Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

спеціальність *125 Кібербезпека*
(код і назва спеціальності)

освітній ступень *магістр*
(назва освітнього рівня)

освітньо-наукова програма *кібербезпека*
(назва освітньої програми)

на тему: Застосування механізмів Dark Web для вдосконалення рівня захисту Інтернету речей

Виконавець: студентка ІІ курсу, групи КБм-21

Гончаренко Наталія Аркадіївна
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	Оцінка	Підпис
Науковий керівник	Толюпа С. В.		
Рецензент	Степанов М. М.		
Нормоконтроль	Даков С. Ю.		

Київ
2022

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту інформації

_____ Н.В. Лукова-Чуйко

«____»_____20__року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студентці КБм-21 (група) Гончаренко Наталії Аркадіївні (прізвище ім'я по-батькові)

Тема дипломного роботи Застосування механізмів Dark Web для вдосконалення рівня захисту Інтернету речей

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 29.10.2021.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень	Процес захисту інформації, що зберігається, оброблюється і передається між «розумними» пристроями та Інтернет.
Предмет досліджень	Методи захисту IoT-мереж від кібератак із застосуванням основних принципів роботи Dark Web.
Мета	Підвищення рівня захищеності Інтернету речей за рахунок впровадження основоположних механізмів функціонування Dark Web.
Вихідні дані для проведення роботи	Методи захисту IoT-мереж від атак за допомогою технології onion-маршрутизації трафіку.

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна Удосконалення архітектури типової мережі «розумних» пристроїв за рахунок поєднання технологій «темної» павутини та використання окремої апаратної платформи із програмним забезпеченням.

Практична цінність Покращення рівня захищеності IoT-мереж для звичайних користувачів та організацій різних форм власності.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Обґрунтування вибору теми роботи. Попереднє складання змісту магістерської роботи.	29.10.2021 – 24.11.2022
Первинний аналіз літературних джерел. Збір і обробка конкретних теоретичних положень.	25.11.2022 – 15.02.2022
Проведення необхідних практичних досліджень. Написання та оформлення магістерської роботи.	16.02.2022 – 24.04.2022
Перевірка роботи науковим керівником. Оформлення і друк пояснювальної записки.	25.04.2022 – 20.05.2022

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект Зниження витрат на покриття збитків через компрометацію особистих даних.

Соціальний ефект Покращення рівня захищеності IoT-мереж для звичайних користувачів та організацій різних форм власності.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ _____
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ЕК _____

УДК 004.492.2

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Застосування механізмів Dark Web для вдосконалення рівня захисту Інтернету речей» складається зі вступу, трьох розділів, що містять 40 рисунків та 2 таблиці, висновків, списку використаних джерел із 35 найменувань. Загальний обсяг роботи становить 80 аркушів, з яких 4 аркуші займає список використаних джерел, без урахування додатків.

Об’єкт дослідження – процес захисту інформації, що зберігається, оброблюється і передається через незахищене середовище між «розумними» пристроями та мережею Інтернет.

Предмет дослідження – методи захисту IoT-мереж від існуючих видів кібератак із застосуванням основних принципів, на яких функціонує «темна» павутина.

Мета дослідження – підвищення рівня захищеності Інтернету речей за рахунок впровадження основоположних механізмів функціонування Dark Web.

У даній роботі досліджено сучасні загрози та методи протидії атакам на «розумні» пристрої, проведено аналіз впливу технологій Dark Web та пошукового агрегатора Shodan на стан безпеки Інтернету речей та побудовано захищену IoT-мережу з використанням принципів onion-маршрутизації трафіку.

Наукова новизна: удосконалення архітектури типової мережі «розумних» пристроїв за рахунок поєднання технологій «темної» павутини та використання окремої апаратної платформи із спеціалізованим програмним забезпеченням.

Отримані у ході проведеного дослідження результати можуть бути використані в процесі модернізації існуючих IoT-мережах та забезпечать дійсно надійний рівень захисту трафіку всередині від несанкціонованого доступу.

Ключові слова: Інтернет речей (IoT), Dark Web (темна павутина), Deep Web, «розумні» пристрої, TOR, onion-служба, Shodan, анонімність, Raspberry Pi, Home Assistant.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

БСМ	–	Бездротова сенсорна мережа
ІБ	–	Інформаційна безпека
ІТ	–	Інформаційні технології
НСД	–	Несанкціонований доступ
ПЗ	–	Програмне забезпечення
CaaS	–	Crime-as-a-Service
CVE	–	Common Vulnerabilities and Exposures
Dark Web	–	«Темна» павутина
DDoS	–	Distributed Denial of Service
DNS	–	Domain Name System
ECC	–	Elliptical Curve Cryptography
FTP	–	File Transfer Protocol
Hidden Service/Onion Service	–	Прихована служба (сервер)
Honeypot	–	«Медова» пастка
HTTP	–	Hypertext Transfer Protocol
I2P	–	Invisible Internet Project
IoT	–	Internet of Things (Інтернет речей)
KRACK	–	Key reinstallation attack
MITM	–	Man-in- the-Middle
SBC	–	Single Board Computer
SCADA	–	Supervisory Control And Data Acquisition
SQL	–	Structured Query Language
SSH	–	Secure Shell
SSL	–	Secure Sockets Layer
TOR	–	The Onion Routing
VPN	–	Virtual Private Network

ВСТУП

Актуальність. В останні роки Інтернет речей став одним із найбільш стрімких напрямків розвитку серед тенденцій інформаційного простору. Однак розширення спектру викликів для безпеки, таких як вразливості програмного забезпечення та кібератаки, часто змушують багатьох споживачів утриматися від широкого використання «розумних» пристроїв. Такі проблеми є особливо критичними для організацій у ланках охорони здоров'я, фінансів, виробництва, логістики, роздрібної торгівлі та інших галузей, в яких вже розпочалось активне залучення різноманітних IoT-систем. Оскільки на згадані системи все частіше покладаються обов’язки управління надзвичайно складними об’єктами інфраструктури, питання безпеки та надійності даних, що циркулюють у відповідних IoT-мережах, є як ніколи актуальним не тільки для окремих осіб, а й суспільства та держави в цілому.

Проведений у даній роботі аналіз доводить, що на сьогоднішній день відомі методи захисту Інтернету речей є малоефективними або подекуди відсутні взагалі. Як результат, основними причинами виникнення проблем безпеки IoT-пристроїв є їх незахищене необмежене підключення до Інтернету та відсутність будь-яких механізмів контролю доступу для створення безпечної комунікації. Крім того, загрози експлуатації вразливостей в IoT зазвичай виникають через фізичну нестачу ресурсів в IoT-системах (з точки зору обчислювальної потужності, об’єму пам’яті і т.д.), відсутність стандартизації в використовуваних протоколах безпеки, а також завдяки частій несумісності між собою апаратного та програмного забезпечення від третіх сторін. Все це робить недоцільним впровадження складних та надійних алгоритмів шифрування трафіку для створення безпечного каналу зв’язку між IoT-пристроями, що непомірно підвищує їх сприйнятливість до різних типів атак.

Таким чином, актуальним науковим завданням, що має теоретичне і практичне значення, є удосконалення існуючих методів захисту Інтернету речей.

Мета роботи полягає у підвищенні рівня захищеності Інтернету речей за рахунок впровадження основоположних механізмів функціонування Dark Web. Для досягнення цієї мети в роботі необхідно вирішити такі *завдання*:

1. розглянути сутність поняття Інтернету речей та «розумного» будинку як його невід'ємної частини;
2. визначити основні вектори загроз для IoT-пристроїв та існуючі методи їх захисту;
3. дослідити вплив Dark Web, у тому числі мережі TOR, на безпеку Інтернету речей;
4. проаналізувати на практиці можливості пошукового агрегатора Shodan для виявлення та експлуатації уразливостей в IoT-пристроях;
5. розглянути особливості існуючих конфігурацій щодо організації типової мережі «розумних» пристроїв;
6. запропонувати концептуальну архітектуру нового рішення для підвищення рівня захисту Інтернету речей на основі механізмів Dark Web;
7. визначити основні переваги та недоліки пропонованого рішення.

Виходячи з такого, у роботі *об'єктом дослідження* є процес захисту інформації, що зберігається, оброблюється і передається через незахищене середовище між «розумними» пристроями та мережею Інтернет. *Предмет дослідження* – методи захисту IoT-мереж від існуючих видів кібератак із застосуванням основних принципів, на яких функціонує «темна» павутина.

Для вирішення вище окресленого наукового завдання в роботі використані *методи* інформаційного пошуку, аналізу та синтезу (при розкритті теоретичних положень та уточненні понятійного апарату), метод максимальної правдоподібності, імітаційне моделювання (при перевірці отриманих результатів), а також задіяне проведення експерименту.

Наукова новизна одержаних результатів полягає у значному удосконаленні архітектури типової мережі «розумних» пристроїв за рахунок поєднання технологій «темної» павутини (у тому числі й onion-маршрутизації) та використання окремої апаратної платформи із спеціалізованим програмним забезпеченням, що дозволило

захистити розглянуту IoT-мережу майже від усього спектру поширених кібератак, до яких є надзвичайно сприйнятливими її інші класичні аналоги конфігурації.

Практичне значення одержаних результатів. Отримані у ході проведеного дослідження результати можуть бути використані в процесі модернізації існуючих IoT-мережах та забезпечать дійсно надійний рівень захисту трафіку всередині від несанкціонованого доступу. Створені рекомендації можуть бути корисними при проектуванні та експлуатації корпоративних IoT-систем у контексті планування захисту від витоку важливої інформації.

Апробація результатів роботи:

1. Гончаренко Н. А. Dark Web як частина Всесвітньої павутини та його вплив на суспільство. IV Міжнародна науково-практична конференція «Прикладні системи та технології в інформаційному суспільстві» (AISTIS) – Київський національний університет імені Т. Г. Шевченка, 30 вересня 2020.

2. Гончаренко Н. А. Безпека Інтернету речей (IoT) проти пошукового агрегатора Shodan. Всеукраїнська науково-практична Інтернет-конференція «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» – Київ, Державний університет телекомунікацій, 25 лютого 2021.

3. Гончаренко Н. А. Застосування механізмів Dark Web для забезпечення нового рівня захисту IoT. IV Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) – Київський національний університет імені Т. Г. Шевченка, 15-16 квітня 2021.

4. Serhii Toliupa, Nataliia Honcharenko, Yuriy Shcheblanin. The Potential Danger of Shodan Search Engine. VIII International conference «Information Technology and Implementation» (IT&I-2021) – Taras Shevchenko National University of Kyiv, December 1-3, 2021.

РОЗДІЛ 1
ОСНОВНІ ПРИНЦИПИ ФУНКЦІОНУВАННЯ ІНТЕРНЕТУ РЕЧЕЙ

1.1 Основна проблематика безпеки функціонування Інтернету речей

1.1.1 Загальне визначення механізмів роботи Інтернету речей

З кожним днем ми стаємо все більш залежними від технологій, що зумовлено прискореним розвитком Інтернету речей (IoT) – складної мережі фізичних пристроїв та систем із доступом до мережевого підключення, яке дозволяє їм обмінюватися даними через Інтернет [1]. Мабуть, таке явище вважалося б науково-фантастичним 30 років тому, однак сьогоднішня реальність доводить, що кіберфізичні системи пронизують усі аспекти нашого сучасного життя. Їх застосування включає моніторинг навколишнього середовища, управління інфраструктурою, охорону здоров’я, транспорт та ін.

У сучасному світі концепція взаємодії онлайн-пристроїв – Інтернет речей – уже затверділа як окремий напрямок інформаційної безпеки (ІБ). Швидше за все, більшість людей давно використовують технології IoT у своєму житті, навіть не усвідомлюючи цього. У звіті Business Insider Intelligence за 2016 рік [2] зазначається, що до 2020 року до мережі Інтернет буде підключено близько 34 мільярдів пристроїв, 24 мільярди з яких будуть пристроями IoT, а лише решта 10 мільярдів – традиційними обчислювальними пристроями, такими як смартфони, комп'ютери та планшети. Тим, хто вважає, що вони володіють лише «традиційними обчислювальними пристроями», а не пристроями IoT, доведеться переглянути свої переконання ще раз, бо насправді деякі настільки звичні нам речі можуть мати далеко неочевидний зв'язок з глобальною мережею, а ступінь їх захищеності у нашій свідомості буде занадто завищена [3].

У чому ж полягає основна особливість функціонування згаданого IoT-пристрою? IoT-пристрій здатен самостійно підключатися до Інтернету та

взаємодіяти з його середовищем через збір та обмін даних. Такі «розумні» девайси зазвичай мають обмежену обчислювальну спроможність і оперують лише кількома конкретними функціями. Отже, увесь Інтернет речей дійсно стосується у деякому розумінні незвичних пристроїв, підключених до Інтернету. Тут під поняттям «незвичного» будемо мати на увазі все, що не можна вважати традиційним комп'ютером [4].

Сфера впливу Інтернету речей поширилася на майже усі аспекти людського життя, серед яких окремої уваги варті:

- медицина та охорона здоров’я;
- аграрний сектор;
- управління критичною інфраструктурою;
- побутові прилади та портативні пристрої;
- організація захищеного периметру;
- моніторинг об’єктів;
- архітектура «розумних» будинків.

На рисунку 1.1 узагальнені основні аспекти людської діяльності, що є найбільш уразливими до загроз IoT [5]:

Рисунок 1.1 – Сфери впливу загроз безпеки IoT

Варто відзначити, що інфраструктура «розумних» будинків користується доволі високим попитом як і серед звичайних споживачів, що прагнуть полегшити керування власними домівками, так і серед зловмисників, ціллю яких є несанкціонований збір користувацьких даних та порушення стабільної роботи відповідних IoT-систем.

Розглянемо структуру типового «розумного» будинку, що зображений на рисунку нижче:

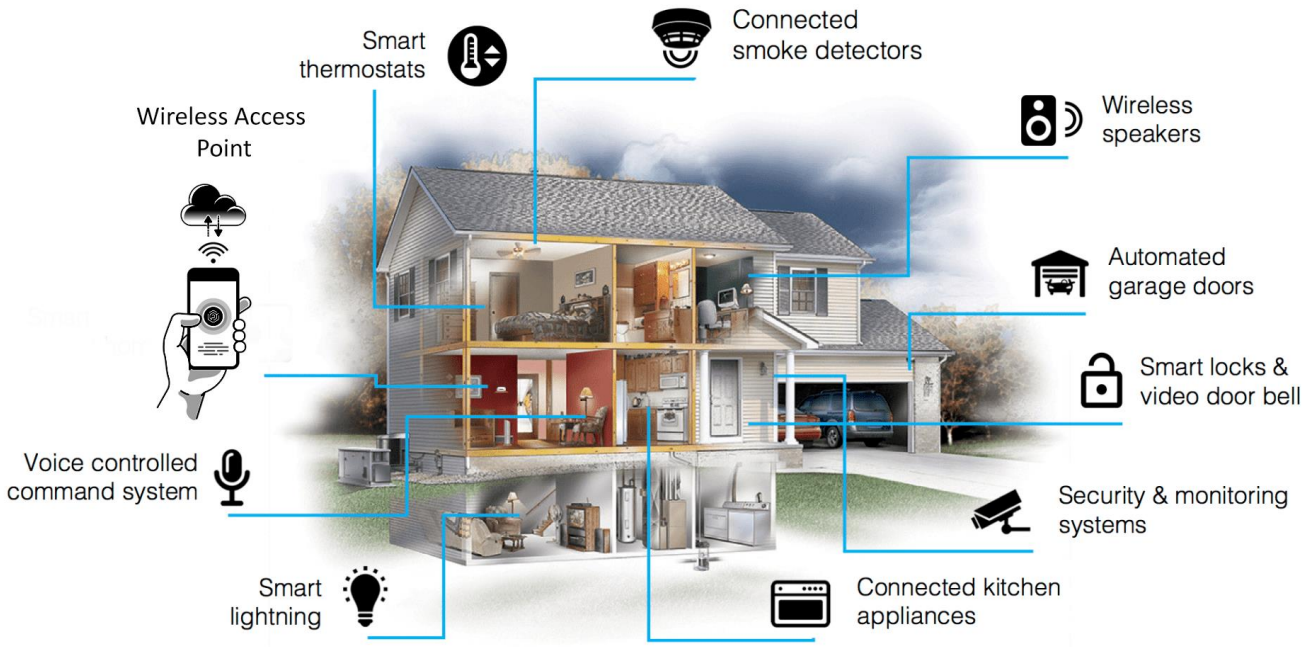

Рисунок 1.2 – Інфраструктура типового «розумного» будинку

У широкому сенсі, «розумний» будинок або Smart House – це будинок, який включає в себе просунуті системи автоматизації для забезпечення його мешканців механізмом розширеного моніторингу та контрою над функціями будівлі [6]. Наприклад, системи «розумного» будинку можуть керувати освітленням, температурою, мультимедіа і т.д.

До порівняння, відділ торгівлі та промисловості Великобританії (DTI) надав наступне визначення «розумного» будинку: «Житло, що включає в себе комунікаційну мережу, яка з'єднує основні електроприлади, і дозволяє здійснювати дистанційний контроль над ними» [6].

Для нормального функціонування кожен із зазначених пристроїв на рисунку має час від часу або ж постійно підтримувати зв'язок із зовнішньою мережею. Дана умова є визначальною у потребі забезпечення надійного захисту IoT-пристроїв.

Окремої уваги варта часта недосконаліть мобільних додатків, що зазвичай використовуються у якості централізованої платформи для керування потужностями «розумного» будинку (рис.1.3).

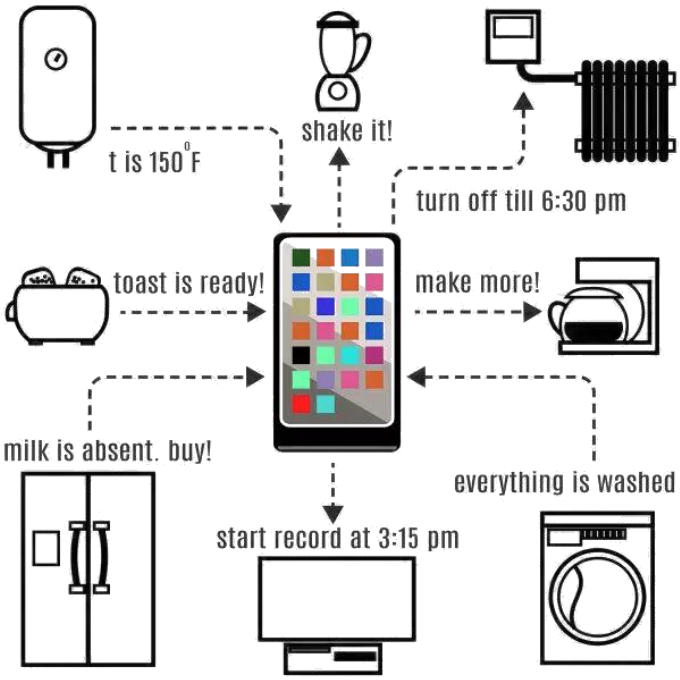

Рисунок 1.3 – Смартфон користувача як єдина платформа управління «розумними» пристроями

Халатність розробників ПЗ може призвести до того, що, отримавши віддалений чи фізичний доступ до телефона власника, зловмисник буде у змозі повністю перейняти управління усіма пристроями будинку.

Наразі ринок технологій може запропонувати своїм користувачам незлічену кількість різноманітних продуктів, проте водночас він зумовлює доволі глибокий рівень фрагментації Інтернету речей, що несе за собою цілий ряд незручностей. Портативність пристроїв представляє ще більшу загрозу зараження не тільки власної, а й інших мереж. Крім того, відсутність стандартизації в галузі призвела до появи численних проблем сумісності, які також суттєво ускладнюють становище зі створення безпечної IoT-інфраструктури [7].

1.1.2 Аналіз існуючих загроз для IoT-пристроїв

Очевидно, технології IoT та люди тісно пов'язані між собою, проте якщо останні можуть контролювати те, що вони здебільшого роблять, то як щодо їхніх девайсів? Переважна більшість користувачів взагалі не вглиблюється у механізми керування безпекою своїх смарт-пристроїв, обмежуючись тим, що просто не діляться паролями доступу до них. Таким чином, пересічний користувач, як правило, перебуває на повній милості виробника цих продуктів в аспекті забезпечення захисту і надійності. Отже, за безпеку згаданих смарт-пристроїв несе відповідальність виключно їх виробник, а якщо його дітище було скомпрометоване, то клієнт може вжити заходів (законних чи інших), щоб повернути свою цифрову ідентичність? Це твердження є докорінно невірним. Навіть якщо уявити розгортання такого сценарію на практиці, то власнику пристрою знадобиться значні час, гроші та ресурси, щоб повернути своє цифрове «Я» до нормального стану. Крім того, спроби зачищення особистої інформації, що описаним чином потрапила на простори Інтернету або в Dark Web, рідко закінчуються успіхом [2]. У даному випадку неможливо не згадати про існування прихованих шарів Всесвітньої павутини – Deep Web і Dark Web. Ще у 2001 році було підраховано [8], що ці шари в 400-500 разів перевищують поверхневий сегмент павутини. З масовим поширенням Інтернету це число тільки зростає, тому старий жарт на кшталт «Я дійшов до кінця Інтернету» тепер стосується лише тієї частини Web, яка є доступною для звичайного користування.

