УДК 621.39
DOI: 10.31673/2409-7292.2023.010010

Опанасенко М. І., Поночовний П. М.

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ БОТНЕТ-АТАК У МЕРЕЖАХ IOT

У статті розглядаються атаки відмови в обслуговуванні (DDoS), які відбуваються на мережевому рівні систем IoT, та їх вплив на різні аспекти функціонування мереж. Коротко обговорюються сценарії DDoS-атак з використанням пропускної здатності мереж та з використанням системних ресурсів. Аналізуються методи виявлення ботнетів у мережі IoT.

Ключові слова: ботнет, IoT мережа, DDoS-атака, кібербезпека.

Вступ

Останнім часом концепція Інтернету речей (IoT) є однією з найбільш динамічних у сфері мереж. Вона широко використовується для надсилання та отримання даних через Інтернет, не вимагаючи взаємодії «людина-комп'ютер» або «людина-людина». Слово «речі» стосується мережевих пристроїв (як фізичних, так і віртуальних) із підтримкою IP. Речі можуть включати телеметричні блоки, безпілотні автомобілі, принтери, камери спостереження, планшети, смартфони, засоби зв'язку (UWB), різноманітні датчики (IrDA), ZigBee, центри обробки даних NFC, стільникові та Wi-Fi мережі. Передбачається, що загальна кількість IoT-пристроїв до 2026 року складе до 76,5 мільярдів [1].

Крім Інтернет-протоколу (IP), ці пристрої підтримують декілька інших важливих технологій, зокрема технологію радіочастотної ідентифікації (RFID), датчики, виконавчі механізми, служби GPS, нанотехнології, зв'язок ближнього поля (NFC) і хмарні обчислення.

Незважаючи на те, що ці пристрої включають додатки IoT, вони є невеликими, малопотужними пристроями, що працюють від батареї, і мають різні компроміси дизайну. Ресурси цих пристроїв, як правило, мають обмежені можливості щодо зберігання та обробки інформації, а також обмежені енергетичні можливості через живлення від батарей. Крім того, вони з'єднані через канали зв'язку малої потужності, в уразливих умовах радіозв'язку та без участі людини [2].

Постановка проблеми

Пристрої IoT є джерелом загроз в аспекті кібербезпеки. Використовуючи уразливості системи безпеки пристроїв IoT, хакери можуть створювати ботнети і віддалено або локально перехоплювати управління такими пристроями. Вони також можуть отримувати несанкціонований доступ і змінювати конфіденційні дані, порушувати нормальну роботу мереж IoT або взагалі пошкоджувати IoT. Уразливість може існувати як в апаратних, так і в програмних компонентах IoT [3]. Уразливості апаратного забезпечення важко виявити і набагато важче виправити через різноманітні вбудовані в них мікропрограми. Уразливості програмного забезпечення існують у програмних компонентах IoT, таких як OSec, протоколи зв'язку та інші програми [4].

Ботнет – це сукупність тисяч або навіть мільйонів інфікованих комп'ютерів, кожен з яких називається ботом або зомбі. Простими словами, мільйони ботів разом утворюють бот-мережу, якою дистанційно керують ботмайстри за допомогою командно-контрольного (C&C) сервера. За своєю суттю бот-мережі складаються з великих мереж комп'ютерів-зомбі, які підпорядковуються одному головному комп'ютеру [5]. Виявлення ботів і реагування на них стали значною проблемою для сучасних систем захисту інформації. Створювачі ботів суттєво вдосконалюють свої технології розповсюдження бот-мереж і C&C, щоб уникнути використання найновіших методів виявлення бот-мереж від спеціалістів з IT-безпеки [6].

Аналіз робіт

Безпеці IoT присвячено значну кількість робіт, які зосереджуються на виявленні вразливостей пристроїв IoT, виявленні вразливостей мережі IoT і виявленні ботнетів IoT.

