Науковий керівник: *к.т.н., доц. Бойко В.Д.*

Ігнатенко Анастасія Ігорівна

Національний університет «Одеська юридична академія», студентка 2-го курсу факультету кібербезпеки та інформаційних технологій

ТИПИ DDoS-АТАК НА ІНТЕРНЕТ-РЕСУРСИ

DDoS-атаки проводять, коли хочуть, щоб інтернет-ресурс тимчасово перестав працювати або суттєво зменшив швидкість своєї роботи. Це популярний спосіб паралізувати роботу онлайн-бізнесу: поки інтернет-ресурс недоступний, відвідувачі будуть співпрацювати з потенційними конкурентами або чекати відновлення його нормальної роботи. В результаті бізнес втрачає прибуток, а іноді і власну репутацію.

DDoS-атаку можна порівняти із пробкою на дорогах. Коли рух перевантажений, ніхто не може рухатися швидко, але всі рухаються повільно. Теж саме відбувається і в мережі, коли інтернет-ресурс не може обробляти всі запити користувачів швидко чи взагалі зупиняє їх обробку.

Здійснення DDoS-атаки використовує велику кількість комп'ютерів, які можна орендувати або заразити шкідливим програмним забезпеченням. У останньому випадку комп'ютер користувача може ненавмисно брати участь в DDoS-атаці [1].

DDoS-атака може бути орієнтована на певні компоненти мережі. Більшість атак типу Denial of Service "відмова в обслуговуванні" націлені на наступні три рівні:

- Мережевий рівень - атаки на цьому рівні включають атаки Smurf, повені ICMP та атаки фрагментації IP/ICMP;
- Рівень передачі - атаки включають, серед іншого, SYN-флуд, UDP-флуд та атаки на TCP-порт.

- Рівень програми - атаки із шифруванням HTTP.

Різниця DDoS-атак до вимог в обслуговуванні

1. *Атаки на TCP-з'єднання*. Атака на TCP-з'єднання встановлює з'єднання із сервером, що обслуговує інтернет-ресурс, але зловмисники навмисно залишають з'єднання відкритим, а сервер може очікувати. Передбачається, що сервер зможе отримувати інші запити. Зловмисник продовжує робити аналогічні запити до сервера, перевантажуючи його і зрештою інтернет-ресурс перестає відповідати на запити будь-яких користувачів.

2. *Об'ємна атака*. Найбільш поширена атака відмови в обслуговуванні називається об'ємною атакою. Зловмисники мають намір зробити так багато одночасних запитів до серверу, використовуючи, наприклад, велику кількість ботів на заражених комп'ютерах, що сервер не може обробляти запити і зрештою відмовляє в обслуговуванні користувачів.

Цей тип атак часто реалізується, наприклад, шляхом виконання численних запитів до відкритого DNS-сервера. Передбачається, що DNS-сервер зрештою надішле надто багато даних і не зможе їх обробити.

3. *Атака фрагментацією*. Атака фрагментації використовує переваги фрагментації IP пакетів, відправляючи на сервер підроблені пакети даних, які перенавантажують сервер. Ця атака використовується в мережах передачі даних, в яких використовується технологія міжмережевого екрану на основі пакетів фільтрації.

4. *Атаки на рівні додатків.* Атаки на рівні додатків - найпростіший із типів атак. Вони виконуються рівні імітації дій користувачів, тому інтернет-ресурсу «здається», що користувачі постійно перезавантажують одну й ту ж сторінку або їх велику кількість. Ці атаки зазвичай більш ефективні та їх важче виявити [2].

Типи посилених DDoS-атак

У рамках посиленої DDoS-атаки зловмисники націлені на вразливість у DNS-серверах. Назва «посилена DDoS-атака» походить від того факту, що невеликі запити перетворюються на великі, що обмежує смугу пропускання сервера і зрештою зупиняє процеси на цільовому сервері. Існує два різних типи посилених DDoS-атак: відображення DNS та відображення CharGEN.

Відображення DNS. Атака з відображенням DNS копіює IP-адресу сервера та надсилає запити на DNS-сервер, а також запитує великі відповіді. У разі такої атаки, може йтися про відповіді, які в 70 разів перевищують нормальний розмір, що швидко завдає шкоди інтернет-ресурсу або обслуговуючому його серверу.

Відображення CharGEN. CharGEN протокол має ряд вразливостей, що надає можливість виконувати атака CharGEN Reflection, коли зловмисник відправляє на сервер безліч невеликих пакетів даних. Зрештою, зловмисник перевантажує сервер відповідями UDP, що призводить до тимчасового виходу його з робо спроможного стану [2].

Які збитки завдають атаки?

