J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

A Study on Log Collection to Analyze Causes of Malware Infection in IoT Devices in Smart city Environments☆

김 동 현[1] 신 지 호[2] 서 정 택[3*]
Donghyun Kim Jiho Shin Jung Taek Seo

ABSTRACT

A smart city is a massive internet of things (IoT) environment, where all terminal devices are connected to a network to create and share information. In accordance with massive IoT environments, millions of IoT devices are connected, and countless data are generated in real time. However, since heterogeneous IoT devices are used, collecting the logs for each IoT device is difficult. Due to these issues, when an IoT device is invaded or is engaged in malicious behavior, such as infection with malware, it is difficult to respond quickly, and additional damage may occur due to information leakage or stopping the IoT device. To solve this problem, in this paper, we propose identifying the attack technique used for initial access to IoT devices through MITRE ATT&CK, collect the logs that can be generated from the identified attack technique, and use them to identify the cause of malware infection.

☞ keyword : Smart city, Internet of Things, Malware, Massive IoT, MITRE ATT&CK

1. Introduction

The smart city refers to a state where physical city facilities are combined with information and communication technology (ICTs) technologies, such as internet of things (IoT), to provide efficient city services [1]. It is used in various fields, such as the environment, manufacture, transportation, and security in smart cities, and these services are provided through IoT devices. The network of a smart city is a massive IoT environment, a network environment in which all terminal devices in life are connected to the network to generate and share information [2]. A smart city collects data from IoT devices in the field and performs appropriate work based on the collected data. As all terminal devices in daily life are connected to the network, millions of IoT devices are installed and connected in smart cities and generate vast amounts of data in real time.

In general, most IoT devices are low-power and low-spec, and they do not have the same security functions as general IT systems, so they are quite vulnerable to cyberattacks [3]. It has been proven that IoT devices without basic security measures are vulnerable to cyberattacks due to vulnerabilities such as remote connection port opening, low firmware versions, and plaintext data transmission [3]. The Mirai bot is a representative example of how the vulnerabilities of IoT devices can be exploited. The Mirai bot, which was first released in 2016, accesses IoT devices through remote access protocols, such as SSH and Telnet, and performs a dictionary attack to infect malware. Infected IoT devices identify peripheral devices and repeatedly perform a dictionary attack to form a botnet, which is used for DDoS attacks [4]. As a result of the DDoS attack, nearly 1,200 servers were stopped, allowing us to check possible security threats through IoT devices. In addition to DDoS attacks, attackers can access IoT devices to leak users' sensitive data or run ransomware

1 Dept. of Information Security, Gachon University, Seongnam, 13306, Korea
2 Police Science Institute, Korean National Police University, Asan, 31539, Korea
3 Dept. of Computer Engineering, Gachon University, Seongnam, 13306, Korea
* Corresponding author: Jung Taek Seo (seojt@gachon.ac.kr)
[Received 31 October 2022, Reviewed 8 November 2022(R2 09 January 2023, Accepted 17 January 2023]
☆ This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2021-0-01806, Development of security by design and security management technology in smart factory)
☆ A prelimimary version of this paper was presented at APIC-IST 2022.

to compromise the availability of IoT devices. In a smart city, as the number of IoT devices is vast, the attack targets that can be accessed is expanded, and the risk is higher than in normal conditions. If an IoT device is installed in a smart city and it stops operating, it can cause human and material damage.

It is necessary to respond to cyberattacks such as malware infection on IoT devices in smart cities. However, since millions of IoT devices in the massive IoT environment use heterogeneous hardware, software, protocols, and applications, it is difficult to manage because the same logs are collected in batches, and the number of logs collected is also huge. Even if an IoT device is infected with malware due to these problems, it is difficult to expect a prompt response, and even if the infection is confirmed, the damage is likely to have spread.

This paper proposes a method of collecting logs by limiting the collection log to solve the difficulty of batch log collection stemming from heterogeneous hardware, software, and protocols for IoT devices. To this end, we attempted to overcome the current limitations by analyzing the intrusion process performed to infect existing IoT devices with malware through MITRE ATT&CK and designation of logs generated in the process as the target of collection. The paper makes the following contributions:

- It identifies the cause of infection by analyzing the previously distributed IoT device malware infection method.
- Through the MITRE ATT&CK framework, it reduces the number of collected logs by defining seven initial access techniques and collection logs for the initial access techniques that attackers use on IoT devices.
- A method for collecting logs from IoT devices installed in smart city sites and a collection log format were proposed, and they were divided into 10 specific items. This helps solve the difficulty of collecting identical logs due to the heterogeneity of hardware, software, and protocols of IoT devices installed in smart city sites and improves log management convenience.

