**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ**

**КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ**

# Пояснювальна записка

до магістерської роботи
на тему:

# «ТЕХНОЛОГІЇ ТА МЕТОДИ ВИЯВЛЕННЯ ШКІДЛИВИХ ЗАПИТІВ В КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ОСНОВІ ПРОТОКОЛУ DNS»

Виконав: студент 6 курсу,
групи БСДМ-62 спеціальності 125 Кібербезпека освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Гаврилей О.П.
(прізвище та ініціали)
Керівник Довженко Н.М.
(прізвище та ініціали)
Рецензент _____
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.

КИЇВ – 2021

# РЕФЕРАТ

Текстова частина магістерської роботи: 60 сторінок, 15 рисунків, 3 таблиці, 20 джерел.

*Об'єкт дослідження* – процес виявлення шкідливих запитів.

*Предмет дослідження* – технології виявлення шкідливих запитів.

*Мета роботи* – дослідити технології виявлення шкідливих запитів в комп'ютерних мережах на основі DNS протоколу.

*Методи дослідження* – опрацювання літератури за даною темою, аналіз статичних даних та стандартів.

В роботі проведено основні відомості про технології та методи виявлення шкідливих запитів в комп'ютерних мережах на основі протоколу DNS.

Проаналізовано різні види мережевих атак на протокол DNS, та досліджено основні методи виявлення шкідливих запитів в комп'ютерних мережа, розглянуто інструменти виявлення шкідливих запитів. Розгорнуто технології для виявлення шкідливих запитів та проведення досліджень щодо комп'ютерних мереж.

*Галузь використання* – інформаційна безпека.

ІНФОРМАЦІЙНА БЕЗПЕКА, IDS, КІБЕРБЕЗПЕКА, ВИЯВЛЕННЯ ШКІДЛИВИХ ЗАПИТІВ, ELASTIC, КОМП'ЮТЕРНІ МЕРЕЖІ, ПРОТОКОЛ DNS, МЕРЕЖЕВІ АТАКИ

# ABSTRACT

Master’s thesis: 60 pages, 15 figures, 3 tables, 20 sources.

*Object of research* – malicious query detection process.

*Subject of research* – malicious query detection technologies.

*The aim of research* – explore technologies for detecting malicious queries in computer networks based on the DNS protocol.

*Research methods* – elaboration of literature on this topic, analysis of static data and standards.

The paper provides basic information about technologies and methods for detecting malicious queries in computer networks based on the DNS protocol.

Various types of network attacks on the DNS protocol are analyzed, and the basic methods of detection of malicious requests in computer networks are investigated, the tools of detection of malicious requests are considered. Technologies for detecting malicious requests and conducting research on computer networks have been developed.

*Field of use* – information security.

INFORMATION SECURITY, IDS, CYBER SECURITY, DETECTION OF HARMFUL REQUESTS, ELASTIC, COMPUTER NETWORKS, DNS PROTOCOL, NETWORK ATTACKS

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

DNS — Domain Name System

TLD — top-level domain

SSL — Secure Sockets Layer

DNSSEC — Domain Name System Security Extensions

URI — Uniform Resource Identifier

DoT — DNS over TLS

DoH — DNS over HTTPS

TLS — Transport Layer Security

DGA — Domain generation algorithm

DDoS — Distributed denial-of-service

IDS — Intrusion Detection System

NDR — Network Detection and Response

**ЗМІСТ**

Стор.

# ВСТУП

*Актуальність дослідження.* Особи та організації покладаються на Інтернет як на важливе середовище для особистих і ділових операцій. Зловмисники можуть використовувати різні підходи, щоб приховати свою діяльність у скомпрометованих мережах та приховано спілкуватися між серверами зловмисника та жертвами.

Аналізуючи дані представлені в щорічному звіті компанії DNSFilter протягом 2020 і 2021 років, DNS відіграє роль у приблизно 80% атак. Завдяки захисту від кібератак на основі DNS організації можуть негайно заблокувати до 33% загроз на основі DNS і збільшити видимість додаткових загроз на 47%, захищаючи себе від атаки нульового дня, а також інших відомих загроз [1]. Для протидії цим атакам потрібно застосовувати сучасні методи кібербезпеки для захисту систем, мереж і програм від постійних кіберзагроз.

Тому для виявлення шкідливих мережевих атак потрібно застосовувати інструменти, які аналізують запити DNS і блокувати доступ до шкідливих, підозрілих або інших вибіркових типів доменів. Які потенційно можуть бути шкідливими.

Щоб унеможливити компрометацію мережі

*Об’єкт дослідження* – процес виявлення шкідливих запитів.

*Предмет дослідження* – технології виявлення шкідливих запитів.

*Мета роботи* – дослідити технології виявлення шкідливих запитів в комп'ютерних мережах на основі DNS протоколу.

*Наукові завдання:*

– дослідити основні види мережевих загроз;

– методи виявлення шкідливих запитів;

– на основі літератури та статистичних даних зібрати інформацію про найбільш поширені вразливості DNS;

– дослідити методи виявлення та протидії шкідливим запитам в

комп'ютерних мережах;

– розглянути інструменти виявлення шкідливих запитів;

– розгорнути технології виявлення шкідливих запитів в комп'ютерних мережах на основі протоколу DNS.

Метою даної роботи є дослідження технологій виявлення шкідливих запитів в комп'ютерних мережах та розгортання на їх основі систем виявлення шкідливих запитів які допоможуть більш ефективніше знаходити шкідливі запити.

*Практичне значення одержаних результатів* полягає в впроваджені технологій для виявлення шкідливих запитів

*Апробація результатів.* Основні наукові результати роботи доповідалися та обговорювалися на 1 конференції:

1. Всеукраїнська наукова конференція на тему «Актуальні проблеми кібербезпеки», Навчально-наукового інституту захисту інформації, 27 жовтня 2021р.

# 1 АНАЛІЗ СУТНОСТІ ТА ЗМІСТУ ШКІДЛИВИХ ЗАПИТІВ В КОМП'ЮТЕРНИХ МЕРЕЖАХ НА ОСНОВІ ПРОТОКОЛУ DNS

## 1.1. Призначення, структура та функції DNS

DNS є однією з основ Інтернету, надзвичайно складної та децентралізованої системи, яка перетворює зручні для читання доменні імена (наприклад, havrs.com) у числові IP-адреси.

DNS має ієрархічну структуру дерева, яка називається простором імен DNS. Кожна крапка в імені домену вказує на поділ між рівнями в структурі дерева. Верхній шар структури дерева DNS представляє кореневий рівень, який починається з крапки. Під кореневим рівнем є домени верхнього рівня (TLD), який відповідає таким дочірніми кореневими доменами, як .com, .org, .edu.ua та інші. Далі, TLD також має дочірні домени, які посилаються на другий рівень доменів або авторитетні сервери доменних імен [2]. Нарешті, повне доменне ім’я (FQDN) розташовує імена хостів або субдомени в ієрархії DNS. Наприклад, процес пошуку наступного доменного імені dn.dut.edu.ua. завжди починається з крапки, яка є кореневим сервером у структурі дерева DNS. Потім кореневий сервер пересилає запит до відповідного TLD, який у цьому випадку є .edu.ua.

Далі TLD надсилає запит до доменів вторинного рівня. Як тільки запит отримує авторитетний сервер доменних імен, він шукає еквівалент субдомену та повертає його IP-адресу [3]. Детальніше можна переглянути ілюстрацію ієрархії доменних імен на (рис. 1.1.).

Кожен запис у домену зону організовано за допомогою текстового представлення, яке називається записом ресурсу (RR). Кожен ресурсний запис складається з п’яти полів, як показано в (табл. 1.1.), розділених пробілами/табуляціями.

Таблиця 1.1

Поля в ресурсному записі

| Name | Time to Live (TTL) | Record Class | Record Type | Record Data |
|---|---|---|---|---|

Ці поля або компоненти коротко визначені нижче:

- Ім’я (Name): це поле є у формі FQDN, але його можна залишити порожнім, і в цьому випадку запис автоматично успадковує ім’я з попереднього запису.
- Час життя (TTL): це значення визначає проміжок часу, після якого DNS-сервери можуть видаляти кешовані відповіді та виконувати нові запити для отримання актуальної інформації. Якщо значення відсутнє, тоді за замовчуванням використовується глобальне значення TTL, яке визначено у верхній частині файлу зони.
- Дані запису (Record Data): поле даних запису складається з одного або кількох інформаційних компонентів, залежно від кожного типу запису. Це інформація відповіді, призначена імені запису ресурсу.

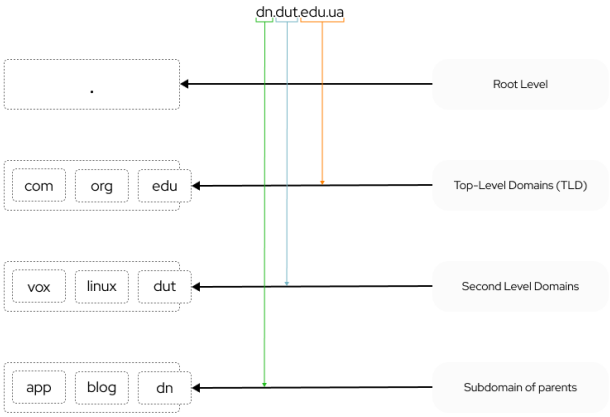


Рис. 1.1. Ієрархічна структура DNS

Якщо локальний DNS розпізнавач має кешовану копію записів, він відповідає на хост-машину відповіддю на запит, але якщо він не має кешованої копії, він починає запитувати ієрархію DNS, починаючи з кореневого DNS-сервера. Кореневі

сервери DNS утворюють основу інфраструктури DNS і містять інформацію про авторитетні сервери імен TLD. Використовуючи частину запиту TLD, кореневі сервери DNS відповідатимуть DNS розпізнавачу відповідною IP-адресою сервера імен [4]. Цей процес триватиме рекурсивно, поки не буде досягнуто кінцевої зони. Остання зона міститиме відповідь на вихідний запит DNS.

Компанії що займаються розробкою вебпереглядачів та компанії з кібербезпеки, підтримують свої DNS-розпізнавачі для користувачів, щоб кожен охочий міг обрати сервіс який буде швидше та точніше знаходити записи, а також забезпечувати безпеку передачі DNS записів. В (табл. 1.2.) наведено лідерів ринку які надають доступ до власних DNS сервісів, а також пропонують ряд додаткових функцій для забезпечення безпеки даних кінцевих користувачів.

Таблиця 1.2.

Провайдери публічних DNS сервісів

| DNS Провайдер | Адреса доступу | Функції безпеки | Додаткові функції |
|---|---|---|---|
| Google DNS | 8.8.8.8 &8.8.4.4 | Підтримка DoH & DoT | Anycast DNS, DNSSEC, |
| OpenDNS (Cisco) | 208.67.222.222 & 208.67.220.220 | Підтримка DoH | Фільтрація контенту, DNSCrypt |
| Cloudflare | 1.1.1.1 &1.0.0.1 | Підтримка DoH & DoT | Anycast DNS, DNSSEC |
| Quad9 | 9.9.9.9& 149.112.112.112 | Підтримка DoH & DoT | IPv6, Захист від фішингових атак, DNSCrypt |
| NextDNS | 45.90.28.237 & 45.90.30.237 | Підтримка DoH & DoT/QUIC | IPv6, захист від повторного зв'язування DNS, підтримка від NRD та DGA |

Кожний користувач має змогу розгорнути свій власний DNS сервер який буде обробляти всі запити та буде налаштований під потреби власника. Використовуючи CoreDNS який розробляється як програмне забезпечення з відкритим вихідним кодом та використовує UDP/TCP, TLS (RFC 7858) та gRPC і

має систему плагінів кожен з яких легко втілює якусь окрему можливість DNS. Система плагінів також дозволяє створювати свої власні плагіни для розширення можливостей DNS сервера. CoreDNS базується на хмарних технологіях та розгортається за допомогою Kubernetes який підтримує інший тип робочого навантаження, і стандартна конфігурація CoreDNS може не відповідати всім потребам. Серед альтернативних рішень слід виділити SkyDNS, Istio та PowerDNS, які дозволять використовувати всі можливості власного DNS сервера, та мати повний контроль за даними.

Є три найважливіші речі, на які слід звернути увагу при налаштуванні DNS. Перш за все, «надійність». Хоча більшість DNS-серверів працюють безперебійно, не всі вони здатні забезпечити необхідну продуктивність. Друге, що повинно турбувати при виборі DNS провайдера це «Швидкість», оскільки вона відіграє важливу роль в отриманні доступу до потрібних ресурсів мережі. Захист це третя складова при обранні провайдера який може забезпечити протидію атак на основі DNS, в (табл. 1.2.) представлено 5 найвідоміших провайдерів та технології захисту які вони пропонують для користувачів.

## 1.2. Аналіз методів забезпечення безпеки комп'ютерних мереж

Через те що DNS є одним із важливих та найстаріших компонентів комп'ютерних мереж, одна із фундаментальних проблем яка його спіткала це відсутність конфіденційності в реалізації технології що не відповідає сучасним тенденціям в безпеці. Якщо запити DNS не є захищеними ні одним із сучасних методів безпеки, урядам стає легше цензурувати Інтернет на рівні провайдерів, а зловмисникам стежити за поведінкою користувачів в Інтернеті.

Такі технологічні гіганти як Microsoft, Google та Mozilla сумісно з деякими компаніями які займаються кібербезпекою об'єдналися та розробили низку стандартів та технологій які були спрямовані на захист DNS запитів.

*DNSCrypt.* Більшість користувачів які використовують сучасні технології захисту такі як https який захищає вебтрафіку від перехоплення та заміни, але на жаль, багато хто забуває ще про одну незахищену сторону, а саме про DNS-запити.

Архітектура DNS за рідкісним винятком залишається незмінною з 1983 року. Щоразу, коли ви хочете відкрити сайт, браузер надсилає запит із зазначенням домену на DNS-сервер, який у відповідь надсилає необхідну IP-адресу. І запит, і відповідь на нього передаються у відкритому вигляді, без шифрування. Це означає, що провайдер, адміністратор мережі або зловмисник який застосовує MITM атаку, може не тільки зберігати історію використання всіх ваших сайтів, але й підміняти відповіді на ці запити.

