DDOS-АТАКИ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ

Мухаммаджонов Мухаммаддиёр Маъмуржон угли
Курсант Университета общественной безопасности
Республики Узбекистана
Мухаммаджонов Орифхон Маъмуржон угли
Слушатель Московского Университета
МВД имени В.Я.Кикотя

ARTICLE INFO

Qabul qilindi: 10- November 2023 yil
Ma’qullandi: 14- November 2023 yil
Nashr qilindi: 18-November 2023 yil

KEY WORDS

Хакер, Зомби-устройства, DDoS, HTTP , UDP, TCP.

ABSTRACT

В статье рассматривается технологии и инструменты, используемых для реализации DDoS-атак, а также современных методов исследования и защиты от таких атак..

Оружием хакеров раньше являлись в основном компьютеры, в наше время в век цифровых технологий в их арсенал входят все устройства подключенный к сети интернет что облегчило сбор устройств: компьютеры, ноутбуки, смарт часы, планшеты, мультиварки, Яндекс станции и всё что входит в умный дом и даже видео регистраторы.

Все эти устройства можно назвать (зомби-устройствами) так как они не целенаправленно и не знай того выполняют команды руководителя прям как зомби.

Таким образом, хакер собирает целую зомби-сеть заражая устройства и в нужный момент направляет их по определённой цели перегружая сервис.

Непосредственно весь арсенал находится на серверах для их хранения, сами сервера бывают двух видов физические и облачные, физические сервера работают с не большим преимуществом нежели облачные.

Мощность атаки зависит от количества серверов так как на один сервер вмешается определённое количество устройств.

Заражение осуществляются с помощью захвата хостов устройства будущего зомби либо перехватом главного управления методом перебора паролей (брутфорс). Главной виной этого является уязвимости устройств, не знание пользователей и пробоины в самих устройствах.

DDoS атака на минималках можно так назвать, используя стрессоры. Стрессорами в основном пользуются новички, которые ещё ничего особо не знают и не имеют больших вложений. Сами стрессоры это (сайт) к которому подключены сервера. Затем нужно пройти авторизацию после чего покупается подходящий доступ от этого зависти мощность атаки, производимый на объект затем вбивается ссылка, выбирается метод атаки и запускается. При выборе атак с стрессора доступны такие

методы как HTTP уровень 7, UDP TCP 4 уровень. Как говорилось выше данный метод для новичков, а самым наивысшим уровнем является (Botnet) но его содержание обходится не за малые деньги: во-первых необходимы определённые умения настройки ботнета, во-вторых нужно покупать так как никто бесплатно не будет делится, в-третьих необходимы сервера для размещения плюс нужно найти сервера которые не будут банить, а так же установки на файл криптованный для заражения устройств[1].

Не просто так делают обновление это проводится со временем выявления слабостей в система.

Одна из целей DDoS-атака является коммерческая:

- Личная выгода (получить выкуп) — вывести из строя систему и в последствии потребовать деньги за прекращение атаки либо атака будет продолжатся что может отрицательно повлиять как и на клиентскую базу так и на прибыль.
- В случае конкуренции для временного ликвидирования соперника. Например, вывести из строя сайт в момент сезона продаж кога тот или иной товар востребован, таким способом перебить клиентскую базу у конкурента.

Бывают и иные причины атак:

- геополитические;
- просто ради развлечения;
- ради «хакерской» практики;
- из «обиды» на какой-либо сайт, сервис или бренд.

Какой бы не являлась причина DDoS-атака в конечном итоге выходит одно выход из строя и обрушение сайта. Методы недопустимости сайта могут быть таких видов, например:

1. Заполнение вашего сетевого канала паразитным трафиком: запросами ботов и ненужными пакетами.
2. Утилизация ресурсов: ваш веб-сервер или СУБД оказывается перегружен обработкой запросов ботов и не выдаст реальным клиентам необходимую информацию.

Кроме недоступности сервиса есть и другие последствия DDoS-атак:

– Если вы используете облачный сервер, это может быть связано с финансовыми затратами, поскольку трафик оплачивается.

– Если активны не более двух ваших сайтов, поисковые боты будут понижать вас в рейтинге. Вам необходимо будет восстановить свой высокий рейтинг в поисковых системах.

– Как уже упоминалось выше, после восстановления активности сервиса клиенты перестанут вам доверять и могут уйти к вашим конкурентам, что и нужно вашим конкурентам.

