

ОПАСНАЯ ЗАВИСИМОСТЬ Чем больше информационные технологии и интернет входят в нашу жизнь, тем более зависимыми от них становятся бизнес-процессы. Антон Разумов, руководитель группы консультантов по безопасности компании Check Point, рассказывает, что 10–15 лет назад в рамках конкурентной борьбы было модно срывать отправку банками информации в межрегиональный центр информатизации при ЦБ РФ. Это могло привести к очень серьезным последствиям вплоть до отзыва лицензии, но для остальных компаний такого рода атаки не имели особого смысла. Сейчас же ситуация существенно изменилась. «Как вы думаете, во сколько обходится день простоя интернет-магазина или недоступность сайта по продаже билетов? Как минимум это упущенная прибыль за соответствующий период времени, — рассуждает господин Разумов. — Кроме того, помимо прямых финансовых потерь следует учитывать и существенные репутационные риски даже для традиционных компаний и даже возможность штрафных санкций. Что уж говорить о сервисах, специализирующихся на предоставлении онлайн-услуг, таких как Evernote, BaseCamp, SalesForce, платных разделах на новостных сайтах, интернет-аукционах».

Помимо такого фактора, как падение стоимости организации кибератак, играет существенную роль также и формирование рынка вокруг этой зловредной деятельности. Евгений Царев, заместитель директора департамента продуктов и услуг компании LETA, считает, что пять-десять лет назад рынок киберпреступности еще только формировался и нередки были случаи атак из любопытства или «обиды» на бывшего работодателя. Сейчас киберпреступность — это настоящая отрасль, и люди туда идут с целью заработка. По этой причине подавляющее число кибератак приходится на финансовый сектор. Сейчас очень остры проблемы с DDoS-атаками и атаками на системы дистанционного банковского обслуживания (ДБО). «Сегодня нет точной статистики по инцидентам в системах ДБО, почти все банки тщательно скрывают эти факты, однако по нашему опыту можно сказать, что таких инцидентов очень много», — говорит господин Царев.

ЗАЩИТА ЛУЖИНА В некотором роде решением для защиты от подобного рода угроз эксперты считают популярные сегодня «облака»: они позволяют использовать ресурсы, сравнимые с распределенными мощностями атакующих, но и их может не хватить. Хотя в этом случае можно просто наращивать ресурсы. «Так же, как перед новогодними праздниками поступают интернет-магазины, просто запуская дополнительные сервера, можно поступать и при повышении нагрузки в моменты DDoS-атак, в том числе автоматически. Это удобно своей простотой и оперативностью, но может оказаться довольно дорогостоящим решением», — заключает господин Разумов.

Также эксперт предупреждает о том, что если компания решила защищать свои ресурсы с помощью специализированных устройств, нужно помнить: они не способны защитить от перегрузки канала, поскольку устанавливаются на сайте клиента. Даже если в компании гигабитное подключение к интернету, то ботнет из 1 тыс. машин с под-



СЕГОДНЯ ЗАКАЗАТЬ DDoS-АТАКУ НА РЕСУРС КОНКУРЕНТА ИЛИ ПРОСТО НЕПРИЯТЕЛЯ МОЖЕТ ЛЮБОЙ ЖЕЛАЮЩИЙ. ЦЕНА УДОВОЛЬСТВИЯ — \$70-90 В СУТКИ

ключением в 10 Мбит/с (что сейчас далеко не редкость для домашних пользователей) с легкостью забьет канал и сделает сервис недоступным для легитимных пользователей. Хотя этот вариант защиты наиболее простой во внедрении и относительно недорогой.

Юрий Наместников, ведущий антивирусный эксперт «Лаборатории Касперского», считает наиболее эффективным на сегодня способом борьбы с этой угрозой распределенные системы фильтрации трафика. Чаще всего это программно-аппаратный комплекс, который поддерживается в актуальном состоянии рядом специалистов различного профиля: от системных администраторов до вирусных аналитиков, изучающих поведение DDoS-ботов. Подобные комплексы способны отразить даже очень мощные DDoS-атаки, и «Лаборатория Касперского» предоставляет услугу защиты от DDoS-атак именно на основе этой технологии.

