**АНАЛИЗ DDOS-АТАК И МЕТОДОВ ЗАЩИТЫ ОТ НИХ**

***Аннотация***

*В данной статье рассматриваются виды DDoS-атак, приводятся методы противодействия атакам при условие наличия комплексной системы защиты.*

**Ключевые слова:** отказ в облуживании, Ddos-атака, противодействие, защищенность, уязвимость.

**Keywords**: denial of service, Ddos attack, counteraction, security, vulnerability.

В настоящие время, очень редко, что найдется хоть одно предприятие, без разницы на её сферу деятельности, где бы ни использовались интернет технологии. Для многих предприятий отказ или трудности работы в сети приводят к огромным материальным убыткам, конкуренты и злоумышленники не упустят шанса этим воспользоваться, проводя полный спектр атак, приводящих к весьма серьезным и масштабным последствиям [1].

Например, атакам подвергаются не только интернет-магазины, веб-сайты, но и предприятия малого и среднего бизнеса, реже — персональные компьютеры отдельных физических лиц. Вследствие данных действий, как правило, нанести пострадавшему материальный вред и при этом атакующий должен остаться анонимным для избежание уголовной ответственности [2] . В единичных случаях dos и ddos-атаки являются одним из способов частного мошенничества. Если у пользователя не установлена комплексная или слабая защита от ddos-атак, то злоумышленник может полностью остановить работу системы.

Для того, чтобы представить насколько большой материальный ущерб ddos-атака может нанести предприятию, стоит подчеркнуть, что её может провести даже обычный старшеклассник. Конечно, она будет не масштабна, чаще всего крупное и даже среднее предприятие атаковать не получиться, но все осознают: чем больше развито предприятие, тем больше злоумышленников на него могут напасть.

Дословно с английского ddos- атака переводится, как «отказ в обслуживание», то есть целью такой атаки является создание некоторых условий, при которых пользователям будет частично или полностью ограничен доступ к определённой системе. Часто случается так, что ddos-атака просто инструментом для проведения дальнейших негативных действий.

Рассмотрим, чем являются ddos -атаки направленная на «отказ в обслуживании». Это злонамеренные действия, приводящие к отказу в обработке запросов или полного закрытие доступа пользователей.

Атаки на отказ в обслуживании можно условно разделить на два типа:

1. низкоуровневые (сетевой и транспортный уровни в модели OSI);
2. высокоуровневые (уровень приложений).

Первые являются, применением «грубой силы», когда огромное число ботов одновременно отправляет пакеты-запросы на один хост сервера, приводя его к «отказу в обслуживании». Во втором случае, число участников намного меньше, но пакеты-запросы имеют сложную структуру и рассчитаны на «отказ из строя» определенного рода приложения. Далее мы подробно поговорим о каждом из этих типов атак и методах борьбы с ними.

Обычно проведение ddos -атаки ограниченно лишь возможностями и фантазией мошенников, но существуют обычная квалификация по виды ddos - трафика [3] :

• HTTP-запросы- чаще всего с помощью таких запросов пользователь работает с сайтом предприятие.

• Для крупных и средних предприятий часто используются ICMP. Один из самых опасных методов, по широковещательному адресу злоумышленник отправляет поддельный ICMP-пакет, в котором адрес атакующего меняется на адрес жертвы.

В борьбе с ddos -атаками можно выделить следующие методы:

* превентивные;
* реакционные;
* пассивные и активные.

Ниже приведён краткий список основных методов защиты от ddos-атак.

**Разделение ресурсов**. Существенно помогает противостоять ddos -атакам распределение и разграничение ресурсов на различных серверах или даже разных дата-центрах. Даже при успешной ddos -атаке выйдет из строя максимум атакованный сервер. Подобным способом можно исключить отказ работы всей системы и ограничеться только частичным «отказам».

**Встречная реакция.** Существует множество предприятий, которые предлагают услуги по вычислению и противодействию ddos -атак, и обнаружение злоумышленника, чтобы привлечь их к уголовной ответственности. Так же, при необходимых вычислительных и серверных мощностях атакуемого, возможно отразить трафик назад к атакующему. Данный метод довольно непростой в применении и требует хорошей материальной основы, а также квалифицированного администратора сервера. Плюсы этого метода защиты - значительная материальная база и специалисты с обширным опытом работы в сфере информационной безопасности [4].

