

телеком

DDoS с большой дороги

IT-безопасность

(Окончание. Начало на стр. 25)

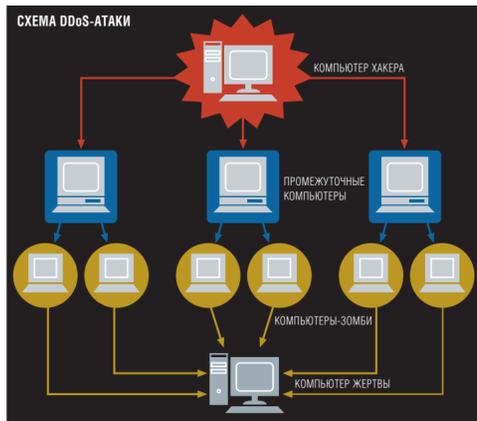
Особого внимания заслуживают именно «солдаты». Как правило, на компьютеры незаметно (при помощи вируса или через брешь в системе безопасности) внедряется специальная программа, которая никак себя не проявляет до поступления команды сверху. Случается, что «солдаты» могут дремать многие месяцы и даже годы, прежде чем будет подчинен воле хакера. Владельцы этих компьютеров даже и не подозревают, что участвуют в атаке. Из-за этой особенности в профессиональной среде специалистов по информационной безопасности такие солдаты получили название «зомби».

В компьютерном андеграунде зомби-сети являются основой гордости и торговли. Хакеры тратят много усилий и средств на их создание. Им требуется разрабатывать или заказывать специальные вредоносные программы, проводить их многократную рассылку, чтобы получить в сухом остатке работающую сеть достаточно мощных компьютеров. На подпольных форумах часто можно встретить объявления об аренде таких зомби-сетей или реализации атак с их помощью.

Как заработать и как заработать

Прошли времена, когда DDoS был уделом хулиганов и носителей диагноза геростратовой мании величия. Сегодня любителям под силу провести атаку разве что на себе подобно. Серьезные компании, бизнес которых зависит от интернета, используют мощные средства противодействия, справиться с которыми способен только настоящий профессионал. Со временем на услуги этих людей возник устойчивый спрос: заказы со стороны конкурентов, политические заказы, вымогательство и шантаж. А с другой — объективные экономические законы, согласно которым спрос рождает предложение. Постепенно на этой почве выросла настоящая индустрия.

Часте всего для проведения DDoS-атак хакеры используют вредоносные программы се-



ОСНОВНЫЕ ВИДЫ DDoS-АТАК

Флуд (англ. flood — наводнение) — наиболее распространенный вид. Связан с «бомбардированием» целевой системы большим количеством бессмысленных или неправомерных запросов с целью исчерпать ее ресурсы (процессора, памяти, пропускной способности канала) и провоцировать замедление или полный отказ. **Использование ошибок** в программе, приводящей к возникновению необрабатываемой исключительной ситуации и аварийному завершению серверного приложения. **Недостаточная проверка** данных пользователя, приводящая к исчерпанию процессорных ресурсов либо исчерпанию памяти. **Атака второго рода** — атака, которая стремится вызвать ложное срабатывание системы защиты и таким образом привести к недоступности ресурса. **Комбинированная атака** — комбинация описанных атак, направленных на отказ в обслуживании.

МЕТОДЫ ОБНАРУЖЕНИЯ DDoS-АТАКИ

Сигнатурные — в потоке сетевых данных производится качественный анализ и поиск определенных пакетов, свойственных DDoS. Малоэффективно против новых типов атак. **Статистические** — количественный анализ потока сетевых данных с целью выявления аномалий, свойственных DDoS. Главный недостаток — наличие ложных срабатываний и недостаточная эффективность. **Гибридные** — сочетают в себе достоинства обоих методов.