З вищезазначеної точки зору, безпеку Інтернету речей можна розглядати як стратегію та набір механізмів захисту, що мають на меті цілеспрямований захист пристроїв мережі від можливості здійснення проти них кібератак. Таким чином, без дотримання відповідного рівня безпеки будь-який підключений IoT-пристрій вразливий до зламу. Найчастіше інфіковані шкідливим програмним кодом «розумні» пристрої можуть використовуватися у якості ботнетів для запуску DDoS-атак на цільову мережу, у роботу якої зловмисник має намір втрутитися. На відміну від звичайних IT-пристроїв, величезний набір апаратних та операційних систем, на

базі яких працюють IoT-пристрої, неможливо захистити одним і тим же чином, оскільки єдиного засобу для профілактики від зараження, сумісного з більшістю IoT-платформ, не існує [9]. На рисунку 1.5 узагальнені основні причини надзвичайної ефективності здійснення атак на більшість IoT-мереж:

Рисунок 1.5 – Основні виклики для безпеки IoT

Застосування слабких парольних політик сприяє різкому підвищенню ефективності брут-форсу, а зростаюча кількість IoT-пристроїв все ще запускається та працює на застарілих версіях операційних систем. Використання неактуальних апаратних/програмних платформ часто виникає через неможливість забезпечення поставок цих компонентів від надійних виробників. До прикладу, програмне забезпечення від стороннього постачальника, що не пройшло перевірку на наявність відомих вразливостей, забезпечує чудову основу для компрометації кінцевих користувачів. Також варто не забувати, що доволі велика частина виробників «розумних» пристроїв використовує практику приховування розширених налаштувань конфігурації за жорстко закодованими парольними комбінаціями, що згодом стають публічно доступними в мережі Інтернет. Іноді ж для повноцінної інтеграції IoT-пристрою його користувач змушений встановлювати додаткові

непотрібні мережеві сервіси, які нерідко нехтують вимогами безпечного зберігання даних [9].

Окрім зазначеного на рисунку переліку загроз, додатковою причиною для занепокоєння є те, що з кожним днем все більша кількість різновидів IoT-пристроїв безперервно продовжує підключатися до глобальної мережі, що веде до значного розширення спектру можливих атак. Більше того, вся ефективність впроваджених засобів мережевої безпеки зводиться до рівня захищеності найменш безпечного пристрою, якщо вважати цей пристрій таким, що вже має певні механізми захисту. 98% всього трафіку IoT-пристроїв циркулює у незашифрованому вигляді, що ставить під загрозу конфіденційні дані їх користувачів [9].

Як наслідок, найбільша частка нападів підпадає на використання експлойтів, виявлених при мережевому скануванні, а також віддалене виконання коду, ін'єкції команд та ін. На рисунку 1.6 видно, що майже половина згаданих атак зловживають загальновідомими вразливостями пристрою, а після його зламу намагаються отримати доступ до якомога більшого сегменту мережі через вибірковий пошук слабких сторін її інших вузлів [9]. Однак природньо, що бізнес в умовах постійної конкуренції намагається скоротити витрати на впровадження засобів вбудованої безпеки до своєї продукції, у тому числі і за рахунок використання неякісних матеріалів для дизайну в цілому.

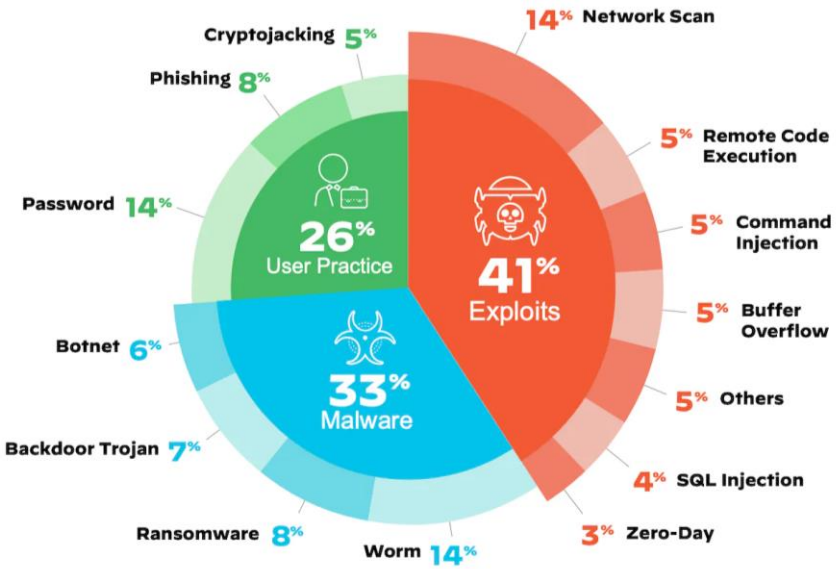

Рисунок 1.6 – Основні напрямки експлуатації вразливостей IoT-пристроїв

Наведемо найпоширеніші типи кібератак, що застосовуються зловмисниками для ураження IoT-пристроїв:

1. Man-In-The-Middle Attack (MITM) – атакуючий видає себе за легітимну одиницю мережі.

2. ThingBot – зловмисник перехоплює контроль над групою пристроїв, перетворюючи їх на ботнет-мережу, без відома власника.

3. Крадіжка інформації – зловмисник отримує доступ до конфіденційних даних жертви та використовує їх у своїх злочинних намірів.

4. Атака з переустановкою ключа (KRACK) – атака повторного відтворення на будь-яку Wi-Fi-мережу, що використовує протокол WPA-2. Вперше виявлена бельгійськими дослідниками Метті Ванхоефом и Франком Пісенсом у 2016 році.

5. Атака типу «відмова в обслуговуванні» (DDoS) – атакуючий намагається вивести з ладу вузол цільової мережі шляхом одночасної відправки надмірної кількості запитів із різних пристроїв.

Розмиті положення політики інформаційної безпеки у розрізі забезпечення конфіденційності даних споживачів призводять до того, що їх особиста інформація може стати доступною третім сторонам через хмарні платформи вендора.

Підсумовуючи вище сказане, легко дійти до висновку, що механізми захисту IoT повинні поширюватися на усі пристрої, які підключені до мережі, щоб забезпечувати безперервну безпеку останніх від зростаючого спектру загроз.

1.1.3 Традиційні методи забезпечення захисту IoT-пристроїв

На жаль, єдиного рішення, яке б забезпечило більш-менш належний захист будь-якої IoT-системи, не існує. Тим не менше, під час проектування архітектури мережі «розумних» пристроїв буде корисним згадати про положення так званого відповідального використання IoT-ресурсів. Вони можуть включати доволі традиційні методи захисту пристроїв у мережі, що завжди будуть до послуг звичайних користувачів (рис. 1.7):

Рисунок 1.7 – Принципи відповідального використання IoT-ресурсів

Розглянемо кожен з них детальніше [7]:

1. Призначити адміністратора. Наявність окремої людини, яка виступатиме адміністратором IoT-пристроїв, допоможе спростити керування мережею. Ця роль є особливо критичною для облаштування робочого місця при віддаленій роботі вдома, коли експерти зі сторони роботодавця мають обмежений контроль над функціями безпеки домашніх мереж своїх працівників, що може в подальшому негативно вплинути на роботу корпоративних ресурсів.

2. Встановити надійні та унікальні паролі до панелі керування розумним будинком, а також домашньої мережі Wi-Fi, самого маршрутизатора та всіх пов'язаних облікових записів. Сильні паролі найдієвіше допомагають запобігти багатьом кібератакам. Для надійного створення та зберігання всього переліку

паролів у нагоді стануть спеціальні парольні менеджери, які відображатимуть останніх у межах єдиного захищеного додатку.

3. Регулярно оновлювати програмне забезпечення на смартфонах, планшетах та розумних гаджетах. Як зазначалося раніше, уразливості є головним і постійним питанням у галузі безпеки IoT. Навіть досить давно віднайдені із них все ще експлуатуються кіберзлочинцями задля проведення атак, доводячи факт того, наскільки довго непропатчені пристрої можуть залишатися доступними в Інтернеті.

4. Впровадити додаткові рішення та інструменти захисту там, де це можливо (наприклад, двофакторну аутентифікацію). Суттєвою проблемою при налаштуванні вбудованих параметрів безпеки IoT-пристроїв є їх сильна обмеженість в гнучкості та адаптації. У таких випадках користувачі можуть компенсувати цю прогалину за допомогою інших рішень, які забезпечують багатошаровий захист та шифрування кінцевих точок.

5. Використовувати спеціалізовані контролери (наприклад, на основі Raspberry Pi) для керування розумним будинком.

6. Створити сегментацію мережі, наприклад, шляхом використання технологій VPN. Користувачі можуть мінімізувати ризик атак, пов'язаних з IoT, створивши незалежні мережі для пристроїв IoT та інших цілей. Сегментація не тільки допомагає запобігти поширенню деструктивної дії атак, а також ізолює ймовірно проблематичні пристрої, які неможливо негайно вилучити в режимі офлайн.

7. Забезпечити гладкий зв'язок усіх пристроїв із хмарою їх виробника. IoT-пристрої і хмарні сервіси стають все більш взаємозалежними, тому важливо враховувати наслідки впливу однієї технології на іншу. Функціонал хмарних рішень доцільно розглядати у якості ще одного інструменту для забезпечення додаткових можливостей захисту кінцевих IoT-систем.

8. Враховувати відмінності використовуваних IoT-пристроями протоколів. Для спілкування пристрої IoT використовують не лише Інтернет, але й величезний набір різних мережевих протоколів, від відомих Bluetooth та NFC, до менш знайомих NRF24, NRFXX, LPD433, оптичного та інфрачервоного зв’язку.

Адміністратори мережі повинні розуміти алгоритми роботи усього цього набору протоколів, що використовуються в їх системах, аби зменшити ризики реалізації загроз безпеки.

9. Обмежити постійне використання GPS. Деякі пристрої та додатки IoT полюбляють зловживати дозволом на використання GPS-сервісів. Пересічним користувачам корисно мати за звичку відключати GPS, коли його застосування не зумовлене безпосередніми потребами відповідного пристрою. Організаціям, зокрема, важливо володіти у своєму розпорядженні засобами моніторингу GPS-сигналу.

10. Пріоритетність безпеки Wi-Fi. Даний пункт може включати в себе низку заходів, як-от: налаштування правил вбудованого брандмауера в маршрутизаторі, деактивацію функцій WPS-кнопки та вибір оптимального методу шифрування трафіку (WPA-2). Крім того, створення надійної конфігурації маршрутизатора шляхом відключення його інших невикористовуваних налаштувань також є важливою частиною цього кроку.

11. Постійний моніторинг стану вузлів мережі та поведінки пристроїв. Знання показників адекватної роботи (швидкість, типова пропускна здатність тощо) пристроїв та мережі можуть допомогти їх власникам спостерігати за відхиленнями, які часто свідчать про наявність шкідливого програмного забезпечення.

Список заходів неповний, але основна ідея полягає в тому, що не варто використовувати пристрої IoT за принципом «простого вставляння вилки до розетки». Тож, контроль над конфіденційністю є основним ключем для безпечного використання технологій IoT.

Практика показує, що дані положення працюватимуть лише за умови придбання продуктів від перевірених часом вендорів, які навряд стануть ризикувати власною репутацією через виявлення бекдорів спільнотою своїх же споживачів. Звичайно, китайські безіменні аналоги коштуватимуть дешевше, проте їх злам – зовсім нескладне завдання навіть для недосвідчених хакерів.

Окрім використання зазначених рекомендацій безпеки, користувачі також повинні бути обізнані про інтеграцію нових розробок в існуючі технології IoT.

Останнім часом захисту IoT приділяється все більше уваги. Постійно проводяться дослідження щодо того, як забезпечити безпеку конкретних галузей діяльності, де застосовуються IoT-пристрої, як контролювати пов’язані з ними загрози та адаптуватися до майбутніх стандартів зв’язку, таких як 5G. Користувачам також необхідно розуміти, що IoT – це мінливе поле, тому механізми безпеки завжди повинні бути у змозі пристосовуватися до змін всередині нього [7].

1.2 Дослідження впливу Dark Web на безпеку Інтернету речей

1.2.1 Рівні розмежування Web-простору

Багато з нас використовують терміни Інтернет та Всесвітня павутина (World Wide Web) як взаємозамінні, але насправді вони не є синонімами. Інтернет та Web – це дві окремі, хоча і пов’язані речі. Інтернет – масивна мережа мереж (мережева інфраструктура), що з'єднує мільйони комп'ютерів у всьому світі, утворюючи одну систему, в якій будь-який комп'ютер може спілкуватися з будь-яким іншим комп'ютером, якщо вони обидва підключені до цієї мережі. З іншого боку, Всесвітня павутина, або просто Web – це спосіб доступу до інформації через Інтернет або ж модель обміну інформацією, яка побудована на самій верхівці Інтернету. Для передачі даних Web використовує протокол передачі гіпертексту (HTTP) – єдиний метод, за допомогою якого транспортуються дані від відправника до отримувача. Проте Інтернет, а не Web, також використовується ресурсами електронної пошти, робота яких спирається на SMTP та FTP протоколи. У свою чергу, Web – лише частина Інтернету, хоч і досить велика. Нарешті, Deep Web – це, простіше кажучи, частина Web, яка прихована від очей рядового користувача. До нього не можуть отримати доступ звичайні пошукові системи. Цей масивний підрозділ Інтернету в 500 разів більший за видимий Інтернет [10].

Як результат, виділяють три якісно різні рівні Web-простору [11]:

- Загальнодоступна мережа: зазвичай вона відноситься до незашифрованої мережі. Цей сегмент Web має відносно низьку анонімність, оскільки більшість веб-сайтів регулярно ідентифікують користувачів за їхньою IP-адресою.

- Deep Web: стосується вмісту в Інтернеті, який не є частиною загальнодоступної мережі. Проведемо аналогію: супер-агент мусить виконати ціль X у локації Y. Але замість того, щоб шукати Y за картою, йому доведеться відвідати Y безпосередньо. На агента чекають для виконання X за умови, якщо йому буде відома адреса Y, але при цьому він не матиме ніяких вказівок, як туди дістатися. Інтернет занадто великий, щоб його могли повністю охопити пошукові системи; таким чином, глибока павутина значною мірою завжди присутня. У Deep Web, як правило, згадуються веб-сторінки, що невидимі для засобів традиційних пошукових систем. Найчастіше для сканування «глибоких» веб-ресурсів використовують спеціальні веб-сканери, які на основі ключових термінів, наданих користувачами або зібраних з інтерфейсів запиту, звертаються до відповідної веб-форми.

- Dark Web (темна павутина): частина глибокої павутини, до якої можна отримати доступ лише за допомогою певного програмного забезпечення, конфігурацій або авторизації, часто використовуючи нестандартні протоколи та порти зв'язку. Onion-маршрутизація використовується для доступу до таких веб-сайтів, сукупність яких називається мережею TOR. Трафік при такій маршрутизації багаторазово шифрується, а потім надсилається через кілька мережевих вузлів, які називаються onion-маршрутизаторами. Як тільки хтось «лущить цибулю», кожен маршрутизатор видаляє шар шифрування, щоб розкрити інструкції маршрутизації, і надсилає повідомлення наступному маршрутизатору, де процес повторюється. Цей прийом заважає стороннім вузлам дізнатися походження, пункт призначення та вміст передаваних даних.

Наступна схема відображає різницю між Deep Web, Dark Web та мережею Інтернет (рис. 1.8):

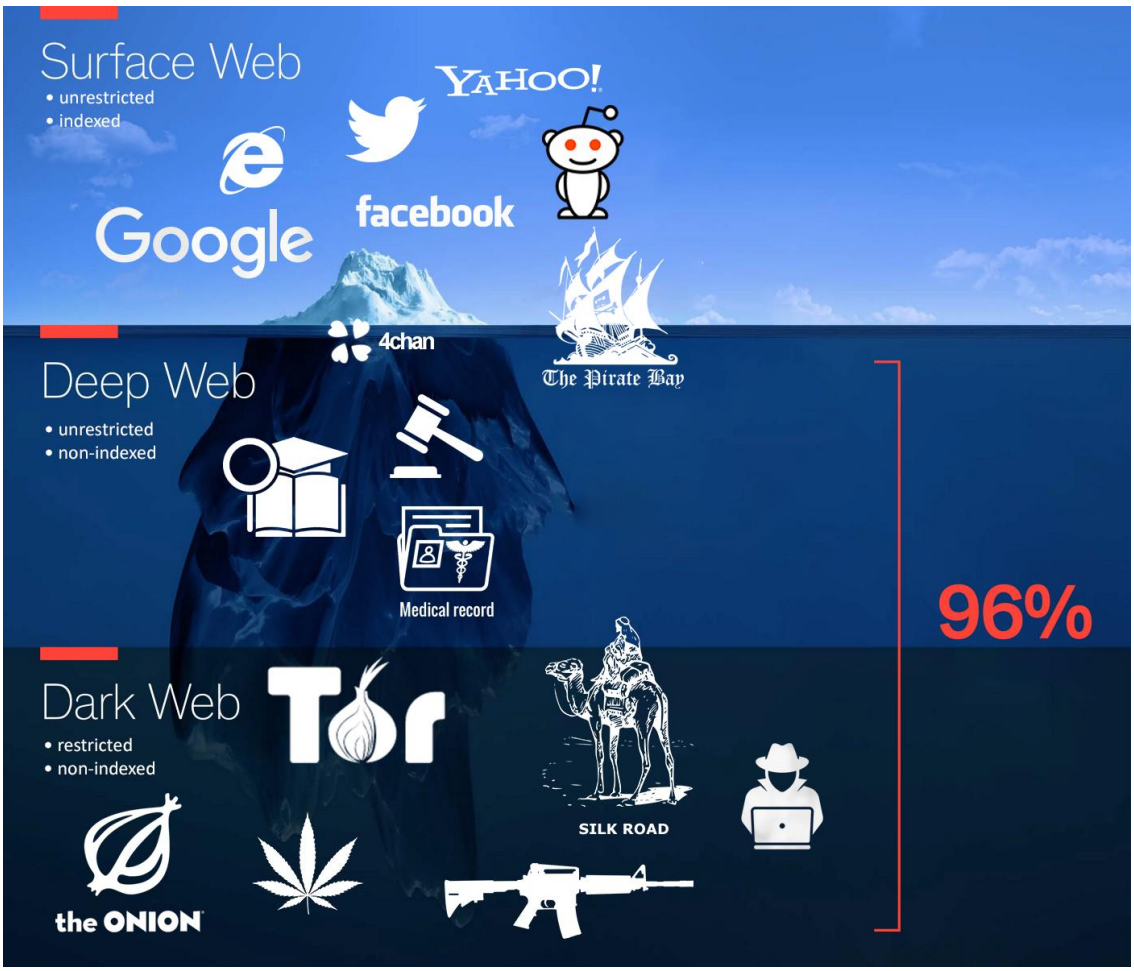

Рисунок 1.8 – Відмінності між Deep Web, Dark Web та Surface Internet

Таким чином, відсутність видимої діяльності в нетрадиційних мережах, таких як Deep Web і, зокрема, TOR, не обов'язково означає, що вони не існують. Насправді, згідно з основоположним принципом, який керує темною павутиною, цю діяльність просто важче помітити. Цілком можливо, що переважна більшість веб-сайтів може виходити в Інтернет у визначений час, мати коротке вікно активності, а потім зникати, роблячи себе більш складними для відстеження [10].

1.2.2 Мережа TOR як спосіб доступу до ресурсів Dark Web

Щодня активність в Інтернеті залишає сліди, які формують нашу цифрову ідентичність у віртуальному просторі. Анонімність використання Інтернету гарантується тоді, коли адреси Інтернет-протоколу (IP) неможливо відстежити. Отож, темна павутина – це частина глибокої павутини, яка була навмисно прихована

та недоступна для стандартних веб-браузерів. Темні веб-сайти служать платформою для користувачів Інтернету, для яких анонімність є критично необхідною умовою, оскільки такі сайти не тільки забезпечують захист від несанкціонованих користувачів, але також зазвичай включають шифрування для запобігання моніторингу. Порівняно відомим інструментом для доступу до контенту, що знаходиться в Dark Web, є мережа TOR. Мережа TOR – це анонімна мережа, доступ до якої можна отримати лише за допомогою спеціального веб-браузера, який називається браузером TOR (модифікований Mozilla Firefox ESR). Вперше дебютований як проект The Onion Routing (TOR) у 2002 році Американською морською дослідницькою лабораторією, він був методом анонімного спілкування в Інтернеті [10].

Як згадувалося раніше, TOR використовує концепцію так званої «цибульної» маршрутизації, за правилами якої трафік користувача спочатку шифрується, а потім передається через ланцюг вузлів-посередників, що присутні в мережі TOR. Таким чином, засобами цієї мережі створюється багатошарове шифрування, за рахунок якого значно ускладняється можливість відстеження шляхів циркуляції даних. Як результат, пов’язати особу користувача з будь-якою єдиною точкою неможливо [12].

Користувач запускає через TOR-браузер на комп’ютері «цибульний» проксі-сервер, який періодичного утворює/розриває ланцюги із серверами мережі TOR та реалізує функціонал програмного інтерфейсу SOCKS. Трафік користувача проходить через три випадково обрані проксі-вузли мережі TOR. Перед відправкою пакети послідовно шифруються трьома ключами: спочатку – для третього вузла, потім – для другого та в кінці – для першого. Кожен вузол TOR при отриманні зашифрованого клієнтом трафіку таким же чином послідовно знімає верхній рівень шифрування, а решту даних пересилає наступному випадковому посереднику (рис. 1.9).

Всередині мережі TOR трафік перенаправляється від одного вузла на інший і, нарешті, досягає вихідної точки, з якої незашифрований пакет даних вже прямує до кінцевої адреси одержувача (сервера). Для сервера призначення останній вузол

мережі буде вважатися джерелом походження даних. Потім трафік від сервера повертається назад до користувача.