Виявлення вразливостей пристроїв IoT. Статичний аналіз пристроїв IoT є одним із методів, який використовується для виявлення їх вразливостей. Так у [7-8] здійснено масштабний аналіз безпеки 32 тисяч образів мікропрограм вбудованих пристроїв і знайдено 38 невідомих уразливостей у понад 693 образах мікропрограм, які поширюються різні продукти. У [9] проведено статичний аналіз вихідного коду та створено тести на 123 платформах розумного дому та 499 програмах розумних речей. Вони виявили два недоліки в конструкції цих платформ. Ці недоліки дизайну призводять до надання додатку Smart Things привілейованого, а не окремого доступу. Автори також довели, що асинхронний зв'язок (підсистема подій) між пристроями та інтелектуальними додатками небезпечний і може призвести до витоку конфіденційної інформації. У [10] описано, як використати вразливість у частині реалізації протоколу Zigbee light розумних ламп Philips Hue для виконання віддаленого оновлення мікропрограми. Після використання вразливості ключ, який використовувався розумними лампами Philips, було вилучено за допомогою атаки на боковий канал. Цей ключ використовується для шифрування та автентифікації оновлення. Після цього хробак швидко поширився від зараженої лампи до інших ламп за допомогою бездротового зв'язку ZigBee. Така атака дозволяє зловмиснику контролювати міське освітлення або використовувати лампи для здійснення DDoS-атак. Було зроблено кілька досліджень, щоб розробити технології Internet Wide Scan для пошуку вразливих пристроїв IoT. У [11] автори запропонували модель для покращення продуктивності Internet Wide Scanner Zmap.

Виявлення вразливостей мережі IoT. Існує кілька підходів для виявлення вразливостей мережі IoT. У [12] автори запропонували техніку, яка виконує зворотне проектування протоколів IoT, щоб визначити формат повідомлення протоколів і створити повідомлення тестового файлу з певними помилками відповідно до формату повідомлення. Цей метод зменшує розмір тестових файлів, які використовуються в підході Fuzzing. У [13] автори перевірили аналіз ефективності на основі графіка на прототипі системи розумного будинку. Прототип складався зі смартфона, що керує розумною світловою системою, і домашнього динаміка Google. Основна ідея їхнього підходу полягає в тому, щоб побудувати графік трафіку на основі певних вхідних файлів і ідентифікувати корельовані підграфи. Це дозволило їм визначити вразливі місця на основі рівня чутливості різних ключових слів. Вони також продемонстрували, як використовувати вразливі sup-графи для проведення різних атак. Автори публікації [14] проаналізували трафік зашифрованого відеопотоку для систем відеоспостереження та помітили, що шаблон трафіку відрізняється для різних дій користувачів. Це означає, що зловмисник може отримати інформацію про користувача, аналізуючи розмір і швидкість трафіку, навіть якщо трафік зашифрований. У [15] автори досліджували швидкість мережевого трафіку кількох пристроїв IoT і виявили, що пасивні спостерігачі мережі можуть аналізувати мережевий трафік і виводити конфіденційну інформацію.

Мета роботи – дослідити способи та методи виявлення ботнетів у мережі IoT для протидії можливим DDoS-атакам.

Сценарії DDoS-атак

DDoS – це еволюція атаки на відмову в обслуговуванні (DoS), яка є режимом передачі один до одного. Мета полягає в тому, щоб надіслати велику кількість підроблених або безглуздих пакетів на цільовий комп'ютер, вичерпати пропускну здатність мережі та системні ресурси жертви, зупинити або перервати системні служби та запобігти іншим звичайним користувачам отримати доступ до необхідних ресурсів. Однак із розвитком комп'ютерного обладнання та мережевого зв'язку DoS-атаки стали складнішими, тому була розроблена DDoS-атака [16]. Це ботнет, що складається з двох або більше зламаних комп'ютерів, розподілених по всьому світу, які запускають DoS-атаку на ту саму ціль для досягнення мети переривання або зупинки мережевої служби сервера (рис. 1).

Ботнет означає, що хакери використовують троянські віруси або вразливості системи для написання програм DDoS-атаки, перетворюючи інші комп'ютери на зомбі-комп'ютери (BOT) і формуючи контрольні вузли, які можна використовувати для надсилання підроблених або спам-пакетів для блокування мережі цільової мережі.

