УДК 004.7

Т.І. Коробейнікова, Т.Б. Федчук

ОГЛЯД ПИТАННЯ БЕЗПЕЧНОГО ДОСТУПУ ДО РЕСУРСІВ СИСТЕМИ ДОМЕННИХ ІМЕН

Національний університет «Львівська політехніка»

Анотація. Система доменних імен (DNS) виконує перетворення IP-адреси сервера у доменне ім'я, що дозволяє користувачам отримувати доступ до ресурсів без необхідності запам'ятовувати їх IP-адреси. Цей протокол є невід’ємною частиною сучасного Інтернету. Однак, усі комунікації між клієнтом та сервером відбуваються по незашифрованому каналі, що робить їх вразливими до різних атак, таких як: Spoofing, Eavesdropping, Phishing та інших. Для подолання даної проблеми було розроблено протоколи DNSSEC (DNS Secure), DoT (DNS over TLS) та DNS over HTTPS (DoH). Серед них останній, DoH, найкраще справляється із забезпеченням безпеки DNS-даних. DoH шифрує DNS-трафік між клієнтом та сервером та забезпечує конфіденційність та цілісність даних. Однак це призводить до проблеми у правильному визначенні DoH-трафіку. В даній статті будуть описані засоби дослідження виявлення та аналізу небезпечного DNS-трафіку, що базуються на основі аналізаторів трафіку та методу ML. Запропоную комбіновану методику для подолання загроз та подані порівняльні характеристики протоколів безпеки DNS. Таким чином існує необхідність у застосуванні гібридного методу дослідження шкідливого DNS-трафіку, що базується на комплексному використанні аналізаторів трафіку, машинного навчання та людського досвіду для отримання статистичних даних. Тому ця область досліджень є важливою а також малодослідженою в аспекті безпеки доменних структур. Ціллю даного дослідження є продовження розвитку та вивчення технології DNS за допомогою протоколів шифрування та ідентифікації, а також аналізу шкідливого трафіку з використанням алгоритмів машинного навчання.

Ключові слова: Хост, інкапсуляція, класифікатори трафіку, Система Доменних Імен, Машинне Навчання, рекурсивний ресолвер.

Abstract. The Domain Name System (DNS) is responsible for translating server's IP address into a domain name, enabling an end user to access a resource without having to remember it’s IP address. This protocol is the basis of the modern Internet, but all messages between the client and the server pass through an unprotected communication channel, which makes it vulnerable to various types of attacks (Spoofing, Eavesdropping, Phishing and others). To overcome this problem, DNSSEC (DNS Secure), DoT (DNS over TLS) and DNS over HTTPS (DoH) protocols were developed. The last one was the most effective. DoH encrypts DNS traffic between the client and the server and also guarantees data integrity and confidentiality. This creates a problem in the correct recognition of DoH traffic. The article will describe research tools for detecting and analyzing malicious DNS traffic based on traffic analyzers and machine learning methods. Comprehensive methods for overcoming threats will be proposed and comparative characteristics of DNS security protocols will be presented. Thus, there is a need to apply a hybrid method of investigating malicious DNS traffic based on the combined use of traffic analyzers, machine learning, and human expertise to obtain statistical data. And that is why this topic of research is relevant, insufficiently researched in terms of the security of domain structures. This work is dedicated to the further development and research of DNS technology using encryption protocols and identification and analysis of malicious traffic, based on machine learning algorithms.

Key words: Host, encapsulation, traffic classifiers, Domain Name System, Machine Learning, recursive resolver.

DOI: https://doi.org/10.31649/1999-9941-2024-59-1-40-53.

Вступ та актуальність

Інформаційні технології стали невід’ємною частиною життя сучасного людства і активно використовуються у повсякденні, професійній діяльності, також в освіті (в т.ч., дистанційній) й науці [1]. Розвиток сучасного Інтернету прискорюється, включаючи значний обсяг веб-ресурсів, що є наслідком грамотно вибудованої ієрархічної системи доменних імен DNS, що є невід’ємною складовою в інформаційних технологіях. Протокол DNS перетворює доменні імена в IP адреси і навпаки. Традиційно запити DNS є незашифрованими, що робить їх вразливими до перехоплення, модифікації чи аналізу.

Методи безпечного DNS-трафіку мають на меті гарантувати безпеку та конфіденційність при функціонуванні системи доменних імен. DNS схильний до різного роду атак, скажімо: Spoofing, Eavesdropping, Phishing [2-5]. Отже, забезпечення безпеки DNS-трафіку стає все більш важливим завданням як у науковій, так і в практичній сфері, оскільки зловмисники використовують сучасні методи та швидкі підходи для прослуховування, перехоплення та крадіжки DNS-даних. [4, 6]

Одним із сучасних засобів подолання вразливостей DNS є DNS over HTTPS (DoH). Відомо, що для підвищення безпеки протоколу DNS застосовують шифрування трафіку і його подальше передавання через прихований складений канал. Зрозуміло, що для успішного проведення досліджень, виявлення та аналізу небезпечного DoH-трафіку найбільш ефективно та актуально використовувати методи машинного навчання.[7].

Згідно проведених досліджень у роботах авторів Qasem Abu Al-Haija, Manar Alohaly, Ammar Odeh, автори показали двоступеневу схему виявлення зловмисного DoH трафіку [6, 8] за допомогою комбінації різних методів навчання, вони пропонують двошарову систему. На першому рівні трафік аналізується за допомогою алгоритму «випадкових лісів» (Random Forest, RF), що дозволяє ідентифікувати його як DoH або не-DoH. На другому рівні, DoH-трафік аналізується за допомогою класифікатора «адаптивних дерев» (Adaboost, ADT), щоб визначити, чи є він безпечним DoH або шкідливим DoH. Дана система працює з мінімальною кількістю ознак, які були відібрані з використанням аналізу головних компонентів (PCA), і зменшує кількість вибірок за допомогою методу випадкової недостатньої вибірки. Експериментальна

оцінка, яку вони провели, показала, що система має високу продуктивність з точністю прогнозування на рівні 99,4%, а також мінімальні часові витрати, які становлять 0,83 секунди для першого шару та 2,27 секунди для другого. Це наштовхує нас на думку, що ефективність машинного навчання у дослідженні DoH-трафіку є високою.

Отже, існує потреба у подальшому дослідженні і розвитку безпеки сервісу DNS із використанням протоколів шифрування, процесів аналізу та визначенню шкідливого трафіку за допомогою алгоритмів машинного навчання (ML, machine learning).

Мета

Метою цього дослідження є ретельний аналіз питання безпечного доступу до ресурсів системи доменних імен, з метою подальшого вивчення способів поліпшення ефективності виявлення та ідентифікації загрозливого DNS-трафіку за допомогою алгоритмів ML для забезпечення безпеки та конфіденційності DNS-даних в межах клієнт-серверних сесій.

Задачі

1. Виконати огляд вразливостей сервісу DNS;
2. Виконати ґрунтовний аналіз протоколів DNS, DoH та DoT;
3. Окреслити розвиток сервісів та протоколів безпечного доступу до ресурсів доменних структур.

Аналіз вразливостей сервісу DNS

Відомо, що кожен комп'ютер в мережі Інтернет має унікальну IP-адресу, що дозволяє іншим комп'ютерам спілкуватися з ним. У початковій стадії розвитку мережі Інтернет користувачі могли отримати доступ до веб-сервера, використовуючи його IP-адресу. Наприклад, для відвідування веб-сайту CloudFlare користувач повинен ввести числову IP-адресу веб-сервера 104.16.132.229, замість символьної cloudflare.com.

У 1980-х роках надзвичайний ріст кількості хостів в Інтернеті призвів до ускладнення процесу запам'ятовування та управління IP-адресами кожного окремого хоста [9]. Paul Mockapetris вирішив цю проблему, запропонувавши систему доменних імен (DNS). Дана система здійснювала перетворення числових ідентифікаторів хостів на символьні альтернативи і навпаки [10].

