# KISA Cyber Security Issue Report : Q3 2019

Ministry of Science and ICT

KOREA INTERNET & SECURITY AGENCY

## Contents

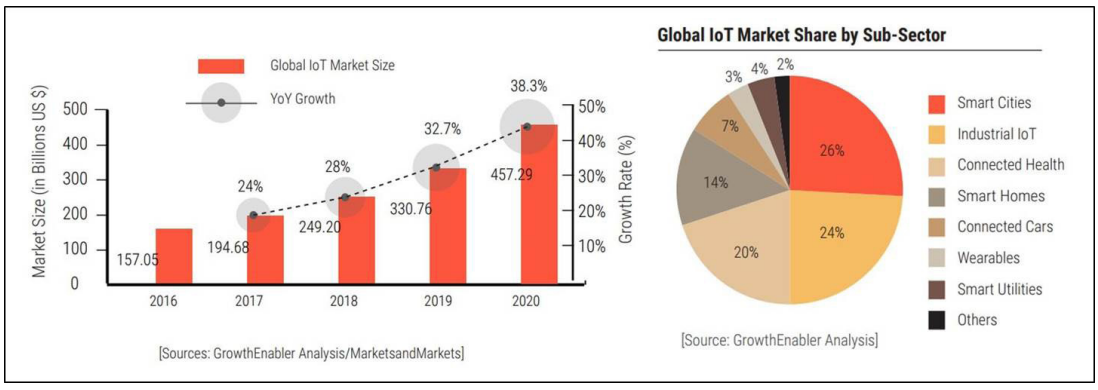
# Experts column

# 1. APT attacks using IoT and the latest countermeasure technologies

Joon Pang
CEO of Coontec

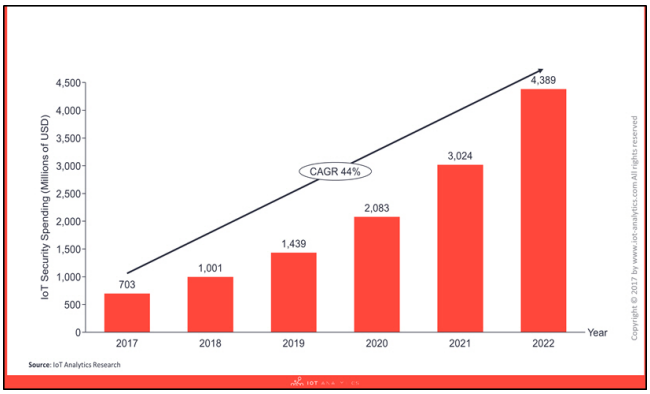
## 1) IoT market and security trends

According to various market forecasts and a report that analyzed the number of network-connected devices, the IoT market is growing by more than 20% each year and expanding its size quickly. GrowthEnabler's report that analyzed the IoT growth data in each area shows that the IoT markets are growing quickly, particularly in the smart city, industrial IoT market, and healthcare market.




[Figure 1] IoT Market Share 〈Source : GrowthEnabler Analysis〉

The security sector is also growing fast as the IoT industry grows, and the security requirements in the industrial control facility sector, medical devices, and smart city have been detailed in Korea. The security issue is a high priority in the industrial IoT sector, in particular, since the IoT security threat can lead to catastrophic physical damage. On May 3, nine agencies signed an agreement and began joint R&D to implement a security monitoring and control system. This is the result of realizing the need to develop technologies for preemptive responses, as cyber threats to energy control systems have been continuously reported overseas.




산업통상자원부 http://www.motie.go.kr

**보도참고자료**

정부혁신 보다나은 정부

**배포 즉시** 보도하여 주시기 바랍니다.

| 배포일시 | 2019. 5. 3.(금) | 담당부서 | 정보보호담당관실 |
|---|---|---|---|
| 담당과장 | 여영섭 과장(044-203-5590) | 담 당 자 | 양희준 사무관(044-203-5597) |

**사이버위협으로부터 발전제어망 보호를 위한 공동연구 착수**

**- 산업부, 국가정보원 · 발전사 공동으로 발전시스템 사이버보안 강화키로 -**

□ 산업통상자원부(장관 성윤모)는 5. 3.(금) 국가정보원, 발전사 등 9개 기관과 함께 발전제어시스템 보안관제 체계구축을 위한 연구개발을 공동으로 추진하기로 하고 필요한 업무협약을 체결했다.

* 산업통상자원부, 국가정보원, 한국수력원자력(주), 한국남동발전(주), 한국중부발전(주), 한국서부발전(주), 한국남부발전(주), 한국동서발전(주), 한국지역난방공사, 한전KDN

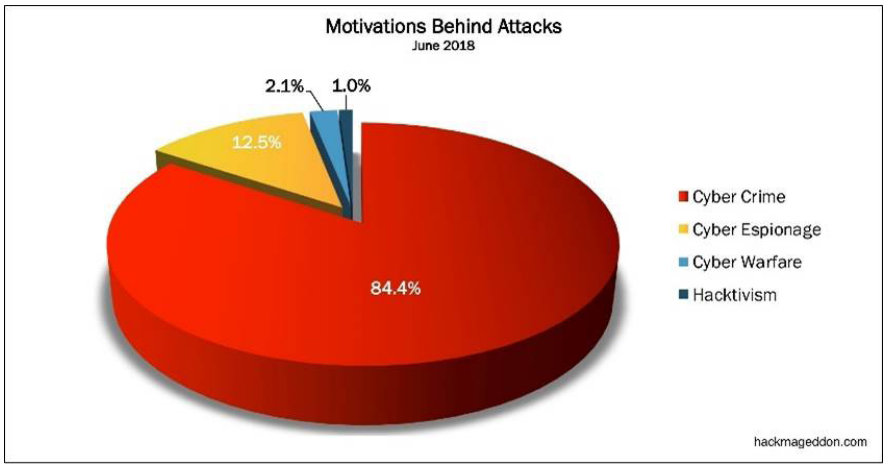


[Figure 2] IoT Industry Growth and Signing of Agreement for Security Monitoring and Control System R&D (Ministry of Trade, Industry and Energy)
〈Source: An overview of the IoT Security Market Report 2017–2022〉

The growing interest in domestic IoT security threats is due to the continued reports of cyber threats to IoT in Korea and other countries and the increasing number of incident cases.

## 2) Trend of IoT attacks

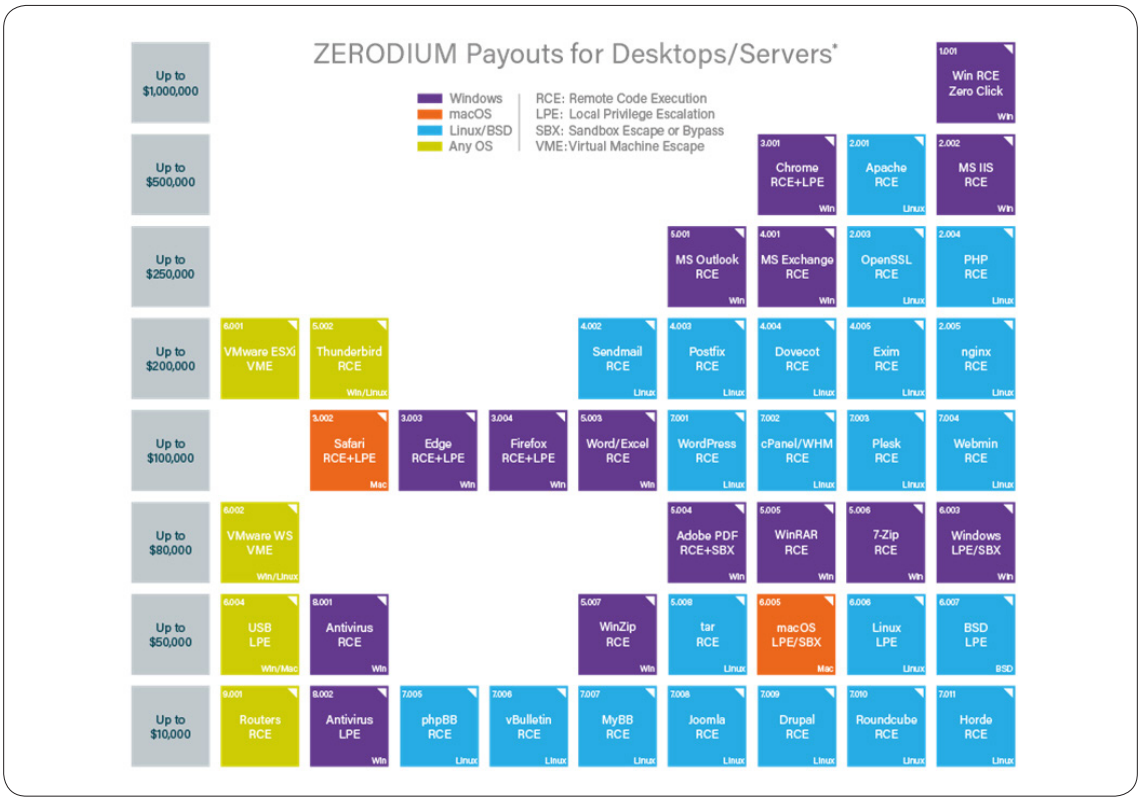
Before reviewing the trends of IoT cybersecurity attacks, it is necessary to examine the motivation for recent cyberattacks. An analysis of the motivation for recent cyberattacks shows that 84.4% had a criminal objective. It explains why advanced persistent threat (APT) attacks are increasing.




