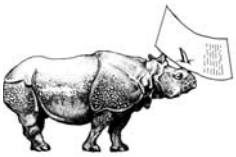

Олег Демидов

ЦИФРОВОЙ ДЖИНН НА СЛУЖБЕ ТЕГЕРАНА

*

С сентября 2012 г. по март 2013 г. информационные системы и онлайн-сервисы ряда американских финансовых организаций подверглись массированным и продолжительным DDoS-атакам. В списке жертв оказались такие гиганты, как *Bank of America, Citigroup, Wells Fargo, U.S. Bancorp, Capital One, HSBC*, вынужденные потратить тысячи человеко-часов и многие десятки тысяч долларов на защиту от атак и ликвидацию их последствий. Этот сюжет наряду с разоблачением *Лабораторией Касперского* грандиозной кибершпионской сети *Red October* стал одной из центральных тем в сфере кибербезопасности в начале 2013 г., хотя, строго говоря, ни технологии атаки, ни их масштаб и последствия не являются чем-то беспрецедентным. Технология DDoS стара, почти как сам интернет, да и банки США давно уже стали излюбленной мишенью киберпреступников: только в 2011 г. взлом клиентских аккаунтов обернулся для американских банков убытком в 64 млн долларов.

Необычно то, что в организации атак обвиняется не хакерская группировка и даже не ставшие уже привычными в амплуа обвиняемых Китай и Россия, американские эксперты единодушно указывают на Иран. Еще интереснее то, что на этот раз американцы, судя по всему, говорят всерьез, и, скорее всего, они правы. Хотя официальный Тегеран категорически опровергает причастность к атакам, их некриминальный политизированный характер бросается в глаза.

Во-первых, исполнители ни разу не воспользовались возможностью похитить средства со счетов атакуемых банков, хотя могли попытаться это сделать. При этом атаки носили затяжной, длительный характер, то есть преследовали целью нанесение максимального финансового и имиджевого ущерба банкам. Кроме того, банковские службы информационной безопасности столкнулись с *передовой* разновидностью DDoS-атаки. Для генерации избыточного трафика в адрес информационных систем банков использовались не обычные *ботнеты* из зараженных пользовательских машин, а взломанные не до конца понятным способом дата-центры облачных сервисов.

Такой метод организации атаки сильно осложнил противодействие DDoS-трафику, чья мощность достигала 70 гигабит в секунду. Для создания столь интенсивного потока DDoS-пакетов традиционным способом требуется сеть из нескольких сотен тысяч зараженных пользовательских машин.

Нельзя также не отметить, что атаки начались спустя полгода после того, как в рамках пакета санкций Иран был отключен от крупнейшей международной межбанковской платежной системы *SWIFT*, что приблизило страну к финансовому кризису. Наконец объектами атак стали исключительно американские банки. Подобная

избирательность в целом не характерна при эксплуатации крупных *ботнетов* — в киберпространстве государственные границы условны, а системы защиты в банках США далеко не самые слабые.

На этом фоне уже не столь важно, что ответственность за атаки взяла на себя некая группа *Cyber fighters of Izz ad-din Al qassam*, назвав их местью за отказ властей США удалить из Сети антиисламские материалы. Подобные заявления в общем-то не имеют значения, так как их нельзя ни подтвердить, ни опровергнуть, а столь крупные серии атак редко совершает единственная команда.

Куда важнее, что у Белого дома есть все основания считать нынешнюю серию атак вернувшимся из Тегерана бумерангом, который запустила еще администрация Буша-младшего в попытке найти изящное невоенное решение кризиса вокруг иранской ядерной программы. Согласно недавним утечкам в СМИ, беспрецедентно сложные средства кибершпионажа (*Flame, Gauss, Duqu* и другие) и кибердиверсий (*Stuxnet*) были внедрены в ближневосточные сети за последние годы в рамках программы *Олимпийские игры*, одобренной в 2006 г. Бушем и претворенной в жизнь первой администрацией Обамы. Результатом, как считается, стала паника среди иранских специалистов, угроза запуску АЭС в Бушере, потеря более тысячи центрифуг на обогатительном комбинате в Натанзе, многомиллионные убытки и существенное торможение иранской ядерной программы. Без единого выстрела и без учета санкций.

