Антикиллер: возможна ли эффективная защита от DDOS-атак?

Игорь КИРИЛЛОВ

Атака типа «отказ в обслуживании» (DDoS) является сегодня одной из наиболее известных угроз в сфере информационной безопасности. Легкость, с которой можно получить доступ к этому кибероружию, способствует его быстрому распространению. Но эффективная защита возможна, хотя и может обойтись недешево.

Представьте, что вы стоите в очереди в кафе быстрого питания. Ваш запрос достаточно стандартный — вы просто хотите перекусить в обеденный перерыв. Перед вами всего один человек, но ведет он себя достаточно странно. Вместо того чтобы, как все, заказать набор из нескольких типовых продуктов, на что уходит обычно не более минуты, он требует, чтобы ему приготовили миллион чашек кофе и выпекли столько же пончиков. Такой запрос физически невозможно обработать, и в реальной жизни подобного клиента просто отправили бы по известному адресу. Но представим, что продавец все же пытается его выполнить. Естественно, в таком случае больше никто из клиентов еще долго не получит доступа к продуктам, и кафе потеряет реальных покупателей, да и сам этот странный человек, скорее всего, не станет забирать свой заказ. В результате — убытки и потери для бизнеса. В среде людей подобную ситуацию можно представить лишь теоретически, но в мире вычислительных машин такая схема загрузки сервера обработкой огромного количества бесполезных запросов получила название атаки типа «отказ в обслуживании» (Denial of Service, DoS). В случае, когда нападение осуществляется сразу из нескольких источников, такую атаку именуют «распределенной» Distributed Denial of Service. Собственно DDoS и является сегодня наибольшей угрозой, поскольку единый источник DoS-атак все современные системы безопасности уже давно научились выявлять и блокировать.

Проблема осложняется тем, что организовать DDoS можно быстро и недорого. От подобных нападений страдают сайты коммерческих компаний, государственных структур и других организаций. В то же время эффективно противодействовать серьезному нападению относительно сложно и дорого, для этого приходится прибегать либо к использованию дорогостоящих аппаратных решений, либо пользоваться услугами коммерческих онлайн-сервисов. Но все равно ни одни из методов не дает 100% защиты, если за вас решили взяться всерьез.

Удивительно и то, как быстро злоумышленники учатся извлекать пользу из новых концепций и технологий. На службу DDoS уже поставлены «облака» и даже «Интернет вещей».

Угроза из принтера

С точки зрения злоумышленников, DDoS-атака — это просто дешево и элегантно. Так же, очевидно, полагают и некоторые бизнесмены, не пренебрегающие «грязными» методами конкурентной борьбы. В последние годы расценки на организацию подобной угрозы постоянно падают, а число предложений растет. Первые сведения о DoS/DDoS-атаках датируются 1996 годом, и за прошедшие двадцать лет они ощутимо эволюционировали. Сейчас все вообще стало до смешного просто. Услуги по организации DDoS открыто предлагаются через Интернет. Стоимость зависит от продолжительности атаки, ее интенсивности и степени защищенности поражаемого ресурса. Так, большинство коммерческих сайтов, размещенных у недорогих хостинг-провайдеров, вообще никак не защищены от распределенной атаки. «Положить» такой ресурс на сутки стоит в среднем $40 (минимальная средняя цена, за которую злоумышленники возьмутся устроить «отказ в обслуживании»). При этом исполнители (назовем их «налетчики») дают почти полную гарантию эффективности, что, по отзывам на тематических ресурсах, полностью соответствует действительности. Сайт с минимальной базовой защитой выведут из строя за $60–70 в сутки.

Бывает и дешевле. Но, как говорят эксперты, за «демпинговыми» предложениями в основном стоят начинающие «специалисты», обычно студенческого возраста. Сложную систему обороны пробить бывает достаточно трудно, предложений здесь на порядок меньше. Счет выставляют по ситуации —

Надійний захист від DDoS-атак

A10 Networks ARBOR NETWORKS IMPERVA

NETWELL УКРАЇНА

Україна, 03037, Київ, пр. В. Лобановського, б. 56 / 21а, 8 поверх
Тел.: +380 44 359 07 79 E-mail: kiev@netwell.com.ua www.netwell.com.ua

несколько сотен долларов вначале, затем ценник может значительно увеличиться, вплоть до $1 тыс. в сутки и более. Самое неприятное в этой ситуации, что эффективная защита может обойтись на порядок дороже, но без нее ваш интернет-ресурс гарантированно выведут из строя, так что выбора особо нет.