Звичайно, можна відмовитися від використання DNS-сервера провайдера і вказати в налаштуваннях роутера сторонні рішення (наприклад, Google Public DNS, CloudFlare або OpenDNS). Але за відсутності шифрування це не розв'язує проблему. Провайдер може втрутитися і тут, підмінивши відповідь на свою.

Розробники популярного сервісу OpenDNS запропонували розв'язання проблеми ще кілька років тому. Вони створили програмну утиліту DNSCrypt з відкритим вихідним кодом та однойменний протокол, який відіграє для DNS-запитів таку саму роль, як і SSL для HTTP [5].

По-перше, DNSCrypt шифрує за допомогою стійкої еліптичної криптографії повідомлення між комп'ютером та DNS-сервером. Це захистить їх від прослуховування та MITM-атаки.

По-друге, відсутня прив'язаність до сервера провайдера або налаштування свого роутера. DNSCrypt звертається за адресами безпосередньо на вказаний сервер зі списку довірених DNS серверів.

До цього часу для застосування DNSCrypt користувачам необхідно було встановити на комп'ютер окрему утиліту. Це не складно, але без поширення знань про загрозу та способи її вирішення навряд чи варто розраховувати на масове застосування цієї технології.

*DNSSEC.* Спеціальна група з розробки Інтернету (IETF) багато років працює над створенням стандартів для розширення системи безпеки доменних імен

(DNSSEC). DNSSEC захищає користувачів і програми Інтернету від підроблених даних системи доменних імен (DNS) за допомогою криптографії з відкритим ключем для цифрового підпису даних авторитетної зони, коли вони входять до DNS, а потім перевіряють їх у місці призначення.

Цифровий підпис допомагає запевнити користувачів, що дані походять із зазначеного джерела і що вони не були змінені під час передачі. DNSSEC також може встановити, що доменне ім’я не існує. Ці можливості необхідні для підтримки довіри до Інтернету (рис. 1.2.).

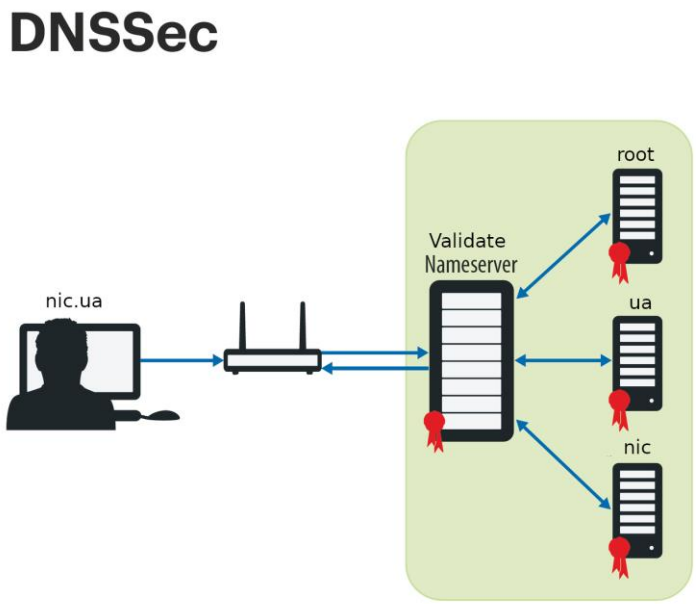


Рис. 1.2. Схема роботи DNSSEC

У DNSSEC кожна зона має принаймні одну пару відкритих/приватних ключів. Відкритий ключ зони публікується за допомогою DNS, тоді як закритий ключ зони зберігається в безпеці. Закритий ключ зони підписує окремі записи даних DNS у цій зоні, створюючи цифрові підписи, які також публікуються разом із DNS.

DNSSEC використовує жорстку модель довіри, і цей ланцюг довіри перетікає від батьківської зони до дочірньої зони. Ланцюг довіри встановлюється, коли зони вищого рівня (батьківські) підписують відкриті ключі нижчих (дочірніх) зон [6].

Авторитетними серверами імен для цих різних зон можуть керувати реєстратори, постачальники Інтернет-послуг (ISP), компанії з вебхостингу або самі реєстранти.

Коли кінцевий користувач хоче отримати доступ до вебсайту (або будь-якого інтернет-ресурсу), спеціальна вебсторінка на комп'ютері користувача запитує IP-адресу вебсайту з рекурсивного сервера імен. Коли рекурсивний сервер імен запитує запис адреси, він також запитує ключ DNSSEC, пов'язаний із зоною. Цей ключ дозволяє серверу рекурсивних імен перевіряти, що отриманий запис IP-адреси ідентичний запису на авторитетному сервері імен.

Якщо рекурсивний сервер імен визначає, що запис адреси був надісланий авторитетним сервером імен і не був змінений під час передачі, він визначає доменне ім'я (надає запитувану IP-адресу), і користувач може отримати доступ до сайту. Якщо запис адреси було змінено, рекурсивний сервер імен не дозволяє користувачеві отримати доступ до шахрайської адреси. DNSSEC також може довести, що доменне ім'я не існує. У результаті цього процесу запити та відповіді DNS захищені від атак «людина посередині» (MITM) і тих видів підробок, які можуть перенаправляти користувачів Інтернету на шахрайські вебсайти.

*DNS-over-TLS.* DoT, описаний у специфікації RFC 7858, використовує добре відомий протокол безпеки транспортного рівня (TLS) і таким чином успадковує всі його переваги безпеки. За замовчуванням розпізнавач DoT прослуховує порт 853 для вхідних запитів DNS, які мають бути зашифровані (рис. 1.3.). Цей нестандартний порт був обраний, щоб полегшити відмінність між DoT і не-DoT з'єднаннями [7]. Однак адміністратори, які розгортають DoT, можуть вибрати інший порт за умови, що розпізнавач і клієнти згодні. Відхід до повідомлень DNS із відкритим текстом у протоколі не дозволяється ні для клієнта, ні для сервера.

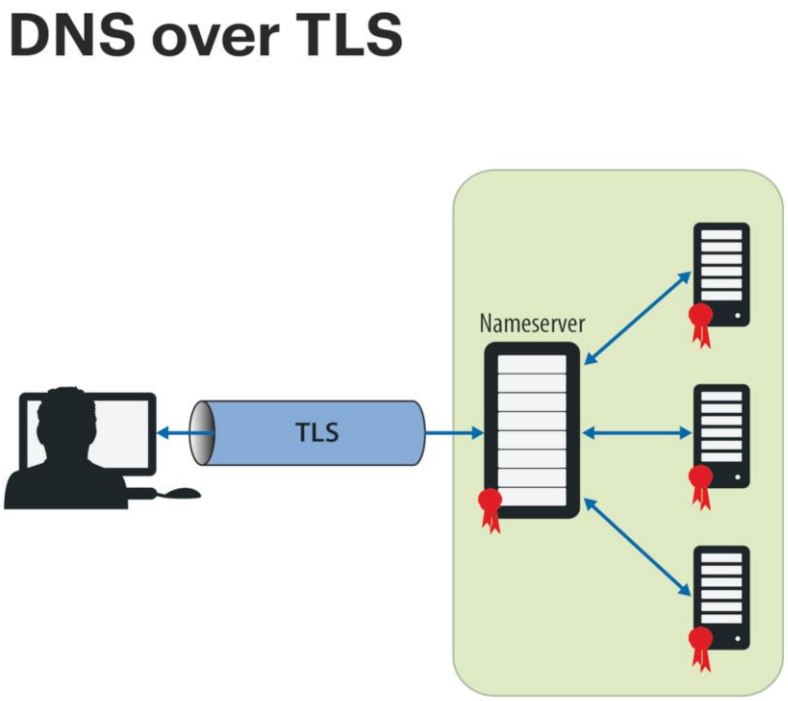


Рис. 1.3. Схема роботи DoT

Протокол, який показано вище, складається з двох RTT під час першого контакту. По-перше, DNS-клієнт виконує рукостискання TCP з розпізнавачем, до якого він вибрав підключення. Далі клієнт DNS виконує рукостискання TLS із сервером. Клієнт не обов'язково повинен автентифікувати сервер, оскільки це залежить від профілю, який використовується. Тому самопідписані сертифікати також прийнятні. Після успішного завершення рукостискання обидві сторони отримують ключ сеансу, який використовується для наступних пакетів. На третьому кроці клієнт DNS надсилає свої DNS-запити через встановлений канал TLS. Для зменшення пропускної здатності можна конвертувати декілька запитів DNS. Повідомлення, надіслані через цей канал TLS, приховані від будь-якої проміжної сторони; тому запити та відповіді DNS залишаються конфіденційними, будь-які маніпуляції можна виявити.

DoT підтримує два профілі використання, які визначені у RFC 8310 і відрізняються конфіденційністю, яку вони надають. Клієнти можуть вибирати, за яким профілем слідувати, і таким чином, можуть встановлювати налаштування

DNS під свої вимоги. Адміністратори також можуть примусово використовувати профіль використання.

Збалансований: цей профіль не гарантує повну конфіденційність, але намагається досягти якомога вищого її рівня. Таким чином, якщо підключення до серверів не можна автентифікувати або зашифрувати, вони все ще прийнятні для клієнта. Цей профіль свідомо оцінює доступність як основну, а конфіденційність як другорядну мету, і, таким чином, може призвести до небезпечних з’єднань.

Жорсткий: це профіль, орієнтований на конфіденційність, і не дозволяє встановлювати з'єднання з серверами, які не можуть бути зашифровані або автентифіковані. Це обмежує доступність, але гарантує конфіденційність повідомлень DNS. Перехід до незахищених з’єднань заборонений.

Рекомендується використовувати жорсткий профіль конфіденційності для забезпечення належної безпеки в більшості налаштувань.

*DNS-over-HTTPS.* Основним завданням при розробці технології DoH стала допомога користувачам в захисті, як описано в стандарті RFC 8484, є найновішим стандартом для зашифрованого DNS і використовує сеанси HTTPS для обміну повідомленнями DNS. Це уможливлює маскування в іншому HTTPS-трафіку (рис. 1.4.).

У контексті DNS-запитів та можливого зловживання ними існує дві основні загрози безпеці користувачів: трекінг та спуфінг.

Трекінг це збір інформації про запити користувача та продаж її стороннім особам. Навіть якщо вдома або на роботі використовуються надійні DNS-сервери, у громадських місцях завжди є можливість підключитися до бездротової мережі з небезпечним DNS-сервером, який відстежуватиме всі запити користувача і передавати їх зловмисникам.

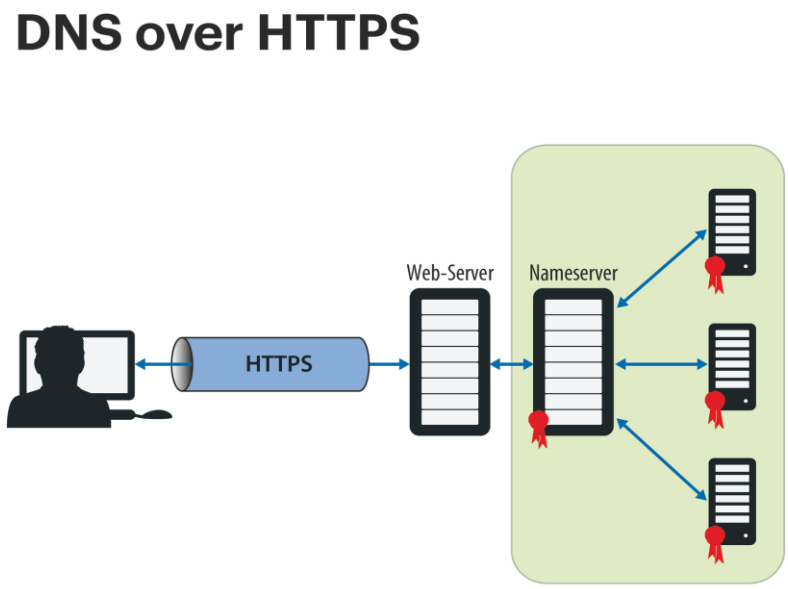


Рис. 1.4. Схема роботи DoH

Спуфінг – це реалізація атаки «Людина посередині» (Man-in-the-Middle, MitM). Зловмисник, який бачить ваші запити, може підмінити відповідь від DNS-сервера та направити вас на шкідливий або шахрайский сайт [8]. Якщо користувач не буде уважний у таких випадках, це може закінчитися встановленням різних шкідливих програм на комп'ютер та розкриттям даних (акаунтів, паролів, даних про платіжні картки), що робить цю загрозу особливо небезпечною.

Частково проблема вирішується технологією DNSSEC, яка використовує принцип асиметричного шифрування з відкритим ключем. Всі відповіді від DNS-сервера підписані цифровим підписом, перевірити підпис може будь-хто, а для підписання використовується секретний ключ [9].

DoH використовує шаблони URI для надсилання запитів DNS і може використовувати методи GET та POST. При використанні розпізнавача Cloudflare 1.1.1.1/1.0.0.1 запити структуровані таким чином:

- Запит GET надсилається на адресу https://1.1.1.1/dns-query?dns, де значення параметра DNS містить повідомлення DNS, закодованого в base64url.
- Запит POST надсилається на https://1.1.1.1/dns-query в тілі повідомлення. Крім того, вказується заголовок application/dns-message.

Слід відзначити, що RFC не визначає шлях DNS-запиту. Однак списки загальнодоступних розпізнавачів показують, що розпізнавачі зазвичай дотримуються цього формату. Веб-браузери можуть виконувати запити самостійно, оскільки вони поставляються з механізмом HTTP.

