ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ДОСТУПУ КОРИСТУВАЧІВ ДО ІНТЕРНЕТУ НА БАЗІ DNS-ПЛАТФОРМИ QUAD9»

Виконав студент 6 курсу, групи БСДМ-61
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Александров В. С.
(прізвище та ініціали)
Керівник Кожухівська О. А.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Інститут ННІЗІ
Кафедра Інформаційної та кібернетичної безпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Гайдур Г.І.
«___» _____ 2022 року

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Александрову Владиславу Сергійовичу
(прізвище, ім'я, по батькові)

1. Тема магістерської роботи: «Технологія забезпечення безпечного доступу користувачів до Інтернету на базі DNS-платформи Quad9»

керівник магістерської роботи Кожухівська Олена Андріївна, д.т.н.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом закладу вищої освіти від «11» жовтня 2022 року № 170.

2. Строк подання студентом магістерської роботи 15.12.2022 р.

3. Вихідні дані до магістерської роботи
інформаційна система підприємства;
набір сервісів DNS-платформи Quad9;
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Аналіз проблеми забезпечення безпечного доступу користувачів до Інтернету.
2. Аналіз методів та засобів забезпечення безпечного доступу користувачів до Інтернету на базі DNS-платформи Quad9.
3. Порядок застосування технології забезпечення безпечного доступу користувачів до Інтернету.

5. Перелік графічного матеріалу

1. Тема магістерської роботи.

2. Об’єкт, предмет, мета та наукові завдання дослідження.

3. Результати аналізу проблеми забезпечення безпечного доступу користувачів до Інтернету.

4. Результати аналізу методів та засобів забезпечення безпечного доступу користувачів до Інтернету на базі DNS-платформи Quad9.

5. Рекомендації щодо забезпечення безпечного доступу користувачів до Інтернету.

6. Висновки за результатами роботи.

6. Дата видачі завдання 12.10.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.	Визначення актуальності проблеми забезпечення безпечного доступу користувачів до Інтернету.	22.10.2022 р.	
2.	Аналіз наукової та технічної літератури з питань теми магістерської роботи.	02.11.2022 р.	
3.	Аналіз проблеми забезпечення безпечного доступу користувачів до Інтернету.	12.11.2022 р.	
4.	Дослідження методів та засобів забезпечення безпечного доступу користувачів до Інтернету на базі DNS-платформи Quad9.	24.11.2022 р.	
5.	Розроблення рекомендацій щодо забезпечення безпечного доступу користувачів до Інтернету.	03.12.2022 р.	
6.	Оформлення результатів дослідження.	10.12.2022 р.	
7.	Підготовка доповіді до захисту.	15.12.2022 р.	

Студент Александров В. С.
(підпис) прізвище та ініціали

Керівник магістерської роботи Кожухівська О. А.
(підпис) прізвище та ініціали

ВІДГУК РЕЦЕНЗЕНТА
на магістерську роботу

студента Александрова Владислава Сергійовича
на тему: «Технологія забезпечення безпечного доступу користувачів до Інтернету на базі DNS-платформи Quad9»

Актуальність: Система доменних імен (Domain Name System, DNS) – це протокол, який переводить зручні для користувача доменні імена в зручні для комп'ютера IP-адреси. Ця система призначена для спрощення роботи користувачів в Інтернеті.

Оскільки DNS була розроблена з урахуванням зручності користувачів, а не вимог безпеки, кіберзлочинці знаходять способи використовувати зв'язок DNS-клієнт/сервер, використовуючи шкідливі домени для експлуатації, зараження і нанесення шкоди користувачам та організаціям.

Система Quad9 реалізує сервіс безпеки DNS, використовуючи аналітику безпеки від IBM X-Force Exchange та 18-ти інших партнерів для блокування більшості шкідливих доменів, інфраструктур ботнетів і шкідливих програм.

В Quad9 реалізується канал раннього попередження X-Force Exchange API, що дозволяє аналітикам безпеки швидше реагувати на здійснювані або майбутні атаки шляхом попередження їх про сотні нових шкідливих доменів, які з'являються щодня.

У міру того, як поверхня атак продовжує розширюватися, нескінченний потік нових шкідливих доменів робить захист від майбутніх загроз все важчим. Тому тема магістерської роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі було встановлено зміст проблеми методів та засобів забезпечення безпечного доступу користувачів до Інтернету.
2. Було досліджено методи та засоби забезпечення безпечного доступу користувачів до Інтернету на базі DNS-платформи Quad9.
3. Розроблені відповідні рекомендації щодо методів та засобів забезпечення безпечного доступу користувачів до Інтернету.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою магістерської роботи.

Недоліки:

1. У магістерській роботі бажано було б провести порівняльний аналіз методів та засобів забезпечення безпечного доступу користувачів до Інтернету.
2. У роботі не завжди застосовуються посилання на використані джерела інформації.

Висновок: Враховуючи недоліки, магістерська робота заслуговує оцінку **добре**, а студент **Александров В. С.** – присвоєння кваліфікації магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Якість роботи	
Виконано на замовлення підприємства	
Виконано за тематикою НДР	
Виконано з макетом	
Виконано з застосуванням ЕОМ та МПТ	√
Має практичну цінність	√
Проект-частина комплексної теми	

Підпис рецензента (_____)

Підпис засвідчую
Підпис особи, що засвідчує (_____)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

ПОДАННЯ
ГОЛОВІ ДЕРЖАВНОЇ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ МАГІСТЕРСЬКОЇ РОБОТИ

Направляється студент Александров В. С. до захисту магістерської роботи
(прізвище та ініціали)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія захисту хмарних сервісів підприємства на базі FortiCASB»

Магістерська робота і рецензія додаються.

Директор інституту _____ Савченко В.А.
(підпис) (прізвище та ініціали)

Довідка про успішність

Александров В. С. за період навчання в інституті
(прізвище та ініціали студента)
ННІЗІ з 2021 року по 2023 рік повністю виконав навчальний план за напрямом підготовки, спеціальністю з таким розподілом оцінок за:
національною шкалою: відмінно ____%, добре ____%, задовільно ____%;
шкалою ECTS: A ____%; B ____%; C ____%; D ____%; E ____%.

Секретар інституту, факультету (відділення) _____ Бреславська Т.В.
(підпис) (прізвище та ініціали)

Висновок керівника магістерської роботи

Студент ***Александров В. С.*** обрав тему роботи, метою якої було розробити рекомендації щодо забезпечення безпечного доступу користувачів до Інтернету. Перелік використаних джерел свідчить про вміння студентом розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання магістерської роботи Александров В. С. показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану магістерську роботу студента Александрова Владислава Сергійовича на оцінку **«добре»** та присвоїти йому кваліфікацію магістр з кібербезпеки за спеціалізацією інформаційна та кібернетична безпека.

Керівник магістерської роботи _____ Кожухівська О. А.
(підпис) (прізвище та ініціали)
“____” _____ 2022 року

Висновок кафедри про магістерську роботу

Магістерська робота розглянута. Студент Александров В. С.
(прізвище та ініціали)
допускається до захисту даної магістерської роботи в Державній екзаменаційній комісії.

Завідувач кафедри Інформаційної та кібернетичної безпеки
(назва)

_____ Гайдур Г.І.
(підпис) (прізвище та ініціали)

“____” _____ 2022 року

РЕФЕРАТ

Текстова частина магістерської роботи: 65 сторінок, 12 рисунків, одна таблиця, 14 джерел.

Об'єкт дослідження – забезпечення безпечного доступу користувачів до Інтернет.

Предмет дослідження – технологія забезпечення безпечного доступу користувачів до Інтернет на базі DNS-платформи Quad9.

Мета роботи – розробити рекомендації щодо застосування методів та засобів забезпечення безпечного доступу користувачів до Інтернет на базі DNS-платформи Quad9.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Сьогоднішні загрози, які надходять з кіберпростору, зумовлюють необхідність забезпечення безпечного доступу користувачів (як кінцевих користувачів, так і організацій та компаній) до Інтернет. Існує нагальна потреба у відповідному ефективному сервісі захисту від кібератак, автоматично блокуючи веб-сайти, які, як відомо, крадуть особисту інформацію, заражають пристрої користувачів шкідливим ПЗ або здійснюють шахрайські дії.

Рішення Quad9 на базі DNS-платформи розроблено для забезпечення додаткового рівня захисту. Це досягається шляхом маршрутизації DNS-запитів через мережу серверів безпеки по всьому світу. Рішення Quad9 базується на даних про загрози, які зібрані від ряду компаній, що займаються кібербезпекою, для оцінки ризиків кожного веб-сайту, що відвідує користувач в режимі реального часу і блокує доступ до них. Рішення Quad9 забезпечує підвищену безпеку для приватних осіб, бізнес-користувачів і їх клієнтів в мережах, пристроях, цифрових активах і продуктах IoT.

В роботі проаналізовано проблему забезпечення безпечного доступу користувачів до Інтернет. Проведено аналіз існуючих методів та засобів забезпечення безпечного доступу користувачів до Інтернет на базі DNS-платформ. Досліджено методи та засоби забезпечення безпечного доступу користувачів до Інтернет на базі DNS-платформи Quad9. Розроблено алгоритм забезпечення безпечного доступу користувачів до Інтернет на базі DNS-платформи Quad9. Розроблено рекомендації користувачам щодо безпечного доступу до Інтернет на базі DNS-платформи Quad9.

Галузь використання – кібербезпека інформаційних систем.

ГЛОБАЛЬНА МЕРЕЖА ІНТЕРНЕТ, СИСТЕМА ДОМЕННИХ ІМЕН, ЗАХИСТ КОРИСТУВАЧІВ, МЕТОДИ ТА ЗАСОБИ БЕЗПЕЧНОГО ДОСТУПУ КОРИСТУВАЧІВ, DNS-ПЛАТФОРМА QUAD9

ABSTRACT

Master’s thesis: 65 pages, 12 figures, one table, 14 sources.

Object of research – the ensuring secure user access to the Internet.

Subject of research – the technology for providing users with secure access to the Internet based on the Quad9 DNS platform.

The aim of research – to develop recommendations on the application of methods and means of ensuring users' secure access to the Internet based on the Quad9 DNS platform.

Research methods – elaboration of literature on the topic, analysis of operational documentation, international standards and their comparison.

The master's thesis is devoted to ensuring safe access of users (both end users and organizations and companies) to the Internet. There is an urgent need for a suitable and effective cyber attack protection service, automatically blocking websites known to steal personal information, infect users' devices with malware or engage in fraudulent activities.

The Quad9 solution based on the DNS platform is designed to provide an additional level of protection. This is achieved by routing DNS queries through a network of security servers around the world. Quad9's solution is based on threat data collected from a number of cybersecurity companies to assess the risks of each website a user visits in real time and block access to them. The Quad9 solution provides enhanced security for individuals, business users and their customers across networks, devices, digital assets and IoT products.

The paper analyzes the problem of ensuring users' safe access to the Internet. An analysis of existing methods and means of ensuring secure access of users to the Internet on the basis of DNS platforms was carried out. The methods and means of ensuring secure access of users to the Internet based on the Quad9 DNS platform were studied. An algorithm has been developed to ensure users' safe access to the Internet based on the Quad9 DNS platform. Recommendations for users on safe access to the Internet based on the Quad9 DNS platform have been developed.

The field of use – cybersecurity of information systems.

GLOBAL INTERNET NETWORK, DOMAIN NAME SYSTEM, USER PROTECTION, METHODS AND MEANS OF SECURE USER ACCESS, QUAD9 DNS PLATFORM

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

APIs – Application Programming Interfaces

C&C – Command and Control

DBIR – Data Breach Investigations Report

DNS – Domain Name System

GDPR – General Data Protection Regulation

IDS – Intrusion Detection System

IoT – Internet of Things

IP – Internet Protocol

IPsec – IP security

SaaS – Software as a Service

TLD – Top-Level Domain

VCDB – VERIS Community Database

VERIS – Vocabulary for Event Recording and Incident Sharing

VPN – Virtual Private Networks

ВСТУП

Актуальність дослідження. Сучасні людина та бізнес не уявляються без застосування глобальної мережі Інтернет. У той же час Інтернет несе загрозу злочинних дій по відношенню до них. Тому постає гостра проблема забезпечення безпечного доступу користувачів до Інтернету.

Для того, щоб Інтернет став ефективним інструментом, користувачі повинні довіряти своїй здатності користуватися онлайн-послугами та не боятися крадіжок, шахрайства або зловживання їх пристроями зловмисниками. Державні та приватні оператори мереж потребують захисту від зловмисного використання ресурсів інфраструктури та атак на своїх користувачів або клієнтів. Тому постає проблема створення та використання відповідних методів та засобів забезпечення безпечного доступу користувачів до Інтернет.

Рішення Quad9 є безкоштовним сервісом, який замінює налаштування провайдера Інтернету або корпоративного сервера доменних імен (DNS) за замовчуванням. Коли комп'ютер користувача виконує будь-яку транзакцію в Інтернеті, яка використовує DNS, рішення Quad9 блокує пошук зловмисних імен хостів із найсвіжішого списку загроз. Ця блокувальна дія захищає комп’ютер користувача, мобільний пристрій або систему IoT від широкого кола загроз, таких як зловмисне програмне забезпечення, фішинг, шпигунське програмне забезпечення та бот-мережі, і може покращити продуктивність, а також гарантувати конфіденційність.

Система Quad9 використовує дані про загрози понад десятка провідних компаній у галузі кібербезпеки, що забезпечує в реальному часі уявлення про те, які веб-сайти безпечні, а які сайти, містять шкідливе програмне забезпечення чи інші загрози. Якщо система виявить, що сайт, до якого хоче потрапити користувач, інфіковано, то йому буде автоматично заблоковано доступ, захищаючи його дані та комп'ютер.

Вищесказане визначає актуальність теми даної магістерської роботи,

основний зміст якої становлять дослідження методів та засобів забезпечення безпечного доступу користувачів до Інтернет на базі DNS-платформи Quad9.

Об'єкт дослідження – забезпечення безпечного доступу користувачів до Інтернет.

Предмет дослідження – технологія забезпечення безпечного доступу користувачів до Інтернет на базі DNS-платформи Quad9.

Мета роботи – розробити рекомендації щодо застосування методів та засобів забезпечення безпечного доступу користувачів до Інтернет на базі DNS-платформи Quad9.

Наукові завдання:

проаналізувати існуючі загрози безпечному доступу користувачів до Інтернет;

визначити зміст проблеми забезпечення безпечного доступу користувачів до Інтернет;

дослідити існуючі методи та засоби існуючих загроз безпечному доступу користувачів до Інтернет;

розробити алгоритм забезпечення безпечного доступу користувачів до Інтернет на базі DNS-платформи Quad9;

розробити рекомендації щодо забезпечення безпечного доступу користувачів до Інтернет.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів полягає в розробці рекомендацій щодо застосування методів та засобів забезпечення безпечного доступу користувачів до Інтернет.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ДОСТУПУ КОРИСТУВАЧІВ ДО ІНТЕРНЕТ

1.1. Аналіз існуючих загроз безпечному доступу користувачів до Інтернет

В [1] зазначається, що кіберзлочинці продовжують атакувати державні та приватні організації із загрозливою швидкістю. Зловмисники часто націлені на державні та приватні організації, тому що знають, що їх командам безпеки необхідно запускати складні системи, а також мати справу з численними сторонніми системами і службами. Багато команд з кібербезпеки також борються зі скороченням бюджетів на безпеку і нестачею кваліфікованих фахівців з кібербезпеки і мережевих технологій для заповнення відкритих вакансій. Пандемія COVID-19 і подальше зростання віддаленої роботи державних службовців і запитів громадян на доступність державних ресурсів в Інтернеті тільки погіршили їх проблеми з безпекою [1].

Одним з улюблених векторів атак кіберзлочинців на організації є шкідливе ПЗ. Розповсюдження шкідливих програм призводить до виконання шкідливих дій на пристроях. Воно може бути введено в систему в різних формах, таких як електронні листи або шкідливі веб-сайти. Різні типи шкідливих програм мають різні можливості в залежності від їх передбачуваного призначення, наприклад, розкриття конфіденційної інформації, зміна даних в системі, надання віддаленого доступу до системи, подання команд системі або знищення файлів або систем тощо [1].

Хоча шкідливі програми бувають різних видів, найбільш поширеним типом, використовуваним проти організацій, сьогодні є програми-вимагачі. Програми-вимагачі це тип шкідливого ПЗ, який блокує доступ до системи, пристрою або файлу до тих пір, поки не буде сплачено викуп. Програми-вимагачі роблять це, шифруючи файли на кінцевій точці, погрожуючи стерти файли або блокуючи

доступ до системи. Це може бути особливо небезпечно, коли атаки програм-вимагачів зачіпають лікарні, центри екстреного виклику і іншу важливу інфраструктуру [1].

Іншим поширеним типом шкідливого ПЗ є «трояни» – це шкідливі програми, що представляють собою додаток або програмне забезпечення, яке можна встановити. Трояни можуть надати зловмисникові бекдор і згодом отримати повний доступ до пристрою, дозволяючи зловмисникові вкрасти банківську і конфіденційну інформацію або завантажити додаткове шкідливе ПЗ. Результати Verizon Data Breach Investigations Report за 2020 рік показують, що різні варіанти троянів брали участь в більш ніж 50% інцидентів, пов'язаних з шкідливим ПЗ в державному секторі [1].

Завантажники або допери – це шкідливі програми, які, крім власних шкідливих дій, дозволяють іншим, часто більш небезпечним, шкідливим програмам проникати в заражену систему. Дані, зібрані Verizon Data Breach Investigations Report за 2020 рік, показують, що майже 25% інцидентів в державному секторі пов'язані з завантажувачами або дроперами [1].

Шпигунське ПЗ записує натиснення клавіш, прослуховує їх через комп'ютерні мікрофони, отримує доступ до веб-камер або робить знімки екрану і відправляє інформацію зловмисникові. Цей тип шкідливого ПЗ може надати доступ до імен користувачів, паролів, будь-який іншої конфіденційної інформації, що вводиться з клавіатури або видимої на моніторі, а також потенційно інформації, що переглядається через веб-камеру. Кейлогери, які в основному записують натискання клавіш, є найбільш поширеним типом шпигунського ПЗ, а ZeuS, найвідоміший кейлоггер, вже кілька років входить до списку десяти шкідливих програм MS-ISAC [1].

Click Fraud є шкідливим ПЗ, яке генерує підроблені автоматичні переходи на рекламні веб-сайти. Ці оголошення приносять дохід при натисканні. Чим більше кліків, тим більше виручка. Kovter є одним з найбільш поширених різновидів шахрайства з кліками, останні кілька років входить до списку десяти шкідливих програм MS-ISAC [1].

