Причина неувядающей популярности DDoS-атак в качестве криминального инструмента кроется в относительной простоте и дешевизне организации атаки. Сначала хакер с помощью вредоносных программ получает контроль над компьютерами, создавая так называемую зомби-сеть. При этом массовые заражения злоумышленнику не нужны: когда зомби-сеть достигает нужного объема — десятка тысяч зараженных машин, — вредоносная программа изымается из открытого доступа. При этом структура зомби-сети включает в себя промежуточные звенья между управляющей консолью и конечными компьютерами. В случае, если делом займутся правоохранительные органы, они придут к ничего не подозревающим пользователям зараженных машин.

Типичная схема атаки выглядит следующим образом: управляемый преступником компьютер посылает «заказ» для ботнета. Приговор ресурсу проходит через прокси-сервер, обеспечивающий анонимность хакера, после чего немедленно приводится в исполнение. Десятки тысяч компьютеров посылают постоянные запросы на атакуемый сервер, который не справляется с нагрузкой. В результате сайт недоступен, а задача выполнена. Создание зомби-сетей с нуля практикуется, но не слишком популярна: программное обеспечение также стоит немалых денег, и, что немаловажно, развертывание ботнета требует времени, тогда как желающим насолить конкуренту, как правило, нужен блицкриг. «Обычно в ботнет входит не одна тысяча компьютеров. В час X все зараженные машины получают команду и начинают атаковать определенный сервер. Атака заключается в формировании большого количества запросов к серверу, ответы которого будут просто игнорироваться. Легальные клиенты либо получат от сервера ответ с большими задержками, либо не получат его вообще»,— утверждает Виталий Камлюк, старший вирусный аналитик «Лаборатории Касперского».

Владимир Гайкович, генеральный директор компании «Информзащита», полагает, что в случае войны с Грузией речь шла о следующих цифрах: «Подобные DDoS стоят до $3000 в день. Проблема в том, что защита от них обойдется уже в $200 тысяч, и без каких-либо гарантий противодействия. Стоимость одного дня атаки и время „обрушения“ сайта зависит от большого числа факторов: выявленные средства защиты на атакуемой системе, пропускная способность канала и прочих».

ИМИДЖЕВЫЕ ПОТЕРИ Убытки, которые несут пострадавшие стороны, подсчитать крайне сложно: косвенный ущерб может в десятки раз превышать прямой. К примеру, атака на интернет-магазин, длящаяся сутки, означает существенные потери в средствах для владельцев магазина: нет доступа к сайту — нет покупателей, нет покупателей — нет денег. Та же атака продолжительностью несколько недель способна создать серьезную угрозу бизнесу и даже привести к закрытию ресурса. В случае же с виртуальной войной DDoS-атаки наносят куда более значимый имиджевый урон, чем материальный, считают эксперты.

«Смысл атаки на официальные сайты властных органов очевидны — продемонстрировать слабость структур безопасности, отвечающих за сохранность серверов,— комментирует Павел Данилин.— Это грандиозная имиджевая потеря, в том числе и лично для президента Грузии».

Но не стоит также преуменьшать силу информационного влияния официальных сайтов. «Новости с сайта президента России являются обязательной составляющей для всех информагентств, аналогичная ситуация и с сайтом Саакашвили. Блокируя такой ресурс, пресекается поступление через него информации, идет вызов грузинским специалистам по сетевой безопасности. Вариант с „самострелом“ — будто грузины сами обрушили себе сайты, чтобы вызвать сочувствие у общественности,— я полностью исключаю»,— говорит Павел Данилин.

МАЛО КТО ЗАДУМЫВАЕТСЯ О ТОМ, ЧТО ИНФОРМАЦИОННАЯ ВОЙНА В ИНТЕРНЕТЕ БЫВАЕТ ВЫГОДНА ИНОГДА ДАЖЕ КОМПАНИЯМ, ДЕЙСТВУЮЩИМ ЛЕГАЛЬНО. НАПРИМЕР, ПРОИЗВОДИТЕЛЯМ АНТИВИРУСОВ

ПАВЕЛ СОЛОВЬЕВ

ПОТЕРИ КРУПНЫХ КОРПОРАЦИЙ В СЛУЧАЕ DDOS-АТАКИ МОГУТ СОСТАВЛЯТЬ $200 ТЫС. ЗА ДЕНЬ. В СЛУЧАЕ ПОЛИТИЧЕСКОГО КОНФЛИКТА ОСНОВНОЙ УРОН ОТ ВИРТУАЛЬНЫХ АТАК — ИМИДЖЕВЫЙ

С ним согласен Владимир Гайкович: «DDoS-атаки на сайты не наносят особого урона, кроме имиджевого. В этом случае стоимость ущерба зависит лишь от того, кто во сколько свой имидж оценивает. Гораздо хуже, если такие атаки будут вестись на DNS- и почтовые серверы: в этом случае у госучреждений из средств связи останутся лишь телефон и факс».