[Figure 3] Statistics of Motivation for Cyberattacks 〈Source: www.hackmageddon.com〉

In other words, APT attacks are increasing because attackers can expect significant monetary gains from the attacks. They can trade attack tools easily on the Dark Web, and attack code, like ransomware, can negotiate with victims to make profit directly. This is why threats and attacks using cyber weapons are taking place at the national and political level.

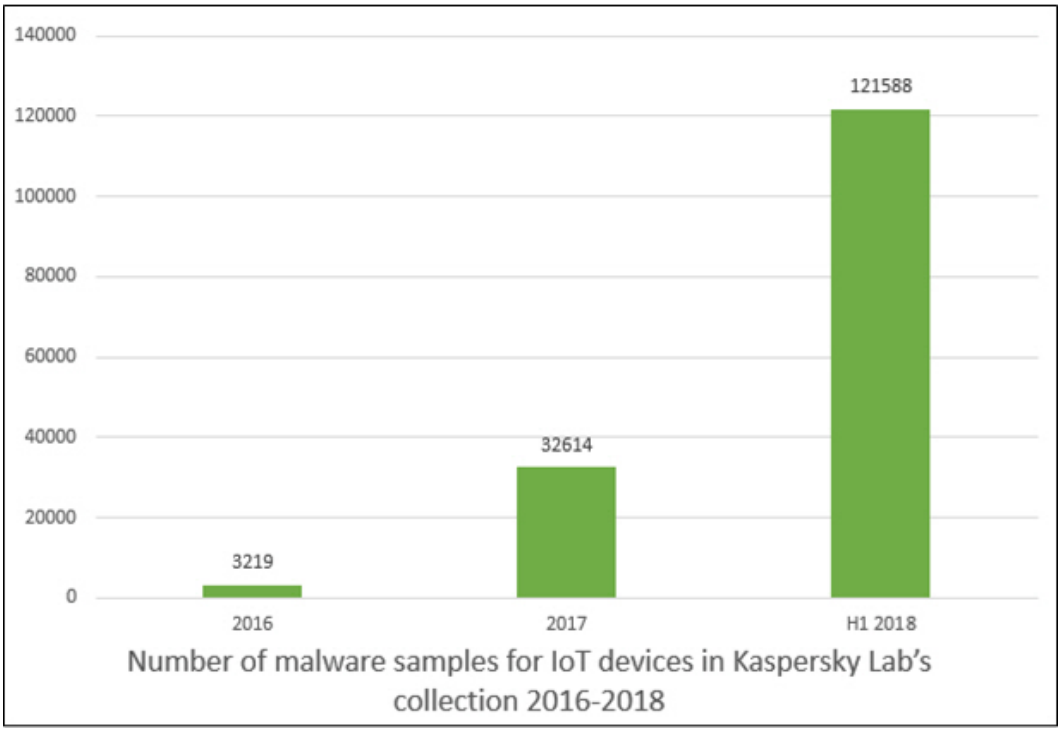
The Dark Web market has grown greatly, as of late. Finding exploits and vulnerabilities is a complicated task that only skilled and advanced attackers can perform. However, the Dark Web has provided markets to link hackers who have know-how with potential criminals. One can buy ransomware code for $270 and a total package for IoT botnet for about $1,000 on a famous Dark Web site. The highest-level APT attack codes are priced at $10,000 – $1,000,000. It is apparent that the Dark Web is now a commercial entity. It is providing more opportunities for many attackers.




[Figure 4] Prices of Malware

Such a strong monetary incentive has led to an overall increase in the number and variants of malware, and is causing many enterprises to struggle with defending against cyberattacks. As such, they are utilizing more advanced tools and defense techniques.

Cyberattacks against IoT devices can be understood in the same context. Criminal interest in cyberattacks against IoT devices has continued to grow. According to an IoT report by Kaspersky Lab, based on internally collected information from honeynet and deceptions, more than 120,000 IoT devices suffered from variant malware attacks in the first half 2018, and malware attacks against smart devices increased 10 times in 2017 compared to 2016. Kaspersky Lab has warned that the malware attacks against IoT devices are growing very quickly.




[Figure 5] Number of Detected Malware against IoT Devices 〈Source: Kaspersky Lab〉

Why are the attacks mainly targeting IoT devices growing so fast? It is not surprising that IoT devices are attractive attack targets. The awareness of IoT system security of major industrial infrastructure and enterprises is still very low, and many sites do not have the systems or software to protect their IoT devices from specific attacks. Moreover, many sites have failed to patch known security vulnerabilities.

Most IoT devices developed in the past basically did not have design guidelines for security. From the attacker's viewpoint, they are the weakest link in the chain and the easiest attack point to exploit inside an organization.

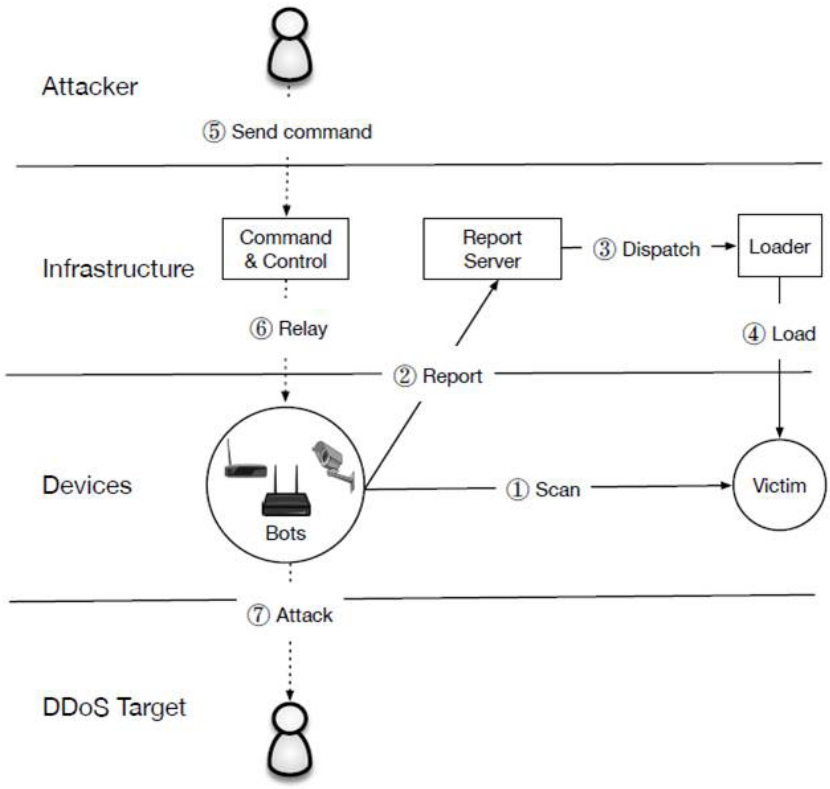
### 3) Analysis of IoT security threat cases

As described above, IoT is a system that is very easy to breach for attackers. Many enterprises and organizations have not yet established security guides for the security and quality management of IoT devices. As such, they are often out of the scope of security management in an organization. Security measures are not updated or patched regularly, and there is no security management methodology of known security vulnerabilities and password management. Very few of them have introduced a security solution to malware attacks against IoT. This section analyzes the most widely used IoT malware and the latest defense technologies against them.

| # | Malware Downloaded | Attack Rate |
|---|---|---|
| 1 | Backdoor.Linux.Mirai.c | 15.97 % |
| 2 | Trojan-Downloader.Linux.Hajime.a | 5.89 % |
| 삽 | Trojan-Downloader.Linux.NyaDrop.b | 3.34 % |
| 4 | Backdoor.Linux.Mirai.b | 2.72 % |
| 5 | Backdoor.Linux.Mirai.ba | 1.94 % |
| 6 | Trojan-Downloader.Shell.Agent.p | 0.38 % |
| 7 | Trojan-Downloader.Shell.Agent.as | 0.27 % |
| 8 | Backdoor.Linux.Mirai.n | 0.27 % |
| 9 | Backdoor.Linux.Gafgyt.ba | 0.24 % |
| 10 | Backdoor.Linux.Gafgyt.af | 0.20 % |

[Figure 6] Top 10 Malware Downloaded to Infected IoT Devices 〈Source: Kaspersky Lab〉

The Mirai malware has many variants because the source code is open source [1] and applies a wide range of bypass and avoidance techniques.