Шкідливе ПЗ найчастіше проникає в організації через шкідливий спам, небажані електронні листи, які або направляють користувачів на шкідливі веб-сайти, або змушують користувачів завантажувати або відкривати шкідливі програми, або шкідливі оголошення, шкідливі програми, представлені через шкідливу рекламу. Спільною рисою між цими векторами і різними типами шкідливих програм, які вони можуть привнести в IT-системи організації, є те, що вони майже завжди пов'язані або з користувачами, або зі шкідливим програмним забезпеченням, *яке вони ненавмисно завантажують при підключенні до шкідливих веб доменів* [1].

У зв’язку з COVID-19 багато компаній перешли на дистанційну роботу, щоб бізнес продовжував працювати. Зловмисники роблять все можливе, щоб отримати вигоду з ситуації, що склалася [2].

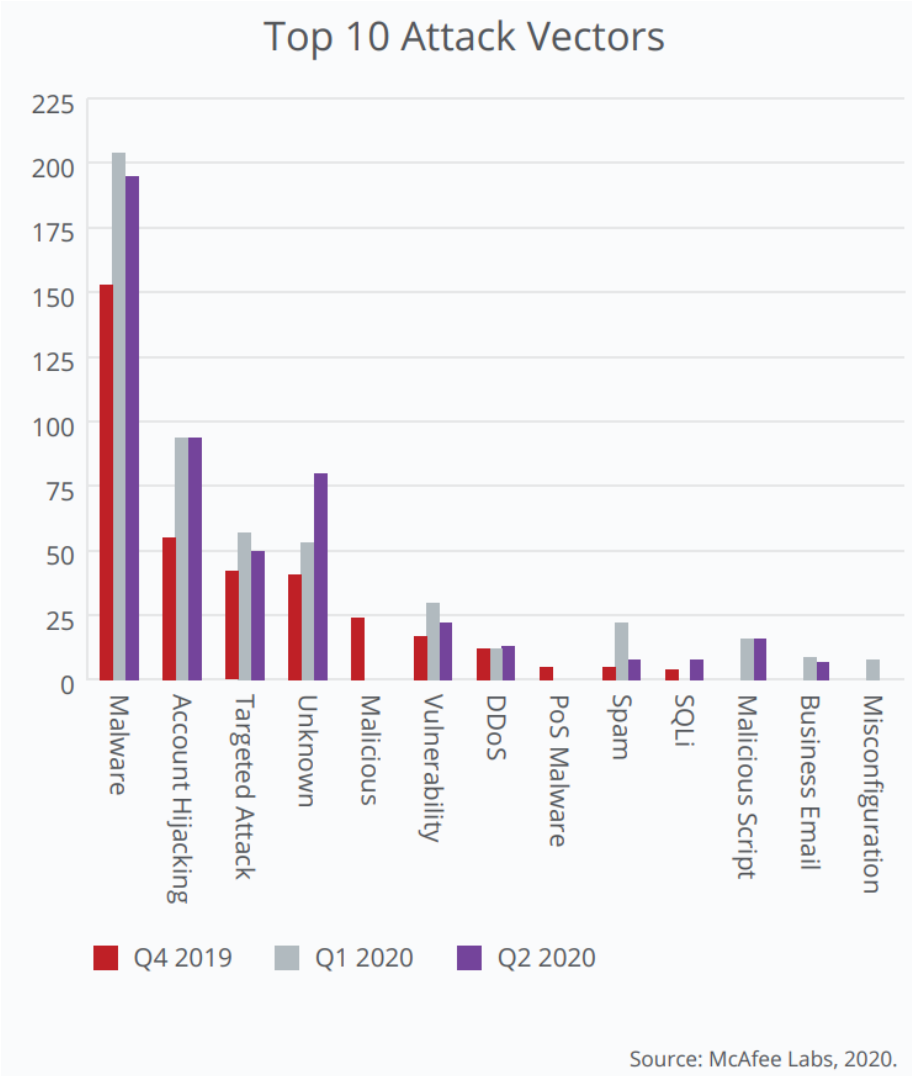


Рис. 1.1. Основні вектори атак за даними McAfee Labs [2]

Шкідливе програмне забезпечення визначило вектори атак (рис. 1.1) у другому кварталі 2020 року, на що припадає 35% публічно повідомлених інцидентів. Загальна кількість атак на викрадення облікового запису склала 17%, а цільових атак – 9% [2].

Наведемо статистику загроз шкідливого програмного забезпечення [2].

У другому кварталі 2020 року McAfee Labs спостерігали 419 загроз за хвилину, що майже на 12% більше порівняно з попереднім кварталом. Застосування нової шкідливої програми щодо PowerShell зросла на 117% порівняно з I кварталом, включаючи Donoff PowerShell.

Застосування нової шкідливої програми щодо Office зросло на 103% порівняно з цифрами за перший квартал, включаючи помітне зростання завдяки документам, що породили PowerShell, а саме Donoff.

Застосування нового Malicious Signed Binaries зросло на 25% порівняно з попереднім кварталом, причому частина цього зростання, ймовірно, була зумовлена Android Mobby Adware.

Застосування нового шкідливого забезпечення Coin Miner зросло на 25% порівняно з попереднім кварталом, завдяки розповсюдженню додатків Coin mining та Hashbuster.

Нове зловмисне програмне забезпечення щодо Linux зросло на 22% порівняно з попереднім кварталом, що частково пов'язано з Gafgyt (IoT) та Mirai (IoT). Нове шкідливе програмне забезпечення для мобільних пристроїв зросло на 15% порівняно з попереднім кварталом, частково завдяки Android Mobby Adware.

Нове шкідливе програмне забезпечення для IoT збільшилось на 7%, включаючи зростання завдяки Gafgyt та Mirai. Кількість спостережуваних програм-вимагачів залишалося стабільним в порівнянні з першим кварталом 2020 року. Нове шкідливе ПЗ для iOS впало на 77% разом з зниженням Tiniv після різкого зростання в першому кварталі.

Кількість нових шкідливих програм для експлойтів знизилося на 21% за перший квартал за рахунок зниження кількості Exploit-CVE-2010-2568 і фільтрації Parasitic.

Кількість нових шкідливих програм для Javascript скоротилося на 18% в порівнянні з попереднім кварталом, включаючи скорочення числа майнерів Javascript. Кількість нових шкідливих програм для MacOS скоротилося майже на 8% в порівнянні з попереднім кварталом, про що свідчить зменшення Backdoor Shlayer і Adware Bundlore.

Події в грудні 2020 року, пов'язані з кампаніями SUNBURST, що використовують платформу SolarWinds Orion, виявили новий вектор атаки: ланцюжок поставок, який буде використовуватися і далі [3].

Постійно зростаюче використання підключених пристроїв, програм та веб-сервісів у будинках робить користувачів більш сприйнятливими до домашнього цифрового злому. Ця загроза ускладнюється тим, що багато людей продовжують працювати вдома, тобто ця загроза впливає не лише на споживача та його родину, але й на підприємства [3].

Користувачам мобільних пристроїв потрібно буде остерігатися фішингу чи обманутих повідомлень, спрямованих на їх використання та обман за допомогою мобільних платіжних служб. Використання QR-кодів значно прискорилося під час пандемії, викликаючи привид нового покоління методів соціальної інженерії, які прагнуть використати споживачів та отримати доступ до їх особистих даних[3].

У [3] говориться, що 13 грудня 2020 року галузь кібербезпеки дізналася, що зловмисники скомпрометували програмне забезпечення для моніторингу та управління IT SolarWinds Orion і використовували його для поширення бекдор шкідливого програмного забезпечення під назвою SUNBURST серед десятків клієнтів цієї компанії, включаючи кілька високопоставлених урядових агентств США. Ця кампанія SolarWinds-SUNBURST є першою великою атакою на ланцюжок поставок в своєму роді, і багато хто називає її «Кібер-Перл-Харбор», яку американські експерти з кібербезпеки передбачали вже півтора десятиліття [3]. Зазначається, що використання атаки ланцюжка поставок змінило підхід до захисту від кібератак. Ця атака на ланцюжок поставок діяла в масштабі хробака, такого як WannaCry в 2017 році, в поєднанні з точністю та летальністю атак Sony Pictures 2014 року або Управління кадрів США (OPM) в 2015 році. Через кілька

годин після його виявлення масштаби кампанії стали лякаюче очевидними для організацій, відповідальних за національну безпеку США, економічну конкурентоспроможність і навіть конфіденційність і безпеку споживачів [3].

Це дозволяє противникам США красти інформацію всіма способами, від міжурядових повідомлень до національних секретів. Зловмисники, в свою чергу, можуть використовувати цю інформацію, щоб вплинути або впливати на політику США за допомогою зловмисних витоків. Кожне зламане агентство може мати різні другорядні кібер-бекдори, а це означає, що не існує єдиного рецепту для запобігання вторгнення через федеральний уряд [3].

Хоча деякі можуть стверджувати, що урядові установи є законними цілями для шпигунських дій з боку держави, кампанія SUNBURST також торкнулася приватних компаній. На відміну від державних мереж, які зберігають секретну інформацію в ізольованих мережах, приватні організації часто мають важливу інтелектуальну власність в *мережах з доступом до Інтернету*. Буде важко визначити, яка саме інтелектуальна власність або особисті дані про співробітників були вкрадені, а повний масштаб крадіжки може ніколи не бути відомим [3].

Цей тип атаки також становить загрозу для окремих осіб і їх родин, з огляду на те, що в сьогоднішніх будинках з високим ступенем взаємозв'язку злом компаній побутової електроніки може привести до того, що зловмисники будуть використовувати свій доступ до інтелектуальних пристроїв, таких як телевізори, віртуальні помічники і смартфони, для крадіжки інформації або виступати в якості шлюзу для атак на підприємства, поки користувачі працюють віддалено з дому [3].

Що робить цей тип атаки настільки небезпечним, так це те, що він використовує надійне програмне забезпечення для обходу кіберзахисту, проникнення в організації-жертви за допомогою бекдор і дозволяє зловмиснику зробити будь-яку кількість другорядних кроків. Це може включати в себе крадіжку даних, знищення даних, утримання критичних систем для викупу, організацію збоїв системи, які призводять до кінетичних пошкоджень, або просто імплантацію додаткового шкідливого контенту по всій організації для збереження

контролю навіть після того, як первісна загроза, здається, минула [3].

McAfee [3] вважає, що виявлення кампанії SolarWinds-SUNBURST розкриває методи атак, які інші зловмисники по всьому світу спробують відтворити в 2021 році і в наступний період.

Все більш щільне використання безлічі підключених пристроїв, додатків і веб-сервісів в професійному і приватному житті збільшить поверхню атаки підключеного будинку до такої міри, що це призведе до нових значних ризиків для приватних осіб і їх роботодавців. Хоча загроза для підключених будинків не нова, новиною є поява розширених функціональних можливостей як домашніх, так і бізнес-пристроїв, а також той факт, що ці пристрої підключаються один до одного частіше, ніж будь-коли раніше [3].

Це посилюється збільшенням частки віддаленої роботи – це означає, що багато хто з нас використовують ці підключення пристрою частіше, ніж будь-коли. У 2020 році глобальна пандемія перемістила співробітників з офісу в будинок, перетворивши домашнє середовище в робоче. Фактично, з початку пандемії коронавируса моніторинг пристроїв McAfee Secure Home Platform показує зростання числа підключених домашніх пристроїв на 22% у всьому світі і на 60% в США [3]. Більше 70% трафіку з цих пристроїв виходять від інтелектуальних пристроїв: телефони, ноутбуки, інші ПК і телевізори, а понад 29% – пристрої IoT, такі як пристрої потокової передачі, ігрові консолі, носимі пристрої та інтелектуальні ліхтарі [3].

McAfee побачила, що кіберзлочинці зосередили свою увагу на домашній поверхні атаки, збільшивши кількість різних схем фішингових повідомлень по каналах зв'язку. Кількість шкідливих фішингових посилань, заблокованих McAfee, зросла з березня по листопад більше ніж на 21%, в середньому понад 400 посилань на будинок. *Це збільшення є значним і передбачає потік фішингових повідомлень з шкідливими посиланнями, що потрапляють в домашні мережі через пристрої з більш слабкими заходами безпеки* [3].

Мільйони окремих співробітників стали нести відповідальність за IT-безпеку свого роботодавця в домашньому офісі. Багато з домашніх пристроїв

виробники вже не підтримують оновленнями безпеки, що усувають нові загрози або уразливості. Це контрастує з корпоративним офісним середовищем, заповненим захищеними пристроями та посиленими заходами безпеки корпоративного рівня [3].

Мережеве обладнання споживчого рівня, яке зконфігуроване коистувачами та не має централізованого управління, регулярних оновлень програмного забезпечення та моніторингу безпеки з боку підприємства. З цієї причини кіберзлочинці будуть використовувати будинок як майданчик для атаки для кампаній, націлених не лише на приватних користувачів, а й на корпорації. Хакери скористаються відсутністю в будинку регулярних оновлень прошивки, відсутністю функцій захисту, слабкою політикою конфіденційності, експлойтом вразливостей і вразливістю користувачів до соціальної інженерії. Скомпрометувавши домашнє середовище, ці зловмисники будуть запускати різні атаки як на корпоративні, так і на споживчі пристрої в 2021 році [3].

Пандемія COVID-19 також прискорила темпи переходу корпоративних IT в хмару, збільшуючи потенціал для нових корпоративних схем атак, пов'язаних з хмарою. З ростом впровадження хмарних сервісів та платформ великою кількостю підприємств, що працюють з дому, зростає не тільки кількість користувачів хмари, але і набагато більше даних як в русі, так і в транзакціях [3].

Дані про використання хмари McAfee від більш ніж 30 мільйонів користувачів McAfee MVISION Cloud по всьому світу показують, що загальне використання корпоративної хмари у всіх галузях за перші чотири місяці 2020 року збільшилась на 50%. Microsoft O365 на 123%, збільшення використання бізнес-сервісів, таких як Salesforce, на 61%, а також найбільше зростання сервісів для спільної роботи, таких як Cisco Webex (600%), Zoom (+ 350%), Microsoft Teams (+300 %) тощо [3].

З січня по квітень 2020 року корпоративний хмарний трафік з некерованих пристроїв збільшився на 100% по всіх вертикалях. У той же період McAfee засвідчила сплеск атак на хмарні акаунти, що, за оцінками, в цілому збільшилася на 630%, з варіаціями в секторах, на які були спрямовані атаки [3].

Зростаюча частка некерованих пристроїв, які отримують доступ до корпоративної хмари, *фактично перетворила домашні мережі в розширення корпоративної інфраструктури*. Кіберзлочинці розроблятимуть нові методи атак для підвищення ефективності проти тисяч різнорідних домашніх мереж. Одним із прикладів може бути широко поширена атака методом грубої сили проти користувачів O365, коли зловмисник намагається використовувати вкрадені облікові дані і використовувати погану практику користувачів щодо повторного використання паролів на різних платформах і в різних додатках. Згідно з опитуванням безпеки, проведеного Google в 2019 році, до 65% користувачів повторно використовують один і той же пароль для кількох або всіх облікових записів [3].

Крім того, кіберзлочинці можуть використовувати штучний інтелект і машинне навчання для обходу традиційних технологій мережевої фільтрації, розгорнутих для захисту хмарних сервісів. Замість запуску класичної атаки методом грубої сили з скомпрометованих IP-адрес до тих пір, поки IP-адреси не будуть заблоковані, будуть використовуватися алгоритми оптимізації ресурсів, щоб переконатися, що скомпрометовані IP-адреси запускають атаки проти кількох служб і секторів, щоб максимально продовжити термін служби скомпрометованих IP-адрес, які використовуються для атак. Розподілені алгоритми і навчання з підкріпленням будуть використовуватися для виявлення планів атак, спрямованих, в першу чергу, на запобігання блокуванню облікових записів [3].

McAfee [3] також прогнозує, що в міру розвитку корпоративної хмарної безпеки зловмисники будуть змушені вручну розробляти цілеспрямовані експлойти для конкретних підприємств, користувачів і додатків. Вважається, що в найближчі місяці і роки зловмисники почнуть використовувати поверхні загроз на різних пристроях, в мережах і в хмарі. Також McAfee прогнозує, що витончені кіберзлочинці будуть все частіше націлюватися, залучати і компрометувати корпоративні жертви, використовуючи соціальні мережі як вектор атаки [3].

Кіберзлочинці будуть і далі покладалися на фішингові електронні листи як на вектор атаки для компрометації організацій через окремих співробітників. Однак у міру того, як організації впроваджують системи виявлення спаму, запобігання втрати даних (DLP) і інші рішення для запобігання спроб фішингу на корпоративні облікові записи електронної пошти, більш витончені зловмисники звертаються до співробітників через платформи соціальних мереж, до яких ці всі більш ефективні засоби захисту не можуть бути застосовані [3].

Як висновок, існуючі загрози безпечному доступу користувачів до Інтернет як приватних, так і корпоративних, вимагають залучення зовнішніх ресурсів, створення та застосування відповідних сервісів забезпечення безпеки даного доступу.

1.2. Призначення, функції та компоненти системи доменних імен

Розглянемо систему доменних імен (Domain Name System, DNS) як основу сервісу забезпечення безпеки доступу користувачів до Інтернет.

DNS – це розподілена обчислювальна система, яка забезпечує доступ до ресурсів Інтернету за допомогою зручних для користувача доменних імен, а не IP-адрес, шляхом перетворення доменних імен в IP-адреси і навпаки [4].

Інфраструктура DNS складається з обчислювальних і комунікаційних об'єктів, званих серверами імен, кожен з яких містить інформацію про невелику частину простору доменних імен. Дані доменного імені, що надаються DNS, призначені для доступу до будь-якого комп'ютера, розташованого в будь-якому місці в Інтернеті [4].

Основними цілями безпеки для DNS є цілісність даних і автентифікація джерела, які необхідні для забезпечення дійсності інформації про доменне ім'я і підтримки цілісності інформації, що передається про доменне ім'я [4].

Компоненти DNS часто піддаються атакам типу «відмова в обслуговуванні», мета яких порушити доступ до ресурсів, чиї доменні імена обробляються атакованими компонентами DNS.

Інтернет – найбільша комп'ютерна мережа в світі, яка налічує сотні мільйонів користувачів. З точки зору користувача кожен вузол або ресурс в цій мережі ідентифікується унікальним ім'ям – доменним ім'ям, наприклад www.nist.gov. Однак з точки зору мережевого обладнання, яке спрямовує обмін даними через Інтернет, унікальний ідентифікатор ресурсу – це IP-адреса, наприклад 172.30.128.27. Щоб отримати доступ до Інтернет-ресурсів за допомогою зручних доменних імен, а не IP-адрес, користувачам *потрібна система, яка переводить доменні імена в IP-адреси і навпаки*. Цей переклад є основним завданням механізму, званого системою доменних імен (DNS) [4].

