УДК 621

Н.В. ГРИПИНСЬКА, Н.І. ПРАВОРСЬКА
Хмельницький національний університет

ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІД ЧАС ВПРОВАДЖЕННЯ ІНТЕРНЕТУ РЕЧЕЙ

Інтернет речей активно впроваджується в сучасному інформаційному просторі. Інтернет речей – це об'єднання великої кількості пристроїв з різним за обсягом програмним забезпеченням автономних пристроїв. В сучасному інформаційному середовищі визначають п'ять типових видів зловмисників, що можуть взаємодіяти з IoT. В статті наведено основні засади забезпечення безпеки IoT, що мають бути забезпечені в ході проектування та експлуатації систем IoT.

Ключові слова: безпека, інформаційний простір.

N.V. GRYPYNSKA, N.I. PRAVORSKA
Khmelnytsky National University

IMPLEMENTATION OF CYBER SECURITY OF INTERTET-OF-THING

Internet of things is actively being implemented in the modern information space. Internet of things are a combination of a large number of devices with different sizes of autonomous software. In today's information environment, there are five typical types of intruders that can interact with IOT. The article provides the basic principles of security of IOT that must be ensured in the design and operation of IOT systems. Analysis of cyber attacker shown. Also discovered problems with authorisations in IoT devices with common types of logins and passwords. Magnificent increasing of IoT and IoT's net bring new types of botnets and attacks.

It is shown common rules to increase security level of IoT devices to protect IoT and IoT nets against attacks. Due to increasing of program code size new technologies to check IoT's codes required. Certification can be a key to reach required level of safety and protection level.

Keywords: security, information space.

Вступ. Кевін Ештон, що є співзасновником Auto-ID Center, першим ввів термін «Інтернет Речей», саме так він назвав свою доповідь для «Procter & Gamble» в 1999 році. Це була спроба впровадити нову ідею радіочастотної ідентифікації (RFID) в ланцюг поставок виробничих товарів, а в результаті привернуло гарячу увагу до самої ідеї підключення до мережі нових типів пристроїв.

Розробками в сфері досліджень і стандартизації інтернету речей займаються багато країн на рівні національних ініціатив, наприклад ANSI (США), BSI (Великобританія), ETSI (Європа),а також на рівні інтернаціональному: ITU, ISO, IEC.

У сфері бізнесу існує EPCglobal – ініціатива GS1з розвитку індустрії стандартів для електронного коду продукту (EPC), створена для підтримки використання RFID у виробництві, що дозволить у майбутньому об'єднати в мережу масову продукцію для постійного моніторингу та контролю якості споживчих товарів.

Інтернет речей (Internet of things, IoT) має великий вплив на наше життя – 5 мільярдів пристроїв зараз і 25 мільярдів до 2020 року [1] – від управління інфраструктурою та фабриками до машин легеневого серця та безлічі інших медичних пристроїв у наших лікарів офіси та лікарні, пристрої в наших автомобілях та будинках. Станом на 2018 рік вже вироблено більше 50 мільярдів контролерів типу ARM різними

Але це не безпечно. Одна з оцінок розвитку інтернету речей надає економічний ефект в межах 3,9 трлн до 11,1 трильйона доларів на рік до 2025 році. Фактичний вплив буде залежати від прийняття рішень підприємствами та споживачами. Безпека стане ключовим елементом цього прийняття – і вартості бізнесу.

Захист рішень на базі IoT від тих, хто планує завдати шкоди, буде мати вирішальне значення для зростання IoT, а також для особистої та ділової безпеки.

Постановка проблеми дослідження

Атакуючі користувачі, ймовірно, шукатимуть можливості поставити під загрозу критичну інфраструктуру кожної країни, а також пов'язану набагато ширшими зв'язками екосистему споживчих та промислових пристроїв, відомих як інтернет речей. Інтернет речей з'єднує мільярди нових пристроїв з інтернетом, але це також розширює потенціал атаки кібер-дійових осіб проти мереж та інформації. Дослідники з безпеки продовжують розкривати вразливі місця у споживацьких продуктах, включаючи автомобілі та медичні прилади. Якщо атакуюча сторона отримає можливість створювати значні фізичні ефекти в обраній країні через кібер-засоби, вони отримають нові можливості для примусу та стримування. Наприклад, кібератака на українську енергетичну мережу в 2015 році призвела до відключення живлення протягом декількох годин.