Однако бумеранги имеют свойство возвращаться. Иранцы неплохо научились перенимать приемы своего высокотехнологичного оппонента: в 2012 г. им удалось перехватить контроль над сверхсекретным американским беспилотником *RQ-170 Sentinel* и скопировать его. Теперь, похоже, режим аятолл готов дать Вашингтону сдачи и *на его поле* — в киберпространстве. Конечно, не стоит ждать новостей о поражении американской атомной и военной инфраструктуры иранскими червями, сопоставимыми со *Stuxnet* — в ближайшие годы подобные инструменты иранские хакеры и военные специалисты в одиночку не освоят — не та база.

Но этого и не требуется. Для нанесения чувствительного экономического ущерба, а тем более в демонстрационных целях, старый добрый DDoS остается доступным и эффективным инструментом. Ущерб американских банковских организаций от недавней волны атак не называется, но в общей сложности речь идет о миллионах долларов. Даже частичный отказ сервисов онлайн-банкинга в результате атаки для такого гиганта, как, например, *Citigroup*, может обернуться убытками на многие сотни тысяч долларов в час. С трудом верится, но еще в 2000 г., почти на заре электронной коммерции, серия DDoS-атак *Rivolta*, направленная против *Yahoo!*, *eBay, Amazon* и ряда других крупных сервисов, нанесла, по разным оценкам, ущерб на сумму от 7,5 млн до 1,2 млрд долл. Сегодня ставки гораздо выше — только рынок онлайн-торговли в США за 2011 г. составил 161,5 млрд долл., не говоря уже про электронный банкинг. Все эти бурно растущие сегменты интернет-экономики — потенциальные цели для DDoS-атак, абсолютной защиты от которых не существует, пока есть беспечные пользователи, позволяющие своим машинам быть частью ботнетов.

Кроме того, DDoS-атаки недорого обходятся их организаторам. Если полный цикл создания *Stuxnet* потребовал, по оценкам специалистов, от шести месяцев до двух лет работы высококлассной команды специалистов, нескольких миллионов долларов и работы с агентурной сетью в Иране (для внедрения червя в АСУ ТП в Натанзе), то DDoS-атаку может устроить и школьник, причем не выходя из дома. Рынок *троянов* и других вредоносных программ для создания зомби-сетей — ботнетов, используемых в DDoS-атаках, — ширится год от года, и его продукция неуклонно дешевеет. Тегеран, конечно, не располагает финансовыми ресурсами Вашингтона, но 30–40 тысяч долларов на *ботнет* из сотен тысяч машин вряд ли станут для

него тяжким бременем. Еще сотня-другая тысяч долларов и неплохая команда специалистов — и за несколько месяцев готов новый инструмент типа взломанных дата-центров, с которым можно пытаться всерьез потрепать нервы американским банкам. Следует ожидать, что Иран будет и дальше пользоваться такими инструментами, усматривая в этом собственный асимметричный ответ на враждебные кибероперации в своих сетях.

Определенная логика в этом есть. DDoS не поставит Белый дом на колени, не обезопасит иранскую атомную программу и в случае чего не поможет предотвратить военную операцию против Тегерана. Но, во-первых, обеспечивается демонстрационный эффект — так советские ВВС бомбили Берлин в августе 1941 г. в разгар военной катастрофы на фронте. Во-вторых, массированные *ответные* атаки заставляют Вашингтон, да и Тель-Авив тщательнее взвешивать риски и оценивать последствия следующей возможной операции в иранских сетях.

Что не менее примечательно, избирая целью системы банков, а не сети госструктур, иранцы пытаются заставить американский частный сектор и его клиентов — избирателей — хоть в небольшой степени ощутить на себе издержки противостояния вокруг иранской ядерной программы. Риски же с иранской стороны минимальны — как всегда, технические сложности атрибуции атак и международно-правовой вакуум не позволяют возлагать на государства ответственность за вредоносную деятельность в киберпространстве. Впрочем, те же соображения о почти нулевых рисках ранее играли на руку создателям *Stuxnet* и *Flame*.