Олег Глебов рекомендует для защиты от внешнего воздействия позаботиться о специализированных средствах очистки трафика или договориться с провайдером, который замкнет замусоренный трафик на собственные системы очистки или перенаправит их на арендованные у другой фирмы. Услуга такой удаленной защиты от DDoS, когда трафик идет через дата-центр внешней компании, специализирующейся на его очистке, стоит для средней пропускной возможности сети не более 700–1000 рублей за месяц аренды. На рынке также имеются аппаратные средства защиты от DDoS, которые представляют собой высокоспециализированные решения с пропускными способностями до 25–40 Гбит/с на устройство. Объединение таких продуктов в «ферму очистки» позволяет строить масштабируемые решения для каналов уровня глобальных ЦОД, крупных провайдеров и магистралей.

Существует также такая угроза, как внутренний DDoS. В этом случае внутренние компьютеры сети, подвергшиеся заражению, начинают забивать канал или серверные мощности других компьютеров компании. Внешние центры очистки у провайдера или устройства на границе периметра не смогут перехватить такой трафик. «В проведении такой атаки зачастую немаловажным является человеческий фактор, — предупреждает господин Глебов. — Если компания максимально защищена от проникновения извне, то злоумышленники будут стараться получить доступ в сеть организации уже не техническими методами, а при помощи социальной инженерии».

В таком случае в качестве носителей вредоносного кода могут быть использованы PDF-документы или зараженные письма. Такие комплексные элементы обмена данными потенциально содержат средства для атаки и используют уязвимости системы. Для крупных компаний внутренний DDoS объясняется низкими показателями безопасности филиалов, которые проще атаковать и заразить. А далее по смежным каналам передачи данных филиальная сеть может развернуть массивный DDoS против ресурсов головного ЦОД. Во избежание проблем внутри корпоративной сети организации нужно иметь систему очистки трафика на ядре сети, при этом сама сеть должна быть жестко разграничена на общие и критичные ресурсы.

В целом, утверждает Олег Шабуров, средства защиты не только успевают за киберпреступниками, но и работают на опережение. Пример тому — «облачные» репутационные технологии. Ежедневно появляются новые угрозы, которые не идентифицируются традиционными способами, основанными на сигнатурах, эвристических и поведенческих методах, а также системах предотвращения вторжений. Поэтому для защиты от новых и неизвестных угроз используются репутационные технологии, например комплекс Norton Insight Network, который анализирует анонимные данные о распространении программ более чем на 175 млн компьютеров клиентов и автоматически при-

сваивает высокоточные рейтинги безопасности более чем 2,5 млрд уникальных файлов. В базе данных содержатся рейтинги практически всех существующих вредоносных и безопасных файлов.

ТРАТЫ НЕИЗБЕЖНЫ Для компании B2B-Center вопрос информационной безопасности критически важен. Фирма поддерживает несколько электронных торговых площадок и использует все ресурсы: и человеческие, и программные, и аппаратные, чтобы сделать работу на электронной площадке максимально безопасной. Ситуацию на рынке оценивает генеральный директор электронной площадки B2B-Center Алексей Дегтярев: «В связи с тем что проблема актуальна, тем более с учетом того, что возможность организовать кибератаку не составляет труда, затраты на обеспечение информационной безопасности с каждым годом будут только расти».

Бизнес все больше уходит в интернет, поэтому угрозы информационной безопасности постоянно растут. «Чем больше размер онлайн-бизнеса, тем выше риск самых разных киберугроз, а значит, и бюджет построения защиты от угроз тоже должен становиться выше, — рассказывает Александр Трошин, технический директор «Манго Телеком». — На данный момент я бы посоветовал тратить любой компании с активным бизнесом в онлайн от 30% до 50% IT-бюджета на построение и поддержку серьезной системы ИБ. В среднем же сейчас на такую систему компании тратят не более 10%». Евгений Царев говорит, что сегодня доля расходов на информационную безопасность в общей смете расходов на IT не должна быть ниже 10–15%. А для телекоммуникационных и финансовых систем — не ниже 20%. «Что касается критичных систем, то доля ИБ должна быть выше, вплоть до 50% общих расходов», — заключает эксперт.

По мнению Олега Глебова, расходы на сдерживание DDoS-атак могут распределяться неравномерно. Можно заниматься постоянным наращиванием мощностей, расширением каналов или анализом и противодействием атак с помощью классических мер (блокировка). Даже в рамках небольших бюджетов на рынке ИБ есть возможность использовать как самые простые аппаратные решения, так и «облачные» средства защиты от DDoS (DDoS protection-as-a-Service). В ряде случаев компания не всегда готова перенаправлять собственный трафик за пределы своей сети, особенно если он содержит коммерческую информацию или персональные данные пользователей. В таких случаях необходимо организовывать комплексные системы защиты как от внешних, так и от внутренних DDoS-атак. Но тогда, как уже говорили эксперты, главной проблемой будет пропускная способность интернет-каналов «последней мили».