За оригінальною концепцією, DNS мав ієрархічну структуру подібну до дерева, яка складалася з трьох рівнів: кореневого рівня (Root Layer), верхнього рівня або рівня домену (Top Level Domain – TLD) і авторитетного рівня (Authoritative Layer) [10]. Процес перетворення символьних імен на IP-адресу починається з моменту, коли інтернет-клієнти, а саме веб-браузери, подають DNS-запит і передають його до рекурсивного ресолвера (Recursive DNS resolver), який, у свою чергу, передає запити до декількох ітеративних ресолверів. DNS-ресолвер – це сервер, призначений для прийому запитів від клієнтських машин через веб-браузери. Зазвичай ресолвер відповідає за додаткові запити, щоб задовольнити DNS-запити клієнта. Він має надіслати запит до кореневого ресолвера для домену верхнього рівня (наприклад: .com, .edu, .gov і т. д.). Сервер домену верхнього рівня (TLD) є наступним кроком у пошуку конкретної IP-адреси і містить останню частину імені хоста (наприклад: для сайту example.com сервером верхнього рівня є "com"). Цей самий процес повторюється для ресолвера TLD, який надсилає запит до авторитетного ресолвера, наприклад example.com. Авторитетний сервер імен є останньою ланкою у запиті до сервера імен і, якщо він має доступ до запису, до якого був здійснений запит, він повертає IP-адресу для відповідного імені хоста зворотньо до DNS-ресолвера, який зробив початковий запит. У кінці рекурсивний ресолвер може здійснити запит про піддомен www всередині домену example.com і повернути клієнту його IP-адресу, як показано на рисунку 1.

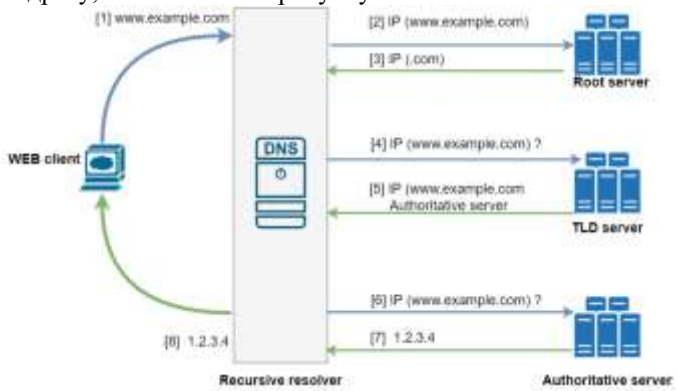

Рисунок 1 – Схема функціонування DNS

DNS-трафік не зашифрований, а запити та відповіді надсилаються у відкритому вигляді (UDP/53), і це означає, що будь-хто може слідкувати за обміном даних. Навіть якщо використовується HTTPS, сам запит DNS не шифрується [11,12]. Такий відкритий вид комунікації дає можливість зловмисникам здійснювати атаки на передані DNS-дані. Протокол DNS не має вбудованих механізмів захисту, що створює очевидні загрози для цілісності, автентифікації та конфіденційності. На рисунку 2 зображена модель потенційних DNS-загроз. Початкові DNS-повідомлення, що передаються мережею, не захищені від втручання і можуть бути заміненими «в реальному часі» нападником, що може залишитися непоміченим для клієнта. Через відсутність автентифікації, зловмисник може прикидатися справжнім DNS-ресолвером за допомогою атаки "людина посередині" (Man In The Middle) [3–4, 13]. Якщо зловмисник успішно виконає таку атаку, він може надсилати клієнту підроблені IP-адреси, що перенаправляють трафік на шкідливі сервери.

Рисунок 2 – Модель потенційної DNS загрози

Додатково, нападники можуть використовувати відсутність конфіденційності в DNS. Якщо зловмисник має контроль над маршрутом DNS-трафіку, він може стратегічно блокувати конкретний потік даних, застосовуючи різні види обмежень (DNS Policy). Ці обмеження можуть фільтрувати запити DNS користувача та згідно з установленими правилами перенаправляти трафік до неіснуючого ресурсу або просто блокувати запит і повертати помилку для клієнта. Ще один, менш активний метод, полягає у захопленні та аналізі DNS-трафіку для збору даних про активність користувача. З огляду на широке поширення DNS-трафіку, це може призвести до повної втрати конфіденційності для користувача Інтернету.

Прогалина у захисті конфіденційності даних впливає не лише на безпеку, а іноді й на права людини [14]. Важливий внесок у збереження конфіденційності особистих даних користувачів внесла постанова GDPR (The General Data Protection Regulation – Загальний Регламент Захисту Даних), яка набрала чинності 25 травня 2018 року і є найсуворішим законом про конфіденційність і безпеку в світі. Незважаючи на те, що він був прийнятий Європейським Союзом (ЄС), цей закон накладає обов'язки на організації у будь-якому регіоні, де вони здійснюють направлення або збирають дані, пов'язані з особами в ЄС [15, 16].

Згідно з Global DNS Threat Report [17], який представив Ромен Фушеро, дослідник із кібербезпеки IDC (International Data Corporation), більше, ніж 88% організацій у всьому світі зазнали атак на систему DNS протягом 2022 року, що в середньому становить 7 атак на кожну організацію. Звіт також показав, що DNS-фішинг, підробка DNS, зараження шкідливим програмним забезпеченням через DNS-трафік та атаки DoS/DDoS були найпоширенішими атаками на сервіс DNS. У результаті таких атак організації в середньому втратили 942 тис. доларів, відповідно до кожної атаки [18].

Аналіз протоколів DNS, DoH та DoT

Для розв’язання проблеми безпеки DNS-даних у 1999 році був розроблений набір специфікацій DNSSEC з метою забезпечення автентифікації кінцевих точок та цілісності даних, однак він залишав проблеми з конфіденційністю не вирішеними. Система DNSSEC перетворювала IP-адресу на доменне ім’я з криптографічною цілісністю. Таким чином, DNSSEC міг бути використаний для імітації або маніпулювання DNS-даними, або ж для дослідження та перенаправлення цих даних. Проте DNSSEC не вирішував проблеми конфіденційності і мав низький рівень впровадження [19].

У минулому протокол HTTP також мав схожі проблеми з безпекою даних, як DNS, і не мав відповідних механізмів безпеки до впровадження SSL (Secure Sockets Layer), а потім TLS (Transport Layer Security). Використання TLS і SSL у HTTP призвело до розвитку протоколу HTTPS. TLS і SSL діють як проміжний шар, забезпечуючи цілісність, шифрування та автентифікацію.

Проміжний шар безпеки TLS відіграє ключову роль для протоколів DoH (DNS over HTTPS) та DoT (DNS over TLS). DoT – це протокол безпеки, який використовує шифрування та інкапсуляцію DNS-запитів і відповідей в стандартний TLS-сегмент транспортного рівня. При використанні DoT на стороні веб-клієнта ініціюється TLS-сесія із ресолвером, що включає перевірку його сертифікатів публічного ключа та обчислення секретного ключа. Після встановлення сесії відбувається обмін зашифрованим DNS-трафіком через порт (TCP/853) [20].

Проте, у 2018 році DoT не став загальноприйнятим стандартом, і DoH не був впроваджений як альтернативний для уніфікованого використання [19]. Однак, криптографічні властивості DoH такі ж, як у DoT, DoH шифрує DNS-трафік для забезпечення цілісності і конфіденційності DNS-з’єднання. На противагу від DoT, DoH передає дані не з трафіком TLS, а за допомогою повідомлень HTTPS. Ці HTTPS-повідомлення передаються через TCP/443, як і звичайний трафік HTTPS [2–5, 21]. Таким чином, можна провести порівняння мережевого стеку протоколів DNS, DoT та DoH. (рис. 3).

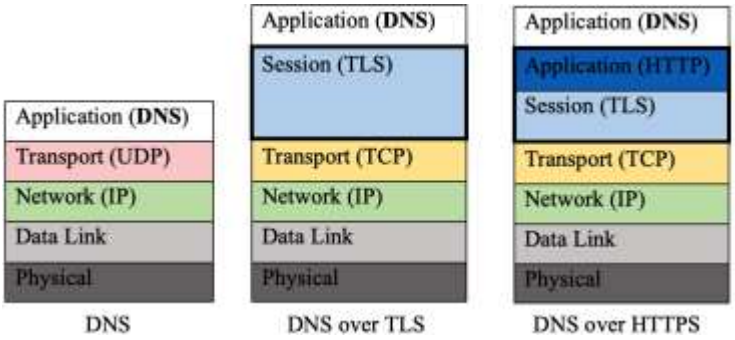

Рисунок 3 – Еквіваленти мережевого стеку протоколів DNS, DoT та DoH у порівнянні [11]

Протокол DoH працює за схемою запит-відповідь, із урахуванням відмінностей між версіями HTTP. HTTP 1.1 офіційно не рекомендований RFC [8] через низьку продуктивність, однак більшість ресолверів та браузерів підтримують його. Головна проблема обмеження продуктивності HTTP 1.1 – це відсутність підтримки декількох одночасних запитів у межах одного з'єднання. Згідно із дослідженнями авторів K. Hynek, D. Vekshin, J. Luxemburk, T. Cejka, A. Wasicek, браузери Chrome версії 94 та Firefox версії 91 зменшують затримку продуктивності, створюючи декілька паралельних з'єднань (зазвичай два). Перемикаючись між цими з'єднаннями, вони можуть виконувати квазіодночасні запити. Згідно з RFC 8484 [8], кожне повідомлення містить лише один DNS-запит або DNS-відповідь. Таким чином, мережеві сканери можуть підраховувати кількість запитів/відповідей, переданих у шифрованому каналі, що надає об’єктивнішу інформацію про обмін DNS-повідомлень [8]. Проте, ніяка інша інформація не може бути безпосередньо отримана з мережевих сегментів, що мають TLS-шифрування.