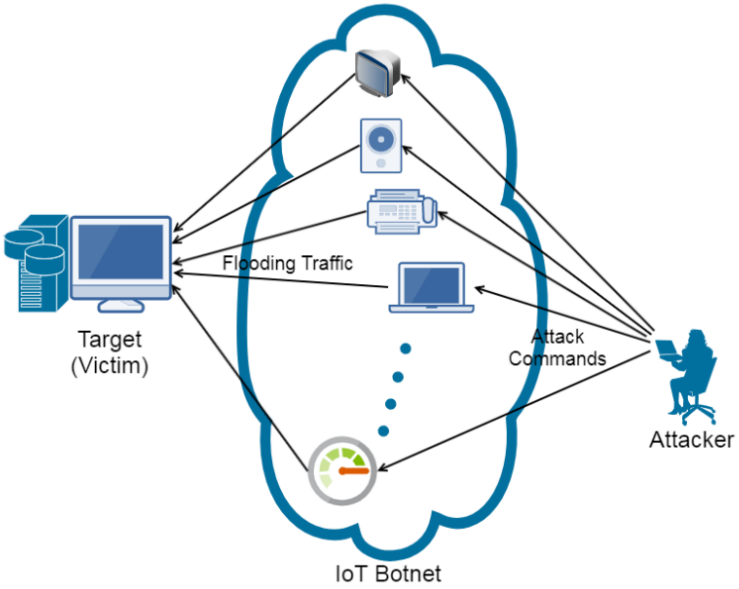


Рис. 1. Принципова схема ботнет DDoS-атаки [16]

1. DDoS-атаки з використанням пропускної здатності мережі

Ботнети передають великі пакети трафіку, щоб використовувати пропускну здатність мережі, тому комп'ютер жертви часто блокується.

Атака Flood на протокол дейтаграм користувача (UDP). При використанні протоколу UDP для передачі пакетів автентифікація не потрібна, і на комп'ютер жертви може бути надіслано велику кількість пакетів, що може перенаситити пропускну здатність і зробити звичайні служби недоступними. Цей метод атаки показаний на рис. 2.

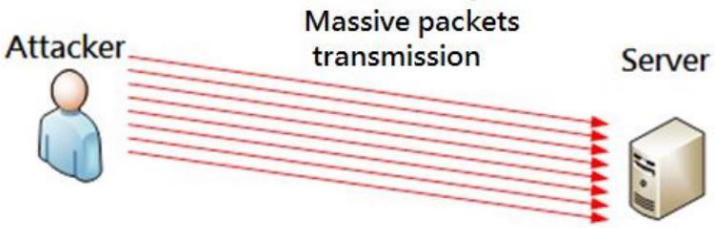


Рис. 2. UDP Flood атака [16]

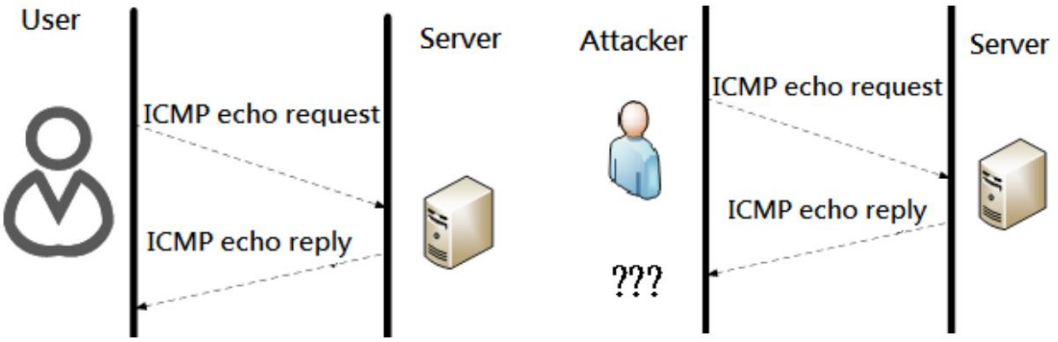
Атака Flood на протокол керуючих повідомлень Інтернету (ICMP). При використанні команди ping клієнт надсилає пакет заголовка exo-запиту ICMP серверу, а сервер надсилає пакет заголовка exo-відповіді ICMP клієнту, щоб перевірити, чи можна правильно встановити з'єднання між ними. Однак, під час атаки ICMP-флуд за короткий час надсилається велика кількість команд Ping на атакований сервер, споживаючи ресурси хост-сервера та викликаючи збій служби (рис. 3).