мейства SdBot, Rbot и BlackEnergy Bot. Это мощные системы, за плечами которых несколько лет непрерывного технологического совершенствования. В их арсенале развитое управление, функции автоматического обновления, перехвата данных и рассылки спама, — говорит Александр Гостев, ведущий антивирусный аналитик «Лаборатории Касперского», — По моим подсчетам, для отключения любого из 99% российских сайтов потребуется зомби-сеть из примерно 20 тыс. компьютеров. При этом ресурсы современных хакеров могут многократно превышать эту цифру.

Большинство DDoS-хакеров выполняют коммерческие заказы по нейтрализации конкурентов. Как правило, они распространяют объявления о своих услугах при помощи анонимных рекламных рассылок и разнообразных форумов. В целях конспиративного общения всегда ведется с анонимных адресов, дабы исключить возможность нежелательного контакта с правоохранительными органами, а оплата принимается на подставные счета обезличенных платежных систем и строго по принципу «вечером деньги — утром стулья».

По этой причине заказчик всегда рискует: он может стать

жертвой банального мошенничества, когда исполнитель исчезает сразу же после перечисления денег. В отсутствие гарантии он может связаться с любителями, которые не смогут достичь поставленной цели. Он может сам стать жертвой шантажа. Наконец, не исключено, что под видом хакеров ему придется общаться с правоохранительными органами.

Как в любом другом криминальном бизнесе, здесь нет жестких тарифов. Цена DDoS-атаки зависит от слишком многих факторов и ее колебания могут составлять до тысячи раз. К примеру, услуги любителей могут стоить 2–3 тыс. рублей за день атаки. Профессиональная «бомбардировка» веб-сайта средней руки — 7–10 тыс. рублей. Масштабная атака на хорошо защищенный сервер — до нескольких десятков тысяч долларов в день.

PR на DDoS

В последнее время эксперты отмечают использование феномена DDoS в неправомерных целях. «Иногда хочется задать вопрос — а был ли мальчик? Мне известны несколько случаев, когда на DDoS-атаки сваливали неадекватность IT-службы, из-за которой нарушалась нормальная работа систем. Согласитесь, большинство с сочувствием отнесется к жертве хакерской атаки и скорее всего, легко простит ошибку, — комментирует Евгений Преображенский, генеральный директор компании PerimeterX. — Факт наличия атаки проверить очень сложно и даже при таком раскладе данные можно легко фальсифицировать».

DDoS-атаки также используются для привлечения всеобщего внимания — в рекламных и политических целях. До сих пор сообщения об успешных атаках вызывают интерес публики и неминуемо занимают заголовки СМИ. Случается, что государства голословно обвиняют друг друга во враждебных действиях, используя в качестве доказательной базы тот самый пресловутый DDoS. Один из наглядных примеров — заявление эстонских «специалистов», которые якобы вычислили источник атак на правительственные сайты: он находился нигде иначе, как в

Кремле. И хотя несурзности этому обвинению не занимать, заявление попало в официальные каналы и было широко растиражировано западными СМИ как наглядное доказательство агрессивного поведения России в отношении небольшого демократического государства.

Несмотря на то, что тому нет прямых доказательств, многие эксперты не исключают, что технология DDoS активно используется и на правительственном уровне. Логично предположить, что в условиях сегодняшней зависимости бизнеса от коммуникаций и СМИ от интернета DDoS является весьма эффективным аргументом в политической борьбе и может представлять собой эффективный инструмент выяснения отношений между государствами в случае их обострения. Было бы очень неосмотрительно не учитывать этого и не проводить соответствующих исследований, как в области защиты, так и нападения.