Інфраструктура DNS складається з обчислювальних і комунікаційних об'єктів, географічно розподілених по всьому світу. Існує більше 250 доменів верхнього рівня, таких як .gov і .com, і кілька мільйонів доменів другого рівня, таких як nist.gov і ietf.org [4].

Відповідно, в інфраструктурі DNS є багато серверів імен, кожен з яких містить інформацію про невелику частину простору доменних імен. Інфраструктура DNS функціонує за рахунок співпраці між різними залученими організаціями [4].

Дані доменного імені, що надаються DNS, призначені для доступу до будь-якого комп'ютера, розташованого в будь-якому місці в Інтернеті. Оскільки дані DNS повинні бути загальнодоступними, збереження конфіденційності даних DNS, що відносяться до загальнодоступних IT-ресурсів, не є проблемою. Основними цілями безпеки для DNS є цілісність даних і автентифікація джерела, які необхідні для забезпечення дійсності інформації про доменне ім'я і підтримки цілісності інформації, що передається про доменне ім'я [4].

Доступність служб і даних DNS також дуже важлива; Компоненти DNS часто піддаються атакам типу «відмова в обслуговуванні», мета яких порушити доступ до ресурсів, чиї доменні імена обробляються атакованими компонентами DNS. DNS схильний тим же типам вразливостей (на рівні платформи, програмного забезпечення та мережі), що і будь-яка інша розподілена обчислювальна система. Однак, оскільки це інфраструктурна система для

глобального Інтернету, вона володіє наступними *особливостями*, відсутніми в багатьох розподілених обчислювальних системах [4]:

відсутність чітко визначених кордонів системи – суб'єкти, які беруть участь, не підпадають під дію обмежень географічних або топологічних правил;

немає необхідності в забезпеченні конфіденційності даних – дані повинні бути доступні будь-якій особі, незалежно від її місцезнаходження або приналежності.

Через ці особливості звичайні атаки на мережевому рівні, такі як маскування і фальсифікація повідомлень, а також порушення цілісності розміщених і розповсюджуваних даних, мають зовсім інший набір функціональних впливів, а саме [4]:

маскарад, який підробляє ідентичність вузла DNS, може відмовити в доступі до служб для набору Інтернет-ресурсів, для яких цей вузол надає інформацію (тобто доменів, що обслуговуються вузлом).

Ця відмова призначена не тільки для обмеженого набору клієнтів, але і для всієї сукупності всіх клієнтів, яким необхідний доступ до цих ресурсів;

підроблена інформація DNS, надана маскувальниками або зловмисником, може зламати інформаційний кеш вузла DNS, надаючи цю підмножину інформації DNS (тобто сервер імен, що надає послуги доступу в Інтернет для користувачів підприємства), що призведе до відмови в обслуговуванні ресурсів;

порушення цілісності інформації DNS, резидентної в її авторитетному джерелі, або інформаційному кеші посередника, який накопичив інформацію з кількох історичних запитів, може порушити пов'язаний процес пошуку інформації DNS. Це може привести або до відмови в обслуговуванні для функції розпізнавання імен DNS, або до неправильного перенаправлення користувачів на шкідливий набір незаконних ресурсів;

якщо дані розпізнавання імен, розміщені в системі DNS, порушують вимоги до контенту, визначені в стандартах DNS, це може мати несприятливі наслідки, такі як збільшення робочого навантаження на систему DNS або обслуговування застарілих даних, що може привести до відмови в обслуговуванні інтернет-

ресурсів. У більшості програм незалежність програмних даних (як у звичайних системах управління базами даних (СУБД)) забезпечує певну ступінь захисту від несприятливих впливів через наявність помилкових даних. У разі DNS вміст даних визначає цілісність всієї системи.

Ґрунтуючись на цих функціональних впливах, рекомендації щодо розгортання безпечного DNS, в цілому складаються з наступних загальних і специфічних для DNS рекомендацій [4]:

необхідно запровадити відповідні заходи безпеки системи і мережі для захисту середовища хостингу DNS, такі як виправлення операційної системи і додатків, ізоляція процесів і відмовостійкість мережі;

необхідно забезпечити захист транзакцій DNS, таких як оновлення даних розпізнавання імен DNS і реплікація даних, в яких задіяні вузли DNS, що знаходяться під контролем підприємства. Транзакції повинні бути захищені за допомогою кодів автентифікації повідомлень на основі хешу;

необхідно забезпечити захист повсюдної транзакції запиту/відповіді DNS, яка може включати будь-який вузол DNS в глобальному Інтернеті, з використанням цифрових підписів на основі асиметричної криптографії;

необхідно забезпечити контроль вмісту даних розпізнавання імен DNS за допомогою набору обмежень цілісності, які можуть забезпечити правильний баланс між продуктивністю і цілісністю системи DNS.

Як зазначається в [4] Інтернет є найбільшою комп'ютерною мережою в світі, яка налічує понад 580 мільйонів користувачів. З точки зору користувача кожен вузол або ресурс в цій мережі ідентифікується унікальним ім'ям: доменним ім'ям. Деякі приклади Інтернет-ресурсів:

веб-сервери – для доступу до веб-сайтів;

поштові сервери – для доставки повідомлень електронної пошти;

сервери додатків – для віддаленого доступу до програмних систем і баз даних.

Однак з точки зору мережевого обладнання (наприклад, маршрутизаторів), яке спрямовує пакети зв'язку через Інтернет, унікальний ідентифікатор ресурсу –

це адреса Інтернет-протоколу (IPv4 або IPv6), представлений у вигляді серії з чотирьох чисел, розділених крапками (наприклад, 123.67.43.254). Щоб отримати доступ до Інтернет-ресурсів за допомогою зручних доменних імен, а не цих IP-адрес, користувачам потрібна система, яка переводить ці доменні імена в IP-адреси і навпаки. Цей переклад є основним завданням механізму, званого системою доменних імен (DNS).

Користувачі отримують доступ до Інтернет-ресурсу (наприклад, веб-сервера) через відповідний клієнт або призначену для користувача програму (наприклад, веб-браузер), вводячи ім'я домену. Щоб зв'язатися з веб-сервером і отримати відповідь веб-сторінці браузеру необхідна відповідна IP-адреса. Вона викликає DNS, щоб надати цю інформацію. Ця функція зіставлення доменних імен з IP-адресами називається дозволом імен. Протокол, який DNS використовує для виконання функції розпізнавання імен, називається протоколом DNS [4].

Описана вище функція DNS включає наступні компоненти. По-перше, DNS повинен мати репозиторій даних для зберігання доменних імен і пов'язаних з ними IP-адрес. Оскільки кількість доменних імен велике, міркування масштабованості і продуктивності диктують необхідність його розподілу. Можливо, навіть буде потрібна реплікація доменних імен для забезпечення відмовостійкості.

По-друге, має бути програмне забезпечення, яке управляє цим репозиторієм і забезпечує функцію розпізнавання імен. Ці дві функції (управління репозиторієм доменних імен і надання служби розпізнавання імен) виконуються основним компонентом DNS, сервером імен. Існує безліч категорій серверів імен, що розрізняються за типом обслуговуються даних і виконуваних функцій. Для доступу до служб, що надаються сервером імен DNS від імені користувача програм, існує ще один компонент DNS, званий перетворювач (револьвер). Існує дві основні категорії перетворювачів (кешуючий/рекурсивні/дозволяючий сервери імен та перетворювачі-заглушки), які розрізняються по функціональності.

Протокол зв'язку; різні компоненти DNS; політики, керуючі конфігурацією цих компонентів; процедури для створення, зберігання і використання доменних

імен складають інфраструктуру DNS [4].

Інфраструктура DNS складається з обчислювальних і комунікаційних об'єктів, географічно розподілених по всьому світу. Щоб зрозуміти цю інфраструктуру DNS, необхідно спочатку вивчити структуру організації доменних імен.

Простір доменних імен (сукупність всіх доменних імен) організовано у вигляді ієрархії. Самий верхній рівень ієрархії – це кореневий домен, представлений точкою («.»). Наступний рівень в ієрархії називається доменом верхнього рівня (top-level domain, TLD). Є тільки один кореневий домен, але багато TLD. Кожен TLD називається дочірнім доменом кореневого домена. У цьому контексті кореневий домен є батьківським, оскільки він знаходиться на один рівень вище TLD. У кожного TLD, в свою чергу, може бути багато дочірніх доменів. Нащадки TLD називаються доменами другого рівня або рівня підприємства [4].

У поданні доменного імені символ кореневого домену зазвичай опускається. Наприклад, розглянемо доменне ім'я marketing.example.com. Крайня права мітка в цьому доменному імені («com.») – це TLD. Наступна мітка зліва («example») – це домен другого рівня або рівня підприємства. Крайній лівий мітка («marketing») – це домен третього рівня. Також можливо мати домен четвертого рівня, домен п'ятого рівня і так далі. Оскільки кожна з міток в marketing.example.com називається доменом (TLD, домен другого рівня, домен третього рівня тощо), об'єднання всіх цих міток від поточного рівня до TLD є повністю визначеним доменним ім'ям (fully qualified domain name, FQDN) [4].

Є тільки один кореневий домен. Існує кілька сотень (можливо, скоро будуть тисячі) TLD, розділених на наступні три типи:

country-code TLDs (ccTLDs) – домени, пов'язані з країнами і територіями. Існує більше 240 ccTLD. Приклади включають .uk, .in і .jp;

sponsored generic TLDs (gTLDs) – спеціалізовані домени зі спонсором, які представляють зацікавлену спільноту. Ці TLD включають .edu, .gov, .int, .mil, .aero, .coop і .museum;

unsponsored generic TLDs (gTLDs) – домени без спонсора організації. Список підтримуваних gTLDs включає .com, .net, .org, .biz, .info, .name і .pro.

Існує кілька мільйонів доменів корпоративного рівня (другого рівня або нижче). Фактично, станом на грудень 2008 р тільки в .com gTLDs було понад 77 мільйонів зареєстрованих доменних імен. Часткова ієрархія простору імен DNS показана на рис. 1.2.

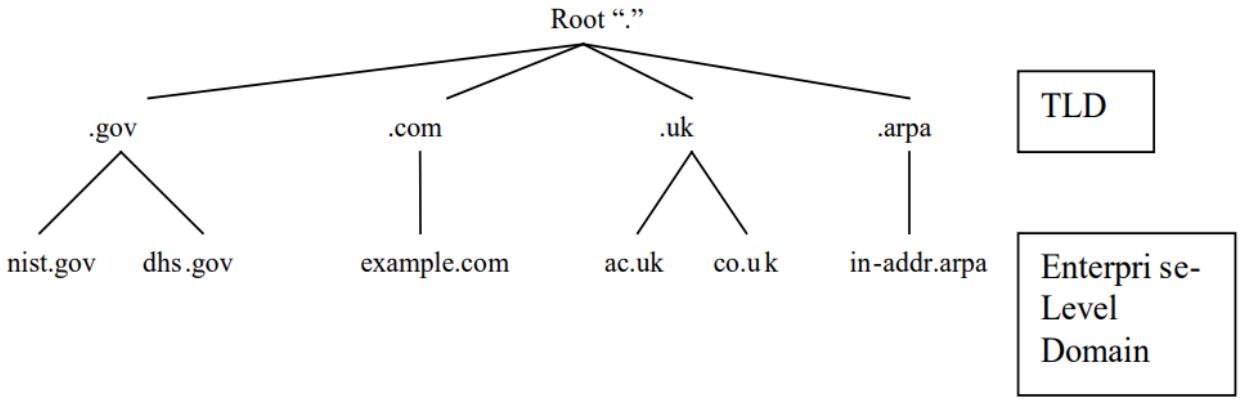


Рис. 1.2. Часткова ієрархія простору імен DNS [4]

В інфраструктурі DNS є багато серверів імен. Кожен сервер імен містить інформацію про частину простору доменних імен. Сервери імен пов'язані з рівнями щодо перших трьох рівнів простору доменних імен. З кореневим рівнем пов'язано 13 серверів імен і вони називаються кореневими серверами. Два кореневих сервера в даний час знаходяться у веденні американської приватної корпорації VeriSign. Інші використовуються іншими організаціями по всьому світу в якості послуг для Інтернет-спільноти [4].

Організації, в яких працюють сервери імен, пов'язані з TLD, називаються реєстрами. Як правило, ccTLD управляються призначеними реєстрами у відповідних країнах, а глобальні реєстри керують gTLD. Наприклад, VeriSign в даний час управляє серверами імен для TLD .com і .net, некомерційна організація під назвою Public Internet Registry (PIR) управляє серверами імен для TLD .org, а інша некомерційна організація EDUCAUSE управляє серверами імен для .edu TLD. Однак всі ці реєстраційні організації можуть бути змінені. Особи, які зареєстрували домен, повинні бути знайомі з контактними особами (званими

реєстраторами) свого конкретного реєстру. Сервери імен, пов'язані з доменами рівня підприємства і нижче, або управляються безпосередньо організаціями, які володіють цими доменами, або передаються на аутсорсинг постачальникам послуг Інтернету (ISP) або іншим постачальникам послуг [4].

Інфраструктура DNS функціонує за допомогою співпраці між різними залученими організаціями (організаціями, які управляють кореневими серверами, реєстрами, які керують TLD тощо). Некомерційна корпорація приватного сектора, Інтернет-корпорація з присвоєння імен і номерів (ICANN), виступає в якості технічного консультанта та координаційного органу по аспектам DNS. Наприклад, ICANN формулює політику управління кореневими серверами. ICANN також є органом для створення нових TLD. ICANN була створена в 1998 році Міністерством торгівлі США [4].

Користувач (тобто фізична або юридична особа), який бажає зареєструвати доменне ім'я (яке може бути тільки доменом корпоративного рівня в рамках TLD), повинен зв'язатися з уповноваженим органом, званим реєстратором (який може стягувати плату, залежно від TLD). Реєстратори – це компанії, які уповноважені реєструвати доменні імена в конкретному TLD (або навіть в субдомені TLD, наприклад, co.uk.) для кінцевих користувачів. Реєстратори є по всьому світу. Коли реєстратор отримує запит на реєстрацію користувача, реєстратор перевіряє доступність імені, звіряючись з реєстром, який керує відповідним TLD (або субдоменів в TLD). Якщо ім'я є, реєстратор реєструє ім'я у відповідному реєстрі. Потім реєстр додає нове ім'я в свою базу даних реєстру і публікує нове ім'я в DNS. Зверніть увагу, що в деяких доменах (наприклад, в деяких кодах країн gTLDs) одна і та ж організація виступає в якості реєстру і реєстратора для імен в домені. Не існує проміжної організації, яка реєструє доменні імена від імені власника домену [4].

Організаціям, які реєструють і отримують доменне ім'я рівня підприємства, часто доводиться створювати дочірні домени для правильної ідентифікації Інтернет-ресурсів, пов'язаних з різними функціональними одиницями. Наприклад, власник доменного імені example.com може створити піддомен доставки для

створення та ідентифікації ресурсів, пов'язаних з відділом доставки організації. Точно так само багато інших піддомени (в даному контексті домени третього рівня) можуть бути створені для правильної ідентифікації всіх Інтернет-ресурсів організації. Однак часто в якій-небудь одній організації (власник домену другого рівня) буде багато доменів третього рівня, але мало Інтернет-ресурсів (веб-серверів, серверів додатків тощо) у кожному з цих доменів. Отже, неекономічно призначати унікальний сервер імен для кожного з цих доменів третього і нижнього рівня. Крім того, з адміністративної точки зору зручно згрупувати всю інформацію, що стосується основного домену організації (тобто домену другого рівня або рівня підприємства) і всім його піддоменів, в один ресурс і керувати ним як єдиним цілим [4].

Щоб полегшити це групування, DNS визначає поняття зони. Зона може бути або цілим доменом, або доменом з одним або декількома піддоменами. Зона – це об'єкт на сервері імен, який настроюється та під яким описується інформація про всі Інтернет-ресурси, що відносяться до домену і заданого набору піддоменів. Таким чином, зони є адміністративними компонентами простору імен DNS, так само як домени є структурними компонентами.

В результаті термін *зона* зазвичай використовується навіть для позначення домену, який управляється як автономний адміністративний об'єкт (наприклад, коренева зона, зона .com). Термін *зона* використовується для позначення об'єкта ресурсу, який містить інформацію про один або декількох доменах і управляється як єдиний адміністративний об'єкт. Іншими словами, зона – це ресурс всередині розгорнутої установки сервера імен, який настроюється та містить інформацію про доменне ім'я [4].

Володіючи цим загальним знанням інфраструктури DNS (серверів імен та перетворювачів), доменних імен, зон, серверів імен різних рівнів (наприклад, кореневих серверів і серверів TLD) і перетворювачів, функція розпізнавання імен тепер може бути визначена більш докладно. Коли користувач вводить URL-адресу www.example.com в веб-браузер, програма браузера звертається до певного типу перетворювача, званому перетворювачем-заглушкою, який потім зв'язується

з локальним сервером імен (званим рекурсивним сервером імен або сервером перетворення імен).

Дозволяючий сервер імен перевірить свій кеш, щоб визначити, чи є у нього справжня інформація (інформація визначається як дійсна на основі відповідних критеріїв), щоб надати IP-адресу для доступного інтернет-ресурсу (www.marketing.example.com). Якщо немає, дозволяючий сервер імен перевіряє кеш, щоб визначити, чи є в ньому інформація про сервер імен для зони marketing.example.com (оскільки це зона, яка, як очікується, буде містити ресурс www.marketing.example.com).

Якщо IP-адреса сервера імен знаходиться в кеші, наступний запит перетворювача буде спрямований проти цього сервера імен. Якщо IP-адреса сервера імен marketing.example.com недоступний в кеші, перетворювач визначає, чи є у нього інформація про сервер імен для зони, яка на один рівень вище, ніж marketing.example.com (наприклад, example. com). Якщо інформація про сервер імен для example.com недоступна, наступним пошуком буде сервер імен зони .com в кеші [4].

Якщо повний пошук в кеші (як описано вище) не дає необхідної інформації, дозволяючий сервер імен не має альтернативи, крім як почати пошук з запиту сервера імен в самій верхній зоні в ієрархії простору імен DNS (кореневий сервер). Якщо пошук в кеші успішний, та дозволяючий сервер імен повинен запросити сервери імен на одному з рівнів нижче кореневої зони (в даному контексті – marketing.example.com, example.com або .com). Оскільки набір ітеративних запитів, що починаються з кореневого сервера, включає набір, що починається з будь-якого з серверів нижнього рівня, в цьому розділі описується процес розпізнавання імен, починаючи з запиту, відправленого на кореневий сервер що дозволяє сервером імен на рівні підприємства [4].