З огляду на концепцію мережевого рівня, DoH подібний до стандартного обміну даними через HTTPS. Він встановлює з'єднання через TCP/443, проводить TLS handshake та передає дані у зашифрованому вигляді. Це дозволяє аналізувати вміст DNS-запитів та надає додатковий рівень захисту. Типова система, що базується на аналізі DNS-даних – це батьківський контроль, який блокує доступ до певних web-ресурсів шляхом вибіркового блокування DNS-запитів [22]. Навпроти, коректне розпізнавання DoH є складною задачею, для вирішення якої потрібно використовувати спеціалізовані моделі машинного навчання. Наразі не відомий жоден комерційний продукт, який би використовував статистичні методи або ML для розпізнавання та блокування DoH трафіку.

Давайте розглянемо протокол DoT. Він використовує порт TCP/853 і підтримує традиційну фільтрацію за портами TCP/UDP. Це дозволяє мережевим інженерам управляти та блокувати DNS-трафік для захисту мережі від зловмисників, зберігаючи конфіденційність DNS-зв'язку. Однак це може мати свої недоліки, такі як відкритий порт TCP/853 для атак. Наприклад, зловмисники можуть атакувати цей порт із використанням великого обсягу трафіку, щоб призупинити роботу DoT. В таких випадках протокол DoH стає важливим рішенням, оскільки він інкапсулює DNS-трафік у звичайні HTTPS-запити, що робить DNS-з'єднання менш помітним для традиційних засобів фільтрації за портами TCP/UDP. Однак, відсутність видимості в мережі може також означати, що атаки можуть пройти непоміченими. Таким чином, зловмисники можуть використовувати протокол DoH для створення прихованих каналів з зовнішніми серверами керування командами, що дозволяє їм здійснювати крадіжки даних та інші дії [23].

Протокол DoH був прийнятий Міжнародною організацією стандартизації мережевих технологій (IETF) як документ RFC (RFC 8484 [24]) у 2018 році. На даний момент існує дві реалізації цього протоколу. Перша реалізація, згідно з RFC 8484, використовує класичний формат "Wire" DNS, який інкапсулюється у протоколі HTTPS. "Wire format" - це двійкове представлення об'єкта DNS; зазвичай це Повідомлення (Message) або Ресурсний запис (Resource Record). Методи Write і Read визначені у типі змінних IWireSerialiser, використовуються для серіалізації та десеріалізації об’єкта DNS. Класи WireWriter і WireReader використовуються для кодування та декодування типів даних. У даному представленні об’єкта DNS також визначені зручні методи для підтримки байтового масиву або потоку. Повідомлення в форматі «Wire Format» передаються через HTTP-запити GET/POST, відповідно до

визначень, наведених у RFC 1035.

Існує альтернативний підхід до DoH, який використовує формат JSON згідно з RFC 8427 [25]. У цьому випадку дані DNS кодуються і передаються через HTTPS-запит GET. Зараз більшість DNS-провайдерів (приблизно 90%) використовують традиційний «Wire format», який може бути переданий через HTTPS-GET (наприклад, https://dns-resolver.com/?dns=<base64-encoded-query>) або HTTPS-POST [26]. Тим не менш, підтримка DoH на основі JSON спостерігається лише у приблизно 30% DNS-провайдерів [27]. У практичному застосування всі браузери, які підтримують DoH, використовують формат «Wire format», що сумісний із RFC 8484, разом із методом POST HTTP. Під час POST-запитів, DNS-запит включається у тіло HTTP-запиту, а тип MIME (application/dns-message) вказується у заголовку Content-Type. Медіатип (MIME) вказує формат файлу або документа.

Використання JSON формату було запропоновано Google і, хоча цей формат не є офіційно стандартизованим, він дозволяє уникнути потреби в парсері DNS-формату та полегшує аналіз DNS-повідомлень, що подаються у текстовій формі [28]. Підхід JSON відрізняється читабельністю та зручністю маніпулювання даними на основі текстових повідомлень.

Деякі основні браузери пропонують використання JSON, хоча цей формат не є активним за замовчуванням. На рисунку 4 наведено приклад відповіді на DNS-запит типу AAAA для домену example.com, де записи AAAA відповідають доменній IPv6-адресі.


```
{
 "Status": 0,
 "TC": false,
 "RD": true,
 "RA": true,
 "AD": true,
 "CD": false,
 "Question": [
  {
   "name": "example.com.",
   "type": 28
  }
 ],
 "Answer": [
  {
   "name": "example.com.",
   "type": 28,
   "TTL": 86400,
   "data": "2001:db8:85a3:0:0:8a2e:370:7334"
  }
 ]
}
```


Рисунок 4 – Приклад DNS-відповіді на AAAA запит

Відповідно до постійного збільшення кількості доменних структур і складністю фіксації зашифрованого DoH-трафіку, стає очевидним, що дослідження з'єднань DoH і виявлення шкідливого трафіку залишаються актуальними завданнями для науковців.

Подальший розвиток сервісів та протоколів безпечного доступу до ресурсів доменних структур

DNS over HTTPS має декілька відмінностей від DNS over TLS, на зразок використання механізмів HTTP/2 (механізм HTTP Push, стиснення HTTP-заголовків, паралельність потоків тощо), використання TLS 1.2 і вище та інтеграція з загальною системою HTTP (кеш, проксі, аутентифікація, тощо). Особливість моделі передачі даних HTTP Push: клієнт надсилає серверу запит лише один раз. Після першого запиту сервер продовжує надсилати нові оновлення клієнту, допоки вони доступні. Клієнт не повинен думати про надсилання додаткових запитів на сервер для отримання даних. Це значно

економить пропускну здатність мережі та зменшує навантаження на сервер. Якщо клієнт (міжсерверна комунікація) знаходиться в тому самому просторі, що й сервер, або якщо сервер встановлює безпечне з’єднання з клієнтом, клієнт може бути підключений через кінцеву точку API, яка називається URL-адресою зворотного виклику.

Важливим є те, що DoH було обрано як механізм безпеки для DNS-даних у веб-браузерах завдяки гнучкій інтероперабельності браузерів з API протоколу HTTP [28]. І саме тому DoH є в центрі уваги наукових досліджень в галузі мережевої безпеки.

Відомо, що дослідження цифрових відбитків DoT та DoH активно проводились [28-31]. Цифровий відбиток (digital fingerprint) – це унікальний цифровий ідентифікатор, використовується для забезпечення автентифікації. Він містить набір даних, які ідентифікують налаштування браузера та клієнтського пристрою як унікальні. Програмне забезпечення для зняття відбитків зберігає дані відбитків на стороні сервера, які поза межами доступу для користувача. Це дозволяє ідентифікувати та відстежувати інтернет-користувачів, навіть якщо вони відхиляють дозвіл на використання cookie. Цифровий відбиток розширив відстеження користувачів і пристроїв без використання файлів cookie у реальності, і його стало надзвичайно важко контролювати або регулювати.

Звісно, так як DoT може бути ідентифікованим завдяки використанню порта tcp/853, водночас DoH не має очевидної відмінності від звичайного HTTPS-трафіку, оскільки використовує tcp/443. Тому одним із завдань цієї роботи є ідентифікація DoH-трафіку, з яким не справляються традиційні фаєрволи та аналізатори даних. Вирішення даної задачі потребує гібридного підходу у використанні методів ML та попередніх наукових досліджень у галузі мережевих технологій та кібербезпеки [32].