Teardrop Attack. Кожен пакет сегментується та зміщується перед передачею, а інформація про обробку записується для подальшого збирання пакетів. Teardrop-атака використовує цей метод для підробки інформації про зсув, щоб пакет не міг бути належним чином зібраний, що спричиняє помилки.

2. DDoS-атаки з використанням системних ресурсів

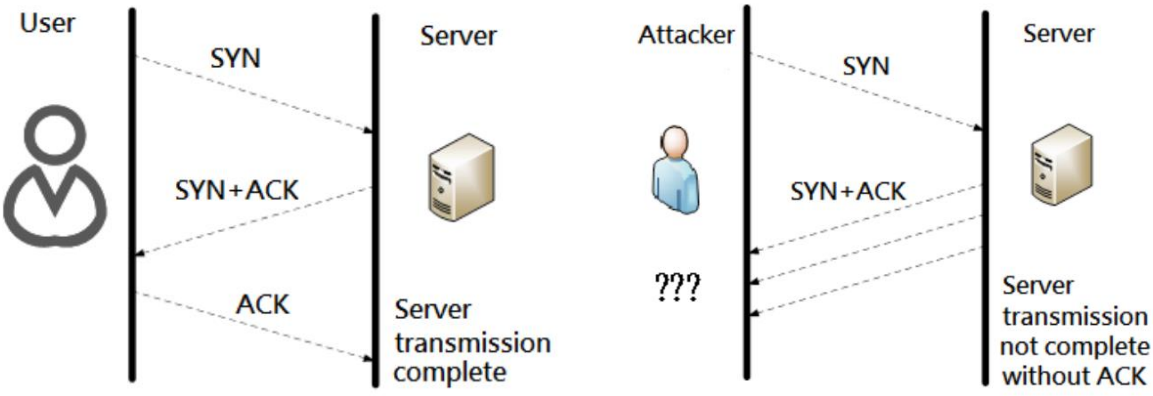
Споживання системних ресурсів спричинене вразливістю системної передачі або фальшивими IP-адресами, які виснажують системну пам'ять або ресурси ЦП і зрештою призводять до призупинення або переривання служби.

Атака SYN Flood. Атаки SYN flood використовують вразливість тристороннього рукостискання між відправником і одержувачем у протоколі керування передачею (TCP). Існує два типи атак SYN flood. Зловмисник може навмисно не повертати інформацію ACK або використовувати підроблену IP-адресу джерела в SYN-флуді, щоб змусити сервер надсилати пакети SYN + ACK на підроблену IP-адресу. Оскільки це підроблена IP-адреса, сервер не може отримати відповідь на пакет ACK і тому сервер надсилатиме пакети SYN + ACK, доки не закінчиться час очікування. Це, у свою чергу, споживає пропускну здатність сервера та ресурси пам'яті. На рис. 4 показано процес тристороннього встановлення зв'язку під час звичайної передачі TCP. У правій частині рисунка показано процес тристороннього встановлення зв'язку під час передачі TCP під час атак SYN flood.



а) нормальний режим б) атака ICMP Flood

Рис. 3. Діаграма атаки ICMP Flood [16]



а) рукостискання у нормальному режимі б) атака SYN Flood

Рис. 4. Діаграма атаки SYN Flood [16]

Атака на локальну мережу (LAND). Основна відмінність від SYN-флуду полягає в тому, що підроблена IP-адреса змінюється на таку ж, як IP-адреса атакуваного хоста. У результаті хост постійно посилає пакети SYN + ACK собі назад, утворюючи нескінченний цикл і споживаючи ресурси атакованого хоста.

Атака DNS Flood. DNS flood – це мережева атака на DNS. Надсилаючи довільно згенеровані DNS-запити до DNS-сервера через бот-мережі, сервер не може знайти відповідні імена субдоменів, що спричиняє переривання служби DNS.

Методи виявлення ботнетів у мережі IoT

Основні методи з виявлення ботнетів IoT можна класифікувати на: виявлення на основі аномалій, на основі сигнатур, на основі специфікацій та на основі гібридного виявлення.