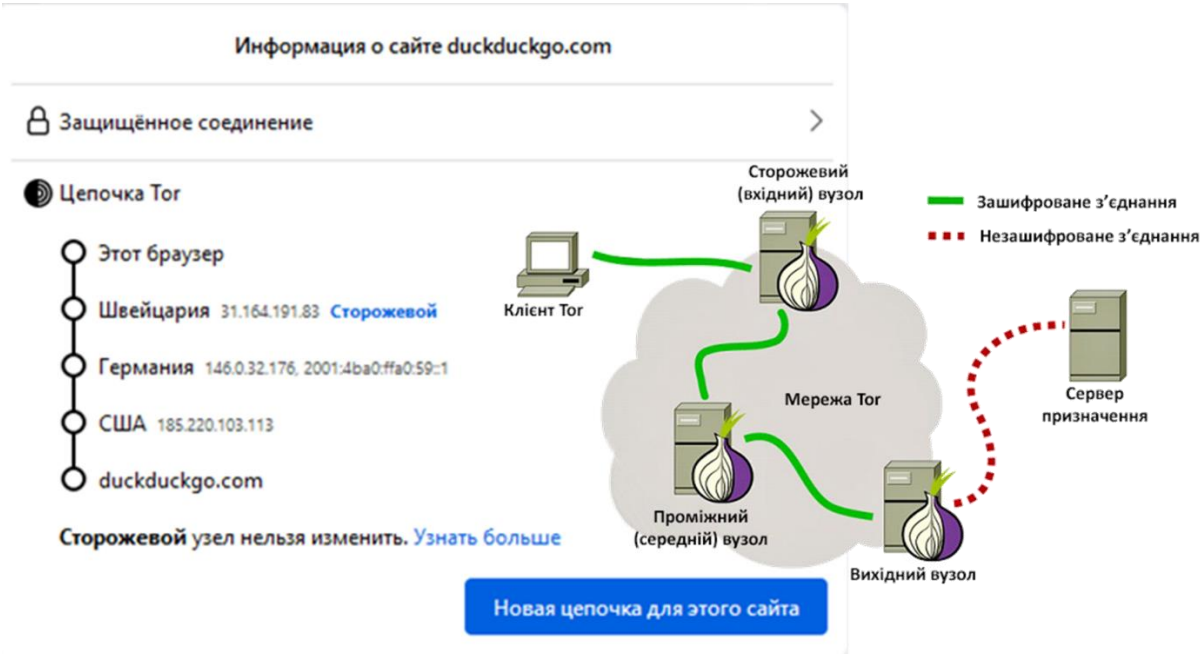

Рисунок 1.9 – Схема роботи вузлів мережі TOR

Чи може вихідний вузол отримати доступ до незашифрованого трафіку користувача? Як зазначають розробники TOR Project, це цілком можливо. Однак справжнє походження трафіку цей вузол дізнатися не в змозі, оскільки він буде вважати відправником даних попередній вузол мережі [13].

Починаючи з 2004 року, TOR також може забезпечити анонімність і для серверів, що дозволяє приховувати їх знаходження в Інтернеті, за допомогою спеціальних налаштувань анонімної мережі [12]. Приховані служби (hidden service/onion service) доступні тільки через спеціальні псевдодомени верхнього рівня .onion. Мережа TOR розпізнає ці домени та анонімно надсилає відповідним прихованим службам інформацію для обробки останніми за допомогою стандартного програмного забезпечення, налаштованого для прослуховування лише непублічних інтерфейсів (закритих для зовнішнього доступу).

Приховані служби внутрішнього псевдодомену .onion не індексуються звичайними пошуковими системами та недоступні через звичайні браузери. До того

ж, для зовнішнього спостерігача безпосередньо перейти на сервер, де зберігаються ресурси сайту, як і визначити його місцезнаходження, майже неможливо. На рисунку 1.10 видно, що для забезпечення анонімності кінцевого сервера застосовуються ті ж самі принципи перенаправлення трафіку, що і для користувача.

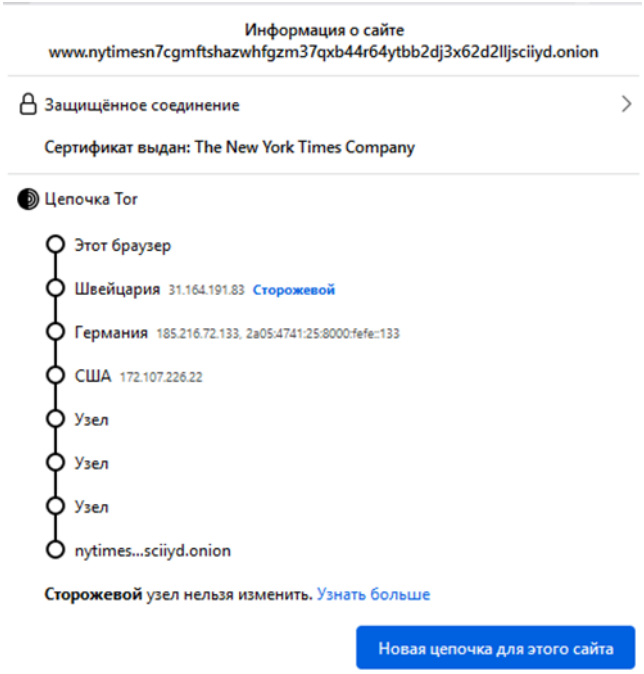

Рисунок 1.10 – Приклад ланцюга доступу до офіційної onion-служби видання «The New York Times»

Існують спеціальні пошукові сервіси для onion-сайтів, але через особливості функціонування Dark Web вони не дуже добре справляються зі своїм завданням. Тому в Dark Web набули високої популярності різноманітні словники посилань, за допомогою яких можна швидко знайти ресурс по необхідній темі, що особливо зручно для новачків.

Оскільки TOR спрямовує Інтернет-трафік через всесвітню добровільну мережу серверів, приховуючи інформацію про користувача та уникаючи будь-яких заходів моніторингу, це робить Dark Web дуже доречним ресурсом для кіберзлочинців, які постійно намагаються приховати свій незаконний промисел. Також можливість серфінгу просторами Інтернету з повною анонімністю сформувала платформу, яка дозріла до того, що її використання у деяких країнах

вважається незаконною діяльністю. Подібна діяльність, зокрема, найчастіше охоплює [10]:

- ринки збуту заборонених речовин;
- шахрайство з кредитними картками та викрадення особистих даних;
- витоки конфіденційної інформації;
- продаж крадених товарів;
- зброя та екзотичні тварини;
- тероризм;
- незаконні фінансові операції;
- hidden wiki (один із найвідоміших словників посилань);
- азартні ігри;
- та ін.

При цьому варто зазначити, що саме по собі використання TOR не несе за собою ніяких правових протиріч із законодавством.

Інша відома мережа під назвою I2P надає багато тих самих функцій, що і TOR, однак I2P була спроектована як мережа в Інтернеті, в якій трафік циркулює тільки її в межах. Варто відмітити, що TOR забезпечує кращий анонімний доступ до відкритого Інтернету, а I2P забезпечує більш надійну модель роботи «мережа в мережі» [14]. Слід також згадати, що TOR пропонує можливість користувачу контролювати свою історію переміщень. Для деяких соціальних груп суспільства даний механізм несе, на противагу, досить вагоме позитивне значення: наприклад, інсайдери мають змогу повідомляти новини, які влада з певних причин воліє приховати для журналістів введенням цензури; правозахисники отримують широке поле для боротьби з репресивними діями своїх урядів; дисиденти можуть уникнути контролю авторитарних режимів.

Темна павутина також є найкращим каналом для обміну таємними документами. Анонімні повідомлення мають важливе місце в політичному та соціальному дискурсі. Багато людей бажають приховати свою особистість через побоювання щодо політичної чи економічної розправи.

Професор Австралійського національного університету Пітер Грабоскі (Peter Grabosky) зазначає [15], що віртуальна злочинність нічим не відрізняється від злочинності в реальному світі – вона просто відбувається в іншому, новому середовищі: «Віртуальна злочинність в основному така ж, як і реальна злочинність, з якою ми знайомі. Безумовно, деякі прояви є новими, але велика кількість злочинів, скоєних за допомогою комп'ютерів або проти них, відрізняється лише в площині сприйняття суспільством. Хоча технологія реалізації, а особливо її ефективність, може бути безпрецедентною, злочин [все одно] принципово знайомий. Мова йде не про що інше, як про звичайний злочин, вчинений докорінно неординарним методом».

1.2.3 Основні виклики Dark Web для Інтернету речей

Безпека в темній павутині має вирішальне значення для зміцнення впевненості та надійності використання інформаційних технологій (IT). Відсутність безпеки в кіберпросторі підриває довіру до інформаційного суспільства. Прикладом цього є достатня кількість інцидентів по всьому світу, що часто призводять до крадіжки грошей, активів та конфіденційної військової, комерційної та економічної інформації, а тому невпинно зростає потреба в захисті особистої інформації, фондів та активів і навіть національної безпеки. Як результат, сфера дії кібербезпеки набуває інтересу як з боку державного, так і приватного секторів. З появою комп'ютерних та IT-програм, кіберзлочинність стала значним викликом у всьому світі. Тисячі кіберзлочинців щодня намагаються атакувати комп'ютерні системи, щоб незаконно отримати до них доступ через Інтернет. Щомісяця випускаються сотні нових комп'ютерних вірусів та спам, які мають на меті пошкодити комп'ютерні системи, викрасти чи знищити їх дані. Реалізація таких загроз є дорогою не лише з точки зору кількості, але й з точки зору якості. В останні роки експерти дедалі більше турбуються про захист комп'ютерних та комунікаційних систем від зростаючої кількості кібератак, включаючи [10]:

- навмисні спроби несанкціонованого доступу до комп’ютерних систем з метою викрадення важливих даних;
- здійснення незаконних фінансових переказів;
- порушення цілісності і маніпулювання даними;
- виконання будь-яких інших незаконних дій.

З розвитком комп’ютерної безпеки зміцнення стійкості мережі посилюється. Відповідно до звіту Австралійського центру кібербезпеки (ACSC), культура суспільства пристосувалась до цього середовища, зосередившись на цілях з низьким ризиком та високою винагородою за їх досягнення, а також із акцентом на розробці методологій соціальної інженерії для здійснення нових атак. Крім цього, усюдисуща природа Інтернету дозволила зловмисникам отримувати більш деталізовані профілі користувачів мережі шляхом експлуатації та аналізу їх цифрових слідів, що призвело до вищих показників атак типу фішинг, крадіжок особистих даних та шахрайства, а також до розробки вузькоспеціалізованих інструментів шкідливого програмного забезпечення [10].

На жаль, через використання ресурсів Dark Web для недобросовісної діяльності, річний обіг незаконними та несанкціонованими предметами у глобальній торгівлі досягає понад декілька десятків трильйонів доларів. Економісти оцінили загальний розмір тіньової економіки чорного ринку для товарів і послуг сумою у 16.5 трильйонів доларів на рік, що складає понад 22% світового ВВП [16]. Торгівля на чорному ринку товарів оперує відмінно організованими логістичними ланцюжками, у тому числі зі залученням потужностей контрафактних та сірих ринків, асортимент яких може варіюватися від фірмової продукції великих компаній до життєво необхідних продуктів, таких як фармацевтичні препарати та імплантаційні медичні пристрої. Прибуток від торгівлі такими предметами часто сприяє подальшому розвитку організованої злочинності, а перебування у своєрідному ізольованому середовищі дозволяє товарам сумнівного походження вільно циркулювати по всьому світу.

Сектор IoT також не став виключенням. На просторах Dark Web торгівля краденими, неліцензійними, незаконно ввезеними та підпільно відремонтованими чи

перепрошитими «розумними» пристроями за цінами, нижче ринкових, є доволі поширеним явищем. Особливою популярністю користується апаратура для ведення прихованої зйомки та шпигунства, використання якої є забороненим у деяких країнах без відповідного дозволу.

Останнім часом більша частка монетизації припадає на замовлення кіберзлочину як послуги (crime-as-a-service). У якості доказу дослідники з TrendMicro у своєму звіті [17] наводять текст одного із численних оголошень, що було знайдене на одному із профільних хакерських форумів темної павутини: «Купуємо вразливості, виявлені вами в маршрутизаторах та пристроях IoT. Розглядаємо будь-які пропозиції до оплати, але остаточна сума залежатиме від кількості доступних у мережі пристроїв... Перевага буде надана RCE та іншим вразливостям, які дозволяють віддалено виконувати код на пристрої» (рис. 1.11).

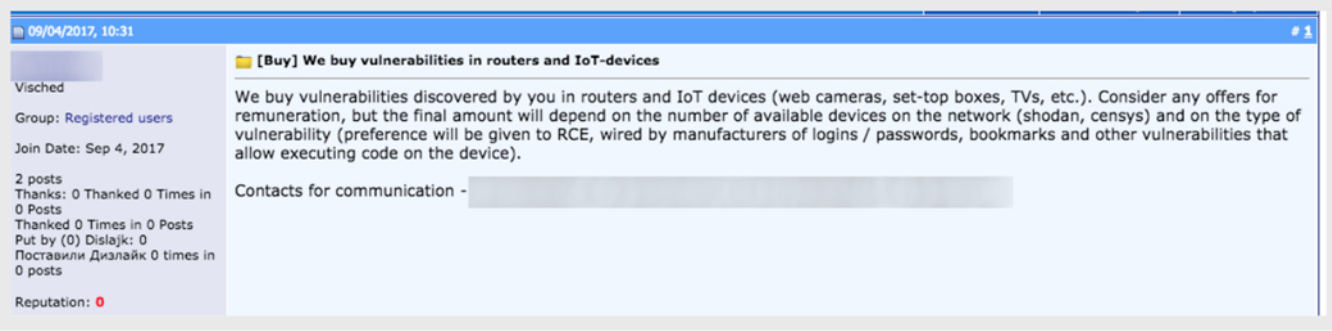

Рисунок 1.11 – Оголошення про купівлю знайдених вразливостей у роутерах

Крім того, ті ж самі дослідники навіть віднайшли пропозиції про продаж модифікованих газових лічильників для підробки показань у платіжках комунальних служб переважно серед країн СНД.

Тим не менше, відомий ботнет Mirai та його видозмінені варіанти все ще продовжують бути найбільш використовуваними серед зловмисників для атак на IoT-інфраструктуру. Не так давно були виявлені оновлені версії цього ботнету з більш розширеною функціональністю, а також відповідні навчальні посібники, які, поміж інших хакерських диверсій, містили детальний опис того, як цим шкідливим ПЗ користуватися (рис. 1.12).

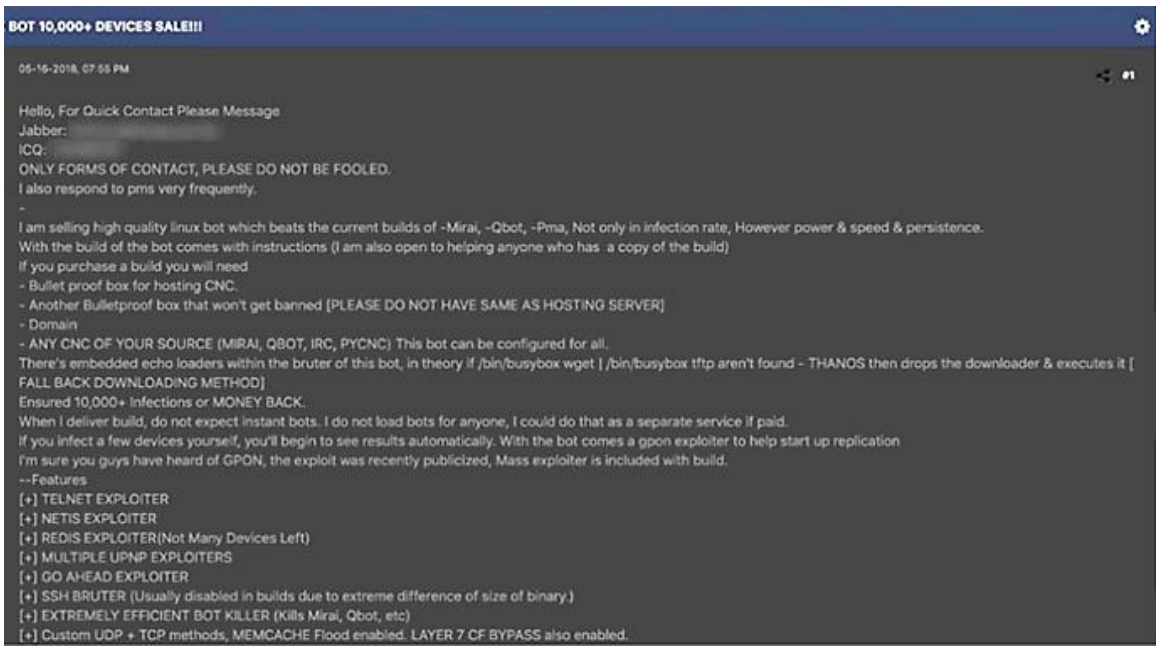

Рисунок 1.12 – Оголошення про продаж модифікованої версії ботнету Mirai на просторах Dark Web

Найчастіше організовані у розподілену ботнет-мережу «розумні» пристрої використовуються для здійснення DDoS-атак на інші ресурси або для проведення операцій криптомайнингу.

Отже, темна павутина має потенціал для розміщення дедалі більшої кількості шкідливих служб та заходів, кількість яких, на жаль, з плином часу тільки збільшується. Дослідники з питань безпеки повинні бути пильними і знаходити нові способи виявлення майбутніх шкідливих ресурсами, щоб якомога швидше боротися з новими загрозами в інформаційному просторі.

Висновки за розділом 1

За приблизними оцінками наукової спільноти, до 2025 року до Інтернету буде під’єднано понад 25 мільярдів IoT-пристроїв. Прискорене впровадження технологій 5G сприятиме зростанню IoT-екосистем, оскільки новий рівень передачі даних та бездротове підключення спонукатимуть все більше підприємств приєднатися до переваг використання IoT. Тому безпека IoT – це найбільш значима вимога на шляху до універсального застосування ресурсів IoT. На жаль, поки що не існує

єдиного рішення для захисту від усіх загроз безпеки IoT, здебільшого через величезну різноманітність архітектури самих пристроїв, систем та їх обчислювальних потужностей. Таким чином, єдиний спосіб успішного пом'якшення існуючих ризиків – це детальне вивчення кожного окремого випадку розгортання IoT-мережі та створення індивідуальної стратегії захисту для нього. Інтеграцію такого рішення слід планувати на самому початку створення відповідної IoT-інфраструктури, а його засоби повинні бути впроваджені у кожен вузол екосистеми протягом усього її життєвого циклу.

Переважна більшість користувачів не має достатньо часу чи знань для забезпечення захисту для всіх своїх пристроїв, а найчастіше розраховує на далекоглядність їх виробників в аспекті створення надійного захисту. Наразі експерти з питань інформаційної безпеки намагаються змінити русло дискусії у сторону того, що злам будь-якої кібернетичної системи відтепер лише питання часу, а не однієї можливості здійснення.

РОЗДІЛ 2
АНАЛІЗ МОЖЛИВОСТЕЙ SHODAN ДЛЯ ВИЯВЛЕННЯ УРАЗЛИВОСТЕЙ ПРИСТРОЇВ ІНТЕРНЕТУ РЕЧЕЙ

2.1 Безпека Інтернету речей проти пошукового агрегатора Shodan

2.1.1 Пошуковий агрегатор Shodan як інструмент OSINT-технологій

У майбутньому кожен пристрій буде зв’язаний з сотнями таких же інших, але чи замислювався хтось про наслідки подібного симбіозу для інформаційної безпеки? Статистика на сьогоднішній день свідчить про те, що ні. Ідея створення механізмів безпеки в IoT залишилась лише задумом, своєрідним додатковим доповненням замість того, щоб бути інтегрованою в дизайн з самого початку життєвого циклу усіх його продуктів.

Як результат, ми отримуємо мережу взаємопов’язаних незахищених пристроїв, які є загальнодоступними з просторів Інтернету. Тут буде як ніколи доцільним згадати про існування проекту, основною метою якого є автоматизація виявлення та подальша каталогізація таких пристроїв.

Shodan – це пошукова система, що у деякому розумінні схожа до Google, проте на цьому уся її подібність закінчується. Замість того, щоб індексувати веб-вміст через порти 80 (HTTP) або 443 (HTTPS), як це робить Google, Shodan сканує в Інтернеті пристрої, що реагують на безліч інших портів, включаючи і ті, що використовуються протоколами FTP (21), SSH (22), Telnet (23), SMTP (25), HTTP (80), SSL (443), RDP (3389), SIP, VNC (5900) та інші. Як тільки Shodan виявляє хост, який відповів на запит через певний порт, він підключається до нього і отримує всю доступну сервісну інформацію про код стану системи, версію ПЗ, яку вона використовує, обслуговуючі сервіси, тип під’єднаного до мережі пристрою і навіть його користувачів [1]. Потім ця інформація індексується разом із даними про

геолокацію цілі. Результати пошуку найчастіше включають веб-камери, медичні пристрої, смарт-хаби і т.д.

Рисунок 2.1 – Результати пошуку за заданим фільтром у Shodan

На сьогодні Shodan встиг отримати почесне звання «найнебезпечнішої пошукової системи у світі» [18], що є доволі сміливою заявою, однак чи може дійсно такий простий, на перший погляд, інструмент нести у собі стільки шкоди? Shodan існує вже трохи більше десяти років, проте потенціал усіх спричинених ним загроз все ще потребує ретельного дослідження. Так у чому ж полягає реальна небезпека?

«Коли люди не бачать потрібних їм речей за допомогою Google, вони вважають, що ніхто не в змозі цього знайти. Це зовсім не так», – зазначає Джон Метерлі (John Matherly), розробник Shodan [18]. Shodan нівелює поширений у колах деяких фахівців принцип «безпеки через неясність» (security through obscurity), за яким будь-яка система, що має суттєві чи потенційні вразливості, вважається надійною, якщо недоліки її конструкції залишаються невідомими для зловмисників. Тому якщо хтось думає, що його IoT-пристрої знаходяться у безпеці тільки через те, що вони не є класичними одиницями Інтернету, на кшталт веб-сайтів, то Shodan швидко руйнує таку ілюзію [19].

Shodan використовує автоматизовані інструменти пошуку, які дозволяють одночасно обробляти масивні запити. Одним із таких інструментів є Shodan Diggity, в основі якого лежить Shodan Hacking Database – база даних, що виступає у якості

своєрідного словника для виявлення різних типів пристроїв, під'єднаних до мережі [18]. Використовуючи інструменти сканування, подібні до NMAP, пошукові «павуки» серверів Shodan обходять та опитують значну частину адресного простору IPv4, в основному намагаючись віднайти кожен пристрій, підключений до Інтернету, і отримати його «цифровий відбиток». Сканери Shodan визначають, які мережеві сервіси використовує кожен знайдений пристрій, а також збирають усі дані з банерів, через які можна ідентифікувати встановлені програмне та апаратне забезпечення. Потім Shodan зручно зберігає всю цю інформацію у згаданій базі даних, що дозволяє користувачам знаходити будь-які пристрої в Інтернеті, які містять дане програмне забезпечення чи обладнання [20].

