

МЕДАЛЬ ЗА ХРАБРОСТЬ

В НАЧАЛЕ ГОДА В ИНТЕРНЕТЕ ПОЯВИЛСЯ САЙТ «ПУТИН ВЗРЫВАЕТ ДОМА», ДАЮЩИЙ ВОЗМОЖНОСТЬ ЛЮБОМУ ЖЕЛАЮЩЕМУ ОДНИМ НАЖАТИЕМ КНОПКИ ПРЕДОСТАВИТЬ МОЩНОСТИ СВОЕГО КОМПЬЮТЕРА ДЛЯ УЧАСТИЯ В DDOS-АТАКЕ. ЦЕЛИ ДЛЯ НАПАДЕНИЯ ВЫБИРАЮТСЯ ВСЕОБЩИМ ГОЛОСОВАНИЕМ. С РАЗВИТИЕМ ТЕХНОЛОГИЙ ОРГАНИЗОВЫВАТЬ КИБЕРАТАКИ СТАНОВИТСЯ ВСЕ ПРОЩЕ И ДЕШЕВЛЕ — ПО ДАННЫМ «ЛАБОРАТОРИИ КАСПЕРСКОГО», КАЖДЫЙ МЕСЯЦ В МИРЕ БЛОКИРУЕТСЯ 2 МЛН СЕТЕВЫХ АТАК. В ДАЛЬНЕЙШЕМ ЭТО ЧИСЛО БУДЕТ ЛИШЬ УВЕЛИЧИВАТЬСЯ.

СВЕТЛАНА РАГИМОВА

ЧЕМ ДАЛЬШЕ В ЛЕС, ТЕМ ТОЛЩЕ ВИРУСЫ Утечки персональных данных в результате спланированных кибератак становятся настоящим бичом крупных IT-компаний. Этой весной хакерами были взломаны интернет-сервисы компании Sony: злоумышленники получили персональные данные и, возможно, номера кредиток более 70 млн человек, а ущерб для бизнеса компании составил до \$170 млн. Согласно данным «Лаборатории Касперского», в России за последний год 96% компаний сталкивались с теми или иными видами киберугроз. Почти половина из них отметила рост числа кибератак, и еще 46% компаний теряли в результате конфиденциальные данные. Среди опрошенных ЛК компаний 14% считают киберугрозы одним из трех наиболее значимых рисков для бизнеса, а 44% уверены, что эти риски войдут в «большую тройку» в ближайшие пару лет.

Сегодня заказать DDoS-атаку на неприятный сайт может позволить себе практически любой желающий. Олег Глебов, специалист департамента маркетинга компании «Информзащита», приводит следующие цифры: стоимость атаки мощностью 20–25 Гбит/с сегодня составляет максимум \$250 в сутки. Юлия Майорова, руководитель дирекции развития бизнеса Orange Business Services, называет еще меньшую сумму — \$70–90 в сутки. По ее словам, такая доступность этой «услуги» делает DDoS-атаки все более и более популярным инструментом в конкурентной борьбе.

Олег Шабуров, старший системный инженер Symantec в России и СНГ, добавляет, что ситуация резко обострилась в последние год-два: даже простым пользователям сети, не имеющим специального компьютерного образования, стали доступны наборы эксплойтов — компьютерных программ для облегчения запуска широкомасштабных атак. «По данным нашего ежегодного аналитического отчета об угрозах безопасности в интернете, число веб-атак, которые ежедневно фиксировались в 2010 году, возросло на 93% по сравнению с 2009 годом», — сообщает господин Шабуров. — При этом две трети угроз были созданы с помощью готовых наборов инструментов».

Немалый вклад в развитие DDoS-атак вносят бот-сети, число которых растет во многом за счет российских злоумышленников. По словам господина Шабурова, не так давно закрытый ботнет Rustock достиг численности более 1 млн подконтрольных компьютеров-ботов. Сеть из 10 тыс. ботов предлагается на черном рынке за символическую сумму \$15. Олег Шабуров опасается, что еще более серьезные проблемы могут возникнуть теперь, когда появилась возможность при необходимости арендовать управление крупными бот-сетями.