Основным источником DDoS-атак являются т.н. бот-сети — распределенные экосистемы ПК, являющиеся латентными носителями особых компьютерных вирусов. Такие компьютеры еще называют «зомби» или «боты». По команде из «центра» эти машины начинают одновременно генерировать запросы на указанный адрес в Сети (часто через промежуточные компьютеры), вызывая отказ атакуемого маршрутизатора или сервера (**рис. 1**).

При этом вирусы в большинстве случаев находятся на ПК обычных пользователей, которые долгое время не подозревают об их наличии. Профессиональные «налетчики», чьи атаки стоят сотни и тысячи долларов США, как правило, имеют в подчинении сеть из нескольких десятков тысяч ботов и способны генерировать балластный трафик, измеряемый десятками Гбит/с.

Более того, на практике возможности «налетчиков» высокой квалификации ограничены только насущной необходимостью. Если надо, уровень атаки (и ее стоимость, естественно) может достигать просто фантастических показателей. Так, интенсивность трафика крупнейших DDoS-атак составляет сотни Гбит/с (400–500 Гбит/с в 2015 году).

Вот кое-что из новых примеров: в начале 2016 года совершено нападение на один из информационных ресурсов BBC (официальный сайт предвыборной кампании Дональда Трампа). Интенсивность атаки превысила 600 Гбит/с. В середине сентября 2016 года был атакован сайт Брайана Кребса — американского журналиста и активного борца с киберпреступностью. Его расследование позволило вычислить двух израильских хакеров и ликвидировать вредоносный ресурс vDOS. В результате через несколько дней после задержания преступников (которыми, к слову, оказались два 18-летних парня) на сайт журналиста обрушился «шторм» интенсивностью более 620 Гбит/с. Атаку удалось отразить с большим трудом при помощи сервиса Akami, который оказал журналисту безвозмездную поддержку.

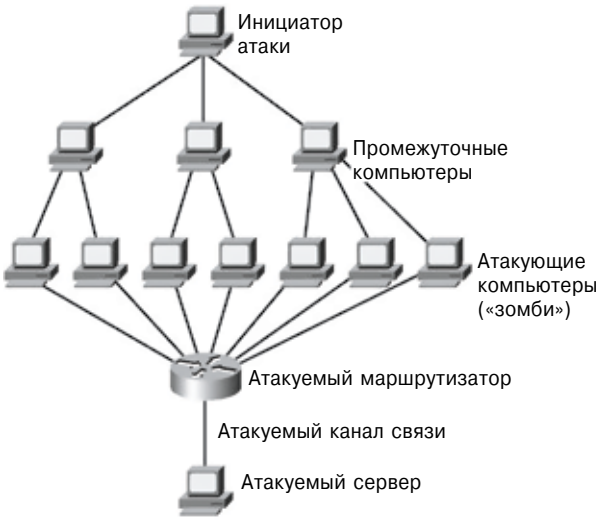

Рис. 1. Общая схема DDoS-атаки

В том же месяце мощная акция была организована против французского хостинг-провайдера OVH. Здесь, впервые в истории Интернета. интенсивность DDoS-атаки превысила 1 Тбит/с. Для генерации такого объема трафика было задействовано более 150 тыс. ботов. При этом злоумышленники использовали сложные комбинированные алгоритмы нападения и продолжали оказывать давление на атакуемые ресурсы в течение многих дней. В целом ценой больших усилий атаку удалось купировать, но указанные цифры говорят о потенциальных возможностях «налетчиков». Более того, современные технологии способствуют интенсификации DDoS. Так, рассмотренная атака опиралась на бот-сеть, состоящую главным образом из устройств IoT (Internet of Things, «Интернет вещей») — веб-камер, маршрутизаторов и даже термостатов. К тому же, по данным профильных организаций, анализировавших инцидент, всего бот-сеть, атаковавшая сайт, могла включать в себя до 400 тыс. устройств.