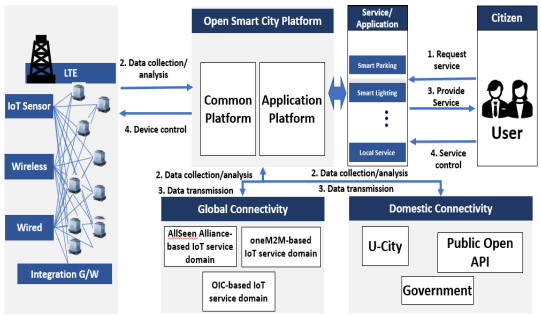
This paper includes four chapters. In Chapter 2, the related research is analyzed. In Chapter 3, the cause of malware infection in existing IoT devices is analyzed and log collection methods and log formats are proposed to identify the cause of malware infection in IoT devices in consideration of the smart city environment. In Chapter 4, the research results and future lines of research are discussed.

2. Background and Related Work

2.1 Background

2.1.1 Smart city Service Architecture

When a user requests a service, a smart city has a structure in which data collected from IoT devices or services are provided through open data [5]. Figure 1 shows the service structure of the smart city environment.

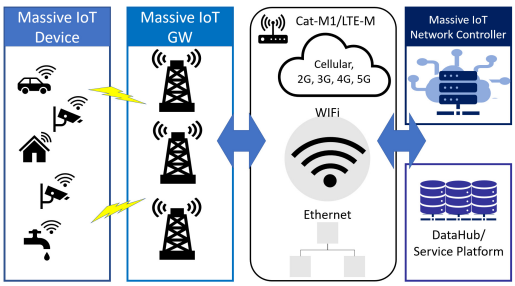


(Figure 1) Smart city service architecture

2.1.2 Smart city IoT Device Data Collection Process

The IoT device performs data collection and control commands in the field, and the gateway serves to deliver the data collected by the IoT device to the IoT controller and service platform through a communication network [6]. Figure 2 shows the process of collecting data from IoT devices in a smart city environment.

In this structure, when an IoT device in the field is infected with malware, the malware can propagate to the central server, gateway, and other IoT devices and DDoS attacks can be performed from infected devices to central servers.



(Figure 2) Massive IoT data collection process

2.1.3 MITRE ATT&CK

MITREATT&CK is accessible to anyone. It serves as a knowledge base that includes information about the attacker's tactics and techniques based on real data. Attack tactics and techniques are divided into Enterprise, Mobile, and ICS. Enterprise represents attack tactics and technologies for general IT systems such as Windows, Linux and etc[7]. Such attack tactics are described in Table 1.

(Table 1) MITRE ATT&CK Tactic [7]

Tactic	Description
Reconnaissance	Information gathering for attack execution
Resource Development	Developing resources to conduct an attack
Initial Access	System initial access tactics
Execution	Malware Execution Tactics
Persistence	Tactics for continuing malicious behavior
Privilege Escalation	Elevate the attacker's privileges for malicious behavior
Defense Evasion	Tactics to evade detection of malicious behavior
Credential Access	Credential theft
Discovery	Gathering intrusion system and network information
Lateral Movement	Peripheral system access through network discovery
Collection	Collecting arbitrary data that attackers want
Command and Control	Perform malicious behavior through the server communication
Exfiltration	Stealing data collected and generated by the system
Impact	Manipulating, interrupting, and destroying system data

Among the attack tactics, initial access refers to attacks being performed through various attack vectors. Representative attack techniques include 'External Remote Services' and 'Default Accounts.' To respond to these attack techniques, MITRE ATT&CK provides mitigation and detection items through which users can detect and mitigate attack techniques. In particular, the detection item can also check information about logs generated through the attack technique.

