ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В IOT

Подлісний Г.С., Штангей С.В.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: hlib.podlisnyi@nure.ua,
svitlana.shtanhei@nure.ua

Abstract

The object of the research it the recognition of the current problems in cybersecurity of IoT technologies, such as the lack of reliable operational systems, inadequate security authentication, frivolous approach to confidential information. Also object of the research include potential ways of preventing issues and methods that could be applied in order to avoid any of unpleasant and dangerous threats. This includes usage of encryption, providing more secure network protocols and updating of operational systems and software. The subject of research is to define cybersecurity flaws and problems in IoT systems that exist in current moment and future obstacles that will appear due to fast developing and providing everywhere this technology.

IoT – це система, що складається з взаємопов'язаних комп'ютерних пристроїв, механічних та цифрових машин, які мають унікальні ідентифікатори та мають здатність передавати дані через мережу без участі людини. Майже кожен телефон та комп'ютер приєднаний до мережі інтернет. Не тільки ці пристрої є частиною всесвітньої павутини, але й IoT. Важливим питанням зараз є кібербезпека цих пристроїв, бо без актуального впровадження засобів їх захисту виникає багато загроз конфіденційності, здоров'ю та комфорту життя сучасного користувача .

Найбільш поширеною та руйнівною атакою, яка часто використовує пристрої інтернету речей, є DDoS [2], яка може бути реалізована через зараження великої кількості пристроїв шкідливим програмним забезпеченням. Операційні системи, що були інфіковані, разом утворюють «ботнет», який працює для координації атаки на цільовий сервер. Зафіксувати підозрілу активність допоможе відстеження сегментів трафіку, який надсилає пристрій на транспортному рівні моделі OSI.

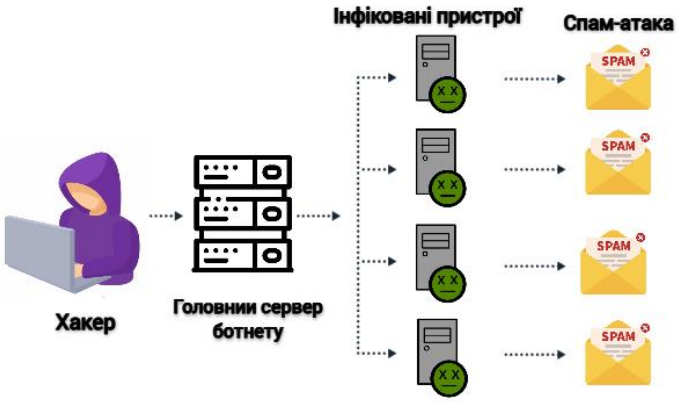

Рис 1 . Схема ботнету

Тільки з 2019 по 2022 рік кількість цих атак зросла на 487%[1]. Захист IoT від зараження шкідливим ПО є складним питанням, бо вони більш вразливі через низку факторів, таких як: нерегулярне оновлення, відсутність захисних програм, необізнаність користувачів, відсутність

шифрування. Прикладом вірусу, що завдав великої шкоди багатьом сервісам, є Mirai Botnet, який зміг об'єднати багато зламаних маршрутизаторів, відеокамер, відеопрогравачів та організував напрямлені DDoS атаки. Такого виду загрози можливо уникнути, використовуючи дуже примітивні, але надійні засоби превентивної безпеки. Користувачі часто не задумаються про надійність паролів, шо є вразливим місцем для звичайного перебору пароля – брутфорсу. В дослідженні від Nordpass[8] був здійснений аналіз найпопулярніших паролів та було знайдено, що понад 4 929 113 користувачів використовували пароль password.Звичайна зміна заводських налаштувань автентифікації ускладнить перебір пароля в рази, адже встановлена попередньо конфігурація не має мету надійності. Іноді достатньо змінити версію програмного забезпечення на більш нову, або знайти патч безпеки для конкретного пристрою. Зазвичай всю потрібну прошивку можливо завантажити із сайту виробника.

Наступною проблемою є відсутність конфіденційності. Це зумовлено тим, що більша частина інтернет трафіку, який генерується IoT, не шифрується. У цьому є деякий сенс, адже процес шифрування може сповільнити працю пристроїв, що спочатку були спроектовані не для безпечної передачі даних, а просто для виконання своєї роботи. До пристроїв, що часто не використовують шифрування, але передають персональну інформацію є камери відеоспостереження, які використовують протокол RTSP. Поширеним протоколом серед пристроїв інтернету речей є MQTT, який не шифрує дані. Такого виду трафік, при перехваті за допомогою утиліт, таких як Wireshark, можуть бути легко зчитані. Це є видом атаки типу MitM, тобто «людина посередині», а саме її різновид - sniffing. Прикладом масового випадку є вірус VPNFilter[5], який у 2018 році інфікував понад 500 тисяч маршрутизаторів та перехоплював персональний трафік користувачів. Також зловмисник може змінити перехоплені дані або додати зайву інформацію, і тоді це буде загрозою packet injection. У випадку IoT – це загроза, адже якщо хакер підробить пакет із сигналом до якогось пристрою, то він може надіслати хибну команду та зупини коректну працю. Є ще декілька версій MitM, як наприклад session hijacking, або «перехоплення сеансу», коли хакер заволодів ідентифікатором сесії і може здійснювати дії від імені користувача. Потенційним рішенням є використання надійних протоколів зв'язку - SSL та TLS, які можуть запобігти простому зчитуванню інформації.

