DOI: 10.59647/978-617-520-936-3/1

Сучасні методи захисту від DDoS-атак у мережах

Вадим Заїка, студент,[1 i] (ORCID: 0009-0008-8415-0378)

[1] *Київський національний університет будівництва і архітектури, 03037, м. Київ, проспект Повітряних Сил, 31, Україна*

АНОТАЦІЯ

У даній тезі аналізуються DDoS-атаки, їхні типи та ефективні стратегії захисту мереж. Описані основні види атак, а також методи їхнього нейтралізації, зокрема фільтрація трафіку і використання CDN. Розглянуто економічно ефективні рішення для забезпечення захисту як для великих компаній, так і для малого бізнесу. Підкреслено важливість моніторингу трафіку у реальному часі та адаптивних методів захисту для швидкого реагування на нові загрози.

Ключові слова: DDoS-атака, сервер, зловмисник, захист, IP-адреса, трафік, мережа.

1. ВСТУП

DDoS-атаки – розподілені атаки на відмову в обслуговуванні. Вони є однією з найсерйозніших загроз для сучасних комп'ютерних мереж. Їх мета полягає в тому, щоб перенавантажити мережеві ресурси, такі як сервери чи мережеве обладнання, тим самим зробивши їх недоступними для користувачів. З розвитком технологій і збільшенням кількості підключених до мережі пристроїв, DDoS-атаки стають все більш складними і руйнівними, що вимагає ефективних методів їхнього запобігання та захисту.

2. ТИПИ DDOS-АТАК

DDoS-атаки можуть мати різні форми, зокрема:

Атаки на рівні мережі (Network Layer Attacks): атакуючі надсилають великий обсяг трафіку, щоб перенавантажити мережеву інфраструктуру.

Атаки на рівні додатків (Application Layer Attacks): ці атаки спрямовані на вразливості в додатках, наприклад, через перевантаження веб-сервера запитами.

Протокольні атаки (Protocol Attacks): використання вразливостей у протоколах, таких як TCP/IP, для виснаження ресурсів мережевих пристроїв.

З розвитком технологій DDoS-атаки стають більш складними. Це вимагає постійного вдосконалення захисних систем та впровадження нових методів аналізу трафіку для виявлення загроз. Крім того, важливою задачею залишається розробка економічно ефективних рішень, які будуть доступними як для великих компаній, так і для середнього бізнесу.

3. МЕТОДИ ЗАХИСТУ ВІД DDOS-АТАК

Захист від DDoS-атак вимагає комплексного підходу, що включає кілька методів:

- Фільтрація трафіку: Використання міжмережевих екранів (фаєрволів) та систем виявлення вторгнень (IDS/IPS) для фільтрації підозрілого трафіку ще на ранніх етапах атаки. Фільтрація трафіку дозволяє визначити шкідливі пакети, характерні для DoS-атак, і запобігти їх проникненню в систему. Процес фільтрації включає ідентифікацію аномалій в мережевому трафіку, аналіз пакетів, що надходять, та відсікання трафіку, який перевищує допустимі норми або виглядає підозріло. Наприклад, ці системи можуть ідентифікувати та блокувати IP-адреси, з яких надходить підозрілий трафік, або обмежувати кількість запитів, що надходять від одного джерела. Для фільтрації трафіку використовуються такі інструменти та платформи, як брандмауери та системи запобігання вторгненням (IPS) для фільтрації трафіу на вході до мережі та блокують підозрілі запити. Також доцільним є використання розподілених мереж доставки контенту (CDN) для перерозподу запитів через географічно розподілену мережу серверів, що дозволяє зменшити навантаження на один сервер. Використання різноманітних методів та рівнів фільтрації дозволяє виявляти та запобігати атакам ще на ранніх етапах, мінімізуючи їхній вплив на інфраструктуру. Інструменти, такі як наприклад Wireshark, забезпечують глибокий аналіз трафіку, допомагаючи фахівцям у сфері безпеки швидко реагувати на потенційні загрози та забезпечувати безперебійну роботу мережевих ресурсів.
- Застосування розподілених мережевих структур: Використання Content Delivery Networks (CDN) та Anycast для розподілу трафіку по різних серверах. Це дозволяє уникнути перевантаження окремих вузлів і забезпечує стійкість до атак. Наприклад, CDN може автоматично перенаправити трафік на інші сервери, якщо один із серверів зазнає атаки.
- Автоматизовані системи виявлення DDoS-атак: икористання спеціалізованих систем, які виявляють аномальні потоки трафіку і автоматично вживають заходів для їх блокування. Такі системи можуть базуватися на алгоритмах машинного навчання для виявлення аномалій у трафіку, які можуть свідчити про DDoS-атаку.

Хмарні сервіси захисту від DDoS: икористання послуг провайдерів, що спеціалізуються на захисті від DDoS-атак, таких як Cloudflare чи Akamai. Ці сервіси використовують глобально розподілені мережі для фільтрації трафіку, запобігаючи його потраплянню на основні сервери компанії. Наприклад, Cloudflare має мережу з понад 200 дата-центрів по всьому світу, що дозволяє ефективно обробляти та блокувати шкідливий трафік.

Akamai Technologies є одним із лідерів у сфері захисту від розподілених атак на відмову в обслуговуванні (DDoS), забезпечуючи своїм клієнтам стійкість і високу продуктивність навіть під час великих атак. Захисні рішення Akamai використовуються як для захисту від DDoS, так і для підвищення надійності мереж і оптимізації доставки контенту. Унікальність платформи полягає в її потужній інфраструктурі, здатній обробляти величезні обсяги трафіку, що є важливим аспектом для запобігання атакам на мережевому рівні.

