УДК 004.056.53

DDoS-атака: классификация и особенности

Харитонов Виктор Сергеевич
Национальный исследовательский Мордовский государственный университет им. Н.П. Огарёва
студент

Черяпкин Дмитрий Павлович
Национальный исследовательский Мордовский государственный университет им. Н.П. Огарёва
студент

Аннотация
В данной статье затрагиваются проблемы хранения и обеспечения безопасности информации. Рассматриваются основные особенности и виды DDos-атак в современном мире.
Ключевые слова: DDos-атака, ICMP-флуд, SYN-флуд, DNS, CGI, информационная безопасность.

DDoS-attack: classification and characteristics

Kharitonov Viktor Sergeevich
Oragev Mordovian State University
student

Cheryapkin Dmiry Pavlovich
Oragev Mordovian State University
student

Abstract
This article addresses the problem of storage and security of information. Explains the basic features and types of DDos attacks in the modern world.
Keywords: DDoS-attack, ICMP-flood, SYN-flood, DNS, CGI, information security.

В современном мире одним из самых важных ресурсов является информация: будь-то личные данные или счета коммерческой организации, мы надеемся, что они останутся неприкосновенны. Бурное развитие техники привело к тому, что сейчас почти вся информация хранится на цифровых носителях. Это заметно облегчает и ускоряет обмен данными, ведь в электронном виде информацию хранить проще, большие объемы данных можно быстро копировать, переписывать, передавать на расстояния [1]. В связи с этим остро встает вопрос об обеспечении безопасности личных

данных. Если для частного лица утрата такой информации несет скорее моральный ущерб, то крупные финансовые компании теряют как потенциальных клиентов, так и серьезные материальные убытки. На данный момент существует много способов незаконным образом получить личную информацию о «жертве», но одним из самых распространенных является, так называемая, DDoS-атака.

В настоящее время уже трудно определить, когда была запущена первая DDoS-атака. Но чаще всего источники указывают крупномасштабный инцидент 17 августа 1999 года, когда атаке подвергся IRC сервер университета Миннесоты. Это привело к тому, что сервер университета был непригоден для использования в течении нескольких дней. В феврале 2000 года DDoS-атаки ощутили на себе такие крупные кампании как Yahoo, eBay, CNN, Amazon, ZDNet. Киберпреступники парализовали работу системы и закрыли доступ пользователей к услугам в течении нескольких часов. После того, как эффективность DDoS-атак была наглядно продемонстрирована, хакеры начали использовать их в качестве инструмента для вымогательства денег. К 2010 году скорость атак возросла до 22000 от скорости среднего интернет-пользователя. К этому времени, DDoS-атаки стали политическими. Группа Anonymous атаковала сайты глобальных платежных систем: Visa, Mastercard и Paypal. Такие агрессивные политические атаки приобрели название хактивизма.

Хактивизм — это использование компьютеров и компьютерных сетей для продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации [2]. Сегодня такие объединения, как Anonymous и LulzSec являются наиболее известными хактивистскими группами. На данный момент DDoS-атаки можно разделить на три вида:

1) атаки с насыщением полосы пропускания; 2) атаки, нагружающие ресурсы сервера; 3) атаки с помощью неправильно настроенных DNS серверов

Атаки с насыщением полосы пропускания характеризуются большим количеством обычно бессмысленных или сформированных в неправильном формате запросов, называемых «флудом» (англ. *flood* — «наводнение», «переполнение»), к компьютерной системе или сетевому оборудованию. Понятие «DDoS-атака» практически равносильно понятию «флуд», и в обиходе и тот и другой часто взаимозаменяемы. Особого распространения получили такие виды флуда как: HTTP, ICMP, UDP, SYN. ICMP-флуд — один из самых опасных видов DDoS-атак, злоумышленник использует широковещательную рассылку для проверки работающих узлов в системе, отправляя ping-запрос. Затем адрес атакующего меняется на адрес жертвы. Все узлы в сети пришлют жертве ответ на ping-запрос. Поэтому ICMP-пакет, отправленный злоумышленником через усиливающую сеть, содержащую 200 узлов, будет усилен в 200 раз [3]. Для такой атаки обычно выбирается большая сеть, чтобы у компьютера-жертвы не было никаких шансов. Стоит особо выделить SYN-флуд, который представляет большую опасность для работоспособности сети. Данный тип атаки использует TCP протокол. Когда

жертва принимает SYN-пакет через открытый порт, она должна послать в ответ SYN-ACK пакет и установить соединение. После этого инициатор посылает получателю ответ с ACK-пакетом. Данный процесс условно называется рукопожатием. Однако, во время атаки SYN-флудом рукопожатие не может быть завершено, т.к. злоумышленник не отвечает на SYN-ACK сервера-жертвы. Данное потенциальное соединение будет помещено в очередь. Из очереди оно выйдет только по истечении 75 секунд. Этим пользуются злоумышленники и отправляют сразу несколько пакетов SYN на компьютер жертвы с интервалом в 10 секунд, чтобы полностью исчерпать ресурсы системы [4].

