Лещенко Б. С., магістрант, гр. КБм-21-1,
Єфіменко А. А., к.т.н., доц.,
завідувач кафедри комп'ютерної інженерії та кібербезпеки
Вакалюк Т. А., д.пед.н., проф.,
професор кафедри інженерії програмного забезпечення
Державний університет «Житомирська політехніка»

ЗАГРОЗИ БЕЗПЕКИ ДОМЕННОЇ СИСТЕМИ ІМЕН

Для максимального охвату всіх можливих дій зловмисників варто дослідити відомі сценарії експлуатації вразливостей.

Згідно інформації наданої компанією EfficientIP (компанія, яка займається автоматизацією та безпекою та спеціалізується на безпеці DNS), близько 79% компаній постачальників послуг в 2020 році стикалися з тими чи іншими атаками пов'язаними з DNS.

В звіті під назвою «IDC 2020 Global DNS Threat Report» сказано, що обізнаність щодо безпеки DNS стабільно зростає з року в рік, але середня кількість атак зростає, так само як і грошові втрати компаній від цих атак. Значний розвиток хмарних технології безпосередньо вплинув на важливість справнопрацюючого DNS.

Збої в роботі доменної системи імен завдають шкоди, без перебільшення, всім сферам людської життєдіяльності починаючи сферою телекомунікацій і фінансовими сервісами і закінчуючи сферами освіти та охорони здоров'я. Окрім високої частоти атак, телекомунікаційні провайдери також стикаються з більш втратними атаками – близько 8% організацій заявили, що вони сумарно постраждали від збитків у розмірі понад 5 мільйонів доларів внаслідок атак на DNS.

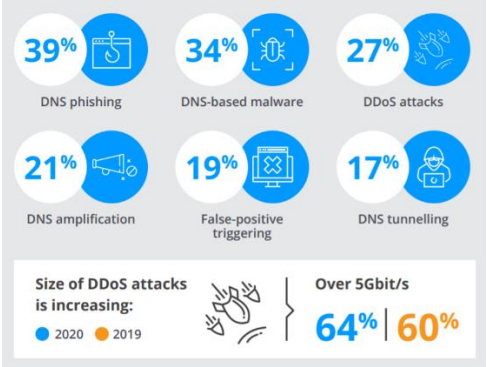

Рис. 1. Рейтинг популярності експлуатації типів атак пов'язаних з DNS

Найбільш поширеними типами атак на DNS є фішинг (37%), шкідливе програмне забезпечення націлене на DNS (34%), DDoS атаки (27%), атаки з блокування доменів, які «виснажують» ресурси серверів доменної системи імен (22%) та атаки ампліфікації (підсилення), які в результаті можуть спричинити відмову роботи мережі компанії, тим самим викликати серйозні економічні втрати (21%) (див. рис. 1).

Огляд видів атак варто почати з атак з «отруєння» кешу (DNS Cache Poisoning Attack). Вона є однією з найчастіших атак, і її головна ціль це перенаправлення користувачів на підробні вебсайти. Користувач буде переходити по правильній адресі, але його все одно буде спрямовано на шахрайську сторінку. Потенційні сторінки для підміни можуть бути абсолютно різними, починаючи від новинних ресурсів і до сайтів банківських установ.

Наступний вид атак це, так звані, розподілені атаки з відмовою в роботі з «відбиттям» (Distributed Reflection Denial of Service). Суть цих атак полягає в тому, щоб зменшити доступність серверів жертв або взагалі призвести до повної відмови в роботі. З великої кількості керованих хостів надсилаються запити на сервер жертви. Використовуватись можуть різноманітні протоколи.

Схожий тип атаки називається атака «фантомними» доменами (Phantom domain attack). В ході такої атаки зловмисник направляє на DNS сервер запити з доменами, яких не існує. Сервер пересилає ці запити далі та очікує відповіді. Якщо таких запитів багато, то це значно знижує продуктивність DNS серверу.

Ще один подібний вид DoS атаки – TCP SYN Flood атака. Ця атака може бути застосована на будь якому обладнанні, що використовує протокол TCP. Як відомо, протокол TCP працює по системі потрійного рукостискання: клієнт передає SYN запит, потім сервер передає клієнту SYN/ACK відповідь, далі клієнт передає ACK на сервер. Суть TCP SYN Flood атаки полягає в тому, що зловмисник направляє багато SYN пакетів на сервер, а ACK пакети не надсилає. В цьому випадку сервер очікує на ACK пакет та залишає порти в напіввідкритому стані. Якщо таких фіктивних SYN запитів безліч, то може статись така ситуація, що сервер не буде мати вільних портів для легітимних користувачів.

Список використаних джерел

1. Liska A. DNS Security Defending the Domain Name System / A. Liska, S. Geoffrey. – Cambridge: Elsevier Inc, 2016. – 212 с. – (1).

PETTERS J. DNS Security Guide [Електронний ресурс] / JEFF PETTERS. – 2020. – Режим доступу до ресурсу: https://www.varonis.com/blog/dns-security/.