Відповідно до досліджень науковців K. Hynek, D. Vekshin, J. Luxemburk, T. Cejka, A. Wasicek – JSON формат даних передбачений переважно для одноразових запитів додатками, які не вимагають великої продуктивності або швидкого часу відповіді [8]. Затримка роботи протоколу DNS безпосередньо впливає на продуктивність мережевих програм [33]. Значна кількість дослідників провели вимірювання наслідків впровадження DoH на продуктивність, і ці результати узагальнено у таблиці 1. Порівняльний аналіз досліджень стосується впливу DoH на продуктивність. Параметри вимірювання включають дані та джерело вимірювань, а результати визначають основні висновки щодо впливу DoH на продуктивність порівняно з традиційним DNS.

Таблиця 1 – Порівняння досліджень, пов’язаних з продуктивністю DoH. Вимірювання

Автор	*Рік*	*Параметри вимірювання*	*Результати*
McManus [34]	2018	Користувачі Firefox	Незначний вплив, додана затримка 6 мс
Böttger та ін. [35]	2019	Один клієнт	Незначний вплив на затримку під час повторного використання з’єднання
Borgolte та ін. [22]	2019	Самоемульовані мережеві умови	Вибірковий вплив, в залежності від умов мережі
Hounsel та ін. [36]	2020	Самоемульовані мережеві умови	Вибірковий вплив, в залежності від умов мережі
Hounsel та ін. [37]	2021	Згенеровано через кінцеві точки по всій Північній Америці	Вибірковий вплив, залежно від використовуваного ресолвера DoH
Chhabra та ін. [38]	2021	Глобальні вимірювання серед 224 країн	Вибірковий вплив, залежно від умов мережі
Mbewe та ін. [39]	2021	Згенеровано через кінцеві точки по всій Африці	Вибірковий вплив, залежно від умов мережі
Jerabek та ін. [40]	2022	Згенеровані, одна локація	Вибірковий вплив, залежно від використовуваного ресолвера DoH

Перше дослідження щодо затримки DoH, опубліковане МакМанусом [34] з Mozilla у 2018 році, показало, що середня затримка програм, спричинена DoH, складає всього 6 мс. Наступне дослідження, проведене Бёттгером та іншими [35], сконцентроване на порівнянні виконання DoH з традиційним DNS. Їхні результати показують, що DoH додає значну затримку, коли з'єднання використовується для одного запиту. Однак, якщо з'єднання DoH використовується повторно для кількох запитів, додаткова затримка мінімальна. Інше дослідження, проведене Хаунселлом та іншими [36], показує, що затримка DoH і надійність значно залежать від вибору ресолвера. Це також підтверджують Джерабек та інші [40], які досліджували поведінку розпізнавача DoH і розподіл розмірів пакетів DoH залежно від використаного ресолвера. Згідно з їхніми результатами, деякі ресолвери DoH використовують довгі HTTP-заголовки, що призводить до більших пакетів і, отже, до більших накладних витрат.

Більш детальне дослідження було проведено Чхаброю та іншими [38], які досліджували вплив DoH на продуктивність у всьому світі. Їхні результати показують, що користувачі з країн з високим рівнем доходу та якісною інтернет-інфраструктурою мають менші шанси на сповільнення продуктивності, спричинене DoH, що може вплинути нерівномірно на користувачів з країн із меншими економічними можливостями. Їхні висновки також підтверджуються дослідженнями Хаунселла та інших [37], Боргольте та інших [22] і Мбеве та інших [39], які також показують, що DoH має незначний вплив при низьких мережевих затримках. Згідно з цими дослідженнями [22, 38, 41] при роботі з перевантаженими або мобільними мережами 3G, традиційний DNS значно перевершує DoH.

На 2023 рік, DoH підтримується (деколи навіть включається за замовчуванням) більшістю актуальних веб-браузерів на сьогоднішній день, таких як Chrome (починаючи з версії 83.0), Edge, Firefox, Opera та Brave. Присутні також рідні ресолвери з підтримкою DoH у Microsoft Windows [8] і сучасних дистрибутивах GNU/Linux (наприклад, через systemd-resolved). DoH підтримується основним програмним забезпеченням сервера доменних імен, таким як BIND (починаючи з версії 9.17.10), KNOT resolver (починаючи з версії 5.2.0) і Unbound (починаючи з версії 1.12.0). Також існує проксі-сервер DoH від Cloudflare, який називається cloudflared. Принаймні вісім реалізацій клієнта DoH відомі, а також щонайменше шість серверних реалізацій, які перераховані на dnscrypt.info.

Використання клієнтського DoH-трафіку було досліджено S.Garcia та ін. [42]. У статті представлено три великі набори даних від великого європейського університету, великого європейського інтернет-провайдера послуг та глобальної компанії із кібербезпеки. Результати показують, що обсяг трафіку DoH зріс протягом 2020 року; однак DoH залишається відносно рідкісним порівняно з традиційним DNS. Підсумок досліджень, пов'язаних з впровадженням DoH, показаний у таблиці 2.

Таблиця 2 – Порівняння параметрів DoH

Автор	*Рік*	*Параметри Вимірювання*	*Результати*
Deccio та ін. [43]	2019	Через відкриті ресолвери	Впровадження< 1%
Garcia та ін. [42]	2021	Адресний простір IPv4 Трафік від 3 організацій	931 DoH-сумісні IP-адреси, обсяг трафіку DoH зростає, DoH зустрічається відносно рідко.

Оскільки основною перевагою DoH є підвищена конфіденційність кінцевих користувачів [21], її було детально вивчено багатьма дослідниками [25, 44]. Загалом існує загальний скептицизм щодо достатності шифрування DNS для збереження конфіденційності користувачів. Тому були запропоновані додаткові механізми приватності DNS під назвою EDNS (Extension Mechanisms for DNS – механізми розширення для DNS) padding. Клієнти з підтримкою DoH відправляють запити з додаванням випадкового вмісту, щоб вирівняти розміри всіх пакетів. Padding зменшує можливість витоку інформації через сторонній канал. Атака сторонніми каналами (side-channel attack) – це експлойт системи безпеки, спрямований на збір інформації або вплив на виконання програми системи, шляхом вимірювання або використання непрямих ефектів системи чи її апаратного забезпечення, а не націлювання безпосередньо на програму чи її код. Найчастіше ці атаки спрямовані на вилучення конфіденційної інформації, зокрема криптографічних ключів, шляхом вимірювання випадкових апаратних випромінювань.

Цифрові відбитки web-сайтів можуть бути уражені атаками сторонніми каналами. Атака на відбиток web-сайту (Website fingerprinting – WFP) є окремим випадком аналізу трафіку. Вона виконується локальним перехоплювачем (eavesdropper) і має на меті отримати інформацію про вміст (тобто web-сайт, до якого спрямовується запит) зашифрованих і анонімних з’єднань шляхом спостереження за шаблонами мережі між відправником і першим вузлом анонімізації (тобто вузлом входу). Тут зловмисник просто використовує метадані, такі як розмір пакета та його напрямок, не порушуючи шифрування, щоб (пасивно) перехопити мережевий трафік, зловмисник або контролює скомпрометований мережевий пристрій на шлях або керує вузлом зловмисного входу. Атака на відбитки базується на припущенні, що з'єднання з кожним сайтом створює унікальну послідовність розмірів пакетів, яку зловмисник може використовувати для визначення переданого та зашифрованого вмісту [45]. Bushart і співавтори [46] та Siby [45] провели атаку на відбитки web-сайтів, використовуючи трафік DoH, із відключеним EDNS padding. Автори вказують, що їх підхід потребує менше даних для обробки, зберігаючи при цьому аналогічну точність порівняно з традиційними відбитками, які винайшов Edward Richard Henry ще наприкінці 19-го століття. Обидва документи також оцінювали трафік з увімкненим EDNS padding і вони успішно визначали запитувані імена з точністю більше ніж 70% при використанні HTTP1.1.

Hynek та ін. [8] провели експеримент, схожий на [45], визначаючи дійсні запити із трафіку DoH; однак вони намагалися визначити фактичний обсяг трафіку DoH і показали, що можливо визначити кількість запитів або версій протоколу HTTP для доменів, які використовували DoH за допомогою стандартного протоколу. Більше того, їм вдалося розпізнати доменні імена з точністю 90% при використанні HTTP 1.1.