Широке включення "розумних" пристроїв у повсякденні об'єкти – це зміна того, як люди та машини взаємодіють між собою та навколишнім світом, часто підвищуючи ефективність, зручність та якість життя. Їх розгортання також приводило до появи нових вразливих місць як в інфраструктурі, яку вони підтримують, на яку вони покладаються, так і на процеси, якими вони керують.

Кібер-хакери вже використовували пристрої IoT для розповсюджених атак на відмову від обслуговування (DDoS), і ми оцінюємо їхнє продовження. У майбутньому державні та недержавні агенти скоріше за все використовуватимуть пристрої IoT для підтримки розвідувальних операцій або внутрішньої

безпеки або для доступу або нападу цільових комп'ютерів мережі.

Проблема безпеки в інтернеті речей

Мільйони пристроїв вже підключені через інтернет та в приватних хмарах. Gartner та інші прогнозують до 2020 року 25 мільярдів підключених пристроїв. При першій появі інтернету речей в 2013 році, навіть поважна безпека Oxford Dictionary як предмет свого першого прикладу, що визначає Internet of Things наступним чином [2]: "Взаємозв'язок через інтернет обчислювальних пристроїв, вбудованих в повсякденні об'єкти, що дозволяють їх для надсилання та отримання даних. "Якщо одне не може перешкоджати інтернету речей, щоб трансформувати те, як ми живемо та працюємо, це буде розбиттям безпеки". Два останніх прикладу демонструють вразливі місця у промислових та комерційних програмах.

1) Сталеві млини: нападники вразили металургійний комбінат у Німеччині, маніпулюючи та руйнуючи системи управління та запобігаючи зупиненню доменної печі регульованим способом, що призвело до "масових пошкоджень". Нападники використовували атаку з метою отримання доступу через ділову мережу заводу, потім прокладали шлях до виробничих мереж, що контролювали устаткування підприємства [4]

2)комерційна посудомийна машина, яка може бути підключена до інтернету, включає в себе вбудований веб-сервер, який "прослуховує порт 80 і схильний до атаки переходу по каталогу; отже, неаутентифікований зловмисник може використати цю проблему для доступу до конфіденційної інформації для наступних атаках " [5].

Доповідь Конгресу дослідницьких служб (CRS) від 2014 року до Конгресу США визначила п'ять типів зловмисників:

1) "Кібертерроризми": "Спонсоровані державою та недержавні актори, які беруть участь у кібератаках як форма війни. Транснаціональні терористичні організації, бойовики та джихадисти використовували інтернет як інструмент планування атак, радикалізацію та вербування, метод розповсюдження пропаганди та засоби комунікації ".

Експеримент DHS Aurora передбачав комп'ютерну атаку на систему управління генератором енергії, яка призвела до припинення операцій та знищення обладнання.

2) Кібершпигуни: "Особи, які викрадають секретну або конфіденційну інформацію, якою користуються уряди або приватні корпорації, щоб отримати конкурентну стратегічну, безпечну, фінансову чи політичну перевагу". У звіті ФБР за 2011 рік зазначено: "Компанія стала жертвою вторгнення та втратила 10 років вартості досліджень і розробок, вартість якої становила 1 мільярд доларів – майже на добу".

3) Киберзахоплення: "Особи, які займаються незаконними кібератаками для отримання грошової вигоди". Важко оцінити, але щорічні глобальні витрати для приватних осіб складають сотні мільярдів доларів (і втрата довіри клієнтів).

4) Кіберагенти: Кіберагенти – це агенти або квазіагенти національних держав, які розвивають свої можливості та здійснюють кібератаки для підтримки стратегічних цілей країни ". У серпні 2012 року серія кібер-атак була спрямована проти Саудівської фірми Арамко, найбільшого у світі виробника та нафтогазової промисловості . Напади спричинили спустошення 30 тисяч комп'ютерів компанії, а сам програмний код вірусу, мабуть, покликаний порушити або зупинити виробництво нафти. Деякі співробітники служби безпеки заявляють, що Іран, можливо, підтримав цю атаку.