З моменту запуску в 2009 році Shodan виявив та проіндексував досить широкий спектр підключених до Інтернету пристроїв, включаючи веб-камери, обладнання сигналізації дорожнього руху, маршрутизатори, брандмауери, системи відеоспостереження, промислові системи управління атомними електростанціями та електричними мережами, побутову техніку і т.д. Ці пристрої були підключені до Інтернету часто навіть без застосування базових засобів захисту, тому доступ до них можна легко отримати, ввівши ім'я користувача та пароль за замовчуванням. На рисунку нижче видно, як швидкий пошук в Shodan зі застосуванням простого фільтру «password default» може виявити тисячі серверів, принтерів, систем управління «розумними» пристроями, які використовують фрази «admin» та «1234» у якості логіну та паролю відповідно [18] (рис.2.2). Схожим ефектом також володіє запит «publicly-known credentials» – нагадування про необхідність зміни стандартного паролю.

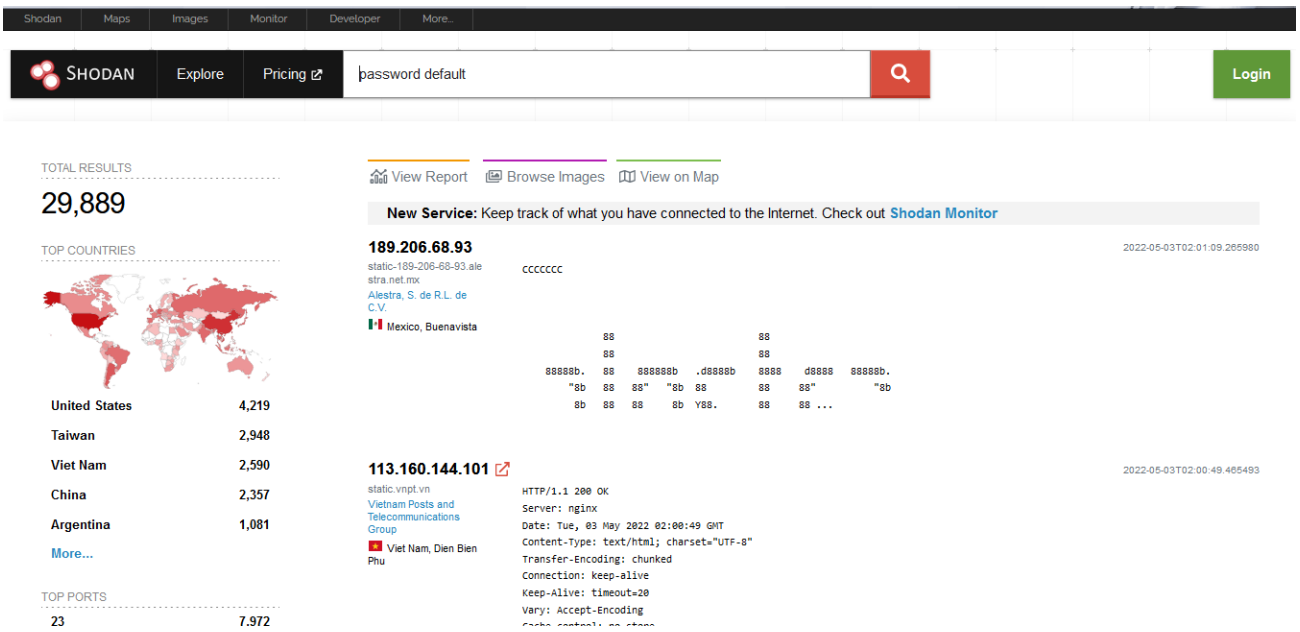

Рисунок 2.2 – Кількість доступних у мережі пристроїв, що використовують логіни/паролі за замовчуванням

Як приклад, звичайна IP-камера може не мати встановленого унікального паролю до своєї панелі керування, оскільки середньостатистичний користувач не надто переймається його зміною після придбання пристрою. Враховуючи те, що Shodan працює протягом 24 годин, 7 днів на тиждень і щомісяця збирає інформацію близько про 500 мільйонів підключених до мережі пристроїв та сервісів, подібна необачність може послужити відмінною відправною точкою для розгортання недоброзичливцями чергової хакерської атаки [18]. Більше того, у деяких випадках системи можуть й зовсім не вимагати ніякої авторизації – достатньо лише мати браузер, щоб під'єднатися до них.

Варто відмітити, що достатня частка знайдених пристроїв все ж таки має певний захист – зазвичай такий, що вимагає автентифікації, але навіть це не дає 100-відсоткової гарантії захищеності від несанкціонованого доступу. У світі кібербезпеки ніщо не залишається статичним, тому список існуючих уразливостей поповнюється новими загрозами кожен день.

Вагомим прикладом для підтвердження вище висловленої думки може стати діяльність однієї з найбільш відомих компаній у галузі комп'ютерних мереж Juniper [1]. У результатах свого недавнього публічного дослідження Juniper показала, що

прошивка, яка працює на деяких їх пристроях, містить жорстко закодований пароль, який дозволить кожному, хто підключається до вразливого пристрою, просто поставити цей пароль у парі до дійсного облікового запису користувача, щоб отримати повний адміністративний доступ до жертви через Telnet або SSH.

Як результат, використовуючи можливості Shodan, ми можемо переглядати список брандмауерів Juniper у пошуку тих, на яких запущена вразлива версія прошивки ScreenOS. Після підключення до панелі управління ми надаємо раніше відомий пароль «<<< %s(un='%s') = %u» для типового облікового запису користувача ScreenOS «system» і отримуємо змогу розпочати віддалене управління пристроями, що містять дану вразливість. Якщо припустити, що лише 10% із проіндексованих 18 000 брандмауерів є вразливими (що є надзвичайно консервативною оцінкою), то це 1800 вразливих одиниць програмного забезпечення Juniper, яке наразі перебуває в мережі Інтернет [1].

На жаль, сьогодні до Інтернету підключені набагато вразливіші речі, аніж звичайна інфраструктура «розумного» будинку. Мова йде про системи управління електростанціями, світлофори, лабораторне обладнання, конвеєрні лінії та інше.

Наведемо ще один показовий випадок. Під час доповіді на одній із конференцій Defcon незалежний тестувальник з ІБ Ден Тентлер (Dan Tentler) продемонстрував, як за допомогою Shodan можливо віднайти панель управління до системи охолодження, водонагрівача та автоматизованих гаражних воріт «розумного» будинку, а згодом і навіть до французької гідроелектростанції. Додатково була виявлені автомийка із можливістю віддаленого керування та хокейний каток у Данії, розморозити який цілком реально одним натисненням кнопки. Крім того, у ході свого експерименту Тантлер спромігся отримати доступ до системи управління дорожнім трафіком цілого міста та показати подальшу перспективу її переведення у тестовий режим шляхом виконання єдиного запиту у командному рядку [18].

Поясненням високого ступеню вразливості виявлених цілей саме серед громадського сектору є те, шо зазвичай Shodan відслідковує пристрої з відкритим доступом переважно поміж систем SCADA (Supervisory Control and Data

Acquisition). SCADA-системи використовуються для віддаленого моніторингу за виробничими процесами у режимі реального часу [1] (рис. 2.3).

Рисунок 2.3 – Веб-панель управління системою крематорію, доступ до якої був за допомогою інструментів Shodan

Однак чому така кількість IoT-пристроїв не має належного захисту? Головна причина полягає у тому, що більшість із цих пристроїв не мали мати зв’язку з Інтернетом взагалі. Уявімо, що якась організація придбала систему контролю над термостатами, якою мусить управляти комп’ютер. Найімовірніше, у який спосіб IT-відділ спробує залучити цей комп’ютер до системи нагріву? Замість прямого підключення, його співробітники вирішують поєднати обидві системи через окремий веб-сервер із відкритим портом, що зробить останній доступним для решти світу. І звісно ж, будь-які механізми захисту будуть відсутні. Як висновок, концептуально ані термостати, ані система обігріву не повинні були мати виходу в Інтернет, що б повністю нейтралізувало ефективність дії Shodan проти них.

Більше того, будь-хто, хто створює подібну до Shodan пошукову систему, на відміну від Метерлі, зовсім не зобов’язаний робити дане досягнення публічно відкритим [19]. Цілком можливо, що подібні проекти вже давно існували на просторах Dark Web та користуються не меншою популярністю, аніж їх всесвітньо відомий аналог. Цікаво, що там же пропонуються до придбання преміум-аккаунти Shodan [17] (рис. 2.4):

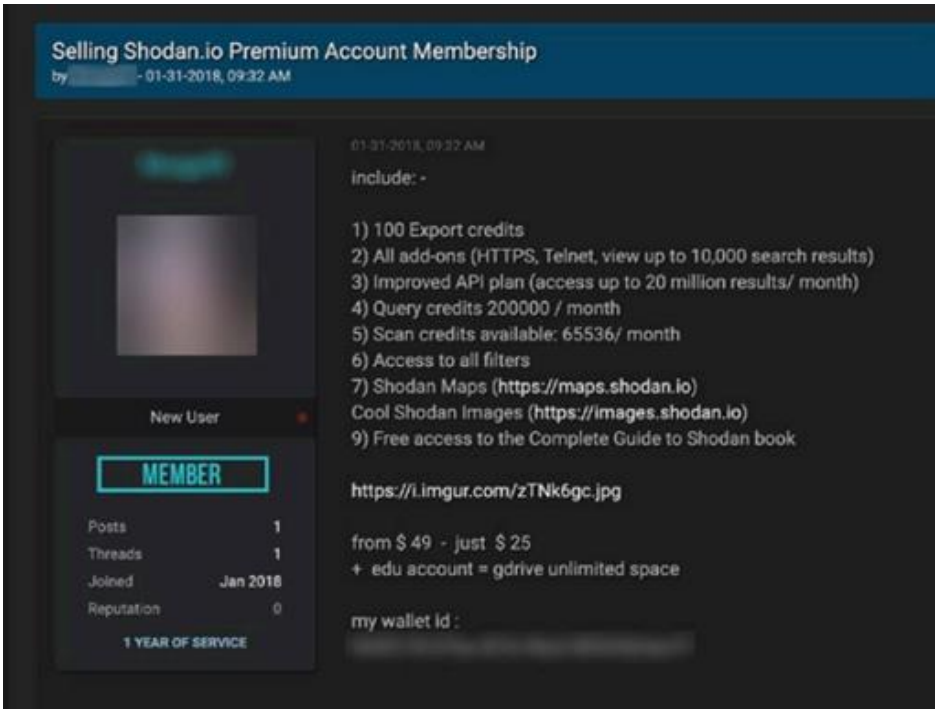

Рисунок 2.4 – Пропозиція щодо придбання преміум-аккаунту Shodan на профільному форумі у Dark Web

На жаль, Shodan все ще залишається привабливим для кіберзлочинців, у тому числі за рахунок своєї можливості виявляти раніше згадані SCADA-системи. Як наслідок, національна безпека багатьох країн може бути компрометована, оскільки атаки на відповідну інфраструктуру уже потенційно стануть можливими [1]. Попри все, варто зазначити, що якби стандарти в галузі безпеки IoT мали б належну реалізацію, то такий інструмент, як Shodan, став би непотрібним.

З іншої сторони, розробник Shodan сприяє активному використанню своєї пошукової системи серед середніх та великих компаній. Наприклад, Shodan може допомогти провести емпіричний аналіз певного сегменту ринку шляхом надання інформації про ті мережеві пристрої, якими люди найбільше користуються. Shodan також стане у нагоді при моніторингу комп’ютерів внутрішньої мережі, що мають доступ до Інтернету [21].

Останнім часом Shodan значно поповнив колекцію власних фільтрів, тому їх можливо використовувати для деяких нетривіальних завдань. Окрім традиційного пошуку вразливих систем, це може бути аналіз поширеності веб-інструментів (у всьому світі та по регіонам), дослідження популярності мережевих пристроїв різних

компаній, оціночна частка стандартних рішень для управління мережевими ресурсами та інший порівняльний аналіз на основі фактичного стану мережі. Замість збору статистики звичайними способами, тепер можна просто опитати декілька мільярдів реальних пристроїв через Shodan [21].

2.1.2 Дослідження синтаксису пошукових запитів у Shodan

За замовчуванням Shodan використовує введене користувачем слово у якості точного виразу для пошуку. Як і в Google, пошукова фраза може бути уточнена спеціальними операторами для того, щоб звузити область пошуку на основі метаданих у відбитках зібраних пристроїв. Однак у Shodan ці слова-оператори свої – це фільтри. Як правило, ймовірність знайти щось цікаве за допомогою Shodan прямо пропорційна якості пошукової фрази. Списки поширених паролів, звіти відомих компаній, що спеціалізуються на пошуку вразливостей – найкращі джерела збору інформації для створення ефективних запитів у Shodan. Таким чином, запорука успішного пошуку – правильно підібрані ключові слова та фільтри, які вкупі утворюватимуть влучну пошукову фразу [22].

Розглянемо деякі з найпоширеніших пошукових фільтрів Shodan:

- country: назва країни у буквенному коді, наприклад: nginx country:US;
- city: назва міста, наприклад: nginx city:"New York" country:US;
- os: версія операційної системи, наприклад: microsoft-iis os:"windows 2003";
- port: порт у форматі цілого числа, наприклад: proftpd port:21;
- hostname: назва домену, наприклад: nginx hostname:.us;
- net: пошук за IP-адресою, наприклад, 1.1.1.1;
- before/after: пошук до/після вказаної дати у форматі день/місяць/рік, наприклад: before:11/10/2022.
- назва вендора, наприклад: org:"Juniper";
- назва конкретного типу пристрою або служби, наприклад: product:"NetScreen".

Більш-менш повний перелік налічує близько 60 задокументованих фільтрів [23]. Щоб вміти вдало їх застосовувати, необхідно згадати про тлумачення основних кодів відповідей HTTP [22]:

- 200 OK Request succeeded;
- 301 Moved Permanently Assigned a new permanent URI;
- 302 Found Resides under a different URI;
- 303 See Other;
- 401 Unauthorized Request requires authentication;
- 403 Forbidden Request is denied regardless of authentication;
- 404 Not Fouund;
- 405 Method not Allowed.

Дані про кожний пристрій зберігаються в структурі, яку розробники називають банером. Під банером мається на увазі відповідь, яку надав пристрій при зверненні пошукового «павука» Shodan до нього [24]. Ось як вона виглядає (рис. 2.5):


```
{
    "data": "Moxa Nport Device
            Status: Authentication disabled
            Name: NP5232I_4728
            MAC: 00:90:e8:47:10:2d",
    "ip_str": "46.252.132.235",
    "port": 4800,
    "org": "Starhub Mobile",
    "location": {
        "country_code": "SG"
    }
}
```


Рисунок 2.5 – Приклад структури банера у Shodan

Залежно від кількості отриманої інформації, банер може містити набагато більше значень, за допомогою яких можна проводити фільтрацію. За замовчуванням пошук проводиться лише в полі data, що частково пов'язано з міркуваннями безпеки. Вміст data може сильно відрізнятися в різних банерах. Типовий сценарій пошуку передбачає, що користувач спочатку формує загальний запит до поля data, після чого додає необхідні назви фільтрів. Тоді Shodan проводить вибірку усіх пристроїв,

в яких поле data містить вказаний запит, а потім звужує область результатів з урахуванням відповідних фільтрів [24].

Насамперед розглянемо типовий банер «401 Unauthorized Request» пристрою Cisco, якщо ми введемо у пошук єдине слово «cisco». (рис):

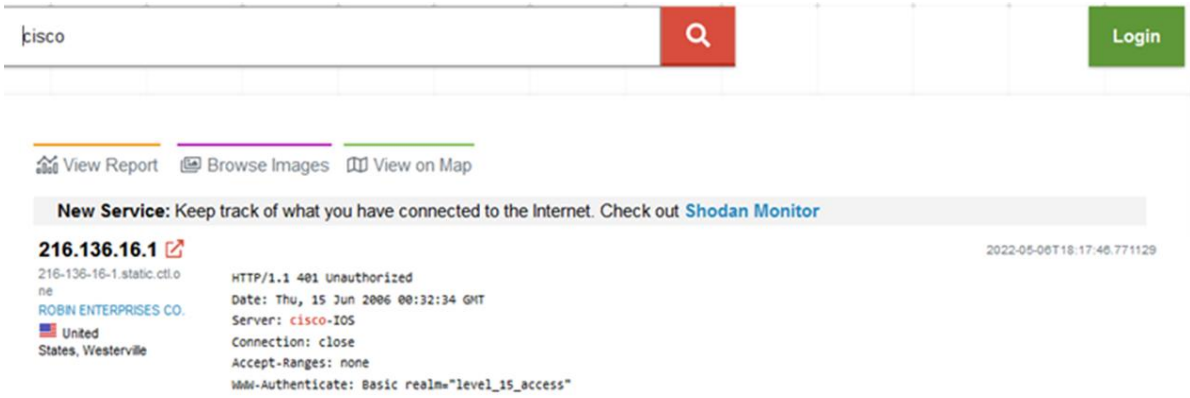

Рисунок 2.6 – Типовий банер «401 Unauthorized Request» пристрою Cisco

Для Shodan не важливо, як відповість той чи інший мережевий вузол. Ця пошукова система лише протоколює зібрані відповіді та зберігає їх у своїй базі, доступ до якої надається всім охочим: ознайомчий – безкоштовно, а деталізація різних рівнів – за гроші. Варто відмітити, що рядок WWW-Authenticate: Basic realm="level_15_access" вказує на необхідність введення логіну та паролю. У свою чергу, за запитом «200 cisco» пристрій, який у більшості випадків не вимагає явної авторизації, поверне банер зі статусом ОК [22]. Додатковою ознакою відсутності будь-якого захисту є вираз «Last-Modified» (рис. 2.7):

Рисунок 2.7 – Вираз «Last-Modified» як ознака пристрою, який не потребує аутентифікації

Достатньо перейти за посиланням виду «IP-адреса:80», аби потрапити на сторінку веб-консолі управління обраним пристроєм.

Оскільки Shodan не має детальної довідки та надто дружнього інтерфейсу, спочатку багато хто просто не розуміє, з чого розпочати пошук. Як правило, новачки переглядають чужі (і часто вже застарілі) запити, при цьому погано уявляючи практичну вигоду від пошуку по ним. Знайти бажане за допомогою Shodan можливо лише тоді, коли відомі хоча б якісь деталі на тему шуканого об’єкта. Для цього не буде зайвим ознайомитися з думками відповідних експертів та самого Метерлі, який доволі часто ділиться цікавими знахідками на форумах та в соціальних мережах [21]. Наприклад, вітряні генератори фірми Nordex визначаються за ідентифікаційним рядком «jetty 2000», а багато мережевих сховищ – за відповіддю «220 NASFTPD Turbo station».

Наведемо іще приклади деяких пошукових запитів, результати яких варті окремої уваги [24]:

- Мобільні пристрої, перетворені на камери спостереження під управлінням Android Webcam Server найпершої версії – «Android Webcam Server v0.1.200». Також можна зробити пряму вказівку на відсутність аутентифікації за допомогою «-Authenticate».
- FTP-сервери з можливістю анонімного доступу – «230 Anonymous access granted».
- Мережеві сховища (NAS) Lenovo/EMC з паролем за замовчуванням – «Set-Cookie: iomega=», де iomega – колишня назва підрозділу виробника. На більшості знайдених пристроїв буде встановлений стандартний логін/пароль (admin/admin), як це було на еталонній моделі ix4 300d.
- Бездротові камери з веб-інтерфейсом – «WIRELESS INTERNET CAMERA».
- Камери відеоспостереження Sony Professional Solutions за назвою моделі – «SNC-DH160». У 2016 році відбувся гучний скандал у зв'язку з виявленням бекдору у десятках моделей камер цього виробника.
- HID-контролери VertX, що належать Spectrum Business – «door controller org:"Spectrum Business" port:4070».
- Поточний статус акумулятора Tesla PowerPack – «http.title:"Tesla PowerPack System" http.component:"d3" -ga3ca4f2».

- Рентген-апарати DICOM – «"DICOM Server Response" port:104».
- Принтери Xerox – «ssl:"Xerox Generic Root"».
- Панелі управління вмістом рекламних білбордів Samsung – «Server: Prismview Player» (рис. 2.8):

Рисунок 2.8 – Сервер управління білбордом Samsung

Наведений вище перелік далеко не є вичерпним та, за матеріалами автора Jake Jarvis з репозиторія GitHub [25], може налічувати сотні інших фраз для пошуку вразливих пристроїв. Якщо за певним запитом було знайдено занадто мало пристроїв, можна спробувати повторити пошук через деякий час. Shodan шукає не лише у своїй базі даних, але й водночас сканує Інтернет у режимі реального часу, тому іноді перелік результатів зростає на очах приблизно у 10-20 нових одиниць за хвилину.

Shodan – не єдина у своєму роді пошукова система для дослідження секретів Інтернету речей, також існує немало подібних їй аналогів. Наприклад, це можуть бути Thingful, IoT Crawler та інший не менш небезпечний наступник Shodan – Censys [26].

2.1.3 Відповідальність та основні ризики при використанні Shodan

Питання про законність використання Shodan є досить суперечливим і дотепер. Зазвичай у цьому випадку користувацька спільнота керується принципом «все, що не заборонено, дозволено». Відсутність явної міжнародної або національної заборони у вигляді будь-яких нормативних документів на подібні пошукові системи дуже просто пояснити їх корисністю: більшість користувачів Shodan часто є працівниками правоохоронних органів або фахівцями з ІБ, що займаються тестуванням та моніторингом вразливих місць у мережах [27].

Тим не менше, кожен раз, звертаючись до послуг Shodan, цілком можливо ненавмисно (або ж навмисно) порушити закон. Shodan дуже витончено розмиває кордони між дозволеним та забороненим, дозволяючи з легкістю знайти як ресурси, що спрямовано були створені для загального використання, так і «двері», які випадково залишили «незамкнутими» В останньому випадку доступ до такої інформації може бути виявитися неправомірним відповідно до законів країни, де фізично розташований піддослідний пристрій, тому варто завжди об’єктивно оцінити наслідки перш, ніж діяти [20].

Очевидно, що можливостями Shodan також користувалися багато зловмисників, а тепер вони полюють на необачних новачків платформи через розміщення так званих «медових приманок» (honeypot) у пошуковій видачі [20].

Першочергово основна задача honeypot – навмисно піддатися атаці або будь-якому іншому несанкціонованому дослідженню, що в подальшому дозволить вивчити стратегію атакуючої особи та визначити перелік засобів, за допомогою якого можуть бути вражені реальні об'єкти мережі. Honeypot може бути реалізований у вигляді як спеціального сервера, так і окремого мережевого сервісу, завданням якого є привернення уваги хакерів.