Второй вывод из этой истории столь же очевиден — понимание киберпространства как поля боя без правил и ограничений утверждается в мире все шире, в том числе среди тех, кто испытал эффекты кибероружия на себе. Иранцы, вероятно, сочтут свой асимметричный ответ малой толикой адекватного возмездия за кибервойну последних лет. И следует помнить, что Тегеран пришел к идее конфронтации с Вашингтоном в киберпространстве лишь после того, как стал жертвой *Stuxnet* и его *наследников*. Организаторы кибероперации в иранских сетях, можно сказать, открыли новое измерение противостояния — и теперь движение в этом измерении стало двусторонним, что в общем закономерно.

Уместно привести историческую аналогию, вновь связанную с бомбардировками Второй мировой войны. В начале французской кампании 1940 г. Британия избегала бомбардировок Германии, ссылаясь на международное право. В свою очередь, германские ВВС воздерживались от ковровых бомбардировок городов. Однако 14 мая 1940 г. люфтваффе все же разбомбили Роттердам, уничтожив около тысячи мирных жителей. Это событие стало поворотной точкой в политике союзников в отношении бомбардировок самой Германии. 24 августа 1940 г. британцы впервые бомбили Берлин, в феврале 1942 г. королевские ВВС перешли к тактике ковровых бомбардировок, а через три года совместная англо-американская бомбардировка превратила в огненный ад Дрезден, забрав жизни 25 тысяч человек.

Конечно, конфликты в киберпространстве пока не столь ужасны и смертоносны, но общая логика та же: высвобождая из технологических и международно-правовых оков новые средства и способы ведения конфликтов, стоит ждать, что рано или поздно их обратят уже против тебя. А загнать джинна военной технологии и тактики обратно в бутылку крайне сложно — история ОМУ-разоружения и нераспространения тому пример.

Все это вдвойне верно, когда речь идет об изначально асимметричном конфликте — в Сети государства на нападение отвечают не защитой, а нападением, а значит, речь идет даже не о *zero-win*, а о *lose-lose approach*. Кто выиграет противостояние в киберпространстве — Вашингтон со сверхсовременными орудиями киберсаботажа или Тегеран с *дешевым и сердитым* DDoS? Да никто, иранцы будут затягивать пояса, заменять центрифуги и на всякий случай отгораживаться от гло-

Подробнее с материалами по информационной безопасности Вы можете ознакомиться в разделе «Международная информационная безопасность и глобальное управление интернетом» на сайте ПИР-Центра по адресу: net.pircenter.org

бальной сети, а американские банки считать убытки и латать прорехи в деловой репутации. Ну и зачем оно нужно?

Хороший вопрос в устах российского представителя, скажем, на трибуне ООН в наступившем году. Россию, давнего борца за кибермир на международной арене, давно уже беспокоит почти бесконтрольное использование различных программ в целях и способами, явно выходящими за рамки обычного киберкриминала. Вместе с тем подход, на который само российское руководство делало ставку еще с 1998 г. — запрет на разработку и использование кибероружия государствами для решения военно-политических задач в отношении других государств, прописанный в глобальном договоре/конвенции ООН, — пока не удается воплотить в жизнь. Хотя с момента выдвижения ключевой российской инициативы — концепции Конвенции об обеспечении международной информационной безопасности — прошло больше года, усилия РФ и ее партнеров (КНР и ряда стран центральноазиатского региона) наталкиваются на фундаментальное препятствие. Суть его уже раскрыта выше на примере *DDoSa по-ирански*: играть в кибервойну может каждый, схватить его за руку — никто, а закон щита и меча в киберпространстве работает плохо — оборона всегда отстает.

Примерно к 2012 г. российское руководство, осмыслив эту картину, пришло к пониманию того, что, пытаясь договориться о лучшем на трибунах ООН, придется как можно скорее и интенсивнее готовиться к худшему — дальше тянуть нельзя. Иными словами, необходимо включить отражение киберугроз в спектр приоритетных задач вооруженных сил, как можно скорее начать создавать всеобъемлющую национальную систему кибербезопасности и обеспечения защиты критической инфраструктуры и, конечно, активно наращивать собственный киберпотенциал. Целый букет разнообразных технических, законодательных и иных мер по каждому из этих направлений принесли 2012 и начало 2013 гг. — и это лишь начало.

Примечание