[Figure 7] Outline of Mirai Botnet Attack Procedure

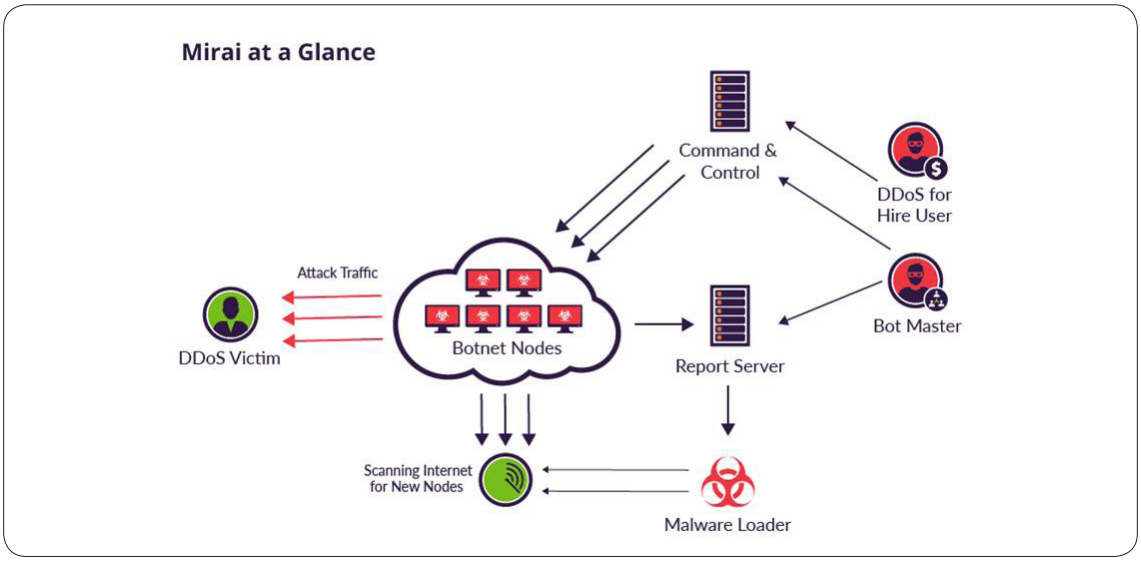
① The Mirai botnet scans the IPv4 address domain of an IoT device that runs telnet and SSH and attempts to log in with the IP and password in the hardcoded dictionary.

② If it logs in successfully, it sends the IP and credential data of the target system to the report server.

③ The report server runs the loader to infect the attack target.

④ The infected device scans other attack targets and perform the DDoS attack on a command from the C&C server.

1) https://github.com/jgamblin/Mirai-Source-Code




[Figure 8] Network Configuration for Mirai Botnet Attack

The Mirai malware can be cross-compiled to be operable in various architectures such as ARM, PowerPC, MIPS, and SuperH.

In conclusion, existing IT network security systems require the following new functions to cope with IoT malware such as Mirai.

- Monitoring of network traffic and detection of abnormalities by identifying IoT assets and understanding the protocol of IoT devices
- IoT malware analysis to detect the variant IoT malware
- Internal observation to respond to zero-day IoT malware by advanced attackers

Although the senders of existing emails that were sent to domestic targets used Korean names and were disguised as emails sent by a specific company, most of them were very simple or contained no content.

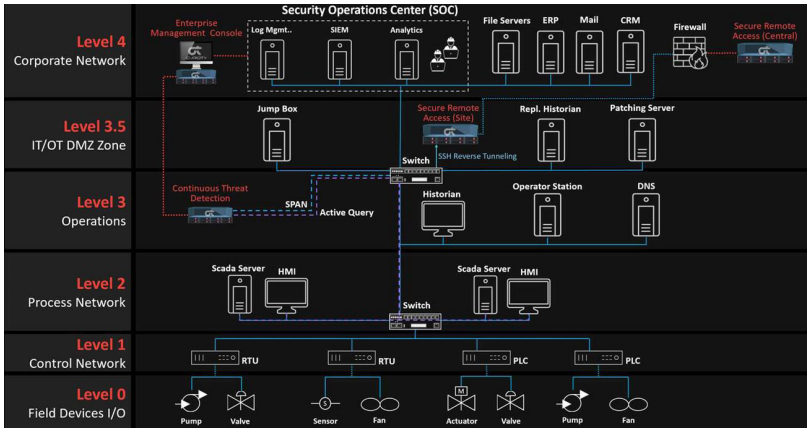
## 4) Latest technologies to cope with IoT APT

### 4-1) Detection of network-based industrial IoT abnormalities

The security monitoring and control system is the fundamental basis for a defense in cybersecurity. In industrial IoT security, the targets of monitoring and control are expanded from the information assets (servers, network equipment, and applications) connected to the network to include all equipment such as the controllers, PLC, and DTU that operate the industrial control facilities.

As described above, the malware targeting IoT devices for an attack is downloaded to an IoT device and identifies and attacks other devices using communication messages such as those for network scan and C&C. If the attacked IoT devices are not identified, the person in charge of the enterprise security cannot detect the abnormality in the internal network at all and would have difficulty identifying the internal asset for a response. Therefore, identification of assets is critical since the damage can occur immediately, due to the characteristics of the industrial control facilities.

Moreover, unlike conventional IT security monitoring and control, it must identify the unknown types and protocols. As shown in the following diagram, the network of industrial control facilities consists of the IT network, OT network, and DMZ zone. Existing security solutions support the IT network, but they must support the protocols used in the industrial control facilities to identify the industrial control assets.




[Figure 9] Configuration for Each Layer of Industrial Control Facility 〈Source : Claroty〉

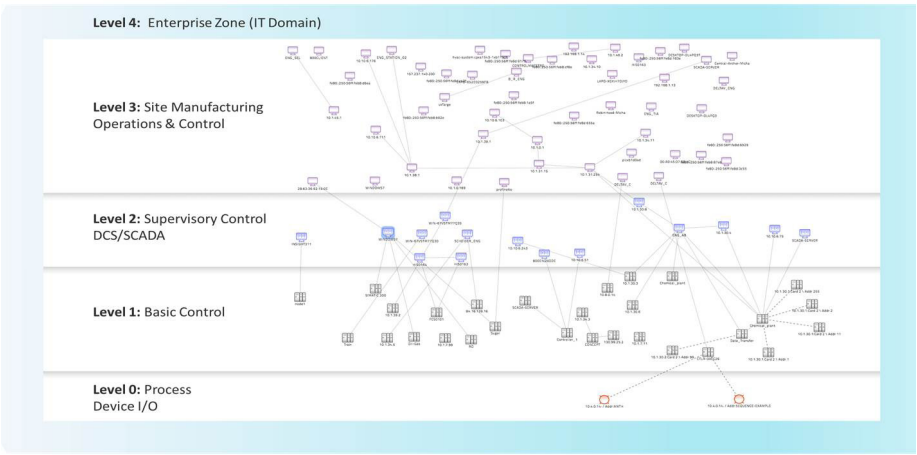
**Passive – continuous, real-time monitoring of OT networks**