На основі аномалії. Цей підхід виявляє ботнет IoT шляхом розпізнавання аномальної поведінки в мережі. Для досягнення цієї мети необхідно заздалегідь профілювати нормальну поведінку мережі IoT. У [17] автори розробили метод на основі аномалії надлегкого пакета для виявлення ненормального корисного навантаження в пакеті, використовуючи ефективну техніку зіставлення для бітового шаблону, що вимагає лише операції ADD з наступним інкрементним лічильником, і реалізовано як таблицю пошуку для швидкого та гнучкого оцінювання пакетів. У [18] запропоновано AutoBotCatcher, який використовує концепцію ланцюга блоків для виявлення децентралізованих ботнетів P2P. Базуючись на тому факті, що IoT-боти в одній бот-мережі зазвичай спілкуються один з одним, AutoBotCatcher розроблено для виявлення пристроїв бот-мережі та позначення їх як однієї спільноти шляхом аналізу обміну мережевим трафіком між різними пристроями. AutoBotCatcher використовує агентів для моніторингу трафіку, який обмінюється між пристроями IoT. Ці агенти повідомляють інформацію, яку вони збирають як транзакцію ланцюга блоків, великому довіреному об’єкту в мережі, що називається генератором блоків, який моделює взаємну контактну інформацію пристрою IoT як граф взаємних контактів. Потім він використовує метод Лувена [19] для визначення спільноти ботнетів на основі графа.

Недоліки поведінкового методу – помилкові сигнали при непередбачуваній поведінці користувачів; хибні спрацьовування за непередбачуваної мережевої активності; часові витрати на етапі навчання системи.

На основі сигнатур. Автори [20] запропонували систему виявлення ботнета IoT на основі сигнатур, яка використовує технологію системи виявлення вторгнень (IDS), яка зазвичай використовується для моніторингу мереж на відомі шкідливі дії та порушення політики на основі збігів сигнатур атак. У їхній системі модулі IDS налаштовані на роботу в гібридному режимі. Модуль виявлення та брандмауер під назвою Router IDS і спрощений модуль моніторингу під назвою Detector IDS. Ці модулі розповсюджуються в мережі пристроїв Інтернету речей, що не потребує модифікації програмного забезпечення на датчиках чи пристроях. Detector IDS реєструє мережевий трафік і надсилає його до IDS маршрутизатора, який виявляє шкідливу поведінку вузла, якщо вона схожа на відому атаку. У [21] запропоновано підхід на основі хоста під назвою BotRevealer для виявлення ботнета IoT на ранньому етапі зараження, використовуючи життєвий цикл ботнета як загальну сигнатуру для виявлення. Вони аналізують запущений процес і мережеву активність на хості на основі статистичних характеристик послідовності пакетів і порівнюють їх із моделлю поведінки трафіку ботнета.

Недоліки сигнатурного методу – необхідність оновлювати бази сигнатур виявлення нових атак; неможливість виявлення атак, які не описані в експертній системі; неможливість виявити атаки, що відрізняються від сигнатурного опису або без опису.

На основі специфікації. Цей підхід схожий на підхід на основі аномалій, але враховує специфікації системи. У [22] запропоновано техніку автоматичного втручання для специфікацій мережевого протоколу зловмисного програмного забезпечення, використовуючи зразки зв’язку зловмисного програмного забезпечення та двійкові файли зловмисного програмного забезпечення. Оскільки кожне зловмисне програмне забезпечення має власний двійковий формат, а кожен протокол C&C має власне сімейство зловмисних програм, це забезпечить шаблон для структури зловмисного програмного забезпечення. Автори запропонували поле системи типів повідомлення, яке описує всі типи полів у

© Опанасенко, М. І., & Поночовний, П. М. (2023). Технологія забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock. Сучасний захист інформації, 1(53), 72–78. https://doi.org/10.31673/2409-7292.2023.010010.

повідомленні, а потім використовує алгоритм інтерференції типів для втручання в структуру повідомлення. Оскільки більшість мережевого трафіку C&C зашифровано, тому вони застосовують динамічний аналіз трафіку для вилучення системних ключів C&C. У [23] автори запропонували техніку виявлення для ботнетів IoT на етапі розповсюдження зловмисного програмного забезпечення, коли заражені пристрої починають використовувати інші пристрої в мережі, використовуючи стратегію атаки грубою силою.

Недоліки методу на основі специфікації – хибні спрацьовування пристроїв IoT за непередбачуваної мережевої активності; тривалий час навчання системи.

