resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/perechen-personalnyh-dannyh-podlezhashchih-zashchite/zaschita-personalnykh-dannykh-v-internete/.

Ключові слова: фішинг, шахрайство, фішингові сайти.
Ключевые слова: фишинг, мошенничество, фишинговые сайты.
Keywords: phishing, fraud, phishing sites.

Науковій керівник: *к.т.н., Бойко В. Д.*

Ревацкий Александр Алексеевич
Национальный университет «Одесская юридическая академия»,
студент 3-го курсу, факультета кибербезопасности
и информационных технологий

DOS/DDOS-АТАКА

Dos-атака *(Denial of Service* «отказ в обслуживании»*)* – это атака осуществлена хакерами на центральный сервер с целью довести его до отказа. Также существует **DDoS-атака** (*Distributed Denial of Service* «распределенный отказ в обслуживании») – данная атака выполняется посредством нескольких компьютеров, это могут быть сообщники, боты или даже девайсы людей, которые даже не подозревают что они, являются участником данной атаки. Также многие предпочитают этот вид атаки, чтобы было сложнее отследить атаку обратно к её источнику, так как она поступает с нескольких точек. Приведу пример на библиотеке:

Библиотекарь может помочь найти книгу за 5 минут только 1 клиенту, но если к нему обратятся еще 5 клиентов, тогда им придётся ждать. Если обратятся еще около 20 клиентов, то будет давление и он может ошибаться в выдаче книг и недовольные клиенты из-за ожидания, могут просто уйти в другую библиотеку. А библиотекарь потеряет клиентов.

Хакерам проще организовать DDoS-атаку на систему, чем заполучить полный доступ к системе. Существуют множества мотивов для организации такого вида преступления:

1. Личные причины: достаточно часто атаки происходят на государственные организации или корпорации. В конце 20 века хакеры атаковали веб-узлы FBI, произошло данное событие благодаря недавнему рейду FBI на киберпреступников.

2. Конкуренция: тип таких атак обычно делают на заказ недобросовестные конкуренты компании, чтобы их конкурент потерял деньги и клиентов.

3. Развлечение: начинающие хакеры пробуя себя в это ремесле, атакуют любую организацию, а потом смотрят на площади разрушений своей работы.

4. Выкуп или шантаж: довольно часто перед запуском атаки, хакеры связываются с владельцами и требуют выкуп.

5. Политический протест: иногда через эту атаку хакеры показывают свое несогласие с какими-либо политическим решением.

Первые атаки в истории начали фиксироваться в 1999 году, тогда хакеры атаковали крупные торговые площадки Amazon и eBay.

За последние годы частота атак выросла в 2.5 раза, а запредельная мощность выросла до 1 Тбит/сек.

Минимально время такой атаки может составлять несколько минут, а максимальное которое было зафиксировано около 300 часов. Но есть сведения, что была такая атака, что длилась около месяца.

Потенциальные жертвы атаки:

Государственные корпорации и крупные компании;

Медицинские заведения;

Платежные системы;

СМИ;

Интернет-магазины и разные предприятия;

Биржы криптовалюты;

Онлайн-игры.

Механизм работы DDos-атаки

У каждого сервера есть предел запросов, которые он может обслуживать одновременно. Также предусмотрен предел пропускной способности канала, соединяющий сеть и сервер. Для обхода ограничения, преступник создает компьютеру сеть с встроенным вредоносным ПО, называемую «зомби-есть». Для создания такой сети, преступник делает рассылку(закидывает троян) на почту, в разные мессенджеры. Девайсы, пришедшие в данную сеть не имеют никакой связи между собой. Их цель, только выполнять все задания хакера.

Когда хакер начинает атаку, он отправляет команды захвачены вирусом компьютерам, а те оказывают содействие хакеру. Так генерируется колоссальный объем трафика, который способный «положить» сервер.

Признаки атаки

Обнаружить атаку можно только, после того как хакер добьётся своего, это можно понять по некорректной работе сервера или размещенного контента. Также существует пару признаков, благодаря ним можно выявить данное нападение:

ПО и ОС начинают часто тормозить и сбоить, то есть виснуть, некорректно завершать свою работу;

Огромное получение пакетов с одного или нескольких рядов портов;

Постоянно дублирование одного и того же действия;

Резко возросла нагрузка на сервер, которая отличается от обыденных показателей за день.