ABB Bailey • ABB DMS system • ABB HC800 (Infininet) • ABB Spirit • ABB Symphony Plus • ABB Totalflow Alstom E-Terra • BACNET • Beckhoff AMS • CC Link IE – Field • Cisco Discovery Protocol (CDP) • Citect HMI Cognex Discovery • Control Technologies Inc. (CTI) • Comtrol NS Link • CPHA (Checkpoint High Availability) Digsi4 • Digsi5 • DACP • DHCP • DNP3 • Emerson DeltaV • Emerson Ovation • Emerson ROC Plus • ETHERNET/IP Foxboro RTV • Foundation Fieldbus (FF) • Foxboro LLC • FTP - SEL • GE-ALM • GE Bentley Nevada (BNC3500) GE-EGD • GE-EGD-CMP • GE PAC8000 (AXE) • GE QuickPanel (TRAPI+HTTP) • GE SDI (MarkVie) • GE SDI Classic (MarkVie) • GE SRTP • Goose (IEC-61850) • HART-IP • HiDiscovery - Hirschmann LLC • Honeywell C200 - Ftebcip Honeywell Experion – CeeNTComm (C300, EHPM) • Honeywell EpicMo (C300 management) • Honeywell Firewall CF9 Hot Standby Router Protocol (HSRP) • HTTP • HTTP-XML (specific schemes) • IEC101 • IEC103 • IEC104 Keyence Host-Link Communication • Keyence KV Studio • Keyence Logger • Kongsberg • Knapp • Lantronix Serial GW • Linux High Availability • LLDP • Microsoft DCE RPC • Microsoft DCE RPC – ABB DCS Service Manager Microsoft RDP • Microsoft NTLMSSP (Auth protocol) • Microsoft SAMR • Microsoft CIFS (SMB) Mitsubishi Melsec MNDP • MMS Modbus • MQTT • Modbus ScadaPack • Modbus Modsoft • Modbus Concept • Modbus Eltec Modbus Execload Modbus Schneider • NetBIOS Browser (UDP 138) • NetBios Datagram Service • Niagara Tridium (BMS) • Omniflow Flow computer • OPTO MMP • OSISoft PI • PCCC • Portwell • POP3 • ProConoS (TCP 20547) Profinet DCP • Profinet I/O Profinet Real-Time • RTCP • RCDP • Redlion Crimson • Rockwell CIP • Rockwell PCCC S7Comm Plus • Siemens FWL LOAD (firmware upload) • Siemens P2 • SLMP (CC Link IE Field Basic) • SNMP, SSH Synchrophasor • Telnet- DeltaV Telnet- Moxa • Telnet- Omniflow • Telnet - Hirschmann • Telnet- SEL • TFTP Triconex Tristation • Triconex TSAA Yokogawa VNET (VHF) • Yokogawa odeq

[Figure 10] Protocols Used by OT Networks

Each protocol identifies assets through learning and can detect the abnormalities automatically, based on communication data of the identified asset.

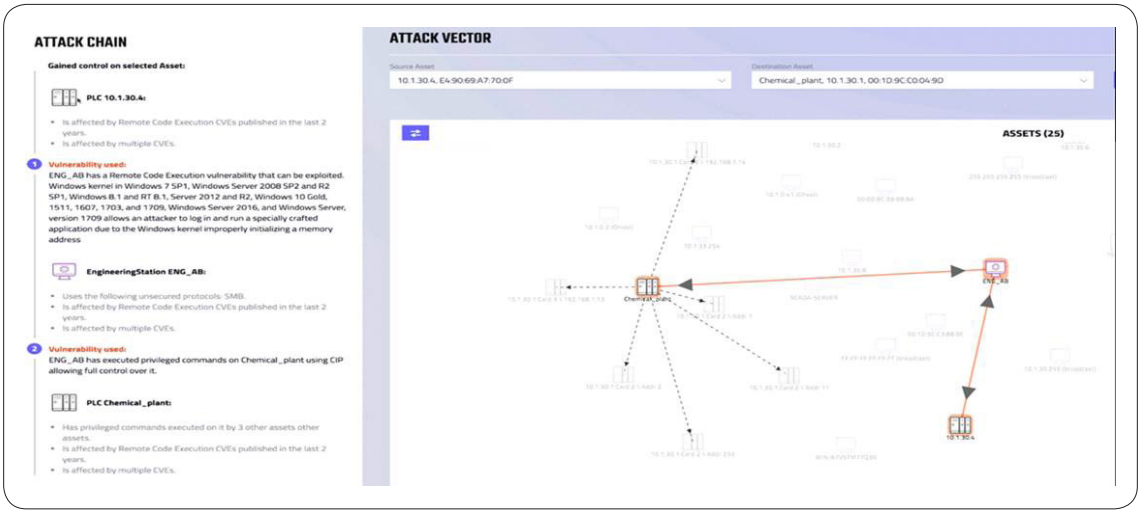
The following diagram depicts the IIoT[2] equipment on each layer of the entire industrial control facility identified through network learning.




[Figure 11] Asset Identification Screen for Each Claroty Layer

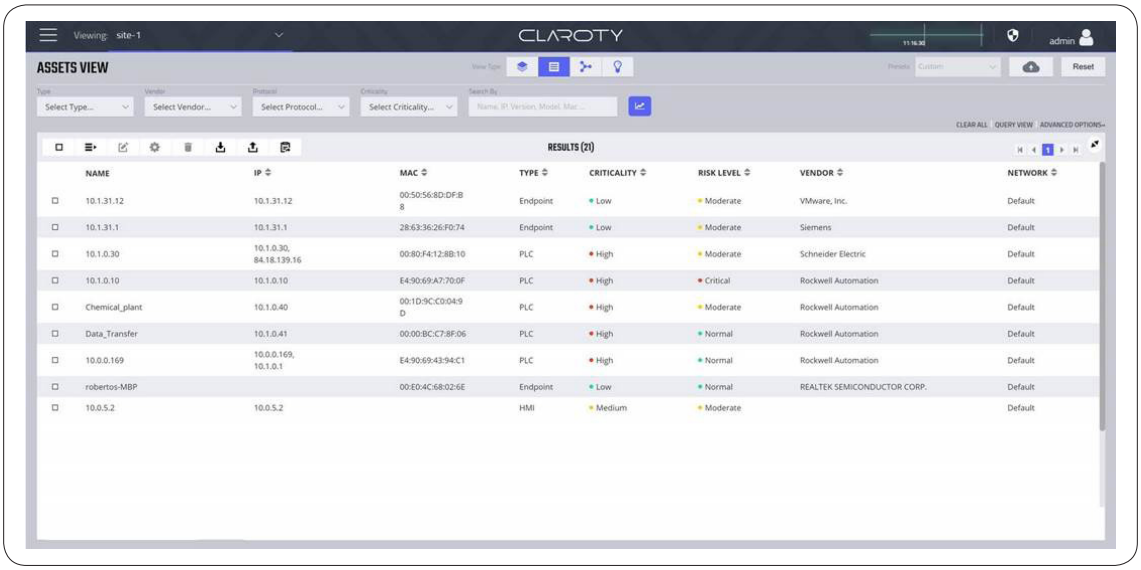
2) Industrial Internet of Things

It is possible to remove a potential attack route by matching the known vulnerabilities based on the device information identified as the asset and simulating the possible attack chains.




[Figure 12] Attack Chain Simulation of Industrial Control Facilities

The following diagram shows the list of IIoT devices and vulnerabilities of each industrial control facility.