Еще одна похожая по интенсивности DDoS-атака произошла в конце октября с.г. Здесь также была задействована сеть IoT; при этом, по данным того же Брайана Кребса, значительная часть балластного трафика сгенерирована принтерами Xerox и Panasonic. Атака была направлена против провайдера Dyn и затронула деятельность многих сервисов на территории США, в т.ч. Twitter, PayPal, Amazon и др.

На постсоветском пространстве мощность наиболее интенсивных атак обычно не превышает нескольких десятков Гбит/с, но, как правило, даже таковые случаются пока что очень редко.

В то же время, как отмечает ***Алексей Музыченко***, заместитель директора департамента облачных и ИКТ-сервисов ***«Датагруп»***: ***«В этом году количество DDoS-атак в Украине выросло в среднем на 25–30%. Страдают главным образом организации финансового сектора, банки, интернет-магазины, государственные структуры. Основной нынешний тренд — это возрастание уровня сложности DDoS-атак, которые становятся все более комплексными. Киберпреступники чаще стали практиковать ведение нескольких атак одновременно. Нападающие быстро меняют тип атаки, если видят, что она теряет эффективность. Также можно отметить, что все чаще используются сравнительно небольшие атакующие бот-сети, растет количество т.н. DDoS-атак с усилением (amplification ddos). Соответственно увеличивается и спрос на услуги защиты, особенно со стороны тех компаний, чей бизнес связан с интернет-сервисами».***

По словам ***Константина Коваля***, директора по информационным технологиям компании ***GigaGroup*** (TM Gigatrans, Gigacenter, Gigacloud): ***«Сейчас модными стали не классические методы «объемных» (т.н. volumetric) DDoS-атак, а более современные и «умные» алгоритмы — типа low-and-slow. Мы наблюдаем уменьшение числа нападений первого типа, которые направлены на быструю блокировку работы Интернет-ресурса. В то же время возросло количество атак второго типа (направленных на приложения), которые медленно, но верно, укладывают ресурс «на лопатки». Такие атаки сложнее отследить, с ними труднее бороться. Ведь для них не подходят старые методы борьбы, да и длятся они дольше, чем классические volumetric-атаки. В силу того, что сейчас DDoS-атаки стали более разумными, определить момент начала нападения становится все сложнее. В Украине, как правило, средняя***

продолжительность агрессивной volumetric-атаки не превышает часа, в то время как low-and-slow длятся неделями».

Преступление как сервис

Что касается глобальной географии атак, то, по данным «Лаборатории Касперского», по состоянию на конец третьего квартала 2016 года 62,6% всех DDoS-инцидентов пришлось на долю КНР, еще 18,7% на США, на третьем месте Южная Корея — 8,7%, на четвертом — Япония (1,6%). Вклад каждой из остальных стран составляет менее 1%. Если говорить про абсолютные цифры, то, по различным данным, каждый день в мире фиксируется в среднем более 2 тыс. DDoS-атак, и число их быстро увеличивается. Длительность наиболее продолжительных из них составляет 10–12 суток и более. Что касается источников нападений, то, по информации той же «Лаборатории Касперского», лидером здесь является Южная Корея — в третьем квартале 2016 года более 45,8% центров управления бот-сетями находилось на территории этой страны. На втором, третьем и четвертом местах находятся КНР, США и Россия — 12,4%, 9,6%, 5,2% соответственно (Украина, с двумя процентами, — в конце первой десятки). Но справедливости ради стоит отметить, что от квартала к кварталу ситуация разительно меняется, что отражает глобальный характер рынка.

Более того, в последние месяцы специалисты все чаще оперируют таким экзотическим до недавнего времени понятием, как Cybercrime as a Service («Киберпреступление как сервис»), что говорит об оформлении разрозненных злоумышленников в некое подобие криминального синдиката, наиболее популярным оружием которого является именно DDoS. На самом деле проблема приняла весьма угрожающий характер, ею даже всерьез занялся Европол. Так, 28 сентября появился очередной отчет 2016 Internet Organized Crime Threat Assessment («Оценка угроз 2016 года, связанных с организованной преступностью в Интернете»), в котором DDoS-атаки называются основной угрозой для любой организации, работающей в Сети.