Honeypot – це ресурс, який сам по собі нічого не робить без наявності будь-якого зовнішнього впливу, а лише збирає невелику кількість інформації, після аналізу якої будується статистика застосованих нападниками методів і визначається можливість створення будь-яких нових рішень для боротьби проти досліджених

видів атак. Наприклад, деякий безіменний невідомий веб-сервер не повинен мати ніяких відвідувачів, тому всі особи, які намагаються отримати доступ до його ресурсів, вважатимуться потенційними хакерами. У свою чергу, honeypot збирає інформацію про особливості поведінки цих осіб та їх методи впливу на «ціль». Після цього експерти в галузі інформаційної безпеки розробляють стратегії реагування на атаки зловмисників.

Shodan також не став винятком. Результати його пошуку теж сповнені пристроями-«медовими пастками» (рис. 2.9), частими жертвами яких стають, усупереч початковій ідеї, звичайні недосвідчені користувачі. Наприклад, якщо файли на знайденому сервері заражені трояном, то комп'ютер самого відвідувача при спробі отримати доступ до нібито вразливого ресурсу з результатів пошуку може бути миттєво атакований через експлойт. Тому не варто забувати про заходи безпеки. Не слід відкривати зовнішні посилання з пошукової видачі Shodan на основному комп'ютері, а краще це зробити в окремому екземплярі віртуальної машини, яку можна знищити у будь-який момент. Використання проксі-серверів, VPN-сервісів та фаєрволів також буде дуже доречним рішенням [20].

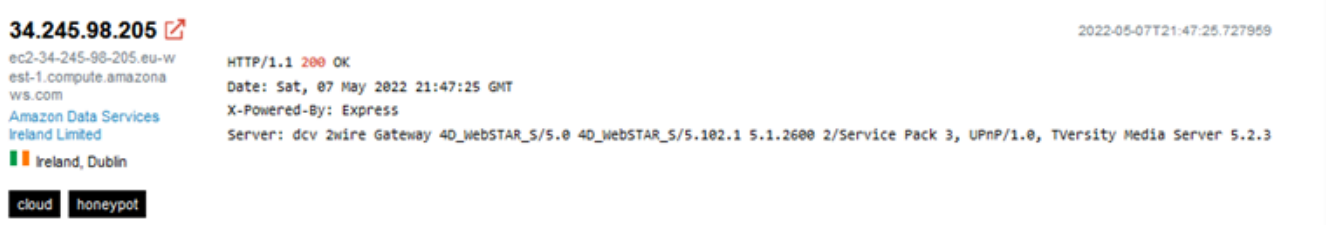

Рисунок 2.9 – Honeypot у пошуковій видачі Shodan

Повертаючись до аспектів роботи в Shodan, спробуємо сформувати загальні принципи законності/незаконності його використання на основі існуючих нормативно-правових актів. Основним міжнародним актом, що регулює функціонування подібних пошукових систем, є Конвенція про кіберзлочинність (Будапештська конвенція) [28]: саме вона ще в 2001 році виокремила основні ознаки того, яка діяльність в Інтернеті є юридично легальною, а яка – ні. Описаними в ній положеннями керуються як держави-члени Ради Європи, так й ряд інших країн-підписантів, у тому числі й Україна. Сполучені Штати Америки ж характеризуються

іншим юридичним апаратом з даного питання, в якому частина ознак неправомірного доступу описана у Федеральному Законі про боротьбу з комп’ютерним шахрайством 1984 року (The Computer Fraud and Abuse Act), а інша ж – в кримінальних кодексах чи законах окремих штатів, наприклад, Закон про комп'ютерні злочини Вірджинії (The Virginia Computer Crimes Act).

За вище згаданими нормативними документами загальні критерії незаконності віддаленого доступу до цифрових пристроїв включають наступне [27]:

- несанкціонований доступ (НСД);
- умисел;
- суспільна небезпека.

Щоб змістовно відповісти на всі подальші питання щодо законності конкретних дій в Shodan, розглянемо кожен з цих пунктів окремо.

Несанкціонований доступ у даному контексті передбачає таку спробу отримання доступу до пристрою, за якої з усіх обставин очевидно, що законний власник не бажає здійснення подібного посягання на свою власність Серед цих обставин може бути не лише наявність засобів захисту, як логін та пароль, але й суто функціональне призначення пристрою.

Якщо ж пристрій обробляє будь-яку інформацію з обмеженим доступом навіть за повної відсутності засобів захисту, то НСД до нього все одно автоматично стає порушенням. Наприклад, несанкціонований доступ до відеокамери в приватному будинку веде до порушення права на особисте життя та його таємницю, до турбінної гідроелектростанції – щонайменше до порушення режиму транспортної безпеки і т.д.

Важливо зазначити, що використання на пристрої слабких чи заводських логінів/паролів за замовчуванням не можна застосувати у якості виправдання, оскільки їх основна функція зі сторони закону – це окреслення наявності забороненої зони для входу. У цьому аспекті навіть невдала спроба отримання НСД тягне за собою покарання, еквівалентне вчиненню замаху.

Більшість країн єдині у розумінні, що якщо будь-якій людині спало на думку отримати несанкціонований доступ до певного пристрою в Інтернеті, то причина,

безумовно, злочинна. І це головна проблема для експертів з безпеки: вони повинні або надати докази того, що власник або виробник пристрою дозволив їм перевірити безпеку таким неординарним чином, або ж довести, що вони є працівниками відповідних наукових установ чи міжнародних організацій, що спеціалізуються на сфері захисту інформації.

Виняток в описаній суворості правового поля становить саме неоднозначність поняття суспільної небезпеки. Наприклад, якщо зловмисник отримав доступ до функцій керування міським світлофором, то це становить небезпеку для суспільства, оскільки одним натисненням кнопки можна з легкістю спровокувати аварію, пробки та інші негативні наслідки. А якщо мова йде про забутий у квартирі після переїзду смарт-годинник? Навряд чи.

Таким чином, визначимо відповіді на наступні питання [27]:

1. Чи є використання Shodan законним? Саме по собі використання пошукової системи є абсолютно законним, оскільки вона лише відображає інформацію, яка знаходиться в Інтернеті в публічному доступі.

2. Чи є законним підключення до віддаленого пристрою, вхід до якого не захищено логіном та паролем? Ні, якщо цей пристрій має суспільне значення (транспорт, телекомунікаційна інфраструктура тощо), відноситься до приватної сфери особистого життя або належить державі. Іншими словами, якщо несанкціоноване управління пристроєм може заподіяти шкоду окремій особі чи суспільству, то це незаконно.

3. Чи є законним підключення до віддаленого пристрою, де у якості засобів захисту використовуються логіни/паролі за замовчуванням? Ні, оскільки такий логін/пароль відіграє не фізичну, а юридичну роль у вигляді попередження про небажаність доступу.

4. Чи є законним підбір паролів для підключення до віддаленого пристрою, знайденого за допомогою Shodan? Підбір вважається незаконним у всіх вище описаних випадках та буде розцінюватися як спроба отримання НСД.

5. Чи є законним підключення до віддаленого пристрою з метою подальшого проведення його дослідження чи аудиту інформаційної безпеки? Законно за умови наявності доказів про дозвіл на здійснення подібної діяльності.

Дискусія з приводу сформованих вище відповідей у наукових колах залишається активною і на даний момент.

2.2 Отримання несанкціонованого доступу до цільового пристрою за допомогою Shodan

Щоб наочно продемонструвати можливості Shodan, проведемо невеликий експеримент. На думку автора роботи, у якості об’єкту буде показовим обрати не надто важливий елемент міської інфраструктури, наприклад, широкоформатний LED-екран, на якому зазвичай відображається реклама. Ніякої шкоди обраному об’єкту завдано не буде.

Оскільки пошук за раніше згаданою фразою «Server: Prismview Player» уже досить жваво обговорюється на всіх профільних форумах завдяки надзвичайній легкості отримання доступу до знайдених пристроїв, його результати більше не становлять вагомого інтересу. Тому переглянемо за допомогою звичайного запиту «LED billboard system» у Google найпоширеніше програмне забезпечення вуличних цифрових моніторів та, як результат, дізнаємося про наявність уразливої систем управління вмістом Lednet.

Використовуючи незадокументований фільтр Shodan «title», спробуємо знайти усі пристрої з уразливою прошивкою. Цікаво, що їх залишилось зовсім небагато, що свідчить про високий рівень обізнаності адміністраторів білбордів щодо недоліків використання саме цієї системи.

З міркувань безпеки усі дії виконуються на окремій віртуальній машині з використанням VPN-сервісу. За сформованим запитом «title:"lednet"» знайдено 10 результатів (рис. 2.10):

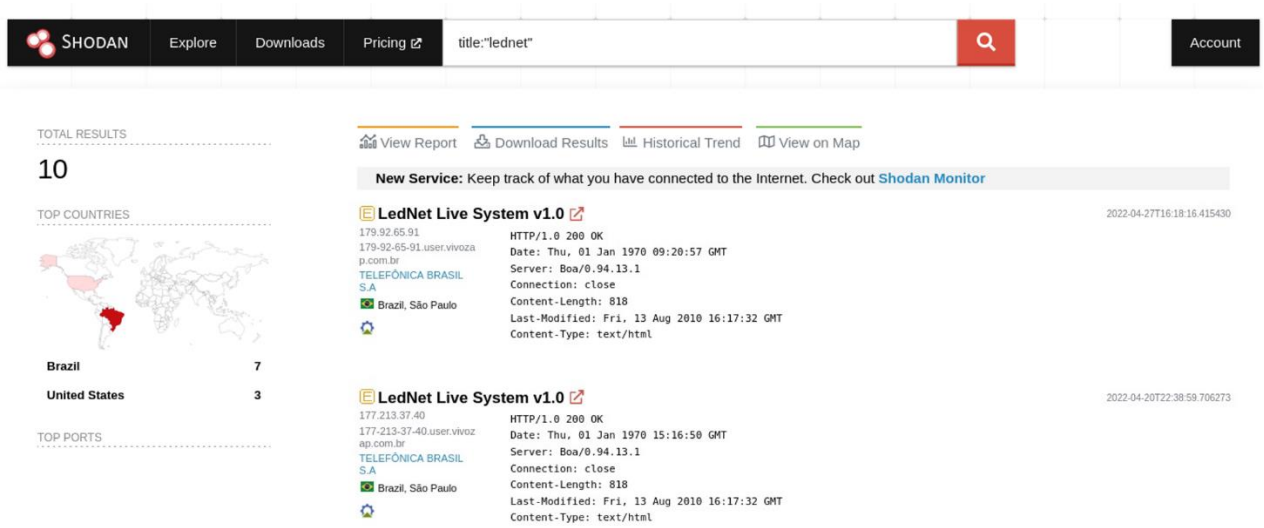

Рисунок 2.10 – Результати пошуку вразливої категорії білбордів

Тим не менше, банер з відповіддю 200 OK не завжди означає відсутність потреби у введенні логіну/паролю. Форма авторизації може бути реалізована через вбудовані засоби у програмному забезпеченні цільового пристрою та з’явитись тільки під час переходу по відповідному зовнішньому посиланню з пошукової видачі Shodan уже після завершення завантаження вмісту веб-сторінки. Найчастіше ж відповідь «401 Unauthorized» означає потребу у негайній авторизації через окреме вікно браузера (рис. 2.11):

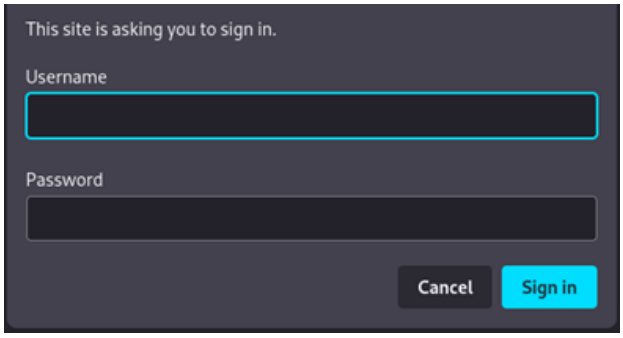

Рисунок 2.11 – Вікно авторизації при переході на сторінку пристрою з банером «401 Unauthorized»

Найперша версія прошивки Lednet вразлива до виконання простої SQL-ін’єкції [29], тому обираємо відповідний результат «LedNet Live System v1.0» з пошуку Shodan, переходимо за зовнішнім посиланням та бачимо типову веб-форму для входу, створену на php (рис. 2.12):

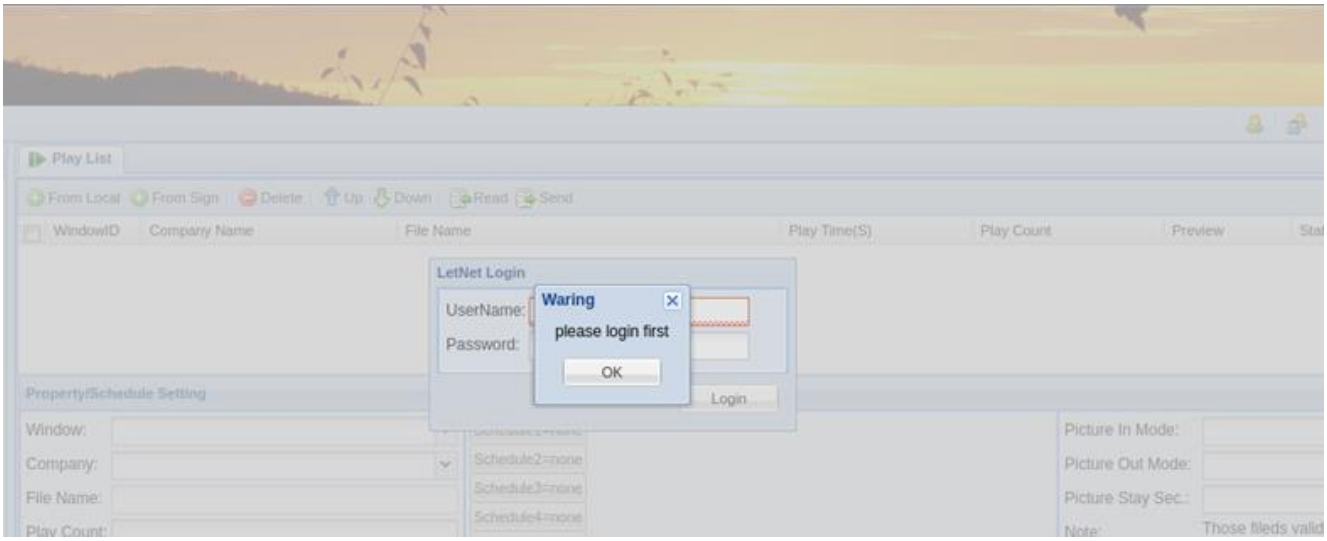

Рисунок 2.12 – Панель управління вмістом вразливого білборда

У нашому випадку вразливість прошивки виявляється шляхом введення користувачем некоректних параметрів (рис. 2.13) у якості логіну («-1558" OR 9005=9005 AND "UxGI"="UxGI») та паролю («0»), після обробки яких базою даних повертається невластива для веб-форми відповідь на запит авторизації.

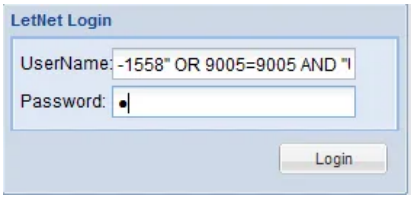

Рисунок 2.13 – Введення користувачем некоректних параметрів для входу

Як результат, після успішного входу ми отримали доступ до управління усіма функціями цільового пристрою (рис. 2.14):

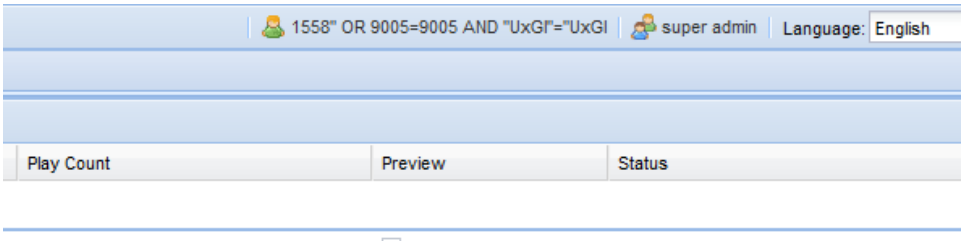

Рисунок 2.14 – Успішна авторизація в панелі управління

Варто зазначити, що на сьогодні описаний вище метод для отримання НСД уже є рідкістю, але даний приклад дуже лаконічно відображає проблему того, як

через відсутність оновлень програмного забезпечення можна провести доволі нескладну, але успішну атаку на вразливі пристрої IoT.

Таким чином, сформуємо загальний алгоритм проведення типової кібератаки з використання Shodan:

1. Визначення типу цільового пристрою.
2. Збір інформації про особливості функціонування апаратного та програмного забезпечення, а саме пошук назв встановлених сервісів та їх конкретних вразливостей, документації від виробника та інших даних, що однозначно характеризують жертву.
3. Формування ефективної пошукової фрази у Shodan.
4. Фільтрація отриманих результатів.
5. Використання експлойту до попередньо знайденої вразливості пристрою чи іншого заздалегідь визначеного методу (вкрай до перебору паролів) для отримання НСД.

Розглянемо більш реалістичний випадок із застосуванням створеного алгоритму. До прикладу, необхідно знайти усі FTP-сервери в певній країні, програмне забезпечення яких містить вразливість до віддаленого виконання коду (RCE). За міркуваннями автора роботи, найпоширенішою службою, яка керує роботою таких серверів, є демон vsFTPd (Very Secure FTP Daemon). За допомогою звичайного запиту «vsftpd vulnerability» у Google дізнаємося про наявність бекдору у версії 2.3.4 vsFTPd (рис. 2.15):

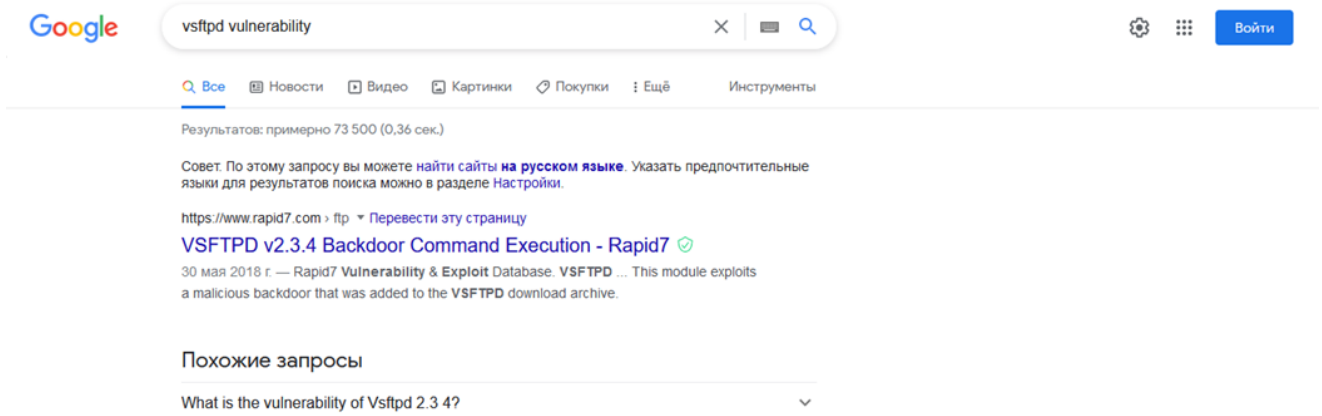

Рисунок 2.15 – Результати пошуку вразливої версії служби FTP-сервера у Google

На основі цього формуємо пошукову фразу для Shodan (рис. 2.16):

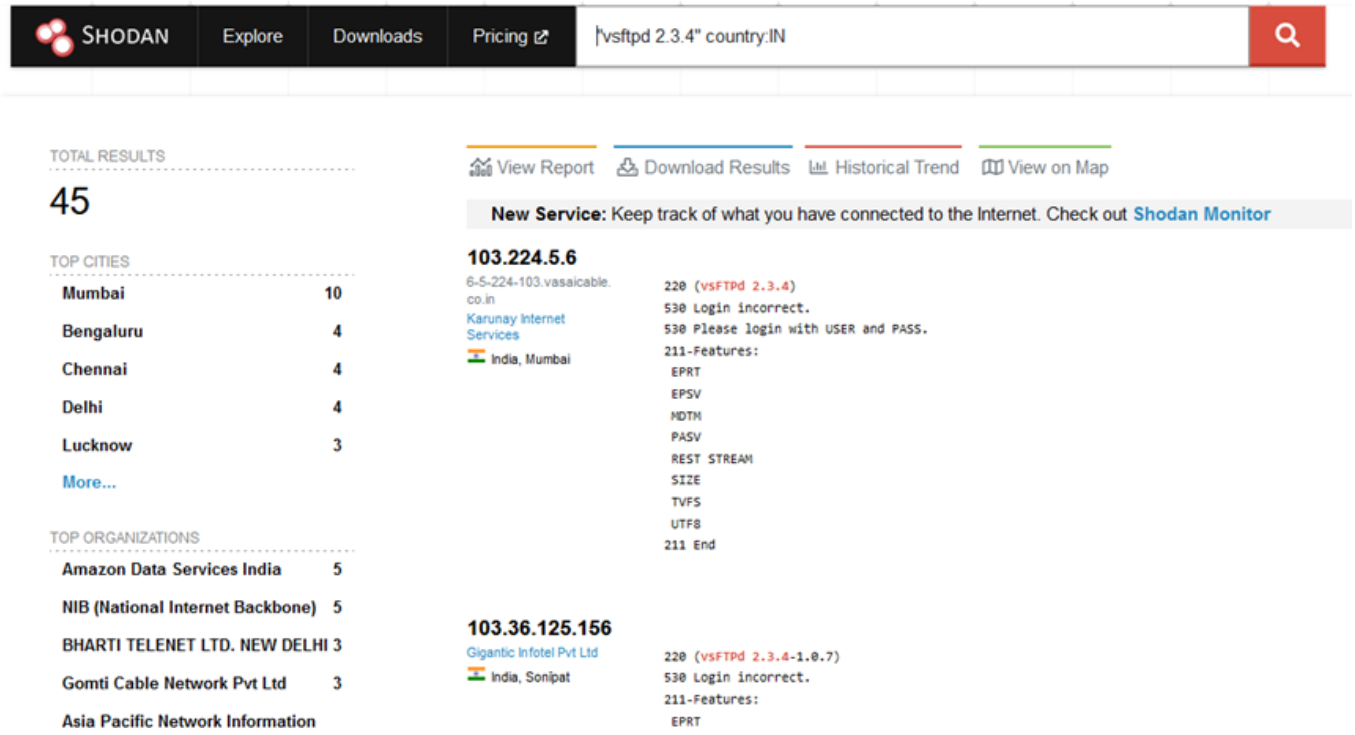

Рисунок 2.16 – Формування пошукової фрази у Shodan

В обраній країні знайдено 45 пристроїв, однак варто відмітити, що далеко не всі з них можуть бути вразливими через вчасно встановлені патчі безпеки.

