УДК 004.03

Віталій ГУСАК., Василь ДАРЧУК, Олена ОКОЛІТА, Ігор ІГНАТЄВ

Тернопільський кооперативний фаховий коледж

АНАЛІЗ ІСНУЮЧИХ РІШЕНЬ ЗАХИСТУ ВЕБ-САЙТ ВІД DDOS-АТАК

Вступ. DDoS-атаки є однією з серйозних та небезпечних загроз для веб-сайтів та загалом цифрової індустрії. DDoS-атаки створюються через масове перевантаження ресурсу трафіком, який надходить із численних джерел. Оскільки DDoS-атаки здатні привести до значних збитків, розробка ефективних методів для їх виявлення та запобігання є напрямком у сфері кібербезпеки [1-4].

Захист від DDoS-атак вимагає комплексного підходу, що включає як технічні, так і організаційні засоби для забезпечення стабільності роботи онлайн-ресурсів та інфраструктури в умовах сучасних кіберзагроз.

Мета: розглянути природу, принцип роботи, типи та вплив DDoS-атак**,** проаналізувати та порівняти існуючі рішеня захисту веб-сайтів від DDoS-атак, розглянути актуальні виклики і тенденції в боротьбі з цими атаками на тлі розвитку нових технологій.

1. Природа та принципи роботи DDoS-атак

DDoS (Distributed Denial of Service) атаки - це методи, спрямовані на перевантаження ресурсів цільового сервера або мережі шляхом генерації великої кількості трафіку з різних джерел. На відміну від традиційних DoS-атак, DDoS-атаки використовують ботнети - мережі заражених пристроїв, що робить атаки більш потужними та важкими для відслідковування. Це можуть бути як комп'ютери, так і інші мережеві пристрої, інфіковані шкідливим ПЗ.

Принцип роботи DDoS-атаки полягає в тому, щоб створити навантаження на сервер, яке перевищує його здатність обробляти запити. Це може призвести до відмови в обслуговуванні (DoS) легітимних користувачів. Атаки можуть бути направлені на переповнення каналу зв'язку або на виснаження ресурсів серверу через великі обсяги запитів або складні обчислення [5].

Для атак зловмисники часто використовують ботнети - мережі заражених пристроїв, які відправляють запити без відома своїх власників. Таке розподілене джерело трафіку робить DDoS-атаки важкими для виявлення та блокування. Ботнети можуть складатися з мільйонів пристроїв, що дозволяє атакувати сервери з великою потужністю.

Основні методи DDoS-атак включають flood - затоплення сервера запитами, що призводить до вичерпання його ресурсів, а також використання вразливостей мережевих протоколів для обману систем безпеки. У сучасних атаках часто використовуються аплікаційні вектори, які націлені на конкретні вебдодатки або API.

2. Різноманітні типи DDoS-атак та їх вплив на сайти та інфраструктуру

DDoS-атаки можуть мати різні типи та методи виконання. Одним з них є volumetric атаки, які перевантажують канали зв'язку великою кількістю запитів, як у випадку UDP flood або ICMP flood, що забивають доступ до серверів.

Інший тип - protocol атаки, наприклад, SYN flood, використовують вразливості мережевих протоколів, витрачаючи ресурси на обробку запитів [4].

Вплив DDoS-атак на інфраструктуру включає зниження продуктивності, втрату доступу до сервісів і фінансові збитки через зупинку роботи сайтів або онлайн-сервісів. Крім того, це може серйозно пошкодити репутацію компанії, оскільки користувачі можуть втратити довіру до ненадійних платформ.

Для захисту від таких атак використовують системи виявлення аномалій, балансування навантаження через CDN та інші спеціалізовані рішення. Регулярні оновлення інфраструктури і тестування допомагають підвищити стійкість до атак і знизити ризики.

3. Огляд існуючих алгоритмів і методів захисту від DDoS-атаки

Захист від DDoS-атак включає кілька основних підходів. Одним із найефективніших є фільтрація трафіку за допомогою алгоритмів виявлення аномалій, які дозволяють блокувати підозрілі запити та обмежувати їх швидкість, відокремлюючи шкідливий трафік від легітимного [3].

Ще одним важливим методом є балансування навантаження через CDN або Anycast, яке перенаправляє трафік на різні сервери, зменшуючи навантаження на основну інфраструктуру. Такі системи автоматично обирають найбільш доступні сервери для обробки запитів.