5) Кібер-хактивісти: "Особи, які виконують кібер-атаки для задоволення, або за філософськими чи іншими негрошовими міркуваннями".

Порівняння атак на пристроях та системах IoT

Атака може бути спрямована на рішення на базі IoT – викрасти дані з пристроїв або серверів або призвести до неправильного поводження пристроїв та заподіяння шкоди пристрою. Також може бути атака з системи IoT за допомогою інших пристроїв IoT для запуску атак на інші IoT пристрої або на інший сегмент інтернет мережі. Оскільки "речі" пов'язані, IoT включає в себе всю інфраструктуру будь-якого рішення IoT, а не лише пристроїв, а також:

- шлюзи, сервери та канали зв'язку, які забезпечують, контролюють та управляють речами;
- всі персональні комп'ютери в цих мережах, з їх вразливими місцями, фактично є точкою доступу для шкідливих програм, щоб атакувати IoT.

Mirai-botnet – масова атака в IoT мережі

В серпні 2016 року було зафіксовано масове ураження Mirai – шкідливим програмним забезпеченням, яке сканує інтернет речей (наприклад, камеру відеоспостереження, дитячий монітор, відеореєстратор, маршрутизатор), яка використовує один із 62 відомих за замовчуванням імен та паролів та їх комбінацій (наприклад, root / root, admin / admin, root / admin і т. д.), атакує пристрій та заражає його Mirai-вірусом для подальшого розповсюдження. Після зараження пристрій відслідковує сервер команд і керування, який керує пристроєм, щоб почати атаку на відмову в обслуговуванні (DoS).

Примітно, що вірус Mirai уникає пристроїв з адресами, виділеними Міністерству оборони США, Поштовій службі США, інтернет-корпорації присвоєння імен та номерів (IANA), GE та HP; виявляє "конкуруюче" шкідливе програмне забезпечення та вилучає його з пам'яті; і блокує віддалене адміністрування портів, намагаючись уникнути перешкод від іншого шкідливого програмного забезпечення або відновлення. Після встановлення ботнету Mirai, зловмисник запускає атаку розподіленої служби відмови (DDoS: атака DoS від багатьох машин), яка підриває ціль, перевантажуючи ресурси, щоб завадити

обслужити служити важливі запити [7–10].

22 вересня 2016 року вірус Mirai був використаний для запуску великої атаки DDoS яка оцінена в 620 гігабіт на секунду, проти відміченого сайту безпеки KrebsOnSecurity, змусивши його відключитись протягом чотирьох днів. 21 жовтня 2016 року Mirai був використаний для запуску DDoS-атаки з ~ 100,000 зловмисних кінцевих точок (переважно IoT-пристроїв) (камери відеоспостереження) на ключовому інтернет-провайдері компанії Dyn Corporation з оцінкою пропускної здатності 1,2 терабіти в секунду. Ця атака припинила понад три години роботу Airbnb, Amazon, BBC, CNN, DirecTV, Etsy, Fox News, GitHub, Netflix, NHL, Reddit, The New York Times, PayPal, Pinterest, Spotify, Starbucks, Tumblr, Twitter і багато інших.

У листопаді 2016 року атака Mirai призвела до відключення маршрутизаторів для 900 000 клієнтів Deutsch Telekom у Німеччині. Це лише деякі з атак на Mirai нападників викликаних копіюванням включені шляхом випуску вихідного коду для Mirai на форумі хакерів, а потім на популярному сайті open source розміщення коду GitHub, і лише один приклад з десятків основних бот-мереж з тисячами варіантів.

Найперші ботнети з'явилися в 1999 році і використовували інтернет-реляційний чат для спілкування з їхніми серверами. Крім атак DDoS, бот-мережі використовуються для розповсюдження спаму та іншого шкідливого програмного забезпечення, вилучення конфіденційної інформації, такої як інформація про кредитні картки, рекламу на завантаження та інші сайти, а також генерування біткойнів [9].