Вопрос о кибертерроризме с использованием DDoS уже не раз поднимался на страницах печати и специализированной прессы. В первый раз об этом феномене заговорили в ноябре 2002 года. Тогда объектами атаки стали корневые серверы интернета, отвечающие за координацию работы всемирной сети в целом. В результате инцидента интернет был ненадолго расколот на национальные подсети, не имевшие возможности общаться между собой. К счастью, последствия удалось быстро преодолеть и восстановить нормальную работу серверов. Однако факт остался фактом: DDoS можно использовать в глобальных террористических целях. В результате таких действий могут быть нарушены важные коммуникации, глобальная экономика понесет многомиллиардные убытки, возникнет угроза жизни и здоровью людей. Увы, мировой паралич из-за отката интернета — это уже было



«Балаковские хакеры» получили по 8 лет за DDoS. Фото Ирины Егоровой

не сценарий дешевого блокбастера, но реальная угроза.

Неуловимые хакеры

В большинстве европейских стран и американских штатов приняты специальные акты, прямо и недвусмысленно определяющие хакерские атаки и ответственность за их реализацию. Российское законодательство в этом смысле более аморфно. Наиболее близкие статьи УК РФ — 272 («Неправомерный доступ к компьютерной информации», санкция — лишение свободы до пяти лет) и 273 («Создание, использование и распространение вредоносных программ для ЭВМ», санкция — лишение свободы до семи лет). Однако ни то, ни другое в случае с DDoS не работает. В ходе атаки неправомерного доступа не совершается, а факт использования вируса вообще недоказуем. Но даже если бы и появилась новая статья, направленная на наказание «эдосеров», она неминуемо вошла бы в категорию бумажек законов, которые на практике не работают. Запретить — одно дело. Совсем другое — найти злоумышленника и доказать его вину. А вот с

этим в России, увы, пока проблемы. За всю историю к уголовной ответственности (да и то по статье 163 УК РФ «Вымогательство») в России были привлечены лишь трое молодых людей (дело «балаковских хакеров»), занимавшихся шантажом и дэдос-атаками британских интернет-букмекеров на сумму около \$4 млн.

Несмотря на усилия властей и модернизацию законодательства, все эти действия, по сути, малоприменимы. При современной архитектуре интернета вычислить хакера практически нереально. Попадая в сети будут только неосторожные любители, а «крупная рыба» будет уходить безнакаленной. Те же «балаковские хакеры», по признанию специалистов, попались по глупости: в один ответственный момент забыли надежно скрыть свой адрес. Проще всего, конечно, выйти на «солдат», но реально привлечь их владельцев к ответственности невозможно — они сами пали жертвами злоумышленников. А несоблюдение норм компьютерной гигиены сегодня не является ни уголовно, ни административно наказуемым деянием. Прав-

да, в США уже раздают призывы к изменению подхода: приравниванию компьютера к объекту повышенной опасности и, соответственно, возникновению ответственности владельца за его надлежащее состояние.

Может сложиться впечатление, что всемирную сеть поразила неизлечимая эпидемия, которая рано или поздно приведет к тотальному коллапсу. В действительности, это не так. Как спрос рождает предложение, так и угроза вызывает ответную защитную реакцию. В последние годы индустрия информационной безопасности разработала ряд достаточно эффективных технологий для борьбы с DDoS. К обиде рекомендаций для снижения опасности и минимизации ущерба от атак относятся использование специального программного обеспечения (межсетевые экраны) и соблюдение общих правил компьютерной гигиены. Домашние пользователи могут сделать выбор из широкого спектра корпоративных продуктов. Для среднего и малого бизнеса потребуются шлюзовые межсетевые экраны, а для крупных организаций — высокопроизводительные брандмауэры. Необходимо также использовать и регулярно обновлять антивирусные программы, дабы незамедлительно не влиться в число зомби-компьютеров.

В перспективе борьба с DDoS неминуемо выйдет на глобальный уровень. Не только потому, что эта угроза приобретает планетарные масштабы. Но также из-за того, что эффективность обнаружения таких атак прямо пропорциональна уровню сбора или анализа статистики. Большинство методов бессильны вблизи цели, но практически безотказны на магистральной сети. На этом уровне можно с высокой вероятностью распознать дэдос, его тип, характер, побочные действия и оперативно разработать механизм защиты.

