УДК 004.056.53:355.451]:004.7 https://doi.org/10.30837/IYF.PCEIP.2024.117

РІЗНОВИДИ ТА МЕТОДИ АТАК НА DNS СЕРВЕРИ

Ляшко М.С.
Науковий керівник – ст. викл. В'юхін Д.О.
Харківський Національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: mykyta.liashko@nure.ua

This work is devoted to the growing threat of cyberattacks on DNS systems and their implications for Internet security. It explains what DNS is and the role it plays in determining IP addresses for domain names. The importance of learning about and understanding the different types of DNS attacks, such as zero-day, rapid-flow, and DNS spoofing, along with their potential consequences, is highlighted. It also discusses effective defence strategies to help prevent or mitigate the effects of such attacks.

Останнім часом постійно збільшується кількість атак на електронні ресурси [1]. При цьому одним з основних факторів захисту є забезпечення безпеки DNS серверів.

Мета доповіді полягає в дослідженні різновидів та методів захисту від атак на Domain Name System (DNS). Доповідь спрямована на розкриття сутності DNS атак, визначення їхніх типів та потенційних наслідків для інформаційної безпеки. Основна мета – висвітлити ефективні та сучасні стратегії захисту, які допомагають уникнути або пом'якшити негативні наслідки DNS атак.

Хоча система доменних імен (DNS) є досить потужною, вона, здається, менше орієнтована на безпеку, тому за останні кілька років спостерігається різке збільшення DNS-атак, і ці атаки не обмежуються лише невеликими веб-сайтами. Багато популярних сайтів, таких як Reddit, Spotify, Twitter, також скаржаться на недоступність для тисяч своїх користувачів.

Розглянемо типи DNS-атак:

– Zero—day attack (Атака нульового дня): У цьому типі атаки зловмисник використовує раніше невідому вразливість у програмному забезпеченні сервера DNS або стеку протоколів.

– Fast Flux DNS (Швидкий потік): Хакери змінюють частоту DNS-запису на вищу, щоб перенаправити DNS-запити. Цей метод допомагає зловмиснику уникнути виявлення.

– DNS-Spoofing (DNS-спуфінг): DNS-спуфінг, також відомий як отруєння кешу DNS, це тип взлому комп'ютерної безпеки. Зловмисники або хакери пошкоджують весь DNS-сервер, замінюючи схвалений IP-адрес фальшивим

IP-адресом в кеші сервера. Таким чином, вони перенаправляють весь трафік на злонамірений веб-сайт і збирають важливу інформацію.

Схематична робота атаки на DNS-сервер представлена на рисунку 1.

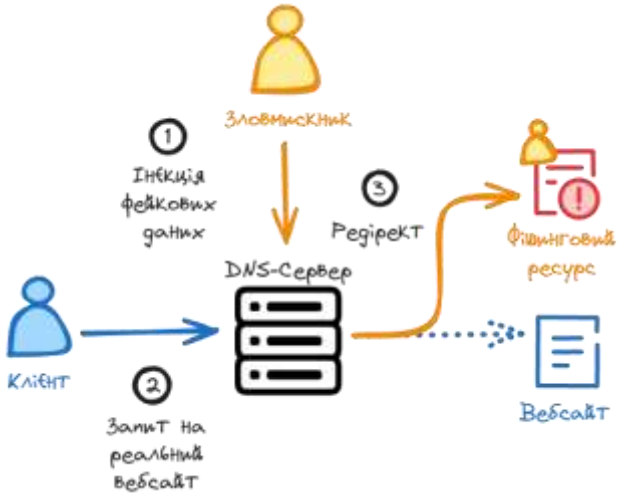

Рисунок 1 – Схематична робота атаки на DNS-сервер

DNS-спуфінг, а також інші методи для отруєння кешу, виконують тільки частину роботу для зловмисників. Наступний і головний крок є відключення користувачів від доступу в Інтернет за рахунок веб-сайтів, які залишились в локальному кеші.

Це одна з найпоширеніших технік фішингу, яку зловмисники регулярно використовують для крадіжки інформації. Оскільки користувачі вводять правильну адресу домена у своїх браузерах, вони ніколи не розуміють, що отримують доступ до підробленого або вкраденого веб-сайту.