– IT-инфраструктура, вовлеченная в ddos-атаки, часто ведет себя некорректно. Например, она отображает пользователям внутреннюю информацию о СУБД, к которой они не могут подключиться. В некоторых случаях ошибки подключения к базе данных сохраняются даже после устранения последствий ddos-атаки.

Существует несколько типов DDoS-атак, с примерами по уровням модели OSI.

Низкоуровневые, которые происходят на уровнях 3-4 модели OSI, т.е. непосредственно затрагивают сетевые и транспортные протоколы:

– Сетевой уровень (3): DDoS-атаки с использованием протоколов IPv4, IPv6, ICMP, IGMP, IPsec, RIP и OSPF. Целью этих атак является само сетевое оборудование.

– Транспортный уровень (4): атаки по протоколам TCP и UDP.

Объектами этих атак являются конечные серверы и некоторые интернет-сервисы.

Такие атаки можно считать самыми распространёнными. В последствии атака не данный уровень приведёт к нарушение работы сетевого оборудования из-за превышения допустимых подключений.

Например, протокол UDP, работающий поверх IP, знает, что информация отправляется в виде дейтаграмм и что заголовки пакетов не содержат IP источника или назначения UDP доверяет адресации протокола IP, работающего поверх него, и протокол IP имеет эти заголовки но не проверяются. Поэтому большинство атак будет основано на изменении одного из IP-адресов (обычно IP-адреса источника). Это известно как спуфинг и является атакой, которая подменяет данные одного из узлов.

Этот тип атаки характеризуется нагрузкой на определенные части инфраструктуры, засорением канала мусором или заполнением таблицы обслуживания.

Высокоуровневые. Он основан на уровень приложения 7, и воздействуют по прикладным протоколам, например, HTTP. Цели таких атак — конечные серверы и сервисы.

Существует много разновидностей DDoS-атак в зависимости от того, что конкретно интересует атакующего[2]. Приведу пример самых распространённых.

Так мы предлагаем проанализировать атаку UDP Flood. Сетевая атака, действующая в бес сеансовом режиме протокола UDP, отправка большого количества UDP-пакетов на порты, их можно определить обнаружив слабые места. В данном протоколе отсутствует система предотвращения перегрузок из-за этого вирусный трафик в короткий временной промежуток захватит всю активную полосу в следствии чего полезному трафику просто не останется места. Ещё одна фишка данного метода подмена IP-адреса, после чего хакер перенаправит поток ICMP-ответов и сохранит активность атакующих хостов и обеспечит анонимность.

МЕТОДЫ ПРЕДОТВРАШЕНИЯ И ЗАЩИТЫ ОТ DDoS-АТАК

1. В целях обословления методов предотвращения и зашиты DDoS атак необходимо проанализировать среду общего анализа инфраструктуры. Сначала разберитесь, что у вас есть, где вы это размещаете, как вы распределяете оружие и какие службы и серверы используете.

2. Определите, какие части вашей инфраструктуры должны быть доступны извне, а какие должны быть закрыты. Например, РСУБД должна быть недоступна извне. Используйте брандмауэры для ограничения доступа и измените порты по сравнению с теми, которые используются по умолчанию, чтобы у злоумышленников не было мяса для разбора.

3. убедитесь, что IP-адреса инфраструктуры не скомпрометированы. Даже если атаки на основные службы отражены, другие элементы инфраструктуры могут стать объектами атак.

Дальше, минимизация зоны атаки

1. настройте параметры сервера брандмауэра. Ни в коем случае не оставляйте настройки по умолчанию. Важно закрыть все адреса и сети, кроме доверенных.

2. также скройте все реальные IP-адреса служб. Это также следует сделать, регулярно меняя их.

3. рекомендуется исключить незашифрованный трафик: перестать использовать HTTP и использовать HTTPS. Это важно не только для вашей собственной безопасности, но и для защиты от DDoS. Это необходимо для того, чтобы злоумышленник мог завладеть вашими пакетами, понять, как вы их формируете, и иметь возможность подделать их в дальнейшем.

4. Затем проверьте свою бизнес-логику и поймите, как и куда легитимные клиенты должны делать запросы. Затем вы узнаете, как отделить легитимных клиентов от нелегитимных.

5. Если на физическом сервере размещена другая служба, вам необходимо разграничить их по ресурсам. Это необходимо для того, чтобы не допустить, чтобы отключенная служба перетянула на себя все ресурсы и повредила другую службу, создав эффект якоря.

Таким образом, можно отметить, что данные атаки являются одними из самых распространенных и опасных в мире кибербезопасности. Они могут нанести серьезный ущерб как отдельным пользователям, так и организациям различного уровня.