Щоб експлуатувати виявлену вразливість, у Kali Linux можна скористатися вбудованими засобами фреймворку Metasploit, де існує готовий модуль для запуску відповідної атаки (рис.2.17):

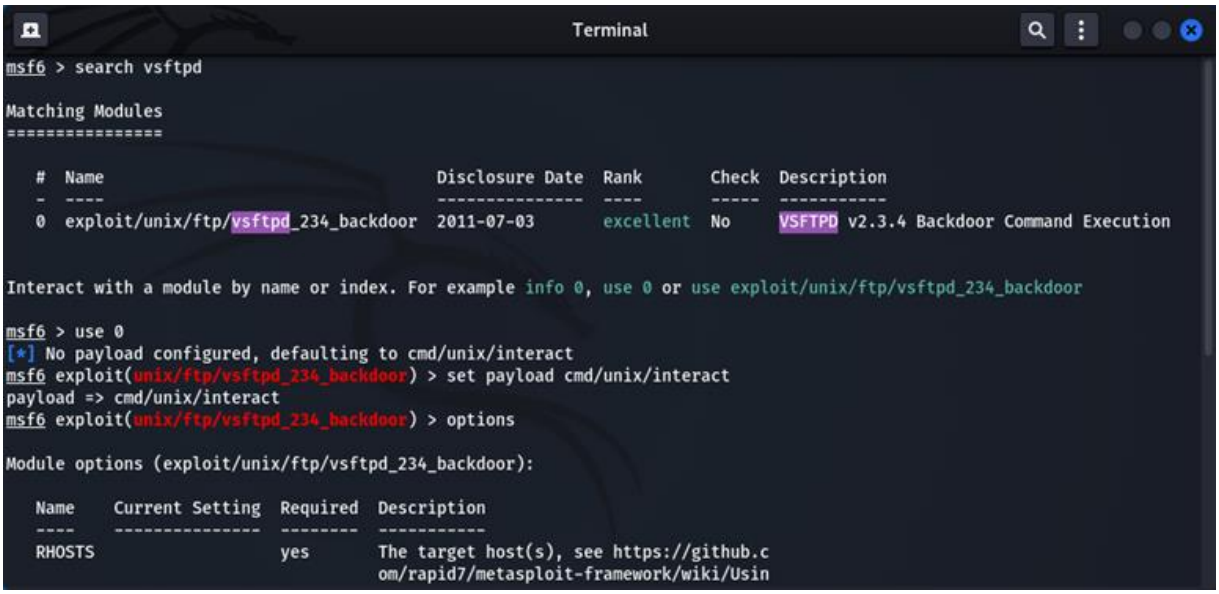

Рисунок 2.17 – Експлуатація вразливості у знайденому FTP-сервері

Якщо цільовий FTP-сервер виявиться непропатченим, ми зможемо отримати повний адміністративний доступ до усіх функцій його управління.

Додатково для пошуку пристроїв за ідентифікаційними номерами їх офіційних вразливостей (CVE), у Shodan дуже зручно використовувати окремий фільтр «vuln», однак він доступний лише для власників певних тарифних планів.

Таким чином, отримані результати доводять практичну ефективність роботи з Shodan для пошуку та подальшого дослідження вразливих пристроїв глобальної мережі.

Висновки за розділом 2

Як кінцеві споживачі, ми повинні ретельно проектувати інфраструктуру розумних гаджетів і враховувати інформаційні загрози, які надходять до нас разом із придбанням цих пристроїв. Що стосується компаній, то вони зобов’язані переконатися, що володіють у своєму розпорядженні належним механізмом управління ризиками, який включатиме у себе не тільки можливість постачання корисного продукту, а і відповідні засоби для забезпечення його безпеки.

Без створення належних стандартів безпеки, які регулюватимуть діяльність в IoT, користувачі продовжуватимуть долучати до мережі незахищені пристрої. Таким чином, уряду та великим організаціям слід впровадити необхідні вимоги до обробки інформації, щоб інструменти на кшталт Shodan стали абсолютно недієвими.

Варто відмітити, шо не так давно Комітет комерції Сенату США затвердив Закон про розвиток інновацій та зростання Інтернету речей (DIGIT), метою якого є створення робочої групи, яка зосередиться на питаннях безпеки, приватності та інших проблемах IoT. Крім того, Міністерство внутрішніх справ і зв'язку Японії планує створити знак сертифікації безпеки для пристроїв IoT і займається його впровадженням з 2018 року.

РОЗДІЛ 3
КОНЦЕПЦІЯ DARK WEB ЯК ЗАСІБ СТВОРЕННЯ БЕЗПЕЧНОГО ІНТЕРНЕТУ РЕЧЕЙ

3.1 Дослідження можливості застосування механізмів Dark Web для підвищення рівня безпеки Інтернету речей

Як відомо, Dark Web вимагає спеціальних інструментів та програмного забезпечення для навігації його ресурсами. Dark Web – це місце, де люди зазвичай знаходять свої вкрадені та скомпрометовані дані, доступні для продажу, разом із усіма іншими незаконними артефактами – від наркотиків до медичних карток та зброї. Цей рівень Всесвітньої павутини побудований на маршрутизації трафіку через так звані однорангові мережі комп'ютерів по всьому світу, в результаті чого відстежити шляхи переміщення даних майже неможливо. Однією з конфігурацій, на якій працює Dark Web – це мережа TOR, що реалізує протокол маршрутизації за прототипом «цибулі». Іншими словами, програмне забезпечення TOR дозволяє користувачеві переглядати окремий шар мережі, використовуючи згадані однорангові з'єднання. Безпека досягається завдяки величезному затемненню та постійним змінам шляхів і ланцюгів передачі інформації.

Як виявляється, Dark Web може насправді послугувати ключем до більш безпечної стратегії функціонування IoT. В рамках дослідження питань безпеки експеримент Guardian показав, як Home Assistant (проект домашньої автоматизації з відкритим кодом) можна встановити на Raspberry Pi 3 (дуже недорогий процесорний комплект IoT) та забезпечити захист останнього, застосувавши ті самі поняття безпеки, що використовуються в мережі TOR, а саме запускаючи його як приховану «цибульну службу». Іншими словами, користувач запускає службу, приховану від інших вузлів мережі TOR, і лише пристрої з правильними даними для автентифікації здатні фактично спрямовувати та обмінюватися інформацією між собою [3].

Результат, як вважає директор проекту Guardian Натан Фрейтас, претендує на якісно більш безпечний спосіб під’єднання розумного дому до мережі, одночасно зберігаючи його від потенційних кібератак. Фрейтас підсумовує, що «все, що ми зробили, це поєднали апаратну частину у вигляді смарт-хаба на базі Raspberry Pi 3 із відкритим програмним забезпеченням Home Assistant, щоб продемонструвати концептуальну роль, яку може відігравати TOR у вашому домі».

Насправді, розглянута ідея не просто перетворює згаданий домашній смарт-хаб у звичайну приховану tor-службу, яка, як правило, застосовується для того, щоб надати користувачеві доступ до веб-сайту шляхом маршрутизації трафіку мережею із тисяч волонтерських комп'ютерів. Замість цього Smart Home System використовує менш відому особливість TOR, яка називається прихованою службою аутентифікації. Усі інші комп'ютери не можуть підключатися до цільового пристрою без надання певного значення, що міститься у файлі cookie. Таким чином, користувач все ще може мати доступ до будь-якого із своїх пристроїв свого розумного дому через програми або Інтернет, але потенційний хакер навіть не зможе їх віднайти. Завдяки наявності такого типу аутентифікації, лише суб’єкти з визначеним файлом cookie можуть підключитися до розумного дому, інакше TOR навіть не дозволить дістатися до раніше створеної прихованої служби [30].

Традиційно, коли використовуються пристрої IoT, вони підпадають під одну з двох категорій. У першій категорії пристрій спілкується з найбільш вигідною для свого виробника інфраструктурою, при цьому безпека не обов'язково пріоритетна. Крім того, у цій категорії виробник, швидше за все, реєструє всі взаємодії та приватні дані користувача для власного використання. У другій категорії пристрій може зажадати від свого власника створення правила вільного доступу на маршрутизаторі для відкриття зовнішнього зв'язку. Обидва підходи збільшують ризик компрометації кінцевого власника і роблять його гаджети вразливими до сканування такими мережевими інструментами як Shodan. Отже, рішення про взаємодією з мережею TOR робить новим та унікальним те, що користувач не підключається безпосередньо до сервера виробника або ж не мусить втручатися у правила роботи домашнього роутера [3].

Для більш лаконічної візуалізації наведеної ідеї у якості прикладу можна навести принцип роботи маятника Ньютона (рис. 3.1), де крайня ліва кулька є власне користувачем, крайня права – пристроєм IoT, а всі інші між ними – одноранговими мережами кожна відповідно. Жодна з куль в цій системі не знає кінцеву точку передачі або ініціатора спілкування, вона лише відправляє дані до сусідньої кульки.

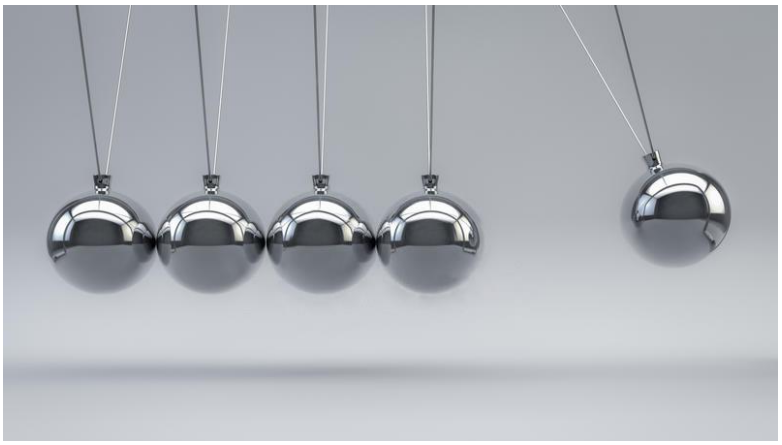

Рисунок 3.1 – Маятник Ньютона

А тепер уявімо популяцію доступних куль у мережі TOR і кількість нелінійних шляхів (так званих ланцюгів за термінологією TOR), які динамічно створюються та розриваються. Цей приклад чудово показує частину можливостей, які з’являються при використанні TOR разом з IoT [3].

3.2 Аналіз існуючих конфігурацій щодо організації типової мережі «розумних» пристроїв

Розглянемо типовий приклад системи автоматизації управлінням «розумного» будинку, що складається з двох точок доступу та декількох різних IoT-пристроїв, під’єднаних до кожної з них (рис. 3.2). Кожна точка доступу має помірні обчислювальні спроможності та відповідає за забезпечення критичних функції зв’язку, захисту і управління пристроями. Обидві точки використовують методи шифрування трафіку всередині мережі на основі еліптичних кривих (Elliptical Curve Cryptography).

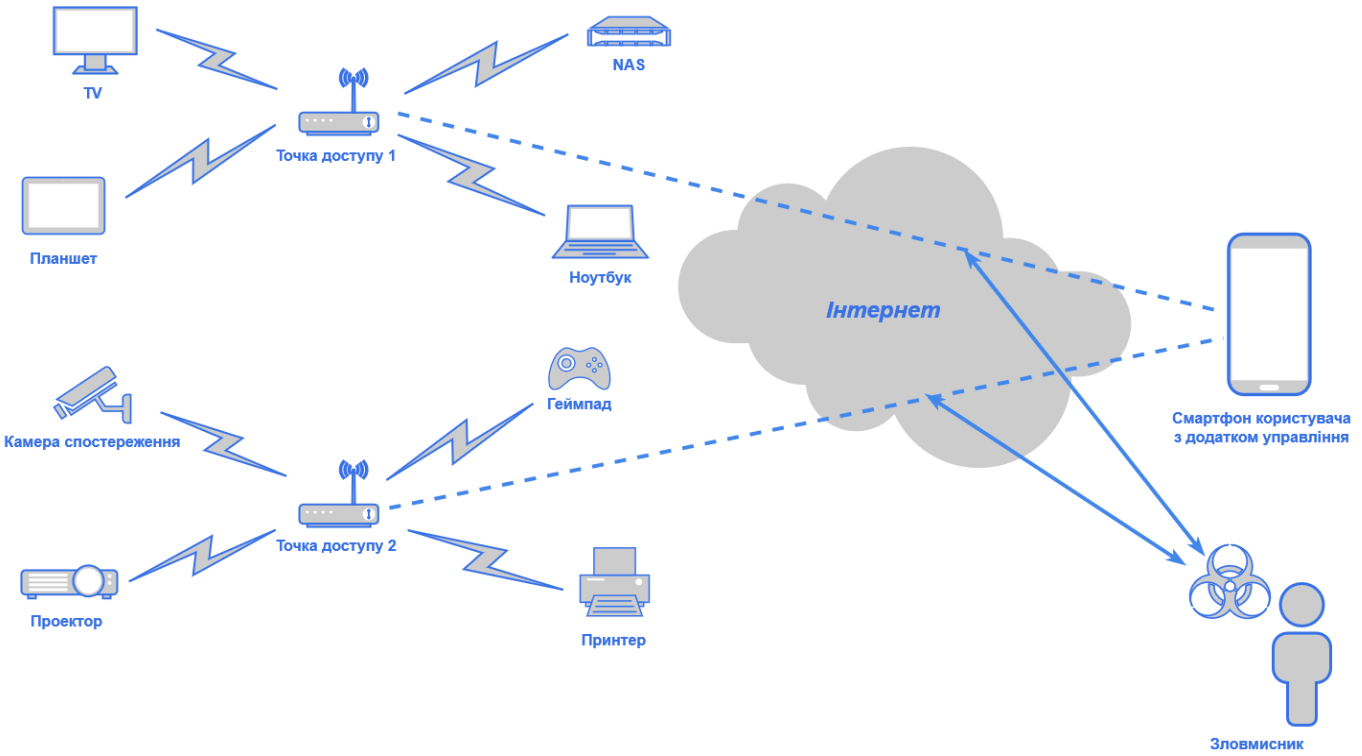

Рисунок 3.2 – Приклад організації мережі з відкритим обміном даних через Інтернет

Основна проблема функціонування наведеної вище структури мережі полягає у тому, що всі пакети передаються через Інтернет у відкритому вигляді. Атакуючий зі значними обчислювальними ресурсами може з легкістю реалізувати атаку для перехоплення цих пакетів і подальшого маніпулювання ними. Крім того, здійснення атаки з переустановкою ключа (KRACK) дозволяє скомпрометувати увесь трафік безпровідної мережі навіть без зламу шифрованого ключа аутентифікації. Тому IoT-мережа, робота якої контролюється через засоби публічного Інтернету, завжди буде привабливою для величезної кількості зловмисників [31].

Інший поширений підхід до керування IoT-мережами передбачає залучення потужностей хмарних сервісів вендора для передачі та отримання трафіку (рис. 3.3).

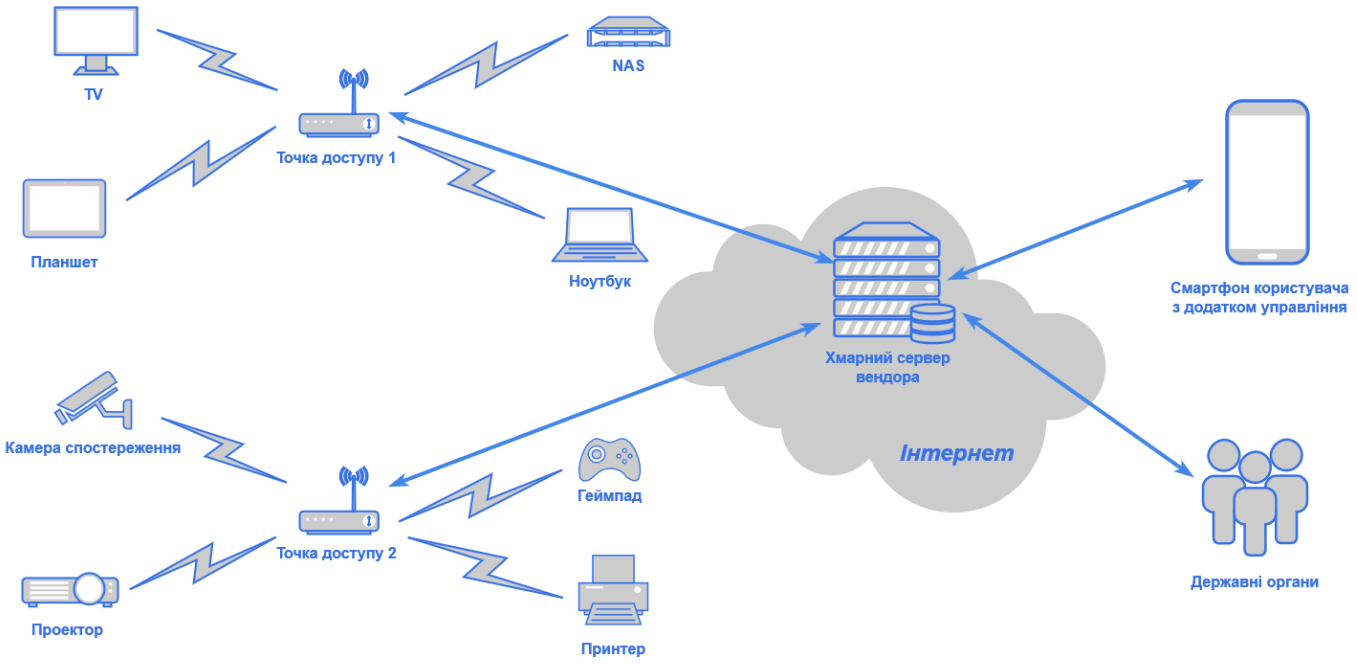

Рисунок 3.3 – Приклад організації мережі зі залученням хмарних ресурсів вендора

Захист усіх відправлених маршрутизатором користувача пакетів відбувається з використанням протоколу HTTPS, який вимагає наявності дійсного SSL-сертифікату, аби забезпечити автентичність особи-відправника. Використання хмари пропонує своїм споживачам вищий рівень безпеки даних, однак аж ніяк не їх конфіденційності. На сьогоднішній день закони багатьох країн постановляють про можливість обов'язкової співпраці хмари вендора з відповідними державними установами для надання останнім необхідних даних про своїх користувачів без права на відмову. Це означає, що чутлива інформація, яка зберігається у хмарі, не є захищеною від ока держави та її наглядових органів. Хоча зараз на ринку технологій існує багато спеціалізованих рішень для організації мережі «розумних» пристроїв на кшталт Ubi, Wink Hub, MyQ та інших смарт-хабів, вони не задовольняють ніяким вимогам у забезпеченні конфіденційності даних.

Як результат, жодна із існуючих мережевих структур не може гарантувати надійного захисту для кінцевого споживача мережі «розумних» девайсів. Тому вирішення проблеми реагування на численні виклики безпеки в IoT-мережах, ймовірно, полягає у внесенні змін до фізичної архітектури відповідних IoT-пристроїв з метою ефективного розподілення наявних обчислювальних потужностей та створення комплексного механізму захисту усієї мережі. Однак такі модифікації в

апаратному і програмному забезпеченні існуючих IoT-систем зазвичай є доволі непомірними у розрізі витрати часу та коштів.

Крім того, властива IoT-пристроям схильність до автономної роботи робить їх дуже доречною ціллю для зловмисників. До прикладу, бездротові сенсорні мережі (БСМ) потребують використання протоколу IEEE 802.15.5, який реалізує лише базові механізми аутентифікації та, більше того, монопольно розповсюджується на усі інші IoT-пристрої за рахунок відсутності будь-яких альтернатив. Тут під поняттям БСМ мається на увазі така розподілена мережа з кількох датчиків та об'єднаних через спільний радіоканал допоміжних пристроїв, яка функціонує на засадах самоорганізації з мінімальним втручанням людського фактору. У межах функціонування інфраструктури «розумного» будинку її поширеними компонентами можуть бути датчики температури, рівня освітлення, тиску чи вібрації, сенсорні датчики руху і т.д.

Модель загроз IoT зазнала кардинальних змін саме після того, як подібні мережі отримали вільний вихід до Інтернету, тим самим надавши можливість віддаленого доступу до своїх сенсорних вузлів, що є найбільш вразливими через мізерні обчислювальні спроможності. Природньо, що цей фактор не дозволяє впровадити складні протоколи захисту (наприклад, «цибульної» маршрутизації).

Як висновок, після аналізу існуючих засобів захисту IoT-мережі потреба у створенні захищеної точки доступу, яка забезпечувала б конфіденційність, надійність, безпеку та масштабованість усіх її пристроїв, є очевидною. Таким чином, для того, щоб забезпечити перспективу повсюдного прийняття IoT-мереж, реалізація тріади властивостей ІБ у них – конфіденційності, цілісності і доступності – є основною та необхідною умовою для досягнення IoT-системами високого рівня довіри всередині суспільства.