Для захисту від volumetric атак і SYN flood використовують анти-DDoS сервіси та фаєрволи, які фільтрують шкідливий трафік, перш ніж він потрапить на сервер. Це допомагає знизити навантаження та запобігти атакам.

4. Порівняння ефективності різних підходів до захисту

Різні підходи до захисту від DDoS-атак мають різний рівень ефективності в залежності від типу атаки та специфіки системи. Однимb із основних критеріїв порівняння є:

- швидкість реагування на атаку;
- можливість масштабування захисту;
- зручність в налаштуванні.

Швидкість реагування. Рішення на основі розподілених мереж, такі як Cloudflare і Akamai, є найбільш ефективними з точки зору швидкості реагування. Завдяки великій кількості точок присутності, ці системи здатні оперативно перенаправляти трафік і запобігати навантаженню на основний сервер.

Масштабованість. Використання розподілених мереж забезпечує значну масштабованість, оскільки атаки можуть поглинатися через численні сервери. Це особливо важливо для великих компаній, які можуть бути об'єктами дуже великих атак. Алгоритми на основі машинного навчання також можуть адаптуватися до нових типів атак, що робить їх більш масштабованими на довгостроковій основі.

Зручність у налаштуванні. Для деяких рішень, таких як Imperva Incapsula, налаштування є досить зручним завдяки інтуїтивно зрозумілому інтерфейсу. Проте, для більш складних рішень, таких як Akamai, потрібні додаткові технічні знання для правильного налаштування та моніторингу системи [1].

5. Актуальні виклики і тенденції в боротьбі з DDoS на тлі розвитку нових технологій та інфраструктури

Сучасні DDoS-атаки стають складнішими через розвиток нових технологій, зокрема Інтернету речей (IoT). Внаслідок низької безпеки багатьох IoT-пристроїв зловмисники створюють великі ботнети, що дозволяє їм здійснювати атаки з масштабними обсягами трафіку. Це збільшує навантаження на мережі та сервери і ускладнює виявлення джерел атак.

Іншим викликом є збільшення точності і спеціалізації атак, таких як application layer атаки. Замість традиційних volumetric атак, зловмисники орієнтуються на виснаження окремих компонентів інфраструктури, наприклад, вебдодатків чи баз даних, що робить такі атаки важче виявляти і нейтралізувати.

Машинне навчання та штучний інтелект активно впроваджуються для розпізнавання аномального трафіку. Ці технології дозволяють автоматично виявляти нові види атак і адаптуватися до змін у поведінці зловмисників, що значно підвищує ефективність захисту від DDoS [2].

Нарешті, з розвитком хмарних технологій та засобів для розподіленого захисту, таких як CDN і Anycast, з'являється можливість ефективно масштабувати захист від DDoS. Це дозволяє швидко обробляти великий обсяг трафіку і зменшувати навантаження на основні сервери, що робить інфраструктуру більш стійкою до атак.

Висновок. На основі проведеного аналізу можна зробити висновок, що DDoS-атаки є одними з найбільш поширених та руйнівних загроз для веб-ресурсів і онлайн-сервісів. Їх природа полягає в масованому навантаженні на сервери чи мережеві ресурси за допомогою великої кількості запитів від численних джерел, що часто здійснюється через зловмисно заражені пристрої (ботнети).

Перелік використаних джерел.

1. Kostiuk, O., Tkachuk, I. (2022). Методи і засоби захисту від DDoS-атак в умовах сучасних кіберзагроз. Київ: Наукова думка.

2. Zaitsev, M., Ivashchenko, I. (2023). DDoS Attack Mitigation Using AI-Based Techniques. Journal of Cybersecurity and Information Technologies, 8(4), 45-59. https://doi.org/10.1016/j.cybersec.2023.06.001

3. Bashirov, D., Guseva, A. (2021). Modern Approaches to DDoS Attack Detection and Prevention. Journal of Computer Science and Engineering, 12(3), 221-235. https://doi.org/10.1109/JCSSE.2021.9530845

4. Petrov, A., Kryvonos, O. (2023). Захист від DDoS-атак за допомогою машинного навчання та аналізу трафіку. Харків: ХНУРЕ.

5. Shalaginov, A., Romaniuk, V. (2022). Using Cloud-Based Solutions for DDoS Attack Mitigation. Proceedings of the International Conference on Cybersecurity, 2022, 212-218. https://doi.org/10.1109/CyberSec.2022.00054