Багато організацій, що займаються інформаційною безпекою, збирають події зі своїх серверів DNS для моніторингу шкідливої активності. По DNS-запитам можна визначити цільові атаки на інформаційні системи, і навіть виявити зараження комп'ютерів шкідливими програмами. Також на їхній основі створюються правила кореляції для SIEM-систем. Тому використання DoH дуже ускладнює моніторинг шкідливої активності. Для розвязання проблеми були придумані перевірочні домени. Для відключення DoH потрібно додати запис із таким доменом на локальний DNS-сервер. Наприклад, Firefox перевіряє ім'я dnsin.pp.ua, і якщо DNS-сервер відповість помилкою на запит такого імені, браузер буде використовувати DoH. В іншому випадку інформація про такий домен буде отримана і DoH не використовуватиметься. Крім того, у популярних DNS-серверах реалізовано функцію батьківського контролю (обмеження ресурсів небажаних для дітей), відповідно, при використанні DoH її робота буде не коректною.

Загалом, протокол DoH працює подібно до DoT. Їхні протокольні повідомлення містять той самий вміст, за винятком додаткової упаковки повідомлень DoH. Однак така упаковка в поєднанні з роботою на тому самому порту, що й звичайний веб-трафік, дає додаткові переваги конфіденційності.

Ризики які можуть спіткати деяких осіб та організації які покладаються на DNS для блокування зловмисного програмного забезпечення, увімкнення батьківського контролю або фільтрації доступу в браузері до вебсайтів. Якщо ввімкнено, DoH обходить обмеження локального розпізнавача DNS і порушує ці спеціальні політики. Увімкнувши DoH за замовчуванням для користувачів, Firefox дозволяє користувачам (через налаштування) та організаціям (через корпоративні політики) вимикати DoH, коли це заважає бажаній політиці безпеки організації.

Коли DoH увімкнено, браузер за замовчуванням спрямовує запити DoH на DNS-сервери, якими керує надійний партнер, який має можливість бачити запити

користувачів. Також браузери використовують політику довіреного рекурсивного розпізнавання (TRR), яка забороняє партнерам які постачають послуги DoH збирати особисту інформацію користувачів. Щоб зменшити ризики, між компаніями укладаються угоди які зобов'язують дотримуватись політики компанії щодо обробки даних користувачів. Інформація, які саме імена використовуються для відключення DoH при використанні конкретного сервісу, не розголошується.

### 1.3. Види мережевих атак на протокол DNS

*Підробка DNS/Отруєння кешу:* вид атак, при яких підроблені дані DNS вводяться в кеш розпізнавача DNS, в результаті чого розпізнавач повертає неправильну IP-адресу для домену [10]. Замість того, щоб перейти на правильний вебсайт, трафік може бути перенаправлений на шкідливий ресурс або в будь-яке інше місце, яке забажає зловмисник, дуже часто користувачів перенаправляє на копію сайту відомої організації, який використовується для зловмисних цілей, таких як розповсюдження шкідливого програмного забезпечення або збір конфіденційної інформації для входу в особисті облікові записи та видавання себе за іншу людину.

*Тунелювання DNS:* цей вид атака використовує інші протоколи для тунелювання через запити та відповіді DNS. Зловмисники можуть використовувати SSH, TCP або HTTP для передачі шкідливого програмного забезпечення або викраденої інформації в запити DNS, які не завжди може помітити більшість міжмережевих екранів [11].

Зловмисники використовують DNS-розпізнавач для маршрутизації запитів на сервер C2 зловмисника, де інстальована програма тунелювання. Після встановлення з’єднання між жертвою та зловмисником через DNS-розпізнавач, тунель можна використовувати для ексфільтрації даних або виконання інших шкідливих цілей.

*Атака NXDOMAIN*: це тип атаки DNS flood, коли зловмисника відправляє DNS-серверу велику кількість запитів, запитуючи записи про доменні імена, які не

існують, намагаючись викликати відмову в обслуговуванні для правомірного трафіку [12]. Це можна досягти за допомогою складних інструментів атаки, які можуть автоматично генерувати унікальні субдомени для кожного запиту. Атаки NXDOMAIN також можуть бути спрямовані на рекурсивний розпізнавач з метою заповнення кешу розпізнавача небажаними запитами.

*Атака фантомного домену.* Має схожі результати подібні до атаки NXDOMAIN на розпізнавач DNS. Зловмисник налаштовує купу «фантомних» серверів домену, які або дуже повільно відповідають на запити, або взагалі не відповідають [13]. Потім розпізнавач отримує потік запитів до цих доменів, що змушує очікувати відповідей, що призводить до повільної роботи та відмови в обслуговуванні.

*Випадкова атака на субдомен:* у цьому випадку зловмисник надсилає запити DNS для кількох випадкових, неіснуючих субдоменів одного законного сайту. Мета полягає в тому, щоб створити відмову в обслуговуванні для авторитетного сервера імен домену, що унеможливлює пошук веб-сайту з сервера імен. Як побічний ефект, від цього також можуть постраждати провайдери, які обслуговують зловмисника, оскільки кеш їх рекурсивного розпізнавача буде завантажено поганими запитами.

*Атака блокування домену:* зловмисники організовують цю форму атаки, встановлюючи спеціальні домени та розпізнавачі для створення TCP-з'єднань з іншими законними розпізнавачами. Коли цільові розпізнавачі надсилають запити, ці домени відправляють назад повільні потоки випадкових пакетів, пов’язуючи ресурси розпізнавача.

*Атака на DNS посилення та DoS, DDoS:* атака посилення DNS – це тип атаки DDoS, під час якої зловмисники використовують загальнодоступні відкриті DNS-сервери, щоб заповнити ціль трафіком відповіді DNS. Зловмисник надсилає запит пошуку DNS відкритому DNS-серверу з адресою джерела, підробленої як адресу цілі. Коли DNS-сервер надсилає відповідь на запис DNS, вона натомість надсилається до цільової групи.

*Викрадення DNS.* Існує три типи викрадення DNS:

- Зловмисники можуть зламати обліковий запис реєстратора домену та змінити ваш DNS-сервер імен на той, який вони контролюють.
- Погані суб'єкти можуть змінити запис A для IP-адреси вашого домену, щоб замість цього вказувати на їх адресу.
- Зловмисники можуть зламати маршрутизатор організації та змінити DNS-сервер, який автоматично передається на кожен пристрій, коли користувачі входять у вашу мережу.

Протягом багатьох років зловмисники успішно розгортали різні атаки на основі DNS проти мереж компанії та їх користувачів. Зловмисники часто використовують DNS для встановлення команд та контролю (C2) ботнет мережі. Це може призвести до отримання несанкціонованого доступу до мережі, переміщення в бік або вилучення даних.

*Алгоритм генерації домену (DGA):* зловмисники розробляють DGA, щоб зловмисне програмне забезпечення могло швидко створити список доменів, які можна використовувати для надання інструкцій та отримання інформації від зловмисного програмного забезпечення [14]. Зловмисники часто використовують DGA, щоб вони могли швидко змінювати домени, які вони використовують для атак зловмисного програмного забезпечення, оскільки програмне забезпечення та постачальники намагаються якомога швидше заблокувати та знищити шкідливі домени.

*Швидкий потік (Fast Flux):* зловмисники встановлюють кілька IP-адрес для кожного зловмисного доменного імені та швидко змінюють їх, щоб уникнути контролю за IP-адресами, що ускладнює пошук загроз для пошуку їх місцезнаходження.

*Шкідливі нещодавно зареєстровані домени (NRD)* – це будь-який домен, який був зареєстрований за останній місяць. Зловмисники часто створюють невеликі варіації законних доменів, намагаючись обманути користувачів, щоб вони натиснули на них. Шкідливі NRD зазвичай активні лише протягом короткого періоду часу, що ускладнює їх виявлення.

*Атаки переприв'язування DNS:* успішне використання атаки переприв’язування DNS перетворює браузер жертви на проксі-сервер для атаки перевірених пристроїв у приватній мережі користувача для подальших атак на пристрої, які, на думку окремої особи або організації, є недоступними для зловмисників. Атаки переприв’язування DNS не так добре відомі або не сприймаються організаціями так само, як експлойти «XSS», і тому багато організацій можуть не мати чітких дій щодо їх захисту.

Цей вид атаки в основному використовувався для вразливих пристроїв Інтернету речей споживчого рівня (IoT), таких як системи домашньої автоматизації та споживчі камери відеоспостереження, які в подальшому зловмисники використовували для атаки на корпоративні мережі. Зловмисникам важко націлюватися на краще підтримувані та перевірені корпоративні мережі, але також і винагороди. Оскільки атаки з переприв’язуванням DNS покладаються на комбінацію двох факторів, які організації зазвичай не враховують і не обмежують: той факт, що браузери зазвичай виконують будь-який JavaScript, наданий за замовчуванням і без підказки або дозволу користувача, а також прийняття клієнтами та міжмережевим екраном відповідей DNS з низьким значення TTL поза мережею.

Для використання переприв’язування DNS, зловмисник може використовувати браузер жертви як проксі-сервер для доступу до перевірених пристроїв локальної мережі. Сканувати локальні IP-адреси на наявність пристроїв і націлювати конкретні пристрої з подальшими атаками з привілейованої мережі. Багато пристроїв, які представлені в локальних мережах, як правило, мають паролі за замовчуванням, слабкі паролі або, іноді, взагалі відсутню автентифікацію, оскільки вони недоступні зловмисникам у загальнодоступному Інтернеті і тому не вимагають жорсткого контролю, такого як надійна автентифікація.

В ідеальному сценарії для зловмисника вони зможуть повністю скомпрометувати один цільовий пристрій і встановити бекдор канал доступу, наприклад, зворотну оболонку до власного сервера, і використовувати його для подальших атак на інші пристрої в межах екранованого сегмента мережі.

Організації можуть бути самовпевненими і вірити, що лише споживчі мережі слабко захищені технічними засобами контролю, а корпоративні служби та пристрої краще захищені від простих атак. Однак організації продовжують розгортати такі служби, як Redis, MongoDB та memcache, у локальних мережах без аутентифікації – ці служби перекриваються від прямого доступу зловмисників через публічний Інтернет, але можуть бути скомпрометовані через атаки переприв'язування DNS. Усі локальні служби у приватній мережі повинні використовувати надійну аутентифікацію та заходи захисту CSRF. Саме тому, що послуги не доступні безпосередньо в загальнодоступному Інтернеті, слід сприймати як причину не забезпечувати належну аутентифікацію та контроль доступу до них.

**Висновки до розділу 1**

Проаналізовано методи роботи та взаємодії важливих компонентів мережі, які потребують використання сучасних методів захисту DNS запитів, за допомогою стандартів та програмних реалізації.

Виокремлено основні види мережевих атак, спрямованих на використання недоліків безпеки в інфраструктурі DNS, для перехоплення даних користувачів, види атак отруєння кешу, тунелювання DNS, атаки на посилення DNS та перепривязування DNS.

Зазначено, що DNS – один із важливих та найстаріших компонентів комп'ютерних мереж, основною проблемою якого є відсутність конфіденційності в реалізації технологій, які не відповідають сучасним тенденціям в безпеці. Якщо запити DNS не є захищеними легше цензурувати Інтернет на рівні провайдерів, а зловмисникам стежити за поведінкою користувачів в Інтернеті.

Отримано дані, що локальні служби повинні використовувати надійну аутентифікацію та заходи захисту мережевих служб, тому що послуги не доступні безпосередньо в загальнодоступному Інтернеті, сприймаються як причина не забезпечувати належну аутентифікацію та контроль доступу до них.

# 2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ШКІДЛИВИХ ЗАПИТІВ

## 2.1. Дослідження методів виявлення шкідливих запитів

Кіберзлочинці постійно розробляють все більш складні та небезпечні програми зловмисного характеру для компрометації користувачів комп'ютерної мережі. Хоча DNS історично вважається незахищеним місцем інфраструктури, але він також може бути активною частиною хорошої стратегії глибокого захисту.

Сучасні системи моніторингу комп'ютерної мережі дозволяють відслідковувати всі події які відбуваються в системі, та створювати на базі них алгоритми виявлення та протидії зловмисним запитам.

Виявити шкідливі запити можна за такими параметрами як імена веб-доменів, які використовувалися для роботи зловмисних мереж, таких як ботнети, та інших типів шкідливого програмного забезпечення, і були залучені до шкідливих дій з фішингу та спама. Існує ряд методів і підходів, які використовуються для виявлення доменів для поширення шкідливих запитів.

Ці підходи можуть доповнювати один одного для підвищення рівня точності. Загалом їх можна класифікувати як підходи на основі класифікації та підходи, засновані на висновках. Підхід, заснований на класифікації, передбачає створення класифікатора з використанням функцій домену, які були вилучені з даних DNS. Класифікатор може бути додатково збагачений за допомогою даних, отриманих від функцій мережі або хост-машини. Потім класифікатор можна додатково навчати, використовуючи відомі набори даних шкідливих та нешкідливих доменів, щоб він міг виявляти нові раніше невідомі шкідливі доменні імена.

Підхід, заснований на висновках, передбачає створення зв’язків між доменами за допомогою даних DNS для виділення та визначення наявності значущих зв’язків на основі певних критеріїв. Якщо між доменами існує будь-який

зв’язок, алгоритм висновку використовується для визначення шкідливості домену на основі його зв’язку (прямого чи непрямого) з відомими шкідливими доменами.

В деяких випадках для виявлення шкідливих запитів використовуються методи на основі сигнатур, які ідентифікують зловмисне програмне забезпечення шляхом порівняння потенційної шкідливих запитів з базою даних сигнатур або попередньо знайдених і задокументованих шкідливих запитів. Головна перевага цієї методики в тому, що вона може бути дуже ефективною і швидкою. Основний недолік – шкідливі запити не буде виявлено, якщо вони раніше були невідомі та використовується новий вид шкідливих атак. Оскільки цей метод може виявляти лише шкідливі запити, які насправді було ідентифіковано раніше, воно має дуже низький рівень помилкових спрацьовувань. Однак, оскільки він може виявляти лише зловмисні запити, які було ідентифіковано раніше, воно має високий рівень помилкових негативних результатів.

Використовуючи програми для моніторингу мережевого трафіку працюють системи, які виявляючи будь-який вид діяльності, який не є частиною звичайної роботи сервісів. Програма виявлення аномалій відстежує діяльність системи та класифікує її як нормальну чи аномальну поведінку. Відмінність цього методу від методу на основі сигнатур полягає в тому, що він виявляє шкідливі запити на основі класифікації, а не шаблонів. Основна перевага цього методу полягає в тому, що він може виявляти невідоме зловмисне програмне забезпечення, оскільки він покладається не на базу даних вже ідентифікованих шкідливих запитів, а на виявлення шкідливої поведінки.