Юрий Наместников, ведущий антивирусный эксперт «Лаборатории Касперского», связывает уменьшение цены DDoS-атаки в первую очередь с ужесточением конкуренции на киберпреступном рынке. По его словам, в качественном плане технологии DDoS-атак за последние десять лет не



ПО СЛОВАМ ЭКСПЕРТОВ, ДОЛЯ РАСХОДОВ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ В ОБЩЕЙ СМЕТЕ РАСХОДОВ НА IT НЕ ДОЛЖНА БЫТЬ НИЖЕ 10–15%

очень изменились, а вот количество ботсетей, созданных для атак, увеличилось в разы, что и привело к появлению конкуренции на этом рынке. В борьбе за клиента киберпреступникам приходится снижать цены на свои услуги.

ЦИФРОВОЙ ХОЛЕСТЕРИН При отсутствии у подвергшегося атаке сайта средств защиты такое кибернападение забьет любой отдельно взятый ресурс в интернете. Неудивительно, что эта проблема стоит в России и во всем мире очень остро. Вот лишь несколько примеров крупных DDoS-атак за прошедшие годы.

В 2009 году была совершена атака на сайт интернет-платежей Assist, партнером которого в то время была компания «Аэрофлот». Недельный простой сайта стоил компании потери контракта с «Аэрофлотом» и серьезно подорвал репутацию платежной системы. Нередко DDoS-

атаки являются средством нечестной конкурентной борьбы. Так, в 2010 году на крупнейший сайт сообщества яхтсменов России (rusregata.ru) планомерно проводились акции, совпадающие с проведением регат. На рынок регатного спорта в то время выходило много новых организаций, которые вели себя довольно агрессивно с коммерческой точки зрения.

А в момент назначения губернатора Нижегородской области была осуществлена крупная атака на сайт «Виртуальная Выкса», который тогда в режиме реального времени освещал трагедию наиболее пострадавшего от лесных пожаров района Нижегородской области. Аналитики связали эту DDoS-атаку со стремлением подорвать имидж губернатора в преддверии его назначения на должность.

За прошедший год участились случаи использования DDoS-атак на сайты, которые оплачивают услуги рекламных агентств, увеличивающих посещаемость других интернет-ресурсов. В такой схеме работы владелец сайта оплачивает каждое уникальное посещение по ссылке, созданной и раскручиваемой нанятым агентством. Тем са-

мым оплачивается посещаемость ресурса. Успешно проведенная DDoS-атака позволяет подделать переход по ссылке, тем самым накручивая статистику. При этом для реального посетителя, который обратится к сайту, он будет вне доступа. Владелец сайта, с одной стороны, теряет посетителей на время атаки, с другой еще вынужден оплатить все поддельные посещения.

«Нередко DDoS-шторма являются лишь вуалью, с помощью которой скрывают более сложные атаки или факты утечки данных», — рассказывает Олег Глебов. — Важно понимать, что в конечном итоге DDoS-атака влечет за собой для организаций неминуемую потерю прибыли, которая существенно превышает затраты хакера на сам DDoS. Способствует такому положению дел и безразличие со стороны провайдера по отношению к проблемам безопасности клиентов. Как минимум отдельный пользователь или компания будет всегда обязана оплачивать огромный трафик DDoS-атаки. В очень редких случаях провайдер оговаривает DDoS форс-мажор с клиентом в рамках стандартного соглашения».

В РОССИИ ЗА ПОСЛЕДНИЙ ГОД 96% КОМПАНИЙ СТАЛКИВАЛИСЬ С ТЕМИ ИЛИ ИНЫМИ ВИДАМИ КИБЕРУГРОЗ. ПОЛОВИНА ИЗ НИХ В РЕЗУЛЬТАТЕ ТЕРЯЛА КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