Атаки, нагружающие ресурсы сервера, направлены на переполнение ресурсов операционной системы или приложений. При этом типе атаки используется не канал связи, а собственно сама система. Из-за того, что каждая система имеет множество ограничений по параметрам, то целью атакующего является вынудить программу превысить этот лимит. В связи с этим происходит чрезмерный расход вычислительных мощностей на сервере и он опять же перестаёт отвечать на запросы пользователей[5]. К таким атакам относят следующие виды: отправка «тяжёлых» пакетов, переполнение сервера лог-файлами, неправильно настроенная система квотирования (CGI). CGI (Common Gateway Interface) — стандарт интерфейса, используемого для связи внешней программы с веб-сервером [6]. Если хакер получит доступ к CGI, то он сможет написать скрипт, который задействует немало ресурсов сервера, таких как оперативная память и процессорное время. Такая атака в довольно короткие сроки нагрузит сервер до такой степени, что тот не сможет обрабатывать запросы от легальных пользователей.

Атаки с помощью неправильно настроенных серверов DNS особо опасны, так как без лишних усилий могут сгенерировать трафик порядка сотен Гбит/с. Атаки такого типа обычно разделяются на два вида: атаки на уязвимости в программном обеспечении на DNS-серверах и отражение DNS-запросов(DNS reflection). В первом случае, злоумышленник подменяет IP-адрес DNS-сервера домена жертвы. После чего атакуемый при запросе HTML-страницы, попадает либо в «чёрную дыру» (если IP-адрес был заменён на несуществующий), либо прямиком на сервер злоумышленника. Таким образом внутренняя сеть оказывается полностью отрезанной от внешней сети. Второй тип атаки связан с некорректной настройкой DNS-сервера. Обычно DNS-серверы сконфигурированы так, чтобы обрабатывать только запросы своих пользователей, но существует большое количество компаний, которые неправильно их сконфигурировали, так что они принимают запросы от любого пользователя интернета. DNS-запросы обычно идут по протоколу UDP, где можно легко подделать заголовок с обратным IP-адресом. Соответственно, злоумышленники направляют к плохо сконфигурированным DNS-серверам поток DNS-запросов с IP-адресом жертвы, а сервер отвечает на указанный адрес. Таким образом, генерируется трафик. Чтобы максимально усилить его, злоумышленники отправляют такие запросы, чтобы ответ на них был как можно больше по объёму: например,

запрос списка всех DNS-записей в определённой зоне. Установленные у провайдеров серверы обычно имеют большую пропускную способность, так что сгенерировать несколько сотен Гбит/с не такая сложная задача[7].

На данный момент DDoS-атаки представляют большую угрозу для онлайн-бизнеса. Постоянно развиваясь и используя все новые и новые средства взлома, а так же комбинирую уже известные типы атак (многовекторные атаки) злоумышленники способны обойти почти любую защиту. Для обеспечения безопасности необходимо следить за новинками и способами защиты в данной области. Понимание этой угрозы очень важно для разработки стратегии ИТ-безопасности организации.

Библиографический список

1. Информационная безопасность в современном мире // deHack. [Электронный ресурс]. Режим доступа: http://dehack.ru/arts/informatsionnaja_bezopasnost_v_sovremennom_mire/ (дата обращения: 12.12.2016).
2. Krapp P. Terror and Play, or What was Hacktivism? // Grey Room. 2005. №21. С. 70-93.
3. DDoS великий и ужасный // Хабрахабр. (29.08.2014). [Электронный ресурс]. Режим доступа: https://habrahabr.ru/company/ua-hosting/blog/233903/ (дата обращения: 12.12.2016).
4. DoS-атака // Wikipedia. — (09.11.2016). [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0 (дата обращения: 13.11.2016).
5. DDoS – атака. Основные виды // Defence Laboratoty. (26.03.2013). [Электронный ресурс]. Режим доступа: http://deflab.ru/blog/DDoS-i-zashita-ot-nego/ddos-ataka-vidi.html (дата обращения: 12.12.2016).
6. CGI // Wikipedia. (27.07.2016). [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/CGI (дата обращения: 13.11.2016).
7. Ализар А. DDoS-атака 65 Гбит/с через открытые DNS-резолверы // Xakep. (18.09.2012). [Электронный ресурс]. Режим доступа: https://xakep.ru/2012/09/18/59335/ (дата обращения: 12.12.2016).