УДК 004.056

С.В. Лазаренко, д-р техн. наук, професор,
А.Ю. Кириленко, старший викладач,
Д.І. Муха, аспірант
(Національний авіаційний університет, Україна)

Актуальність запобігання DDoS-атакам

У сучасному цифровому світі DDoS-атаки (розподілені відмови у сервісі) стали однією з основних загроз для організацій та індивідуальних користувачів, що вимагає ретельного аналізу та ефективних стратегій захисту. Проведено аналіз об'єктів та можливих уражень, що спричиняють DDoS-атаки. Досліджено кількість та потужність DDoS-атак за останні роки, а також поточний стан щодо захисту від них.

Об'єкти DDoS-атак та аналіз уражень, що спричиняють ці атаки.

Розподілені атаки типу «відмова у сервісі» (DDoS), легко запускаються, часто мають високу ефективність та є однією з найпоширеніших загроз на сучасному ландшафті кібербезпеки. Простіше кажучи, DDoS-атака має на меті порушення зв'язку з користувачами або їх обслуговування шляхом перевантаження мережі жертви величезним обсягом шахрайського трафіку, як правило, через бот-мережу рис.1 [1].

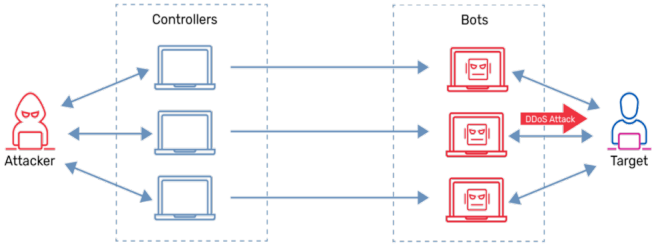

Рисунок 1. Зовнішній вигляд DDoS-атаки - порушення зв'язку з мережею жертви.

DDoS-атаки можуть бути спрямовані на різноманітні цілі, включаючи веб-сервери, мережеві інтерфейси, інфраструктуру хмарних сервісів, а також інші компоненти, що входять до складу корпоративних і приватних мереж. Цільові об'єкти атаки вибираються на основі їхньої важливості для забезпечення послуг і функціональності організації, а також на основі їх вразливостей до перевантаження.

Основними об'єктами атак виступають:

1. Веб-сервери та застосунки. Ці системи є поширеними мішенями через їх видимість та доступність з глобальної мережі «Інтернет».

2. Мережеві компоненти. Включають маршрутизатори, комутатори та балансувальники навантаження, які можуть бути залучені для розподілу шкідливого трафіку по мережі[2].

3. Інфраструктура хмарних обчислень. Хмарні платформи можуть страждати від розподілених атак, що націлені на велику кількість інстанцій, запущених користувачами[3].

Аналіз уражень, що спричиняють атаки[4]:

- надмірне використання ресурсів. Більшість DDoS-атак спрямовані на вичерпання системних ресурсів, таких як пропускна спроможність мережі, пам'ять, або процесорний час, що призводить до відмови тих чи інших сервісів;

- слабкі місця у конфігурації. Неправильно налаштовані мережі та системи можуть мати відкриті вектори атак, такі як не аутентифіковані API запити або порти, доступні для загального використання;

- використання застарілого або вразливого програмного забезпечення. Не оновлені системи можуть містити відомі уразливості, які можуть бути використані для ініціації DDoS-атак.

Аналіз цих об'єктів та вразливостей є критичним для розробки ефективних стратегій захисту, що забезпечують як превентивні заходи, так і оперативне реагування на інциденти DDoS-атак.

Актуальність реагування на DDoS-атаки.

За останні три роки кількість та потужність DDoS-атак значно зросла, що спричинено декількома факторами, включаючи розвиток технологій, поширення доступу до великої пропускної здатності та зростання кількості підключених пристроїв до глобальної мережі «Інтернет». Можливо визначити найпоширеніші типи DDoS-атак, якими є[5]:

- Volumetric Attacks;
- Protocol Attacks;
- Application Layer Attacks;
- Fragmentation Attacks;
- Amplification Attacks.

Наведемо основні тенденції та важливі інциденти з цього приводу:

1. Збільшення масштабів і складності атак:

- *рекордні показники* - з 2021 року спостерігається зріст рекордних за обсягом атак. Наприклад, у 2020 році компанія Amazon Web Services відбила атаку з піком у 2,3 Тб/с, що є однією з найбільших атак в історії;

- *мульті-векторні атаки* - сучасні DDoS-атаки часто використовують кілька векторів одночасно, що ускладнює їх виявлення та нейтралізацію. Це може включати одночасне використання великомасштабних волюметричних атак поряд з атаками на програмне забезпечення та протоколи[6].

2. Вплив на критичну інфраструктуру:

- *цілісність державних структур* - урядові сайти і системи в різних країнах стають мішенями для DDoS-атак, спрямованих на порушення або блокування роботи офіційних державних ресурсів;

- *фінансовий сектор* - банки та фінансові установи також постійно зазнають атак, що може призвести до тимчасового зупинення онлайн-послуг.