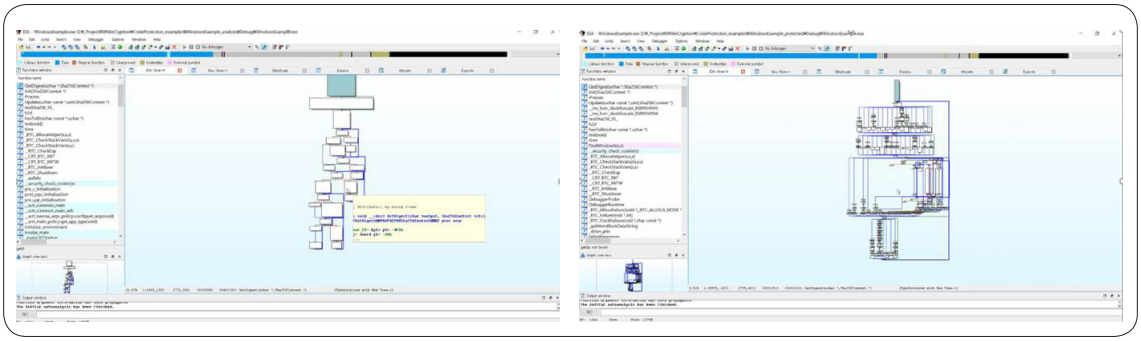



[Figure 13] Asset Information List of Industrial Control Facilities

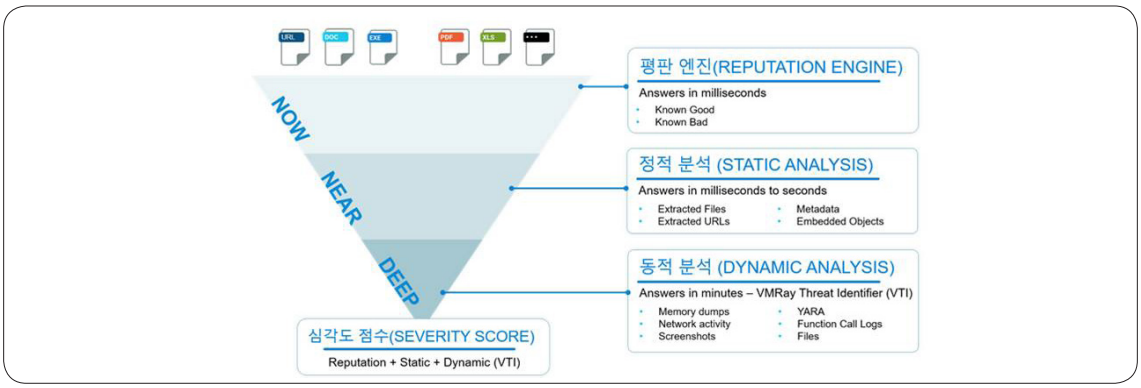
## 4-2) In-depth analysis based on the dynamic behavior of IoT malware

The malware detection procedure generally scans the files based on the signature and deletes or isolates the problem files. However, the signature-based search method can detect malware only when vaccine developers continuously find the specific strings that are identifiable from the binary code of a malware program and add them to the database. It is difficult to respond to variant and new malware in real-time, and it is very difficult to find the malware if it is hidden through obfuscation, masking, encryption, or redundancy techniques. The dynamic behavior-based analysis is the technique of detecting variant and new malware programs by identifying the malicious behaviors, by running them in a virtual environment (since damage can occur due to the malicious behavior if running the malware in an actual environment) to overcome it.

● Obfuscation to make malware analysis difficult



[Figure 14] Before (Left) and After (Right) Applying Code Analysis Prevention Technology

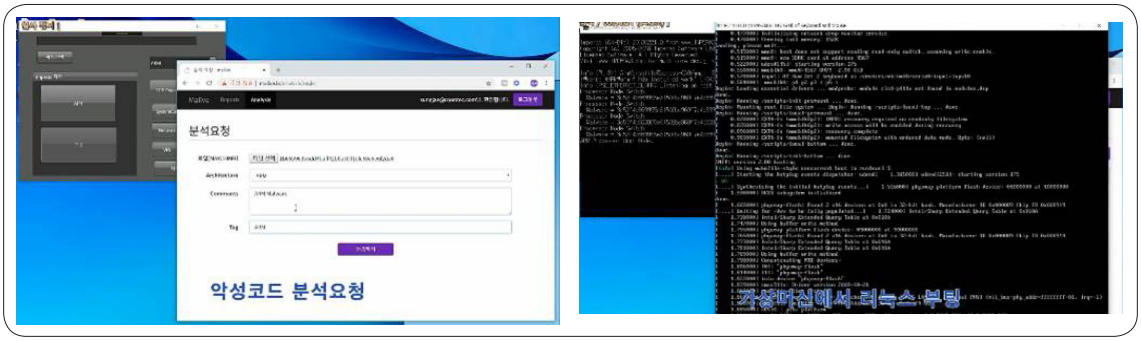



[Figure 15] Malware Analysis Layers 〈Source: VMRay〉

A three-step procedure is needed to run and detect IoT malware in a sandbox.

① IoT malware execution environment

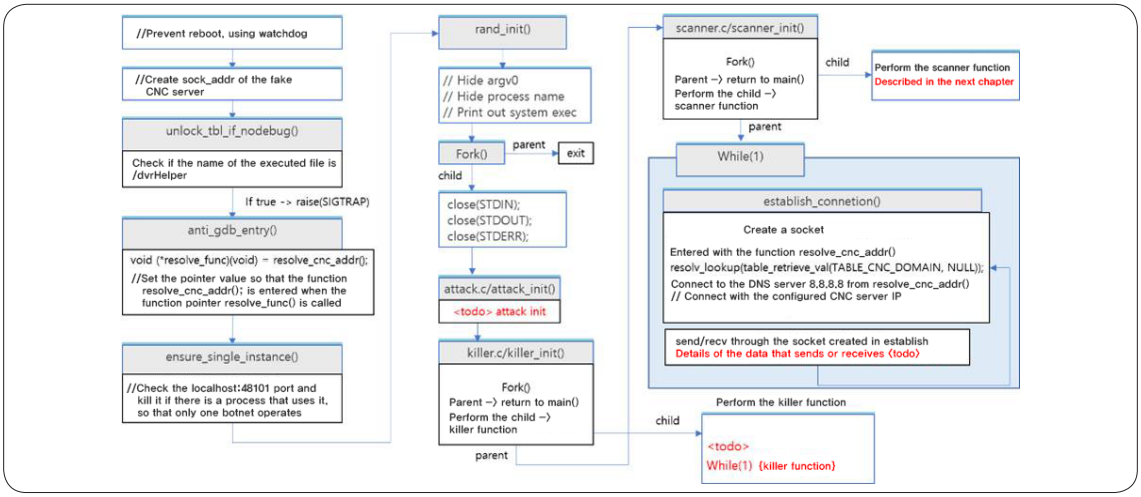
It is necessary to implement an embedded processor such as ARM and MIPS in a virtual system to run IoT malware that runs on embedded devices. This malware can run after the network is configured with the topology to run the Mirai malware.




[Figure 16] Before (Left) and After (Right) Applying Code Analysis Prevention Technology

② Collection of IoT malware behavior

The virtual machine collects the data related to the IoT malware behaviors (memory access, file access, network packet, process, etc.) and identifies the malware behaviors.




[Figure 17] Actual Malware Behaviors

The original file is encrypted, and the domestic vaccine program is checked if it is running when the file extension is changed.

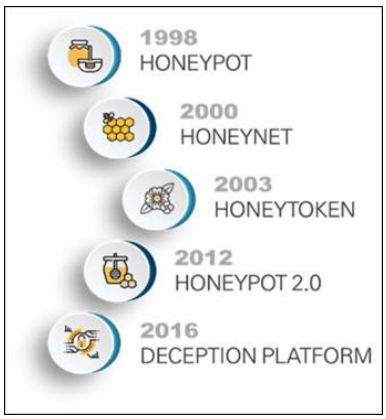
③ Determination of normal/abnormal behavior

The metadata of malware behavior is checked with the normal behavior data, and the malicious behavior is identified using the comprehensive judgment data.

### 4-3) Deception technology

① Difference from a honeynet

A honeypot is a system installed in a network intentionally to detect malicious or abnormal access. For example, configuring the server name to suggest that its network contains confidential information and vulnerable network services, and connecting them can detect an attacker who has exploited the system by bypassing the network defense and accessing it for cracking. Afterward, the honeypot can collect the malicious behaviors of the attacker and obtain the tracking information. Honeypot was introduced by a hacker in 1998 to detect attackers exploiting computers, and a honeynet is a network of honeypots. Although the honeynet has continued to develop, only some security agencies operate it due to the attacker's bypassing technology, limitation of scaling, and difficulties of security log analysis and automation, despite the conceptual strengths.