## 2.2. Методи протидії шкідливим запитам

Для протидії шкідливому трафіку потрібно сформувати методи що дають змогу захистити сучасні комп'ютерні мережі від шкідливих запитів. Ось кілька основних захисних заходів для протидії шкідливим запитам:

Для початку, щоб захистити мережу, потрібно знати інформацію про всі властивості DNS інфраструктури. Часто мережевим командам не вистачає повної видимості через безлад в системі DNS, та незадокументовані частини мережі.

Потрібно реєструвати та відстежувати DNS-запити та дані відповідей. Реєстрація та моніторинг вихідних і вхідних запитів є першим кроком до виявлення аномалій. Крім того, дані із відповідей надають контекстну інформацію, яка дає змогу провести більш ретельний криміналістичний аналіз.

Додатковий захист рекурсивних DNS-серверів. Захист рекурсивних серверів від небажаного доступу та втручання за допомогою DNSSEC, засобів контролю доступу. Надавши розширений доступ адміністратору до системи DNS. Увімкнувши багатофакторну автентифікацію в обліковому записі реєстратора домену та увімкнути службу блокування реєстратора, щоб отримувати попередній дозвіл, перш ніж змінювати записи DNS.

Кожне підключення, здійснене клієнтськими пристроями до домену, записується в журналі DNS. Перевірка трафіку DNS між клієнтськими пристроями та локальними рекурсивним розпізнавачами може виявити велику кількість інформації для криміналістичного аналізу. Запити DNS можуть виявити: ботнети, зловмисне програмне забезпечення, що підключаються до серверів C&C, які веб-сайти відвідував користувач, до яких шкідливих доменів та доменів DGA було здійснено доступ.

Під час аналізу кожного журналу DNS потрібно перевіряти кожен домен, до якого надсилають запити:

- База даних шкідливих доменів (регулярно оновлюється)
- Алгоритм генерації домену (DGA)

Будь-який домен, який відповідає будь-якому з вищезазначених критеріїв, заслуговує на увагу, і сповіщення генерується разом із клієнтом, який звернувся до нього, та інформацією про геолокацію домену (IP, країна).

Використовуючи аналіз поведінки, відслідковується обсяг підключень до кожного домену, до якого здійснюється доступ в організації. Якщо обсяг трафіку

до певного домену перевищує середній, запускаються сповіщення. Коли доступ до домену здійснюється вперше, перевіряється наступне:

- Динамічний домен
- Дата реєстрації домену
- Зв'язок домену, з відомими вразливими TLD

Останні тенденції показують, що кіберзлочинці можуть створювати динамічні домени як центри управління та контролю. Ці домени активуються на дуже короткий термін, а потім відкидаються, що робить вищенаведені перевірки ще важливішими [16].

Система доменних імен (DNS) робить можливим будь-яке мережеве спілкування. DNS може здаватися невидимою силою або сутністю, доки не відбудеться інцидент, тоді стає зрозуміло, що якщо служба DNS не працює, нічого не працює. Оскільки DNS є опорою мережевих додатків, інфраструктура DNS має бути високо доступною. Щоб виконати важливе резервування, потрібно мати принаймні первинний і вторинний DNS-сервери.

Щоб забезпечити роботу критично важливих сервісів, необхідно мати принаймні два внутрішні DNS-сервери. Усі служби активного каталогу, обміну файлами та електронної пошти покладаються на належну роботу DNS. Без справних і функціональних внутрішніх DNS-серверів внутрішні пристрої не можуть спілкуватися. Якщо один DNS-сервер зіткнувся з проблемою, інший почне автоматично використовувати вторинний DNS, у випадку якщо основний не відповідає. IP-адресою внутрішнього DNS-сервера може бути будь-яка адреса в межах діапазону IP-адрес приватної мережі. Безперервна реплікація з первинних серверів на вторинні забезпечує синхронізацію записів DNS і захист від збоїв. Це дає гарантію, що ніколи не наступить момент, коли для кінцевого користувача будуть недоступні послуг сервісу.

Приховати DNS-сервери та інформацію про DNS допоможе уникнути атак зловмисника який за допомогою інформації про програмне та апаратне забезпечення може використати експлойт вже відомої вразливості, та скомпрометувати систему DNS. Не кожен DNS-сервер і кожна частина інформації

повинні бути доступними для всіх користувачів. По-перше, потрібно зробити доступними лише сервери та дані, необхідні особам, які використовують ці сервери. Це особливо важливо, якщо доменні імена повинні бути видимими для користувачів. По-друге, потрібно відключити доступ до головного DNS-сервера. Основні сервери не повинні бути видимими для зовнішніх користувачів.

Записи для цих серверів не повинні бути доступні в жодній загальнодоступній базі даних серверів імен. Лише вторинні DNS-сервери повинні розглядати запити від кінцевих користувачів. Якщо DNS-сервер доступний із-за меж мережі організації, цей сервер має бути лише авторитетним DNS-сервером. Зовнішнім користувачам не потрібно запитувати ваші рекурсивні DNS-сервери. Відповідь лише на ітераційні запити для відповідних зон, для яких сервер є авторитетним, є високопродуктивною конфігурацією. Нарешті, лише системні адміністратори та IT-персонал повинні мати доступ до основних серверів у організації. Якщо залишити основні DNS-сервери видимими для всіх користувачів, це може стати серйозною проблемою безпеки.

DNS-сервери є частою мішенню кібератак. Захист інфраструктури DNS є важливим кроком у запобіганні злому у вашій організації. Щоб уникнути серйозного впливу на налаштування DNS, не забудьте застосувати заходи безпеки, наведені нижче.

*Увімкнення ведення журналів DNS.* Журнал DNS є найефективнішим способом моніторингу активності DNS. Журнали дають вам знати, якщо хтось втручається у ваші DNS-сервери. Окрім активності клієнта, журнали повідомляють про проблеми із запитами або оновленнями DNS.

Журнали DNS також показують інформацію яка може допомогти в знаходженні атаки отруєння кешу. У цьому випадку зловмисник змінює дані, що зберігаються в кеші, і відсилає клієнтів на потрібний ресурс. Наприклад, IP-адреса www.youtube.com може бути змінена на IP-адресу шкідливого сайту. Коли клієнт надсилає запит до DNS для youtube.com, сервер повертає неправильний IP. Потім користувачі відвідують веб-сайти, які вони не хотіли відвідувати, і стають мішенню хакерів.

Незважаючи на те, що журнал налагодження DNS піднімає безпеку на більш високий рівень, деякі системні адміністратори вирішують вимкнути його. Основна причина - підвищення продуктивності. Відстеження активності мережі може допомогти виявити деякі види атак, наприклад DDoS. Тому потрібно завжди вмикати журнали DNS, які допоможуть зібрати інформацію про події в мережевих інтерфейсах.

*Блокувати кеш DNS.* Щоразу, коли надходить запит від клієнта, DNS знаходить інформацію та зберігає її в кеші для подальшого використання. Цей процес дозволяє серверу швидше відповідати на ті самі запити до кореневого DNS серверу. Зловмисники можуть використовувати цю функцію, змінюючи збережену інформацію.

Ще одним кроком від увімкнення журналів налагодження DNS є блокування кешу DNS. Ця функція визначає, коли можна змінити кешовані дані. Сервер зберігає інформацію пошуку протягом визначеного періоду часу TTL. Якщо блокування кешу вимкнено, інформацію можна перезаписати до закінчення терміну TTL. Це залишає місце для атак отруєння кешу.

Залежно від операційної системи блокування кешу може бути ввімкнено за замовчуванням. Шкала блокування кешу зростає до 100 відсотків. Якщо значення встановлено на 70, перезапис даних неможливий для 70% TTL. Якщо для блокування кешу встановлено значення 100, зміна кешованої інформації блокується до закінчення терміну TTL.

*Фільтрація запитів DNS для блокування шкідливих доменів.* Фільтрація DNS один із ефективний спосіб запобігти доступу користувачів до веб-сайту або домену. Основна причина блокування розпізнавання імен для домену полягає в тому, якщо відомо, що цей домен є шкідливим. Коли клієнт надсилає запит на заблокований веб-сайт, DNS-сервер припиняє будь-яке спілкування між ними.

Фільтрація DNS значно зменшує ймовірність проникнення вірусів та шкідливих програм у мережу користувача. Коли клієнт не може отримати доступ до шкідливої сторінки, кількість загроз, які можуть сканувати всередині інфраструктури, мінімальна.

Окрім безпеки, функціональні можливості дозволяють заблокувати домен через бізнес-політику або з міркувань продуктивності. Список заблокованих доменів може включати соціальні мережі, сторінки потокового відео чи будь-який інший веб-сайт. DNS може фільтрувати запити за користувачем, групою або заблокувати доступ для всіх користувачів.

Сучасні рішення щодо безпеки програмного забезпечення та брандмауера включають фільтрацію DNS як стандарт. Деякі з цих пристроїв надають регулярно оновлювані списки несправних доменів. Використовуючи готове програмне рішення, автоматизувавши фільтрацію DNS і уникнути додавання нових записів вручну. Для формування списку фільтрацій доменів

*Перевірка цілісності даних DNS за допомогою DNSSEC.* Розширення безпеки системи доменних імен (DNSSEC) гарантують, що клієнти отримують дійсні відповіді на свої запити. Цілісність даних досягається за допомогою цифрового підпису DNSSEC даних DNS, які надаються серверам імен. Коли кінцевий користувач надсилає запит, DNS-сервер надає цифровий підпис з відповіддю. Таким чином, клієнти знають, що отримали достовірну інформацію для надісланого ними запиту.

Цей додатковий рівень безпеки допомагає відбиватися від атак протоколу DNS. Оскільки DNSSEC забезпечує цілісність даних і повноваження походження, атаки підробки DNS і отруєння кешу успішно запобігаються. Тоді клієнти впевнені, що відвідують сторінки, які збиралися відвідати.

*Налаштувати списки контролю доступу.* Списки контролю доступу (ACL) – це ще один спосіб захисту DNS-серверів від несанкціонованого доступу. Тільки IT-адміністратори та системні адміністратори повинні мати доступ до обслуговування основного DNS. Налаштування списків керування доступом, щоб дозволити вхідні з’єднання з сервером імен із певних хостів, гарантує, що лише призначений персонал може спілкуватися з серверами організації.

Крім того, списки ACL повинні визначити, які сервери можуть здійснювати перенесення зон. Зловмисники можуть спробувати визначити налаштування зони, надіславши запити на перенесення зони через вторинні сервери DNS. Якщо сервіси

заблокують всі запити на передачу зони через вторинні сервери, зловмисник не зможе отримати інформацію про зону. Така конфігурація не дозволяє третім сторонам отримати уявлення про те, як організована внутрішня мережа.

Завжди є можливість вдосконалювати дизайн DNS та безпеку вашої інфраструктури. Постійні загрози ховаються та чекають, щоб використати вразливості у системі. Користувачі зловмисного програмного забезпечення намагатимуться використати будь-яку службу чи протокол, а DNS пропонує прихований шлях для вилучення даних та оновлення шкідливих програм. Одноразові або скомпрометовані доменні імена використовуються в компаніях зі спамом, керуванні ботнет мережами, фішингу та завантаженні шкідливих програм. Шкідливі запити отруюються, щоб порушити процеси розпізнавання імен і використовувати сервери імен для своїх потреб.

Склад запитів і шаблони трафіку можуть вказувати на DoS-атаки, використання сервера імен або розпізнавача, неправильну роботу пристроїв, заражені хости, доставку шкідливих даних, отруєння відповідей або контроль бот-мереж у вашій мережі.

*Розподілена атака відмови в обслуговуванні (DDoS).* Запити з адрес, які ви не авторизували для використання і які не фільтрують вихід, є можливими ознаками атак DDoS, особливо якщо вони збігаються з великим обсягом запитів DNS або запитами, які використовують протокол керування передачею (TCP) замість протоколу дейтаграм користувача (UDP). Запити з підроблених адрес також можуть вказувати на DDoS [15].

*Атака сервера імен або розпізнавача*. Неправильно сформовані запити DNS можуть бути викликані декількома діями, включаючи використання вразливостей сервера імен або роздільника, визначених IP-адресою призначення. Ці запити також можуть свідчити про те, що пристрій у мережі не працює належним чином або про невдалу спробу видалити зловмисне програмне забезпечення.

*Заражені хости.* Запити, які надіслані неавторизованим розпізнавателями, є вагомими ознаками інфікованого хоста у вашій мережі. Ви також можете побачити запити із запитом на вирішення відомих зловмисних доменних імен або імен із

загальними характеристиками алгоритмів генерації домену (DGA), які вже пов’язані з діяльністю зловмисного програмного забезпечення.

*Доставка шкідливих даних.* Надзвичайно великі повідомлення-відповіді часто зустрічаються в атаках посилення, спрямованих на малу кількість або низький рівень ресурсів. Ненормальні відповіді в розділах «Відповідь» або «Додатково» можуть бути викликані спробами отруєння кешу або прихованими каналами. Відстеження характеристик довжини та складу ваших відповідей DNS може інформувати вас про зловмисні наміри.

*Зміна відповіді DNS.* Якщо відповіді DNS демонструються для ваших власних доменів, які розв’язують незнайомі IP-адреси, або відповіді від серверів імен, на розміщення яких ви не уповноважені, можливо, зовнішні сторони змінили відповіді. Ці відповіді також можуть свідчити про викрадення вашого реєстраційного облікового запису. Іншою ознакою модифікації відповіді або захоплення є позитивні відповіді, які мають бути перераховані на NXDOMAIN.

*Контроль ботнету.* Відповіді з IP-адрес, призначених мережі широкосмугового доступу, або інших підозрілих IP-адрес можуть бути ознакою контролю бот-мереж у вашій мережі. Ботнети також можуть викликати появу трафіку DNS на незвичних портах. Ботнети також можуть викликати велику кількість відповідей NXDOMAIN або відповідей, доменів з коротким терміном існування (TTL).