Botnot Ponmocup, згідно з детальним 40-сторінковим звітом від компанії Fox IT, є основою для великої екосистеми із добре утримуваною інфраструктурою та підтримкою в інтернеті. Він включає принаймні 25 плагінів та 4000 варіантів. Очікується, що в 2011 році на її піці активності вдалося контролювати 2,4 мільйони машин і вкрасти мільйони доларів.

Цей аналіз Mirai та інших бот-мереж ілюструє кілька моментів:

- Зловмисне програмне забезпечення на пристроях IoT може використовуватися для створення атак на інші пристрої в інтернеті, включаючи сервери та інфраструктуру інтернету.
- Код атаки може бути досить складним, включаючи наступальні заходи, спрямовані на інше зловмисне програмне забезпечення та захисні заходи для запобігання його вилученню, його захист та плутанини аналітиків.
- Результати можуть бути надзвичайно руйнівними та мати фінансові наслідки.

Mirai-botnet – масова атака в IoT мережі

Наприкінці 2016 р. Д-р Йоганнес Ульріч [16] в інтернет-Storm Center здійснив простий експеримент. Доктор Ульріч підключив відеореєстратор із загальним ім'ям користувача та паролем до звичайного кабельного модема і захопив всі пакети, що йдуть і виходять з відеореєстратора (блокування будь-якого вихідного трафіку, який би атакував інші системи) (рис. 1).

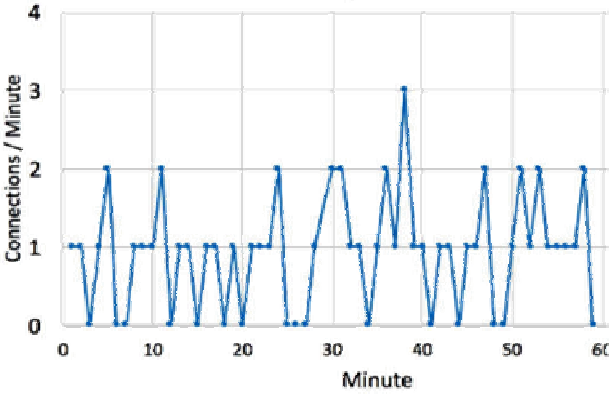

Рис. 1. Підключення до відео реєстратора [16]

Перша спроба входу в відеореєстратор сталася в першу хвилину підключення. Протягом першої години там були 54 унікальних спроби, приблизно одна за хвилину.

Атака на пристрій відбувалась за типовим алгоритмом:

- Спроба декількох логінів, поки не буде успішною.
- Запуск команди, щоб спробувати виявити з'єднання з загальним підключенням.
- Спроба створити бінарний файл. Якщо це вдається, завантажте шкідливе програмне забезпечення (наприклад, бот).
- Сканування для інфікування інших (у цьому випадку з швидкістю > 100 з'єднань за секунду).
- З'єднання зі своїм майстром.

Основні засади забезпечення безпеки

Проектування систем IoT для забезпечення безпеки – це спосіб життя з завданнями на всіх етапах життєвого циклу. Більшість із цих завдань значною мірою пов'язані з дизайном та розробкою програмного коду. Отже, основні вимоги що потрібно розглянути, це: 1) запити; 2) загрози, які ви хочете захистити.

Ті, хто пов'язаний з безпекою, повинні збалансувати захист від витрат та час на його забезпечення. Але занадто багато компромісів або забагато винятків призведуть до вразливості системи безпеки платформи IoT. Пристрій запуску повинен бути бути одним із кінців ланцюжка довіри переходячи від пристрою до серверних додатків. А. Справжня безпечна завантаження вимагає апаратного забезпечення.

1. Комунікаційні технології. Шифрування сьогодні є прийнятною частиною будь-якого рішення для безпечного IoT. Але шифрування є складним і має наслідки від апаратного забезпечення до ключового управління. Проте час і витрати на розробку та експлуатацію безпечних комунікацій, достатніх для вирішення запланованих загроз, можна легко занизити.