На гібридній основі. Виявлення ботнета IoT на гібридній основі зазвичай використовує два підходи виявлення. Наприклад, виявлення ботнета IoT на основі сигнатур можна поєднати з виявленням ботнета IoT на основі аномалій або з підходом на основі специфікацій. Це має перевагу мінімізації частоти хибно-позитивних і хибно-негативних результатів системи виявлення. У [24] запропоновано систему виявлення ботнета IoT із низьким енергоспоживанням і сигнатурами та використання методів теорії ігор, щоб вирішити, чи потрібен агент IDS для активації виявлення аномалії чи ні. Таким чином, підвищення точності виявлення при зниженні енергоспоживання в пристрої IoT. Ще одна гібридна система виявлення була запропонована у [25]. Ця система поєднує в собі моделі виявлення вторгнень на основі аномалій і специфікацій для виявлення атак в IoT. Агент виявлення на основі специфікацій буде розташований на вузлах маршрутизаторів; він аналізуватиме поведінку хост-вузла та надсилатиме результати на кореневий вузол, де розташований агент виявлення аномалій. Цей агент базується на архітектурі Map reduce і використовує алгоритм оптимального шляху, використовуючи дані, надіслані маршрутизаторами, для проектування моделі кластеризації та виявлення зловмисної поведінки за допомогою механізму голосування [26].

Недоліки гібридного методу полягають у поєднанні недоліків методів, які застосовуються, за виключенням скомпенсованих.

Висновок

Зі швидким впровадженням пристроїв Інтернету речей у наше повсякденне життя зростає занепокоєння щодо використання вразливостей цих пристроїв для створення бот-мереж Інтернету речей і здійснення різних типів атак. DDoS-атаки, що походять від бот-мереж Інтернету речей, становлять неминучу загрозу для сучасного Інтернету через здатність зловмисників генерувати великий обсяг пакетів із мільйонів скомпрометованих пристроїв Інтернету речей.

Основні методи з виявлення ботнетів IoT класифікуються на: виявлення на основі аномалій, на основі сигнатур, на основі специфікацій та на основі гібридного виявлення. Ці методи мають численні переваги, але включають і недоліки, які не можуть бути компенсовані навіть при їх поєднанні.

Перелік посилань

1. Statistical Portal. Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (in Billions). Available online: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.
2. Dambaye, S.S.; Kolhe, M.V.L. A Survey: Managing Resource-Constrained Devices in IoT. Int. J. Innov. Res. Comput. Commun. Eng. 2016, 4, 21011–21015.
3. Al-Haija, Q.A. On the Security of Cyber-Physical Systems Against Stochastic Cyber-Attacks Models. In Proceedings of the 2021 IEEE International IoT, Electronics, and Mechatronics Conference (IEMTRONICS), Toronto, ON, Canada, 21–24 April 2021; pp. 1–6.
4. Al Dalaien, M.N.; Bensefia, A.; Hoshang, S.A.; Bathaqili, A.R.A.; Xu, X.; Mohanan, V.; Budiarto, R.; Aldmour, I. Internet of Things (IoT) Security and Privacy. In Powering the Internet of Things with 5G Networks; Mohanan, V., Budiarto, R., Aldmour, I., Eds.; IGI Global: Hershey, PA, USA, 2018; pp. 247–267.
5. Albulayhi, K.; Sheldon, F.T. An Adaptive Deep-Ensemble Anomaly-Based Intrusion Detection System for the Internet of Things. In Proceedings of the 2021 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, 10–13 May 2021; pp. 187–196.

6. Abu Al-Haija, Q.; Al-Dala'ien, M. ELBA-IoT: An Ensemble Learning Model for Botnet Attack Detection in IoT Networks. J. Sens. Actuator Netw. 2022, 11, 18. https://doi.org/ 10.3390/jsan11010018

7. Basheer Al-Duwairi, Wafaa Al-Kahla, Mhd Ammar AlRefai, Yazid Abdelqader, Abdullah Rawash,Rana Fahmawi. SIEM-based detection and mitigation of IoT-botnet DDoS attacks. International Journal of Electrical and Computer Engineering (IJECE), Vol. 10, No. 2, April 2020, pp. 2182–2191

8. A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti. A Large-Scale Analysis of the Security of Embedded Firmwares. In 23rd {USENIX} Security Symposium ({USENIX} Security 14), pages 95–110, 2014.

