13. Dezember 2024;
Zürich, Schweiz

ABSCHNITT 18.
INFORMATIONSTECHNOLOGIEN UND –SYSTEME

DOI 10.36074/logos-13.12.2024.052

DDOS-АТАКИ: АКТУАЛЬНІ ТЕНДЕНЦІЇ ТА ВИКЛИКИ

Жакомін Дмитро Юрійович[1]

1. здобувач вищої освіти факультету
Навчально-наукового інституту кібербезпеки та захисту інформації
Державний університет інформаційно-комунікаційних технологій, УКРАЇНА

DDoS (розподілена відмова в обслуговуванні) атака є одним з найпоширеніших і небезпечних видів кіберзагроз, які продовжують зростати в частоті та потужності. Ці атаки мають серйозні наслідки для бізнесу, зокрема фінансові втрати, шкоду репутації та можливість вимагання викупу. Останні дослідження показують значні зміни в тенденціях DDoS-атак, що вимагає від компаній активного впровадження стратегій захисту.

У першій половині 2024 року зафіксовано 445,000 DDoS-інцидентів, що на 46% більше, ніж у першій половині 2023 року. Найсильніша атака досягла 1,7 Тбіт/с, що вказує на зростання масштабів загроз [3].

Атаки з потужністю понад 300 Гбіт/с можуть призводити до серйозних збоїв в обслуговуванні. Основні сектори, що страждають від DDoS-атак, включають [3]:

- Ігрову індустрію (49% випадків)
- Технології (15%)
- Фінансові послуги (12%)
- Телекомунікації (10%)
- Електронну комерцію (7%)

В середньому, DDoS-атака коштує бізнесу близько 6,130 доларів за хвилину простою, враховуючи втрати в доходах та витрати на відновлення.

DDoS-атаки можуть завдати шкоди репутації компанії, знижуючи довіру клієнтів. Постраждалі організації часто втрачають клієнтів через недовіру до їх здатності захистити приватні дані.

Зловмисники адаптують свої методи для використання специфічних вразливостей у цільових галузях, що робить атаки більш ефективними [2].

Основні тенденції, що призводять до зростання шкоди, включають [1]:

- Ботнети: IoT-ботнети використовуються для запуску масових, об'ємних DDoS-атак, які можуть швидко перевантажити мережі.

- Атаки на прикладному рівні: Складні атаки на прикладному рівні (L7) виснажують ресурси серверів, що призводить до їх зупинки.
- Шифрування: Приблизно 90% інтернет-трафіку зараз зашифровані, і зловмисники використовують зашифрований трафік для запуску потужних SSL DDoS-атак.
- Обсяги: Переважно завдяки ботнетам, обсяги DDoS-атак продовжують зростати. Наприклад, атака Dyn у жовтні 2016 року досягла 1,2 Тбіт/с, а через три роки AWS зафіксував UDP-рефлексійний напад обсягом 2,3 Тбіт/с, що вважається найбільшою DDoS-атакою в історії.

Впровадження рішень для активного моніторингу та нейтралізації DDoS-атак є критично важливим. Використання сучасних кібербезпекових інструментів дозволяє швидко реагувати на атаки та зменшувати їх наслідки.

DDoS-атаки продовжують бути серйозним викликом для бізнесу в усіх сферах. Підвищення частоти та потужності цих атак вимагає від організацій розробки та впровадження надійних стратегій захисту, щоб зменшити фінансові та репутаційні ризики. Інвестування в безпеку є необхідним для збереження бізнес-операцій у сучасному кібернетичному середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

[1] What Is a DDoS Attack? Distributed Denial of Service. (б. д.). Cisco. https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html
[2] The Economics of DDoS Attacks and Their Prevention - Innovation in Business. (б. д.). Innovation in Business. https://www.innovationinbusiness.com/the-economics-of-ddos-attacks-and-their-prevention/
[3] DDoS Attack Trends for Q1–Q2 2024: Insights from Gcore Radar Report | Gcore. (б. д.). Gcore. https://gcore.com/blog/radar-q1-q2-2024-insights/