www.orange-business.ru

17.06.2014

Йохан Балийон: Потенциал российского рынка защиты от DDoS огромен

На вопросы Anti-Malware.ru любезно согласился ответить Йохан Балийон, директор департамента глобальных решений и услуг Orange Business Services, Россия и СНГ. *Это интервью продолжает цикл публикаций "Индустрия в лицах".*

Йохан Балийон

Окончил университет прикладных наук Hanzehogeschool Groningen (Нидерланды) по специальности электроника и информационные технологии.

Обладает опытом свыше 25 лет в области телекоммуникаций и ИТ. С 1986 года работал в компании KPN, крупнейшем операторе фиксированных линий связи в Нидерландах, где занимал управленческие позиции в департаменте клиентских программ. До 2000 года активно развивал международные телекоммуникационные проекты компании в Африке, Азии, Восточной Европе и странах Карибского бассейна. В 2006 году Йохан Балийон присоединился к Orange Business Services (Нидерланды), в его обязанности входила разработка решений и архитектуры для крупнейших международных заказчиков компании. Перед переводом в Россию занимал должность директора департамента глобальных решений.

Давайте поговорим об основах. Что такое «DDoS-атака» с точки зрения Orange BusinessServices?

DDoS — это распределенная атака, направленная на отказ от обслуживания и приходящая от большого числа источников, компьютерных устройств. Как правило, это зараженные вредоносными программами компьютеры (ботнеты), трафик от которых направляется на жертву. Ей может стать вебсайт или онлайн-сервис. В результате атаки пользователи не могут попасть на сервер и воспользоваться им. Проблема в том, что от подобных атак нельзя отгородиться полностью, но при помощи специальных средств защиты можно уменьшить их влияние на функциональность ресурса и отфильтровать паразитный трафик.

Как эволюционировало понятие «DDoS-атака» за последние несколько лет?

К сожалению, с каждым днем частота и мощность DDoS-атак увеличивается. Атаками, измеряемыми гигабайтами в секунду, уже никого не удивишь. Большое количество DDoS-атак затрагивают протокол NTP (Network Time Protocol, сетевой протокол для синхронизации внутренних часов). Где-то около 7-8% от всех серверов NTP до сих пор используют старые версии ПО, что делает их уязвимыми. Эту лазейку используют злоумышленники. Когда ее прикроют, в скором времени обязательно появится другая, а затем еще одна. Этот процесс бесконечен.

Какие типы атак наиболее популярны у злоумышленников?

Обычно атаки проводятся на логическом уровне 3 или 4 (в модели OSI, сетевой и транспортный уровни соответственно). Атаки на уровне 7 (прикладной уровень) встречаются редко, но постепенно набирают популярность.

Каковы источники DDoS-атак, есть ли здесь какие-то тенденции?

Источниками атак являются зараженные компьютерные устройства, объединенные в ботнет. Мобильные устройства на базе операционной системы Android , которые являются частью ботнета, также становятся источниками DDoS-атак. Иногда атаки идут от ботнетов, состоящих из зараженных серверов.

Большинство атак по-прежнему исходит из США, но в последнее время постепенно начал набирать обороты и Китай. Экономика Азии находится на подъеме, и мы думаем, что в ближайшей перспективе Китай станет первым в списке стран-источников DDoS-атак. Причина — большое количество компьютеров с устаревшей Windows XP, чаще всего пиратской, на которую не устанавливаются обновления безопасности. Таким образом, эти компьютеры неизбежно станут частью различных ботнетов.

Какие компании наиболее подвержены DDoS-атакам? Кто находится в группе риска?

DDoS-атакам подвержены любые компании, располагающие ресурсами в сети Интернет. Большой популярностью у киберпреступников пользуются системы онлайн-банкинга, сайты финансовых организаций, социальные сети, онлайн СМИ, а также, по какой-то причине, сайты турагентств.

Некоторое время назад наш сайт был также атакован. Мы просто не знали, куда звонить и что делать. Крайне неприятная ситуация.

Отличный пример! Ваш сайт как раз же распространяет информацию, которая невыгодна злоумышленникам. Скорее всего, именно поэтому вы и стали их мишенью. Один известный блогер Кребс часто подвергался DDoS-атакам, так как очень подробно расписывал у себя в блоге, как они организовываются.

Каковы причины атак, что движет злоумышленниками?

Мотивы для проведения DDoS-атак могут быть самыми разными. Злоумышленники нарушают работу сайтов, чтобы они перестали функционировать, продавать товары и приносить деньги владельцам. Подобные атаки могут быть делом рук недобросовестных конкурентов.

Некоторым людям могут банально не нравиться определенные вебсайты. Самый простой способ избавиться от неугодной информации — сделать ее недоступной для обычных пользователей при помощи DDoS-атак.