Наслідки відмови серверів в обслуговуванні інтернет-ресурсів можуть мати серйозні наслідки будь-якого суб'єкта цифрового простору. Важко підрахувати прямий ефект, коли ціна обумовлена, наприклад, втраченим бізнесом, усуненням пошкоджень та можливими судовими витратами. Згідно з звітом Corero NetWork Security за 2018 рік, компанії, що спеціалізується на запобіганні DDoS-атак, типова DDoS-атака може коштувати компанії, загалом до 50 000 доларів. Для більших компаній сума може бути ще вищою.

Проведення DDoS-атаки не є безкоштовним. Багато кіберзлочинців побачили тут можливість для бізнесу та пропонують бажаючим заказати DDoS-атаку. Наприклад, ціна атак типу "відмова в обслуговуванні", що продаються в темній мережі, варіюється в залежності від того, як довго триває атака і наскільки велика вона [4].

Законодавчі аспекти DDoS-атак

Атаки типу «відмова в обслуговуванні» вважаються незаконними за законами багатьох країн, і в майбутньому вони будуть визначені як незаконні за законами багатьох інших країн. На відміну від спуфінгу, наприклад, окремі компоненти атаки типу «відмова в обслуговуванні» можуть бути незаконними.

Атака відмови у обслуговуванні може порушувати закони кількох країн одночасно. У США, наприклад, атака типу «відмова в обслуговуванні» вважається федеральним злочином, а у Великій Британії за DDoS-атаку можна отримати до 10 років в'язниці. Звісно, треба відшкодувати нанесені збитки [5].

Можливості відстеження DDoS-атаки

Відстеження атак типу «відмова в обслуговуванні» може бути важким. Проблема в тому, що вони використовують велику кількість комп'ютерних ботів, і буває складно знайти справжнього організатора.

Атаки відмови в обслуговуванні можуть бути ідентифіковані, коли вони відбуваються за допомогою різних інструментів безпеки. Однак можливо вже занадто пізно зупиняти їх на цьому етапі. Справді, багато компаній активно витрачають багато грошей на боротьбу з DDoS-атаками [5].

Запобігання DDoS-атаці "відмова в обслуговуванні"

Атаки типу Denial of Service «відмова в обслуговуванні» найчастіше використовуються для виведення з ладу інтернет-ресурсів та корпоративних служб. Однак у деяких ситуаціях, таких як онлайн-ігри, атака відмови в обслуговуванні також може бути використана проти користувача.

VPN приховує IP-адресу користувача, тому проти нього не може бути проведена пряма DDoS-атака.

Список використаних джерел:

1. Як це працює: DDoS. : Веб сайт. URL: https://ssl.com.ua/blog/what-is-ddos/ (Дата звернення: 1.11.2021).

2. Що таке DDOS-атаки? : Веб сайт. URL: https://aws.amazon.com/ru/shield/ddos-attack-protection/ (Дата звернення: 1.11.2021).

3. Які бувають DDoS-атаки і чому захищатися складніше з року в рік. : Веб сайт. URL: https://www.orange-business.com/ru/blogs/kakie-bivayut-ddos-ataki-i-pochemu-zaschischatsya-slozhnee-iz-goda-v-god (Дата звернення: 1.11.2021).

4. Corero – перша лінія захисту від DDoS атак. : Веб сайт. URL: https://ko.com.ua/corero_-_pervaya_liniya_zashhity_ot_ddos_atak_107497 (Дата звернення: 1.11.2021).

5. Атака відмови в обслуговуванні. : Веб сайт. URL: https://uk.wikitechpro.com/858843-ddos-GBFMYW (Дата звернення: 1.11.2021).

Ключові слова: DDoS-атаки, DNS-сервера, IP-адресу, запобігання, відстеження**,** законодавчі аспекти.

Ключевые слова: DDoS-атаки, DNS-сервера, IP-адрес, предотвращение, отслеживание, законодательные аспекты.

Keywords: DDoS-attacks, DNS-servers, IP-address, prevention, tracking, legislative aspects.

Науковий керівник: *к.т.н., доц. Задерейко О.В.*

Іванова Ірина Олександрівна

Національний університет «Одеська юридична академія»,

студентка 3-го курсу факультету кібербезпеки та інформаційних технологій

ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ БАЗ ДАНИХ

Актуальність теми обумовлена зростанням використання інформаційних баз у державних установах, корпораціях та підприємствах. Вторгнення, викрадення або пошкодження яких призводить до руйнівних наслідків у фінансовій, репутаційній, а інколи й в юридичній сферах.

Можна виокремити декілька основних причин які привертають увагу до безпеки даних та змушують використовувати більше ресурсів задля забезпечення безпеки БД.

Насамперед це кіберзлочинність, засоби якої постійно удосконалюються, з’являються нові способи проникнення до систем, створюється нове шкідливе програмне забезпечення та віруси.

По-друге, це проблема юридичної відповідальності. Права людини в міжнародному законодавстві про захист персональних даних являються одним з основоположних в інформаційному просторі, а отже постійно змінюються і стають все більш суворими. Відповідальність за недотримання нормативних