Каковы же причины DDoS-атак и кто чаще всего становится их жертвами? Как правило, мотивов не так уж и много, а точнее — три: недобросовестная конкуренция, шантаж и месть (некоторое количество, не более 10%, атак осуществляется в качестве тренировки или развлечения). Соответственно, объектами нападений чаще всего становятся коммерческие компании — главным образом банки и другие финансовые учреждения, розничные интернет-магазины, турфирмы, сервисы продажи билетов, агентства недвижимости и т.д. Ущерб от DDoS-атаки может быть различным. В принципе любая компания может точно или приблизительно подсчитать, во сколько обойдется день или час простоя ее интернет-сайта. Естественно, что в различные периоды сумма будет разной. Так, остановка ресурса онлайн-торговли во время предпраздничных распродаж или туристического сервиса в сезон отпусков может привести даже к разорению компании или, по крайней мере, серьезному отставанию от конкурентов и потере доли рынка, не говоря уже о непосредственно упущенной выгоде.

О степени угрозы говорит, например, случай с разоблачением в начале этого года международной группировки злоумышленников, которые при помощи DDoS-атак вымогали деньги у различных онлайн-сервисов (в основном сетевых казино и платежных систем). За отказ от нападения преступники получали до $25 тыс., расчеты производились с помощью «криптовалюты» биткоин. Также в последнее время выросло количество политически-мотивированных DDoS-атак, но это тема отдельной статьи.

Прямая и явная угроза

Атаки типа DDoS — это общее название большого семейства технологий, включающих в себя множество различных методов и подходов. При этом нападение может осуществляться на любом уровне модели OSI (**табл.**). Сегодня чаще всего это 3–4 (сетевой либо транспортный) уровни. Но в последнее время резко увеличилось число нападений на седьмом уровне (приложений), что объясняется сравнительной простотой данного метода ввиду появления новых инструментов для его реализации. Результатом такой атаки, использующей различные уязвимости в прикладном ПО или ОС, становится выход из строя программы или даже операционной системы. Неприятной особенностью атаки на уровне приложений является то, что ее крайне трудно выявить, поскольку она с высокой степенью достоверности имитирует полезный трафик.

Таблица. Примеры DDoS-атак на различных уровнях модели OSI

Тип атаки	Уровень модели OSI*	Задействованные протоколы	Формы воздействия	Последствия
MAC-флуд	2 (канальный)	802.3, 802.5	Переполнение коммутаторов пакетами данных	Исчерпание пропускной способности атакуемой сети за счет фактической блокировки работы портов коммутатора
ICMP-флуд	3 (сетевой)	IP, ICMP, ARP, RIP	Переполнение канала ICMP-запросами	Ухудшение пропускной способности атакуемой сети вплоть до полной неработоспособности
SYN-флуд, Smurf-атака	4 (транспортный)	TCP, UDP	Отправка жертве ICMP-запросов с измененными адресами	Заполнение канала связи балластными запросами, сбои в работе сетевого оборудования
Атака на Telnet	5 (сеансовый)	RPC, PAP	Делает недоступным сервер Telnet на коммутаторе	Потеря контроля над коммутатором
Ложные SSL-запросы	6 (представительский)	ASCII, EBCDIC	Обработка каждого SSL-запроса требует значительных аппаратных ресурсов	Истощение аппаратных ресурсов сервера. Аномально высокая нагрузка на вычислительную подсистему
Запросы http get и http post	7 (прикладной)	FTP, HTTP, POP3, SMTP	Загрузка изображений и видеороликов, запрос на подтверждение обратной связи	

* На первом (физическом) уровне речь может идти только о непосредственном повреждении оборудования или сетевых соединений

Максим АНОШКО, ведущий специалист компании «Нетвелл-Украина»