2.1.4 Collect Log Analysis Through Smart city IoT Device

In this section, we analyze the characteristics of each IoT device used in the services provided by the smart city and describe the data that can be collected based on this. In smart city services, IoT devices are used for smart parking, smart buses, garbage collection management services, smart street lights, and smart crosswalks. These smart services are defined as follows

- Smart parking: Transportation services that support parking, such as vacant seat guidance and parking lot guidance.
- Smart buses: A service that provides users with related information such as bus routes, expected arrival time of destination, and bus arrival time.
- Smart waste management: Environmental services such as real-time monitoring of waste discharge and provision of optimal collection routes.
- Smart lighting: Remotely control street lights so that they operate only when necessary, or they provide crime prevention services through CCTV.
- Smart crosswalk: Pedestrian detection and vehicle stop detection system to prevent traffic accidents near crosswalks.

Table 2 shows whether network communication with IoT devices is used for each of the services provided in the smart city mentioned above and whether collectible data are available in the smart city.

(Table 2) Smart city IoT Device & Sensor Characteristics [8]

Service	IoT Device & Sensor	Generation data
Smart parking	Vehicle detector	Vehicle presence
	Vehicle indicator	Lamp status
Smart bus	OBD-II sensor	Bus status
	Entrance and exit door sensor	Whether to get on or off
	Temperature and humidity sensor	Temperature inside and outside the bus
	Passenger sensor	Number of passengers
	GPS	Bus location
Smart waste management	Garbage load detection sensor	Amount of garbage
	Collection vehicle detection sensor	Collection vehicle location information
Smart lighting:	Light sensor	Ambient light information
	Vehicle traffic and pedestrian detection sensors	Vehicle and pedestrian traffic information
	Environmental sensor	Information such as temperature, humidity and air quality
	CCTV	Video information
Smart crosswalk	Pedestrian detection and car stop sensor	Pedestrian traffic and vehicle stopping information
	Voice guidance assistant	Whether the voice is output normally

2.2 Related Work

Forensic methods against cyberattacks that can occur in IoT devices and a framework for event logging and data collection for IoT devices in the cloud environment has been proposed, but the problem of log collection due to heterogeneous hardware, software, applications, and protocols in a massive IoT environment, such as a smart city, has not been solved.

The study of [10] sought to connect the log and MITRE ATT&CK, and it was possible to identify the attack on the log generated through the SIGMA rule. By using the attack technique ID of MITRE ATT&CK as a log, it was possible to provide more intuitive results.

The study in [11] utilized the MITRE ATT&CK and Cyber Kill Chain to identify evidence of advanced persistent threat (APT) attacks and constructed the attack stages by utilizing logs. It identified evidence of APT attacks through logs and mapped them to each framework to provide attack information. This study confirmed that when MITRE ATT&CK is used, information on cyberattacks can be effectively displayed.

In [12], to address the problem of the inability to apply the existing general IT system's forensic process to IoT, DFIF-IoT, a procedure for analyzing the cause of infection by malware in IoT devices, was proposed. Utilizing the forensic procedure proposed in this study makes it possible to effectively identify the cause of malware infection for IoT devices, but in a massive IoT environment, such as a smart city, analysts cannot analyze each IoT device through the corresponding procedure.

In [13], technologies used in IoT malware in the continuously evolving Linux environment were standardized through MITRE ATT&CK. This study revealed that technologies used in IoT malware could be distinguished through MITRE ATT&CK.

In the previous study, research on forensics for cyberattacks targeting IoT devices and research on identifying and detecting attacks by linking logs with MITRE ATT&CK were conducted. However, existing research cannot solve the difficulties of log collection due to various hardware, software, protocols, and applications of massive IoT, such as smart city, so research is needed to resolve these issues. In this paper, we propose identifying the attack techniques that can be used for initial access to IoT devices through MITRE ATT&CK, collect the logs that can be generated from the identified attack technique, and use it to identify the cause of malware infection.

3. Proposed Log Collection Method

The IoT device in massive smart city IoT environments communicates with the central manager through the network. For network communication, IoT devices and sensors communicate through protocols such as MQTT and LoRa. There are millions of IoT devices in a smart city, and even within the same network, it is difficult to collect the same

logs from all IoT devices using heterogeneous hardware, software, protocols, or applications. Due to these characteristics, the types and numbers of logs generated by millions of IoT devices are vast, so it is difficult to utilize all the logs to determine the cause of malware infection. Considering these issues, this section proposes the minimum number of log items that can be collected and the collection target and method for identifying the source of malware infection in heterogeneous IoT devices.