Hynek та ін. [33] провели експеримент, аналогічний атаці WFP [45] і полягав у вивченні поведінки реалізації протоколу DoH у web-браузерах Firefox і Chrome, а також рівня деталізації, який можна виявити шляхом спостереження та аналізу інформації на рівні пакетів. У роботі було використано навченого класифікатора ML, який надавав певне уявлення про окремі доменні імена лише на основі захопленого зашифрованого з’єднання DoH. Метою дослідження було визначення реальних запитів в межах одного DNS-повідомлення. Вони аналізували форму трафіку DoH і трафік мав такі критерії: кількість запитів, версії протоколу HTTP, розміри повідомлень DoH. Останній параметр, вони використовували, щоб визначити запитані доменні імена з точністю 90% при використанні HTTP 1.1 та 70% при використанні HTTP2. Однак їх метод виявився непридатним, коли було увімкнено функцію використання EDNS.

Атака на зниження приватності була досліджена Huang та ін. [47]. Вони провели атаку, блокуючи з'єднання DoH, змушуючи браузери повертатися до традиційного незашифрованого DNS без помітного сповіщення в інтерфейсі користувача. Згідно з дослідженням [47], виробники браузерів не вважають цю атаку вразливістю, але скоріше добре задокументованою функцією, яка також описана в RFC 8310 [48]. Вплив атаки на зниження може бути зменшений за допомогою відповідного сповіщення про втрату приватності, однак жоден з виробників браузерів не планує інтегрувати його [47].

Інше питання приватності, пов'язане з DoH – це централізація провайдерами DoH, можлива кореляція та зловживання IP-адресами клієнтів і DNS-запитами. Проблема централізації даних розглядається у пропозиції про Oblivious DoH (ODoH), яка використовує анонімний проксі для запитів. Проксі має інформацію про IP-адреси клієнтів, але не може перевіряти вміст пакетів. Ресолвери можуть читати вміст пакетів, але не знають IP-адреси клієнта поза проксі. В даний час ODoH перебуває на стадії розробки проекту RFC з доступним відкритим кодом [8].

У таблиці 3 представлене порівняння досліджень DoH щодо конфіденційності. У сфері застосування для простоти вводяться спрощені позначення: *C* – співвідношення зашифрованих і незашифрованих DNS-даних на рекурсивному ресолвері, *FP* – атака на відбитки (Fingerprinting attack), *DG* – атака на пониження, *P* – пропозиція нової технології.

Таблиця 3 – Порівняння приватності DoH

Автор	*Рік*	*Сфера застосування*	*Результати*
Shulman та ін. [49]	2014	*C*	Виконання кореляційної атаки для виведення предметної області.
Bushart та ін. [46]	2019	*FP*	ML-модель для розпізнавання веб-сайтів, точність 86,1% без механізму захисту.
Siby та ін. [45]	2019	*FP*	ML-модель для відбитків веб-сайтів, точність 90,08% без захисного механізму.
Hynek та ін. [42]	2019	*FP*	ML-модель для визначення доменного імені за запитом, точність 90,14% без механізму захисту.
Huang та ін. [47]	2020	*DG*	Виконання атаки на пониження версії DoH у веб-браузерах.
Singanamalla та ін. [50]	2020	*P*	Пропозиція Oblivious DoH щодо підвищення рівня конфіденційності користувачів DoH.

На основі досліджень [22, 33, 51] щодо впливу масового розгортання DoH, можна зробити висновок, що протокол DoH є проблемою безпеки, оскільки багато існуючих автоматизованих інструментів мережевої безпеки покладаються на незашифровані DNS-повідомлення. Атакери можуть використовувати підвищену конфіденційність у зашифрованих DNS-повідомленнях, щоб приховувати свої шкідливі дії (видозміна DNS-трафіку, викрадення DNS-даних між клієнтом та сервером, проведення MiTM-атаки, тощо). Навіть якщо DoH забезпечує конфіденційність DNS, він не захищає від підміни DNS-розпізнавання («отруєння DNS-кешу») та дозволяє створення DNS-тунелів [8]. Отруєння DNS-кешу (DNS poisoning) – це внесення фальшивої інформації в DNS-кеш, у такий спосіб, що DNS-запити повертають неправильну відповідь, а користувачі перенаправляються на підробні web-сайти. Отруєння DNS-кешу також відоме як «DNS spoofing». Оскільки DNS-перетворювачі зазвичай не можуть перевірити дані у своїх кешах, неправильна DNS-інформація залишається в кеші, доки не протермінується «час життя» (Time to live – TTL) або допоки її DNS-запис не буде видалений вручну. Низка вразливостей робить можливим отруєння DNS-кешу, але основна проблема полягає в тому, що DNS створено для набагато меншого за розмірами Інтернету та базується на принципі довіри.

Останнім часом було проведено багато досліджень з інтенсивності використання трафіку DoH. Загалом з’явився науковий інтерес до теми «DNS resolving у кібербезпеці», та все ж є ще багато тем, які були малодосліджені або не дослідженні взагалі. Це дає підґрунтя для розвитку напрямку наукового

дослідження протоколу DoH, який з точки зору безпеки можна розділити на дві категорії: 1) Виявлення присутності DoH в мережі та 2) Виявлення шкідливого DoH-трафіку.

Висновки

У даній роботі було досліджено понад 50 наукових джерел, це дозволило проаналізувати основні принципи та функції протоколів безпечного доступу в доменних структурах. Була сформульована основна проблематика протоколу DoH – це складність розпізнавання та аналізу його даних під час клієнт серверних сесій. Запропонований гібридний механізм для ефективного виявлення та подальшого аналізу DoH-трафіку, що базується на комбінованому використанні алгоритмів аналізу трафіку, ML та набутого людського досвіду для збору статистичних даних.

Система доменних імен DNS є важливою складовою для доступу до інтернет-ресурсів, забезпечуючи послідовність, гранульованість та ієрархічність. Дана система є необхідною для функціонування інформаційного простору та її неможливо повністю замінити. Однак через свої особливості вона стає джерелом ризику, яким зловмисники легко можуть скористатися. Ці ризики включають атаки на цілісність DNS-трафіку, наприклад атаки типу MITM; атаки на конфіденційність DNS-даних, такі як DNS Spoofing, DNS poisoning і DNS Fishing; атаки, які спрямовані на порушення автентифікації DNS-трафіку, наприклад Website fingerprinting attack; а також атаки, спрямовані на виведення з ладу DNS-ресолверів, такі як DoS та DDoS.

Впровадження нового протоколу DNS over HTTPS усуває загрози, притаманні традиційному DNS, забезпечуючи шифрування та конфіденційність даних в межах клієнт-серверних з'єднаннях, проте водночас створює додаткове навантаження на трафік.

Розробка істотно нових моделей для дослідження та аналізу DoH-трафіку із забезпеченням високої ефективності ключових показників може надати мережевим інженерам, кіберінженерам та фахівцям в галузі захисту комп'ютерних мереж якісні рішення, що необхідні для створення кібербезпечного інформаційного простору, його управління, моніторингу та неперервного захисту.

Дані фактори дозволяють сформувати подальші етапи дослідження: 1. Аналіз та розпізнавання шкідливого DoH-трафіку; 2. Дослідження ефективності застосування ML-тренованої моделі ідентифікації шкідливого типу трафіку; 3. Удосконалення методології виявлення шкідливого DoH-трафіку; 4. Дослідження алгоритмів роботи аналізатора перенаправлення даних; 5. Удосконалення технології розпізнавання шкідливого DoH-трафіку з допомогою класифікатора машинного навчання; 6. Розробка методики безпечного доступу до ресурсів DNS; 7. Оцінка застосування інформаційної системи доступу до ресурсів DNS.

Список літератури

[1] Гороховський О. І., Трояновська Т. І., Азаров О. Д. *Інформаційна технологія доставки контенту у системах комп'ютеризованої підготовки спеціалістів*, Вінниця: ВНТУ, 2016.

[2] Коробейнікова Т. І., Захарченко С. М. *Комп'ютерні мережі: навч. посібник,* Львів: Видавництво Львівської політехніки, 2022.

[3] Т. І. Коробейнікова, С. М. Захарченко, *Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник*, Львів: Видавництво Львівської політехніки, 2021.

[4] Захарченко С.М., Трояновська Т. І., Бойко О.В. *Побудова захищених мереж на базі обладнання компанії Cisco*, Вінниця : ВНТУ, 2017.