Универсальных средств защиты от DDoS, к сожалению, не существует

Ситуация с DDoS-атаками в Украине крайне неутешительная, мы наблюдаем рост их количества с каждым годом. Это отмечают многие аналитические компании, специалисты в области информационной безопасности, а также сами заказчики, которые все чаще сталкиваются с тем или иным видом сетевых угроз. Если ранее эти угрозы были по большей части общими и узнаваемыми, то сейчас атаки значительно эволюционировали и приобрели целенаправленный, точечный характер. Их длительность составляет от нескольких часов (как правило, за это время злоумышленники просчитывают требуемый вектор воздействия) до нескольких дней или даже недель с необходимой периодичностью. Ущерб, наносимый злоумышленниками, особо возрос в финансовом и государственном секторах. Если ранее количество атак исчислялось сотнями, то сейчас это десятки тысяч разнообразных по своей природе зловредных действий.

Так называемый «классический DDoS», разнообразные флуд-атаки, большинство из которых могут быть подавлены средствами безопасности периметра, пограничными маршрутизаторами, – уже не в моде. Этот вид угроз все еще широко применяется, но скорее для сокрытия более серьезных угроз злоумышленников, чем для простого переполнения канала или блокирования работы веб-ресурсов. Эти угрозы имеют обобщенные признаки внедрения – цепочку действий, известную как kill chain. Как правило, это поэтапные действия в следующей последовательности: «разведка» – «вторжение» – «захват» – «похищение». Такие атаки получили название APT (Advanced Persistent Thread) – «развитая устойчивая угроза».

Современные злоумышленники не ограничены в технических и финансовых возможностях на разработку, планирование и, собственно, осуществление злонамеренных действий относительно жертвы. Внедренные структурные единицы системы безопасности компаний, межсетевые экраны, IPS/IDS и т.д. не способны защитить от проникновения, они лишь доставят временное неудобство киберпреступнику. Риск того, что жертва пропустит серьезную угрозу, очень велик.

Учитывая всю сложность и разнообразие атак, нельзя утверждать, что есть универсальное решение, которое спасет от всех угроз. Наша компания предлагает решения от общепризнанных лидеров рынка ИТ-безопасности: специализированные комплексы подавления и расследования инцидентов вторжений разработки Arbor Networks, высокопроизводительные TPS-платформы A10 Networks, «облачные» сервисы защиты от DDoS – Imperva Incapsula. Спрос на средства противодействия и защиты за 2014–2016 годы вырос на порядок. С каждым годом количество внедрений оборудования для обороны критически важных и/или уязвимых сегментов сетевой инфраструктуры растет.

К основным видам DDoS-атак можно отнести главным образом различные виды «флуда» (от англ. flood — поток, глупая болтовня), которые путем отправки большого количества бесполезных запросов со множества адресов позволяют эффективно заполнить канал передачи данных или исчерпать вычислительные ресурсы сервера. «Флуд-атаки» чаще всего осуществляются на 3-м и 4-м уровнях OSI. Например, в случае http-флуда вредоносный ПК отправляет жертве небольшие http-пакеты, провоцируя атакуемый сервер на отправку ответных пакетов (размер которых больше). При должной интенсивности запросов канал переполняется достаточно быстро. Флуд по различным алгоритмам часто осуществляется также на уровне TCP, UDP, ICMP-протоколов.

Еще одним распространенным способом атаки является т.н. метод «медленных Post-запросов» (Slow HTTP Post). В случае обычного post-запроса со стороны клиента веб-сервер принимает данные, заключенные в тело сообщения, для хранения и никаких проблем с этим, обычно, не возникает. Но в случае DDoS запрос имеет особые параметры — во-первых, большой объем, а во-вторых, он отправляется маленькими частями, скажем, по одному байту. В результате сервер открывает большое количество соединений для приема каждого однобайтового сообщения, что существенно замедляет его работу. Вместо post-запроса может быть использована «медленная» отправка http-заголовка со схожим результатом воздействия, тогда такой метод называется Slow HTTP headers. Для замедления работы атакуемого сервера могут использоваться также особые боты, имитирующие работу программных роботов поисковой системы Google и множество других ухищрений. Арсенал преступников постоянно растет.

Защита из «облака»?