*DNS створює проблеми для традиційного моніторингу.* Традиційні засоби виявлення та запобігання погано обладнані для захисту від такого типу прихованої посткомпромісної діяльності  це одна з причин, чому DNS є таким популярним методом атаки. Реєстрація DNS має численні підводні камені та ускладнення. По-перше, система не дуже добре масштабується. Журнали DNS об’ємні. Один запит DNS може генерувати більше 10 подій на хості Windows. Високі вимоги до обчислень і сховища.

Навіть якщо увімкнено деяке ведення журналу DNS, набір даних не завжди надійний. Якщо DNS розміщено третьою стороною, то служби DNS надають можливість ввімкнути ведення журналу, але знайти джерело запиту надзвичайно

важко. Журнал DNS-серверів даних і формат цих журналів також можуть сильно відрізнятися від сервера до сервера, що ускладнює їх співвіднесення та аналіз.

*Брандмауери.* Брандмауер часто є основним пристроєм безпеки мережі для моніторингу, дозволу або блокування трафіку та даних; однак трафік DNS зазвичай дозволяється проходити через засоби захисту периметра, наприклад брандмауери, які зазвичай блокують вхідний і вихідний шкідливий трафік. Звичайно, можна визначити правило, яке забороняє будь-які запити DNS з IP-адрес за межами виділеного номерного простору, але розширене тунелювання DNS метод атаки, який надсилає хвилі неіснуючих субдоменів на DNS розпізнавача безперервно працюючи за межами кешу, щоб вичерпати його ресурси.

*Системи виявлення вторгнень (IDS).* Традиційний IDS покладається на сигнатури для виявлення зловмисної активності, а це означає, що ці інструменти не можуть динамічно виявляти незвичайну поведінку в порівнянні зі звичайними шаблонами. Це робить C2 на основі DNS привабливою тактикою ексфільтрації для зловмисників, які хочуть уникнути виявлення IDS. Зловмисники використовують DGA і фрагментацію даних, щоб уникнути виявлення за допомогою жорстких підписів IDS, які включають явні IP-адреси, доменні імена або обмеження розміру корисного навантаження.

Рішення виявлення та відповіді мережі (NDR) унікально підходить для виявлення шкідливої активності DNS. На відміну від виявлення на основі сигнатур, яке має бути налаштовано для виявлення загроз, NDR використовує машинне навчання для аналізу мережевого трафіку, щоб встановити базовий рівень, який допоможе зрозуміти, як виглядає нормальна поведінка DNS та підозріла поведінка в будь-якому середовищі. Потім він виявляє аномальну поведінку, яка може означати атаку. Базові показники встановлюються для таких речей, як кількість зроблених запитів, географічні розташування, історія домену та ентропія структур запитів. Відхилення потім можуть бути використані для швидкого визначення діяльності після компрометації.

Візьмемо, наприклад, тунелювання DNS. Хоча трафік DNS, як відомо, є шумним, за допомогою поведінкових базових показників і аналізу машинного

навчання можна відокремити шумний трафік DNS від шумного тунельного трафіку DNS, який ставить під загрозу ваше середовище. Шум від скомпрометованого пристрою може включати безперервні запити до маяка сервера C&C або раптове збільшення обсягу запитів, які зазвичай пов’язані з вилученням даних.

Виявлення машинного навчання та поведінки, які використовуються NDR для виявлення індикаторів компромісу, також можуть бути розширені до межі для більш високоякісного виявлення вторгнень на основі DNS.

DNS-атаки та зловживання DNS є поширеними з певної причини. Вони добре ухиляються від застарілих інструментів безпеки та приховано працюють у мережі. Хоча немає срібної кулі для захисту від них, перегляд моделей поведінки DNS в мережі може виявити діяльність після компромісу, перш ніж це може призвести до порушення даних.

### 2.3. Інструмент виявлення шкідливих запитів

Система виявлення вторгнень (IDS) – це система, яка автоматизує процес виявлення вторгнень. IDS намагається виявити інциденти в системі до того, як порушиться певна політика. Існує багато причин інцидентів у системі, таких як зараження шкідливим програмним забезпеченням, зловмисник який отримує доступ до системи або перевіряє систему на наявність вразливостей, або зловживання системою авторизованими користувачами, що призводить до порушення політики безпеки [17].

Мета IDS полягає в тому, щоб попередити адміністраторів системи про такі інциденти на їх ранній стадії, перш ніж вони завдадуть будь-якої шкоди, і підтримати адміністраторів системи в їх реагування на шкідливі інциденти. Хоча багато інцидентів носять шкідливий характер, інші не є такими, наприклад, користувач може помилково ввести адресу, що призведе до спроби отримати доступ до критичної системи, до якої особа неавторизована. Тому IDS має бути в змозі класифікувати потенційно шкідливі інциденти з достатньою точністю, тобто з низьким рівнем хибно негативних і хибно позитивних результатів. Помилковий

негатив виникає, коли зловмисний інцидент класифікується як невинний, а хибнопозитивний коли невинний інцидент класифікується як зловмисний.

Типовий IDS використовує багато підходів для виявлення інцидентів у системах. Керівництво NIST до систем виявлення вторгнень описує три поширені підходи: аналіз на основі сигнатур, на основі аномалій та аналіз протоколів із визначенням стану.

Системи виявлення вторгнень на основі мережі NIDS відстежує мережевий трафік для окремих сегментів мережі або пристроїв і аналізує мережеві, транспортні та прикладні протоколи для виявлення підозрілої діяльності [18]. NIDS широко розгортаються багатьма організаціями на кордонах своєї мережі. Датчик, який збирає мережеві дані для NIDS, може бути розгорнутий у двох режимах:

- у вбудованому режимі датчик розміщується так, щоб весь трафік проходив через нього;
- перебуваючи в пасивному режимі, датчик отримує копію мережевого трафіку (таким чином можна уникнути збільшення затримки мережевого трафіку).

NIDS надає різноманітні можливості безпеки. Як мінімум, він збирає інформацію про хости в мережі, наприклад, яка операційна система запущена на кожному хості та програмах. NIDS, як правило, має широкі можливості ведення журналів і збору даних. Більшість NIDS використовують кілька методів виявлення, починаючи від сигнатур і закінчуючи поглибленим аналізом загальних протоколів із визначенням стану. Деякі NIDS здатні подолати методи ухилення, які використовуються шкідливими програмами, таким чином підвищуючи точність результатів виявлення. Існують обмеження, пов’язані з NIDS.

Оскільки NIDS відстежує весь трафік в мережі, їх продуктивність є критичною, особливо у великій мережі з високим навантаженням. Насправді NIDS часто використовує кілька шарів фільтрів, щоб зменшити обсяг трафіку, який проходить через дорогий процес аналізу [19]. Це також допомагає підвищити точність виявлення, оскільки зменшує шум у вхідних даних. Іншим недоліком NIDS є те, що він сприйнятливий до деяких атак із залученням великого обсягу

трафіку, наприклад атаки «Відмова в обслуговуванні». Таким чином, здатність протистояти таким видам атак є важливим фактором при розробці NIDS.

*RITA (Real Intelligence Threat Analytics).* При вирішенні питань з виявлення шкідливих запитів в комп'ютерній мережі інструмент під назвою RITA відіграє важливу роль у виявленні комунікацій команди та управління за допомогою аналізу мережевого трафіку. В основному цей інструмент спрямований на те, щоб допомогти організаціям знайти шкідливу активність у своїй мережі. При цьому він виявляє шкідливу активність не за допомогою сигнатур, а в основному за допомогою статистичного аналізу мережевих пакетів.

Кожен набір даних має загальну кількість фрагментів, які він може утримувати, перш ніж повернути дані. Наприклад, якщо набір даних наразі містить 24 блоки даних і налаштовано на утримання максимум 24 фрагментів, то наступний фрагмент, який буде імпортовано, автоматично видалить перший фрагмент перед введенням нових даних. Це призведе до створення бази даних, яка все ще містить 24 шматки. Якщо кожен фрагмент містить годину даних, у вашому наборі даних буде 24 години даних які будуть поділені та відсортовані для зручного аналізу. Зазвичай RITA використовується разом з іншими додатками для візуалізації та глибокого аналізу, і має ряд функцій які допомагають в підготовкі даних для інтеграції з більш комплексними системами виявлення шкідливих даних.

*Brim.* Заснована Стівом МакКенн компанія Brim Security, яка розробила бібліотеку libpcap і є однією із розробників tcpdump, створили додаток на основі моделі плагінів, де плагіни реалізують специфічний для домену досвід взаємодії. Програма значно спрощує роботу навіть з файлами захоплення пакетів (pcap) дуже великих розмірів (рис.2.1.). За допомогою Pcaps файлі, спеціалісти з інформаційних технологій отримують, аналізують та передають дані для усунення несправностей мережі.

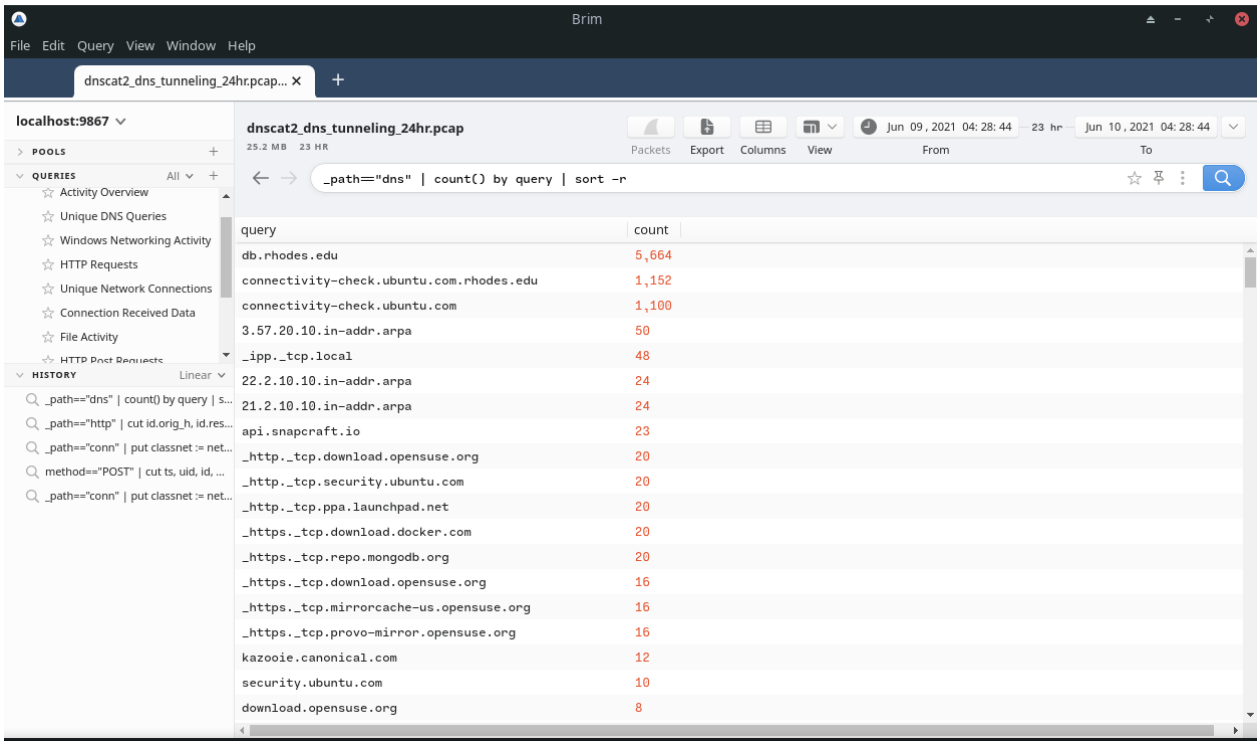


Рис. 2.1. Програмний інтерфейс Brim

Наразі він пропонує засіб для пошуку в записах і журналах великих пакетів через систему аналізу мережевого трафіку Zeek. Користувачі можуть здійснювати пошук у журналах і деталізувати пакети з певного потоку, запустивши tshark який був реалізований у Wireshark. Brim підтримує лише один домен – безпеку, але в активній розробці знаходиться ще декілька доменів. Поки користувач переглядає свої дані, плагін безпеки автоматично запускає похідний пошук у фоновому режимі, наприклад, щоб приєднатися до пов’язаних подій журналу за допомогою поля UID, і представляє ці отримані результати у зручній візуалізації. Цей інструмент в основному використовується для аналізу мережевих пакетів формату NDJSON, Zeek TSV, ZNG, ZSON, CSV, pcap.

*Elastic*. До складу цього додатку входить багато сервісів які допомагають створити зручну систему починаючи з моніторингу трафіка та відслідковування аномальних подій, закінчуючи сервісами з машинного навчання, які допомагають створенню комплексної мережевої безпеки інформаційної системи. Далі буде розглянуто основні компоненти які будуть використані в подальшій роботі:

Агент Packetbeat встановлюється на пристрої, в яких потрібно відслідковувати мережевий трафік та надсилати на платформу Elastic. Packetbeat відрізняється від інших біт-продуктів своїми параметрами способу реалізації. Оскільки інформація, про активність DNS, пасивно отримується з трафіку, отриманого на контрольованому інтерфейсі.

Для роботи з зібраними даними використовується програмний продукт під назвою logstash який отримує масив даних мережевого трафіку та передає їх elasticsearch який взаємодіє з kibana для візуалізації результатів. У разі виявлення шкідливих запитів в інформаційній системі фіксується дані про імя домену, геолокаційні дані, а також дані про зв'язок домена з об'єктами чорного списку. Таким чином результат Elasticsearch можна використати для додавання домену до чорного списку, тому домен більше не зможе використовувати для виконання тунелювання DNS.

Адміністратор мережі зазвичай не приділяє особливої уваги трафіку DNS та інколи забувають про те, що протокол DNS також можна використовувати для обміну даними. Цей недолік використовують зловмисники для «командування та контролю» або крадіжки даних за допомогою тунелювання DNS. Тому трафік DNS в мережі слід відстежувати, та блокувати його, щоб запобігти тунелюванню. Однак це не ідеальне рішення, оскільки цей метод також блокує доступ користувача до адреси хоста. Іншим підходом є використання DNS Sinkhole. DNS Sinkhole – це DNS-сервер, який може надати неправильну IP-адресу (підробку) із запиту DNS, тому до цільового домену більше не можна отримати доступ [20]. Цю умову можна використовувати для запобігання зв’язку з сервером зловмисного програмного забезпечення або тунелю DNS.