Для защиты от DDOS-атак необходимо принять комплекс мер. В первую очередь, это может быть использование специальных средств защиты, таких как профилактические меры, сетевые экранные брандмауэры и технологии обнаружения атак.

Кроме того, важно также обеспечить качественную работу сетевой инфраструктуры и регулярно проводить проверки на наличие уязвимостей. Также следует заботиться о квалификации сотрудников, которые имеют дело с сетевой безопасностью, обучая их необходимым методам и технологиям защиты.

Не стоит забывать, что DDOS-атаки постоянно эволюционируют и адаптируются к новым условиям. Поэтому важно следить за новыми тенденциями и развивать соответствующие методы борьбы. В целом, только сочетание всех вышеуказанных мер позволит обеспечить надежную защиту от DDOS-атак.

В ходе изучения темы было разъяснено как проводить DDoS- атаку и методы зашиты от них. А так же причины их проведения, почему и для чего в наше время занимаются этим. DDoS-атаки являются серьезной угрозой для безопасности интернет сервисов начиная от простых магазинов заканчивая государственными интернет сервисами.

Это атака основана на переполнений запросами памяти того или иного сервера с целью вывести из строя всю работоспособность. Когда человек заходит на веб-сайт и нажимает на вкладку, происходит запрос к серверу. Хостинг-провайдеру, которому принадлежит этот сервер, требуется определенный объем памяти для обработки

каждого запроса и предоставления пользователю необходимой информации. И в зависимости от метода атаки заполняются определённые части памяти, в случае их переполнения сайт как и любой механизм не выдерживает и выходит из строя.

Литература:

1.Махмудов Р. М., Ибрахимов А. Р. ҲАРБИЙ ХИЗМАТЧИ ВА ОФИЦЕРЛАРНИ БОШҚАРУВ ФАОЛИЯТИНИНГ МАЗМУНИ ВА МОҲИЯТИ //PEDAGOGS jurnali. – 2022. – Т. 19. – №. 1. – С. 143-146.

2.Махмудов Р. М., Хайдаров И. О. АХБОРОТ–ПСИХОЛОГИК ХАВФСИЗЛИКНИНГ ШАХСГА ТАЪСИР ЭТУВЧИ ВОСИТА ВА УСУЛЛАРИ //PEDAGOGS jurnali. – 2023. – Т. 28. – №. 1. – С. 30-33.

3. МАХМУДОВ Р. М., ЎҒЛИ Э. А. А. ЖАМОАТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШДА ҲАРБИЙ ХИЗМАТЧИЛАРНИНГ ПРОФЕССИОНАЛ БЎЛИБ ШАКЛЛАНИШИГА КАСБИЙ БУЗИЛИШНИНГ САЛБИЙ ТАЪСИРИ //Journal of new century innovations. – 2022. – Т. 13. – №. 1. – С. 18-24.

4. Muratovich M. R., Abduraxmonovich Q. A. HUQUQBUZARLIKLARNING PROFILAKTIKASI TO ‘G ‘RISIDAGI QONUN-JAMOAT TARTIBINI SAQLASHNING HUQUQIY ASOSI SIFATIDA //PEDAGOGS jurnali. – 2022. – Т. 10. – №. 1. – С. 216-225.

5. Махмудов Р. М. ҚУРОЛЛИ КУЧЛАР ТИЗИМИДА МУРАББИЙ-ҲАРБИЙ ХИЗМАТЧИ АЁЛЛАРНИ КАСБИЙ ФАОЛИЯТГА ТАЙЁРЛАШДАГИ МЕТОДИК ИШЛАРИНИНГ ЎЗИГА ҲОСЛИГИ //PEDAGOGS jurnali. – 2023. – Т. 30. – №. 1. – С. 119-122.

6. Наркулов , А. К. у. (2023). ЗНАЧИМОСТЬ ПАТРУЛИРОВАНИЯ В ОБЕСПЕЧЕНИИ ОБЩЕСТВЕННОГО ПОРЯДКА. Innovative Development in Educational Activities, 2(20), 239–243. Retrieved from https://openidea.uz/index.php/idea/article/view/1763

7.НАРКУЛОВА И. THE USE OF COMPUTER LINGUODIDACTICS IN THE PROCESS OF TEACHING THE RUSSIAN LANGUAGE //Social sciences.