[5] Азаров О. Д., Захарченко С. М., Кадук О. В., Орлова М. М., Тарасенко В. П. *Комп'ютерні мережі*, Вінниця: ВНТУ, 2013.

[6] Abu Al-Haija, Q.; Alohaly,M.; Odeh, A. A. "Lightweight Double-Stage Scheme to Identify Malicious DNS over HTTPS Traffic Using a Hybrid Learning Approach", *Sensors.* 23, 3489. 2023. https://doi.org/10.3390/s23073489.

[7] Коробейнікова Т.І., Федчук Т. Б. "Інформаційна технологія безпечного доступу до ресурсів DNS на базі ML-тренованих моделей ідентифікації трафіку", *International periodical scientific journal «SWorldJournal»*, № 21, С. 80–91. 2023. DOI:10.30888/2663-5712.2023-21-01.

[8] K.Hynek, D.Vekshin, J. Luxemburk, T.Cejka, A. Wasicek, "Summary of DNS over HTTPS Abuse", *IEEE Access*, Volume 4, 2016. DOI: 10.1109/ACCESS.2022.3175497

[9] Jose G.-L.; Mary K.S.; Carol A.W. *Internet Protocol Handbook. In The Domain Name System (DNS)* Handbook; DTIC: Fort Belvoir, VA, USA, 1989; Volume 4.

[10] Paul M. "Domain Names–Implementation and Specification"; *Internet Engineering Task Force*; ISI: Marina del Rey, CA, USA, 1987.

[11] Park J.; Khormali A.; Mohaisen M.; Mohaisen A. "Where are you taking me? Behavioral analysis of open DNS resolvers", *In Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Portland, OR, USA, 24–27 June 2019; pp. 493–504.

[12] Cheng Y.; Liu Y.; Li C.; Zhang Z.; Li N.; Du Y. "In-Depth Evaluation of the Impact of National-Level DNS Filtering on DNS Resolvers over Space and Time", *Electronics*, 11, 1276. 2022.
[13] Mauro Conti, Nicola Dragoni, and Viktor Lesyk, "A Survey of Man In The Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027 - 2051. 2016.
[14] Pavur, J.; Moser, D.; Lenders, V.; Martinovic, I. "Secrets in the sky: On privacy and infrastructure security in dvb-s satellite broadband", *In Proceedings of the 12th Conference on Security and Privacy inWireless and Mobile Networks*, Miami, FL, USA, pp. 277–284. 2019.
[15] Ben Wolford, "What is GDPR, the EU's new data protection law?" [Online]. Available: https://gdpr.eu/what-is-gdpr.
[16] Böttger, T.; Cuadrado, F.; Antichi, G.; Fernandes, E.L.; Tyson, G.; Castro, I.; Uhlig, S. "An Empirical Study of the Cost of DNSover-HTTPS", *In Proceedings of the Internet Measurement Conference*, Amsterdam, The Netherlands; pp. 15–21. 2019.
[17] Romain Founchereau, "Securing Anywhere Networking. DNS Security for Business Continuity and Resilence". June 2022. [Online]. Available: https://efficientip.com/blog/how-to-secure-anywhere-networking-with-dns-2022-threat-report-highlights.
[18] Romain F. "DNS Security for Business Continuity and Resilience"; *IDC*: Needham, MA, USA, 2022.
[19] Carlos López Romera, Carlos Hernández Gañán,Víctor García. *DNS Over HTTPS Traffic Analysis and Detection*, UOC , 2nd June, 2020.
[20] Hu Z.; Zhu L.; Heidemann J.; Mankin A.;Wessels D., Hoffman, P.E. "Specification for DNS over Transport Layer Security (TLS)"; *Internet Engineering Task Force*, Fremont, CA, USA, 2016.
[21] Hoffman P.E.; McManus P. "DNS Queries over HTTPS (DoH)"; *Internet Engineering Task Force:* Fremont, CA, USA, 2018.
[22] K. Borgolte, T. Chattopadhyay, N. Feamster, M. Kshirsagar, J. Holland, A. Hounsel, and P. Schmitt, "How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem," *Performance, and Policy in the Internet Ecosystem* (July 27, 2019), 2019.
[23] Albulayhi, K.; Smadi, A.A.; Sheldon, F.T.; Abercrombie, R.K. IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses. Sensors 2021, 21, 6432. [CrossRef] [PubMed]
[24] P. E. Hoffman and P. McManus, "DNS Queries over HTTPS (DoH)," RFC 8484, Tech. Rep. 8484, Oct. 2018. P. Mockapetris, "Domain names - implementation and specification,"RFC 1035 (Internet Standard), RFC Editor, pp. 1–55. [Online]. Available:https://www:rfc-editor:org/rfc/rfc1035:txt
[25] E. Brumaghin and C. Grady, "Covert channels and poor decisions:The tale of dnsmessenger," Mar 2017. [Online]. Available: https:/blog:talosintelligence:com/2017/03/dnsmessenger:html
[26] C. Cimpanu, "Here's how to enable DoH in each browser, ISPs be damned," Dec 2020, https://www.zdnet.com/article/dns-over-https-willeventually-roll-out-in-all-major-browsers-despite-isp-opposition/.P. E. Hoffman, "Representing DNS Messages in JSON," RFC 8427. [Online]. Available: https://rfc-editor:org/rfc/rfc8427:txt
[27] S. García, K. Hynek, D. Vekshin, T. Cejka, and A. Wasicek, "Large scale measurement on the adoption of encrypted DNS," *CoRR*, vol. abs/2107.04436, 2021. [Online]. Available: https://arxiv:org/abs/2107:04436
[28] DNS Over HTTPS Traffic Analysis and Detection. Carlos López Romera, Carlos Hernández Gañán,Víctor García Font 2nd June, 2020.
[29] Rebekah Houser, Zhou Li, Chase Cotton, and Haining Wang, "An Investigation on Information Leakage of DNS over TLS," *in CoNEXT '19: Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies*, 2019.
[30] Bushart Jonas and Christian Rossow, "Padding Ain't Enough: Assessing the Privacy Guarantees of Encrypted DNS," *CoRR*, vol. abs/1907.01317, July 2019.
[31] Marc Juarez, Sandra Siby, Claudia Díaz, Vallina-Rodriguez Narseo, and Carmela Troncoso, "Encrypted DNS --> Privacy? A Traffic Analysis Perspective," *in NDSS Symposium*, 2020.
[32] K. Bumanglag and H. Kettani, "On the Impact of DNS Over HTTPS Paradigm on Cyber Systems," *in 2020 3rd International Conference on Information and Computer Technologies (ICICT)*, 2020, pp. 494–499.
[33] K. Hynek and T. Cejka, "Privacy Illusion: Beware of Unpadded DoH," in *2020 11th IEEE Information Technology, Electronic and Mobile Communication conference (IEMCON)*, 2020.
[34] P. McManus, Aug 2018. [Online]. Available: https://blog:nightly:mozilla:org/2018/08/28/firefox-nightly-securedns-experimental-results.
[35] T. Böttger, F. Cuadrado, G. Antichi, E. L. a. Fernandes, G. Tyson, I. Castro, and S. Uhlig, "An Empirical Study of the Cost of DNS-over-HTTPS," in *Proceedings of the Internet Measurement Conference, ser. IMC '19. New York, NY, USA: Association for Computing Machinery*, 2019, p.15–21. [Online]. Available: https://doi:org/10:1145/3355369:3355575

[36] A. Hounsel, K. Borgolte, P. Schmitt, J. Holland, and N. Feamster, Comparing the Effects of DNS, DoT, and DoH on Web Performance. New York, NY, USA: Association for Computing Machinery, 2020, p.562–572. [Online]. Available: https://doi:org/10:1145/3366423:3380139

[37] A. Hounsel, P. Schmitt, K. Borgolte, and N. Feamster, "Can Encrypted DNS Be Fast?" *in Passive and Active Measurement, O. Hohlfeld, A. Lutu, and D. Levin, Eds. Cham: Springer International Publishing*, 1, pp.444–459. 2021.

[38] R. Chhabra, P. Murley, D. Kumar, M. Bailey, and G. Wang, "Measuring DNS-over-HTTPS Performance around the World," in *Proceedings of the 21st ACM Internet Measurement Conference*, ser. IMC '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 351–365. [Online]. Available: https://doi:org/10:1145/3487552:3487849.