DNS Sinkhole використовує список доменів для блокування. Користувачі можуть самостійно скласти список або завантажити його з веб-сайту (наприклад urlblacklist.com, malwaredomain.com. Щоб отримати домен, який підозрюється у DNS-тунелі, необхідно відстежувати та реєструвати весь DNS-трафік у мережі. Ці журнали можна отримати з багатьох ресурсів, таких як DNS-сервер, система виявлення зловмисників (IDS), проксі-сервер і журнал комп’ютера. Щоб виявити

тунелювання DNS з журналу, аналіз слід виконувати вручну, використовуючи пакет аналізатора захоплення, наприклад Wireshark. Такий підхід вважався складним для виконання та потребує часу, особливо якщо ми хочемо візуалізувати результат, нам потрібен інший інструмент. Іншим підходом є використання методу аналізу корисного навантаження та аналізу трафіку. Аналіз корисного навантаження може виявити певні тунелі DNS, тоді як аналіз трафіку може виявити тунелювання DNS універсально.

Аналіз трафіку – це підхід, який ми використовуємо для вирішення проблем, про які ми говорили раніше. Ми використовуємо аналіз трафіку з кількістю унікального імені хоста як індикатор компромісу за допомогою Elastic. Elasticsearch має компоненти, які можна використовувати в цьому дослідженні, такі як Packetbeats, Kibana та Watcher. Packetbeats – це сніфер у реальному часі, який фіксує трафік DNS, Watcher надішле сповіщення електронною поштою, коли відбувається тунелювання DNS, а Kibana – це панель візуалізації, яка показуватиме графічну панель доменних імен, які мають найбільш унікальне ім’я хосту. Сподіваємося, що ця комбінація допоможе адміністратору захищати мережу та контролювати її.

*Zeek.* Представляє собою програму з відкритим вихідним кодом для аналізу мережевого трафіку, яка найчастіше використовується для виявлення поведінкових аномалій у мережі з метою забезпечення кібербезпеки інформаційних систем.

Zeek надає можливості, подібні до систем виявлення мережевих вторгнень (IDS), однак, розглядати Zeek виключно як IDS не ефективно описує широту його можливостей. Це пояснюється тим, що Zeek дає змогу центрам операцій безпеки (SOC) робити набагато більше, включаючи виконання реагування на інциденти, криміналістичну експертизу, вилучення файлів та хешування серед інших можливостей.

Досвідчені спеціалісти з інформаційних технологій визначають Zeek IDS як механізм аналізу та класифікації мережевого трафіку. З цієї точки зору Zeek виконує два ключові завдання, які приносять користь організаціям безпеки:

- Перетворює дані про мережевий трафік у події вищого рівня;

- Надає інтерпретатор сценаріїв – надійну мову програмування, яка використовується для взаємодії з подіями та розуміння того, що ці події означають з точки зору безпеки мережі.

Іншими словами, Zeek фіксує метадані про активність у мережі, а потім надає мову програмування, щоб зрозуміти, коли ця діяльність представляє зловмисні чи підозрілі ознаки.

Потім за допомогою метаданих створюються журнали, в яких записується все, що Zeek розуміє про діяльність мережі. Це розуміння включає записи підключення, обсяг переданих і отриманих пакетів, атрибути сеансів TCP та інші метадані, корисні для аналізу поведінки мережі та розуміння контексту цієї поведінки. Ось чому мова програмування Zeek настільки вигідна її можна використовувати для налаштування інтерпретації метаданих відповідно до конкретних потреб організації.

Хороший спосіб зрозуміти, чому це настільки унікально, порівняти його зі звичайними системами IDS на основі правил, такими як Suricata або Snort. Класичним варіантом використання цих інструментів є моніторинг трафіку на цільовому порту за певним атрибутом – певним протоколом або шаблоном байтів, які існують у корисних навантаженнях пакетів. Коли ці умови відповідають правилу, IDS запускає сповіщення.

Zeek надає спосіб виконувати ті ж типи перевірок для атрибутів трафіку, але з додатковим значенням програмного інтерфейсу. Це означає, що Zeek можна використовувати для обчислення числової статистики та відповідності шаблону регулярних виразів.

Функціональні можливості Zeek не закінчуються лише на моніторингу мережевого трафіку, за допомогою реагування на інциденти та криміналістичної експертизи в одному місці. Наприклад, якщо федеральні правоохоронні органи сповіщають підприємство про докази того, що система спрямовується до шкідливого домену, який вони відстежують, Zeek може визначити, яка машина відповідає на запити, таким чином допомогти виявити вразливий компонент комп'ютерної мережі.

Оскільки Zeek веде запис мережевих транзакцій, користувач може повернутися назад і подивитися, як відбулася низка подій, що призвели до цього повідомлення. Ця процедура схожа на судово-медична експертиза яка допомагає визначити поведінку машини перед визначенням шкідливого додатку та зрозуміти, чи зачепила проблема інші машини, та які з них могли бути зараженими раніше.

Сьогодні насправді немає нічого схожого на Zeek. Він забезпечує перевірку трафіку в режимі реального часу для широкого спектру протоколів, а також функціонує як мережевий реєстратор і інструмент збору даних з можливістю виконувати автономний аналіз.

Поширеним випадком використання Zeek є виявлення відхилень у поведінці мережі. Кілька прикладів включають внутрішній хост, який раптово починає спілкуватися з машиною вперше в історії, спілкується з більшою кількістю хостів, ніж зазвичай, або використовує інший або незвичайний протокол.

Хоча цей широкий варіант використання є досить поширеним, однією з великих переваг Zeek є його здатність налаштовуватися під унікальні середовища.

Система точок продажу (POS) є небезпечною для роздрібних продавців, які прагнуть захистити дані кредитних карток, щоб уникнути як фінансових збитків, так і негативних регуляторних наслідків. Zeek можна налаштувати для моніторингу тих систем, що використовуються для транзакцій з кредитними картками, і розуміння, які протоколи використовуються і які системи повинні спілкуватися одна з одною за звичайних обставин. Іншими словами, він характеризує, як виглядає типова модель трафіку до та з POS-терміналів, що дозволяє йому визначити, коли ці моделі відхиляються. Це можна використовувати, щоб швидше помітити потенційні проблеми, а в разі компромісу зрозуміти вплив на дані та масштаби впливу.

## Висновки до розділу 2

Досліджено методи та засоби виявлення шкідливих запитів в комп'ютерній мережі. Проаналізовано підходи, що можуть доповнювати один одного, для підвищення рівня точності виявлення аномалій мережевого трафіку.

Виокремлено методи протидії відомим атакам, що можуть завдати фінансових або репутаційних збитків, у разі якщо проблемам пов'язаним з захистом мережевої інфраструктури буде приділено занадто мало уваги.

Зазначено, що сучасні інструменти моніторингу комп'ютерних мереж дозволяють відслідковувати всі події, які відбуваються на мережевому інтерфейсі для виявлення зловмисних запитів спрямованих на комп'ютерну мережу.

Отримано результати розглянутих інструментів для подальшої роботи: Zeek – для збору та роботи з пакетами мережевого інтерфейсу, Elastic – для аналізу та виявлення шкідливих запитів за рахунок великої кількості функції. Інші інструменти будуть використовуватись для статичного аналізу пакетів та обробки даних подальших досліджень.

# 3 ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ШКІДЛИВИХ ЗАПИТІВ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

## 3.1. Розгортання технологій виявлення шкідливих запитів

Для виявлення шкідливого трафіку в комп'ютерних мережах більшість спеціалістів використовують інструменти для автоматизації збору та подальшого аналізу трафіку. Існує два методи збору даних DNS для аналізу. Система виявлення передає модулі даних DNS або пасивно захопленим DNS-трафіком мережевого інтерфейсу, або зчитує наявні файли PCAP через аналізатор.

Використовуючи інструмент моніторингу мережі Zeek, для збору інформації про пакети з мережевих інтерфейсів у форматі лог файлі, та вказавши параметри конфігурації для обробки даних з пакетів, всі дані зберігатимуться у форматі JSON. Це дозволить передати у зручному вигляді дані отримані з мережевих інтерфейсів, зменшити час на їх обробку та зручний пошук потрібної інформації.

Обробляти велику кількість даних в JSON форматі дозволяє програмний компонент під назвою logstash, який має можливості збирати, опрацьовувати та віддавати оброблену інформацію агентам для синхронізації з платформою Logz.io за допомогою Filebeat(Beats).

Платформа Logz.io використовується для керування журналами, моніторингом інфраструктури та взаємодії з Cloud SIEM, щоб уніфікувати завдання моніторингу, усунення несправностей та безпеки.

Наступним етапом у розгортанні технологій для виявлення шкідливих запитів у інформаційних системах виступає платформа Elastic, яка отримує від Logz.io відфільтровані дані що використовуються для подальшого їх аналіза.

Як показано на (рис.3.1.), розглянуті технології утворюють комплекс технічних засобів для збору, аналізу та виявлення шкідливих запитів в комп'ютерних мережах.

Для досліджень отриманих даних Elastic пропонує можливості машинного навчання які надають змогу створити патерни що допоможуть обрати найкращий класифікатор для швидкого виявлення аномалій та зловмисних атак.

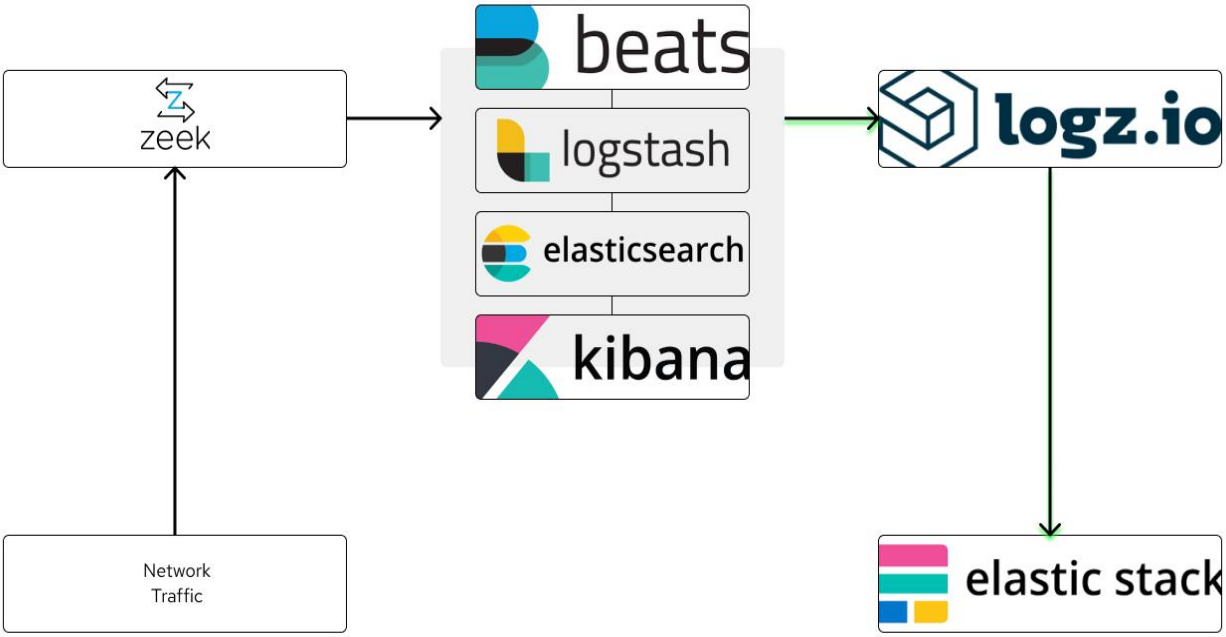


Рис.3.1. Процес аналізу мережевих даних

Завдання машинного навчання виявити рідкісний і незвичайний запит DNS, який вказує на мережеву активність із незвичайними доменами DNS. Це може бути пов’язано з початковим доступом, збереженням, командно-контрольною діяльністю або ексфільтрацією (рис. 3.2.).

Наприклад, коли користувач натискає посилання в фішинговому електронному листі або відкриває шкідливий документ, може бути надіслано запит на завантаження та запуск корисного навантаження з незвичайного домену. Коли зловмисне програмне забезпечення вже запущене, воно може відправляти запити до зловмисного домену DNS, який використовує програмне забезпечення для зв’язку з сервером команд та управління.

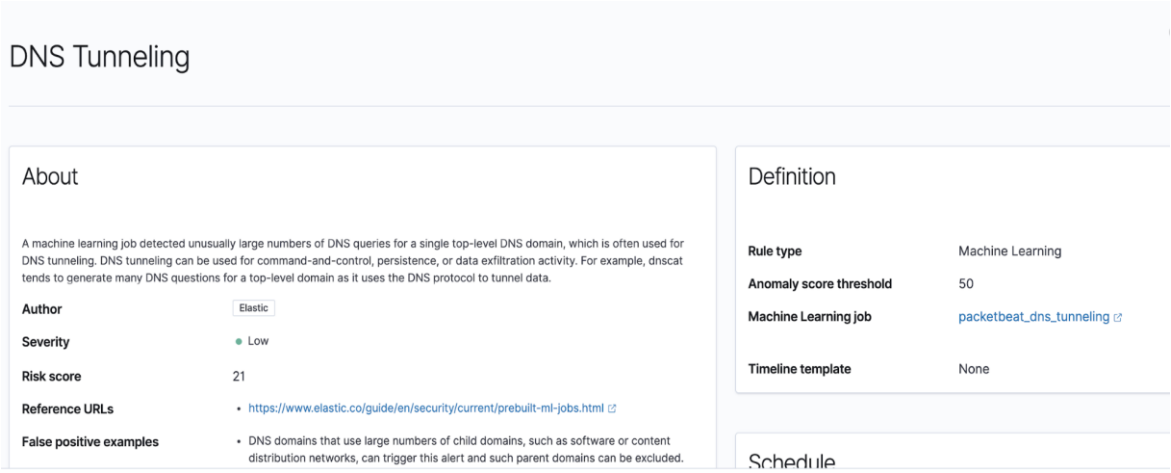


Рис. 3.2. Створення ML задачі

Завдання машинного навчання виявити надзвичайно велику кількість запитів DNS під час використання  тунелювання DNS, це можна використовувати для командно-контрольної діяльності, збереження або вилучення даних. Наприклад, dnscat2 має тенденцію генерувати багато запитань DNS для домену верхнього рівня, оскільки використовує протокол DNS для тунелювання даних.