Зв'язок з кореневими серверами забезпечується так званим файлом «кореневих підказок», який зазвичай присутній на кожному сервері імен в DNS. Файл кореневих підказок містить IP-адресу одного або декількох з 13 кореневих серверів. Кореневий сервер буде містити інформацію про сервери імен для своїх

дочірніх зон (TLDs). TLD (наприклад, .com) буде містити інформацію сервера імен про своїх дочірніх зонах (наприклад, example.com). Інформація сервера імен про його дочірні зони, яка передається в зоні, називається інформацією про делегування. Інформація про делегування – це та, яка використовується зоною для посилання на запити дозволу імен для ресурсу нижче, ніж він в ієрархії доменних імен [1].

Оскільки запит на дозвіл імен в цьому прикладі відноситься до ресурсу в домені третього рівня, кореневий сервер повинен направити запит на сервер імен нижчого рівня. Відповідь дозволяючого сервера імен, який включає відправку цієї інформації щодо делегування, називається відсиланням. Посилання надає ім'я та IP-адреса для серверів імен для зони TLD, яка має відношення до запиту (зона .com) (оскільки запит відноситься до ресурсу в marketing.example.com). Використовуючи це посилання дозволяючий сервер імен потім формулює і відправляє запит на сервер імен зони .com. Цей сервер буде надавати посилання на сервер імен example.com. Якщо домен marketing.example.com входить в зону example.com, запит сервера імен для example.com надасть IP-адресу ресурсу www.marketing.example.com. Схема процесу розпізнавання імен (без операцій пошуку в кеші) приведена на рис. 1.3.

Як зрозуміло з опису процесу розпізнавання імен, сервер імен виконує наступні функції [4]:

забезпечує напрямок в дочірню зону;

забезпечує відображення доменного імені в IP-адресу, зване дозволом доменного імені, або IP-адреса в доменне ім'я, яке іноді називають зворотним дозволом, але насправді це стандартний запит для іншого типу даних;

видає повідомлення про помилку, якщо запит стосується неіснуючого запису DNS.

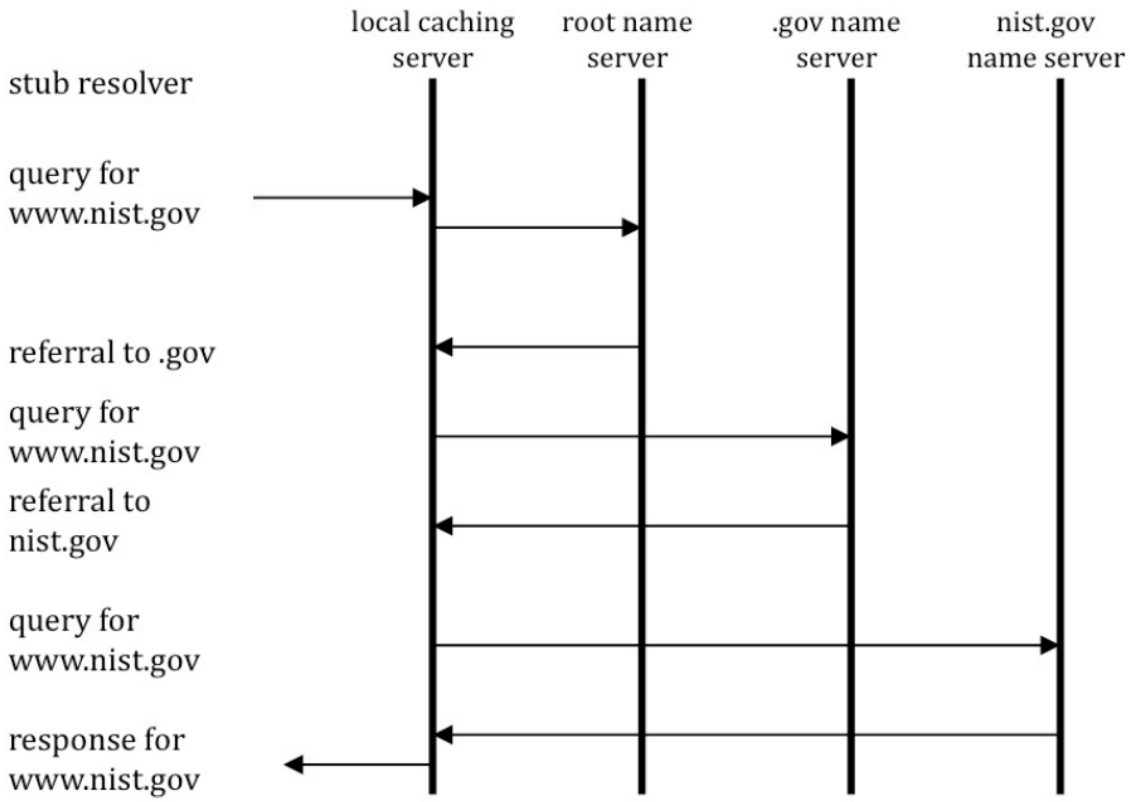


Рис. 1.3. Процес розпізнавання імен (без пошуку в кеші) [4]

Сервер імен виконує ці три функції з тією ж базою даних DNS, яка називається файлом зони. Клас інформації, званий інформацією про делегування, містить інформацію про сервер імен для дочірніх зон в батьківській зоні і використовується при виконанні функції посилання. Функція зіставлення виконується класом інформації в файлі зони, званим авторитетною інформацією, і надається набір ключових слів, в яких перераховані ресурси в цій зоні разом з її доменним ім'ям і відповідною IP-адресою. Оскільки ресурси належать цій зоні, надана інформація вважається достовірною [4].

Таким чином, файл зони містить дві категорії інформації: авторитетна інформація (інформація про всі ресурси для всіх доменів в зоні) і інформація про делегування (інформація про сервери імен для дочірніх зон). Місця в файлі зони, де відображається інформація про делегування, називаються точками делегування. Рівень файлу зони – це рівень самого верхнього домену, для якого він містить достовірну інформацію. У попередньому прикладі файл зони на сервері імен example.com є файлом зони рівня підприємства, а відповідний сервер

імен називається сервером імен рівня підприємства.

Розглянемо компоненти DNS і цілі забезпечення безпеки.

Перш ніж можна буде визначити цілі безпеки, необхідно вказати компоненти DNS. DNS включає в себе наступні об'єкти [4]:

платформа (обладнання та операційна система), на якій знаходяться сервер імен та перетворювачі;

сервер імен та програмне забезпечення перетворювача;

транзакції DNS;

база даних DNS (файли зон);

файли конфігурації на сервері імен та перетворювачі.

Мережева технологія рівня доступу до середовища передачі (тобто мережа Ethernet, що з'єднує заглушку перетворювача і локальний дозволяючий сервер імен) не включена у визначення DNS.

Приватна власність, цілісність, доступність і автентифікація джерела є загальними цілями безпеки для будь-якої електронної системи. Однак очікується, що DNS надаватиме інформацію про дозвіл імен для будь-якого загальнодоступного Інтернет-ресурсу. Отже, за винятком даних DNS, що відносяться до внутрішніх ресурсів (наприклад, серверів всередині брандмауера тощо), які надаються внутрішніми серверами імен DNS через захищені канали, дані DNS, що надаються загальнодоступними серверами імен DNS, не вважають конфіденційними. Отже, конфіденційність не є однією з цілей безпеки DNS. Забезпечення достовірності інформації і підтримка цілісності переданої інформації має вирішальне значення для ефективного функціонування Інтернету, для якого DNS надає послугу розпізнавання імен. Отже, цілісність і автентифікація джерела є основними цілями безпеки DNS [4].

Через величезне розмаїття платформ серверів імен та базових мереж, в яких знаходяться компоненти DNS (наприклад, програмне забезпечення сервера імен та програмне забезпечення перетворювача), запобігти всім типам атак типу «відмова в обслуговуванні» неможливо. Однак необхідно дотримуватися деяким базовим керівним принципам, щоб запобігти атакам типу «відмова в

обслуговуванні», які використовують уразливості в платформі сервера імен, вміст даних файлу зони і конфігурацію управління доступом для певних транзакцій DNS [4].

Існує три основних рівня серверів імен: кореневі сервери імен, сервери імен TLD і сервери імен корпоративного рівня.

1.3. Аналіз існуючих підходів до забезпечення безпечного доступу користувачів до Інтернет

Пересічні та бізнес-користувачі можуть вибирати резервні резольвери DNS. Добре відомі загальнодоступні резольвери:

Cloudflare (1.1.1.1 та 1.0.0.1);

Cisco (208.67.222.222 та 208.67.220.220);

Google (8.8.8.8 та 8.8.4.4);

Quad9 (9.9.9.9 та 149.112.112.112).

Розглянемо найбільш відомі DNS резольвери.

1.1.1.1 – це загальнодоступний розв’язувач DNS, керований Cloudflare, який пропонує швидкий та приватний спосіб перегляду Інтернету. На відміну від більшості розв’язувачів DNS, 1.1.1.1 не продає дані користувачів рекламодавцям. Окрім того, 1.1.1.1 визнано найшвидшим доступним розв’язувачем DNS [5].

DNS розв’язувач – це тип сервера, який управляє перекладом “ім’я до адреси”, в якому IP-адреса узгоджується з доменним ім’ям і надсилається назад на комп’ютер, який його запитував. Розв'язувачі DNS також відомі як рекурсивні розв'язувачі.

Комп’ютери налаштовані на розмову з конкретними засобами вирішення проблем DNS є ідентифікованими за IP-адресою. Зазвичай конфігурацією керує постачальник послуг Інтернету (ISP) користувача в домашніх або бездротових з’єднаннях, а адміністратор мережі – в офісних. Користувачі також можуть вручну змінити засіб розпізнавання DNS спілкування їхніх комп'ютерів [5].

Навіщо використовувати 1.1.1.1 замість розв’язувача ISP? Основні причини

переходу на сторонній розв’язувач DNS – це підвищення безпеки та підвищення швидкості роботи. Що стосується безпеки, Інтернет-провайдери не завжди використовують сильне шифрування на своєму DNS або підтримують протокол безпеки DNSSEC, роблячи їх запити DNS вразливими до порушень даних та піддаючи користувачів таким загрозам, як атаки на шляху. Крім того, провайдери часто використовують записи DNS для відстеження активності та поведінки своїх користувачів [5].

З точки зору продуктивності, розв’язувачі DNS-провайдерів можуть бути повільними та можуть перевантажуватися через інтенсивне використання. Якщо в мережі достатньо трафіку, розпорядник послуг Інтернет-провайдера може взагалі перестати відповідати на запити. У деяких випадках зловмисники навмисно перевантажують рекурсори провайдера, що призводить до відмови в обслуговуванні [5].

Різноманітні служби DNS підтримують DNSSEC. Хоча це хороша практика безпеки, вона не захищає запити користувачів від самих DNS компаній. Багато з цих компаній збирають дані від своїх клієнтів DNS для використання в комерційних цілях, таких як продаж рекламодавцям [5].

На відміну від цього, 1.1.1.1 не виконує збір даних користувачів. Журнали зберігаються протягом 24 годин для налагодження, а потім видаляються. 1.1.1.1 також пропонує функції безпеки, недоступні для багатьох інших загальнодоступних служб DNS, такі як мінімізація імен запитів. Мінімізація імен запитів покращує конфіденційність, лише включаючи до кожного запиту мінімальну кількість інформації, необхідної для цього кроку в процесі вирішення. Потужність мережі Cloudflare дає 1.1.1.1 природну перевагу з точки зору швидких запитів DNS. Оскільки він інтегрований у мережу Cloudflare, яка охоплює 200 глобальних міст, користувачі в будь-якій точці світу отримують швидку відповідь з 1.1.1.1 [5].

Крім того, центри обробки даних у мережі мають доступ до приблизно 25 мільйонів властивостей Інтернету на платформі Cloudflare, що робить запити щодо цих доменів блискавично швидкими. Загалом, незалежний монітор DNS

DNSPerf визначає 1.1.1.1 як найшвидшу службу DNS у світі (рис. 1.4.) [5].

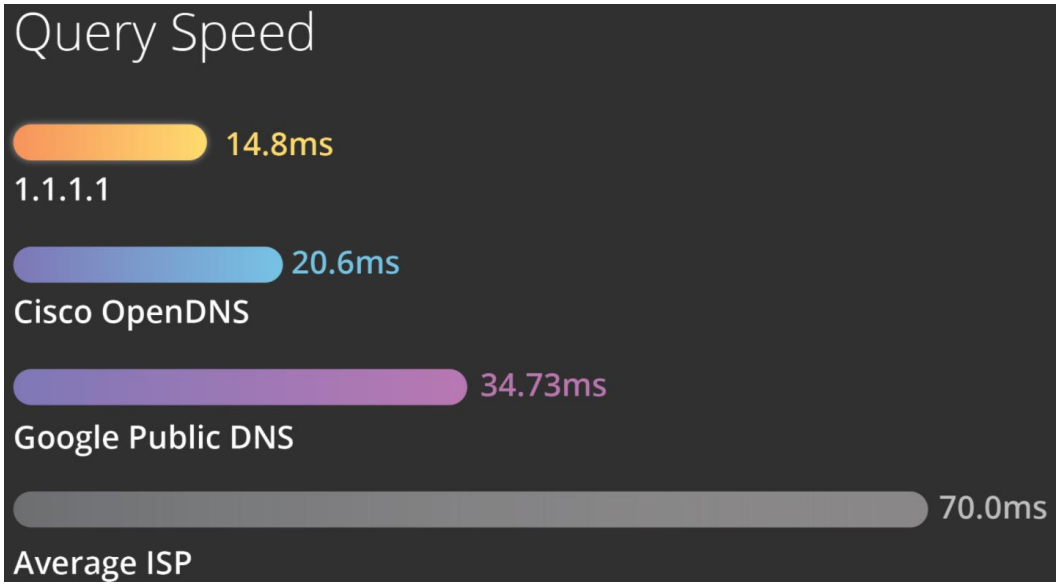


Рис. 1.4. Порівняння швидкості обміну даними служб DNS [5]

Також компанія Cloudflare пропонує сервіс WARP. WARP це додатковий додаток, побудований на версії 1.1.1.1. WARP створює безпечне з'єднання між особистими пристроями (наприклад, комп'ютерами та смартфонами) та послугами, до яких користувач отримує доступ в Інтернеті. 1.1.1.1 захищає лише запити DNS, а WARP захищає весь трафік, що надходить з пристрою користувача. WARP робить це шляхом маршрутизації трафіку через мережу Cloudflare, а не через загальнодоступний Інтернет. Cloudflare автоматично шифрує весь трафік і часто може пришвидшити його, перенаправляючи по маршрутах із низькою затримкою [5].

Таким чином, WARP пропонує деякі переваги безпеки служби віртуальної загальнодоступної мережі, без штрафів за продуктивність та проблем конфіденційності даних, які приносять багато комерційних VPN [5].

1.1.1.1 повністю безкоштовний. Налаштування на настільному комп’ютері займає хвилини і не вимагає технічних навичок або спеціального програмного забезпечення. Користувачі можуть просто відкрити Інтернет-налаштування свого комп’ютера та замінити IP-адресу існуючої служби DNS адресою 1.1.1.1 [5].

OpenDNS від Cisco Systems найбільший і надійний рекурсивний DNS сервіс, що забезпечує кращий доступ до Інтернету для більш ніж 30 мільйонів Інтернет-

користувачів у всьому світі. Безкоштовний сервіс Premium DNS забезпечує безпечний, швидкий і найбільш надійний Інтернет [6].

Основні переваги OpenDNS [6]:

прискорює реакцію на DNS-запити. Дванадцять глобальних дата-центрів OpenDNS стратегічно розташовані в місцях найбільш стабільного і швидкого Інтернет-з'єднання. На відміну від інших провайдерів, OpenDNS використовує складну технологію маршрутизації Anycast, що дозволяє на DNS-запити користувача відповідати з найближчого дата-центру, де б він не знаходився. OpenDNS, в поєднанні з найбільшому в індустрії кешом DNS, надає відповіді на DNS-запити швидше інших провайдерів;

підвищує надійність Інтернету. З великою мережею дата-центрів і технологією Anycast мережі OpenDNS забезпечують нульову затримку для веб-ресурсів. Технологія SmartCache дозволяє отримати доступ до сайтів, які в звичайній ситуації були б недоступні через відмову DNS, тим самим забезпечується надійність Інтернет-можливостей;

підвищує безпеку Інтернету. OpenDNS володіє і управляє технологією PhishTank, найбільшим центром по виявленню фішинг-інформації в Інтернеті. Використання послуг PhishTank дозволяє захистити користувачів від шахрайських веб-сайтів, які намагаються викрасти їх особисті дані і гроші. Крім цього, OpenDNS Premium DNS захищає від найпоширеніших Інтернет-загроз, які продовжують заражати мільйони користувачів: Conficker, найбільші бот-мережі, а також експлойти веб-браузера Internet Explorer;

проста установка. Базові можливості безкоштовні. Налаштування для початку роботи з OpenDNS Premium DNS займає кілька хвилин. Не потрібно ніяких завантажень і додаткового програмного забезпечення. Всі базові можливості надаються безкоштовно.

Розглянемо сервіс Google Public DNS. Оскільки веб-сторінки стають більш складними та включають більше ресурсів із декількох доменів походження, клієнтам потрібно виконати кілька пошуків DNS, щоб відтворити одну сторінку. Пересічний користувач Інтернету виконує сотні пошуків DNS щодня,

уповільнюючи роботу в Інтернеті. Оскільки Інтернет продовжує рости, все більше навантаження покладається на існуючу інфраструктуру DNS [7].

Оскільки пошукова система Google щодня сканує Інтернет і в процесі вирішує та кешує інформацію DNS, то існує можливість використати дану технологію для експериментів з новими способами вирішення деяких існуючих проблем DNS щодо продуктивності та безпеки. Google пропонує послугу користувачам в надії досягти наступних цілей [7]:

надання кінцевим користувачам альтернативу поточній службі DNS. Google Public DNS застосовує деякі нові підходи, які, на їх думку, пропонують більш вагомі результати, підвищений рівень безпеки та, в більшості випадків, кращу продуктивність;

допомога зменшення навантаження на DNS-сервери провайдерів. Скориставшись перевагами глобального центру обробки даних та інфраструктури кешування Google, можна безпосередньо обслуговувати велику кількість запитів користувачів, не вимагаючи запитів інших розв’язувачів DNS;

допомога зробити Інтернет швидшим та безпечнішим. Google запускає цю послугу, щоб перевірити деякі нові способи вирішення проблем, пов’язаних із DNS. Вони сподіваються поділитися тим, що дізнаються, з розробниками DNS-розв’язувачів та веб-спільнотою та отримати їхні відгуки.

Google Public DNS це рекурсивний розв’язувач DNS, подібний до інших загальнодоступних служб. Він забезпечує багато переваг, включаючи покращений захист, швидку продуктивність та більш достовірні результати.