9. E. Fernandes, J. Jung, and A. Prakash. Security Analysis of Emerging Smart Home Applications. In 2016 IEEE Symposium on Security and Privacy (SP), pages 636–654. IEEE, 2016.

10. E. Ronen, A. Shamir, A. Weingarten, and C. O'Flynn. IoI Goes Nuclear: Creating a Zigbee Chain Reaction. In 2017 IEEE Symposium on Security and Privacy (SP), pages 195–212. IEEE, 2017.

11. H. Kim, T. Kim, and D. Jang. An Intelligent Improvement of Internet-Wide Scan Engine for Fast Discovery of Vulnerable IoT Devices. Symmetry, 10(5):151, 2018.

12. J. Luo, C. Shan, J. Cai, and Y. Liu. IoT Application-Layer Protocol Vulnerability Detection Using Reverse Engineering. Symmetry, 10(11):561, 2018.

13. Y. Jia, Y. Xiao, J. Yu, X. Cheng, Z. Liang, and Z. Wan. A Novel Graph-based Mechanism for Identifying Traffic Vulnerabilities in Smart Home IoT. In IEEE INFOCOM 2018-IEEE Conference on Computer Communications, pages 1493–1501. IEEE, 2018.

14. H. Li, Y. He, L. Sun, X. Cheng, and J. Yu. Side-Channel Information Leakage of Encrypted Video Stream in Video Surveillance Systems. In IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications, pages 1–9. IEEE, 2016.

15. N. Apthorpe, D. Reisman, and Nick Feamster. A Smart Home is no Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. arXiv preprint arXiv:1705.06805, 2017.

16. Shu-Hung Lee, Yeong-Long Shiue, Chia-Hsin Cheng, Yi-Hong Li, and Yung-Fa Huang. Detection and Prevention of DDoS Attacks on the IoT. Appl**. Sci.** 2022, 12(23), 12407; https://doi.org/10.3390/app122312407

17. D. Summerville, K. M. Zach, and Y. Chen. Ultra-Lightweight Deep packet Anomaly Detection for Internet of Things Devices. In 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), pages 1–8, Dec 2015.

18. G. Sagirlar, B. Carminati, and E. Ferrari. Autobotcatcher: Blockchain-based P2P Botnet Detection for the Internet of Things. CoRR, abs/1809.10775, 2018.

19. V. Blondel, J. Guillaume, R. Lambiotte, and E. Lefebvre. Fast unfolding of communities in large networks. Journal of Statistical Mechanics: Theory and Experiment, 2008(10): P10008, oct 2008.

20. P. Ioulianou, V. Vasilakis, I. Moscholios, and M. Logothetis. A Signature-based Intrusion Detection System for the Internet of Things. 2018.

21. H. R. Shahriari and E. Khoshhalpour. Botrevealer: Behavioral Detection of Botnets based on Botnet Life-Cycle. The ISC International Journal of Information Security, 10(1):55–61, 2018.

22. L. De Carli, R. Torres, G. Modelo-Howard, A. Tongaonkar, and S. Jha. Botnet Protocol Inference in the Presence of Encrypted Traffic. In IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, pages 1–9, May 2017.

23. A. O. Prokofiev, Y. S. Smirnova, and V. A. Surov. A Method to Detect Internet of Things Botnets. In 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pages 105–108, Jan 2018.

24. H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri. A Lightweight Anomaly Detection Technique for LowResource IoT Devices: A Game-Theoretic Methodology. In 2016 IEEE International Conference on Communications (ICC), pages 1–6, May 2016.

25. H. Bostani and M. Sheikhan. Hybrid of Anomaly-based and Specification-based IDS for Internet of Things Using Unsupervised OPF based on MapReduce Approach. Computer Communications, 98:52–71, jan 2017.

26. Basheer Al-Duwairi, Wafaa Al-Kahla, Mhd Ammar AlRefai, Yazid Abdelqader, Abdullah Rawash, Rana Fahmawi. SIEM-based detection and mitigation of IoT-botnet DDoS attacks. International Journal of Electrical and Computer Engineering (IJECE.), Vol. 10, No. 2, April 2020, pp. 2182–2191.

Надійшла: 04.01.2023 Рецензент: д.т.н., професор Вишнівський В.В.