УДК 004.056.5:004.056.56 https://doi.org/10.30837/IYF.PCEIP.2024.135

РОЗБІР ТА АНАЛІЗ ЗАГРОЗИ ІСНУЮЧИХ ВИДІВ DDOS-АТАК

Павлов О.А.
Науковий керівник – доц. Шаповалова А.С.
Харківський національний університет радіоелектроніки,
каф. інфокомунікаційної інженерії імені В.В. Поповського,
м. Харків, Україна
e-mail: Oleksii.pavlov2@nure.ua

The evolution of Denial of Service (DoS) attacks into sophisticated Distributed Denial of Service (DDoS) threats poses a severe risk to online entities. DDoS attacks, employing botnets, aim not to breach security but to deny authorized users access to websites. These attacks can serve as a smokescreen for other malicious activities and disrupt security measures. DDoS techniques vary, including volume-based, protocol, and application layer attacks. The constant evolution of attack methodologies, from basic scripts to distributed and adaptive strategies, requires advanced monitoring and defense mechanisms. The rise of "service malware" and the expanding attack surface through IoT devices underscore the critical need for scalable defenses against diverse DDoS threats.

Denial of Service (DoS) - це тип кібератак, до якого входять атаки Distributed Denial of Service (DDoS) як підтип. Під час DDoS-атак використовується численні підключені до Інтернету машини, що разом називаються "ботнетом", для максимального навантаження на веб-сайти зловмисним трафіком. Відмінно від інших атак, цей тип атак не спрямований на окремого користувача, а ціль є саме позбавлення користувачів можливості у доступу до ресурсів певних джерел, сайтів та подібного.

Атаки типу DDoS можуть відбуватись систематично, чи проходити в невеликих обсягах. Залежно від типу та кількості трафіку, вони можуть мати як тривалий ефект, так і одноразовий сплеск системи. Головна проблема подібного типу атак в тому, що вони можуть продовжуватись доволі значну кількість часу, що може призвести до краху всієї системи без можливості відновлення. Таким чином, DDoS-атаки можуть стати серйозною проблемою для будь-якої онлайн організації.

Усі DDoS-атаки можна поділити на 3 типи:

- атаки на основи об’єму – як правило використовують велику кількість зловмисного трафіку для того, що б перенавантажити сервер або веб-сайт. За приклад можна взяти feed flood, ICMP та UDP. Об’єм подібних атак вимірюється у бітах на секунду (BPS);
- атаки на протоколи – під час подібних атак на протоколи чи мережевий рівень відправляється велика кількість пакетів до цільової мережевої інфраструктури та інструментів управління. Прикладом подібних атак є SYN

flood та Smurf DDoS. Атаки подібного типу вимірюються в пакетах на секунду (PPS);

- атаки на рівень застосунків – атаки подібного типу передбачають собою використання програмних засобів для максимальної кількості запитів, призначених для перенавантаження серверів та застосунків. Подібні атаки вимірюються в запитах на секунду (RPS).

Кожна атака відрізняється та по своєму є небезпечною для онлайн-ресурсів. Подібні атаки мають дуже потужні наслідки для цілі, на яку вони направлені. Одні з головних наслідків DDoS-атак:

- втрата даних – здебільшого, саме подібного типу атаки призводять до втрати даних цілі, без можливості відновлення.
- повільне завантаження сторінок – здебільшого швидкість завантаження на сайті залежить від доступних серверних ресурсів, які при DDoS-атаках падають до мінімуму, або взагалі перестають бути доступними, що призводить до неможливості використовувати ресурс.
- підвищення уразливості до інших атак – в багатьох випадках подібного роду атаки використовують як прикриття для більш складніших атак, це дає змогу послабити захист та пройти складні частини захисту.
- колосальні втрати – DDoS-атаки змушують сторону захисту приймати міри розгортання більших серверів, що передбачає собою дуже великі суми. Крім того, якщо не виконувати подібних дій, можливість втрати всього ресурсу стає максимальною.

DDoS-атаки зросли за останні місяці, з якістю та частотою атак. Згідно з звітом Cloudflare [2], кількість DDoS-атак у другому кварталі 2023 року збільшилася на 15% порівняно з попереднім кварталом. Середній розмір DDoS-атак також збільшився, і найбільша атака досягла рекордних 2,3 терабайти в секунду.

Найпоширенішими цілями DDoS-атак є фінансові послуги, геймінг та технологічні галузі. Проте жодна галузь не є імунною до DDoS-атак. За останні місяці DDoS-атаки також були спрямовані проти медичних установ, урядових агентств та освітніх установ.

DDoS-атаки є серйозною загрозою для онлайн-сервісів та систем. Вони можуть викликати широкий спектр проблем, від втрати прибутку і збитків репутації до юридичних наслідків та порушень безпеки даних. Впровадження ефективних стратегій запобігання та пом'якшення DDoS-атак є важливим для захисту від цих небезпечних атак.

Список використаних джерел:

1. Takehiro K. DDOS Attack: What it is, and how to stop it.: A Cybersecurity guide for 2024 / K. Takehiro, V. Hayden., 2024. – 260 с.
2. Yoachimik O. DDoS threat report for 2023 Q3 [Електронний ресурс] / O. Yoachimik, J. Pacheco // cloudflare. – 2023. – Режим доступу до ресурсу: https://blog.cloudflare.com/ddos-threat-report-2023-q3.