2. Послуги, мови та інструменти. Слабкі сторони програмного забезпечення у системі та коді є однією з трьох чудових дверей, що призводять до використання вразливостей в роботі IoT. Неадекватні аналізи загроз або вимоги, а також слабкі або невиконані політики та процедури часто призводить до

слабкості програмного забезпечення. Отримання та ретельне використання служб, пов'язаних із безпекою, мов, стандартів дизайну та кодування, а також інструменти, які їх підтримують, можуть здаватися дорогими, доки вартість не призведе до серйозного порушення, якого можна було б запобігти.

3. Сертифікація. Сертифікація безпеки може вимагатись для певного напрямку діяльності. Навіть якщо це не потрібно зараз, усвідомлюючи вимоги щодо сертифікації та включення корисних елементів у практику розробки, вже зараз потрібно створювати безпечні продукти та потенційно підготувати їх до вимог сертифікації в майбутньому

4. Промислова кооперація. Боротьба з хакерами – це асиметрична війна. Співпраця щодо виявлення дефектів, відстеження та спільного використання розробників, навіть конкурентів, стала прийнятною практикою. Так NIST Cybersecurity Framework призвела до розробки основ для організації зусиль щодо впровадження та адаптації практик безпеки в організації.

Незалежно від того, написано цілком однією організацією або в тому числі сторонні операційні системи, проміжне програмне забезпечення, бібліотеки або програми, які використовує продукт, навіть "малі" пристрої можуть мати великі коди.

Кардіостимулятор, що керує серцем людини, може мати 80 000 рядків коду; підключений термостат може використовувати Linux з повним стеком інтернету плюс його додаток; сучасний автомобіль містить понад 100 мільйонів рядків коду. На рис. 2 показано обсяги програмного забезпечення, що використано в ПЗ різних систем [18]

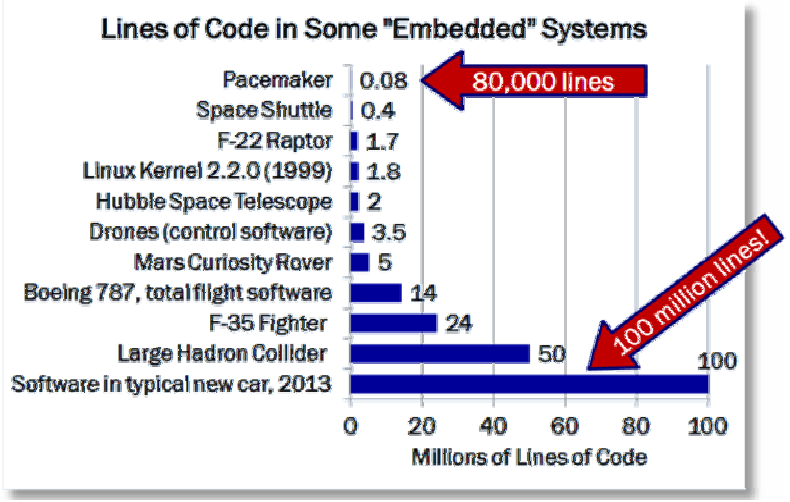

Рис. 2. Типовий обсяг програмного забезпечення у рядках програмного коду [18]

Загрози для безпеки мереж зв'язку поширюються і на IoT, які побудований на них. До них відносяться: несанкціонований доступ, перехоплення даних користувача, порушення конфіденційності, цілісності інформації, DoS-атаки, віруси, експлойтери, мережеві черв'яки тощо. Крім того, існують міжмережеві проблеми аутентифікації, які можуть бути причиною DDoS та DoS-атак.

Висновки

Для інтернету речей стоять ще більш складні проблеми забезпечення безпеки в порівнянні з тими, які характерні для мереж зв'язку. До них додаються можливі проблеми масштабованості мережі, викликані мало передбачуваним обсягом передачі даних від великого числа вузлів, ненадійність програмного забезпечення, тощо.