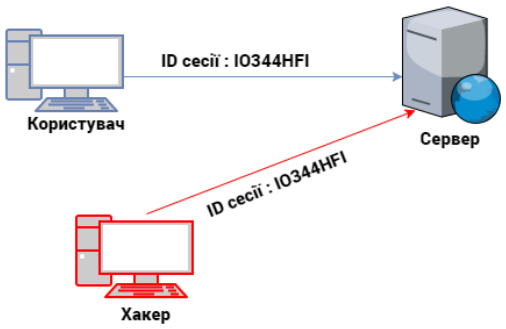

Рис2. Схема атаки session hijacking

Не тільки загроза даним велика проблема, але й порушення інфраструктури країни. IoT широко використовується в промисловості, автоматизації на виробництві та в контролі процесів. Завдяки розумним датчикам, можливо аналізувати велику кількість інформації зі станків заводу, або керувати частинами процесів віддалено. Але це і э проблемою, адже при компрометації таких систем виникають руйнівні наслідки. Прикладом э вірус Triton, що був розроблений хакерами для атаки на контролери безпеки Triconex. Він спроможний на перепрограмування файлу конфігурації, тим самим змінюючи поведінку пристрою. У 2017 році, із його застосуванням, була здійснена атака на нафтохімічну промисловість в ОАЕ [3], в результаті якої виробництво повністю зупинилося на деякий час. Уникнути таких проблем можливо, якщо розроблюється надійне програмне забезпечення, але в сучасному світі, де пришвидшення процесів має ключову роль в розвитку економіки країни, не можливо витрачати багато часу. Використання ненадійних бібліотек програмування та відсутність безпеки центральних серверів, які регулюють працю інтернету речей, пригнічує ситуацію безпеки. Якщо звірятися з прогнозами, вже в 2027 році буде понад 41 мільярд пристроїв IoT[6]. В такому

середовищі, виробники не приділяють великої уваги до кібербезпеки, що в майбутньому призведе до більш руйнівних інцидентів.

Загроза життю теж можлива, адже інтернет речей також використовується в медицині та має назву IoMT. За оцінками, до 2028 року ринок цієї сфери досягне лише в США 446 мільярдів доларів[4]. Через такий стрімкий розвиток, виникає питання шантажу людей. Наприклад маніпулятор може отримати доступ до кардіостимулятора дистанційно та взагалі вбити людину. Проблема полягає в тому, що пристрої такого виду не мають достатньо надійних способів автентифікації. Тобто потенційний зловмисник має змогу керувати пристроєм, начебто він і є власник його. Але охорона здоров'я за допомогою IoMT не обмежується лише кардіостимуляторами, але й розумними датчиками рівня тиску або цукру та фітнес-браслетами. Останні теж можливо зламати та отримати доступ до персональних даних на телефоні[7].

Висновки

IoT проникає в різні сфери нашого життя та трансформує наше суспільство. Основною проблемою інтернет речей є безпека. В доповіді розглянуто проблеми кібербезпеки інформаційних технологій IoT, таких як відсутність надійних операційних систем, автентифікація безпеки та підхід до конфіденційної інформації. Також розглянуто методи, щоб уникнути неприємних і небезпечних загроз. Це включає використання шифрування, забезпечення більш безпечних мережевих протоколів та оновлення операційних систем і програмного забезпечення.

*Л*ітература

1.Зростання прямих DDoS-атак в 2022 році: статистика та тенденції | NWU. *NWU - IT Distributor*. URL: https://nwu.com.ua/bloh/novyny/u-2022-rotsi-zrosla-kilkist-pryamikh-atak-voni-sklali-polovinu-vsikh-ddos-atak (дата звернення: 13.11.2023).

2.What is a DDos Attack?. *Amazon Web Services, Inc*. URL: https://aws.amazon.com/shield/ddos-attack-protection/?nc1=h_ls (дата звернення: 13.11.2023).

3.How does triton attack triconex industrial safety systems?. *Cisco Blogs*. URL: https://blogs.cisco.com/security/how-does-triton-attack-triconex-industrial-safety-systems (date of access: 16.11.2023).

4.Internet of things [iot] in healthcare market size & trends, 2028. *Fortune Business Insights™ | Global Market Research Reports & Consulting*. URL: https://www.fortunebusinessinsights.com/internet-of-things-iot-in-healthcare-market-102188 (date of access: 18.11.2023).

5.Largent W. VPNFilter Update - VPNFilter exploits endpoints, targets new devices. *blog.talosintelligence.com*. URL: https://blog.talosintelligence.com/vpnfilter-update/.

6.Newman P. THE INTERNET OF THINGS 2020: Here's what over 400 IoT decision-makers say about the future of enterprise connectivity and how IoT companies can use it to grow revenue. *Business Insider*. URL: https://www.businessinsider.com/internet-of-things-report?international=true&r=US&IR=T (date of access: 16.11.2023).

7.Nikishaev A. How i hacked Xiaomi MiBand 2 to control it from Linux. *Bitcoin Insider*. URL: https://www.bitcoininsider.org/article/21633/how-i-hacked-xiaomi-miband-2-control-it-linux (date of access: 20.11.2023).

8.Top 200 most common password list 2022. *Securely Store, Manage & Autofill Passwords | NordPass*. URL: https://nordpass.com/most-common-passwords-list/ (date of access: 13.11.2023).