GroupIB: "Мало кто помнит, что заказ или организация DDoS - это уголовное преступление"

[GroupIB: "Мало кто помнит, что заказ или организация DDoS - это уголовное преступление"]Группа информационной безопасности GroupIB - небольшое экспертное учреждение, которое занимается расследованием компьютерных преступлений. Созданное, по официальной информации, в 2003 году, оно обладает техническими и интеллектуальными возможностями для того, чтобы не только получить, но и грамотно оформить техническую документацию по DDoS-атакам для правоохранительных органов. О практике подобных действий, ботсетях, специфике расследований и тактике DDoS-атак злоумышленников нам рассказал генеральный директор компании Илья Сачков.

Специфика рынка

Вполне закономерно, что расследование именно DDoS-атак в России - только зарождающийся процесс. Как отмечает Илья Сачков: "На это направление приходится не больше 5% нашего бизнеса, но это только пока. Число таких компьютерных преступлений увеличивается год от года, поэтому мы рекомендуем обязательно расследовать такие случаи. Это необходимо хотя бы по той причине, что массовая безнаказанность порождает увеличение таких атак: хакеры пока чувствуют, что будет атака удачной или нет, их никто не привлечет к уголовной ответственности".

Причем, в связи с развитием компьютерных технологий и увеличением проникновения ШПД в "народные массы" число любителей заработать "влегкую" таким образом увеличивается. В Сети можно найти конструкторы ботнетов, при наличии минимального технического образования есть шанс не только найти единомышленников на специфических сайтах, но и разобраться с инструментарием для работы с подобными программными комплексами. "Люди не чувствуют, что занимаясь созданием бот-сетей или DDoS-атаками, они совершают преступление,- отмечает Илья Сачков, - а между тем рынок увеличивается в объемах, стоимость конкретных атак уменьшается, исполнителей становится все больше. Те, кто начинал какое-то время назад или руководят целыми преступными группировками или уже заработали себе достаточно денег на то, чтобы чувствовать себя безнаказанными". А, между тем, риски для любой компании, которая занимается бизнесом в Сети увеличиваются лавинообразно: даже крупные компании не брезгуют DDoS-атаками, если надо "завалить" своего конкурента, особенно во время сезонной активности с пиковым потреблением.

Предсказать оборот рынка DDoS никто не в силах - неизвестно точное количество атак, их мощность и цены. Хотя, для развития оперативного мышления и сбора информации, все игроки рынка регулярно проводят не только поиск соответствующих объявлений, но и тестовые "заказы". Кроме того, идет постоянная оперативная работа по внедрению на профильные форумы и чат-каналы, работа с агентурой - утечек из этой среды, как меня уверяли, предостаточно.

[GroupIB: "Мало кто помнит, что заказ или организация DDoS - это уголовное преступление"]

В среднем, "атака на ресурс стоит от 50 до 500 евро в день, - говорит Илья Сачков, - хотя я видел объявление и за 20 евро, но это редкость. Есть и дорогие атаки, но это уже индивидуальный подход и создание ботнета под конкретный "заказ". Правда, надо отметить, что любые действия по покупке, аренде или действию с помощью ботнетов - это потенциальное уголовное преступление не только для исполнителя, но и для заказчика подобной атаки".

По мнению Ильи Сачкова, чаще всего встречаются ботнеты - около 40 тыс. зомби-машин. Технологии ботнетов идут вперед и мощность ботнета не определяется его численностью. Главное это интеллектуальность «бота». Причем, любой ботнет надо постоянно обновлять, регистрировать на него доменные имена, закупать хостинг, перемещать свои серверы и центры управления, покупать новые криптеры и т.д. Для крупного ботнета этим занимается специальная "команда обеспечения". Так называемые "ботнеты-миллионники", по его мнению - не более чем реклама, миф. "Нет смысла создавать такой большой ботнет, поскольку для его управления нужен мощный, по функциональным возможностям, сервер, - говорит он. - Наличие такого решения сразу "привязывает" владельца к определенному ЦОДу, и лишает мобильности основной и резервный ботнет-контроллеры. Скорее уж в атаке будут принимать участие несколько ботнетов с численностью 15-20 тыс. машин: ими можно легко управлять, вводя в действие "эшелон прорыва", "эшелон развития успеха" и т.д., организовать комбинацию атак, а в качестве отвлекающего маневра привлечь "кликеров"".