Однак Google Public DNS не є одним із наведених нижче [7]:

служба імен домену верхнього рівня (TLD);

сервіс DNS-хостингу або відмови. Google Public DNS не є стороннім постачальником послуг DNS-додатків, який розміщує достовірні записи для інших доменів. Якщо необхідно широкомасштабний, програмований, авторитетний сервер імен, що використовує інфраструктуру Google, спробуйте Cloud DNS від Google;

авторитетна служба імен. Загальнодоступні DNS-сервери Google не є

авторитетними для жодного домену. Google підтримує ще один набір серверів імен, які є авторитетними для зареєстрованих доменів, розміщений на .google.com;

служба блокування шкідливого програмного забезпечення. Загальнодоступний DNS Google рідко виконує блокування або фільтрацію, хоча може, якщо це необхідно для захисту користувачів від загроз безпеці. У таких надзвичайних випадках він просто не може відповісти; це не створює змінених результатів.

Google Public DNS впроваджує низку поліпшень безпеки, продуктивності та відповідності [7]:

Продуктивність. Багато постачальників послуг DNS не мають достатньої підготовки, щоб мати можливість підтримувати великі обсяги введення/виведення та кешування та адекватно збалансувати навантаження між своїми серверами. Google Public DNS використовує великі об’єми кеш-пам’яті в масштабі Google та балансує навантаження користувацького трафіку для забезпечення спільного кешування, дозволяючи відповідати на значну частину запитів із кешу.

Безпека. DNS вразливий до різного роду підробних атак, які можуть вразити кеш-пам'ять сервера імен і направити його користувачів на шкідливі сайти. Поширеність експлойтів DNS означає, що провайдерам доводиться часто застосовувати оновлення та виправлення серверів. Крім того, відкриті DNS-розробники вразливі для використання для запуску атак відмови в обслуговуванні (DoS) на інші системи. Для захисту від таких атак Google впровадив кілька рекомендованих рішень, щоб допомогти гарантувати достовірність відповідей, які він отримує від інших серверів імен, а також забезпечити, щоб його сервери не використовувались для запуску DoS-атак. Окрім повної підтримки протоколу DNSSEC, вони включають додавання ентропії до запитів, обмеження швидкості клієнтського трафіку тощо.

Крім того, Google Public DNS може не вирішувати певні домени, якщо вважаємо, що це необхідно для захисту користувачів Google від загроз безпеці.

Правильність. Google Public DNS робить все можливе, щоб щоразу

повертати правильну відповідь на кожен запит відповідно до стандартів DNS. Іноді, у разі запиту щодо помилково введеного або неіснуючого доменного імені, правильна відповідь означає відсутність відповіді або повідомлення про помилку із зазначенням доменного імені не може бути вирішено. Це також може не вирішити певні домени, якщо вважається, що це необхідно для захисту користувачів від загроз безпеці. Google Public DNS ніколи не переспрямовує користувачів, на відміну від деяких відкритих розв’язувальних пристроїв та провайдерів.

Quad9 – це безкоштовна рекурсивна платформа DNS з довільним доступом, яка забезпечує кінцевим користувачам надійний захист, високу продуктивність і конфіденційність. Quad9 був розроблений Global Cyber Alliance (GCA), міжнародною некомерційною організацією, заснованою партнерством правоохоронних і дослідницьких організацій, орієнтованих на боротьбу з системними кіберризиками реальними, вимірними способами [1].

Quad9 блокує відомі шкідливі домени, запобігаючи підключення комп'ютерів і пристроїв Інтернету речей організації до шкідливих або фішингових сайтів. Кожен раз, коли користувач Quad9 натискає на посилання веб-сайту або вводить адресу в свій веб-браузер, Quad9 перевіряє сайт за списком доменів, складеним більш ніж з 18 різних партнерів з аналізу загроз. Кожен партнер по аналізу загроз надає список шкідливих доменів, заснований на евристичному аналізі чинників, таких як виявлення відсканованих шкідливих програм, поведінку мережевих IDS в минулому, розпізнавання візуальних об'єктів, оптичне розпізнавання символів (OCR), структура і зв'язок з іншими сайтами, а також з окремими повідомлення про підозрілу або зловмисну поведінку [1].

На основі результатів Quad9 дозволяє або відхиляє спробу пошуку, запобігаючи підключення до шкідливим сайтам при збігу. Quad9 направляє запити DNS вашої організації через захищену мережу серверів по всьому світу. Його настройка дуже проста, так як не потрібно ніякої реєстрації, і, що найбільш важливо, вона служить дуже винахідливою безкоштовної службою блокування, доступною для будь-якої організації або окремої особи [1].

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ДОСТУПУ КОРИСТУВАЧІВ ДО ІНТЕРНЕТ НА БАЗІ DNS-ПЛАТФОРМИ QUAD9

2.1. Призначення та основні функції DNS-платформи Quad9

Quad9 – це рекурсивна служба DNS, яка забезпечує захист кібербезпеки від шкідливого програмного забезпечення та фішингу. Як неприбуткова організація, Quad9 не збирає та не перепродає персональні дані користувачів та надає надійні послуги приватним особам та організаціям безкоштовно та без договору. Організація була започаткована в 2017 році і зараз вона працює в більш ніж 150 місцях у 90 країнах. Quad9 існує для покращення захисту та конфіденційності кінцевих користувачів у всьому світі, сприяння стабільності та безпеки Інтернету [8].

Quad9 безкоштовний і доступний у всьому світі. Користувачі можуть налаштувати DNS-пристрої на своєму комп'ютері на таких даних 9.9.9.9, 149.112.112.112 та 2620:FE::FE.

Quad9 це перше рішення безпеки DNS, яке поширює захист конфіденційності GDPR на користувачів Інтернету по всьому світу. Quad9, глобальна, неприбуткова система безпеки доменних імен (DNS), оголосила про перенесення своєї штаб-квартири з Каліфорнії в Цюріх, Швейцарія, за підтримки Пакетного центру обміну та SWITCH [8].

Quad9 відокремився від інших постачальників DNS, добровільно поставивши себе під юрисдикцію, яка суворо виконує закони про конфіденційність відповідно до найвищих світових стандартів. Вважається оплотом особистих прав, Швейцарія має законний режим конфіденційності, гармонізований із загальноєвропейським Загальним положенням про захист даних (GDPR). Він надає фізичним особам примусові права та ефективні засоби правового захисту, надаючи користувачам Quad9 по всьому світу повний захист

швейцарським законодавством. Ці та інші важливі поступки та висновки законодавства швейцарського уряду, які забезпечують конфіденційність та безпеку користувачів Quad9, зробили вибір доміцилянта Quad9 природним [8].

Quad9 – єдиний глобальний постачальник послуг безпеки DNS, який пропонує ці універсальні засоби захисту конфіденційності. На відміну від комерційних операторів DNS, які отримують прибуток від продажу особистої інформації користувачів та історії перегляду Інтернету, Quad9 не збирає жодної особистої інформації. Запити та адреси користувачів не збираються і не записуються, і, отже, жодна третя сторона не має до них доступу. Quad9 – це неприбуткова організація з прозорим управлінням та фінансами, що підтримується за рахунок пожертв та спеціалізується виключно на функціонуванні приватних та безпекових служб DNS [8].

Так Джон Тодд, генеральний менеджер Quad9, зазначив: «Претензії щодо захисту конфіденційності рішень щодо безпеки DNS мають значення лише у тому випадку, якщо вони зобов’язані законодавством та забезпечуються уповноваженим органом влади. Політика конфіденційності, яка не підкріплена законом, є порожніми обіцянками» [8].

Quad9 знаходиться під наглядом Федерального уповноваженого з питань захисту даних та інформації та підпорядковується швейцарській юрисдикції. Швейцарський закон про захист даних не містить жодних обмежень щодо громадянства або місця проживання осіб, чиї особисті права мають бути захищені законом. Використовуючи Quad9, будь-хто у світі може отримати такий самий, повністю законно забезпечений захист, як громадянин Швейцарії [8].

Щоразу, коли користувачі користуються Інтернетом, вони залишають цифрові сліди. Рекурсивні постачальники DNS – це точка затримки, через яку проходять усі дії користувачів, і саме тут особиста інформація може бути перевірена, записана та перетворена у досьє на продаж. На відміну від інших великих DNS-провайдерів, які проживають у США – юрисдикції, яка захищає їх від вимог щодо конфіденційності та відповідальності перед користувачами, Quad9 поставив під юридичну силу сильний регулятор конфіденційності. Міцність

швейцарського законодавства у поєднанні з місією Quad9 та прозорою практикою конфіденційності гарантують, що персональні дані ніколи не будуть збиратися, аналізуватися або продаватися [8].

Quad9 виконує відповідну функцію захисту від кіберзлочинності. Незалежні тести показують, що Quad9 також попереджає підключення пристроїв користувачів до 97% шкідливих веб-сайтів. Щоб досягти цього показника успіху, Quad9 збирає інформацію багатьох аналітиків кіберзагроз, включаючи SWITCH, для формування унікальної всеосяжної бази даних шкідливих доменів. Коли користувач Quad9 підключається до Інтернету, Quad9 перевіряє місце призначення в цій базі даних і блокує з'єднання, якщо підключення до нього може зашкодити користувачеві. Quad9 працює в більш ніж 150 місцях у дев'яносто країнах і щодня захищає користувачів Інтернету від понад шістдесяти мільйонів шкідливих атак [8].

Як зазначив Том Клейбер, керуючий директор SWITCH: «Менш ніж за п'ять років Quad9 створив глобальну альтернативу комерційним платформам DNS, орієнтованим на отримання прибутку від даних користувачів. Ми з нетерпінням чекаємо розширення охоплення та впливу Quad9, щоб показати користувачам Інтернету по всьому світу, що безпеку можна покращити, не використовуючи їх конфіденційність» [8].

2.2. Принцип роботи DNS-платформи Quad9

Система доменних імен (DNS) – найважливіший компонент Інтернету. Дана система служить «перекладачем» між розпізнаваними людьми доменними іменами і розпізнаваними машинами місцями розташування в Інтернеті і вважається основною службою для функціонування Інтернету. Хоча DNS зазвичай не використовується в якості засобу контролю безпеки, вона використовувалася для сервісів безпеки інфраструктури.

Захисна DNS (також відома як «брандмауер DNS») – служба DNS, яка обробляє запит як зазвичай, але запобігає перетворення домену для будь-яких

доменів, які вважаються шкідливими [9].

Вважається, що брандмауери DNS є ефективним засобом контролю безпеки, а наявність відкритих або безкоштовних брандмауерів DNS робить це рішення дуже рентабельним. Більш того, інтерактивні навчальні програми і відносна простота настройки спрощують реалізацію цього ефективного засобу захисту навіть для домашнього або особистого використання [9].

Передбачається, що брандмауери DNS могли б пом'якшити одну третину інцидентів, які мають місце, а також могли б запобігти збиткам в розмірі 10 мільярдів доларів в цих інцидентах. Крім того, оскільки цілком імовірно, що захисний DNS (PDNS) міг би зіграти роль в запобіганні однієї третини всіх порушень, то, якби глобальні збитки від порушень склали, наприклад, 300 мільярдів доларів, PDNS могла б зіграти роль у запобіганні 100 мільярдів доларів збитків [9].

Система доменних імен (DNS) має фундаментальне значення для роботи Інтернету. DNS забезпечує переклад імен легких для читання, таких як «globalcyberalliance.org», на комп'ютерні адреси, наприклад 35.202.169.15. Брандмауер DNS захищає користувачів, автоматично блокуючи доступ до відомих шкідливих і небажаних веб-сайтів. Давайте розглянемо найпоширеніший сценарій, а потім покажемо, як він змінюється у разі застосування брандмауера DNS [9].

Розглянемо як працює система без брандмауера DNS [9]:

1. Користувач натискає на посилання, заходить на небезпечний веб-сайт (evil.example.com) і завантажує програму установки шкідливого ПЗ.

2. Програма установки підключається до сайту (bigevil.example.net) з додатковим шкідливим ПЗ, яке ще більше заражає систему.

3. Шкідлива програма взаємодіє з інфраструктурою Command and Control (C&C) (cc.example.org), яка потім може використовувати систему в зловмисних цілях.

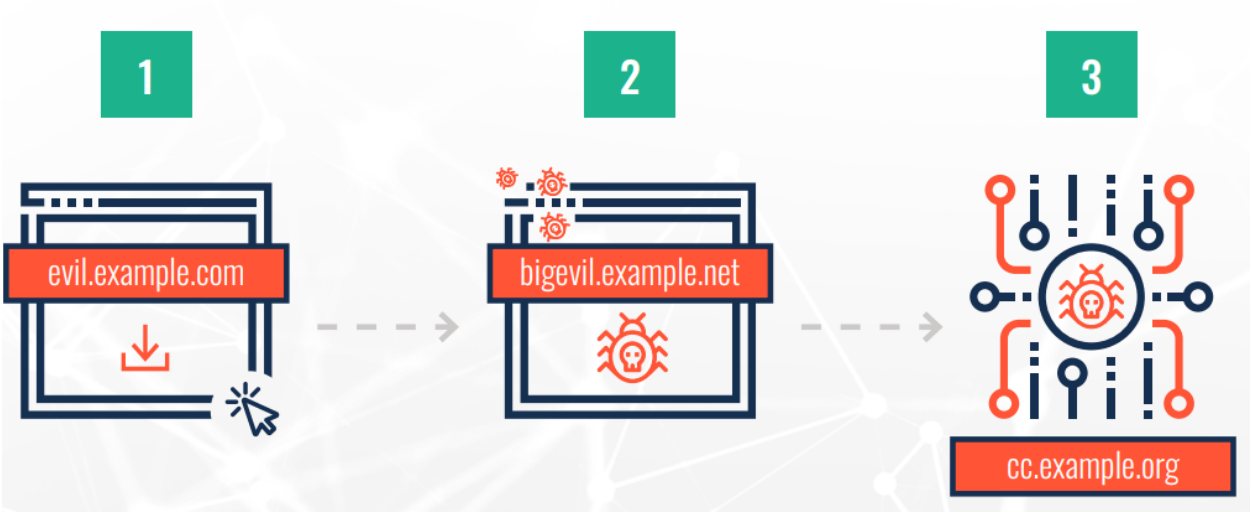


Рис. 2.1. Робота системи без брандмауера DNS [9]

Розглянемо як працює система з брандмауером DNS [9]:

1. Коли людина натискає на (шкідливе) посилання, його браузер зв'язується з DNS-сервером для розв’язання домену. На цьому етапі, якщо сервер знає, що домен є шкідливим, він може відповісти повідомленням «не знайдено». Це призведе до того, що браузер видасть помилку «Не можу знайти цей сайт». Це ефективно запобігає первинній установці шкідливого ПЗ.

2. Якщо первинна установка пройшла успішно, шкідливе ПЗ часто підключається до одного або кількох доменів для отримання додаткових шкідливих програм. Знову ж таки, якщо DNS знає, що домен є шкідливим або використовується не за призначенням, він може відповісти повідомленням «не знайдено», яке знову перерве запит, запобігши з'єднання і завантаження подальшого шкідливого ПЗ.

3. Якщо шкідлива програма все ж буде встановлена, вона, швидше за все, спробує зв'язатися з інфраструктурою C&C в третьому домені, що потребує додаткового перетворення імені.

Брандмауер DNS легко розгорнути, оскільки він не вимагає програмного забезпечення агента на кожному хості. Швидше, він замінює частину вже використовуваної інфраструктури. Це також робить його відносно недорогим і легко керованим центральним пунктом управління. Але наскільки ефективний

брандмауер DNS для запобігання інцидентів? Вважається, що брандмауери DNS, такі як платформа Quad9, можуть істотно вплинути на показники успіху зловмисників. Quad9 – це безкоштовна служба безпеки DNS, розроблена у співпраці з GCA, IBM і Packet Clearing House. Quad9 – лише один із прикладів доступних безкоштовних DNS-сервісів [9].

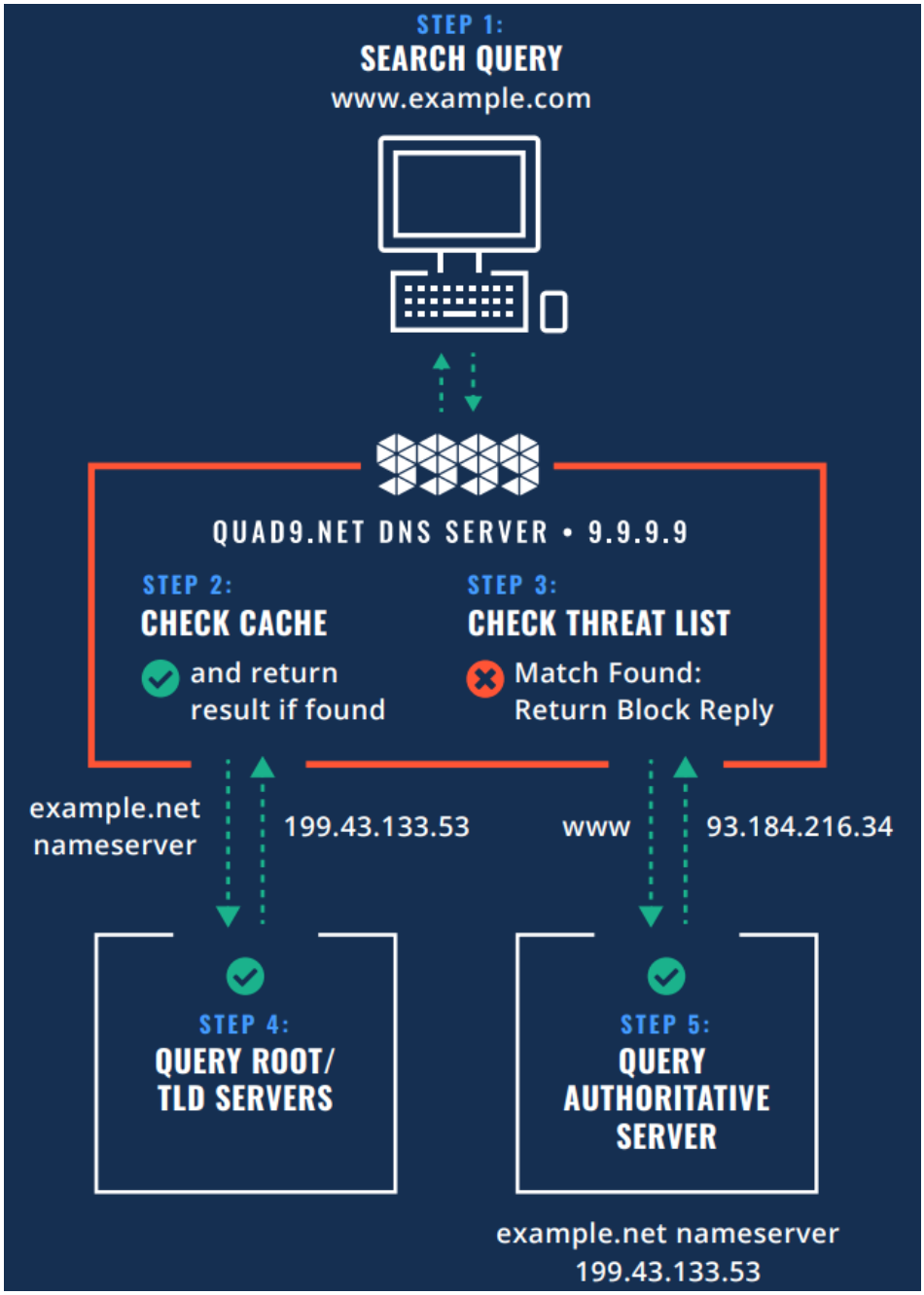


Рис. 2.2. Принцип роботи Quad9 [9]

Розглянемо принцип роботи брандмауера DNS (рис. 2.2).