[39] E. S. Mbewe and J. Chavula, "On QoE Impact of DoH and DoT in Africa: Why a User's DNS Choice Matters," in *Towards new e-Infrastructure and e-Services for Developing Countries*, R. Zitouni, A. Phokeer, J. Chavula, A. Elmokashfi, A. Gueye, and N. Benamar, Eds. Cham: Springer International Publishing, , pp. 289–304. 2021.

[40] K. Jerabek, O. Rysavy, and I. Burgetova, "Measurement and characterization of DNS over HTTPS traffic," 2022. [Online]. Available:https://arxiv:org/abs/2204:03975.

[41] Mbewe, Enock & Chavula, Josiah. (2021). On QoE Impact of DoH and DoT in Africa: Why a User's DNS Choice Matters. 10.1007/978-3-030-70572-5_18.

[42] S. García, K. Hynek, D. Vekshin, T. Cejka, and A. Wasicek, "Large scale measurement on the adoption of encrypted DNS," *CoRR*, vol. abs/2107.04436, 2021. [Online]. Available: https://arxiv:org/abs/2107:04436.

[43] C. Deccio and J. Davis, "DNS Privacy in Practice and Preparation," in *Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies*, ser. CoNEXT '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 138–143.

[44] T. Jensen, "Windows Insiders can now test DNS over HTTPS," May 2020. [Online]. Available: https://techcommunity:microsoft:com/t5/networkingblog/windows-insiders-can-now-test-dns-over-https/ba-p/1381282.

[45] S. Siby, M. Juarez, C. Diaz, N. Vallina-Rodriguez, and C. Troncoso, "Encrypted DNS –> Privacy? A Traffic Analysis Perspective," Dec 2020.

[46] J. Bushart and C. Rossow, "Padding ain't enough: Assessing the privacy guarantees of encrypted dns," *arXiv preprint arXiv*:1907.01317, 2019.

[47] Q. Huang, D. Chang, and Z. Li, "A Comprehensive Study of DNS-over-HTTPS Downgrade Attack," in *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*, 2020.

[48] S. Dickinson, D. K. Gillmor, and T. Reddy.K, "Usage Profiles for DNS over TLS and DNS over DTLS," RFC 8310, Mar. 2018. [Online]. Available: https://www:rfc-editor:org/info/rfc8310.

[49] H. Shulman, "Pretty bad privacy: Pitfalls of DNS encryption," in *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, 2014, pp.191–200.

[50] S. Singanamalla, S. Chunhapanya, M. Vavrusa, T. Verma, P. Wu, M. Fayed, K. Heimerl, N. Sullivan, and C. A. Wood, "Oblivious DNS over HTTPS (odoh): A practical privacy enhancement to DNS," *CoRR*, vol. abs/2011.10121, 2020. [Online]. Available: https://arxiv:org/abs/2011:10121.

[51] A. Fidler, B. Hubert, J. Livingood, J. Reid, and N. Leymann, "DNS over HTTPS (DoH) Considerations for Operator Networks," *Internet Engineering Task Force*, Internet-Draft draft-reid-doh-operator-00, Mar. 2019, work in Progress. [Online]. Available: https://datatracker:ietf:org/doc/html/draft-reid-doh-operator-00.

Стаття надійшла: 04.03.2024.

References

[1] Horokhovs′kyy O. I., Troyanovs′ka T. I., Azarov O. D. *Informatsiyna tekhnolohiya dostavky kontentu u systemakh komp"yuteryzovanoyi pidhotovky spetsialistiv*, Vinnytsya: VNTU, 2016.

[2] Korobeĭnikova T. I., Zakharchenko S. M. *Komp'yuterni merezhi: navch. posibnyk*, L′viv: Vydavnytstvo L′vivs′koï politekhniky, 2022.

[3] T. I. Korobeinikova, S. M. Zakharchenko Tekhnolohiï zakhystu lokal′nykh merezh na osnovi obladnannya CISCO : navch. posibnyk /. – L′viv: Vydavnytstvo L′vivs′koï politekhniky, 2021.

[4] Zakharchenko S.M., Troyanovs′ka T. I., Boyko O.V. Pobudova zakhyshchenykh merezh na bazi obladnannya kompaniyi Cisco, Vinnytsya : VNTU, 2017.

[5] Azarov O. D., Zakharchenko S. M., Kaduk O. V., Orlova M. M., Tarasenko V. P. Komp″yuterni merezhi, Vinnytsya: VNTU, 2013.Abu Al-Haija, Q.; Alohaly,M.; Odeh, A. A. "Lightweight Double-Stage Scheme to Identify Malicious DNS over HTTPS Traffic Using a Hybrid Learning Approach", *Sensors.* 23, 3489. 2023. https://doi.org/10.3390/s23073489.

[6] Abu Al-Haija, Q.; Alohaly,M.; Odeh, A. A. "Lightweight Double-Stage Scheme to Identify Malicious

DNS over HTTPS Traffic Using a Hybrid Learning Approach”, *Sensors.* 23, 3489. 2023. https://doi.org/10.3390/s23073489.

[7] Коробейнікова Т.І., Федчук Т. Б. “Інформаційна технологія безпечного доступу до ресурсів DNS на базі ML-тренованих моделей ідентифікації трафіку”, *International periodical scientific journal «SWorldJournal»*, № 21, С. 80–91. 2023. DOI:10.30888/2663-5712.2023-21-01.

[8] K.Hynek, D.Vekshin, J. Luxemburk, T.Cejka, A. Wasicek, “Summary of DNS over HTTPS Abuse”, *IEEE Access*, Volume 4, 2016. DOI: 10.1109/ACCESS.2022.3175497

[9] Jose G.-L.; Mary K.S.; Carol A.W. *Internet Protocol Handbook. In The Domain Name System (DNS)* Handbook; DTIC: Fort Belvoir, VA, USA, 1989; Volume 4.

[10] Paul M. “Domain Names–Implementation and Specification”; *Internet Engineering Task Force*; ISI: Marina del Rey, CA, USA, 1987.

[11] Park J.; Khormali A.; Mohaisen M.; Mohaisen A. “Where are you taking me? Behavioral analysis of open DNS resolvers”, *In Proceedings of the 2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Portland, OR, USA, 24–27 June 2019; pp. 493–504.

[12] Cheng Y.; Liu Y.; Li C.; Zhang Z.; Li N.; Du Y. “In-Depth Evaluation of the Impact of National-Level DNS Filtering on DNS Resolvers over Space and Time”, *Electronics*, 11, 1276. 2022.

[13] Mauro Conti, Nicola Dragoni, and Viktor Lesyk, "A Survey of Man In The Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2027 - 2051. 2016.

[14] Pavur, J.; Moser, D.; Lenders, V.; Martinovic, I. “Secrets in the sky: On privacy and infrastructure security in dvb-s satellite broadband”, *In Proceedings of the 12th Conference on Security and Privacy inWireless and Mobile Networks*, Miami, FL, USA, pp. 277–284. 2019.

[15] Ben Wolford, “What is GDPR, the EU’s new data protection law?” [Online]. Available: https://gdpr.eu/what-is-gdpr.

[16] Böttger, T.; Cuadrado, F.; Antichi, G.; Fernandes, E.L.; Tyson, G.; Castro, I.; Uhlig, S. “An Empirical Study of the Cost of DNSover-HTTPS”, *In Proceedings of the Internet Measurement Conference*, Amsterdam, The Netherlands; pp. 15–21. 2019.

[17] Romain Founchereau, “Securing Anywhere Networking. DNS Security for Business Continuity and Resilence”. June 2022. [Online]. Available: https://efficientip.com/blog/how-to-secure-anywhere-networking-with-dns-2022-threat-report-highlights.

[18] Romain F. “DNS Security for Business Continuity and Resilience”; *IDC*: Needham, MA, USA, 2022.

[19] Carlos López Romera, Carlos Hernández Gañán,Víctor García. *DNS Over HTTPS Traffic Analysis and Detection*, UOC , 2nd June, 2020.

[20] Hu Z.; Zhu L.; Heidemann J.; Mankin A.;Wessels D., Hoffman, P.E. “Specification for DNS over Transport Layer Security (TLS)”; *Internet Engineering Task Force*, Fremont, CA, USA, 2016.

[21] Hoffman P.E.; McManus P. “DNS Queries over HTTPS (DoH)”; *Internet Engineering Task Force:* Fremont, CA, USA, 2018.