3.1 Analysis of Existing Malware Infection Causes

In this section, we analyze the infection method of previously distributed IoT malware to analyze the cause of IoT malware infection. The infection methods of nine previously distributed IoT malware were analyzed, and as a result of the analysis, the causes of infection with malware could be divided into 'use of a vulnerable account' and 'software vulnerability'. Malware infection due to the use of vulnerable accounts can be caused by brute force and dictionary attacks on initially set default accounts or short, simple accounts when using remote access protocols such as Telnet and Secure Shell (SSH) for IoT devices. Malware infection due to software vulnerability is caused by downloading malware, which is used to obtain system access rights through vulnerabilities caused by bugs, defects, and design problems in the software and protocols used in IoT devices. It can also mean remote code execution (RCE) that is included in a packet and executed remotely. Table 3 shows the infection causes and methods for malware distributed to IoT devices.

(Table 3) Analysis of infection methods by existing IoT malware

Malware	Infection Method
Aidra	If port 23 is open on the IoT device, access the system using an account vulnerable to the Telnet service.
Bashlite	If port 23 is open on the IoT device, access the system using an account vulnerable to the Telnet service and obtain privileges through ShellShock (CVE-2014-6271).
Bricker	If port 23 is open on IoT devices using Dropbear SSH, accounts vulnerable to Telnet service can access the system through brute force and dictionary attacks.
Hajime	If port 23 is open on the IoT device, access the system using an account vulnerable to the Telnet service.
Mirai	If port 23 is open on the IoT device, access the system using an account vulnerable to the Telnet service.
Persirai	If HTTP port 81 is open on the IoT device, it accesses the IoT device and infects the IoT device with malware through authentication bypass vulnerability, RCE vulnerability, and password file leakage.
Reaper	Attempting to install a bot by targeting IoT devices with specific vulnerabilities and sending data with exploit code inserted.
KiraV2	If port 23 is open on the IoT device, access the system using an account vulnerable to the Telnet service, or use the remote code execution vulnerability (CVE-2017-17215) and the JAWS Web Server remote code execution vulnerability.
Mukashi	If port 23 is open on the IoT device, access the system using an account vulnerable to the Telnet service, or use the remote code execution vulnerability (CVE-2020-9054).

3.2 Log Required for Malware Infection Cause Analysis

The methods of infecting the previously used IoT devices that were analyzed in 3.1 with malware can be divided by using a vulnerable administrator account and a vulnerability. If a weak administrator account is used, log-in attempts increase dramatically as the default account and the vulnerable account (ex: root/root) use a prepared list to launch a brute force attack on the IoT device. When vulnerabilities are exploited, different logs will be recorded according to the system's logging policy. If you access the system using a vulnerability in a Windows operating system (OS), the Window Error Reporting (WER) log may be recorded. Table 4 shows some of the logs used to analyze the causes of malware infection in existing IoT devices.

(Table 4) Some of the logs used to analyze the cause of malware infection [14]

OS	Log	Description
Windows	Last Login	User Last Login Time
	Success/Fail Logons	Account login success/failure history
	RDP Usage	Remote access login history
	WER	Collecting and reporting debugging information when hardware/software errors occur
Linux	wtmp	Recent access and reboot history
	secure	All security records from access attempts
	history	Record commands executed by the user
	Message	System-wide message logging

3.3 Designation of Collection Log Using MITRE ATT&CK

In this section, we identify the attack techniques available for malware infection in IoT devices through the MITRE ATT&CK framework and define the logs that need to be collected.

IoT malware, which was previously distributed, was able to distinguish between vulnerable accounts and software vulnerabilities. However, as countless IoT devices are installed in the field, malware infection methods that have not been previously used can be utilized. Accordingly, considering the operating characteristics of IoT devices installed in smart city sites, we want to select an attack technique that can be used as a malware infection method in the MITRE ATT&CK framework and define logs to be collected according to the attack technique.

To achieve their purposes, attackers breaking into existing IoT devices perform malicious actions, such as DDoS, cryptocurrency mining, information theft and leakage, and data destruction. These malicious actions can be performed after exploiting vulnerabilities in protocols and systems or after breaking into IoT devices through a vulnerable administrator account [15]. This method of accessing the system can be classified as initial access in the MITRE ATT&CK framework. Among the tactics provided by the initial access, it represents an initial access technique for an attack. However, not all initial access attack techniques can be used for IoT devices, and it is difficult to use attack techniques that require interaction with users to attack IoT devices. Among the attack techniques, drive-by-download has the prerequisite of visiting a website, so it is not realistic to apply it to IoT devices that collect data and perform physical operations in smart cities. Even in the case of phishing, interaction with the user is required, so it is difficult to use it to infect IoT devices with malware. Table 5 shows the attack techniques that can be used in IoT devices in in initial access attack techniques in the MITRE ATT&CK framework.