Надо отметить, что это уже совсем не баловство, а достаточно четкий бизнес. Решений "для демонстрации" здесь практически не создают, а детских атак, по мнению Ильи Сачкова, минимум ."Спалить свой ботнет просто ради того, чтобы показать его эффективность мало кому интересно. Ведь после первой же атаки стоимость ботнета уменьшается минимум на 40%, он оказывается "засвечен", попадает в блэклисты специализированных компаний", - говорит он. Да и покупать ботнеты никто особенно не готов - это рынок услуги. "Можно купить ботнет, скажем, на 5 тыс. машин, за несколько сотен долларов, - говорит г-н Сачков, - но через 3 дня, без поддержки, их станет 500. Еще неделя и не останется ничего - антивирусные компании тоже работают достаточно

активно".

Структура атак

Интересно, что подобные атаки даже можно разделить по определенным типам. Самый "простой" заказчик, можно даже сказать массовый - их сферы ритейлового бизнеса. Конечно, это не уничтожение палаток конкурентов, да и бутылки с зажигательной смесью в окна никто не бросает. Теперь конкуренты действуют тоньше - заказывают DDoS-атаку на сайт противостоящей на рынке компании. "Особенно часто такие попытки случаются в таких сегментах, как установка пластиковых окон, доставка цветов, кондиционеров, в строительном бизнесе, среди риэлторов, продавцов шин и дисков, - комментирует Илья Сачков. - Атаки не особенно мощные, поскольку денег на это выделяется не очень много. Но заказчика можно вычислить достаточно быстро: обычно это компании из ТОП-5 в рейтинге поисковой системы по соответствующим запросам. Кроме того, кто активно начинает продвигаться в контекстной рекламе, во время атаки на конкурента, тот, с высокой вероятностью, может иметь к ней непосредственное отношение".

[GroupIB: "Мало кто помнит, что заказ или организация DDoS - это уголовное преступление"]

Нарастающая "популярность" - это мошенничества с дистанционным банковским обслуживанием. Причем, "частники" мошенников очень часто не интересуют - их остатки по счетам обычно не велики. Но вот юридические лица - совсем другое дело. "По числу таких атак немного, но по ущербу они могут быть весьма значительными, - отмечает Илья Сачков, - в среднем от 500 тыс. до 1 млн. долл., хотя мы видели платежки до 25 млн. долл. за раз. Здесь схема уже сложнее. Сначала готовится специальный компьютерный вирус, задача которого "проскользнуть" на компьютер пользователя, отсканировать его систему безопасности и найти возможность инициировать загрузку модуля для кражи данных, а также обеспечить его связь со своим модулем управления. Этот же "сканер" определяет и методы защиты, а также версию программы-клиента, которая стоит на компьютере бухгалтера. Соответственно, производится поиск ключей на жестком диске (иногда "для простоты работы" их туда сохраняют - Прим. ред.), а также, если есть, USB-токена.

[GroupIB: "Мало кто помнит, что заказ или организация DDoS - это уголовное преступление"]