При этом Юрий Наместников предупреждает, что сложность атак будет расти, что повлечет увеличение затрат на обеспечение безопасности.

«Эту проблему необходимо решать на высоком уровне и в законодательном порядке пресекать деятельность компаний, которые предлагают услуги по кибератакам», — уверен генеральный директор электронной площадки B2B-Center Алексей Дегтярев.

Того же мнения придерживается Евгений Царев: «Для комплексного противодействия киберугрозам применяются технические (аппаратные и программные), организационные меры. Но этого недостаточно. Мировая практика показывает, что борьба с киберпреступностью малоэффективна без жесткого законодательства и правоприменения. Именно неотвратимость наказания играет решающую роль в борьбе с киберпреступностью. Однако в России в условиях фактической безнаказанности приходится полагаться только на построение эффективной системы информационной безопасности и специализированные компании, которые могут помочь в борьбе с DDoS и другими видами киберугроз». ■

СЕЙЧАС КИБЕРПРЕСТУПНОСТЬ — ЭТО НАСТОЯЩАЯ ОТРАСЛЬ, И ЛЮДИ ТУДА ИДУТ С ЦЕЛЬЮ ЗАРАБОТАТЬ. ПО ЭТОЙ ПРИЧИНЕ ПОДАВЛЯЮЩЕЕ ЧИСЛО КИБЕРАТАК ПРИХОДИТСЯ НА ФИНАНСОВЫЙ СЕКТОР

«БОЛЬШИНСТВО БОТНЕТОВ СЕГОДНЯ ЗАНЯТО РАССЫЛКОЙ СПАМА, А НЕ АТАКАМИ»

Компания SearchInform является одним из старейших российских игроков рынка средств информационной безопасности. Аналитик компании **РОМАН ИДОВ** рассказал корреспонденту **BG** **СВЕТЛАНЕ РАГИМОВОЙ**, как будет меняться ситуация на рынке в ближайшее время.

BUSINESS GUIDE: Насколько сильно изменился характер всевозможных киберугроз в связи с распространением новых технологий?

РОМАН ИДОВ: Сегодня достаточно остро стоит проблема DDoS-атак: нет никаких вычислительных ресурсов, способных эффективно противостоять грамотно спланированной атаке. В некотором роде решением этой проблемы являются популярные сегодня «облачные» технологии: в случае их использования мощности распределенных систем сравнимы с распределенными мощностями атакующих. Но их может не хватать.

Вообще, за последние годы ситуация, конечно, стала хуже. Сайтов вроде putinvzrivaetdoma.org, дающих любому желающему возможность внести свой сильный вклад в DDoS-атаку ненавистного ему ресурса, раньше не было. Хотя если сравнивать ситуацию с распространением спама, то здесь темпы роста уже не так впечатляют: организовывать DDoS не так выгодно и гораздо более рискованно, чем рассылать спам. Поэтому большинство ботнетов, работающих сегодня в сети, занято именно рассылкой спама, а не атаками.

BG: Но, получается, «против лома нет приема»?

Р. И.: Наиболее эффективной защитой от DDoS-атак будет создание распределенной системы, но это достаточно сложно и дорого. Многие пробуют бороться с атаками путем поиска их организаторов, но это также долго и не всегда эффективно. Большинство других приемов: фильтрация запросов, перенаправление атаки и другие — зачастую не дают желаемого эффекта. Однако средства защиты также не стоят на месте. Те же технологии cloud computing весьма эффективны при обслуживании сетевых ресурсов типа социальных сетей, нормальный трафик с которых парализует почти любой корпоративный сайт.

BG: Значит, именно на этот фронт борьбы с киберугрозами в ближайшее время будут брошены основные средства?

Р. И.: Не совсем. На сегодня главной проблемой становится внутренняя безопасность — передача закрытой корпоративной информации за пределы компании самими сотрудниками. Именно в защиту от таких угроз инвестируют сегодня дальновидные компании. Также очень серьезные вложения требуются в защиту от вредоносного ПО. Защита же от DDoS-атак становится делом не такого уж и большого числа компаний.

Больше всех на информационную безопасность тратят финансовые организации, в них они могут составлять 60% от всех затрат на IT. В других компаниях, где ИБ не настолько актуальна, затраты на нее ниже — например, в торговле она может не дотягивать и до 10% от общего объема. Наиболее важным обеспечение безопасности становится для тех компаний, которые работают именно с информацией.