[Figure 18] History of Honeypot

② Deception Technology

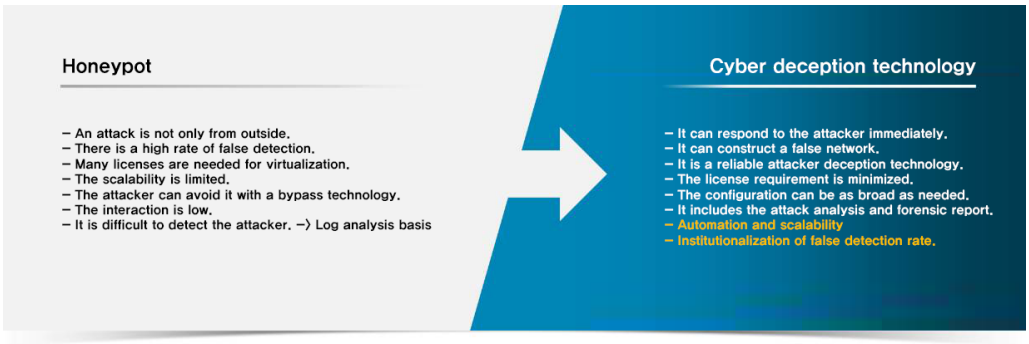
The deception technology that was introduced as an advanced form of honeynet in 2015 is a new area of cybersecurity technology. The cyber deception technology can detect, analyze, and defend against the highest-level attacks, such as zero-day and one-day attacks, in real-time. It is a critical technology in the recent security trends in which APT attacks are the mainstream, and it is difficult to defend IoT devices.

Unlike the existing honeynet, it introduces the concept of deception and baits and automates deception, which is a similar concept as the honeypot. Since the current network can be automatically scanned and cloned, it can construct an indistinguishable deception system in the internal network.

While the existing honeypots can configure only Windows-based IT assets into a honeynet, the deception technology can emulate various systems such as IoT, IIoT, medical devices, PLC, and Linux, and thus is very useful in IoT security.

No security solution features a tool to monitor an attacker after it has breached the internal system by bypassing the network defense layer (IDS/IPS, firewall, and malware analyzer). The deception technology induces the attacker to the false network through the deception, and baits and detects the attacker's access, malware download, and path without noise in real-time.

Since the internal attacker accesses sensitive information in the same path, it can detect the malicious actor inside the enterprise.



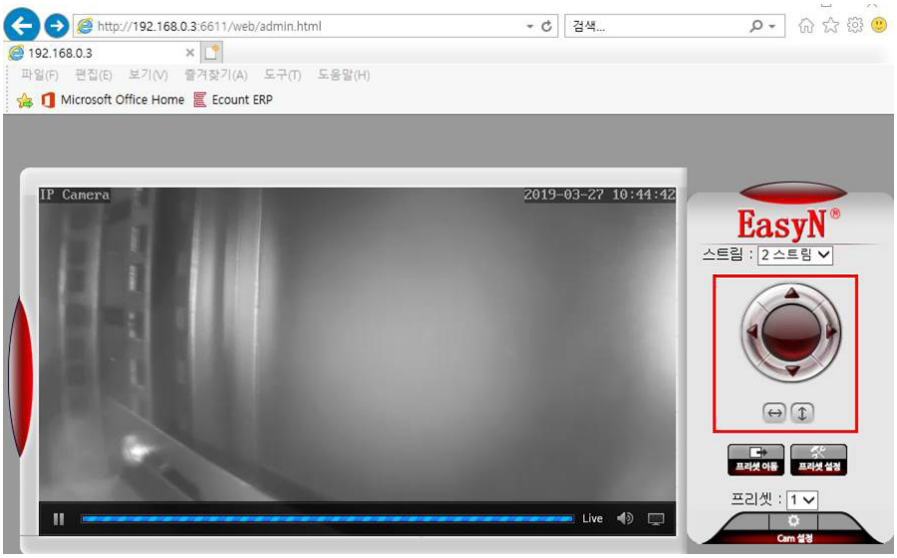

[Figure 19] Difference between Honeypot and Cyber Deception

Existing in-depth defense technologies offer very high accuracy and defense effects against serial attacks with a known attack pattern, but they fail to detect the latest APT attacks using IoT, and it is difficult to defend against them. In-depth defense technology is basically a technology to defend boundaries and thus cannot definitiveely defend against bypass attacks (phishing emails, updates, open IoT devices, internal attackers, and attacks using malicious devices) that has crossed the boundary. A cyberattack can exploit such networks and learn and steal data and knowledge assets without interruption for months. An intelligent network security solution can find an exploiter, but there are many cases of the increased security person's fatigue by many alerts and noises, leading to missed actual alarms and successful exploitation.

A deception technology considers the viewpoint and methodology of human attackers who exploit and search the network to identify and extract data. Integrated with the existing technology, it provides the new visibility to internal networks, generates the alerts with a high probability to existing infrastructure, and shares the threat information.

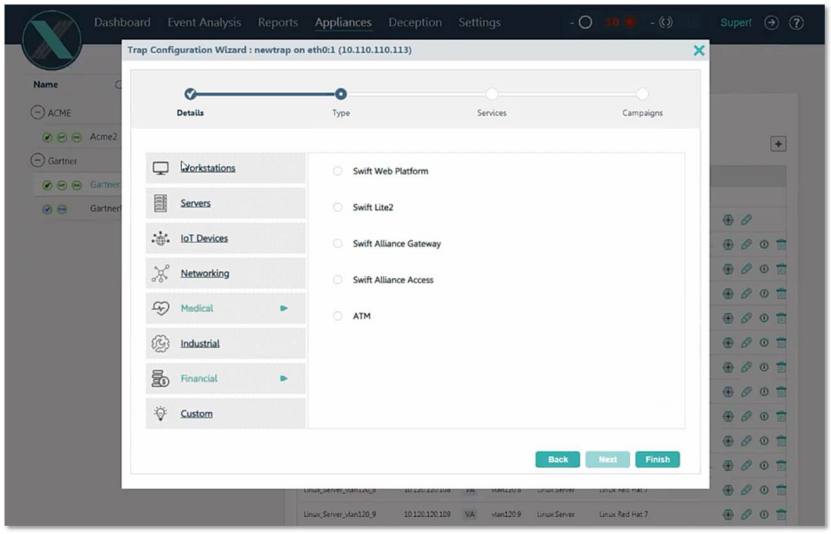
③ Detection of malicious attackers with the deception technology

● Creation of a virtual trap IP cam device using a deception solution




[Figure 20] False IoT Device Creation

- Servicing of port 6611 from the deception device
- The virtual IP cam device is redirected to the actual device to look like the actual device.
- An attempt to attack through the port 6611 of the virtual device is redirected to the actual device.
- The attacker is not aware of the installed trap.
- The deception tool enables easy installation of the virtual device and secures the URL of the attacker (no need for separate TAP, IDS, or IPS).

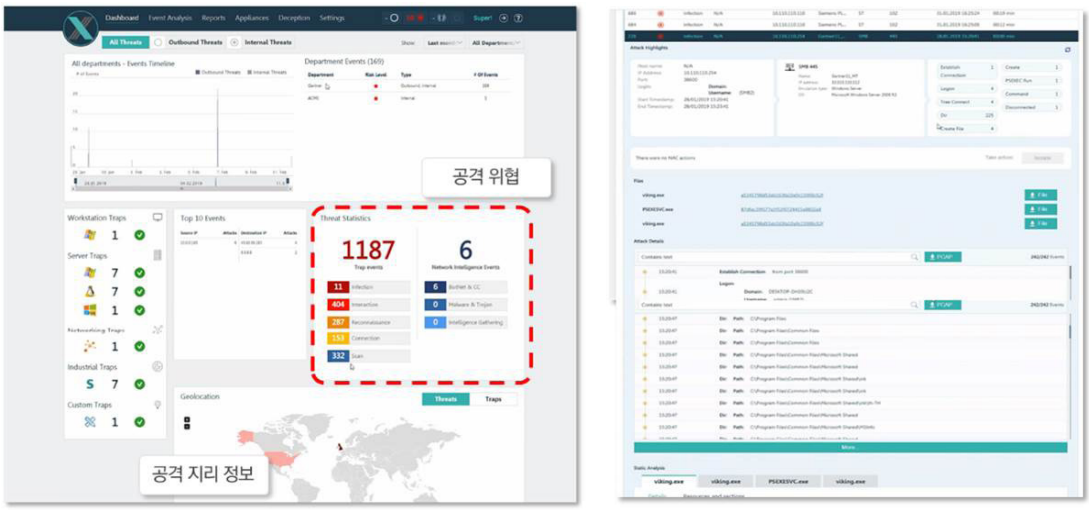



[Figure 21] Deception Network Configuration

The attacker sends the attack URI to the trap using an automated script.