3.3 Опис архітектури пропонованого рішення для підвищення безпеки IoT

3.3.1 Особливості апаратної та програмної імплементації

Щоб розв’язати вище викладену проблему [надання безпечного віддаленого доступу] в існуючій IoT-мережі, необхідно або повністю модифікувати архітектуру кожного її вузла та пов’язаних з ним протоколів, або ж залучити новий проміжний компонент, який би забезпечував впровадження надійного протоколу безпеки. У якості такого компоненту розглянемо одноплатний комп’ютер (SBC – Single-board Computer) Raspberry Pi 3 Model B (рис. 3.4), що володіє достатніми обчислювальними можливостями та об’ємом пам’яті для запуску будь-якої unix-подібної операційної системи. Дослідження показують, що даний продукт із лінійки Raspberry Pi зарекомендував себе як ультрабюджетний мікропроцесорний комплект з підтримкою великої кількості під’єднуваної периферії та мережевих інтерфейсів, тому ідеально підходить для взаємодії з багатьма IoT-пристроями і додатками. Крім того, застосування одноплатних комп’ютерів у ролі точок доступу в IoT дозволяє забезпечити максимальну сумісність та значно спрощує процес розширення мережі під час додавання нових вузлів.

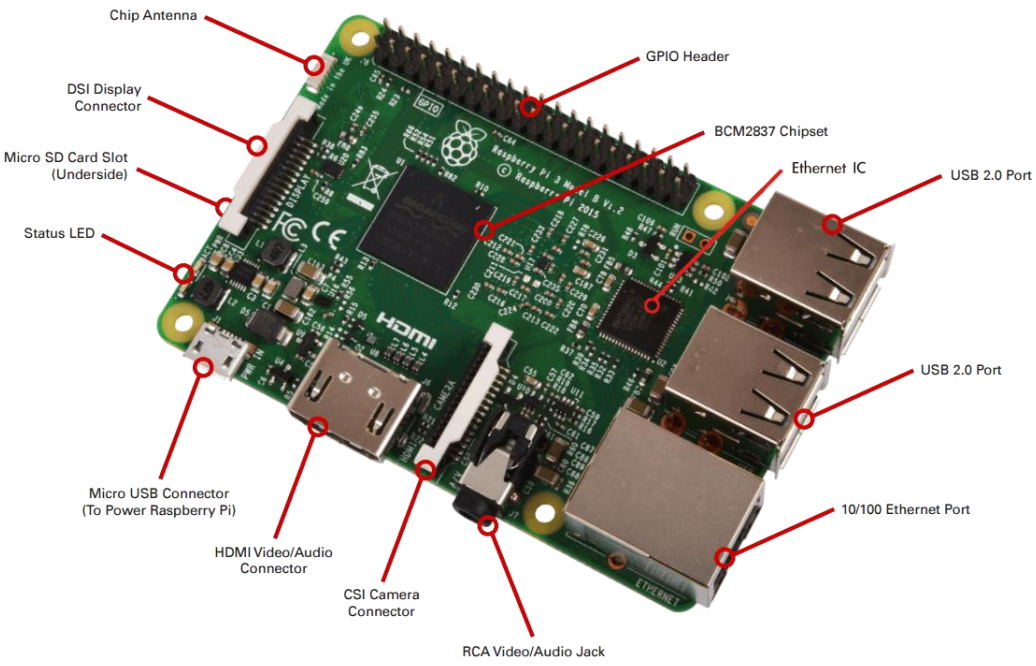

Рисунок 3.4 – SBC Raspberry Pi3 Model B

Метод, пропонований P. S. Ajay Mishael та Joy Paulose з Бангалорського університету Христа (Christ University, Індія) в статті наукового журналу «International Journal of Mechanical Engineering and Technology» (IJMET), полягає у використанні SBC як прихованої за допомогою механізмів Dark Web точки доступу. Доступ до неї може бути отриманий лише сутностями, які володіють унікальними onion-посиланням та 22-бітним cookie для проходження аутентифікації. Усі параметри, що застосовуються для ідентифікації цієї точки доступу, також є цілковито прихованими. Процедура аутентифікації користувача на основі файлу cookie (Cookie-Based Authentication) зазвичай включає наступні кроки [32] (рис. 3.5):

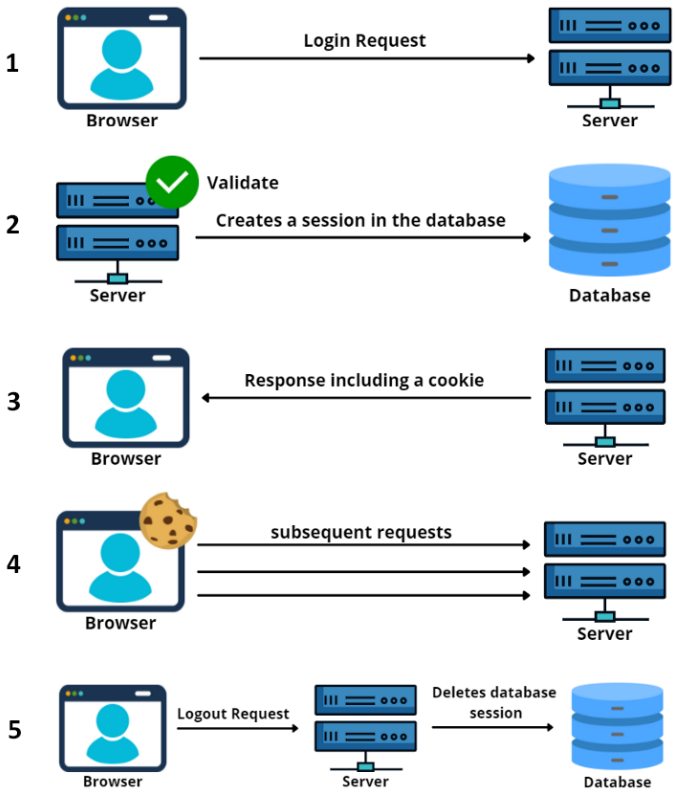

Рисунок 3.5 – Cookie-Based Authentication

1. Користувач ініціює процедуру входу, використовуючи свої облікові дані.
2. Сервер перевіряє правильність введених даних та у разі успіху створює новий сеанс в базі даних.
3. Сервер надсилає браузеру файл cookie, що відправляється у вигляді пари ім’я-значення зі заголовком «Set-Cookie» і містить унікальний ідентифікатор користувача (ID).

4. Браузер зберігає файл в своїй пам’яті та надсилає разом з усіма подальшими запитами. Коли сервер отримує новий запит з cookie, він порівнює отриманий ідентифікатор сеансу з тим, що знаходиться у його базі даних для підтвердження автентичності користувача.

5. Коли користувач виходить із системи, сервер автоматично видалить сеанс із бази даних. У свою чергу, браузер також видалить файл cookie зі своєї пам’яті.

Це повністю автоматизований процес.

Враховуючи положення вище наведеного алгоритму, розглянемо загальну послідовність руху трафіку у пропонованій системі [33; 34] (рис.3.6):

1. Прихована служба передає TOR-вузлам (Introduction Point), які представлятимуть її у мережі TOR, свій публічний ключ та будує з ними ланцюги з’єднання. Прихована служба відправляє розподільчому серверу (Directory Server) файл дескриптора, в якому міститься перелік точок представлення та публічний ключ служби.

2. TOR-клієнт на Android (Orbot) ініціює процедуру з’єднання з прихованою службою шляхом завантаження з розподільчого сервера її дескриптора.

3. Клієнт користувача обирає випадковий вузол мережі TOR у якості точки зустрічі (Randezvous Point), будує ланцюг з випадково обраних вузлів-посередників TOR та відправляє до нього одноразовий секрет.

4. Клієнт створює запрошувальне cookie-повідомлення, яке містить деталі про точку зустрічі, що зашифровані публічним ключем прихованої служби. Це повідомлення доставляється до точки представлення служби через новий ланцюг.

5. Точка представлення доставляє повідомлення через описаний у пункті 1 ланцюг до прихованої служби.

6. Прихована служба розшифровує отримане повідомлення та дізнається адресу точки зустрічі і її одноразовий секрет. Потім прихована служба створює ще один ланцюг з’єднання з точкою зустрічі та відправляє їй знайдений одноразовий секрет. Onion-аутентифікація завершена.

7. Точка зустрічі сповіщає клієнта про успішне з'єднання, а раніше створені з нею ланцюги використовуються для подальшого обміну даними між прихованою службою та клієнтом.

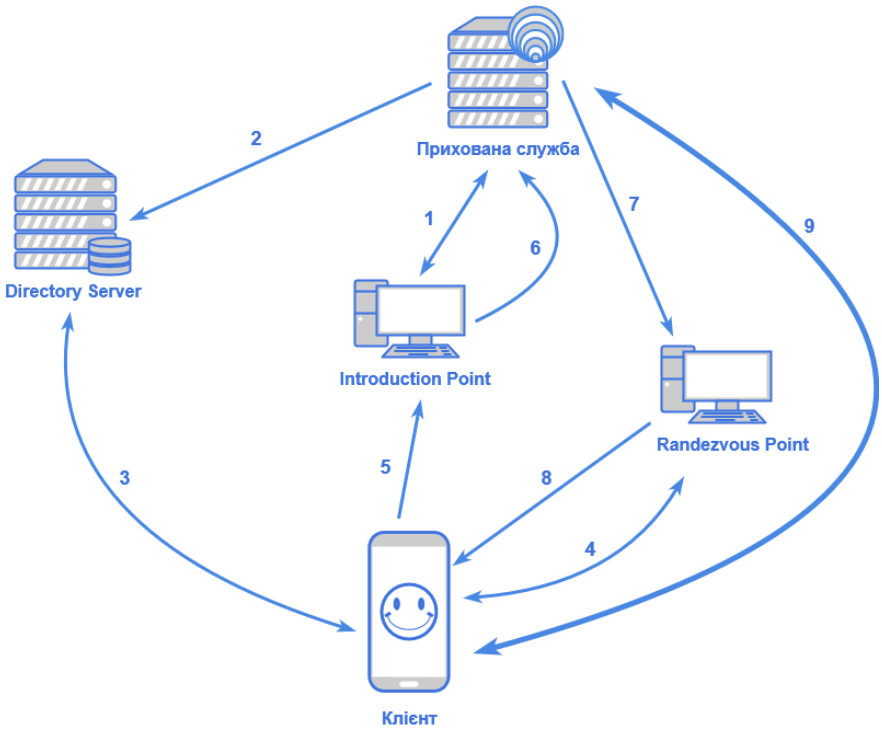

Рисунок 3.6 – Алгоритм кроків onion-аутентифікації

Загалом, повний шлях передачі трафіку після успішної аутентифікації налічує 6 вузлів-посередників мережі TOR: три у ланцюзі, створеному прихованою службою, та ще три у ланцюзі, створеному клієнтом (рис. 3.7). Стандартно будь-який ланцюг TOR складається із трьох випадково обраних вузлів мережі TOR. Кожна ланка цього ланцюга, як зазначалося у пункті 1.2.2 даної роботи, при отриманні даних послідовно знімає один із трьох шарів шифрування, якими одна сторона спілкування зашифрувала пакети перед відправкою через мережу TOR. Таким чином, у нашому випадку після видалення вузлами-посередниками усіх трьох шарів шифрування точка зустрічі отримає звичайний трафік зі стандартним шифруванням HTTPS. Далі точка зустрічі знову зашифрує отримані пакети трьома новими шарами шифрування та направить їх у ланцюг з'єднання, що був створений прихованою службою. Така схема циркуляції трафіку забезпечує однозначну анонімність обох сторін спілкування.

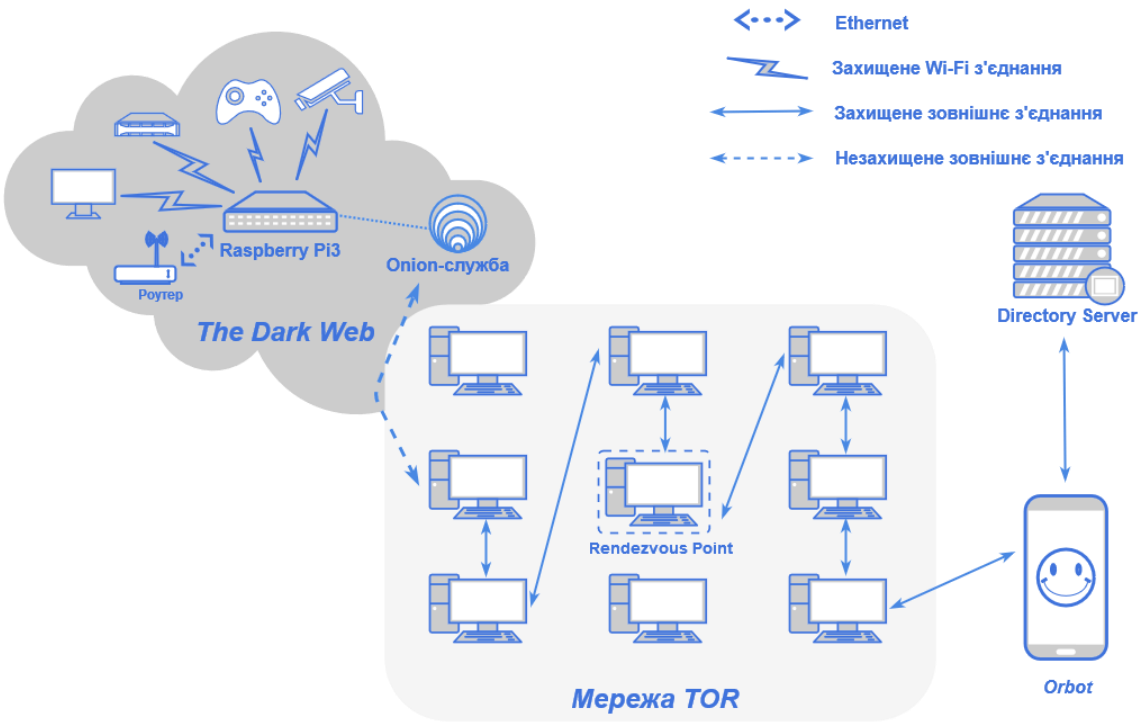

Рисунок 3.7 – Порядок переміщення трафіку у пропонованому рішенні

У розглянутій системі SBC взаємодіє з усіма IoT-пристроями, функціонуючи для них у якості точки доступу та проміжного обробника запитів. SBC відповідальний за збір, оновлення та аналіз інформації, що генерується під'єднаними до нього «розумними» пристроями. Перед тим SBC підключається до домашнього роутера, який надає йому доступ до Інтернету та внутрішньої мережі. Оскільки SBC (Raspberry Pi 3) знаходиться у межах функціонування Dark Web та не реєструється публічними DNS-серверами у жодній доменній зоні, це робить неможливим усі спроби отримання доступу до нього без необхідних даних. Налаштована точка доступу на базі SBC запускає приховану TOR-службу (сервер із програмним забезпеченням TOR Hidden Services), а також розгортає на ньому IoT-прошивку (Home Assistant) для зв'язку «розумних» пристроїв зі смартфоном користувача. Прихована служба не може бути ніким віднайдена до тих пір, поки вона самостійно не повідомить клієнта (Orbot) про своє існування.

Очевидно, що ми розглядаємо особливості функціонування пропонованого рішення при обов'язковому виконанні наступних умов:

- Користувач має встановлений на своєму смартфоні TOR-браузер (Orbot).

- Користувач знає відповідну onion-адресу прихованої служби.
- Користувач володіє необхідним cookie для доступу до прихованої служби.
- IoT-пристрої поєднані з прихованою службою у безпечний спосіб.
- Прихована служба доступна лише через її точки представлення (Introduction Point) у TOR-мережі.

Примітка від автора: Як відомо, технологія NAT, що зазвичай використовується для створення локальної мережі, присвоює усім пристроям всередині єдину публічну адресу їх роутера, таким чином не дозволяючи їм отримувати запити ззовні. Однак у випадку, коли конкретний пристрій відправляє запит до зовнішньої мережі, роутер матиме можливість повернути отриману відповідь саме до нього. Тому, незважаючи на те, що SBC знаходиться у локальній мережі за роутером, це не завадить створеній прихованій службі спілкуватися з вузлами мережі TOR, оскільки вона завжди першою ініціює процедуру встановлення вихідного зв'язку у будь-якому ланцюзі.

За допомогою рисунку 3.8 конкретизуємо ролі, які будуть покладені на необхідне для створення пропонованої IoT-мережі апаратне та програмне забезпечення.

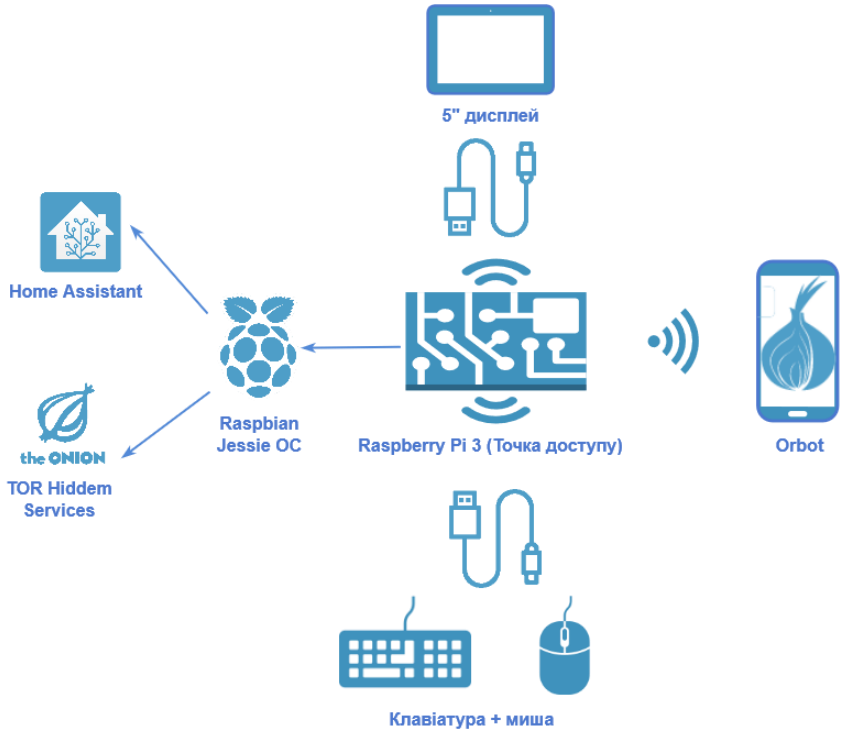

Рисунок 3.8 – Модель візуалізації пропонованого рішення

Апаратна частина передбачає залучення наступних компонентів:

- Raspberry Pi 3 model B (SBC) – точка доступу для пристроїв «розумної» мережі (1 ГБ RAM, Quad Core 1.2GHz Broadcom BCM2837 64-bit CPU, розширений 40-pin GPIO, 4 USB 2.0 порти, повнорозмірний HDMI порт, CSI порт, DSI порт, Micro-SD порт, 2.5A джерело живлення). Окрім розгортання функцій прихованого сервера, також використовується для встановлення платформи управління IoT-мережею.
- Ноутбук або будь-який смартфон – панель управління «розумною» мережею.
- Клавіатура, миша, дисплей – периферія для взаємодії з Raspberry Pi 3.

Програмні компоненти:

- Home Assistant – платформа автоматизації управління інфраструктурою «розумного» будинку з відкритим кодом, що працює на Python. Home Assistant контролює роботу усіх IoT-пристроїв мережі.
- TOR Hidden Services – відкрите програмне забезпечення для запуску SBC у якості прихованої служби (сервера в Dark Web), що доступне для всіх unix-подібних операційних систем.
- Raspbian (Raspberry Pi OS) – офіційна операційна система з відкритим кодом для Raspberry Pi. Raspbian володіє відмінною підтримкою від розробників та має широку базу навчальних матеріалів.

Реалізація пропонованого рішення має на меті створення IoT-мережі із виконанням наступних кроків:

1. Операційна система Raspbian Jessie 4.9 встановлюється на Raspberry Pi 3 (SBC).
2. На Raspberry Pi 3 інсталюються всі необхідні пакети (і їх залежності) для запуску Home Assistant.
3. Далі завантажується програмна зв’язка TOR Hidden Services і вносяться необхідні зміни до її конфігураційного файлу «torrc», щоб запустити приховану службу.

4. Після налаштування точки доступу вносяться відповідні зміни до конфігураційного файлу «torrc» клієнта.

5. Після перезапуску усіх TOR-сервісів веб-панель інтерфейсу Home Assistant має стати доступною на клієнті користувача.

Під час запиту користувача на перехід по відомому йому onion-посиланню та за умови обов'язкового надання 22-бітного cookie аутентифікації, веб-сторінка Home Assistant відкриється у TOR-клієнті (браузер Orbot на Android). Будь який зловмисник, що має на меті пошук місцезнаходження прихованої служби, повинен зламати три шари TLS-шифрування, яке на сьогоднішній день вважається одним із найкращих стандартів у сфері криптографії. Таким чином, доступ до прихованої служби може бути отриманий на смартфоні через Orbot, в якому значення cookie було попередньо внесене до відповідного розділу налаштувань у самому додатку.

Без використання cookie, прихована служба не буде доступною через Orbot. У разі отримання запиту від користувача на перехід по відомому йому onion-посиланню без відповідного значення 22-бітного cookie для аутентифікації, Orbot виведе сторінку з помилкою з'єднання (рис. 3.9). Власник точки доступу може створити та відкликати необмежену кількість cookie, що дозволяє створити надійну систему контролю доступу.

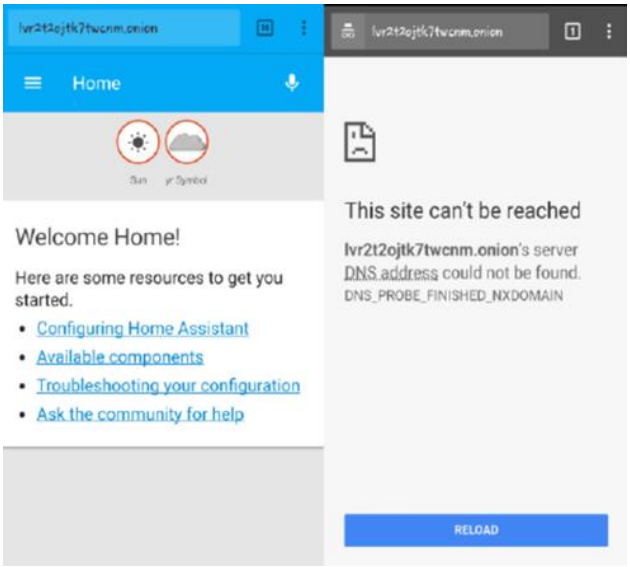

Рисунок 3.9 – Спроба доступу до панелі управління Home Assistant з наявним cookie для аутентифікації та без

Як результат, щоб отримати змогу керувати потужностями пропонованої IoT-мережі, користувач має володіти наступними даними:

- onion-посилання на приховану службу;
- 22-бітне значення cookie для аутентифікації; та
- логін і пароль від аккаунту Home Assistant.