Тому стає складніше виявити цю атаку. Іноді користувачі не можуть ідентифікувати її до закінчення часу життя (time to live (TTL)). TTL або час для життя — це час, коли DNS-розпізнавач пам'ятає DNS-запит до закінчення терміну його дії.

DNS-атаки (атаки, спрямовані на систему доменних імен) можуть бути широким спектром, і для їх захисту використовують різні методи. Ось деякі популярні методи захисту:

– DNSSEC (DNS Security Extensions): DNSSEC є розширенням DNS, яке надає механізми для перевірки цілісності та автентичності даних DNS. Вона захищає від атак, таких як DNS-підробка (DNS spoofing) та DNS-отруєння.

– Фаєрволи (Firewalls): Використання фаєрволів може допомогти обмежити доступ до DNS-серверів та блокувати небезпечний трафік. Регулярно оновлюйте правила фаєрвола, щоб враховувати нові загрози.

– Моніторинг трафіку: Системи моніторингу трафіку можуть виявляти незвичайний або великий обсяг запитів до DNS-серверів, що може бути

індикатором DNS-атаки. Автоматизовані системи можуть блокувати або обмежувати такий трафік.

– Фільтрація DNS-запитів: Використання фільтрів DNS дозволяє блокувати доступ до веб-сайтів зі списком небезпечних або небажаних доменних імен. Це може допомогти захистити від атак, які використовують зловмисні домени.

– Anycast DNS: Anycast є технологією, яка дозволяє розміщувати одне і те саме IP-адресу на різних місцях у мережі. Це підвищує доступність та стійкість до витоку DNS-атак, розподіляючи трафік між кількома серверами.

– Обмеження DNS-запитів: Встановлення обмежень на кількість запитів від одного користувача або IP-адреси може допомогти уникнути перевантаження DNS-сервера через DDoS-атаки.

– Регулярні оновлення програмного забезпечення: Переконайтеся, що програмне забезпечення DNS-серверів і DNS-клієнтів регулярно оновлюється для усунення вразливостей і покращення безпеки.

– Безпека внутрішньої мережі: Захищайте внутрішню мережу від зловмисних елементів, які можуть впливати на DNS. Це включає в себе застосування методів захисту від вірусів, шкідливих програм і внутрішніх загроз.

– Отримуйте регулярне уявлення про те, що відбувається в мережі. Ви можете скористатися такими технологіями, як IPFIX, NetFlow і інші, щоб досягти бажаного результату.

Для зменшення ризиків DNS-атак адміністратори серверів повинні прийняти кілька заходів безпеки. Це включає використання оновлених версій програмного забезпечення DNS та регулярне налаштування серверів для здійснення дублювання. На особистому рівні користувачі також можуть допомогти уникнути загроз безпеки, скинувши свій DNS-кеш. Атаки на систему DNS можуть мати серйозні наслідки для безпеки даних та інформаційної інфраструктури, тому важливо вжити всі можливі заходи для їх уникнення.

Список використаних джерел

1. Сєвєрінов О.В., Шевцов В.О., Сокол-Кутиловська А.С. Аналіз сучасних методів атак на електронні ресурси органів управління. // Системи озброєння і військова техніка 1 (2017): 65-68.

2. What Are DNS Attacks? Paloalto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-a-dns-attack (дата звернення: 03.03.2023)

3. What is DNS Spoofing | Cache Poisoning Attack Example. Imperva. URL: https://www.imperva.com/learn/application-security/dns-spoofing/ (дата звернення: 03.03.2023)

4. DDoS-атаки з DNS-посиленням: як це працює і як їх зупинити?. Triolan.net. URL: https://triolan.net/wiki/knowledgebase.php?article=11 (дата звернення: 03.03.2023)

5. Колтаков О. А. Аналіз основних показників якості з'єднання з сервером DNS / О. А. Колтаков // Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023): матеріали дев'ятої Міжнародної науково-технічної конференції, 7 грудня 2023 р. – Харків : ХНУРЕ, 2023. – С. 91-92.