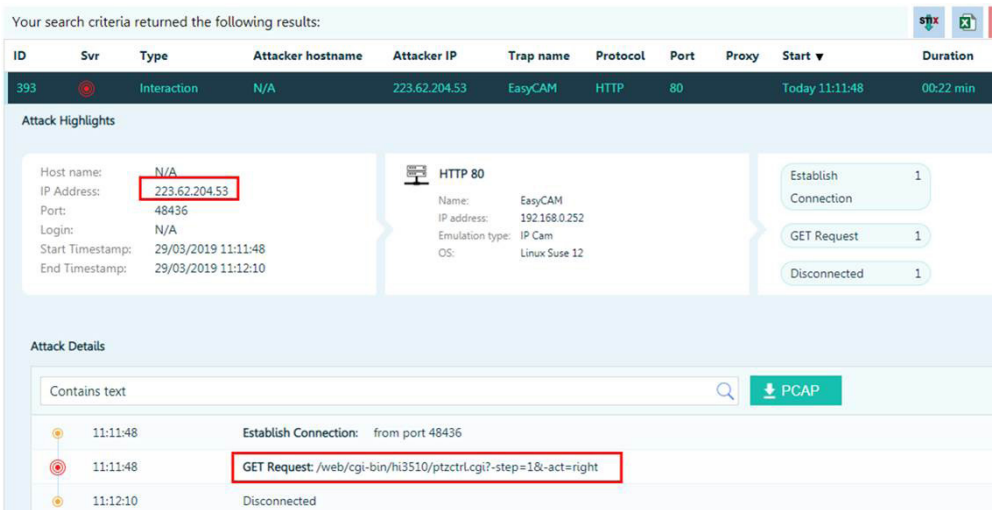
```
params ={
        'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko',
        'Cookie': 'streamselectcook=0; noshow=0; browser=0',
        'Authorization': 'Basic [redacted]ODg='
        }

url = 'http://[redacted]3:6611/web/cgi-bin/hi3510/ptzctrl.cgi?-step=1&-act=left'

res = requests.get(url,headers=params)
print (res.text)
```

[Figure 22] IP Camera Attack Code




[Figure 23] Deception Network Detection and Forensic result

The deception system can identify the attacker's IP and attack command, and obtain the network data PCAP file.




[Figure 24] IP Camera Attack Code and Attacker Information

### 4-4) Need to inspect the cyber kill chain and establish the defense system through IoT cyber simulated training

The simulated cyber training can train the internal infrastructure and members using various scenarios and enhance the overall security capability of the enterprise by inspecting the CERT scenarios and unexpected internal vulnerabilities and security regulation.

The simulated training based on IoT attack scenarios can inspect the overall IoT defense system and vulnerabilities and supplement the inadequate IoT security process in the internal security regulation of enterprises.

## 5) Conclusion

As discussed above, it is difficult to respond to IoT security threats such as APT attacks using IoT with the existing IT network security.

IoT uses dedicated processes, software stacks, and protocols, and cannot be easily updated for security, as MS Windows can. As such, there is a definite limitation, technologically and organizationally, in using the IT security governance as is.

However, the number of smart IoT devices is increasing quickly as 5G wireless communication is launched, and some forecasts expect the number to be multiple of the total world population by 2020. However, manufacturers are still not specifying the security priority for IoT. Many guides for initial settings or new firmware versions do not notify of the need to change the default password, and general end-users still feel that the update process is complicated. Therefore, IoT devices have become the main targets of cybercrime and the most vulnerable part. IoT devices can be infected more easily than conventional PCs, but they have the role of crucial infrastructure in the network environment. Moreover, some IoT devices manage the Internet traffic of all devices and become the linkage to other assets.

As such, it is necessary to identify and continuously supplement IoT vulnerabilities in the seven steps of the cyber kill chain (reconnaissance, weaponization, delivery, exploitation, installation, command control, and actions on objective) to respond to the latest APT attacks using IoT. We suggest the following technologies be upgraded in the future.

a) Network monitoring by identifying IoT assets
b) Behavior-based analysis to explore variant IoT malware
c) Construction of false IoT network to detect APT attacks
d) Inspection of vulnerabilities through IoT cyber simulated training

① Reference

1. https://securelist.com/new-trends-in-the-world-of-iot-threats/87991/
2. https://www.opswat.com/blog/why-advanced-persistent-threats-are-targeting-internet-things
3. https://www.techrepublic.com/article/using-a-d-link-router-watch-out-for-hardcoded-backdoors-that-give-hackers-admin-access/
4. https://thehackernews.com/2018/04/iot-hacking-thermometer.html
5. https://hackernoon.com/did-you-know-that-printers-are-a-major-cyber-attack-vector-eddfbd8f99bb
6. https://itsecuritything.com/mole-a-smartwatch-poses-no-real-world-threat/
7. https://zerodium.com/program.html

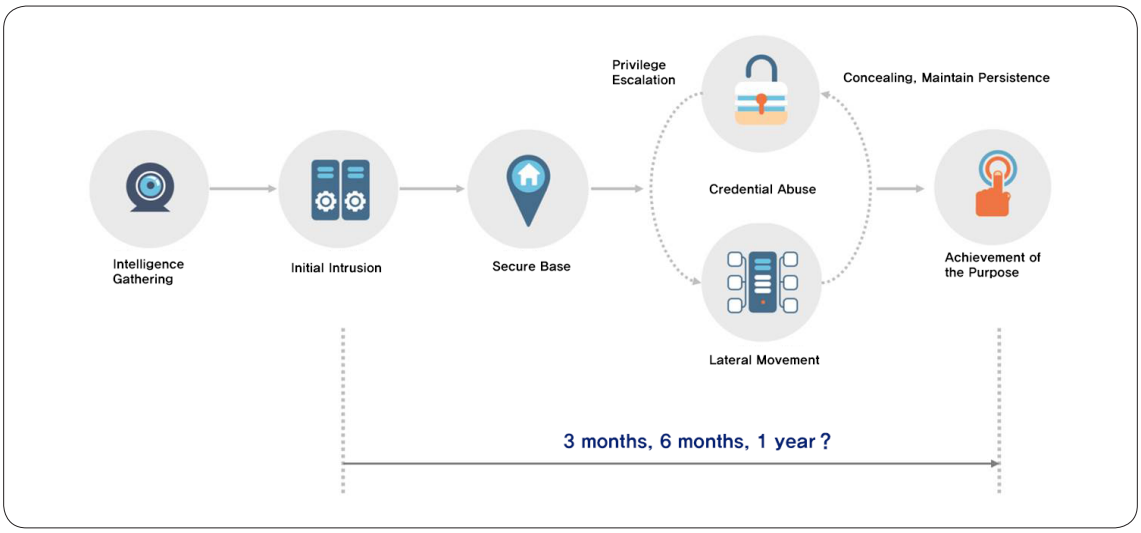
## 2. Strategy to detect host-based targeted attacks

Kim Jin-kook,
CEO of Plainbit Co., Ltd.

While showing-off and socially disrupting cyberattacks were often found in the past, most of the recent occurences are strictly for monetary gain. The cyberattacks with monetary purpose tend to be targeted attacks, since most of them, except for ransomware, must be carried out secretly until they attain their goals.

It is difficult to detect these targeted attacks with specific rules, since the attack types differ according to the attack target, environment, and purpose. It is also difficult to analyze the causes of incidents, since they induce human error such as spear-phishing email access and visiting a vulnerable website, or use techniques like attacking of supply chains and exploiting vulnerabilities.

### 1) Overview of targeted attacks




[Figure 25] Steps of Targeted Attacks

The above diagram shows the general steps of targeted attacks. The attack collects information to exploit a network from outside and performs the initial intrusion using a vulnerable point.

Afterward, it collects information from the exploited system and secures the base that is available for C2 communication with the outside and accesses the internal systems. It continues to spread laterally and achieves its purpose.

It typically takes three to six months for a targeted attack to achieve its purpose after the initial breach. According to 2019 M-Trends by FireEye, it takes about 204 days on average for an organization to identify the intrusion after the initial breach (in the Asian-Pacific region). The response to targeted attacks must focus on reducing this period.

### 2) Defense failure and detection strategy

The responses in many organizations concentrate on blocking the initial intrusion. However, it is realistically impossible if there is human error involved in detecting the initial breach or if a zero-day vulnerability is used. Therefore, the defense strategy to block initial intrusions would eventually fail.

The defense against targeted attacks must concentrate on the period from the initial intrusion to the achievement of the purpose. Since the attacker uses much time and resources and continues to perform the attack actions even if some of them are blocked if the expected value of the purpose is high, the defender must establish a strategy to detect this period. The detection strategy can be mainly divided into a network strategy and a host strategy.