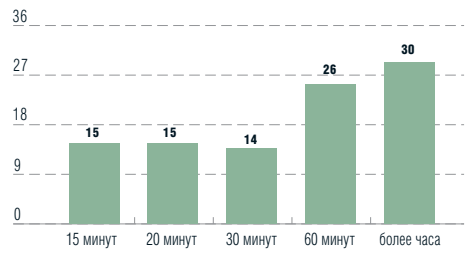
ПОНИЖЕНИЕ РЕЙТИНГА Но виртуальные столкновения могут также стать причиной и нанесения ущерба экономике государства. В первые дни российско-грузинского конфликта ведущие аудиторские конторы получили спам, компрометирующий экономическую деятельность Грузии. В результате Standard & Poor's и Fitch понизили рейтинг, обозначающий инвестиционную привлекательность государства. Финансовые аналитики утверждают, однако, что экономические последствия для сторон конфликта ощутимы, но не столь значительны. Заметный невооруженным глазом обвал индексов, заставивший паниковать мировую общественность, отразился и на России: с момента начала войсковых операций до закрытия последних торгов прошедшего августа на фоне осложнений отношений с Западом и оттока иностранного капитала из финансовой системы РФ индекс РТС снизился на 27,5%. Ощутимые последствия были и в инвестфондах: участники ПИФов, сорвавшие куш в июне, ликуют, остальные пытаются пристроить куда-нибудь свои стремительно обесценивающиеся накопления. Впрочем, подобная ситуация скорее всего продлится до октября, когда закончится финансовый год и ведущие компании предоставят свои отчеты. Поскольку в Грузии рынок акций находится в зачаточном состоянии, влияние фондового кризиса на страну было еще меньшим. «Единственная публично торгуемая на западных биржах бумага — акции Bank of Georgia (GDP), которые с 8 августа подешевели на 30%,— замечает Александр Осин, главный экономист УК „Финам Менеджмент“.— Надо отметить, что эти активы к концу прошлого месяца уже с начала текущего года теряли в цене порядка 100%, при этом американские бумаги финансового сектора в этот период оставались стабильны. Поэтому 80–90% указанного снижения я бы отнес на счет влияния южноосетинского конфликта».

Тем не менее, по мнению Александра Осина, даже для страны с неликвидным фондовым рынком последствия на других фронтах крайне существенны: «В августе 2008 золотовалютные резервы Национального банка Грузии сократились на $341 893 600, или на 26%. Очевидно, что часть этого сокращения вызвана общемировой финансовой конъюнктурой, сложившейся под влиянием ипотечного кризиса в США. Однако, учитывая, что весьма значимый для американских компаний полугодовой сезон отчетности в тот период уже подходил к концу, военный конфликт с Россией стоил Грузии порядка 80–90% этой суммы». Александр Осин считает, что, если объем нефти, поступающей транзитом через трубопровод, расположенный на территории Грузии, сократится, вооруженный конфликт может стоить грузинской стороне еще от $100 до $300 млн. Именно такие суммы корпорации, пользовавшиеся данным маршрутом ранее, заплатят российским транзитерам. Эксперт также сообщил, что платежный дефицит Грузии составляет порядка $750 млн, или около 5% ВВП, что с точки зрения глобальной статистики довольно много.

ВИРТУАЛЬНЫЕ ВОЙНЫ Были и попытки спекуляций на войне: например, спам, разосланный от имени Джорджа Сороса, призывал получателей ни в коем случае не читать книгу «Проект Россия». Впрочем, подобное поведение спамеров не редкость: как только в реальном мире происходит заслуживающее внимания событие, в ящики пользователей сыплется спам с соответствующими заголовками для привлечения внимания. Но редко кто задумывается о том, что от информационных войн в интернете выгода иногда бывает даже для компаний, действующих полностью легально. Многие из них, обладающие широкой способностью пропускных каналов (например, известнейшая американская телекоммуникационная корпорация AT&T), предоставляют за определенную плату защиту от DDoS-атак. Весь вредоносный трафик перенаправляется на сервер AT&T благодаря системе фильтрации, а атакуемый сайт остается доступным для пользователей. Надо отметить, что в России подобные услуги также существуют — и, что неудивительно, пользуются спросом, поскольку развертывание собственной защиты от атак стоит крайне дорого.

В арсенал желающего самостоятельно бороться со злоумышленниками должно входить отказоустойчивое программное обеспечение для фильтрации пакетов, мощные каналы доступа в интернет и сервер, способный обрабатывать миллионы мусорных запросов в минуту. Как и в случае с развертыванием зомби-сети, здесь требуется время, которого у владельцев атакуемого ресурса чаще всего нет: атаку нужно отразить сразу, поэтому покупка разовой услуги экономически выгоднее. Другой хороший пример — антивирусы: ни для кого не секрет, что во время любой эпидемии вирусов количество покупок программного обеспечения для защиты от вредоносных программ резко растет. «В августе продажи одного из популярных антивирусов в Грузии подскочили чуть ли не в десять раз»,— сообщает нам анонимный источник.

Автор доклада «Виртуальная криминалистика» Айан Браун в своем исследовании заявляет, что в компьютерное противостояние друг с другом вовлечено более 120 стран. «По сути, настоящей виртуальной войны мы еще не видели,— говорит Александр Гостев, аналитик „Лаборатории Касперского“.— Это были лишь шалости отдельных недовольных граждан или же групп киберпреступников. Но настоящие виртуальные войны ждут нас впереди. Тогда уже не надо будет искать виновных в DDoS-атаках: все военные действия в киберпространстве будут вестись открыто». ■



СРЕДНЯЯ ПРОДОЛЖИТЕЛЬНОСТЬ БЛОКИРОВОК DDOS-АТАК ПРОВАЙДЕРАМИ (%)
ИСТОЧНИК: ARBOR NETWORKS.