(Table 5) Initial access attack technique of MITRE ATT&CK that can be used for IoT devices

Technique	Description	Availability
Drive-by compromise	Infecting the website with malware and accessing the user's system	X
Exploit public-facing application	Accessing the system by exploiting weaknesses in software, protocols, etc.	O
External remote services	Adversaries may leverage external-facing remote services to initially access and/or persist within a network	O
Hardware additions	Add hardware to make it accessible to attackers	O
Phishing	Sending phishing messages for system access	X
Replication through removable media	System access via removable media	O
Supply chain compromise	Compromising hardware/software in the supply chain, or accessing systems through software dependency tool corruption	O
Trusted relationship	System access through privileged users, organizations, etc.	O
Valid accounts	System access through a valid account	O

In initial access attacks for MITRE ATT&CK, attack methods used for IoT devices can be divided into two forms: physical and network-mediated attacks. The attack technique that physically performs the initial access is hardware addition and replication through removable media, and the remaining attack techniques gain initial access to the IoT device through the network. The logs generated during the MITRE ATT&CK initial access attack technique can be generated from standard user actions, such as USB insertion into IoT devices for updates, accessing IoT devices for software and firmware management, and remote inspection. Therefore, if a log that can be generated through the initial access attack technique is generated and collected, it is considered as being caused by a malicious user. Based on this, it is recommended that the first priority from IoT devices be collected to use it in the process of investigating the cause of malware infection. Table 6 describes the logs to collect.

(Table 6) MITRE ATT&CK's Initial Access Attack Technique Collection Log

Technique	Collection Log Description
Exploit Public-Facing Application	Generate logs due to usage, crashes, errors, etc. of applications used in IoT devices.
External Remote Services	When accessing remote services used by IoT devices, all accounts are considered as malicious users and log is generated for account authentication and access.
Hardware Additions	Logs are generated by considering the addition of hardware such as an external device communication port newly connected to the IoT device installed in the smart city as an act of a malicious user.
Replication Through Removable Media	Connecting to an IoT device via USB is considered malicious and creates a log.
Supply Chain Compromise	Generate logs when connecting to an external network for hardware, firmware, and software management.
Trusted Relationship	All users who access IoT devices, such as remote metering, are considered malicious users and generate logs.
Valid Accounts	All users who access the IoT device are considered malicious users, and account authentication-related logs are generated.

3.4 The Process of the Log Collection Method

This section proposes a method of collecting logs from IoT devices installed in smart city sites. Smart city has a huge number of logs collected into a massive IoT environment, and it is difficult to collect the same logs from all devices due to the heterogeneity of IoT devices' hardware, software, and protocols.

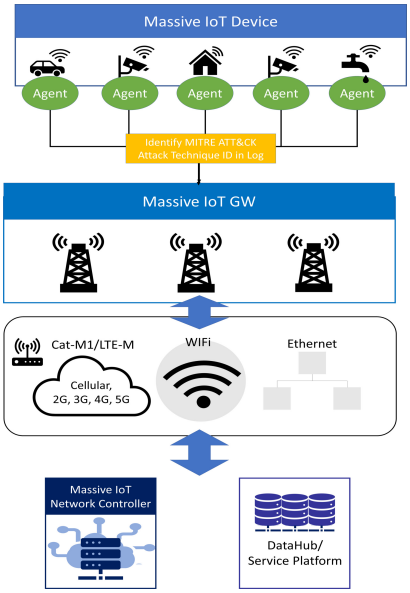
In the existing smart city, data collected from IoT devices are delivered to the gateway through protocols such as LoRa and MQTT, and the gateway delivers it to the IoT controller of the smart city and the central manager of the data hub. In general, logs can be delivered along with the data collection process. This method is difficult to solve the problem due to the heterogeneity of IoT devices and the vast number of logs. To address this problem, this paper proposes limiting the collection log. We propose installing an agent on an IoT device to detect the generation of logs related to the cause of IoT malware infection, as defined in Section 3.3, and collect only those logs.

By limiting the logs to be collected, the number of logs to be collected may be reduced to improve the log collection speed. In addition, the number of logs is reduced, making it easy to manage the logs. Through this, the central manager of the smart city can quickly determine whether a malware is infected and quickly respond to cyberattacks.