У свою чергу, зловмисник, що знаходиться у процесі пошуку нових цілей серед IoT-пристроїв, не в змозі віднайти точку доступу, оскільки її просто не існує на просторах публічного Інтернету. Навіть якщо атакуючому вдається виявити приховану службу, він мусить подолати два додаткових рівня захисту (cookie та облікові дані користувача у Home Assistant), що є дуже малоймовірним сценарієм розвитку подій. Більше того, у разі зламу точки доступу, адміністратор IoT-мережі може з легкістю відновити її попередній стан шляхом відкликання усіх cookie для аутентифікації.

Для більш наочного уявлення про особливості конфігурації мережі, розглянемо процес програмного налаштування Raspberry Pi 3 у якості прихованої точки доступу [35]:

1. Встановлення TOR Hidden Services. Для зручності під’єднуємося до Raspberry Pi 3 з комп’ютера через SSH. Після установки залежностей для Home Assistant виконуємо команду «sudo apt get install tor» для встановлення основної служби TOR (рис. 3.10). Далі запустити службу можна, просто ввівши у командному рядку «tor».

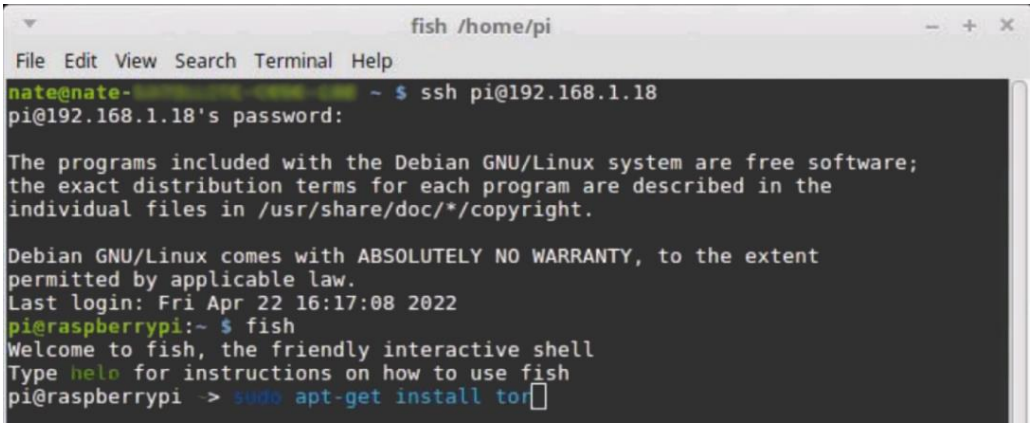

Рисунок 3.10 – Встановлення служби TOR

2. Налаштування конфігурації TOR. Виконаємо команду «sudo nano /etc/tor/torcc», щоб відкрити конфігураційний файл TOR у режимі редагування та перейдемо до секції з назвою «This section is just for location-hidden services». Одразу ж після коментаря про призначення цієї секції додамо три нових рядка (рис. 3.11):

- HiddenServiceDir /var/lib/tor/homeassistant/
- HiddenServicePort 80 127.0.0.1:8123
- HiddenServiceAuthorizeClient stealth haremote1

У кінці збережемо зміни та вийдемо з редактора.

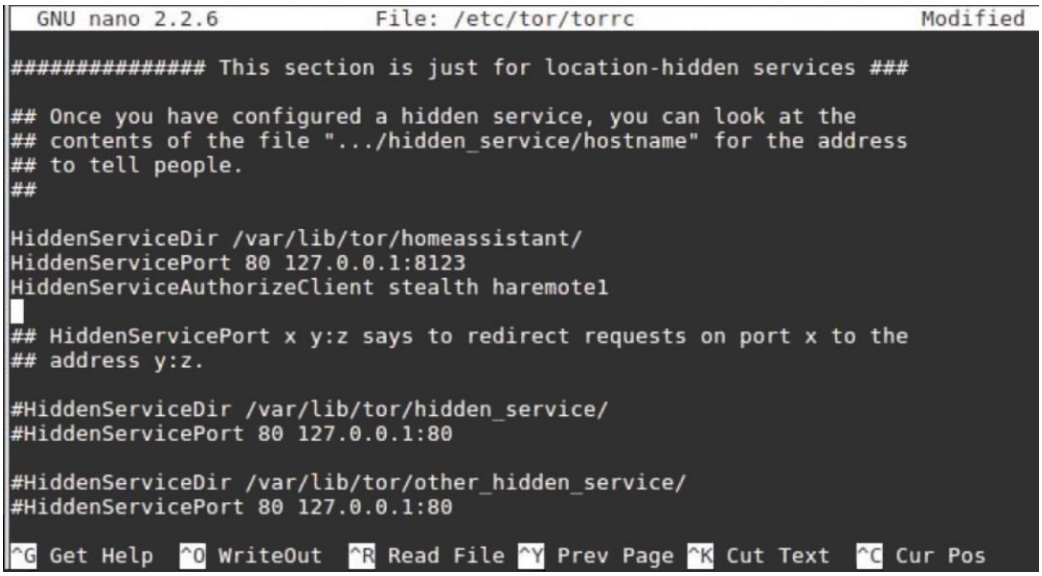

Рисунок 3.11 – Налаштування конфігураційного файла «torcc»

3. Перезапуск TOR та отримання даних про приховану службу. Використаємо команду «sudo /etc/init.d/tor» для перезапуску TOR та застосування усіх внесених змін. Далі за допомогою команди «sudo more /vat/lib/tor/homeassistant/hostname» ми зможемо дізнатися onion-посилання на нашу приховану точку доступу та її 22-бітне значення cookie для аутентифікації. Ці дані матимуть вигляд у форматі «abcdef1234567890.onion ABCDEF1122334455667788 # client: haremote1» відповідно.

4. Надання доступу для клієнта. Останнім кроком залишається занести знайдене значення cookie до налаштувань Orbot в смартфоні. Для цього переходимо у розділ «Torrc Custom Configuration» в Orbot → Menu → Settings. Процедура налаштування завершена.

3.3.2 Переваги та недоліки пропонованого рішення

Як і будь-яка інша система, пропонована IoT-мережа має свої переваги та недоліки. Очевидно, що рішення можна вважати ефективним у тому випадку, коли перше переважає над другим.

Безперечно перевагою є те, що приховані сервери є цілковито захищеними до багатьох поширених атак, таких як DDoS, MITM, ідентифікація «цифрового відбитку» (Website Fingerprinting), підміна особистості, аналіз трафіку та атака з переустановкою ключа (KRACK), оскільки усі пакети проходять через мережу TOR, що унеможливлює їх виявлення та перехоплення. Анонімізація суб'єктів може застосовуватися у якості контрзаходу для запобігання різного роду несанкціонованих дій, що часто експлуатують сліди переміщення трафіку у мережі.

У таблиці 3.1 наведена порівняльна характеристика пропонованого рішення з іншими існуючими системами для організації інфраструктури «розумного» будинку:

Таблиця 3.1

Порівняльна характеристика пропонованого рішення з іншими існуючими системами.

Критерії конфіденційності	**Wink Hub**	**Ubi**	**SmartThings Hub**	**MyQ Garage**	**Пропонована система**
Надійна аутентифікація	Так	Так	Так	Так	Так
Безпечні мережеві сервіси	Ні	Ні	Ні	Ні	Так
Криптографія	Так	Ні	Так	Так	Так
Безпечний мобільний інтерфейс	Ні	Ні	Ні	Ні	Так
Надійна прошивка	Так	Так	Так	Так	Так
Безпечний веб-інтерфейс	Ні	Ні	Так	Ні	Так
Захист чутливої інформації	Так	Ні	Так	Ні	Так
Валідація через TLS	Ні	Ні	Ні	Ні	Так
Захист від MITM-атак	Ні	Ні	Ні	Ні	Так
Захист від атак повторного відтворення	Так	Ні	Так	Ні	Так

Як результат, пропоноване рішення дійсно не вимагає ані відкриття додаткових портів у фаєрволі, ані зв'язку з хмарними ресурсами третіх сторін, як це зазвичай відбувається зі звичайними точками доступу.

Потрібно зазначити, що у цього рішення існують певні недоліки, а саме швидкість передачі трафіку, що залежить від кожного вузла однорангової мережі. Отримані P. S. Ajay Mishael та Joy Paulose результати свідчать, що створена прихована точка доступу відповідала на запити трохи повільніше, аніж її «відкриті» конкуренти. Суттєві ж затримки були помітні лише на початку формування ланцюгів зв'язку, однак після завершення цього процесу взаємодія між прихованою службою та клієнтом є стабільною. У наступній таблиці відображені час відповіді кожної системи під час її пінгування стандартними засобами командного рядка:

Таблиця 3.2

Порівняльна характеристика часу відповіді кожної системи на запити від користувача

Точка доступу	**Час відповіді**
Wink	150 мілісекунд
Ubi	132 мілісекунди
SmartThings Hub	120 мілісекунд
Пропонована система	250 мілісекунд після створення ланцюга зв'язку

Формування ланцюга зв'язку в середньому займає 1500 мілісекунд та варіюється від загальної пропускної здатності мережі TOR. Таким чином, спостерігається компроміс між безпекою та швидкістю мережі, у якому відмовляючись від зручності, ми можемо отримати підвищений рівень захисту [6]. Тим не менше, забезпечення додаткового рівня безпеки за допомогою прихованих служб TOR уже розглядається у якості потенційної зміни підходу, що робить пристрої IoT на порядок більш захищеними.

Серед інших недоліків слід виділити певну складність запуску розглянутої системи, яка вимагає, щоб кожен її пристрій мав можливість роботи з TOR та включав у своєму конфігураційному файлі необхідний програмний код налаштувань.

Як висновок, пропоновану систему можна вважати такою, що задовольняє усім висунутим вимогам у розрізі безпечного функціонування IoT-мережі.

Висновки за розділом 3

Як виявляється, використання одноплатних комп’ютерів (SBC) на кшталт Raspberry Pi 3 у якості прихованих onion-служб може надати будь-якому типу IoT-мережі декілька нових ліній оборони проти зловмисників. Незважаючи на те, що мережа TOR відносно повільна, прогнози на основі статистики вказують на невпинне збільшення кількості вузлів-посередників TOR з кожним роком, що, в свою чергу, позитивно впливає на загальну доступну пропускну здатність усієї мережі TOR. Приховані сервери на базі SBC можна налаштувати для забезпечення захисту масштабних IoT-мереж без додаткових фінансових витрат. Однак, попри все, сфера безпеки IoT, побудованої на засадах анонімності, все ще залишається недослідженою областю у наукових колах.

ВИСНОВКИ

У даній роботі було розв’язане актуальне наукове завдання щодо розробки нової архітектури доказово захищеної IoT-мережі для досягнення цілковито нового рівня захисту Інтернету речей.

Розширення спектру кібератак на IoT-ресурси вимагає застосування просунутих та надійних засобів захисту для забезпечення високого рівня безпеки своїх користувачів. Оскільки такі засоби на сьогоднішній день фактично відсутні через дорожнечу та складність їх впровадження, базові рекомендації щодо захисту «розумних» пристроїв не здатні належним чином протистояти усім загрозам. Переважна більшість користувачів не має достатньо часу чи знань для забезпечення захисту для всіх своїх пристроїв, а найчастіше розраховує на далекоглядність їх виробників в аспекті створення надійного захисту. Як результат, у першому розділі було сформоване визначення поняття Інтернету речей та його похідних складових, проаналізовано причини надзвичайної ефективності здійснення визначеного кола кібератак на «розумні» пристрої та створено загальні інструкції щодо захисту останніх від зламу. Також були пояснені основні аспекти функціонування «темної» павутини, детально розглянуті принципи роботи мережі TOR і onion-ресурсів та визначено характер їх впливу на IoT-системи.

Більше того, існування таких пошукових систем, як Shodan, значно погіршує стан безпеки Інтернету речей в цілому. Проведений експеримент по отриманню несанкціонованого доступу до обраного об’єкту інфраструктури доводить, наскільки довго уразливі IoT-пристрої можуть залишатися доступними для зловмисників зі глобальної мережі. Додатково були досліджені синтаксис фільтрів пошуку Shodan, поширені фрази для виявлення деяких категорій IoT-пристроїв та основні протиріччя в правовому полі щодо використання цього пошукового агрегатора.

Розглянута автором ідея по створенню безпечної мережі з використанням основоположних принципів Dark Web може дати поштовх до розвитку нових

інноваційних пропозицій щодо наступного покоління забезпечення конфіденційності в IoT, навіть незважаючи на те, що еволюція безпеки поки що не може піти таким шляхом. Держава і організації потенційно можуть використовувати дану концепцію, щоб захистити основні пристрої в своїх мережах таким же способом, як це робить сучасний Dark Web, проте з метою досягнення корисних, а не кримінальних цілей. Крім того, була створена імітаційна модель та проаналізовані переваги та недоліки пропонованого рішення.

Поставлені завдання були виконані у повному обсязі. Пропонована IoT-мережа, побудована на базі запропонованого методу, показала високі результати захисту наявних у ній «розумних» пристроїв.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Carthy, M. Shodan: The World's Most Dangerous Search Engine. [Electronic resource] / M. Carthy // LinkedIn. – February 28, 2016. – Access: https://www.linkedin.com/pulse/shodan-worlds-most-dangerous-search-engine-michael-carthy

2. Here's How the Internet of Things Will Explode by 2020. [Electronic resource] / Business Insider // April, 2016. – Access: https://www.businessinsider.com/iot-ecosystem-internet-of-things-forecasts-and-business-opportunities-2016-4-28.

3. Kuzminski, M. Using Darknet Concepts for IoT Security (Tor of Things). / Mike Kuzminski // ISACA Journal – 2017. – Vol. 6 – P. 1-3.

4. Notenboom, L. How Do I Protect My IoT Devices from Being Hijacked? [Electronic resource] / Leo A. Notenboom // October 29, 2021. – Access: https://askleo.com/protect-my-iot-devices/

5. Basatwar, G. IoT Security Optimization Tips & Benefits for Modern Businesses. [Electronic resource] / Govindraj Basatwar // AppSealing Blog – January 6, 2022. – Access: https://www.appsealing.com/iot-security/

6. What is a Smart Home? [Electronic resource] // Smart Home Energy – Access: https://smarthomeenergy.co.uk/what-smart-home/

7. IoT Security Issues, Threats, and Defenses. [Electronic resource] // TrendMicro – Access: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses

8. Bergman, M. The Deep Web: Surfacing Hidden Value [Electronic resource] / M. Bergman // The Journal of Electronic Publishing – August 2001. – Vol. 7, iss. 1. – Access: http://www.gproxx.com/http://blogxd.info/dspace/uk/zawo_buty_ver_wur_xi.pdf.

9. IoT Security – What is It and How Does It Protect Your IoT Devices [Electronic resource] // Paloalto Networks – Access: https://www.paloaltonetworks.com/cyberpedia/what-is-iot-security

10. Chertoff M., Simon T. The Impact of the Dark Web on Internet Governance and Cyber Security / Michael Chertoff and Tobby Simon // Centre for International Governance Innovation and the Royal Institute for International Affairs. – February 2015. – No. 6. – P.2-5.

11. Ozkaya E., Islam R. Inside the Web. / Erdal Ozkaya, Rafiqul Islam // CRC Press, Taylor & Francis Group. – 2019. – P. 8, 10.

12. Tiwari, A. Tor Explained: What is Tor? How Does It Work? Is It Illegal? [Electronic resource] / Aditya Tiwari // Fossbytes. – February 23, 2021 – Access: https://fossbytes.com/everything-tor-tor-tor-works/

13. TOR Support [Electronic resource] // Official website of TOR Project. – Access: https://support.torproject.org/

14. Tchabe G. Nya, Xu Y. Anonymous Communications: A Survey on I2P [Electronic resource] / Tchabe Gildas Nya and Yinhua Xu. – 2014. – www.cdc.informatik.tudarmstadt.de/fileadmin/user_upload/Group_CDC/Documents/Lehre/SS13/Seminar/CPS/cps2014_submission_4.pdf .

15. Grabosky, P. Virtual Criminality: Old Wine in New Bottles? [Electronic resource] / Peter Grabosky // Social & Legal Studies 10. – 2001. – P. 243–249. – Access: http://sls.sagepub.com/content/10/2/243.full.pdf.

16. Smartrac. The deep web, the dark web, and simple things. [Electronic resource] // The Medium. – Aug 1, 2017. – Access: https://medium.com/@smartrac/the-deep-web-the-dark-web-and-simple-things-2e601ec980ac

17. Hilt S., Kropotov V., Mercês F., Rosario M., Sancho D. The Internet of Things in the Cybercrime Underground [Electronic resource] / Stephen Hilt, Vladimir Kropotov, Fernando Mercês, Mayra Rosario and David Sancho // TrendMicro Research. – Access: https://documents.trendmicro.com/assets/white_papers/wp-the-internet-of-things-in-the-cybercrime-underground.pdf

18. Goldman, D. Shodan: The scariest search engine on the Internet [Electronic resource] / David Goldman // CNN Business. – April 8, 2013. – Access: https://money.cnn.com/2013/04/08/technology/security/shodan/

19. Butler, S. Why Is the Shodan Search Engine Potentially Dangerous [Electronic resource] / S. Butler – June 25, 2020. – Access: https://www.technadu.com/why-is-the-shodan-search-engine-potentially-dangerous/105440/

20. Сито для Интернета: интересные вещи с Shodan [Электронный ресурс] // Хабр. Блог компании RUVDS.com. – 19 дек. 2020. – Режим доступа: https://habr.com/ru/company/ruvds/blog/533890/

21. Белая шляпа для Shodan. Как легально использовать поисковик по IoT [Электронный ресурс] // Журнал «ХАКЕР». – 25 окт. 2015. – Режим доступа: https://xakep.ru/2015/11/25/shodan-howto/

22. Примеры поиска в Shodan [Электронный ресурс] // Хабр. – 23 сент. 2014. – Режим доступа: https://habr.com/ru/post/237787/

23. Filter Reference [Electronic resource] // Official website of Shodan Search Engine – Access: https://shodan.io/search/filters

24. Shodan – темный близнец Google [Электронный ресурс] // Хабр. Блог компании RUVDS.com. – 19 дек. 2020. – Режим доступа: https://habr.com/ru/company/ruvds/blog/517638/

25. Jarvis, J. Fascinating & Frightening Shodan Search Queries. [Electronic resource] / Jake Jarvis // The Medium. – May 10, 2019. – Access: https://jakejarvis.medium.com/fascinating-frightening-shodan-search-queries-aka-the-internet-of-sh-t-90d5fa0ffa79

26. The Xakep's Blog. What Can The Censys Do, [Electronic resource] // Magazine «ХАКЕР». – January 8, 2016. – Access: https://xakep.ru/2016/01/08/censys

27. Shodan: границы дозволенного или где кончается белая шляпа хакера [Электронный ресурс] // Хабр. – 19 апр. 2021. – Режим доступа: https://habr.com/ru/post/553160/

28. Конвенція про кіберзлочинність. [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/994_575#Text

29. Атакуем веб-приложения. Уязвимость SQLi. Часть 1 – Теория. [Электронный ресурс] // «Убежище Хакера». – 23 июн. 2018. – Режим доступа: https://telegra.ph/Atakuem-veb-prilozheniya-Uyazvimost-SQLi-CHast-1---Teoriya-06-23

30. Greenberg, A. Now You Can Hide Your Smart Home on the Darknet. [Electronic resource] / Andy Greenberg // The WIRED Magazine. – July 2016. – Access: https://www.wired.com/2016/07/now-can-hide-smart-home-darknet/.

31. P S Ajay M., Paulose J. Securing IoT Networks Using an Onion Routing Based Approach / P S Ajay Mishael and Joy Paulose // International Journal of Mechanical Engineering and Technology (IJMET). – March 2018. – Vol. 9, Issue 3. – IAEME Publication. Scopus Indexed – P. 987-990.

32. Левада, Е. Веб-аутентификация: файлы cookies или токены? [Электронный ресурс] / Евгений Левада // Proglib. – 14 авг. 2021. – Режим доступа: https://proglib.io/p/veb-autentifikaciya-fayly-cookies-ili-tokeny-2021-08-14

33. Patel, A. Tor Hidden Services. [Electronic resource] / Akash Patel // San José State University. – Access: https://www.cs.sjsu.edu/faculty/pollett/masters/Semesters/Fall13/akash/Tor_HiddenService.pdf

34. Tor Hidden Services. [Electronic resource] // Altervista Infodrug. – March 8, 2021. – Access: https://monitoringcenterfordrugs.altervista.org/tor-hidden-services/

35. Tor Onion Service Configuration. [Electronic resource] // Home Assistant Community Guides. – May, 2020. – Access: https://community.home-assistant.io/t/tor-onion-service-configuration/195171

ДОДАТОК А

Тези наукових доповідей:

1. Гончаренко Н. А. Dark Web як частина Всесвітньої павутини та його вплив на суспільство. IV Міжнародна науково-практична конференція «Прикладні системи та технології в інформаційному суспільстві» (AISTIS) – Київський національний університет імені Т. Г. Шевченка, 30 вересня 2020.
2. Гончаренко Н. А. Безпека Інтернету речей (IoT) проти пошукового агрегатора Shodan. Всеукраїнська науково-практична Інтернет-конференція «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» – Київ, Державний університет телекомунікацій, 25 лютого 2021.
3. Гончаренко Н. А. Застосування механізмів Dark Web для забезпечення нового рівня захисту IoT. IV Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем» (PCSITS) – Київський національний університет імені Т. Г. Шевченка, 15-16 квітня 2021.
4. Serhii Toliupa, Nataliia Honcharenko, Yuriy Shcheblanin. The Potential Danger of Shodan Search Engine. VIII International conference «Information Technology and Implementation» (IT&I-2021) – Taras Shevchenko National University of Kyiv, December 1-3, 2021.