Но и средства защиты не стоят на месте. Хотя обходятся они, в общем, недешево, но все же во многих случаях это лучше, чем нести убытки от простоя своего интернет-сервиса или выплачивать отступные кибервымогателям. Методов и технологий защиты сегодня существует немало. Организовать противодействие можно как собственными силами, так и путем аренды соответствующего сервиса у своего провайдера или специализированного «облачного» оператора. Какой из этих подходов лучше — зависит от конкретной ситуации и уровня угрозы. Здесь спор переходит в традиционную плоскость обсуждения преимуществ владения/аренды. В общем случае для небольших компаний достаточно недорогих базовых программных сервисов или защиты, которую штатно обеспечивает хостинг-провайдер.

Однако такие методы защиты, как правило, бесполезны при мощных или алгоритмически сложных «штормах». Здесь поможет либо специализированный аппаратно-программный комплекс, либо подключение внешнего «облачного» сервиса. Но в общем случае эффективная защита от DDoS — это целый комплекс мер, в котором конкретная система защиты является лишь одним из важных элементов. Грамотные действия специалиста по сетевой безопасности, а также предварительная работа, направленная на выявление и устранение потенциально узких мест, способна существенно снизить или даже свести к нулю эффективность большинства DDoS-атак.

Собственно методов борьбы с DDoS множество. Ни один из них не является универсальным и, как правило,

Интенсивность DDoS-атак в Украине растет

Ярослав БОЦМАН, главный консультант отдела разработки системных решений «Эс Энд Ти Украина»

Информационное пространство Украины характеризуется высокой восприимчивостью к DDoS-атакам. Последние годы наша страна стабильно входит в число лидеров по количеству подобных инцидентов. Этому способствует низкий уровень защиты систем и сложная политическая обстановка. При этом однозначно оценить потери от DDoS-атаки достаточно сложно. Размеры ущерба состоят не только из прямого финансового ущерба, но и включают в себя косвенные потери. Как правило, точный подсчет возможен только для систем дистанционного обслуживания абонентов и электронных торговых площадок. Потери от простоя банковского сервиса приблизительно можно оценить в 10% от общего оборота банка за период атаки, т.е. они могут достигать миллионов $.

В Украине основными жертвами DDoS-атак являются информационные системы органов власти (сайты Центризбиркома, Кабинета министров, президента Украины, электронных деклараций и т.д.), коммерческие площадки электронной торговли, интернет банкинг, а также сайты СМИ. Средняя продолжительность атаки составляет около недели и в последнее время остается стабильной, в отличие от интенсивности, которая имеет тенденцию к увеличению.

Максимальная интенсивность атак в Украине зафиксирована на уровне 10 Гбит/с. При этом успешные DDoS-атаки развиваются по двум направлениям – загрузка канала связи и исчерпание системных ресурсов (памяти, процессора и т.д.). Для генерирования большого потока запросов необходимо построение огромной распределенной бот-сети, что на практике достаточно сложно. Поэтому основным трендом в действиях злоумышленников является использование уязвимостей системных ресурсов.

Естественно, что в таких условиях интерес к системам защиты от DDoS-атак растет год от года. К сожалению, экономическая обстановка в нашей стране заставляет компании экономить на внедрении соответствующих систем и очень часто ограничиваться частью функционала защиты, реализованного в рамках других решений (МСЭ, IPS, и т.д.). Но актуальность организации защиты от DDoS-атак приводит к увеличению интереса к специализированным системам, в том числе «облачным».

в зависимости от типа и характера атаки применяется комбинация нескольких подходов. Зачастую функции защиты от подобных атак реализованы в рамках межсетевого экрана (например, экраны ICMP- и UDP-флуда). Система защиты также может выявлять подозрительные запросы — слишком частые/объемные/«медленные». Часто помогает оперативный анализ лог-файлов, позволяющий выявить вредоносные адреса, которые затем можно внести в «черный список». Кстати, таким образом отслеживают также и «подозрительные» страны. Скажем, на ваш сервер вдруг начинает приходить большое число запросов из Южной Кореи (хотя раньше вы с этой страной не работали). Это явный признак DDoS-атаки, которую можно ликвидировать, добавив в «черный список» целую страну.