By limiting the logs to be collected, the process of identifying and collecting related logs through the agent in IoT devices in a smart city, as shown in Figure 3.

3.5 Designation of Log Format

This section defines the log format for collecting logs by limiting them. The collection method proposed in Section 3.3 of this paper proposes to collect only the logs related to IoT malware infection as defined in Section 3.2 through an agent to limit the number of logs. If logs collected by IoT devices are used as they are during the collection process, there is a problem in that it is difficult to collect the same logs from any device because of the heterogeneity of the hardware, software, and protocols. Considering the heterogeneity of these IoT devices, we propose a log format that can integrally represent information related to malicious



(Figure 3) Log identification and collection process through agent

code infection. In [9], studies proposed including in the log data essential to the forensics of IoT devices. Based on this, this study proposed a log format in which detailed items representing data on MITRE ATT&CK's attack technique, OS information for IoT devices, and platform information are added. The log format is divided into nine detailed items considering the characteristics of IoT. Among the detailed items, Related Attack Techniques described related attack techniques, indicating information that allows users who check the log to identify how the attack was performed on the IoT device where the log was generated. In addition, in the log format proposed to identify logs that vary depending on the OS, the OS information of the generated IoT device can be represented to determine the logs to check in future analysis to determine the cause of malware infection.

This log format can solve the problem related to how difficult it is to collect the same log from all devices due to the heterogeneity of the hardware, software, and protocols of IoT devices. In addition, it is easy to manage logs because it integrates and presents related information, and it has the advantage that smart city central managers can accurately identify what attacks have occurred. Table 7 presents a description of the detailed items of the proposed log format.

(Table 7) Description of log format

Log Data	Description
Platform	The field of smart city infrastructure where IoT devices provide services
Unique IoT ID	A physically identifiable unique ID for an IoT device
Geo-location	The physical location of the IoT device sending the log
Timestamp	A log indicating the log creation time and event occurrence time
Device OS	Information that can identify the OS of the IoT device
Application ID	The identifier of the application that caused the attack-related log to be generated
User ID	Data to identify the user who triggered the used ID
Severity	Severity of that log
Related attack techniques	Attack technique ID of MITRE ATT&CK's initial access related to the log

Figure 4 shows an example of a log collected in the log format proposed through the agent of an IoT device.

(Figure 4) Log identification and collection process through an agent

4. Conclusion and Future Works

In this paper, collecting limited logs for use in identifying the cause of malware infection from IoT devices installed in the massive IoT environment of a smart city was proposed. IoT devices installed in smart cities present difficulties in collecting the same log due to heterogeneous hardware, software, applications, and protocols, making it challenging to respond quickly to cyberattacks, such as malware

infection. In this paper, to solve this problem, the attack technique used in IoT devices is classified as the attack technique of the initial approach tactic classified by MITRE ATT&CK. Therefore, the logs collected to determine the cause of malware infection are limited to those that classified attack techniques can generate. In addition, installing an agent in IoT devices to facilitate limited collection log management was also proposed. Through this measure, they can quickly respond to cyberattacks such as malware infection by identifying relevant logs and sending them to a central administrator.

In future studies, we intend to contribute to the cyber safety of smart cities by identifying cyberattacks that may occur in IoT devices and conducting research to derive defensive techniques.

Reference

[1] TTA, “Quaternary Industrial Revolution Core Convergence Case Smart city Concept and Standardization Status”, September, 2018. https://committee.tta.or.kr/data/reportDown.jsp?news_num=6019

[2] DW. KIM, “Massive IoT Service Prospects for 5G Hyper-Connect Society”, NIPA, 2019, https://www.nipa.kr/main/selectBbsNttView.do?key=116&bbsNo=11&nttNo=6843&bbsTy=&searchCtgry=&pageUnit=10&searchCnd=all&searchKrwd=&pageIndex=4

[3] C. Kolias, A. Stavrou, J. Voas, I. Bojanova, and R. Kuhn, “Learning Internet-of-Things Security “Hands-On””, in IEEE Security & Privacy, Vol. 14, No. 1, pp. 37–46, 2016. https://doi.org/10.1109/MSP.2016.4.

