УДК 004.056.53:355.451]:004.7 https://doi.org/10.30837/IYF.PCEIP.2024.155

ДОСЛІДЖЕННЯ ТА АНАЛІЗ МЕХАНІЗМІВ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АТАКАМ ТИПУ DDOS НА СЕРВЕРИ

Топіха Т.Б.
Науковий керівник – ст. викладач В'юхін Д.О.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: tymofii.topikha@nure.ua

The first DDoS attacks appeared in 1996. However, this phenomenon attracted special attention in 1999, when the world's giants - Amazon, Yahoo, CNN, eBay, and E-Trade - were put out of working condition. And to take urgent measures to solve the problem began only in 2000, when again were committed impact on the servers of important companies. Also at this moment russia is using DDoS attacks to undermine the performance of important structures in Ukraine. And even though the attack has existed for more than 20 years, due to the modernization of the attack algorithm it is possible to inflict quite severe damage to the target of the attack

Атака DoS (відмова в обслуговуванні) є методом, в якому атакуючий намагається перешкодити нормальному функціонуванню системи чи сервісу, завантажуючи його надмірною кількістю запитів або шкідливими діями. DDoS (розподілена атака з відмовою в обслуговуванні) використовує багато атакуючих пристроїв для збільшення навантаження на цільовий сервер, збільшуючи ймовірність його відмови в обслуговуванні.

Призначеним для атаки можуть бути будь-які пристрої, які мають доступ до мережі Інтернет, і можуть надсилати запити, такі як комп'ютери, смартфони або побутова техніка. Проте організувати атаку з використанням великої кількості пристроїв може бути складно, тому зазвичай атакуючий використовує комп'ютери, що підкорені вірусами або іншим шкідливим програмним забезпеченням, без відома їх власників [1].

Простий трафік - це HTTP-запити. Основа запиту - HTTP-заголовок. Запитуюча сторона може використовувати стільки заголовків, скільки потрібно, надаючи їм необхідні властивості. Зловмисники, які здійснюють DDoS, можуть змінювати ці заголовки, тому їх важко розпізнати як атаку [2, 3].

HTTP(S) GET-запит - спосіб, яким дані запитуються на сервері. Цей запит може "попросити" сервер передати який-небудь файл, зображення, сторінку або скрипт для відображення у веб-браузері.

HTTP(S) GET-флуд - DDoS атака прикладного рівня (7) моделі OSI. Зловмисник відправляє потужний потік запитів на сервер для переповнення його ресурсів. У цьому випадку сервер перестає відповідати на запити реальних відвідувачів.

HTTP(S) POST-запит - метод, суть якого полягає в тому, що дані поміщаються у тіло запиту для подальшої обробки на сервері. HTTP POST-запит кодує передавану інформацію і поміщає на форму, а потім відправляє

цей вміст на сервер. Цей метод використовується, коли потрібно передавати великі обсяги даних.

HTTP(S) POST-флуд - тип DDoS-атаки, при якому кількість POST-запитів переповнюють сервер, в результаті чого він не може відповісти на них. Це призводить до аварійного зупинення сервера з наступними наслідками.

Всі перераховані запити також передаються по HTTPS, передавані дані в такому випадку шифруються. І подібний захист грає на користь хакерам. Адже, щоб виявити такий запит, сервер повинен спочатку розшифрувати його. А розшифрувати потік запитів під час такої атаки дуже складно і це створює додаткове навантаження на сервер.

ICMP-флуд (або атака Smurf). Досить небезпечний тип атаки. Хакер відправляє підроблений ICMP-пакет, в якому адреса атакуючого змінюється на адресу жертви. Усі вузли надсилають відповідь на цей пінг-запит. Для цього у більшості випадків використовують велику мережу, щоб у комп'ютера-жертви не було жодних шансів.

UDP флуд (або атака Fraggle): Цей тип атаки аналогічний ICMP флуду, проте використовуються UDP пакети. Через перевантаження пропускної здатності сервера жертви відбувається відмова в обслуговуванні.

SYN-флуд: Основою цієї атаки є запуск великої кількості одночасних TCP-з'єднань за допомогою відправлення SYN-пакета з неправильною зворотною адресою.

Відправка "важких пакетів": У цьому типі атаки зловмисник відправляє серверу пакети, які не перевантажують пропускну здатність, але витрачають його процесорний час. Це призводить до збою в системі, і користувачі не можуть отримати свої ресурси.

Для ефективного протидії атакам DDoS важливо вжити комплекс заходів. По-перше, використання захисних пристроїв і програмного забезпечення, таких як файрволи та системи виявлення вторгнень, дозволяє виявляти та блокувати шкідливий трафік. Другим важливим кроком є постійний моніторинг трафіку, щоб вчасно виявляти аномальну активність, яка може свідчити про атаку. Фільтрація трафіку на рівні мережевих пристроїв дозволяє блокувати шкідливі запити перед тим, як вони досягнуть цільового сервера.

Додатково, використання спеціалізованих служб DDoS-захисту може надати ще один рівень захисту, фільтруючи трафік на віддалених вузлах мережі. Резервні мережні канали можуть допомогти розподілити трафік у випадку атаки, що зберігає доступність сервісів. Нарешті, оптимізація програмного забезпечення та конфігурація серверів можуть зменшити вразливість до DDoS-атак шляхом оптимізації ресурсів та обмеження навантаження на сервери.

Список використаних джерел

1. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С. Аналіз сучасних методів атак на електронні ресурси органів управління // Системи озброєння і військова техніка 1 (2017): 65-68.

2. Shin D. How to defend against amplified reflection ddos attacks. URL: https://www.a10networks.com/resources/articles/how-defend-against-amplifiedreflection-ddos-attacks.

3. Виявлення DDoS атак статистичними методами / Т. А. Радівілова та ін. COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES. 2019. URL: https://openarchive.nure.ua/server/api/core/bitstreams/7b8e7f34-ca47-4632-80a2-e527f27e81c1/content.