Широке застосування інтернету речей є результатом інтеграції комп'ютерних технологій, технологій зв'язку і різних областей промислових галузей. Крім порушення інформаційної безпеки традиційних мереж зв'язку (в результаті ризику підслуховування, спотворення інформації, розкриття інформації) пристрої та мережі інтернету речей стикаються з додатковими проблемами безпеки на прикладному рівні – при використанні хмарних обчисленнях, обробці інформації, забезпеченні прав на інтелектуальну власність, захист приватності і т.д.

Мережевий рівень забезпечує доступ, передачу інформації, її обробку та зберігання. Він складається з рівня доступу (мобільні мережі зв'язку) і основного рівня обміну (інтернет, NGN, віртуальні приватні мережі). Більшість сенсорних мереж використовують бездротові мережі зв'язку: персональні мережі (WPAN), локальні мережі (WLAN), міські мережі (WMAN), глобальні мережі (WWAN), а також супутникову мережу. Сенсорні мережі в IoT використовують протоколи зв'язку на основі IP.

У найближчому майбутньому середовище IoT буде безпосередньо причетне до життя простих людей та до бізнесу і державної діяльності. Отже, таку складну структуру необхідно будувати з урахуванням сучасних вимог до інформаційної безпеки. До питання забезпечення захищеності інформації в межах IoT необхідно підходити комплексно і особливо приділяти уваги таким аспектам як безпека кінцевих інформаційних систем і безпека їх взаємодії.

Література

Source: Gartner, Inc. 2014. “Gartner Says 4.9 Billion Connected ‘Things’ Will Be in Use in 2015.” Gartner Newsroom. November 11. http://www.gartner.com/newsroom/id/2905717

Oxford Dictionaries. Accessed April 29, 2017. https://en.oxforddictionaries.com/

Zetter, Kim. 2015. “A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever”. Wired. January 8. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/. Taken from Die Lage der

IT-Sicherheit in Deutschland 2014 (The Situation of IT Security in Germany in 2014).

Bundesamt für Sicherheit in der Informationstechnik (BSI, similar to the Computer Security Division of the Information Technology Laboratory of US NIST).

https://nvd.nist.gov/vuln/detail/CVE-2017-7240.

Congressional Research Service. 2014/ The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress, CRS Report R2984. http://www.fas.org/sgp/misc/R42984.pdf

Wikipedia. “Mirai (malware).” Modified Apr 12, 2017. https://en.wikipedia.org/wiki/Mirai_(malware)

Imperva Incapsula . 2016. “Breaking down Mirai: An IoT DDoS Botnet Analysis” (blog entry). October 26. https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

Barker, C.J. 2016. “Mirai (DDoS) Source Code Review. October

https://medium.com/@cjbarker/mirai-ddos-source-code-review-57269c4a68f

Krebs, Brian. 2017. “3 How Google Took on Mirai.” KrebsOnSecurity . (blog). February 17. (Includes a full analysis.) https://krebsonsecurity.com/tag/ddos/.

Whittaker, Zack. 2016. “Mirai botnet attack hits thousands of home routers, throwing users offline.” November 29. http://www.zdnet.com/article/mirai-botnet-attack-hits-thousands-of-home-routers-throwing-users-offline/

Malwareint. This site tracks several other botnets as well. https://intel.malwaretech.com/botnet/mirai/?t=24h&bid=all

Zawozni, Avishay and Dimi Bekerman . 2016. “1337: 650 Gbps DDoS Attack from the Leet Botnet.” ImpervaIncapsula (blog). December 26. https://www.incapsula.com/blog/650gbps-ddos-attack-leet-botnet.html.

Gamer, Noah. 2015. “The state of botnets in late 2015 and early 2016.” In Simply Security (blog). December 17. http://blog.trendmicro.com/the-state-of-botnets-in-late-2015-and-early-2016/.

Горященко К.Л. Архітектура ARM як потенційна основа грід-інфраструктури наукової бази України / К.Л. Горященко, В.П. Нездоровін, Є. Г. Махрова. Вісник Хмельницького національного університету. – 2012. – №1. – С. 204-208.