Можете рассказать о каких-то примерах DDoS-атак из вашей практики в России?

Так как речь идет о безопасности, мы не можем раскрыть конфиденциальную информацию о клиентах. Но могу сказать, что за последние месяцы количество атак на российские кампании, преимущественно в финансовом секторе, выросло. Некоторые из них обладали силой более 40 Гб/с.

Возможно, в будущем их число и пойдет на спад, но это произойдет, если будут найдены другие методы воздействия на тех, кто сегодня является жертвой злоумышленников.

Есть ли способы защиты от таких сильных атак?

Сегодня ботнеты содержат такое большое количество компьютеров, с которых осуществляются атаки, что нам, как и другим вендорам, остается только одно — максимально снизить ущерб, поскольку сразу полностью остановить подобные атаки невозможно. Нам удается сохранять функциональность вебсайтов и сервисов, чтобы ими по-прежнему могли пользоваться даже во время атаки. Пока мы пытаемся ее остановить, пользователи могут подключиться к сайту через альтернативный канал связи.

Насколько компании в России понимают угрозу DDoS-атак и заинтересованы в мерах защиты?

Ситуация с сервисами по безопасности напоминает работу страховых компаний — к нам начинают обращаться только после того, как что-то плохое уже произошло. Нельзя сказать, что такой подход характерен только для российских компаний. То же самое мы наблюдаем и в Европе. Стоит только случиться DDoS-атаке, как к нам бегут со всех ног и спрашивают, что нужно подписать, чтобы все это прекратилось. Большинство владельцев вебсайтов думают, что эта проблема просто обойдет их стороной.

Возможно, стоит позиционировать ваши услуги как своеобразную страховку от DDoS?

Хорошая мысль! Многим стоит задуматься о страховке от потенциального ущерба. Если заранее позаботиться о решениях, которые позволят защититься от атак, это позволит обеспечить непрерывное функционирование вашего предприятия, а также избежать финансовых и репутационных потерь.

Как вы оцениваете потенциал российского рынка защиты от DDoS?

Если говорить о клиентах, то потенциал тут огромен. Многие компании пока еще не сталкивались с DDoS-атаками. Уязвимость бизнеса возрастает с увеличением его зависимости от онлайн сервисов. Одно дело, когда вы продаете товары через сеть магазинов розничных продаж (физические торговые точки), совсем другое, когда большая часть ваших продаж идет онлайн. Если сайт не работает в течение нескольких часов, это можно пережить, но если атака длится несколько дней, то тут уже можно начинать говорить о риске банкротства. Все больше российских компаний начинают работать и в сети, следовательно, пропорционально растет и потребность в наших услугах.

Давайте поговорим о вашей компании. Все мы знаем Orange в первую очередь как телекоммуникационную компанию. Почему вы решили заняться информационной безопасностью?

Мы начинали как телекоммуникационная компания, однако нашей главной задачей является оказание услуг, связанных с глобальной сетью. Мы не только предоставляем каналы связи для наших клиентов, но также оказываем услуги по управлению локальными сетями и IP-телефонией. Кроме этого, мы можем размещать на своих ресурсах различные сервисы клиентов, например, Microsoft Exchange, а также предоставлять доступ к облачным хранилищам. Когда речь заходит о подобных услугах, то безопасность становится ключевым компонентом.

Таким образом, часть нашего портфеля услуг состоит из аутсорсинговых услуг (*прим.: по модели SaaS*) по управлению прокси-серверами, защиты от вредоносных программ и DDoS. Клиент сам выбирает, что ему нужно. Мы предоставляем полный спектр необходимых услуг для некоторых очень крупных компаний в России и по всему миру из самых разных отраслей, включая финансовый и промышленный сектор. Наличие в нашем портфолио услуг по информационной безопасности является частью бизнес-стратегии Orange.

Мы постоянно проводим исследования на предмет того, что еще хотели бы получить наши клиенты, и стараемся учесть это в стратегии развития Orange. Наша индустрия стремительно меняется и эволюционирует — то, что казалось абсолютно новым вчера, выглядит совершенно обычным сегодня, а завтра и вовсе устареет. Несколько лет назад мы заметили, что количество DDoS-атак начало стремительно расти, поэтому и задумались над технологиями защиты, которые могли бы предложить клиентам.

Как называется ваш сервис для защиты от DDoS-атак?

Наш сервис называется Internet Umbrella (*прим.: в переводе с анг. «Интернет-зонт»*).

Возможно ли с вашей помощью провести расследование произошедшей DDoS-атаки?

Киберпреступники предпринимают много шагов, чтобы не попасться. Они хорошо в этом преуспели. Конечно, мы можем просмотреть сетевые пакеты, но IP-адреса в этих пакетах всегда подставные (*прим.: от зараженных устройств, ботнета*), все действующие лица остаются за кадром. Найти настоящего исполнителя и заказчика атаки практически невозможно.