Один из простых и эффективных вариантов — наращивание собственных вычислительных или сетевых ресурсов. Часто мощный сервер или действительно широкий канал может «перемолоть» атаку. В некоторых случаях при наличии производительного сервера можно даже провести контрнападение против системы злоумышленника. Еще один вариант — использовать распределенные серверы и несколько резервных каналов связи (в случае переполнения одного из них запросы клиентов можно будет направить по другому маршруту). Хорошие результаты приносит также фильтрация трафика. Но в целом методов и подходов к защите от DDoS сегодня множество. Их детальное рассмотрение не входит в план статьи, отметим лишь, что наибольшая эффективность достигается в комбинации превентивных технических мер, применении межсетевых экранов и оперативной реакции службы сетевой безопасности.

В последнее время все большую популярность приобретают «облачные» сервисы, обеспечивающие все вышеперечисленные методы защиты на постоянной и профессиональной основе. Клиенту достаточно лишь подключиться к сети оператора и регулярно вносить абонплату. Такие сервисы очень популярны в мире, но есть они уже и в нашей стране. Например, оператор ***«Датагруп»*** уже более семи лет предлагает услугу по защите клиентов от DDoS-атак под названием DataProtect.

Для противодействия угрозе используются, в частности, программно-аппаратные комплексы операторского уровня. Осуществляется многоуровневая фильтрация и анализ поведения трафика. Как заявляют в «Датагруп», уже через 10 минут после подключения к сервису эффективность отражения атаки составляет 80%. В течение этого времени система автоматически изучает трафик клиентской сети и формирует его базовый профиль. Затем в течение следующих 6–12 часов модуль защиты создает детальный профиль трафика, что позволяет в будущем быстро определять аномальные данные и повысить эффективность защиты до 99,9%. По данным оператора, пропускная способность системы составляет до 10 Гбит/с.

Защита от DDoS-атак имеется в арсенале (как дополнительный сервис) также у многих хостинг-провайдеров, предлагающих в аренду виртуальные и физические серверы. Так, оператор с говорящим названием ***AntiDDOS*** предоставляет соответствующие услуги с 2007 года, в основном используя профессиональные решения Cisco и Juniper. По данным компании, ей неоднократно удавалось отражать атаки интенсивностью 20 Гбит/с, а после модернизации в 2015 году система защиты способна нейтрализовать «шторм» в 60 Гбит/с, о чем говорят специально проведенные тесты, результаты которых представлены на сайте компании.

Еще один оператор, ***Hostlife***, обещает в случае необходимости «побороть» атаку интенсивностью даже в 80 Гбит/с, но стоить это будет недешево — такая защита обойдется в $2 тыс. за месяц. Правда, атаки такой интенсивности в нашей стране пока не отмечены, поэтому более актуальными будут другие расценки. Например, при ежемесячной абонплате $1 тыс. оператор ликвидирует атаку интенсивностью 40 Гбит/с, а за $250 — 10 Гбит/с. При этом DDoS-угрозы, генерирующие трафик 2 Гбит/с, Hostlife готов отразить всего

за $5 в месяц. Как видим — чем более интенсивная атака, тем сильнее растет стоимость ее ликвидации.

Компания ***Tanhost*** («Танграм Украина») готова отражать нападения интенсивностью до 10 Гбит/с, при этом на подавление атаки может уйти от 30 до 50 минут. Расценки колеблются в зависимости от выбранного тарифного плана. Так, минимальная стоимость защиты для одного сайта составляет 6,5 тыс. грн. в месяц плюс 1,3 тыс. грн. за подключение услуги. Самый дорогой тариф подразумевает защиту выделенного сервера с десятью доменами на нем. В этом случае за подключение придется отдать втрое больше — 3,9 тыс. грн., а за ежемесячное использование сервиса — 18,2 тыс. грн. В промежутке между этими крайностями имеется еще шесть стандартных тарифных планов. Защиту от DDoS предлагают в Украине также Gigacenter (на базе оборудования Juniper), UniHost и другие операторы.