По каким критериям делятся DDos-атаки

Они делятся на 3 вида: TCP, UDP и другие. Они являются основными протоколами, которые эксплуатируются для передачи информации в сети интернете, благодаря их уязвимостям хакеры делают атаки. В зарубежных компаниях делят на 5 видов: HTTP, TCP, UDP, ICMP, прочие.

Данное деление типов дает возможность обнаружить, какие именно протоколы более уязвимы к таким нападениям, а какие нет. Также дает возможность исправлять баги защиты, а также создавать новые методы защиты.

По классификации на модели OSI(на которые происходит DDoS-атаки):

2-й уровень – канальный;

3-й – сетевой;

4-й – транспортный;

7-й – прикладной.

По механизму действия. Делятся на 3 блока:

1-й блок-является флуд, то есть создается сильный поток запросов, который забивает весь трафик жертве, к данной группе относятся: *DNS амплификация, фрагментированный UDP флуд, ICMP флуд, NTP флуд, Ping флуд, UDP флуд, UDP флуд с помощью ботнета, VoIP флуд, Фрагментированный ICMP флуд, DNS флуд*.

2-й блок-является атака при которой происходит отказ в обслуживании, то есть использующие уязвимости стека сетевых протоколов: *SYN флуд (SYN Flood), IP null атака, TCP null атака, TCP null / IP null атака, Ping смерти, Атака поддельными TCP сессиями, ACK/PUSH ACK флуд, SYN-ACK флуд, RST/FIN флуд, ACK/PUSH ACK флуд, Атаки с модификацией поля TOS, Атака поддельными TCP сессиями с несколькими ACK.*

3-й блок-является атака на прикладной уровень OSI: *HTTP флуд, Атака с целью отказа приложения, HTTP флуд одиночными запросами, Атака фрагментированными HTTP пакетами, HTTP флуд одиночными сессиями, Сессионная атака. Атака медленными сессиями.*

Как избежать такого вида нападения

Чтобы тебя не застала врасплох DDoS-атака, нужно внимательно и тщательно подготовить свои системы, а именно:

Сервера, обладающие непосредственный допуск во внешнюю сеть, обязаны быть готовые к обычному также стремительному удаленному ребуту. Огромным плюсом станет присутствие 2-го сетевого интерфейса, посредством него возможно приобрести допуск к серверу, если главный канал будет недееспособен.

Программное обеспечение, применяемое на сервере, всё время обязано пребывать в дееспособном состоянии.

Абсолютно все дыры обязаны быть пропатчены, а также обязаны быть установлены последние обновления. Это даст возможность сдержать Dos-атаки, эксплуатирующих баги на сервисах.

Все сетевые сервисы, назначенные с целью административного применения, обязаны быть скрыты brandmouer от абсолютно всех недоброжелателей. В таком случае атакующий никак не сумеет применять их с целью выполнения Dos-атаки либо bruteforce.

На подходе к серверу обязана быть система слежения за трафиком, чтобы отследить любую начинающиеся атаку на систему, а также принять меры её предотвращения.

Спиок використаних джерел:

1. Классификация DDoS-атак; краткий обзор современных технологий: Режим доступа: http://surl.li/hhmc
2. Атака сетевых зомби: Режим доступа: http://surl.li/hhme

Ключевые слова: Кибербезопасность, Атака, Взлом, Афера.
Ключові слова: Кібербезпека, Атака, Злом, Афера.
Keywords: Cybersecurity, Attack, Breaking, Scam.

***Науковий керівник**: к.т.н., доцент Бойко В. Д.*

Лоза Илья Олегович
Национальный университет «Одесская юридическая академия»,
студент 2-го курса факультета кибербезопасности
и информационных технологий

КАРДИНГ

С момента появления пластиковых банковских карт жизнь людей стала в разы проще. Больше не нужно ходить за зарплатой к «начальству», думать где хранить свои денежные средства, а также удобное осуществление покупок. Но преступники не дремлют, и они также начали активно использовать эти возможности в своих не совсем законных целях. А именно