Денис Зенкин

NO COMMENT | THE AGE

Terror's new frontier: cyberspace

Новые рубежи террора: киберпространство

Tom Allard
Tom Olard

Технологии по обеспечению информационной безопасности — последняя площадка борьбы с терроризмом. Как утверждают аналитики, сегодня компьютерные сети управляют всеми жизненно важными сферами, которые становятся весьма уязвимыми для хакерского нападения. Что произойдет, если хорошо организованные преступные синдикаты, агенты враждебных государств и даже террористы выведут из строя компьютерные сети, на которых держится инфраструктура современных обществ?

Секретарь национальной безопасности Соединенных Штатов Майкл Чертофф считает угрозу вполне реальной и отмечает, что в будущем ситуация только ухудшится. Он не стесняется приводить примеры того, как такое разрушительное нападение может произойти. «Представьте, что наши финансовые системы подвергнутся нападению. И это бы парализовало их работу, — сказал он на недавно прошедшей в Сан-Франциско конференции по безопасности. — Происшествие подорвало бы доверие к нашей финансовой системе». А что, если бы террористы предприняли успешную кибератаку, которая нарушила бы работу системы управления воздушного транспорта, или, еще хуже, позволила бы хакерам направлять самолеты, приводя к столкновению их друг с другом или с землей? Одни эксперты считают, что вероятность такого Судного дня чисто гипотетическая, другие — что это просто завуалированное. Однако ответственные за обеспечение безопасности высшие чиновники во всем мире считают, что информационные технологии, на которых строятся экономические системы XXI века, — это ахиллесова пята.

Эта проблема вышла на передний план в Австралии, когда генеральный прокурор Роберт Маклелланд рассказал о том, что правительство рассматривает возможность предоставления права работодателям перехватывать электронные письма своих сотрудников без согласия последних. Подобные предложения входят в пакет новых мер, которые правительство готовится принять, чтобы противостоять угрозе кибератак на потенциально опасные объекты. Заявления генпрокурора вызвали оштрафованную критику со стороны юристов, а главное, подняли вопрос: насколько на самом деле эта угроза серьезна? Пока что отправная точка — это простая констатация факта: разные страны находятся в серьезной зависимости от интернета и других форм компьютерных сетей, необходимых для выполнения почти всех действий, будь то общественные, част-

ные, социальные, экономические или военные нужды. Учитывая зависимость национальных и мировой экономики от IT-систем, успешная и крупномасштабная попытка повредить компьютерные сети могла бы вызвать невероятные проблемы во многих секторах промышленности в разных странах и в итоге во всем мире.

Тем временем число подключенных к интернету и различным компьютерным сетям постоянно растет. «Риск того, что один-единственный обладающий соответствующими знаниями человек может вызвать массовый хаос, огромен, — отмечает Майкл Чертофф. — Кибератаки дают террористам и преступникам возможность нанести такой ущерб, вызвать который в реальном мире они никогда бы не смогли».

Создание киберпространства развивалось бесслесно и открыто. Его открытость как раз и была его главным преимуществом и причиной успеха. Но с точки зрения безопасности — это и самая большая его слабость. «В киберпространстве нет никакого законодательства. Нет никакой ответственности. Нет никаких правил. И развивается оно стихийно», — говорит Бретт Пепплер, бывший офицер разведки, который занимается сейчас исследованиями для австралийского Национально-исследовательского центра по национальной безопасности.

Экспертов по безопасности более всего волнует то, что потенциально опасные национальные объекты жизнеобеспечения подключены к интернету через свои сетевые компьютеры. Такими считаются объекты любого сектора промышленности, разрушение которых, ухудшение или вывод на длительный срок из строя приведет к значительному урону социального или экономического благосостояния нации. К ним относятся финансовые организации и банки, предприятия и учреждения коммунального обслуживания и связи, службы неотложной помощи и аварийные службы, энергетические и продовольственные сети, учреждения здравоохранения, воздушный транспорт и службы водоснабжения. Другими словами, большинство предприятий.