Таким образом, при построении локальной сети, необходимо в достаточной мере защитить все уязвимые узлы системы. В настоящее время существует большое количество методов противодействия и защиты от ddos -атакам, и не стоит пренебрегать защитой, в частности, это касается представителей малого и среднего бизнеса. Нечестные конкуренты сделают всё, чтобы вывести из строя крупного соперника получить его прибыль.

**Боты как основа ddos-атаки.** Однако с учетом мощностей современных серверов в современное время и пропускной способности каналов связи реализовать dos-атаку с одной машины вряд ли получится, такая атака легко определяется и блокируется [5]. Эффективнее использовать зараженные вредоносным кодом совокупность персональных компьютеров не в чем не подозревающих пользователей (боты, зомби), которые по команде злоумышленника будут отправлять запросы на самый уязвимый узел жертвы (предприятие), реализуя распределенные ddos-атаки «на отказ в обслуживании». Типовыми зомби чаще всего становятся домашние персональные компьютеры. Если в корпоративной среде имеется набор методов и средств для защиты персонального компьютера (например, антивирус, межсетевое экранирование и прочее), то на домашних компьютерах, как правило, некоторые из этих средств отсутствует или же практически не применяется. Создание зомби-сетей давно уже перестало быть уделом хакеров-одиночек, это бизнес, приносящий немалый доход их владельцам.

**Общие советы** Приведенные ниже способы защиты будут эффективны при атаках, в которых участвует лишь несколько десятков зомби-компьютеров. Но не стоит считать, что слабые ddos-атаки не смогут нанести ущерб серверу.

Важно, чтоб все серверы, имеющие прямой доступ к внешней сети, должны быть подготовлены к простой и быстрой перезагрузке администратором удаленно. Большим плюсом будет наличие второго, административного интерфейса, через который можно получить доступ к серверу в случае «отказа в обслуживании» основного канала. Далее все сетевые сервисы, предназначенные для административного использования, должны быть укрыты межсетевым экраном от всех, кто не имеет к ним правового доступ. Тогда атакующий не сможет использовать их для проведения ddos-атаки или подбора паролей. Так же, на ближайшем, по отношению к серверу, маршрутизаторе должна быть установлена система, анализирующая проходящий трафика, которая позволит своевременно узнать о начинающейся ddos-атаке и вовремя принять меры по ее предотвращению, например, IPS. Если компания не работает с иностранными клиентами, блокируйте доступ к сайту с нероссийских IP. И в завершение очевидное – программное обеспечение, используемое на сервере, всегда должно находиться в актуальном состоянии.

Следует отметить, что все приведенные приемы направлены на снижение эффективности ddos-атак, ставящие своей главной целью израсходовать ресурсы «железа». От флуда (спама), забивающего канал-запросы мусором, защититься практически невозможно, и единственное главное правильный, но не всегда осуществимый способ борьбы заключается в том, чтобы использовать широкий канал, порядка пару гигабита, который легко пропустит трафик среднего и не большого ботнета.

**Литература:**

1. Атаки DDoS и методы противодействия /[Электронный ресурс] – Режим доступа: http://itband.ru/2018/03/ddos/ (Дата обращения: 20.02.2020) .
2. Уголовный кодекс РФ Статьи 273 «Создание, использование и распространение вредоносных компьютерных программ» (в ред. Федерального [закона](http://www.consultant.ru/document/cons_doc_LAW_200920/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100745) от 07.12.2011 N 420-ФЗ) /[Электронный ресурс] – Режим доступа: http://www.consultant.ru/document/cons\_doc\_

LAW\_10699/a4d58c 1af8677d94b4fc8987c71b131f10476a76/ (Дата обращения: 20.02.2020).

3. DOS и DDoS-атаки: понятие, разновидности, методы выявления и защиты / [Электронный ресурс] – Режим доступа: http://compconfig.ru/net/dosi-ddos-ataki.html (Дата обращения: 20.02.2020).

4. DDoS–атаки. Причины возникновения, классификация и защита от DDoS-атак / [Электронный ресурс] – Режим доступа: http://efsol.ru/articles/ddos-attacks.html (Дата обращения: 20.02.2020).

5. Журнал «Хакер». Боевые DDoS боты и IRC/[Электронный ресурс] – Режим доступа: <https://xakep.ru/2001/08/08/13276/> (Дата обращения: 20.02.2020) .