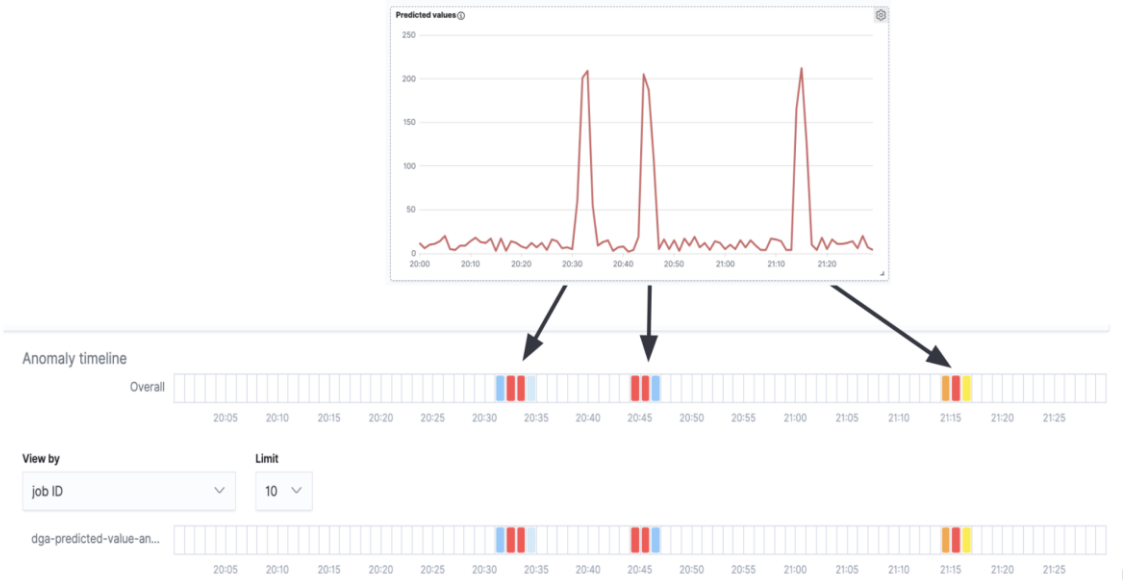


Рис. 3.3. Звіт аномалій при роботі з dnscat2

Слід зазначити, що часто, коли зловмисне програмне забезпечення DGA активно намагається зв’язатися з сервером C&C, воно має тенденцію одночасно генерувати хвилю запитів DNS (рис. 3.3.).

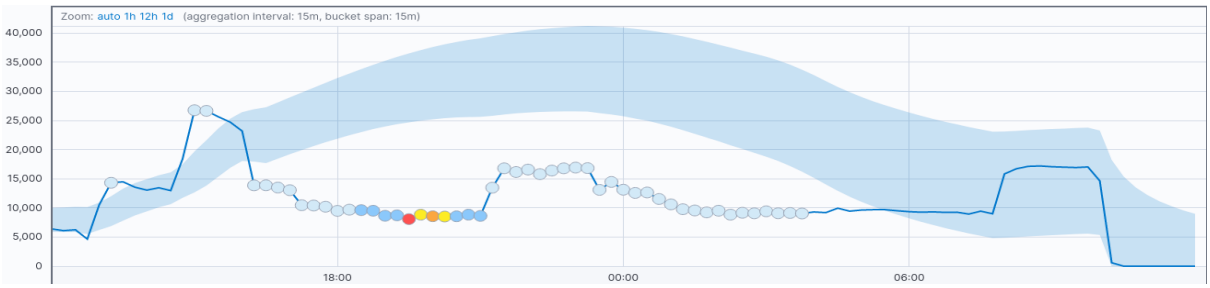


Рис. 3.4. Графік активності шкідливих доменів

У аналізі часових рядів передбачуваних шкідливих доменів з часом спостерігаються піки активності та невеликий шум між піками. Піки вказують на те, що модель класифікувала багато доменів як шкідливі за короткий проміжок часу, і, таким чином, отримали дані справжньої DGA активності, яка продемонстрована на (рис. 3.4.).

На цьому етапі буде проведено аналіз, щоб з’ясувати, чи зможе Elasticsearch виявити DNS тунелювання чи ні. Застосований метод аналізу трафіка. Кожний запит в DNS-тунелі буде створювати нове ім’я хоста, нормальна середня кількість унікального імені хоста нижче 250, через що більш унікальне ім’я хоста вказує на тунелювання DNS. Усі журнали записані та будуть оброблені Watcher за допомогою спеціального сценарію. Після цього Watcher підраховує кількість унікальних назв на основі потужності домену. Кількість унікальних імені хоста в домені візуалізується в Kibana у вигляді графічної панелі. Якщо кількість унікального імені хоста більше 250 і домен не існує в списку довірених доменів, буде надіслане електронне повідомлення з інформацією про виявлені аномальні показники.

### 3.2. Аналіз шкідливих запитів в комп'ютерних мережах

Змоделювавши сценарій та головну мету атаки, яка була спрямована проти системи виявлення шкідливих запитів на етапі тестування та оцінки. Слід пам'ятати, що в сценарії TCP через DNS відправляється значна кількість запитів DNS, що робить його помітним для систем виявлення вразливостей. У

користувацьких сценаріях ексфільтрації DNS та сценаріях командування та контролю зловмисник надсилає обмежену кількість запитів DNS, що робить його менш помітним і системі важко виявляти підозрілі дії, які відбуваються по відношенню до комп'ютерної мережі.

Використовуючи інструмент dnscat2, який продемонстровано на (рис. 3.5.), та обрано як сучасну службу для створення атаки на основі DNS. Для генерації штучних даних, щоб дослідити атаки, було створено віртуальний сервер з операційною системою Ubuntu та встановлено програмний додаток dnscat2, який буде взаємодіяти з хост машиною, яка працює на системі Arch Linux разом з Wireshark.

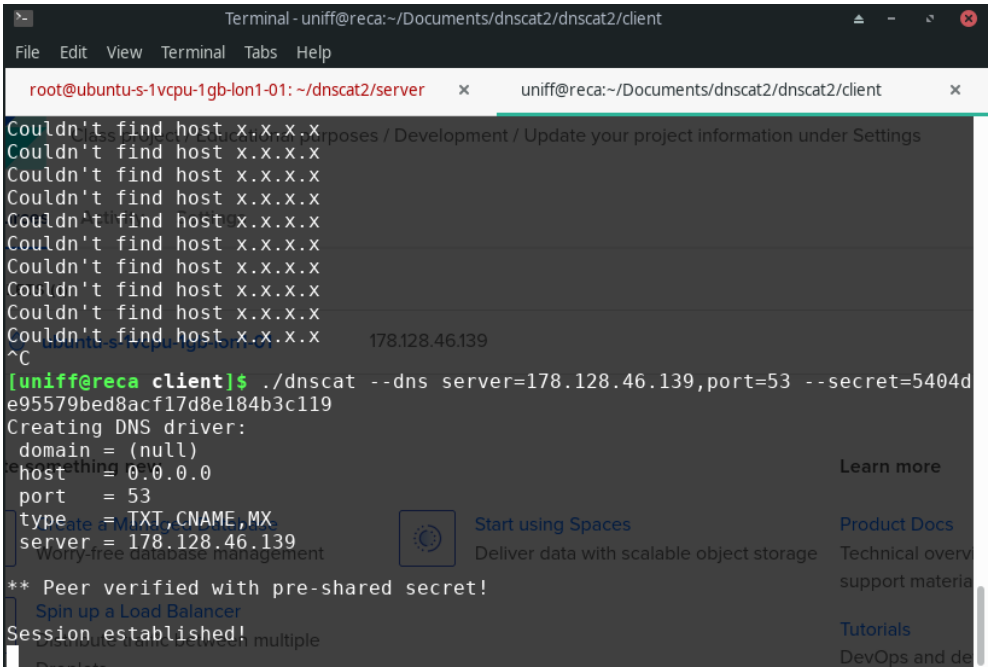


Рис. 3.5. Генерація запитів dnscat2

Щоб оцінити ефективність методів виявлення вразливих запитів, створимо звичайний набір даних DNS. Мережеве середовище для проведення розгортання технологій виявлення шкідливих запитів було встановлено. Зібравши DNS-трафік протягом однієї неділі, підготовлено його для аналізу (рис. 3.6.). Є дві важливі причини для захоплення звичайного трафіку DNS в експерименті. Перша причина полягає в тому, щоб порівняти та вивчити нормальну поведінку трафіку DNS з трафіком DNS, який має атаку тунелювання DNS, тоді як друга причина полягає у

визначенні та встановленні значення порогу на основі нормального рівня трафіку DNS.

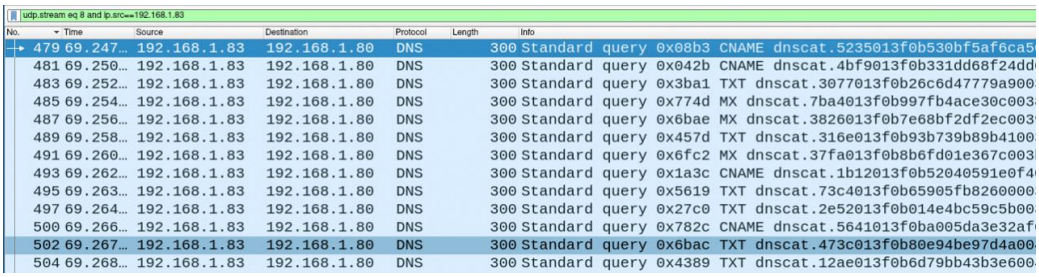


Рис. 3.6. Результати збору даних тунелювання

Через важливість протоколу DNS інструменти тунелювання DNS використовувалися для моделювання атак тунелювання різними методами. Наприклад, інструмент тунелювання DNS (dns2tcp) використовує типи записів TXT для виконання тунелювання, тоді як інструмент тунелювання Iodine DNS використовує записи NULL. Зібравши власний набір даних було розпочато впровадження наборів даних DNS, які містять шкідливий трафік DNS. Набір даних тунелювання DNS включає різноманітний трафік DNS, створений інструментами тунелювання DNS, включаючи Iodine, DNScat2, dns2tcp і fraud-bridge, які описані в Таблиці 3.1. Нарешті, звичайні та шкідливі набори даних DNS об’єднуються, а потім імпортуються в систему виявлення та оцінюються.

Система виявлення складається з двох модулів виявлення: модулів корисного навантаження та аналізу трафіку. Кожен модуль використовує базове значення для визначення аномальної активності. Наприклад, у модулі аналізу корисного навантаження встановлюється базове значення повної довжини кваліфікованого доменного імені на 30 символів. Це значення вибрано на основі рекомендацій експертів з кібербезпеки компанії DG Security. Однак тепер потрібно обрати, яке порогове значення кількості запитів DNS використовувати протягом певного періоду часу для ідентифікації шкідливих доменних імен для модуля аналізу трафіку.

Таблиця 3.1

Інструменти симуляції атак

| Інструменти | Симуляція сценарію | Мета |
|---|---|---|
| iodine | TCP через DNS | Встановлення захищеного з'єднання VPN |
| dns2tcp | TCP через DNS | Встановлення захищеного з'єднання VPN |
| DNSExfiltrator | Техніка ексфільтрації DNS | Вилучення конфіденційних даних |
| Cobalt Strike | Командування та контроль | Виконувати команди та завантажувати файли |
| dnscat2 | Командування та контроль | Виконувати команди та завантажувати файли |
| PacketWhisper | Командування та контроль | Вилучення конфіденційних даних |

Порогове значення використовується в модулі аналізу трафіку для навчальних цілей машинного навчання. Після захоплення даних DNS ми генеруємо підписи текстового представлення з візуалізації. Якщо це зловмисний підпис для домену, ми порівнюємо кількість запитів DNS для доменного імені з базовим значенням, а потім позначаємо навчальний набір даних як шкідливий чи нешкідливий. Таким чином, виникає необхідність провести практичні експерименти для вибору найбільш вигідних значень для кількості запитів DNS протягом встановленого періоду. Модуль аналізу трафіку спеціально спрямований на виявлення високопродуктивних тунельних атак DNS за допомогою сигнатур візуалізації та класифікатора машинного навчання.

Атака тунелювання DNS, така як TCP через протокол DNS, зазвичай надсилає велику кількість запитів DNS для встановлення каналів зв'язку. Тому для цих типів атак можна встановити поріг, коли обсяг трафіку DNS на одне або два стандартні відхилення перевищує середньодобовий трафік. Замість цього ми зосередилися на складнішій проблемі визначення порогового значення для

сценаріїв техніки ексфільтрації DNS. Основною причиною цього типу є відправка певної кількості запитів залежно від розміру файлу. Інструмент DNSExfiltrator використовується для імітації атаки ексфільтрації, яка передає файли за межі скомпрометованої мережі для емпіричного визначення порогу. Кілька файлів розміром від 1 КБ до 1 МБ були передані за межі мережі за допомогою інструменту DNSExfiltrator, і була виміряна кількість фрагментів, що представляють запити DNS. У цьому експерименті використовувалися максимальний повний домен 255 байт і максимальна довжина мітки 63 байти. Якщо розміри запитів і міток DNS зменшити до нижчих значень, це призведе до надсилання ще більшої кількості запитів DNS для певного розміру файлу. Порогове значення встановлюється на основі розміру файлу та кількості блоків DNS. Будемо вважати час і розмір важливими факторами в цій оцінці, оскільки етап навчання модуля аналізу трафіку покладається на захоплення даних DNS кожні n хвилин, де налаштування базуються на щоденному мережевому трафіку. Наприклад, припустимо, що зловмисник хоче експортувати текстовий файл розміром 100 КБ з інформацією про вкрадену кредитну картку за межі мережі організації, використовуючи метод ексфільтрації DNS. Файл розміром 100 КБ потребує 600 запитів DNS протягом 25 секунд, щоб успішно вилучити його за межі мережі організації. До того ж системі виявлення потрібно щохвилини фіксувати дані DNS, а для виявлення атаки значення порогу має бути менше 600.

