УДК 00.004

Алексеев П.А., студент 1 курса,
факультет информационных технологий,
Брянский государственный технический университет,
г. Брянск, Россия

КАК DDOS -АТАКИ РАЗВИВАЮТ ИНТЕРНЕТ

Аннотация. *В статье рассказывается об DDOS атаках и их последствиях, методах защиты и история развития данного явления.*

Ключевые слова: *DDoS — атака, меры защиты, последствия для владельца сайта.*

Annotation. *The article describes DDOS attacks and their consequences, methods of protection and the history of the development of this phenomenon.*

Keywords: *DDoS - attack, protection measures, consequences for the site owner.*

Как DDOS-атаки развивают интернет

DDoS (сокращение от Distributed Denial of Service – распределенный отказ в обслуживании) – попытка нарушения нормального трафика сервера/службы/сети посредством подавления цели перегрузкой потока интернет-трафика. То есть фактически это хакерская атака на компьютерную систему с целью создать такие условия, при которых системные пользователи не смогут получить доступ к предоставленным ресурсам, либо он окажется сильно затруднён. Такой тип атаки похож на схожую и широко встречающуюся угрозу для веб-сервисов – «Отказ в обслуживании» (Denial of Service). Разница лишь в том, что обычное распределенное нападение поступает из одного места, а DDoS-атака по объему более масштабна и исходит из различных источников.

Существует мнение о том, что DDoS-атаку способен провести даже обычный пользователь. Это не совсем верно. Дело в том, что еще несколько лет назад простейшая атака могла исполняться посредством многократного зажатия клавиатурной клавиши F5. Она с быстрой скоростью обновляла интернет-страницу браузера, которая позиционировалась как цель. Ввиду этого сайт мог получить высокую нагрузку трафика и временно выйти из строя. На данный момент затруднительно представить ситуацию, когда злоумышленник один организует DDoS-атаку. В большинстве случаев он использует сеть из компьютеров, которые заражаются специальным вирусом, который должен обеспечить удаленно необходимый доступ к зараженному компьютеру. Как правило, в сети подобных компьютеров существует координирующий сервер. При реализации атаки хакер дает команду этому серверу, который передает соответствующий сигнал каждому боту на выполнение сетевых запросов вредоносного характера.

Главная проблема при смягчении DDoS-атаки заключается в необходимости различить спланированную атаку от потока стандартного трафика. Если сайт какой-то компании при выпуске новинки окажется завален многочисленными клиентами, то полное отключение трафика будет ошибочной мерой. Но если у этой компании внезапно возникнет отчетливо наблюдаемый всплеск трафика, то, скорее всего, необходимо предпринять усилия для смягчения атаки. Отличить посещения реальных клиентов от трафика атаки практически невозможно. В сети Интернет DDoS-трафик может поступать в нескольких вариантах, варьируясь от незамеченных атак с использованием одного источника до сложных многовекторных атак.

Стандартными целями DDoS-атак являются сайты интернет-магазинов, государственных учреждений, и организаций, чья работа основывается на предоставлении услуг в режиме online (например, онлайн-казино). Многие коммерческие организации затрачивают большие средства на обеспечение защиты своих Интернет-сайтов от DDoS-атак. Они вынуждены это делать, так как даже короткий промежуток простоя часто посещаемого сайта может

принести компании большие экономические потери. Услуги по защите от подобных атак довольно дороги, однако их применение в современных условиях оправдано. Помимо подрыва работоспособности ресурсов организации или компании DDoS-атаки могут проводиться как повод для вымогательства. Некоторые компании предпочли бы выплатить денежную сумму во избежание нападения вместо реализации угрозы стабильности их бизнеса.

DDoS-атаки появились в поле зрения общественности в 1999 году, когда случилась целая серия атак на сайты крупных западных компаний (CNN, eBay, Yahoo). В 2000-е гг. подобная преступная деятельность обрела большую популярность. Компания Spamhaus в 2013 году подверглась мощной атаке, сила которой составляла около 300 Гбит/с. Для атаки на компанию злоумышленники применяли DNS-сервера из сети Интернет, которые на тот момент были загружены огромным количеством запросов. В тот день многие миллионы пользователей жаловались на медленную загрузку интернет-страниц из-за перегруженности DNS службы. К настоящему времени данная разновидность киберпреступности стала угрозой глобального масштаба, несмотря на расследования полиции и ряд технических и программных новшеств, применяемых для противодействия DDoS-атакам. По данным специалистов в области информационной безопасности, за последние годы их частотность выросла в два с половиной раза, а пиковая мощность превысила 1 Тбит/сек.

Существует несколько мер, благодаря которым возможно обеспечить защиту от DDoS-атак на весьма высоком уровне. Сначала необходимо точно настроить межсетевой экран, после чего будет возможно следить за подозрительным трафиком, который поступает с других устройств. Фиксирование сетевого трафика также способствует обеспечению защиты от DDoS. Заинтересованных в ней должны настораживать резкие всплески сетевой активности, что может быть одним из признаков осуществления атаки. Также защита от этого явления предполагает систематический мониторинг

состояния компьютерных сетей, так как злоумышленники могут в любой момент времени присоединиться к ним через специальные каналы. Если это случится, то тогда сеть будет заражена зловредным приложением. Попытки ограничения общего трафика или смягчения могут приостановить поток не только «плохого», но и «хорошего» трафика. Нельзя забывать, что атака также имеет возможность адаптации к принимаемым контрмерам. Для того, чтобы остановить или хотя бы максимально смягчить атаку, системный подход будет наиболее эффективным решением.

DDoS - attack, protection measures, consequences for the site ownerПоследствия успешных DDoS-атак могут значительно варьироваться: от отключения сервера дата-центром до полной потери потока клиентов и утраты репутации, что в дальнейшем может привести к потере доверия со стороны партнеров или инвесторов. Многие организации стараются сэкономить и назначают недостаточно порядочных провайдеров защиты, которые не обеспечивают необходимый уровень безопасности. Во избежание таких проблем следует пользоваться услугами надежных и проверенных специалистов.

Как ни странно, изначально DDoS - атака имела положительное значение, так как её проводили для тестирования надёжности каналов связи и выявления возможных проблем в устойчивости систем. С тех пор многое изменилось, и обеспечение защиты от подобных атак обрело очень важное значение. Важно позаботиться о том, чтобы средства безопасности в случае необходимости сработали эффективно. Чтобы DDoS-атака не была полной неожиданностью и нанесла незначительный урон, необходимо постоянно совершенствовать механизмы безопасности наряду с защищаемой инфраструктурой и приложениями. Так не только будут совершенствоваться технологии обеспечения защиты, но также, хоть и вынужденно, дополнительный стимул к развитию получают сетевое оборудование и программное обеспечение.

Итак, распределенные атаки остаются большой проблемой для владельцев интернет-ресурсов по всей планете. Важно понимать, что обеспечение защиты сайта от DDoS-атак является обязательным условием для тех, кто хочет избежать потери доверия или экономических убытков. С этой целью параллельно проводится обновление информационно-технологической инфраструктуры и вводятся в действие различные новшества, приводящие к развитию сети Интернет.

Список используемых источников:

1. Miller Lawrence C. DDoS For Dummies. 2012 – СТР 64-69.
2. Сергей Жмылёв. Распределённые атаки типа DDoS-2015-СТР 34-38.