Были случаи, когда из одной подсети, с одного единственного IP-адреса, приходил гигантский трафик. Он не был весь вредоносным — часть исходила и от обычных пользователей. Казалось бы, можно заблокировать этот адрес и проблема будет решена, но тогда вы закроете доступ и для какого-то числа легитимных пользователей. Не думаю, это можно считать решением проблемы.

Иногда все же можно вычислить реального инициатора атаки, захватить ботнет, но на исполнителей и заказчиков выйти все равно не получится. Не так давно Microsoft захватила управление несколькими крупными ботнетами и ликвидировала их. К сожалению, это помогает лишь на время, потому что все равно появятся новые ботнеты — уязвимые системы никуда не исчезнут.

Насколько я понял, услуга оказывается с использованием оборудования одного из известных вендоров. Почему клиенту просто не купить такое оборудование для себя, в чем состоит добавленная стоимость услуг Orange Business Services?

Здесь стоит вопрос выбора: пользоваться услугами аутсорсинга или делать все своими силами. Когда автомобиль ломается, вы отдаете его на ремонт в специализированный сервис, потому что там работают люди, которые знают, как все сделать быстро и качественно. Вы можете купить программно-аппаратный комплекс для защиты от DDoS, но чтобы он заработал, нужны хорошие специалисты с соответствующей экспертизой. В Orange работают именно такие люди — они отлично знают наш сервис и обеспечивают защиту ресурсов клиентов 24 часа в сутки 7 дней в неделю.

Также существует и техническая сторона вопроса. Представьте, что вы имеете на входе интернет-канал 100 Мб/с. Вы устанавливаете приобретенный программно-аппаратный комплекс, в какой-то момент кто-то начинает вас атаковать. Даже если вы отфильтруете паразитный трафик, и он не будет нарушать работу вашей внутренней сети или сервера, но сам канал все равно будет забит. Как следствие, легитимные пользователи все равно будут испытывать большие трудности с получением доступа к вашим ресурсам. Internet Umbrella использует сеть с очень большой пропускной способностью, ее не

так то просто забить. Поэтому фильтрация трафика на нашей стороне минимизирует влияние DDoS-атак на обычных пользователей.

Что выгоднее покупать для защиты от DDoS: подписку на сервис или программно-аппаратный комплекс?

По цене хорошего программно-аппаратного комплекса вы можете приобрести подписку на наш сервис сроком на три года. Если вы планируете пользоваться этим комплексом более длительный срок, то его покупка будет выгоднее. Но тогда вам придется нанять нескольких специалистов, которые будут проводить мониторинг корректной работы защиты. Одного будет недостаточно, так как он не сможет самостоятельно обеспечить круглосуточную защиту. Конечно, современные средства противодействия DDoS могут работать в автоматическом режиме, но против сложных атак потребуется вмешательство профессионалов, которые будут решать, на что именно нужно обратить внимание в первую очередь. В этом и состоит принципиальная разница в подходах. Последнее, что нужно учитывать, — ущерб от возможной атаки. Во что обойдется компании блокировка Интернет-ресурса на один, два или три дня? Как это повлияет на ее репутацию? Какие будут финансовые потери? Тут мы и возвращаемся к вопросу страховки и оцениваем, насколько сильно нам нужна хорошая и качественная защита.

Мы понимаем, что сервис защиты от DDoS по подписке — это не обязательно самый дешевый вариант, но он гарантирует, что защиту обеспечивают эксперты, которые постоянно следят за ситуацией и, в случае чего, примут необходимые меры. Если вы делаете все самостоятельно, не исключено, что вы можете узнать о начавшейся атаке только через несколько часов. Тут ваши действия по устранению проблемы будут напоминать работу команды пожарников, которые приехали на вызов и стараются потушить уже разгоревшееся пламя.

В чем преимущества ваших услуг в сравнении с конкурентами, например, Akamai, Prolexic или «Лабораторией Касперского»?

У нас есть сервис защиты и своя инфраструктура, свой канал. Мы выступаем в роли своего рода «службы одного окна». В организационном и техническом плане для клиента намного проще иметь один контракт, одного поставщика услуг и единую техподдержку.

Какие планы у компании по развитию своих услуг защиты от DDoS-атак на ближайшее время?

Поддерживать сервис на высоком уровне. С одной стороны, нужно заботиться о производительности нашей платформы, с другой, — очень важна сама система защиты и люди, которые с ней работают. Мы всегда должны знать, что делать в случае обнаружения нового типа атаки. Поэтому вдобавок мы также пристально следим за последними трендами в сфере информационной безопасности.

Спасибо!

Интервью провел **Александр Панасенко.**