Ullrich, Johannes. “The Short Life of a Vulnerable DVR Connected to the Internet.” SANS ISC InfoSecForums . October

Information is Beautiful. New car source: Newcomb, D. 2013. “The Next Big OS War Is in Your Dashboard.” Wired. December 3. http://www.wired.com/2012/12/automotive-os-war/

Горященко К.Л. Риски цілісності інформації на переносних носіях інформації / К.Л. Горященко, О.І. Полікаровських, В.Є. Гавронський, Ю.І. Сніжко // Вісник Хмельницького національного університету. – 2008. – №4. – С. 66-70.

References

1. Source: Gartner, Inc. 2014. “Gartner Says 4.9 Billion Connected ‘Things’ Will Be in Use in 2015.” Gartner Newsroom. November 11. http://www.gartner.com/newsroom/id/2905717

2. Oxford Dictionaries. Accessed April 29, 2017. https://en.oxforddictionaries.com/

3. Zetter, Kim. 2015. “A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever”. Wired. January 8. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/. Taken from Die Lage der IT-Sicherheit in Deutschland 2014 (The Situation of IT Security in Germany in 2014).

4. Bundesamt für Sicherheit in der Informationstechnik (BSI, similar to the Computer Security Division of the Information Technology Laboratory of US NIST).

5. https://nvd.nist.gov/vuln/detail/CVE-2017-7240.

6. Congressional Research Service. 2014/ The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress, CRS Report R2984. http://www.fas.org/sgp/misc/R42984.pdf

7. Wikipedia. “Mirai (malware).” Modified Apr 12, 2017. https://en.wikipedia.org/wiki/Mirai_(malware)

8. Imperva Incapsula . 2016. “Breaking down Mirai: An IoT DDoS Botnet Analysis” (blog entry). October 26. https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html.

9. Barker, C.J. 2016. “Mirai (DDoS) Source Code Review. October

10. https://medium.com/@cjbarker/mirai-ddos-source-code-review-57269c4a68f

11. Krebs, Brian. 2017. “3 How Google Took on Mirai.” KrebsOnSecurity . (blog). February 17. (Includes a full analysis.) https://krebsonsecurity.com/tag/ddos/.

12. Whittaker, Zack. 2016. “Mirai botnet attack hits thousands of home routers, throwing users offline.” November 29. http://www.zdnet.com/article/mirai-botnet-attack-hits-thousands-of-home-routers-throwing-users-offline/

13. Malwareint. This site tracks several other botnets as well. https://intel.malwaretech.com/botnet/mirai/?t=24h&bid=all

14. Zawozni, Avishay and Dimi Bekerman . 2016. “1337: 650 Gbps DDoS Attack from the Leet Botnet.” ImpervaIncapsula (blog). December 26. https://www.incapsula.com/blog/650gbps-ddos-attack-leet-botnet.html.

15. Gamer, Noah. 2015. “The state of botnets in late 2015 and early 2016.” In Simply Security (blog). December 17. http://blog.trendmicro.com/the-state-of-botnets-in-late-2015-and-early-2016/.

16. Horiaschenko K.L. Arhitektura ARM jak potencijna osnova grid-infrastrukturi naukovoї bazi Ukraïni / K.L. Gorjashhenko, V.P. Nezdorovin, Є. G. Mahrova. Visnik Hmel'nic'kogo nacional'nogo universitetu. – 2012. – №1. – S. 204-208.

17. Ullrich, Johannes. “The Short Life of a Vulnerable DVR Connected to the Internet.” SANS ISC InfoSecForums . October

18. Information is Beautiful. New car source: Newcomb, D. 2013. “The Next Big OS War Is in Your Dashboard.” Wired. December 3. http://www.wired.com/2012/12/automotive-os-war/

19. Horiaschenko K.L. Riski cilisnosti informacії na perenosnih nosijah informacії / K.L. Horiaschenko, O.I. Polikarovs'kih, V.Є. Gavrons'kij, Ju.I. Snizhko // Visnik Hmel'nic'kogo nacional'nogo universitetu. – 2008. – №4. – S. 66-70.

Рецензія/Peer review : 20.02.2018 р. Надрукована/Printed :12.05.2018 р.
Стаття рецензована редакційною колегією