[22] K. Borgolte, T. Chattopadhyay, N. Feamster, M. Kshirsagar, J. Holland, A. Hounsel, and P. Schmitt, “How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem,” *Performance, and Policy in the Internet Ecosystem* (July 27, 2019), 2019.

[23] Albulayhi, K.; Smadi, A.A.; Sheldon, F.T.; Abercrombie, R.K. IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses. Sensors 2021, 21, 6432. [CrossRef] [PubMed]

[24] P. E. Hoffman and P. McManus, “DNS Queries over HTTPS (DoH),” RFC 8484, Tech. Rep. 8484, Oct. 2018. P. Mockapetris, “Domain names - implementation and specification,”RFC 1035 (Internet Standard), RFC Editor, pp. 1–55. [Online]. Available:https://www:rfc-editor:org/rfc/rfc1035:txt

[25] E. Brumaghin and C. Grady, “Covert channels and poor decisions:The tale of dnsmessenger,” Mar 2017. [Online]. Available: https:/blog:talosintelligence:com/2017/03/dnsmessenger:html

[26] C. Cimpanu, “Here’s how to enable DoH in each browser, ISPs be damned,” Dec 2020, https://www.zdnet.com/article/dns-over-https-willeventually-roll-out-in-all-major-browsers-despite-isp-opposition/.P. E. Hoffman, “Representing DNS Messages in JSON,” RFC 8427. [Online]. Available: https://rfc-editor:org/rfc/rfc8427:txt

[27] S. García, K. Hynek, D. Vekshin, T. Cejka, and A. Wasicek, “Large scale measurement on the adoption of encrypted DNS,” *CoRR*, vol. abs/2107.04436, 2021. [Online]. Available: https://arxiv:org/abs/2107:04436

[28] DNS Over HTTPS Traffic Analysis and Detection. Carlos López Romera, Carlos Hernández Gañán,Víctor García Font 2nd June, 2020.

[29] Rebekah Houser, Zhou Li, Chase Cotton, and Haining Wang, "An Investigation on Information Leakage of DNS over TLS," *in CoNEXT '19: Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies*, 2019.

[30] Bushart Jonas and Christian Rossow, "Padding Ain't Enough: Assessing the Privacy Guarantees of

Encrypted DNS," *CoRR*, vol. abs/1907.01317, July 2019.
[31] Marc Juarez, Sandra Siby, Claudia Díaz, Vallina-Rodriguez Narseo, and Carmela Troncoso, "Encrypted DNS --> Privacy? A Traffic Analysis Perspective," *in NDSS Symposium*, 2020.
[32] K. Bumanglag and H. Kettani, "On the Impact of DNS Over HTTPS Paradigm on Cyber Systems," *in 2020 3rd International Conference on Information and Computer Technologies (ICICT)*, 2020, pp. 494–499.
[33] K. Hynek and T. Cejka, "Privacy Illusion: Beware of Unpadded DoH," in *2020 11th IEEE Information Technology, Electronic and Mobile Communication conference (IEMCON)*, 2020.
[34] P. McManus, Aug 2018. [Online]. Available: https://blog:nightly:mozilla:org/2018/08/28/firefox-nightly-securedns-experimental-results.
[35] T. Böttger, F. Cuadrado, G. Antichi, E. L. a. Fernandes, G. Tyson, I. Castro, and S. Uhlig, "An Empirical Study of the Cost of DNS-over-HTTPS," in *Proceedings of the Internet Measurement Conference, ser. IMC '19. New York, NY, USA: Association for Computing Machinery*, 2019, p.15–21. [Online]. Available: https://doi:org/10:1145/3355369:3355575
[36] A. Hounsel, K. Borgolte, P. Schmitt, J. Holland, and N. Feamster, Comparing the Effects of DNS, DoT, and DoH on Web Performance. New York, NY, USA: Association for Computing Machinery, 2020, p.562–572. [Online]. Available: https://doi:org/10:1145/3366423:3380139
[37] A. Hounsel, P. Schmitt, K. Borgolte, and N. Feamster, "Can Encrypted DNS Be Fast?" *in Passive and Active Measurement, O. Hohlfeld, A. Lutu, and D. Levin, Eds. Cham: Springer International Publishing*, 1, pp.444–459. 2021.
[38] R. Chhabra, P. Murley, D. Kumar, M. Bailey, and G. Wang, "Measuring DNS-over-HTTPS Performance around the World," in *Proceedings of the 21st ACM Internet Measurement Conference*, ser. IMC '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 351–365. [Online]. Available: https://doi:org/10:1145/3487552:3487849.
[39] E. S. Mbewe and J. Chavula, "On QoE Impact of DoH and DoT in Africa: Why a User's DNS Choice Matters," in *Towards new e-Infrastructure and e-Services for Developing Countries*, R. Zitouni, A. Phokeer, J. Chavula, A. Elmokashfi, A. Gueye, and N. Benamar, Eds. Cham: Springer International Publishing, , pp. 289–304. 2021.
[40] K. Jerabek, O. Rysavy, and I. Burgetova, "Measurement and characterization of DNS over HTTPS traffic," 2022. [Online]. Available:https://arxiv:org/abs/2204:03975.
[41] Mbewe, Enock & Chavula, Josiah. (2021). On QoE Impact of DoH and DoT in Africa: Why a User's DNS Choice Matters. 10.1007/978-3-030-70572-5_18.
[42] S. García, K. Hynek, D. Vekshin, T. Cejka, and A. Wasicek, "Large scale measurement on the adoption of encrypted DNS," *CoRR*, vol. abs/2107.04436, 2021. [Online]. Available: https://arxiv:org/abs/2107:04436.
[43] C. Deccio and J. Davis, "DNS Privacy in Practice and Preparation," in *Proceedings of the 15th International Conference on Emerging Networking Experiments And Technologies*, ser. CoNEXT '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 138–143.
[44] T. Jensen, "Windows Insiders can now test DNS over HTTPS," May 2020. [Online]. Available: https://techcommunity:microsoft:com/t5/networkingblog/windows-insiders-can-now-test-dns-over-https/ba-p/1381282.
[45] S. Siby, M. Juarez, C. Diaz, N. Vallina-Rodriguez, and C. Troncoso, "Encrypted DNS –> Privacy? A Traffic Analysis Perspective," Dec 2020.
[46] J. Bushart and C. Rossow, "Padding ain't enough: Assessing the privacy guarantees of encrypted dns," *arXiv preprint arXiv*:1907.01317, 2019.
[47] Q. Huang, D. Chang, and Z. Li, "A Comprehensive Study of DNS-over-HTTPS Downgrade Attack," in *10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20)*, 2020.
[48] S. Dickinson, D. K. Gillmor, and T. Reddy.K, "Usage Profiles for DNS over TLS and DNS over DTLS," RFC 8310, Mar. 2018. [Online]. Available: https://www:rfc-editor:org/info/rfc8310.
[49] H. Shulman, "Pretty bad privacy: Pitfalls of DNS encryption," in *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, 2014, pp.191–200.
[50] S. Singanamalla, S. Chunhapanya, M. Vavrusa, T. Verma, P. Wu, M. Fayed, K. Heimerl, N. Sullivan, and C. A. Wood, "Oblivious DNS over HTTPS (odoh): A practical privacy enhancement to DNS," *CoRR*, vol. abs/2011.10121, 2020. [Online]. Available: https://arxiv:org/abs/2011:10121.
[51] A. Fidler, B. Hubert, J. Livingood, J. Reid, and N. Leymann, "DNS over HTTPS (DoH) Considerations for Operator Networks," *Internet Engineering Task Force*, Internet-Draft draft-reid-doh-operator-00, Mar. 2019, work in Progress. [Online]. Available: https://datatracker:ietf:org/doc/html/draft-reid-doh-operator-00.

Відомості про авторів

Коробейнікова Тетяна Іванівна, к.т.н., доцент кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка», кафедра безпеки інформаційних технологій

Korobeinikova Tetiana, PhD, associate professor of information technology security department, National university “Lvivska Politechnika”

Федчук Тарас Богданович, аспірант кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка», кафедра безпеки інформаційних технологій

Fedchuk Taras, graduate student of information technology security department, National university “Lvivska Politechnika”

T. Korobeinikova, T. Fedchuk

OVERVIEW OF SECURE ACCESS TO DOMAIN NAME SYSTEM RESOURCES

Lviv Polytechnic National University, Lviv