Что касается мировых сервисов, то в числе наиболее известных можно назвать таких гигантов отрасли, как Akami, CloudFare, CenturyLink, Imperva, Level3, Neustar и др. В целом же, по данным последнего тематического отчета IDC, объем мирового рынка услуг защиты от DDoS-атак составил в 2015 году более $300 млн и продолжает активно расти. Какова здесь доля украинского сегмента, сказать сложно, если даже в РФ этот рынок в прошлом году едва превысил $16,3 млн.

Аппаратные решения

Если по каким-либо причинам арендная модель заказчику не подходит, есть возможность приобрести специальный программно-аппаратный комплекс для защиты от DDoS. Однако высокая стоимость таких устройств — как правило, не менее нескольких десятков тысяч $ — значительно сужает круг потенциальных покупателей, в качестве которых выступают, как правило, крупные коммерческие компании, важные госструктуры, операторы связи, хостинг-провайдеры и т.д. По данным упомянутого отчета IDC, мировой рынок таких систем в 2015 году составил почти $365 млн. В общем случае решение представляет собой производительный x86-сервер с мощной сетевой подсистемой и набором специального фирменного ПО, использование которого оплачивается по лицензии. Наиболее известными производителями сегодня являются такие бренды, как Arbor, Fortinet, Juniper, CheckPoint, Radware, но есть и немало других.

Компания ***Arbor Networks*** (входящая в состав холдинга NetScout Systems) развивает несколько семейств систем защиты от DDoS. Решения самого высокого класса, предназначенные для дата-центров, получили наименование Pravail. Семейство автономных систем TMS включает несколько моделей производительностью от 1,5 Гбит/с до 100 Гбит/с и ориентировано на крупных корпоративных пользователей и операторов. Серия APS — это гибридное решение на базе аппаратного x86-сервера, работающего в сочетании с ресурсами фирменного «облака» Arbor (**рис. 2**).

Система обеспечивает защиту от атак интенсивностью до 40 Гбит/с. В семействе APS еще есть чисто программный модуль, устанавливаемый на сервер в среде Hyper-V, позволяющий ликвидировать атаки до 1 Гбит/с.

Серия систем ***Fortinet*** для защиты от DDoS получила название FortiDDoS и включает в себя несколько моделей с различным диапазоном возможностей (**рис. 3**).

Рис 2. Комплексная система защиты от DDoS-атак Arbor APS

Рис 3. Аппаратно-программная система защиты от DDoS-атак Fortinet FortiDDoS 2000B

Так, младшая из них — 200B — рассчитана на атаку интенсивностью до 4 Гбит/с, а старшая — 2000B — должна эффективно справляться с 16 Гбит/с балластного трафика.

Имеются подобные решения и у ***CheckPoint***, они поставляются на рынок под названием DDoS Protector. Серия включает в себя десять моделей, которые обеспечивают фильтрацию трафика на скоростях от 500 Мбит/с до 40 Гбит/с.

Что касается ***Radware***, то эта компания предлагает сегодня одни из наиболее производительных решений на рынке. Серия устройств DefencePro, в зависимости от модели, нивелирует атаки интенсивностью от 200 Мбит/с до 160 Гбит/с. Также у компании есть собственное «облако», предоставляющее услуги защиты от DDoS (сервисы Radware DDoS Attack Mitigation Service, DefensePipe, DefenseFlow). Семейство решений для защиты от угроз типа «отказ в обслуживании» есть и у ***Juniper Networks***, называется оно DDoS Secure и представляет собой программный пакет, устанавливаемый на аппаратный x-86 сервер.

В общем, выбор средств защиты не менее обширен, чем ландшафт угроз, но при этом атакуемые все равно находятся сегодня в заведомо худшем положении, чем нападающие. Провести DDoS-атаку можно легко, просто, относительно недорого и, главное, полностью анонимно (редкие случаи выявления преступников — скорее исключение). Защититься от «шторма» тоже можно, но для этого уже надо пораскинуть мозгами и ощутимо раскошелиться. Но выбора сейчас особо нет — число DDoS-атак постоянно и быстро увеличивается. Так что о методах защиты необходимо думать уже сейчас, ну или воспринимать проблему философски и надеяться, что пронесет.

Игорь КИРИЛЛОВ, СиБ