". Это было, но только не в Рунете, где мощность в сотни Мбит/с считается уже серьезной. Подобную ситуацию подтверждает и г-н Валькович: " Одна из самых продолжительных атак, зафиксированная нами, длилась 15 дней, согласно же накопленной нами статистике среднее время атаки на наших клиентов гораздо меньше – всего 30 минут. Мощность - очень разная. Самая мощная атака, зафиксированная нами, составила 300 Мб/с, пиковое значение атакующих хостов - 6500. Средняя же мощность не превышает 10 Мб/с, 1500 атакующих хостов". Надо только отметить, что это статистика Orange Business Service – читатели моего блога вспоминали и куда как более мощные атаки, происходившие в РУнете.





Attack Report #3

Attack start time: Jul 20, 10 13:07:24
Attack end time: Jul 20, 10 13:47:53
Attack duration: 0:40:29
Statistics units: pps Set units

Show details for all events

Attack Statistics

	Total	Max. rate	Avg. rate	%
Received	259,260	200.13	108.02	0.00%
Forwarded	123,188	197.18	51.33	47.52%
Replied	81,033	79.58	33.76	31.26%
Dropped	55,039	61.83	22.93	21.23%

Dropped/Bounced packets

	Total	Max. rate	Avg. rate
Rate limiter	55,018	61.83	22.92
Flex filter	0	0.00	0.00
User filter	0	0.00	0.00
Dynamic filter	0	0.00	0.00
Spoofed	65,450	72.38	27.27
Malformed	21	0.18	0.01

Attack duration: 0:40:29
Statistics units: pps Set units

Show details for all events

Attack Statistics

	Total	Max. rate	Avg. rate	%
Received	259,260	200.13	108.02	0.00%
Forwarded	123,188	197.18	51.33	47.52%
Replied	81,033	79.58	33.76	31.26%
Dropped	55,039	61.83	22.93	21.23%

Dropped/Bounced packets

	Total	Max. rate	Avg. rate
Rate limiter	55,018	61.83	22.92
Flex filter	0	0.00	0.00
User filter	0	0.00	0.00
Dynamic filter	0	0.00	0.00
Spoofed	65,450	72.38	27.27
Malformed	21	0.18	0.01

Кстати, на той же страничке с описанием услуги, можно найти традиционные заклинания о том, что "защита от DDoS-атак особенно актуальна для компаний, работающих в сети Интернет, например, это банки, компании, работающие в сфере электронного бизнеса (интернет-магазины), ежедневно использующие системы платежей и заказов, контент-провайдеры, средства массовой информации". В принципе - вполне разумно.

Как отмечает г-н Валькович, разработкой услуги защиты от DDoS в Orange Business Services занимались в течение трех лет: "спасать" кого-то из действующих заказчиков приходилось с частотой один-два раза в месяц, причем, защита осуществлялась в индивидуальном режиме - case-by-case, стандартного решения не было. Но как только в прошлом году мы каждые четыре недели стали получать до 15 запросов на подобные услуги, пришли к решению, что необходимо поставить защиту "на поток".

Название услуги, как оказалось, придумывали достаточно долго - под красивым Internet Umbrella скрывается... Cisco Guard, который используется как основное аппаратно-программное решение для защиты от DDoS. Несмотря на заявления компании Cisco о том, что это решение в будущем имеет весьма ограниченный срок жизни , г-н Валькович выглядел спокойно: "У нас глобальное партнерство с Cisco, мы обладаем золотым статусом в России, поэтому все будет поддерживаться столь долго, сколько это нам необходимо. Мы проводили тендер на поставщика подобной системы: в нем рассматривали Arbor, Cisco Guard, решение Juniper IDP, несколько других поставщиков и самописных решений. Решение Arbor и Cisco оказались лучшими, из них мы выбрали Cisco. Дело в том, что решение от Arbor - с большим запасом мощности и более дорогое, по сути это аппаратно-программный комплекс промышленного класса. Сейчас же, в текущих условиях, нас вполне устраивает решение Cisco. И на ближайший год нам этой платформы хватит, дальше будем искать новое решение ".

Отдельно отметим ситуацию по Cisco Guard: 31 июля 2011 выйдет последняя версия этого софта, после этого, до июля 2015, будет осуществляться поддержка "железа" (то есть просто замена сгоревшего), но только для тех, кто купит сервисные контракты. Но работа над совершенствованием Cisco Catalyst 6500/Cisco 7600 Series Router Anomaly Guard Module and Anomaly Detector Module будет

завершена. Однако, в течение ближайшего года можно ни о чем не беспокоиться - защита от DDoS это не антивирус, который становится бесполезным через неделю после последнего обновления базы, а видов DDoS атак не так много, и новые варианты появляются не часто. По мнению разработчиков, для DDoS-системы от Cisco нет необходимости обновлять базу образов атак каждый месяц: "Последняя версия софта для ADM/AGM на данный момент - 6.1(6) от 13.11.2009. Насколько я понимаю принцип работы ADM/AGM (хотя точно его никто не знает кроме разработчиков), решение анализирует именно аномалии, отличия в характере трафика в обычной ситуации и при DDoS атаке. Практически искусственный интеллект :), - отметил сотрудник российского представительства Cisco у меня в блоге. - Cisco хорошо знает особенности своего решения и наши запросы, поэтому до того времени, как нам потребуется апгрейд системы, наши партнеры предложат нам альтернативу или, вполне возможно, на рынке появится другой более мощный и эффективный вариант".