У проведеному експерименті з системою виявлення було обрано, що система аналізу трафіка фіксує пакети DNS кожні 30 секунд, і встановили 100 як порогове значення, припускаючи, що зловмиснику потрібно вилучити файл розміром щонайменше 50 КБ, що приведе до приблизно 300 запитів DNS за 20 секунд. Слід зазначити, що іноді зловмисник може використовувати техніку затримки між кожним запитом DNS, щоб зменшити шум в трафіку, але модуль аналізу корисного навантаження в цій роботі налаштований для відслідковування цих ситуацій (рис. 3.7.).

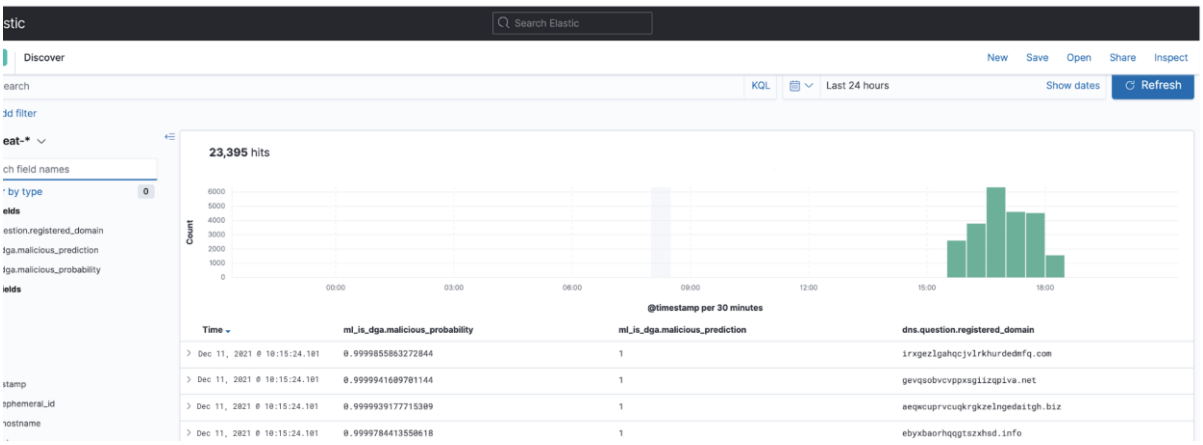


Рис. 3.7. Звіт з отриманих аномалій

Отже, після проведення аналізу шкідливих запитів DNS-трафіку, ми отримали графік виявлених аномалій, серед яких обрали доменні іменна з найвищим індексом, які додамо в чорний список. А також налаштували автоматичну можливість зчитувати трафік DNS з наявних файлів PCAP, щоб ідентифікувати та виявити атаку в автономному режимі з раніше захопленого мережевого трафіку.

### 3.3. Результати реалізації технологій виявлення шкідливих запитів

Провівши дослідження атак тунелювання та ексфільтрація отримані дані було зібрано та відправлено за допомогою додатку Wireshark та Elastic, які застосовувались для збору та виявлення аномальних показників трафіку. Використовуючи Wireshark додатково було отримано дані з мережевого інтерфейсу для більш точного використання їх під час аналізу (рис. 3.7.).

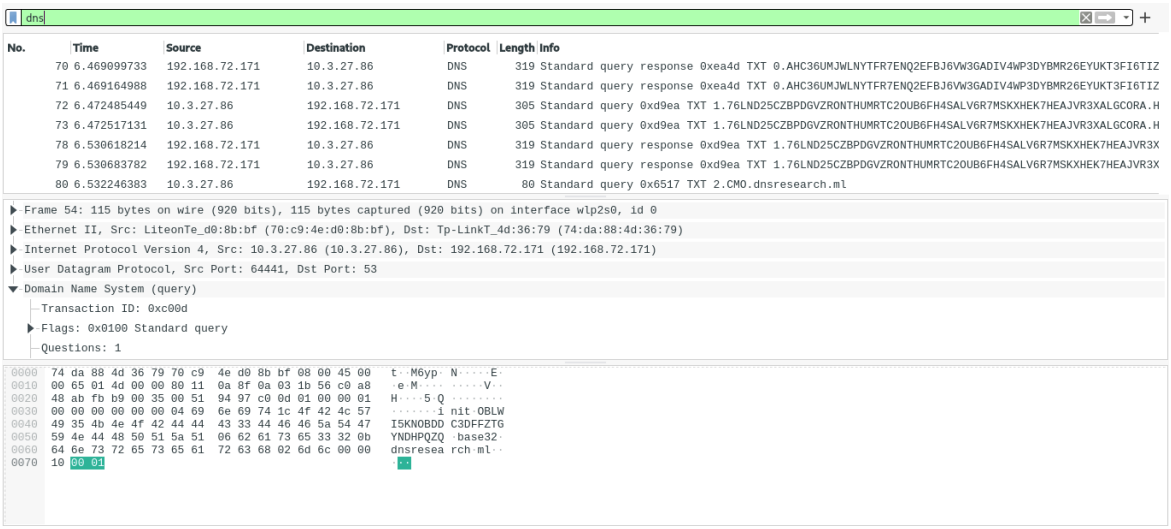


Рис. 3.7. Результат мережевого трафіка DNS тунелювання

Отримавши дані з мережевих інтерфейсів які надалі були відправлені в Elastic для обробки та візуалізації, результатів мережевої активності, під час проведення досліджень (рис. 3.8.).

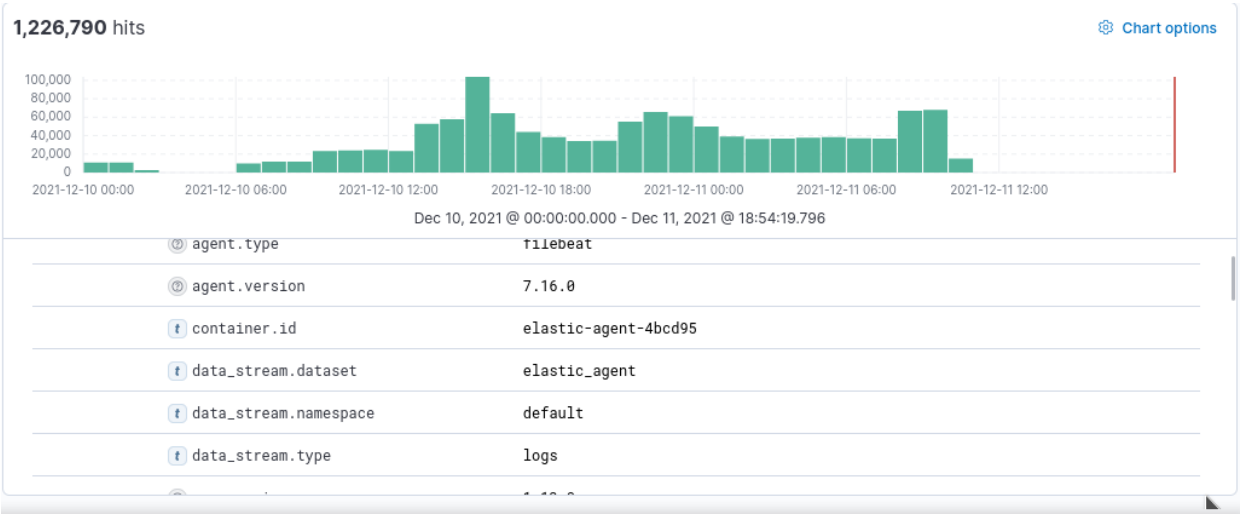


Рис. 3.8. Графік мережевого трафіку при тестуванні

Проаналізувавши дані з отриманих звітів було додано доменні адреси до чорного списку та сформовано нові критерії пошуку шкідливих доменних імен. Результатом виконаної роботи стало розгортання засобів моніторингу мережевого трафіку, що був отриманий за допомогою інструментів створення атак.

Дослідження проводилося в декілька етапі для відхилення даних які не несли дослідницьку цінність.

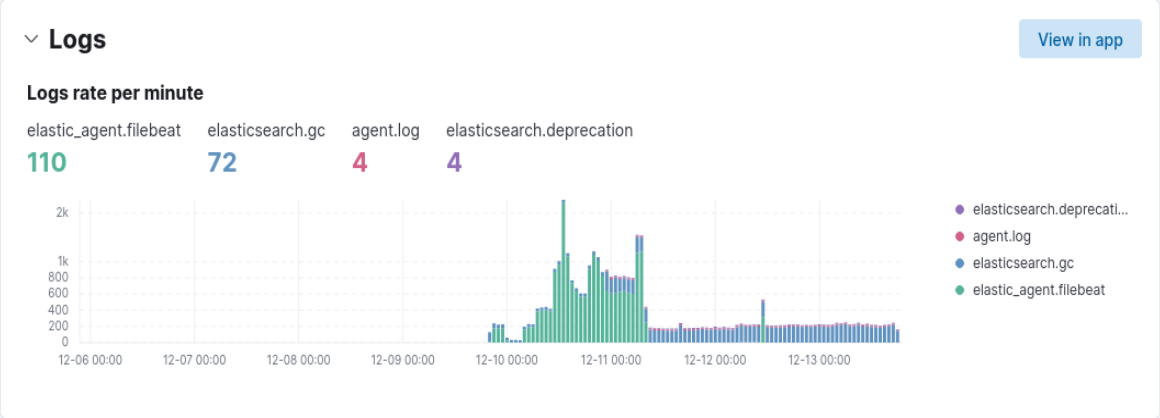


Рис. 3.9. Графік аномалій трафіку

Реалізувавши технології моніторингу DNS-трафіку можна сформувати багато звітів з аномальними даними для команди центру безпеки (SOC), оскільки вони відстежують і аналізують стан безпеки в середині компаній. На додаток до моніторингу брандмауерів і систем IPS для виявлення індикаторів компрометації DNS, інфікованих хостів або спроб тунелювання DNS, команди SOC може розробляти сценарії для протидії та виявленню подібних доменів використовуючи системи DNS фільтрації для створення списків заборонених ресурсів. Що допоможе в майбутньому вберегтись від атак.

## Висновки до розділу 3

Досліджено технології виявлення вразливостей та результати проведення досліджень мережевого трафіку. Впроваджена система виявлення аномалій, спрямована на аналіз мережевих атак на основі DNS.

Проаналізовано два режими виявлення, які спрямовані на атаки тунелювання DNS і ексфільтрацію DNS. Запропонована система виявлення реалізована за допомогою Elastic методів візуалізації та класифікаторів машинного навчання для розрізнення атак на основі DNS.

Виокремлено розробки системи виявлення з використанням візуалізації та машинного навчання.

Зазначено, що існує кілька альтернативних рішень щодо візуалізації мережевого трафіку рідкісних та незвичайних DNS запитів, які вказують на мережеву активність із незвичайними доменами.

Отримано результати реалізації системи виявлення шкідливих запитів комп'ютерних мереж.

# ВИСНОВКИ

В магістерській роботі отримано наступні наукові та науково-практичні результати:

1. Досліджено програмний комплекс Elastic, який використовується для збору та дослідження мережевих пакетів на наявність в них шкідливих запитів, пов'язаних з тунелювання DNS, технікою ексфільтрації DNS та командно-контрольною роботою. Основною метою дослідження в системі є виявлення не тільки високопродуктивних методів тунелювання DNS, але й низько пропускних атак на основі DNS. Ці виявлення були отримані в ході використання програмних засобів.

2. Проаналізовано систему виявлення шкідливих запитів, які можна розбити на такі основні компоненти: візуалізація та виявлення на основі машинного навчання, який надається влаштованими функціями платформи Elastic. Мережевий трафік було отримано за допомогою Zeek та Wireshark протягом одного тижня, щоб створити набір даних для вивчення нормальної поведінки DNS.

3. Виокремлено програмний комплекс Elastik для аналізу мережевого трафіку, який найчастіше використовується для виявлення поведінкових аномалій у мережі з метою забезпечення кібербезпеки інформаційних систем. Також система Elastic надає можливості SIEM систем що спрямовані на виявляйте, дослідження та реагування на мережеві загрози.

4. Зазначено, що в технологіях моніторингу DNS-трафіку формується багато звітів з аномальними даними, які відстежують та аналізують стан безпеки в середині компаній. Моніторинги брандмауерів і систем IPS для виявлення індикаторів компрометації DNS, інфікованих хостів або спроб тунелювання DNS, команди розробляють сценарії для протидії та виявленню подібних доменів, використовуючи системи DNS фільтрації для створення списків заборонених ресурсів і це допоможе в майбутньому вберегтись від атак.

5. Отримано засоби виявлення шкідливих запитів які можуть бути використані фахівцями з кібербезпеки для розгортання систем виявлення шкідливих запитів в комп'ютерних мережах на основі DNS протоколу.

6. Система виявлення має деякі обмеження та недоліки які потрібно усунути в майбутніх роботах. Вразливості проксі-сервер DNS до різних протоколів DNS і атак на сервер, включаючи DoS і DDoS, викрадення сервера, спуфінг DNS і атаки отруєння кешу. Планується, що вирішення цих проблем стане частиною майбутньої роботи зі створення комплексної системи виявлення шкідливих запитів використовуючи власні алгоритми машинного навчання, наприклад, рандомізації вихідного порту та транзакції, щоб запобігти атакі отруєння кешу DNS. Крім того, в майбутньому потрібно розглянути та впровадити DNSSec, додатковий рівень безпеки до існуючого протоколу DNS, щоб підтвердити ланцюг довіри за допомогою криптографії з відкритим ключем для аутентифікації та цілісності даних, а також підвищити загальний рівень системи виявлення шкідливих запитів.