Далее обеспечивается возможность для удаленного управления таким компьютером. Как только бухгалтер начинает работу, контроль перехватывается и, скажем, инициируя отправку текущего платежа в пару тысяч рублей и вводя пароль или одноразовый код, в дополнение к USB-ключу, он может отправить десяток миллионов совсем на другой счет. Те хакеры, которые так работают, конечно, гении. На компьютере того же бухгалтера эмулируются все процедуры работы с банковским сервером, только на самом деле происходит все совсем другое. А для банка все абсолютно легитимно - приказ пришел с компьютера клиента, IP-адрес его, ЭЦП тоже принадлежит клиенту. Соответственно, платежное поручение исполняется. После этого сразу начинается DDoS-атака на банковский сервер с тем, чтобы затруднить клиенту проверку своего счета - ведь пропажу-то можно обнаружить достаточно быстро. Но как только банки начали ощущать такие атаки, особенно под начало операционного дня (все кражи осуществляются с утра в рабочий день чтобы затеряться в потоке других распоряжений и успеть "раскидать" деньги до вечера - Прим. ред.) они сразу стали усиливать контроль за предшествующими транзакциями. Тогда ситуация изменилась – атаковать стали реальные IP-адреса клиентов. Банк в таком случае ничего не видит, а клиент считает, что это массовый перерыв или проблема с сервисом".

[GroupIB: "Мало кто помнит, что заказ или организация DDoS - это уголовное преступление"]

Еще один тип DDoS-атак - это чистое вымогательство, где сама атака используется как повод для получения выкупа за то, чтобы это действие не происходило. Обычно владельцу ресурса приходят по электронной почте письма из серии "заплатите, или ваш сайт "упадет" 13го в пятницу". Причем, далеко не всегда эти угрозы глупы и бессмысленны, но атака, организуемая в таком случае, будет достаточно затратной с т.з. самого злоумышленника, поскольку при этом ему придется "засветить" свою бот-сеть, что снизит ее ценность для последующих атак. Кроме того, "этот вид атак идет на спад, - уверяет Илья Сачков, - если надо вымогателю платить много, то компании предпочитают потратить эти деньги на защиту. Если просят мало, то можно нанять небольшую компанию, которая "прикроет" ресурс в "горячем режиме".

[GroupIB: "Мало кто помнит, что заказ или организация DDoS - это уголовное преступление"]

Даже если кто-то и вздумает заплатить по такому требованию, то это можно сделать только с помощью электронных валют типа WebMoney или Яндекс.Деньги: но все они имеют свои "следы", даже при распылении денег все равно можно отследить на каких кошельках они осели, по каким паспортным данным были обналичены. Аналогичная ситуация и с карточками оплаты: поставить их "на карандаш" в системе для СБ компании-эмитента электронной валюты достаточно просто, это никакая не гарантия анонимности. Платить же деньги на зарубежный счет российские компании просто так не могут - надо будет объяснять ситуацию валютному контролю. Поэтому число таких преступлений уменьшается. Не сидят на месте и СБ тех компаний, которые получают такие письма. К

ним, обычно, относятся очень серьезно. Недавно, к примеру, мы помогли найти злоумышленников двум крупным российским компаниям".

[GroupIB: "Мало кто помнит, что заказ или организация DDoS - это уголовное преступление"]

Не остаются без внимания и информационные ресурсы - интернет-издания или печатные версии бумажных СМИ, социальные сети, а также официальные ресурсы политических партий. "Все небольшие веб-сайты, которые могут сказать хоть что-то интересное в период выборов, обычно "лежат" наглухо, - говорит Илья Сачков, - "отбиться" могут только крупные проекты. К примеру, в марте 2009 года была мощная атака на крупный издательский дом. Суммарная мощность по оценке магистральных провайдеров достигала 20-25 Гбит/с и ресурс все-таки упал. Сегодня они сделали все выводы и у них очень мощная система защиты, балансировки ресурса, который находится на хостинге у "БиЛайн Бизнес" и "Комкор" - повторение такого "падения" вряд ли возможно в принципе. Обычно, мотивация для такой атаки, конечно, состоявшийся или грядущий выход нежелательного для заказчика материала или информационные войны. Причем, с отраслевыми ресурсами, к примеру, по мобильной связи все аналогично - с той только разницей, что для их "падения" надо приложить гораздо меньше усилий. Все зависит, во-первых, от архитектуры ресурса, от его канала доступа в Сеть, в конце-концов можно атаковать его DNS-сервер, провести атаку на его "тяжелый" контент, если есть и т.д."

