УДК 621.396:004.056

DDOS-АТАКИ ТА ЇХ ОЗНАКИ У БЕЗПРОВІДНИХ WI-FI МЕРЕЖАХ

Варейчук В. Е.
Науковий керівник – к.т.н., старший викладач Василенко Т.О.
Харківський національний університет радіоелектроніки, каф. КРіСТЗІ,
м. Харків, Україна
e-mail: viacheslav.vareichuk@nure.ua.

DDoS attacks are one of the most common and dangerous attacks on a Wi-Fi network. Protection systems against them are quite cumbersome and expensive, which only the largest corporations can afford. In order to detect a DDoS attack and not resort to full network monitoring and check all received packets, since detecting this type of attack is quite simple using signs that can be seen without using special equipment and specialized programs. The ability to use the command line and view the Internet interface of the router is enough.

Широке поширення мереж, побудованих на основі протоколу TCP/IP, призвело до розробки методів подолання захисту та появи безлічі програм, призначених для здійснення неправомірних дій у таких мережах. Останнім часом велику популярність набули ddos-атаки. Цей недорогий і ефективний спосіб використовують проти державних і корпоративних ресурсів, з різними цілями, від конкурентної боротьби і здирництва до прикриття інших вторгнень і завдання іміджевого збитку.

Dos (Denial of Service) дослівно перекладатися як відмова в обслуговуванні, ddos – розподілена відмова в обслуговуванні. Під ddos-атакою розуміється сукупність дій, що призводять до перевантаження сервера, зависання системи через помилкові запити [1].

У бездротових Wi-Fi мережах ddos-атаки можуть вражати фізичний і канальний рівні, протоколи автентифікації, вразливі місця операційної системи, а також драй-вери та програмне забезпечення.

Наприклад, для здійснення атаки на канальному рівні, зловмисник посилає службові пакети «відмова від асоціації» від MAC адреси точки доступу до клієнта і навпаки. Оскільки додаткової аутентифікації даних пакетів не потрібно, клієнт розриває поточне з'єднання з точкою доступу. На транспортному рівні ddos-атака відбувається згідно з процесом «трьохстороннього пересилання» протоколу TCP, клієнт посилає пакет із встановленим мітки SYN. У відповідь сервер повинен відповісти пакетом з міткою ASK, після чого з'єднання вважається встановленим. Принцип атаки полягає в тому, що зловмисник, посилаючи SYN-запити, переповнює на сервері (точці доступу, роутері, комп'ютері) чергу на підключення. При цьому він ігнорує SYN+ ASK пакети сервера, не надсилаючи відповідні пакети, або переробляє заголовок пакета таким чином, що SYN+ ASK у відповідь відправляється на неіснуючу адресу. У черзі на підключення з'являються так звані напіввідкриті з'єднання, що очікують підтвердження від клієнта. Під

час закінчення певного тайм-ауту ці підключення відкидаються. Завдання зловмисника полягає в тому, щоб підтримувати наповненість черги таким чином, щоб не допустити нових підключень.

Для того щоб виявити ddos-атаку не обов'язково займатися повним моніторингом мережі і перевіряти всі пакети, тому що виявити такий вид атаки досить просто використовуючи ознаки, які можна побачити не вдаючись до спеціального обладнання та спеціалізованих програм. Достатньо вміння користуватися командним рядком і переглядати інтернет-інтерфейс маршрутизатора.

До основних ознак ddos-атак можна віднести наступні:

1. *Кількість ARP-запитів*. Можна переглянути за допомогою командного рядка. Для маршрутизаторів Cisco потрібно ввести команди show arp або show ip arp. Для інших маршрутизаторів це команди «arp –a» або «arp –v». Також цю ознаку можна переглянути за допомогою інтернет-інтерфейсу. При штатній роботі мережі кількість ARP-запитів у часі залишається однаковим (вагається в невеликих межах). При ddos-атаці кількість ARP-запитів збільшується , порівняно зі звичайною кількістю.

2. *Використання пам'яті маршрутизатора*. Можна переглянути за допомогою router#show memory (лише для маршрутизаторів Cisco). У всіх інших маршрутизаторах цю ознаку можна переглянути за допомогою інтернет-інтерфейсу (не всі моделі підтримують цю функцію). При штатній роботі мережі завантаження оперативної пам'яті маршрутизатора коливається в одних і тих самих межах. При ddos-атаці значно збільшується завантаження пам'яті маршрутизатора, порівняно зі звичайною.

3. *Використання процесорного часу*. Можна переглянути за допомогою командного рядка. Для маршрутизаторів Cisco потрібно ввести команду Router # show proc cpu sort. Для решти маршрутизаторів це: «telnet IP-адреса роутера», після чого потрібно ввести логін і пароль доступу до налаштувань маршрутизатора. В результаті цих дій відобразиться таблиця, що показує завантаженість даного ресурсу. При штатній роботі мережі сумарний процесорний час коливається у мінімальних межах. При ddos-атаці значно збільшується використання процесорного часу, в порівнянні зі звичайним.

4. *Кількість записів у NAT/PAT таблиці*. Можна переглянути за допомогою командного рядка. Для маршрутизаторів Cisco це команда "Router # show ip route" або "Router # show ipv6 route", для всіх інших "show ip nat translation". При штатній роботі мережі кількість записів в NAT/PAT таблиці на всьому проміжку часу практично не змінюється. При ddos-атаці кількість записів у таблиці значно зростає, порівняно із звичайним.

Список використаних джерел:

1. İlker Özçelik, Richard Brooks. Distributed Denial of Service Attacks. Real-world Detection and Mitigation. New York, 2020. DOI: https://doi.org/10.1201/9781315213125