[4] HW. Lee, “Intrusion Artifact cyber-attacks Acquisition Method based on IoT Botnet Malware”, Journal of Internet of Things and Convergence, Vol. 7, No. 3, 2021. https://doi.org/10.20465/KIOTS.2021.7.3.001

[5] X. HE, “ICT Standardization for Smart Sustainable Cities”, ITU, 2019. https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/sg20rgafr/20190827/Documents/s1-p2-He-ICT.pdf

[6] TJ. Park, “Massive IoT network technology trend for smart city application”, The Proceeding of the Korean Institute of Electromagnetic Engineering and Science, Vol. 30, No. 3, pp. 10–15, 2019. https://koreascience.kr/article/JAKO201917550767099.page

[7] MITRE ATT&CK, https://attack.MITRE.org

[8] IITP, “IoT open platform based smart city service casebook”, 2018. https://www.nipa.kr/main/selectBbsNttView.do?key=112&bbsNo=8&nttNo=5098&bbsTy=&searchCtgry=&searchCnd=all&searchKrwd=&pageIndex=3

[9] A. Pichan, M. Lazarescu, and S. T. Soh, “A Logging Model for Enabling DigitalForensics in IoT, in an Inter-connected IoT, Cloud Eco-systems”, 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4). IEEE, 2020. https://doi.org/10.1109/WorldS450073.2020.9210366

[10] K. Kurniawan, A. Ekelhart, and E. Kiesling, “An ATT&CK-KG for linking cybersecurity attacks to adversary tactics and techniques”, 2021. https://www.researchgate.net/publication/355395381_An_ATTCK-KG_for_Linking_Cybersecurity_Attacks_to_Adversary_Tactics_and_Techniques

[11] C. Liu, A. Singhal, and D. Wijesekera, “Forensic analysis of advanced persistent threat attacks in cloud environments”, IFIP. Springer, Cham, 2020. https://doi.ort/10.1007/978-3-030-56223-6_9

[12] V. R. Kebande, and I. Ray, “A generic digital forensic investigation framework for internet of things (IoT)”, 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, 2016. https://doi.org/10.1109/FiCloud.2016.57

[13] V. Chierzi and F. Mercês, “Evolution of IoT Linux Malware: A MITRE ATT&CK TTP Based Approach”, 2021 APWG Symposium on Electronic Crime Research (eCrime), 2021. https://dx.doi.org/10.1109/eCrime54498.2021.9738756

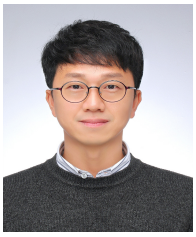
[14] Financial Security Institute, “THE Incident Response MATRIX FOR MALWARE ATTACK”, 2019. https://www.fsec.or.kr/bbs/detail?menuNo=244&bbsNo=6346

[15] A. Wang, R. Liang, X. Liu, Y. Zhang, K. Chen, and J. Li, “An inside look at IoT malware”, International Conference on Industrial IoT Technologies and

Applications. Springer, Cham, 2017.
https://dx.doi.org/10.1007/978-3-319-60753-5_19

◐ Authors ◑

김 동 현(Donghyun Kim)
2022 B.S. in Information Security Engineering Soonchunhyang University, Asan, Korea.
2022~Present. M.S. in Information Security, Gachon University, Seongnam, Korea.
Research Interests : Malware Analysis, CPS Security, ICS Security, Smart city Security, Smart factory Security.
E-mail : 202240222@gachon.ac.kr



신 지 호(Jiho Shin)
2015 M.S. in Digital Forensics, Korea University, Seoul, Korea.
2022 Ph.D. in Information Security Engineering, Soonchunhyang University, Asan, Korea.
2018～Present, Research Officer at the Police Science Institute, Korean National Police University.
Research Interests : Digital Forensic, ICS Security, Cyber-Crime.
E-mail : suchme@police.go.kr

서 정 택(Jung Taek Seo)
1999 B.S. in Computer Engineering, Korea National University of Transportation, Asan, Korea.
2001 M.S. in Computer Engineering, Ajou University, Suwon, Korea.
2006 Ph.D. in Information Security Engineering, Korea University, Seoul, Korea.
2016～2021, Professor at the Dept. of Information Security Engineering, Soonchunhyang University, Korea.
2021～Present, Professor at the Dept. of Computer Engineering Gachon University, Korea.
Research Interests : CPS Security, ICS Security, Smart grid Security, NPP Security, Smart city Security, Smart factory Security, etc.
E-mail : seojt@gachon.ac.kr