Кстати, в данном случае наблюдается уход от "атаки в лоб", когда все решала мощность ботнета, к т.н. "интеллектуальным атакам". "Главное с т.з. злоумышленников определить, где на ресурсе находиться самая большая нагрузка, - говорит Илья Сачков, - и использовать эту уязвимость на "полную катушку". Это может быть загрузка больших файлов, система авторизации, работа с форумом и т.д. То есть то, что можно "положить" небольшими силами. С точки зрения аппаратно-программных комплексов отследить такую атаку сложно, поскольку она производится небольшими силами и не создает никакой избыточной нагрузки паразитическим трафиком, но сервер "кладет" качественно. По сути, это точечные удары вместо "ковровой бомбардировки". К примеру, осенью 2009 года один банк "положили" атакой всего с десятка IP-адресов: каждый из них всего-то эмулировал авторизацию с электронным ключом. Но и такая нагрузка оказалась для системы интернет-банка непосильной. И, к сожалению, именно за такими атаками будущее".

Присутствуют и DDoS-атаки как элемент конкурентной борьбы между преступными группировками и нелегальными партнерскими программами. "Обычно это атаки друг на друга, причем мотив тот же самый, - говорит Илья Сачков, - деньги. Если один ресурс с нелегальными товарами не работает по каким-то причинам, то заказы будут делать в другом месте. Учитывая весьма высокую маржинальность такого бизнеса, для DDoS там есть все основания".

Практика расследования

Основные "двигатели прогресса" в части расследования DDoS-атак - это, конечно, крупные компании, где на уровне совета директоров принимается принципиальное решение о том, что ни одна атака на информационные ресурсы компании не должна оставаться безнаказанной. Это при том, что средняя стоимость расследований DDoS-атак составляет 250-750 тыс. руб. и длится примерно полгода. "Это не оперативно-розыскная деятельность, а аналитическая работа над тем, чтобы получить информацию о исполнителе, - говорит Илья Сачков, - свод информации о типах атак, о использованном управляющем ПО, о географии поступления команд, сравнение с другими ботнетами и ранее известными исполнителями, агентурная работа (тестовые заказы) и т.д. Для "контроля качества" DDoS-атак мы используем свой кластер компьютеров, выставленных в Сеть интернет под разными IP, где присутствует только минимальная антивирусная защита. Они регулярно заражаются различными ботсетями и мы получаем отличную информацию для анализа: что это за ботнет, для каких целей создан, кого атакует. Все эти данные мы заносим в специальную базу данных GroupIB - это наша разработка, где уже хранится порядка 4 тыс. записей по самым разным ботнетам, которые встречались в "диком виде" в Сети интернет и атаковали российские веб-сайты".

В подразделении, которое занимается именно расследованием DDoS-атак в GroupIB работает пять человек. "Эти специалисты не работали в силовых структурах - их типичный опыт это информационная безопасность в крупных компаниях, где они занимались внутренними расследованиями, антифродом и т.д., - говорит Илья Сачков. - Есть конечно, и представители спецслужб, но это уже юридическая плоскость, которая требуется в закреплении технических данных для того, чтобы это стало доказательством".

В целом, получить данные по конкретной атаке, которые станут основой уголовного дела можно за 1-2 месяца напряженной работы. "Не все клиенты готовы платить за это деньги, - комментирует Илья Сачков. - Они считают, что расследованием должны заниматься правоохранительные органы, и их позиция вполне понятна. Проблема только в том, что делать полноценно они этого не могут в силу технической слабости, определенных оргмоментов: они просто "не тянут" брать на работу талантливые кадры. А людей, которые могут не просто разобраться в логике технологического преступления, а понять его схему и собрать доказательную базу, совсем немного. Расследование

нашими силами, обычно, бывает возможно только в том случае, если на то бывает политическая воля от руководства компании. И определенное терпение - на сбор и закрепление юридически значимых доказательств требуется время". В среднем, заказов на подобные расследования компания пока получает до пяти в год.