Брандмауери DNS працюють так само, як і інші брандмауери, перериваючи

потік інформації до шкідливим мережевим місцезнаходженням. На рівні DNS можна заблокувати шкідливі домени, запобігаючи потенційно шкідливій комунікації.

Крок 1 (рис. 2.2) починається з необхідності перетворити доменне ім'я в маршрутизацію Інтернет-адреса. Це може бути ініційовано користувачем, який переглядає Інтернет, або додатком, який намагається отримати доступ до мережного ресурсу, шкідливим програмним забезпеченням або відповідними командами. Незалежно від джерела всі запити відправляються на брандмауер DNS.

На кроці 2 брандмауер DNS перевіряє свій локальний кеш, щоб визначити, кешований чи ні дозвіл. Якщо він знайдений, він поверне маршрутизацію адреса; якщо він не знайдений, брандмауер DNS перевірить запитане доменне ім'я за списком відомих шкідливих адресатів. Якщо запит відповідає зловмисному місцю призначення, брандмауер DNS поверне блокуючу відповідь, яка ефективно запобігає доступу джерела до зловмисного місця призначення.

Однак, якщо доменне ім'я не кешовано і не виявлено в списку зловмисних адресатів, воно буде брати участь в процесі DNS як зазвичай, запитуючи адреси у серверів кореневого домену або домену верхнього рівня (TLD) і, в кінцевому підсумку, у DNS-сервера, який знає маршрутизацію адреса запитаного доменного імені [9].

У проекту Quad9 залучається більше 18 джерел, звідки він отримує інформацію про проблемні доменні імена (IBM's X-Force, GCA's Chief Technical Advisor тощо). Уся ця інформація збирається і конвертується в Response Policy Zone (RPZ) формат. У разі якщо до nameserver приходить запит на домен, який опинився в чорному списку, сервіс віддає помилку (NXDOMAIN) і не резольвіт його. Дані з джерел оновлюються 1-2 рази в день, це, на жаль, не дозволяє сервісу оперативно реагувати на проблемні домени, які щойно з'явилися, однак базовий захист від явно проблемних ресурсів забезпечує [10].

Quad9 включає в себе два списки: білий список, і список однозначно хороших доменів. Білий список формується з Majestic Million проекту, який

публікує популярні доменні імена, з якими користувачі працюють щодня. Список хороших доменів – це лістинг, що складається з ресурсів великих і популярних компаній (AWS, Google, Microsoft Azure), які Quad9 блокуватися не будуть [10].

З одного боку, звичайно ж, проект по своїй структури, не може (принаймні зараз) оперативно реагувати на свіжостворені (або тільки що зламані і заражені, наприклад) проблемні ресурси. Крім того, якщо якась шкідлива програма, фішинг-сторінка або форма виявляться розміщеними на docs.google.com, Quad9 його блокування не виконає [10].

З іншого боку, проект агрегує велику кількість інформації про проблемні домени і надає зручну можливість обмеження доступу до них, що в деяких випадках дійсно може виручити і захистити ПК, мережу або сервер [10].

Крім того, до Quad9 варто придивитися тим, хто давно шукав альтернативу резольвера від Google. Заявлено, що приватність для сервісу так само важлива. В процесі роботи проект збирає тільки деяку телеметрію, і ділиться даними тільки з тими компаніями, які надають інформацію про проблемні домени. При цьому, кожна компанія отримує ту частину даних, яка пов'язана тільки з тими доменними іменами, які були нею надані [10].

Розглянемо види та реалізацію блокування загроз у Quad9.

Система Quad9 інтегрувала як комерційні, так і загальнодоступні канали Threat Intelligence (TI). Кожен з них був обраний на основі його перевіреної здатності ідентифікувати суб’єкти загрози та надавати широкий спектр можливостей для ідентифікації експлойтів, шкідливих програм, програм-вимагачів, шпигунських програм та інших потенційно шкідливих сайтів. Ці домени або хости оновлюються в списках від наших партнерів Threat Intelligence (TI), які надають дані про канали, які швидко оновлюються та розповсюджуються у міру появи нових ризиків на основі домену [11].

Метод блокування. Майже кожна транзакція в Інтернеті починається з пошуку імені. Браузер, мобільний пристрій, програма або система IoT намагається встановити зв’язок з іменем (“www.example.com”) Як початок завантаження сторінки чи іншої взаємодії. Однак імена не мають сенсу для

підключених до Інтернету систем – вони потребують підключення до IP-адреси (“10.10.2.3”). Отже, система відображення імен на номер, відома як система доменних імен (DNS), використовується для пошуку цих імен, а потім виявлення, які IP-адреси з ними пов’язані [11].

Клієнтський пристрій повинен взаємодіяти з так званим «рекурсивним DNS-сервером» або «резольвером», щоб виконати цей пошук. Зазвичай цей розв’язувач надається Інтернет-провайдером, адміністратором локальної мережі або пристроєм домашнього маршрутизатора – це сервер, який знаходиться десь поблизу в мережі. Клієнт підключається до розподільника і надає йому ім'я, а потім, після досить складного набору пошуків, який може охоплювати більшу частину Інтернету, розподільник передає клієнту необхідну IP-адресу [11].

Quad9 замінює локальний розв’язувач, виконуючи точно ту ж функцію, але додаючи список блокуючих доменів, про які відомо, що вони шкідливі. Якщо клієнт запитує зловмисний хост, тоді розв’язувач Quad9 відмовляється відповідати за допомогою IP-адреси, заважаючи клієнту підключатися до зловмисного пункту призначення [11].

Види блокування. Quad9 блокує лише ті сайти, які представляють небезпеку для кінцевого користувача, його обладнання або мережі. Quad9 не блокує вміст, а угоди з провайдерами Threat Intelligence передбачають, що критерії блокування мають бути виключно пов'язаними з безпекою, а не базуватися на інших категоріях. Quad9 не блокує рекламу та веб-трекери. Для користувачів, які хочуть вирішити всі імена, не блокуючи, Quad9 використовує набір IP-адрес, які надають цю можливість [11].

Переваги блокування. Запобігаючи підключенню до шкідливих веб-сайтів, Quad9 усуває ризик ще до того, як вони навіть завантажуються на комп’ютери або до того, як жертва може побачити шахрайський веб-сайт. Неможливість отримати зловмисний хост означає, що захист другого рівня, такий як захист від вірусів або виявлення на основі користувачів, наприклад, перевірка сертифікатів, ніколи не вводиться в дію [11].

Quad9 може запобігти підключенню лише до сайтів, які використовують

DNS в межах їх сигналізації або розподілу. Нещодавнє дослідження показало, що приблизно 33% порушень кібербезпеки можуть бути заблоковані системою DNS, такою як Quad9 [9].

Quad9 припускає, що всі користувачі мають кілька методів захисту від кіберризиків, наприклад антивірусне програмне забезпечення. Але як безкоштовний, легко встановлюваний захист першого рівня, Quad9 надзвичайно ефективний у запобіганні широкому набору інфекцій або шахрайських дій і може бути легко впроваджений майже на всіх підключених до Інтернету пристроях у мережі чи будинку [11].

Джерела блокування даних. Quad9 співпрацює з багатьма джерелами інформації Threat Intelligence, як комерційними, так і загальнодоступними. Ці партнери надають дані про загрози Quad9 як частину своїх місій, щоб допомогти зменшити ризик та кіберзлочинність в Інтернеті, а також тому, що їх партнерство з Quad9 може допомогти їм покращити власну здатність виявляти ці ризики.

Партнери TI постачають Quad9 інформацію про домени або хости, які, на їхню думку, повинні бути заблоковані, і, в свою чергу, партнери отримують від Quad9 майже в реальному часі зворотній зв'язок щодо об'ємних ставок загроз, які вони перелічують. Ці об'ємні дані дозволяють їм зрозуміти зростання чи падіння статусу різних загрозливих кампаній та дозволяють вдосконалити списки ризикованих доменів, які вони надають Quad9. Quad9 – це виключно інструмент розповсюдження даних про загрози, що генеруються партнерами [11].

2.3. Оцінка впливу брандмауера DNS на запобігання загрозам

Першим кроком в кількісній оцінці запобігання втрат, пов'язаних з брандмауерами DNS, є визначення загроз, які залежать від DNS для успішної атаки. Це загрози, яким потенційно можна запобігти, виявити або усунути іншим чином за допомогою брандмауера DNS. Для виявлення цих загроз потрібно добре організована структура загроз, яка підходить для цієї мети [9].

За минулі роки було запропоновано безліч структур або таксономій

кіберзагроз, але багато з них страждають різними вадами, які обмежують або знижують результативність боротьбі з загрозами. Так існує загальнодоступна і перевірена структура, що відповідає вимогам – Словник для запису подій і обміну інформацією про інциденти (VERIS) [9].

Платформа VERIS лежить в основі багаторічного і компетентного звіту Verizon про розслідування витоків даних (DBIR). VERIS був створений для забезпечення надійної схеми для структурованого і повторюваного опису інцидентів безпеки. Він був протестований і вдосконалений протягом 12 років досліджень, що охоплюють сотні тисяч інцидентів. Більш того, сама структура була опублікована майже 10 років тому і використовується організаціями та інструментами по всьому світу для збору, аналізу та обміну даними про інциденти [9].

Verizon запустила відкриту базу даних публічно розкритих інцидентів під назвою VERIS Community Database (VCDB). Як випливає з назви, він використовує структуру VERIS і відкритий для участі і аналізу з боку співтовариства безпеки. Ці ресурси дозволяють нам діяти прямо. По-перше, ми використовуємо структуру VERIS для виявлення загроз, які можна було запобігти за допомогою брандмауера DNS. Потім ми можемо використовувати наше визначення для виявлення інцидентів в VCDB, пов'язаних з цими загрозами. Підстава нашого аналізу на VERIS7 і VCDB позбавляє від необхідності відсівати тисячі інцидентів з розрізнених джерел, щоб визначити ті, які мають відношення до поточного дослідження [9].

Узгодження брандмауера DNS та VERIS.

Структура VERIS дозволяє збирати інформацію про загрози, інциденти і відповіді. Сюди входять дані про те, як швидко організація-жертва виявляє інцидент і реагує на нього. У VERIS загрози описуються за допомогою моделі подій A4. Модель A4 відноситься до чотирьох елементів A (actor, action, asset and attribute) в структурі VERIS: уражених суб'єкту, дії, активу та атрибуту.

Ця модель дає відповідь про те, «хто що зробив, що (чи кого) з яким результатом?» в форму, зручну для обміну і аналізу. Таким чином, класифікація

загрози або інциденту безпеки в VERIS по суті означає ідентифікацію задіяних суб'єктів, дій, активів і атрибутів (A4).

Для цього зосередимося на «діючому» компоненті VERIS. Дії описують, що дійові особи зробили, щоб викликати інцидент або сприяти йому. У кожного інциденту є принаймні одну, але більшість буде включати в себе кілька дій (і часто по декількох категоріях). VERIS визначає сім основних категорій дій при загрозах: шкідливе ПЗ, злом, соціальні мережі, неправомірне використання, фізичні, помилки і екологічні. Кожна з цих високорівневих категорій включає кілька різновидів або типів дій загроз [9].

Розглянемо всі дії, пов'язані з загрозами, за сьома зазначених вище категоріям, щоб визначити ті, які можуть бути зменшено за допомогою брандмауера DNS (рис. 2.3). Для кожної дії загрози надана оцінка тому, що брандмауер DNS може розумно пом'якшити дію загрози, за шкалою від низького (L) до високого (H).

Вплив брандмауера DNS для всіх цих загроз неоднаковий. Він буде прямо і високоефективним для одних, в той час як мінімальним або побічно ефективним для інших. Крім того, брандмауер DNS може активно захищати від певних дій загроз, але може тільки допомагати виявляти інші або реагувати на них [9].

Вимірювання частоти інцидентів, пов'язаних з брандмауером DNS.

Виявивши загрози, які потенційно можуть бути зменшені за допомогою брандмауера DNS, можна виміряти поширеність пов'язаних інцидентів в наборах даних на основі VERIS. Це забезпечить оцінку масштабів і значущості брандмауерів DNS в ландшафті загроз, з якими можуть зіткнутися організації. Простіше кажучи, пошук відповіді на питання: «Яку частку інцидентів можна зменшити за допомогою брандмауера DNS?» [9].

THREAT CATEGORY	THREAT ACTION	RATING
Social	Phishing	H
Malware	action.malware.variety.C2	H
Malware	action.malware.variety.Downloader	H
Malware	action.malware.variety.Export data	H
Hacking	action.hacking.variety.URL redirector abuse	H
Social	action.social.variety.Baiting	L
Social	action.social.variety.Spam	L
Malware	action.malware.variety.Adware	L
Malware	action.malware.variety.Click fraud	L
Malware	action.malware.variety.Client-side attack	L
Malware	action.malware.variety.Ransomware	L
Malware	action.malware.variety.Rootkit	L
Malware	action.malware.variety.Spyware/Keylogger	L
Malware	action.malware.variety.Worm	L
Hacking	action.hacking.variety.Routing detour	L
Hacking	action.hacking.variety.Use of backdoor or C2	L
Misuse	action.misuse.variety.Illicit content	L
Social	action.social.variety.Scam	M
Malware	action.malware.variety.Backdoor	M
Malware	action.malware.variety.Spam	M
Hacking	action.hacking.variety.RFI	M

Рис. 2.3. Оцінка пом'якшення дії загрози брандмауером DNS [9]

Використовуючи VCDB в якості випробувального стенду, можна провести аналіз, щоб підрахувати кількість підтверджених витоків даних, пов'язаних з діями загроз, які були ідентифіковані раніше і перерахованими на рис. 2.3.

Так, команда Verizon провела аналіз за своїм набором даних DBIR і надала відповідні результати. Набір даних DBIR містить 11 079 підтверджених витоків даних, зібраних і проаналізованих за останні п'ять років. З цих порушень 3668 пов'язані принаймні з однією з дій загрози, які потенційно можна було б нейтралізувати за допомогою брандмауера DNS. Це означає, що брандмауер DNS є важливим засобом контролю проти однієї третини порушень в наборі даних DBIR за останні п'ять років (рис. 2.4) [9].

Рис. 2.4. Оцінка впливу брандмауер DNS на загрози [9]

DBIR приводить наступну відмінність між інцидентами безпеки і витоками даних. «Інцидент» – це подія безпеки, яке ставить під загрозу цілісність, конфіденційність або доступність інформаційного активу. «Порушення» – це інцидент, який призводить до підтвердженого розкриття, а не тільки до потенційного розкриття даних неавторизованої стороні [9].

Слід зазначити, що ця оцінка, ймовірно, знаходиться на нижньому рівні, оскільки дані DBIR реєструють тільки відомі дії по загрозам, коли є спостережувані індикатори цих дій по загрозам. Наприклад, іноді стає ясно, що шкідливе ПЗ заразило систему, але Verizon або його партнер не можуть визначити повний спектр функцій шкідливого ПЗ (з різних причин). Отже, навіть якщо б воно мало функціональні можливості для зв'язку з інфраструктурою C&C, воно не було б записано як таке в даних і, отже, не могло бути включене в число інцидентів, які визначили, що підпадають під дію брандмауера DNS [9].

Оскільки природа джерела даних ускладнює кількісну оцінку, то не вимірюється кожен випадок, коли брандмауер DNS міг захистити жертву, і дана оцінка фінансового впливу, ймовірно, трохи занижена. Рис. 2.5 додає додатковий контекст до цього висновку. Він показує основні дії по загрозам VERIS, які були визначені як такі, що підпадають під дію брандмауерів DNS, а також відсоток порушень, пов'язаних з кожним з них. Треба мати на увазі, що вони не виключають один одного. Більшість порушень пов'язано з декількома діями загроз в ланцюжку подій. З цієї причини не має можливості просто підсумовувати зазначені відсотки, щоб отримати загальну пропорцію. Правильна інтерпретація полягає в тому, що в 33% всіх порушень в п'ятирічній вибірці зафіксовано хоча б одне з цих дій за загрозою [9].

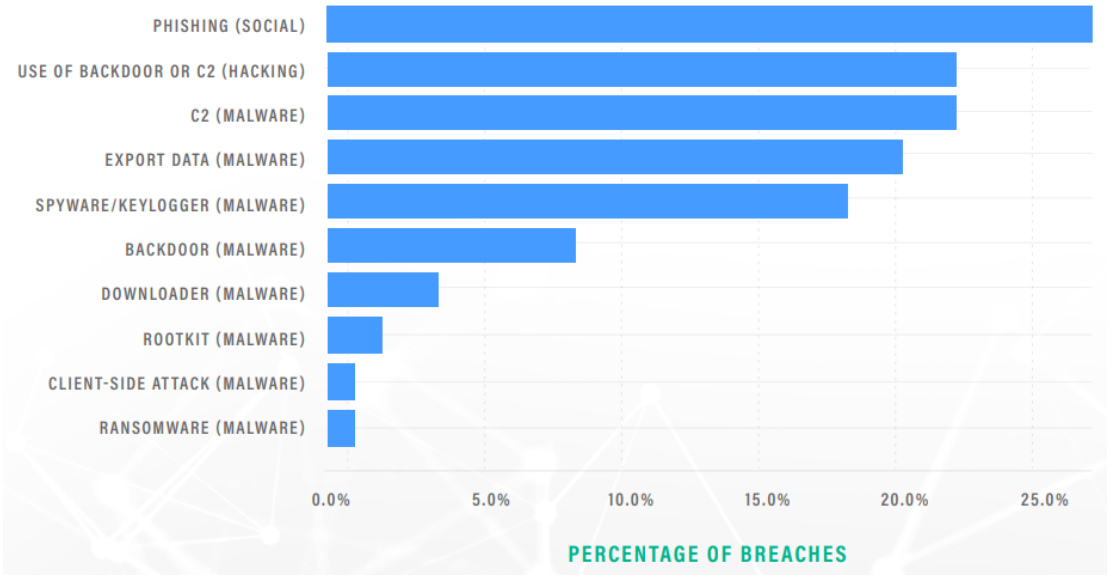


Рис. 2.5. Частота дій за категоріями загроз VERIS в Verizon DBIR Data 2012-2017 pp. [9]

Організації та приватні особи, які розглядають Quad9 або інше рішення брандмауера DNS, можуть застосувати цю третю статистику до свого середовища загроз як приблизна оцінка актуальності управління [9].