Специфика "очистки"

Схема инсталляции защитного DDoS-решения от Cisco в Orange Business Services достаточно типовая. "Центр очистки у нас только один и он расположен в нашем ЦОДе, который находится в южном округе столицы. "Трафик, подверженный в атаке", который мы обнаруживаем, транспортируется сюда для очистки и "выпускается" здесь же. Основные аплинки у нас находятся в Москве, поэтому необходимо доставлять трафик в точку демаркации, где происходит взаимодействие наших "облаков". Причем, при такой топологии сети мы не испытываем сложностей с нагрузкой - трафик, даже чистый, все равно идет через столицу, - говорит г-н Валькович. - По периметру сети расставлены центры анализа информации (т.н. модули детектирования - anomally detector), которые "отлавливают" потенциально опасный трафик в общем потоке. Раньше плохой трафик просто блокировался, сейчас же пытаемся выделить из него легитимные запросы. Центров анализа у нас два: один для внешних клиентов, второй - для внутреннего использования".

Клиентам в Orange Business Services готовы предложить защиту от атаки мощностью до 1 Гбит/с, далее уже работа с аплинками напрямую. "По SLA мы фильтруем не менее 70% вредоносного трафика, - отметил г-н Валькович. - Кстати, возможна ситуация, когда наше оборудование "не видит" атаку, но доступность ресурсов клиента уменьшается. В таком случае мы должны среагировать на запрос его ИТ-сотрудников в течение 30 минут, включить фильтрацию и тюнинг очистки для того, чтобы обнаружить проблему". При атаке от 5 Гбит/с у Orange Business Service автоматически начинает действовать специальный регламент взаимодействия с операторами Level1. "Мы начинаем взаимодействовать с ними вплоть до полной фильтрации определенных блоков адресов, кроме того, блокировка трафика тоже возможна. Как ни странно, но большинство бот-сетей работают из-за рубежа, мощности отечественных бот-сетей для этого пока не хватает: многое идет из Европы, США и Азии. В целом, если атака слишком серьезная, для российских компаний можно полностью перекрыть ресурсы из других стран мира, где у них минимум клиентов, но оставить хорошую связность в России".

Благодаря настройке решения, у каждого клиента есть свой профиль потребления - как только наблюдается аномалия, включается автоматика или ручной режим и весь трафик проходит проверку на легитимность. То, что не проходит - удаляется. "По сути, мы работаем на уровне индивидуальной настройки, - отметил Владимир Валькович. - Для этого в нашем центре поддержки клиентов выделена отдельная группа специалистов, которая занимается вопросами информационной безопасности в круглосуточном режиме. В Help desk тоже выделен специальный сотрудник, который может работать в ручном режиме с DDoS-системой".

Зарождающийся рынок

Большинство клиентов, которые заказывают защиту от DDoS в Orange Business Service, уже испытывали негативный эффект от подобных атак, поэтому их не надо уговаривать подключить подобный сервис. В настоящий момент у компании несколько десятков клиентов в "боевом режиме": кажется, это один из наилучших результатов на российском рынке. Это либо пользователи интернет-доступа по выделенным каналам, либо клиенты ЦОДа. Кстати, пилотная программа "на попробовать" тоже предусмотрена - обычно это срок от 2 до 4 недель. Но только для тех компаний, которые не находятся под атакой – так, отбить пару тестовых запросов.

Стоимость по защите примерно средняя по рынке и начинается от 200 долл. за настройку системы и 250 долл. в месяц за защиту канала мощностью 2 Мбит/с. Более точные цифры мне так и не сказали, отметив, что любой из их компании "могут подсчитать достаточно быстро". "Основные заказчики, потребляющие эту услугу, подключены к Сети на скорости от 10 до 50 Мбит/с, - отмечает Владимир Валькович, - причем конкретная стоимость зависит от уровня SLA, который заказывают наши клиенты".

Число атак, их сила и продолжительность напрямую коррелируют с развитием электронной коммерции по принципу "чем дальше, тем мощнее". В online активно идут процессинговые компании, банки, к Сети подключаются банкоматы и терминалы самообслуживания, полностью электронные магазины услуг и т.д. Для всех них простой - это прямые убытки. "При этом, - отмечает г-н Валькович, - большинство компаний могут если не полностью убрать, то минимизировать поражающий эффект

от подобных атак: для полной блокировки существуют специализированные сети, которые изолированы от публичной сети Интернет".

В целом, рынок защиты от DDoS приобретает только некоторые общие контуры – он находится на ранней стадии своего развития. Российские операторы связи и сервис-провайдеры только-только начинают запускать соответствующие услуги по безопасности и выпускать в "боевой режим" аппаратно-программные комплексы защиты. "Пока что поле для деятельности свободно, - уверен Владимир Валькович. - Сервис-провайдеры и телекоммуникационные операторы связи в наибольшей степени ориентированы не на "захват" сторонних клиентов, а на "обработку" уже существующих заказчиков: это быстрее, дешевле по стоимости привлечения и, в конечном итоге, выгоднее. Поэтому многие из поставщиков таких услуг так неохотно относятся к "пожарным" заказам". "Наши основные заказчики – это крупные российские и иностранные компании, - комментируют менеджеры Orange Business Services, - а им явно не свойственно торопиться, о многих проблемах безопасности они предпочитают думать заранее". Тем более, что защита от DDoS - это только дополнительная опция к уже потребляемым услугам.

А по поводу небольших компаний с самописными решениями Владимир Валькович был еще более скептичен: "Они могут потушить пожар и, возможно, будут дешевле, чем постоянная защита, но для компаний, находящихся в зоне риска, куда более выгодно с точки зрения минимизации потерь от атак иметь оператора, который постоянно оказывает защиту". В принципе – его аналогия понятна: это как таблетка от гриппа, вместо прививки - дает только временный результат.