Правда, есть и другие варианты взаимодействия. Возможно организовать не полноценное расследование, а подготовить пакет документов, информационную справку о совершенном преступлении для МВД. На ее основе и готовится заявление в правоохранительные органы от компании, которая пострадала от атаки. "Обычно там фиксируется сам факт атаки, подробно расписывается ситуация с атакующими ресурсами, приводится информация о структуре атаки, ее мощности и участвовавших бот-системах с локализацией управляющего центра, - говорит Илья Сачков. - Это в большинстве случаев сделать можно оперативно, поскольку наш кластер зараженных машин в таких ботсетях, обычно, участвует. Причем, специально для правоохранительных органов мы указываем как и что мы делали пошагово - с тем, чтобы они, при сборе доказательств, могли повторить нашу методику". Подобные справки заказываются десятками в месяц.

Важным является и сохранность доказательств - клиенту все-таки стоит позаботится о том, чтобы они были в целости представлены для изучения. "Если у клиента ведутся логи, их не надо изымать и очищать. В идеале надо вызвать наших экспертов и отойти от того оборудования, где оно хранится. Мы их качественно изымем оттуда и зафиксируем всеми возможными, юридически достоверными способами, - говорит Илья Сачков. - Кроме того, надо сохранить всю информацию на активном сетевом оборудовании, если оно есть у клиента. Заказать информационное письмо от провайдера, где он подтвердит факт всплеска паразитного трафика: это письмо должно быть на бланке организации, с номером исходящего за подписью ответственных сотрудников компании. Если была заказана услуга "защита от DDoS" - значит еще и логи защитного аппаратно-программного комплекса. Вдобавок, DDoS-атака, обычно, приводит к сбою оборудования компании: необходимо зафиксировать это с помощью внутренней служебной записки. Проблема в том, что клиенты, которые обращаются к нам, часто об этом забывают, что усложняет установку факта атаки. Важен и фактор времени - главное начать работу "по горячим следам", если атака произошла больше месяца назад, а клиент только сейчас "созрел" для расследования, пробовать можно, но шансы весьма невелики: ботнета в том виде, который он был при атаке уже нет, данные логов у провайдеров уже давно затерты и т.д. Идеальный вариант - расследование во время атаки, тогда собирается больше половины необходимой информации".

Кстати, GroupIB оказывает и услуги по поддержке "в горячем режиме". Если DDoS-атака развивается "здесь-и-сейчас", то кроме включения аппаратно-прораммных средств безопасности, можно попробовать "выбить" управляющий центр ботнета. "Для этого у нас есть специальный оперативный дежурный, программа поддержки 24x7 и специальная абонентская поддержка,- говорит Илья Сачков. - Услуга предоставляется совместно с компаниями-партнерами, которые будут работать с трафиком клиента, стоимость - от 20 до 500 тыс. в месяц в зависимости от типов и количества инцидентов. Наша задача - попытаться предотвратить атаку в момент ее возникновения. Если ботнет нам известен, а число таких "засвеченных" систем велико, мы можем связаться с провайдером, где хоститься управляющий центр, и попробовать заблокировать эту учетную запись. Доказательства противоправной деятельности мы, конечно, предоставляем незамедлительно. Пока злоумышленник будет переезжать на резервную площадку, восстанавливать управление ботнетом - уходит время, эффективность атаки снижается. По некоторым "создателям" таких систем у нас есть вся информация, включая их телефоны. Совсем свежий пример - недавно мы зафиксировали мощную атаку на ресурс одного из наших клиентов. Через минут десять мы уже знали телефон злоумышленника, который был нанят для этой акции и позвонили ему в Рязань с вежливой просьбой эту незаконную деятельность прекратить. Судя по тому тону голоса и удивлению, которое мы услышали, это было для него полной неожиданностью: атака была свернута через четверть часа".