Оцінка збитків. Вважається, що частка порушень в наборі даних Verizon, які потенційно можуть бути пом'якшені брандмауером DNS (33%), є найбільш корисним висновком. Дуже рідко можна знайти елемент управління, що поєднує в собі високу віддачу і простоту розгортання. Треба враховувати, що втрати через витік даних можуть істотно відрізнятися. Отже, можна отримати оцінку загальних втрат, пов'язаних як з 3368 порушеннями, зазначеними вище, так і з оцінками глобальних втрат [9].

Важко отримати точну статистику втрат для інцидентів, пов'язаних з кібербезпекою, і ще складніше її зібрати. Дані Cyentia Library та колекція з більш ніж 1300 звітів по індустрії безпеки є джерелами, які надають корисні дані для даної мети. Було включено всі заявлені витрати з явним середнім або медіанним значенням. У таблиці 1 перераховані ці джерела і статистичні дані [9].

Таблиця 1: Джерела і статистика втрат, пов'язаних з витоком даних [9]

YEAR	SOURCE	MEDIAN	MEAN
2015	Kaspersky (Survey) — SMBs	11,000	38,000
2015	Kaspersky (Survey) — Enterprise	84,000	551,000
2015	NetDiligence (Insurance Claims)	76,984	673,767
2016	NetDiligence (Insurance Claims)	60,000	665,000
2016	Romanosky (Advisen)	170,000	6 mil
2017	SailPoint (Survey)		4 mil
2018	Ponemon (Survey)		3.86 mil
2017	Ponemon (Survey)		3.62 mil
2016	Ponemon (Survey)		4 mil

Варто зазначити, що ця статистика втрат, ймовірно, переоцінює «типові» втрати, тому що дослідження, подібні до тих, які показані в таблиці 1, в основному зосереджені на облікованих порушеннях. Таким чином, незначні порушення, які не викликають страхових вимог або обов'язкової звітності, можуть бути недостатньо представлені [9].

Ці точки візуально представлені на рис. 2.6. З таблиці 1 та рис.2.6 легко побачити, що середні втрати істотно більше медіани за всіма джерелами. Це вказує на сильний ухил в правий хвіст серед збитків від порушення. Повідомлені збитки зазвичай не перевищують кількох сотень тисяч доларів, але відносно невелика кількість надзвичайно великих збитків збільшують середнє значення до мільйонів. Серед найбільш серйозних порушень, про які повідомлялося публічно, верхній хвіст збитків обчислюється сотнями мільйонів [9].

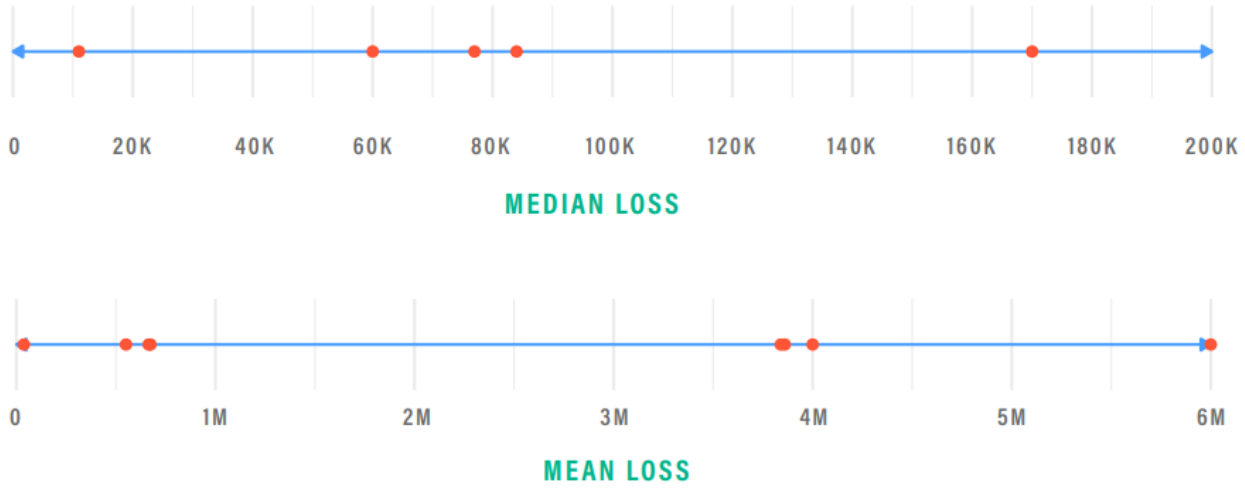


Рис. 2.6. Медіанні і середні значення про збитки від витоку даних зі звітів [9]

Незважаючи на ці великі статистичні дані та застереження, можна розробити надійну модель розподілу збитків, яка наближається до наведених вище даних. Цей розподіл показано на рис. 2.7 і має медіанне значення 70 000 доларів США та середнє значення 2,8 мільйона доларів США. 10% основних порушень мають збитки, які перевищують 3,8 мільйона доларів. Кращі 5% перевищують 11 мільйонів доларів, а кращі 1% перевищують 57 мільйонів доларів. Це навіть пояснює ті рідкісні порушення, які становлять одне з тисячі, які перевищують 200 мільйонів доларів [9].

Повідомлені збитки зазвичай не перевищують кількох сотень тисяч доларів, але відносно невелика кількість надзвичайно великих збитків роздмухують середнє значення до мільйонів.

Рис. 2.7. Розподіл втрат за подію через порушення даних [9]

Маючи такий розподіл втрат за одну подію, можна моделювати збитки за 3668 порушень, виявлених у останньому розділі з набору даних DBIR. Як показано на рис. 2.8 це дає діапазон загальних ймовірних збитків від 8 до 13 мільярдів доларів. Таким чином, рішення брандмауера DNS, таке як Quad9, могло зіграти роль у пом'якшенні майже 3700 з 11 079 порушень та приблизно 10 млрд. доларів США збитків, пов'язаних з цими порушеннями за останні п'ять років [9].

Рис. 2.8. Загальні оціночні втрати від 3668 порушень, ідентифікованих як такі, що пов’язані із брандмауером DNS [9]

Фраза «міг зіграти певну роль», ймовірно, буде звучати для деяких так, як ніби автори навмисно поводяться нечітко або відступають від їх висновків. На рис. 2.8 явно показана невизначеність, яка існує щодо статистики втрат. Двозначність висновків виникає не стільки з оцінки загальних втрат, скільки з невідомої ефективності брандмауера DNS в зменшенні цих втрат. Це сильно залежить від ряду факторів, пов'язаних з рішенням і реалізацією, які не можна виміряти [9].

Брандмауер DNS, розгорнутий в невеликому масштабі, покладаючись на поганий аналіз загроз або налаштований слабо, практично не змінить ймовірних втрат. Дійсно, погано налаштований брандмауер DNS може привести до помилково заблокованим доменам і негативним зовнішнім впливам. Але добре спроектоване і розгорнуте рішення пропонує великомасштабну потенційну ефективність при відносно невеликих затратах. Наприклад, Cisco Umbrella

виявила, що 91% шкідливих програм використовують DNS для обміну даними з C&C [9].

В якості додаткового орієнтиру навесні 2018 року Рада економічних консультантів опублікував звіт, в якому оцінюється, що «шкідлива кібер-активність обійшовся економіці США в розмірі від 57 до 109 мільярдів доларів в 2016 році» [9]. За оцінками McAfee і Центру стратегічних і міжнародних досліджень у 2018 році, глобальні збитки від кіберзлочинності становлять від 445 до 600 мільярдів доларів [9].

Таким чином, брандмауер DNS може запобігти від 19 до 37 мільярдів доларів в США або від 150 до 200 мільярдів доларів у всьому світі [9].

3 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ДОСТУПУ КОРИСТУВАЧІВ ДО ІНТЕРНЕТ НА БАЗІ DNS-ПЛАТФОРМИ QUAD9

3.1. Алгоритм забезпечення безпечного доступу користувачів до Інтернет на базі DNS-платформи Quad9

Quad9 можна використовувати просто встановивши параметри DNS-сервера для вашого пристрою за адресами, вказаними в одному з профілів обслуговування. Реєстрація не потрібна, дані облікового запису не повинні передаватися в Quad9, а також немає договору.

Quad9 можна використовувати безкоштовно дана система не збирає жодних персональних даних про вас. Ви можете налаштувати маршрутизатор або точку доступу Wi-Fi для розповсюдження цих налаштувань, що поширить захист на всі елементи вашої локальної мережі, включаючи пристрої IoT, багато з яких в іншому випадку не мали б жодного захисту від зловмисного програмного забезпечення.

Quad9 пропонує кілька різноманітних послуг для функцій рекурсивних DNS. Кожна з них представлена різною IP-адресою (або, в деяких випадках, іменем хосту), яку необхідно використовувати для налаштування своїх систем [12]:

рекомендовані налаштування;

захищене з ECS налаштування;

незахищене налаштування;

параметри конфігурації для Android;

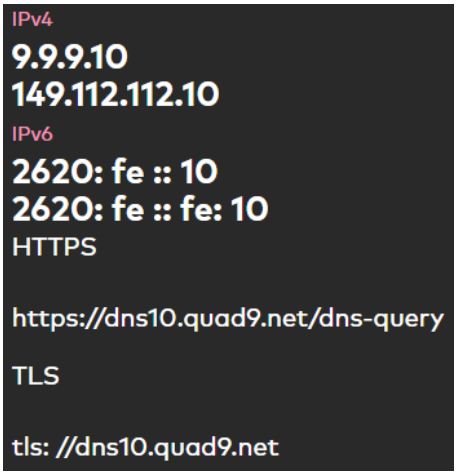
параметри конфігурації DNSCrypt.

Рекурсивні адреси та функції DNS-сервера - Конфігурації на основі сервісу:

Рекомендовані налаштування: блокування зловмисного програмного забезпечення, перевірка DNSSEC (це найбільш типова конфігурація):

Захищене з ECS налаштування: блокування зловмисного програмного забезпечення, перевірка DNSSEC, увімкнена ECS:

Незахищене налаштування: відсутність блокування зловмисного програмного забезпечення, перевірка DNSSEC (лише для експертів!):



Якщо у вас є пристрої, які потрібно налаштувати за IP-адресою, переконайтесь, що всі IP-адреси, перелічені для вибраної послуги, розміщені в

будь-яких областях конфігурації. Введення лише одного з трьох призведе до того, що ви станете вразливими до однобічних відмов. Навіть якщо у вас ще немає протоколу IPv6, додайте ці адреси зі списку, щоб вам не довелося згадувати пізніше – більшість систем ігноруватимуть адреси IPv6, якщо їх не можна використовувати.

Параметри конфігурації для Android:

Quad9 надає програму для користувачів Android, що значно спрощує конфігурацію DNS Quad9 для цих пристроїв. Додаток включає інші функції, такі як повний журнал запитів DNS, повідомлення про події блоків та шифрування (із використанням DNS-over-TLS) усіх запитів до систем Quad9.

Програму “Quad9 Connect” можна знайти у магазині Google Play.

Параметри конфігурації DNSCrypt:

DNSCrypt – рідко використовуваний протокол шифрування DNS, але він підтримується Quad9.

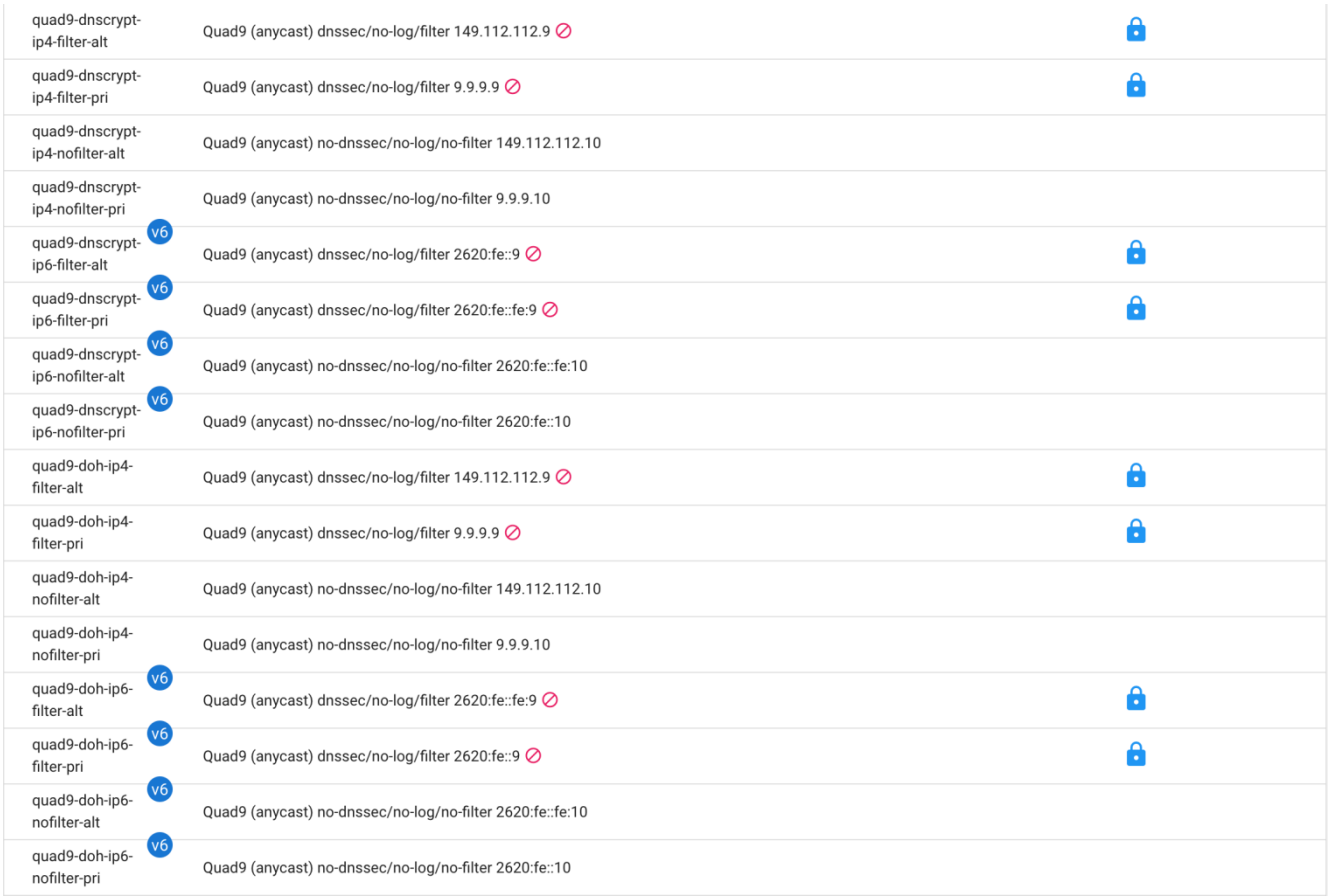


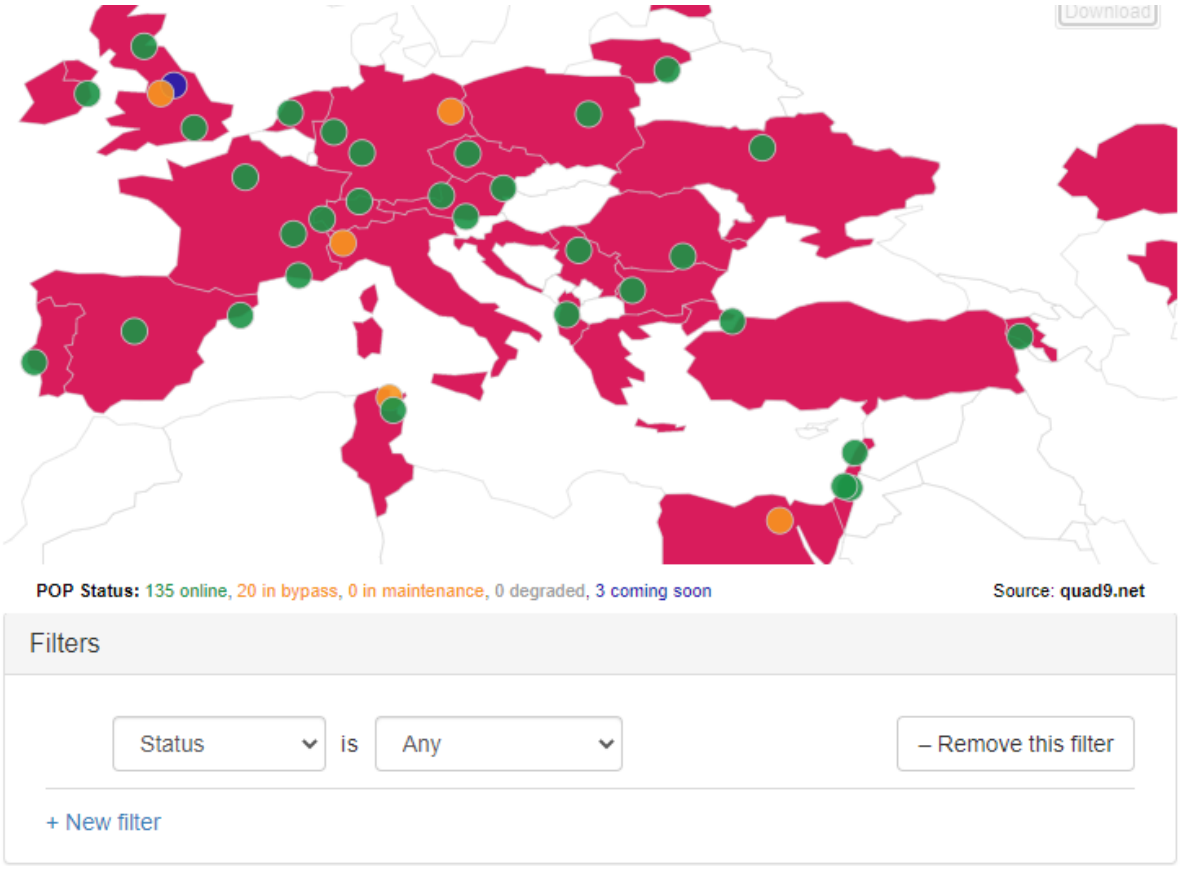
Рис. 3.1. Загальнодоступний список серверів для DNSCrypt

Шифрування за допомогою DNS-over-TLS є частиною пропозиції Quad9. DNSCrypt є протоколом і багато систем з відкритим вихідним кодом підтримують його. Загальнодоступний список серверів для DNSCrypt (рис. 3.1).