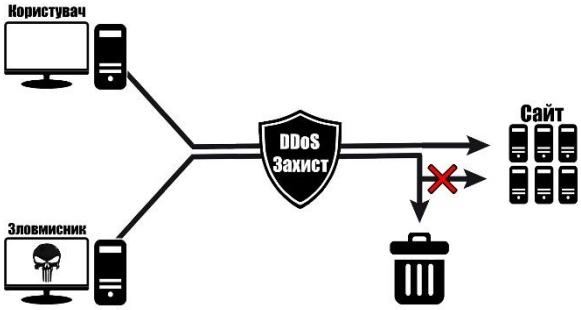

Рисунок 1. Схема захисту від DDoS-атаки

4. ЕТАПИ DDOS-АТАК

1) **Підготовка атаки**:

- **Збір ботнету**: Зловмисник спочатку створює або орендує ботнет — мережу заражених пристроїв, які контролюються з централізованого сервера управління. Ці пристрої можуть бути комп'ютерами, серверами, маршрутизаторами, або навіть мобільними телефонами. Зазвичай, власники пристроїв навіть не підозрюють, що їхній пристрій заражений і використовується для кіберзлочинів.
- **Вибір цілі**: Зловмисник обирає сервер, вебсайт або мережевий ресурс, який буде ціллю атаки. Ціль зазвичай обирається залежно від її вразливості або значущості.

2) Ініціація атаки:

Запуск атаки: Зловмисник віддає команду ботнету розпочати атаку. Це може бути організовано через централізовану систему командування та контролю (C&C), де кожен заражений пристрій починає надсилати масивний потік запитів до цільового ресурсу. Усі пристрої у ботнеті одночасно починають надсилати великі обсяги запитів, перевантажуючи ресурси цільової системи. Запити можуть бути однотипними або різними, в залежності від типу атаки.

3) **Виконання атаки**:

Перевантаження цілі: Інфраструктура цілі починає отримувати величезний обсяг трафіку. Це може бути масовий потік HTTP-запитів, SYN-пакетів або іншого типу мережевого трафіку, залежно від обраного типу DDoS-атаки. Цей трафік може споживати пропускну здатність мережі, процесорні ресурси або пам'ять сервера, що призводить до його значного уповільнення або повного виходу з ладу.

4) **Підтримка атаки**:

Збереження активності: Зловмисник може підтримувати атаку протягом декількох хвилин, годин або навіть днів, залежно від цілей і ресурсів. В деяких випадках атака може зупинятися на короткий час і відновлюватися знову для того, щоб обійти заходи захисту

5) **Завершення атаки**:

Припинення атаки: Зловмисник може припинити атаку, коли досягнуто цілі, або якщо ресурси ботнету вичерпалися. Після завершення атаки, інфраструктура цілі може залишитися нестабільною або зруйнованою, вимагаючи відновлення та аналізу.

6) **Наслідки**:

- **Втрати для цілі**: Ціль може зазнати значних фінансових втрат, втратити репутацію, а також стати вразливою для подальших атак.
- **Аналіз та відновлення**: Після завершення атаки необхідно провести ретельний аналіз логів і трафіку, щоб зрозуміти, як вона була здійснена, і розробити заходи для запобігання подібним інцидентам у майбутньому.

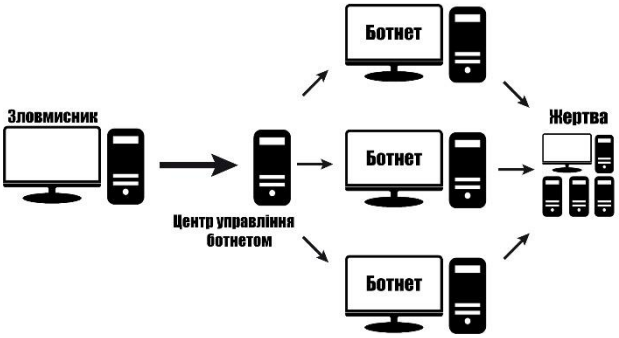

Рисунок 2. Проста схема проведення DDoS-атаки

5. ВИСНОВКИ

Отже, DDoS-атаки становлять серйозну загрозу для стабільності роботи комп'ютерних мереж, і їх ефективне виявлення та запобігання є важливим завданням для спеціалістів у галузі мережевих технологій. Комбінація різних методів захисту, таких як фільтрація трафіку, використання розподілених структур і хмарних сервісів, дозволяє значно знизити ризик і мінімізувати наслідки таких атак. Сучасні системи захисту повинні бути гнучкими, адаптивними та здатними до швидкого реагування на нові загрози. Розробка і впровадження таких рішень є важливим кроком до забезпечення безпеки комп'ютерних мереж у майбутньому.

Список літератури

[1] DoS-атака, Soltanian, Mohammad Reza Khalifeh (10 листопада 2015). URL: https://uk.wikipedia.org/wiki/DoS-атака

[2] Системи захисту від DDoS-атак, URL: https://omnilink.ua/sistemi-zahistu-vid-ddos-atak

[3] Розподілена атака на відмову в обслуговуванні (DDoS), 1992-2024 ESET, spol.s r.o URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/distributed-denial-of-service/

[4] Що таке DDoS-атака?, Microsoft, URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-ddos-attack

[i] *Робота виконана під керівництвом к. т. н., доц. Євгенії Шабали*