3. Зміна мотивації атак:

- політичні та ідеологічні мотиви - окрім традиційних фінансових мотивів, все частіше атаки мають політичне або соціальне підґрунтя;

- державний спонсоринг - збільшення кількості атак, за якими, як підозрюється, стоять уряди країн, що використовують кібератаки як інструмент міжнародного тиску та геополітичної боротьби.

Реакція на атаки

В першу чергу адекватна реакція на атаки залежить від розвитку технологій захисту. Потребує постійне удосконалення технологій захисту, зокрема, вдосконалення систем виявлення і запобігання вторгнень (IDS/IPS), застосування розумних алгоритмів для аналізу трафіку та автоматизації процесів реагування[7].

Важливим інструментом боротьби з кібератаками також є законодавчі ініціативи. У багатьох країнах вживаються законодавчі заходи для підвищення кібербезпеки, що включають зобов'язання компаній відповідати певним стандартам захисту даних та інфраструктури.

Останні три роки продемонстрували, що DDoS-атаки залишаються однією з найбільших кіберзагроз, а їхня складність та частота лише зростають. Це вимагає від усіх секторів економіки, особливо від критичної інфраструктури, постійно працювати над зміцненням своїх захисних систем.

Розглянемо графік потужності DDoS-атак у 2010-2020 роках, наведений на рис. 2.

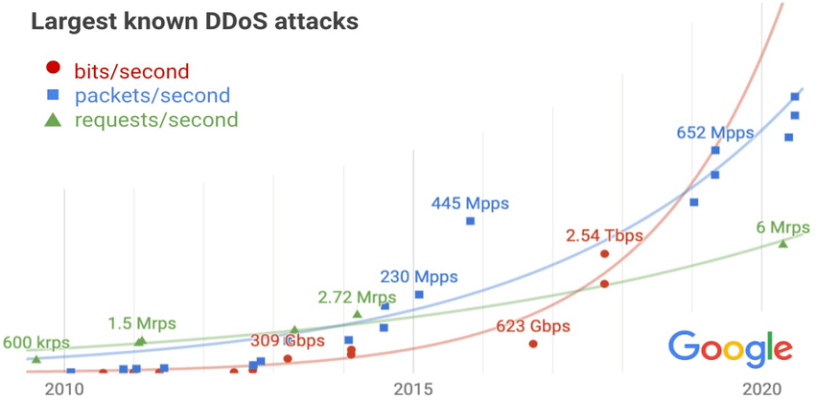

Рисунок 2. Графік потужності DDoS-атак у 2010-2020 роках.

Проаналізувавши графік можливо зазначити, що кількість та потужність атак з кожним роком збільшується. Оцінка ризиків на DDoS-атаки є ключовим компонентом стратегії кіберзахисту будь-якої організації. Цей процес включає ідентифікацію потенційних загроз, аналіз вразливостей, визначення потенційного впливу атаки та розробку стратегій для зменшення ризиків.

Таким чином, на сьогодні є актуальним своєчасне виявлення та запобігання DDoS-атакам[8].

Висновки

У роботі розглянуто поняття DDoS-атаки, проведено аналіз об’єктів та можливих уражень, що спричиняють зазначені атаки. Розуміння цих атак і розробка ефективних заходів захисту є важливими для забезпечення безпеки інформаційних ресурсів у сучасному цифровому світі.

Запобігання DDoS-атакам та захист від них вимагають комплексного підходу, що поєднує в собі передові технології, стратегічне планування, постійне навчання та міжнародне співробітництво. Враховуючи швидкі зміни в кіберпросторі, організації мають бути завжди готові до нових викликів і забезпечувати надійний захист своїх інформаційних активів.

Список літератури

1. Intelligent IT Distribution, Найкращі методи запобігання та захисту від ddos-атак. [Electronic resource] URL: https://iitd.com.ua/news/najkrashhi-metodi-zapobigannja-ta-zahistu-vid-ddos-atak.
2. Пенг Т., Лекі К., Рамамоханарао К. Огляд мережевих механізмів захисту від проблем DoS та DDoS. – Нью-Йорк, ACM Огляди з обчислювальної техніки (CSUR), 2007. № 39 (1). С. 3.
3. Бхардвадж А., Субраманіан М. DDoS-атаки та захист на мережевому рівні: Огляд. – Париж, Комп'ютерні віруси та техніка взлому. 2017. № 13(1). С. 22-53.
4. Кобб С. DDoS-атаки: еволюція, виявлення, профілактика, реакція та толерантність. – Нью-Йорк, Мережева безпека, 2012. № 6. С. 16-19.
5. Дулігеріс К., Мітрокоца А. DDoS-атаки та механізми захисту: класифікація та сучасний стан. – Амстердам, Комп'ютерні мережі, 2004. № 44(5). С. 643-666.
6. Заргар С., Джоші Дж., Тіппер Д. Огляд механізмів захисту від розподілених атак типу "відмова в обслуговуванні" (DDoS). – Піскатавей, IEEE Огляди зв'язків та навчання, 2013. № 15(4). С. 2046-2069.
7. Бхаттачарья Д., Калита Д. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance. 1 видання. – Нью-Йорк, 2016. – 312 с.
8. Ахмад І., Хабібі Лашкарі А., Масуд Р. Виявлення та зменшення впливу DDoS-атак: теорія та практика. – Лондон, Мережева безпека. 2015. № 17(3). С. 242-258.