Необхідно відмітити, що системи Quad9 розповсюджуються по всьому світу у більш ніж 150 місцях у 90 країнах, із запланованим подальшим розширенням. Quad9 має сервери, розташовані переважно в точках обміну Internet, де найбільша концентрація взаємозв'язків відбувається в типовому регіоні між мережами. Це призводить до меншої затримки, оскільки пакети повинні переміщатися через меншу кількість компонентів маршрутизації, і це часто призводить до того, що клієнти та системи Quad9 проживають в одній країні, що додатково знижує ризики перехоплення, втручання або спостереження [12].

Quad9 також розміщує системи в регіональних центрах обробки даних, де поєднання провайдерів транзиту та близькості до великих регіональних мереж кінцевих користувачів робить доставку пакетів настільки ж швидкою та безпечною [12].

В Україні також розміщено сервери Quad9 (рис. 3.2).



				Indonesian Internet Exchange
☺	JNB	Johannesburg	South Africa	NAPAfrica Johannesburg
☺	KBL	Kabul	Afghanistan	National Internet Exchange of Afghanistan
☺	KBP	Kiev	Ukraine	Giganet Internet Exchange
☺	KEF	Reykjavik		
☺	KGL	Kigali	Rwanda	Rwanda Internet exchange
☺	KLA	Kampala	Uganda	Uganda Internet Exchange
☺	KLU	Klagenfurt	Austria	Alpen-Adria-Internet-Exchange

Рис. 3.2. KBP Kiev Ukraine Giganet Internet Exchange як ресурс розгортання Quad9

3.2. Рекомендації щодо забезпечення безпечного доступу користувачів до Інтернет

З кожним днем інформаційні технології все більше проникають в життя сучасної людини. Сьогодні майже кожен має смартфон з доступом до Інтернет-мережі, що дозволяє користувачам завжди бути онлайн. Зокрема у будь-яку мить ви можете перевірити пошту чи месенджер, купити квиток в кіно чи забронювати житло для відпустки та навіть здійснювати платежі, не звертаючись до відділень банку. Всі ці дії в Інтернеті передбачають обмін певною особистою інформацією чи конфіденційними даними, які у разі вашої неуважності можуть опинитися в руках зловмисників.

Для забезпечення захисту ваших персональних даних під час роботи в Інтернет-мережі спеціалісти ESET рекомендують дотримуватися основних правил кібергігієни. В свою чергу кібергігієна – це заходи безпеки, розроблені для захисту пристроїв користувача від інфікування шкідливим програмним забезпеченням та можливого викрадення конфіденційної інформації.

Спеціалісти ESET рекомендують виконати сім кроків для покращення захисту даних [13]:

Перевірка безпеки активних акаунтів.

Першим правилом кібергігієни є перевірка безпеки вже існуючих облікових записів електронної пошти та акаунтів в соцмережах. Зокрема такі веб-сайти як haveibeenpwned.com та breachalarm.com допоможуть з'ясувати, чи був пароль до електронної пошти викрадений зловмисниками.

Аналіз програм. Сьогодні у кожного сайту, магазину та навіть банку є спеціальний мобільний додаток. Проте це не означає, що всі вони мають бути на вашому пристрої. Завантажуйте тільки необхідні для роботи програми. Спеціалісти ESET радять проаналізувати вже завантажені додатки, видалити непотрібні та в подальшому контролювати встановлення кожної програми. Також під час завантаження кожного додатку варто звертати увагу на дозволи, які ви надаєте. Часто шкідливі програми надсилають запит на отримання великої кількості дозволів, які не відповідають їх функціоналу. Це дозволяє збирати багато інформації про користувача з метою отримання прибутку.

Регулярне оновлення. Для запобігання інфікуванню шкідливими програмами варто здійснювати своєчасне оновлення операційної системи та окремих додатків, яке передбачає виправлення вразливостей та помилок в програмному забезпеченні.

Надійний пароль. З метою запобігання несанкціонованому доступу до пристроїв переконайтеся у надійності ваших паролів. Важливо створити складну комбінацію, яка містить не менше 12 символів, великі та малі літери, цифри та символи. Крім цього, для кожного акаунта варто використовувати унікальний пароль. Таким чином викрадення однієї з комбінацій не поставить під загрозу інші облікові записи. Більше рекомендацій за посиланням.

Додатковий рівень захисту. Для покращення безпеки облікових записів використовуйте двофакторну аутентифікацію, яка передбачає підтвердження особистості під час входу в певний акаунт. Найчастіше для цього використовуються SMS-повідомлення або окрема програма. Таким чином у разі викрадення пароля зловмисники не зможуть отримати доступ до ваших даних.

Регулярне резервне копіювання. Необхідним кроком для уникнення втрати важливих даних є регулярне резервне копіювання інформації на зовнішній

жорсткий диск або у хмару. Це допоможе відновити потрібні дані у разі їх шифрування програмою-вимагачем або видалення шкідливим програмним забезпеченням.

Надійний захист. Останнім, але не менш важливим, правилом кібергігієни є використання надійного рішення для захисту вашого комп'ютера чи смартфона від різних загроз, зокрема програм-вимагачів, шпигунських програм, вірусів, троянів та фішинг-атак.

Ці сім основних правил кібергігієни допоможуть вам своєчасно виявити підозрілу діяльність зловмисників та запобігти втраті персональних даних та іншої особистої інформації.

Спеціалісти CERT-UA рекомендують [14]:

Використовуйте ліцензійні/легалізовані операційні системи, інші програмні продукти, своєчасно й систематично їх оновлюйте.

Користуйтеся антивірусним програмним забезпеченням з технологією евристичного аналізу.

Використовуйте програмний міжмережевий екран (брандмауер) та штатні засоби захисту від шкідливого програмного забезпечення.

Здійснюйте регулярне резервне копіювання даних, зберігайте резервні копії на зовнішніх носіях інформації (SSD, HDD тощо) та налаштуйте функцію «відновлення системи».

Не підключайте флешки та зовнішні диски, не вставляйте CD та DVD тощо у ваш комп'ютер, якщо ви не довіряєте повністю їх джерелу. Існують техніки зламування комп'ютера ще до того, як ви відкриєте файл на флешці і задовго до того, як ваш антивірус його просканує. Якщо ви знайшли пристрій всередині офісу або на вулиці, чи отримали його поштою або з доставкою, чи незнайомець дав вам його з проханням роздрукувати документ, або просто відкрити та перевірити його вміст – є велика ймовірність, що пристрій є небезпечним.

Довіряйте лише власним пристроям та будьте обережні з пристроями, які отримуєте від інших людей по роботі або в інших цілях.

При підключенні пристроїв забезпечте їх автоматичну перевірку на

наявність шкідливого програмного забезпечення.

Відключайте автоматичний запуск змінних носіїв інформації (захист від autorun.inf).

Не зберігайте автентифікаційні дані в легкодоступних місцях (наприклад, на робочому столі). Використовуйте для зберігання паролів спеціальні програмні засоби (наприклад, KeePass). Використовуйте стійкі паролі, зокрема такі що:

містять не менше 8 символів;

містять літери, цифри та спеціальні символи;

не містять персоніфікованої інформації (дати народження, номерів телефонів, номерів та серій документів, автотранспорту, банківської картки, адреси реєстрації тощо);

не використовуються в будь-яких інших акаунтах.

Уникайте використання Інтернет-банкінгу, електронних платіжних систем, введення автентифікаційних даних під час доступу до Інтернету через загальнодоступні (незахищені) безпроводові мережі (в кафе, барах, аеропортах та інших публічних місцях).

Будьте особливо обережними з відкриттям вкладень до електронної пошти від невідомих осіб. Сьогодні найактуальнішим засобом розсилання шкідливого програмного забезпечення є електронна пошта. Під час роботи з поштою потрібно перевіряти розширення вкладених файлів та не відкривати файли навіть з безпечними розширеннями. Не переходьте за невідомими посиланнями та не завантажуйте файли, що мають потенційно небезпечне розширення (наприклад: .exe, .bin, .ini, .dll, .com, .sys, .bat, .js тощо) та навіть безпечне (наприклад: .docx, .zip, .pdf), адже можуть використовуватися вразливості, макроси та інші небезпеки. Звертайте увагу на ім'я електронної пошти: навіть якщо воно здається легітимним, усе одно потрібно перевірити (у телефонному режимі або в будь-який інший спосіб), чи дійсно ця особа відправляла вам повідомлення з вкладенням.

Іноді, особливо під тиском часу, буває важко відрізнити шкідливі файли від легітимних. Користуйтеся сервісом VirusTotal для перевірки підозрілих файлів шляхом їх одночасного сканування більш ніж 50 антивірусами. Це набагато

ефективніше, ніж сканування файлів антивірусом в автономному режимі, але враховуйте той факт, що завантажуючи файли на VirusTotal, ви надаєте доступ до нього третій стороні. Звертаємо вашу увагу на те, що, навіть якщо перевірка на VirusTotal не дала результату, це не виключає того, що файл може бути шкідливим.

Тричі подумайте перед відкриттям вкладень.

Під час користування Інтернет-ресурсами (Інтернет-банкінгом, соціальними мережами, системами обміну повідомленнями, новинами,онлайн-іграми) не відкривайте підозрілі посилання (URL), особливо ті, що вказують на веб-сайти, які ви зазвичай не відвідуєте.

Будьте уважним до проявів Інтернет-шахрайства. Найпоширенішим засобом уведення в оману в мережі Інтернет є фішинг. Особливу увагу варто звертати на доменне ім'я Інтернет-ресурсу, що запитує автентифікаційні дані, перш ніж натиснути на посилання: зловмисники можуть замаскувати доменне ім'я, щоб воно виглядало знайомим (facelook.com, goooogle.com тощо) . В іншому разі є велика ймовірність перейти на фішингову сторінку, ззовні ідентичну справжній, та самостійно «віддати» власні автентифікаційні дані.

У разі необхідності введення автентифікаційних даних упевніться в тому, що використовується захищене з’єднання HTTPS, перевіряйте SSL-сертифікат веб-сайту, щоб переконатися, що він не клонований або не підроблений.

Шкідливі URL-адреси можуть бути закодовані у вигляді QR-кодів та/або роздруковані на папері, у тому числі у формі скорочених URL, згенерованих спеціальними сервісами на кшталт tinyurl.com, bit.ly, ow.ly тощо. Не вводьте ці посилання до браузера та не скануйте QR-коди вашим смартфоном якщо ви не впевнені у їх вмісті та походженні.

Використовуйте VirusTotal для перевірки підозрілих посилань так само, як для сканування файлів.

Будьте обережні щодо випливаючих вікон та повідомлень у вашому браузері, програмах, операційній системі та мобільному пристрої. Завжди читайте вміст цих вікон та не «схвалюйте» і не «приймайте» нічого похапцем.

Під час використання віддаленного доступу необхідно обмежити доступ за допомогою «білого списку» (IP whitelisting).

Установіть обмеження кількості введення помилкових логінів/паролей. Регулярно переглядайте журнали логування, планувальник завдань та автозавантаження на предмет несанкціонованих дій.

Сервіси брандмауера DNS варіюються від прозорих і безкоштовних, таких як Quad9, до комерційних з можливістю настройки і реєстрації. Ці сервіси прості в розгортанні і можуть істотно вплинути на показники успіху зловмисників і вплив цього успіху.

Дуже багато організацій та підприємств ще не використовують брандмауер DNS. Наприклад, Cisco Umbrella стверджує, що 68% організацій цього не роблять. Рекомендація для організацій та підприємств: для більшості підприємств найближчим часом варто вивчити ці заходи контролю та впровадити у себе.

Рекомендація фізичним особам: варто використовувати брандмауер DNS, наприклад Quad9.

Рекомендація виробники систем: вважаємо, що виробники систем повинні серйозно подумати про те, щоб використовувати в своїх системах за замовчуванням сервіс брандмауера DNS або зробити інші кроки, щоб спростити його включення.

Рекомендація виробникам маршрутизаторів: зробіть одну кнопку для включення і, можливо, одним клацанням миші для зміни провайдерів.

Рекомендація органам стандартизації: необхідно враховувати брандмауери DNS та розглядати в багатьох стандартах безпеки.

На останок. Використовуйте сервіс Quad9 для забезпечення безпечного доступу користувачів до Інтернет. Даний сервіс можна використовувати просто встановивши налаштування DNS-сервера для вашого пристрою за вказаними адресами. Реєстрація не потрібна, дані облікового запису не повинні передаватися в Quad9, і немає договору. Quad9 можна використовувати безкоштовно. Він не збирає жодних персональних даних про вас. Ви можете налаштувати свій маршрутизатор або точку доступу Wi-Fi для розповсюдження цих налаштувань,

що поширить захист на всі елементи вашої локальної мережі, включаючи пристрої IoT, багато з яких в іншому випадку не мали б жодного захисту від зловмисного програмного забезпечення.

Використання платформи Quad9 може запобігти атаці-вимагателю, запобігти злому вашого банківського рахунку або захистити ваш ноутбук від використання в рамках незаконного кримінального нападу на інших. Усі ці потенційні засоби захисту та багато мільйонів інших втручань мають прямий результат економії для вас, вашого бізнесу чи організації та компаній, на які ви покладаєтесь, таких як банки та фірми електронної комерції.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми забезпечення безпечного доступу користувачів до Інтернет.

Проведено аналіз існуючих загроз безпечному доступу користувачів до Інтернет. Зроблено висновок, що існуючі загрози безпечному доступу користувачів до Інтернет як приватних, так і корпоративних, вимагають залучення зовнішніх ресурсів, створення та застосування відповідних сервісів забезпечення безпеки даного доступу.

Досліджено призначення, функції та компоненти системи доменних імен як основи системи брандмауера DNS. Визначено можливість реалізації сервісів брандмауера DNS.

Проведено аналіз існуючих підходів до забезпечення безпечного доступу користувачів до Інтернет. Проаналізовано можливості загальнодоступних та відомих резольверів, а саме Cloudflare (1.1.1.1 та 1.0.0.1), Cisco (208.67.222.222 та 208.67.220.220), Google (8.8.8.8 та 8.8.4.4) та Quad9.

Проведено аналіз існуючих методів та засобів забезпечення безпечного доступу користувачів до Інтернет DNS-платформи Quad9. Quad9 – це безкоштовна рекурсивна платформа DNS з довільним доступом, яка забезпечує кінцевим користувачам надійний захист, високу продуктивність і конфіденційність. Quad9 блокує відомі шкідливі домени, запобігаючи підключення комп'ютерів і пристроїв Інтернету речей організації та підприємств до шкідливих або фішингових сайтів.

Розглянуто принцип роботи DNS-платформи Quad9 та наведено оцінку впливу брандмауера DNS на запобігання загрозам. Встановлено, що брандмауер DNS є важливим засобом контролю проти однієї третини порушень в наборі даних DBIR за останні п'ять років. Брандмауер DNS може запобігти від 19 до 37 мільярдів доларів в США або від 150 до 200 мільярдів доларів у всьому світі.

Розглянуто алгоритм забезпечення безпечного доступу користувачів до

Інтернет на базі DNS-платформи Quad9 та визначено порядок його розгортання.

Надано рекомендації щодо забезпечення безпечного доступу користувачів до Інтернет, а також керівникам підприємств, розробникам систем безпеки та фахівцям з кібербезпеки.

Таким чином, запропоновані в роботі рекомендації мають сприяти забезпеченню підвищеної безпеки для приватних осіб, бізнес-користувачів і їх клієнтів в мережах, пристроях, цифрових активах і продуктах IoT.

Застосування рішення Quad9 на базі DNS-платформи забезпечує ефективний додатковий рівень захисту. Це досягається шляхом маршрутизації DNS-запитів через мережу серверів безпеки по всьому світу. Рішення Quad9 базується на даних про загрози, які зібрані від ряду авторитетних компаній, що займаються кібербезпекою, для оцінки ризиків кожного веб-сайту, що відвідує користувач в режимі реального часу і блокує доступ до них.

ПЕРЕЛІК ПОСИЛАНЬ

1. Michael Aliperti. Malware, Malicious Domains, and More: How Cybercriminals Attack SLTT Organizations [Електронний ресурс] – Режим доступу: https://www.standingstonebank.com/wp-content/uploads/sites/174/September-Cyber-Tip-Newsletter.pdf.

2. McAfee Labs Threats Report. November 2020 [Електронний ресурс] – Режим доступу: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf.

3. 2021 Threat Predictions Report. McAfee [Електронний ресурс] – Режим доступу: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/2021-threat-predictions-report.

4. NIST Special Publication 800-81-2. Secure Domain Name System (DNS). Deployment Guide. Ramaswamy Chandramouli. Scott Rose. September 2013 [Електронний ресурс] – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-81/2/final.

5. Що таке 1.1.1.1? [Електронний ресурс] – Режим доступу: https://www.cloudflare.com/learning/dns/what-is-1.1.1.1.

6. OpenDNS (Cisco) [Електронний ресурс] – Режим доступу: https://www.comss.ru/page.php?id=759.

7. Introduction to Google Public DNS [Електронний ресурс] – Режим доступу: https://developers.google.com/speed/public-dns/docs/intro.

8. Quad9 public domain name service moves to Switzerland for maximum internet privacy protection. February 14, 2021 [Електронний ресурс] – Режим доступу: https://quad9.net/news/blog/quad9-public-domain-name-service-moves-to-switzerland-for-maximum-internet-privacy-protection/.

9. THE ECONOMIC VALUE OF DNS SECURITY. Adam Shostack, Jay Jacobs and Wade [Електронний ресурс] – Режим доступу: Baker https://www.globalcyberalliance.org/wp-content/uploads/GCA-DNS-Security-

Report.pdf.

10. QUAD9 [Електронний ресурс] – Режим доступу: https://sysadmin.pm/quad9/.

11. Threat blocking [Електронний ресурс] – Режим доступу: https://www.quad9.net/service/threat-blocking.

12. Service Addresses & Features [Електронний ресурс] – Режим доступу: https://www.quad9.net/service/service-addresses-and-features.

13. Основні правила захисту даних — кібергігієна для активного Інтернет-користувача [Електронний ресурс] – Режим доступу: https://eset.ua/ua/blog/view/38/osnovnyye-pravila-zashchity-dannykh-kibergigiyena-dlya-aktivnogo-Internet-polzovatelya.

14. Основні правила кібергігієни. CERT-UA [Електронний ресурс] – Режим доступу: https://cert.gov.ua/recommendation/31.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)