Джейсон Смит, исследователь Института информационной безопасности Квинслендского технологического университета, говорит, что в прошлом большая часть этой инфраструктуры контролировалась или непосредственно людьми, или же автономными системами, которые были в целом безопасны. Но развитие компьютерных технологий и стремление к снижению затрат привели к отказу от человеческого участия, и инфраструктура стала дистанционно управляться системами диспетчерского контроля и сбора данных (СКДА). «Это означает, что стало намного проще вмешаться в работу сетей, — говорит господин Смит. — А также то, что легче стало и получить доступ к информации».

Если бы хакеры запрограммировали или вывели из строя систему СКДА, последствия могли бы стать катастрофическими. С тех пор системы защиты СКДА улучшились, но то же самое произошло и с арсеналом инструментов хакеров. Наибольшую обеспокоенность специалистов вызывают атаки типа отказ в обслуживании (DDoS-атаки, т. е. множество запросов от огромного числа компьютеров со всего мира, зараженных вирусами).

К примеру, в прошлом году была совершена атака на веб-сайты правительства Эстонии. Тогда на серверы ежеминутно посылались тысячи запросов, что вывело их из строя и парализовало работу правительства, а также СМИ и банковских сайтов. Атаки совпали с решением эстонского правительства перенести памятник советскому солдату, установленный во времена СССР в честь победы Красной Армии над нацистами. Некоторые считают, что атака была организована разраженными российскими националистами. Другие же, включая эстонское правительство, увидели там руку российского правительства.

Роберт Маклелланд считает, что реальная проблема состоит в том, что «после такого нападения никаких отпечатков пальцев не найдешь». «Мы не можем узнать, кто именно устроил нападение, что делает традиционную модель сдерживания неспособной препятствовать этой разрушительной войне нападений на наши компьютерные системы», — отмечает Майкл Чертофф. Организованная преступность также взяла подобные инструменты на вооружение. Угроза обвала компьютерной сети — мощный инструмент для шантажа, также как и веровство закрытой коммерчески важной информации.

Готовы ли террористы использовать кибератаки для нанесения массового вреда? Бесспорно, экстремистские группы не лишены амбиций и имеют большой опыт по части использования интернета как эффективного инструмента для вербовки, финансирования и пропагандистских кампаний. На протяжении нескольких последних лет Аль-Каида регулярно угрожает кибератаками, но пока эти угрозы не были подкреплены конкретными действиями.

«Террористические группы владеют определенными компьютерными навыками, они активно нанимают на работу программистов и привлекают все больше и больше сумми денег через киберпреступления, — говорит исследователь ASP (австралийский стратегический институт) Энтони Берджин. — Естественное расширение деятельности для экстремистов станет очередной шаг, когда они попробуют организовать кибератаку на потенциально опасный объект».

Перевела Екатерина Дударева

РЕКЛАМА

IBM

МЕНЬШЕ СЛОВ БОЛЬШЕ СВОБОДНЫХ ДОРОГ

IBM помогает разрабатывать, внедрять и эксплуатировать системы регулирования транспортных потоков в городах по всему миру. В результате загруженность дорог становится меньше, а состояние окружающей среды — лучше. Хотите оптимизировать работу сложных систем? Начните с ibm.com/doing/ru. ОТ СЛОВ — К ДЕЛУ. ВРЕМЯ ПРИШЛО

IBM, логотип IBM являются зарегистрированными товарными знаками или товарными знаками International Business Machines Corporation в США и/или других странах. Названия других компаний, товаров и услуг могут являться товарными знаками или названиями обслуживания третьих лиц. © 2008 IBM Corporation. Все права защищены.