8. Наркулова И. Р. К. ОБУЧАЮЩАЯ ПРОГРАММА «РУССКИЙ ЯЗЫК ДЛЯ ВОЕННЫХ ЮРИСТОВ» КАК ОДИН ИЗ КОМПОНЕНТОВ МЕДИАОБРАЗОВАНИЯ (НА ПРИМЕРЕ КУРСАНТОВ ВЫСШИХ ВОЕННЫХ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ РЕСПУБЛИКИ УЗБЕКИСТАН) //Academic research in educational sciences. – 2022. – Т. 3. – №. 3. – С. 225-233.

9. кизи Наркулова И. Р. ОСОБЕННОСТИ ОБУЧЕНИЯ РУССКОМУ ЯЗЫКУ КУРСАНТОВ-БИЛНГВОВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ //Educational Research in Universal Sciences. – 2022. – Т. 1. – №. 3. – С. 185-193.

10. Narkulova , I. R. qizi. (2023). THE METHODOLOGY OF USING SONGS IN TEACHING RUSSIAN AS A FOREIGN LANGUAGE IN HIGHER MILITARY EDUCATIONAL INSTITUTIONS. Innovative Development in Educational Activities, 2(20), 222–232. Retrieved from https://openidea.uz/index.php/idea/article/view/1761

11. Наркулова Индира Рустам кизи МЕТОДИКА ИСПОЛЬЗОВАНИЯ ПЕСЕН ПРИ ОБУЧЕНИИ РУССКОМУ ЯЗЫКУ КАК ИНОСТРАННОМУ В ВЫСШИХ ВОЕННЫХ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ // ORIENSS. 2023. №9. URL: https://cyberleninka.ru/article/n/metodika-ispolzovaniya-pesen-pri-obuchenii-russkomu-yazyku-kak-inostrannomu-v-vysshih-voennyh-obrazovatelnyh-uchrezhdeniyah (дата обращения: 15.11.2023).

12.Narkulova I. R. Verbs of perception in Russian and the ways of their teaching to cadets of higher military educational institutions //International journal of conference series on education and social sciences (Online). – 2022. – Т. 2. – №. 8.
13. Ёкубова И. Р. Формирование профессиональной компетентности тюркоязычных студентов при обучении русскому языку как иностранному (на примере авторской интерактивной программы «Русский язык для военных юристов») //II Международный конгресс «Языковая политика стран Содружества Независимых Государств (СНГ)». – 2021. – С. 207-209.
14. Наркулова И. Р. СЛОВООБРАЗОВАТЕЛЬНОЕ ВАРЬИРОВАНИЕ ЗАИМСТВОВАНИЙ (НА МАТЕРИАЛЕ СЛОВАРЯ СИ ОЖЕГОВА) //INTERNATIONAL CONFERENCES. – 2022. – Т. 1. – №. 10. – С. 7-9.
15. Астанов Ш. Ш. РОЛЬ РУССКОГО ЯЗЫКА В СОЦИАЛЬНОЙ ЖИЗНИ СТРАН СНГ //ЎЗБЕКИСТОНДА ИЛМИЙ ТАДҚИҚОТЛАР: ДАВРИЙ АНЖУМАНЛАР: 10-ҚИСМ. – С. 136.
16. Ашуров Р. Р. ОСОБЕННОСТИ ПРОФЕССИОНАЛЬНОЙ РЕЧИ ВОЕННОГО ЮРИСТА Ёриев Озодбек Ойбек ўғли //ЎЗБЕКИСТОНДА ИЛМИЙ ТАДҚИҚОТЛАР: ДАВРИЙ АНЖУМАНЛАР: 10-ҚИСМ. – С. 34.
17. АМАНБАЕВ Ж. А., НАРКУЛОВА И. Р. К. Технология организации самостоятельной работы в высших военных образовательных заведениях Республики Узбекистан //МОЛОДОЙ УЧЕНЫЙ Учредители: ООО" Издательство Молодой ученый". – 2022. – №. 23. – С. 136-139.
18. Наркулова И. Р. К. Профессионально-ориентированное обучение русскому языку курсантов юридического профиля на основе интерактивной программы //Science and Education. – 2023. – Т. 4. – №. 2. – С. 1348-1352.
19. Закирова А. О., Наркулова И. Р. Қ. Роль русского языка в работе сотрудников органов внутренних дел //Science and Education. – 2023. – Т. 4. – №. 1. – С. 737-740.
20. Наркулов А. К. У. Роль правоохранительных органов и общественных организаций в сфере обеспечения общественного порядка (на примере США) //Science and Education. – 2023. – Т. 4. – №. 2. – С. 1615-1620.