① Network detection strategy

Excluding the air gap environment in which communication is not possible, the attacker must communicate with outside C2 after the initial intrusion. Since the attack must continuously exchange commands through the reverse connection until it achieves its purpose, the strategy of managing the network flow data and identifying the C2 communication through it is necessary.

② Host detection strategy

The host performs all actions, such as the additional malware download, system and network investigation, malware running, privilege escalation, defense avoidance, and information leakage to achieve the purpose after the initial intrusion.

Therefore, it is necessary to establish a way to detect the techniques used by hosts for attacks.

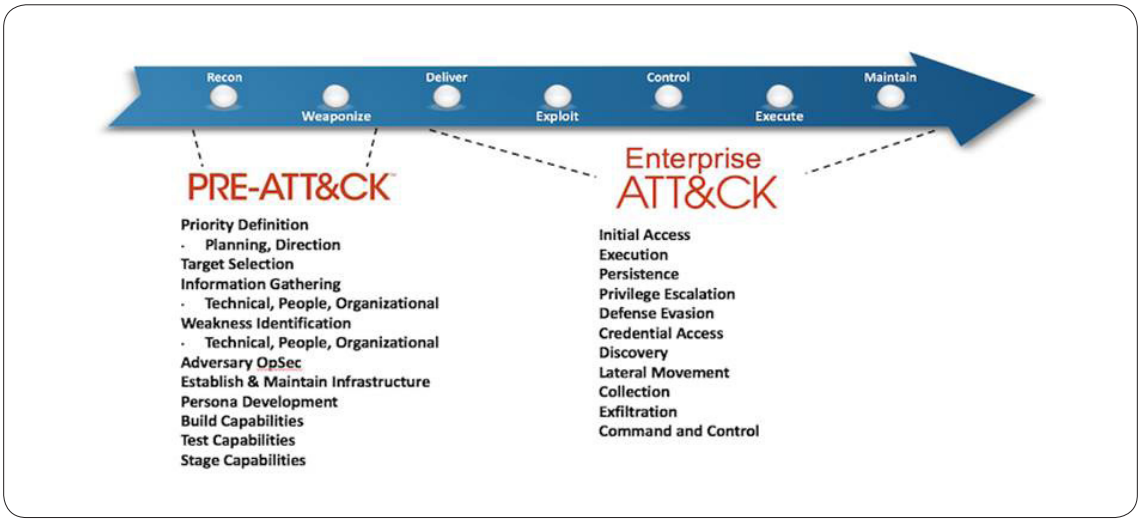
This section describes the host detection strategy. According to the 2019 M-Trends Report by FireEye, the rate of an exploited enterprise to be attacked again is 78% of all surveyed enterprises (2018 average in the Asian-Pacific region). As such, the detection strategy should be able to identify the tactics, techniques, and procedures (TTP) of the attacker, beyond the simple detection of the attack techniques to respond to re-attack by the same attack group.

Let us assume that an attacker goes through a 10-step process from the initial intrusion to the achievement of the purpose. Although it would be great for a defender to detect all attacks at the first step, it is realistically impossible. Therefore, a strategy of detecting each of the 10 steps is needed. Equally important as the detection strategy is the recognition shift for C-level to accept that the identification of attack in step 9 is also the valuable performance.

### 3) Use of ATT&CK matrix

The ATT&CK matrix is the framework defined by the Mitre Corporation as a model to assess the organizational risk by segmenting the attack techniques. There are many models, such as Lockheed Martin's Cyber Kill Chain, MITRE's Cyber Attack Lifecycle, and FireEye' s Attack Lifecycle to define cyberattacks. These models are effective in defining the flow and procedure of cyberattacks.

As the cyberattack has recently advanced, more enterprises have realized the need to go beyond simply defining attacks and defending against them using TTP of attack techniques. The ATT&CK matrix by the Mitre Corporation meets the requirement and is widely used by consultants to assess security threats, verify security solutions, and design cyber response training systems.




[Figure 26] Introduction of Mitre ATT&CK Matrix
(https://attack.mitre.org/resources/enterprise-introduction/)

The ATT&CK matrix divides existing Mitre's Cyber Attack Lifecycle model into the PRE-ATT&CK domain and the Enterprise ATT&CK domain, segments each domain into the category for each attack tactic, and defines the detailed technologies that are suitable for each category. Since the PRE-ATT&CK domain is the preparation stage of an attack, an enterprise cannot identify it through its host. Therefore, it is necessary to focus on the Enterprise ATT&CK domain.

The Enterprise ATT&CK domain defines a total of 12 tactics categories and detailed techniques for each category for Linux, macOS, and Windows platform separately. Twelve categories and more than 260 techniques are defined for Windows.

[Table 1] Description of Categories of Enterprise ATT&CK Matrix

| Category | Description |
|---|---|
| Initial Access | The technique used by the attacker to obtain the initial foothold for intrusion |
| Execution | The technique for the attacker to run the local or remote control code |
| Persistence | The technique to access a system persistently |
| Privilege Escalation | The technique to attain the higher-level privilege in a system or network |
| Defense Evasion | The technique to dodge the defense or detection techniques |
| Credential Access | The technique to access or control the system, domain, and service qualification |
| Discovery | The technique to obtain the knowledge of a system and internal network |
| Lateral Movement | The technique to access and control a remote system over the network |
| Collection | The technique used to identify and collect critical files of a system and network |
| Command and Control | The technique to communicate with the attacker's outside infrastructure from the exploited network |
| Exfiltration | The technique to leak files and information or to escape from the exploited network |
| Impact | The technique to directly reduce the availability and integrity of a system, network, and service |

Of 12 categories, the following 5 categories can be effectively detected in a host. Although other categories can also be detected, they require the detection of the attack tool or installation of additional component for detection. Therefore, there is a limitation of creating the general detection rules for them.

- Initial Access
- Execution
- Persistence
- Defense Evasion
- Lateral Movement

Since the open techniques included in the five categories are all defined, it is necessary to select the most effective technique to establish the detection strategy. Many of the techniques used by attacks are also used for management purposes. Therefore, selecting a wrong detection strategy can increase false detection and make it even more difficult to operate the security system.

CrowdStrike's Global Threat Report 2019 introduced the results of applying the exploitation techniques surveyed last year to the ATT&CK matrix. The following table shows the frequently used techniques for five of the above categories.

[Table 2] Frequently Used Attack Techniques Introduced by Global Threat Report 2019

| Category | Frequently Used Techniques |
|---|---|
| Initial Access | Valid Account, Exploit Public-Facing Application, Supply Chain Compromise, Drive-By Compromise, SpearPhishing Link / Attackment |
| Execution | Comand-Line Inerface, PowerShell Scripting, WMI, Graphical User Interface, Rundll32, Scheduled Task, Service Execution |
| Persistence | Valid Accounts, Web Shell, Registry Run Key / Startup Folder, Scheduled Task, New Service, Create Account, Account Manipulation |
| Defense Evasion | Valid Accounts, Scripting, Masquerading, Disabling Security Tools, File Deletion, Obfuscated Files or Information, Process Injection, Rundll32 |
| Lateral Movement | Windows Admin Shares, Remote File Copy, Remote Desktop Protocol, Remote Service, WMI |

The most frequently used technique between all categories is "Valid Accounts". The attacker performs the initial exploitation, continuity, and defense avoidance through an account that has a valid qualification certificate. Without the audit of account usage, it would be difficult to detect or defend against exploitation, since it is difficult to distinguish an attack through a valid account from normal behaviors. As a result, the detection of malicious attack techniques can be effective only when it is performed within the appropriate-level internal control.

### 4) Detection Using Event Logs

Many enterprises have considered the introduction of the EDR (Endpoint Detection and Response) solution.

As the name suggests, EDR helps to detect and respond to the endpoint environment. The automated detection ability of EDR does not differ much from the existing host security products. However, many EDR solutions support the application of user-defined rules in addition to automated detection. The effectiveness of the EDR is determined by how these rules are defined. Let us define the rules based on the above described ATT&CK matrix technique by assuming that there is no insight into exploitation detection. Although there would be many false positive and excessive detections early, one can receive new insight into the organization environment, which was not available before.

One can consider the detection using event logs if there is no EDR solution or no plan to procure it. The default event log setting of Windows has insufficient capacity and audit items for detecting or responding to exploitations. Therefore, it is necessary to enhance the event log setting. Even when operating the EDR, the host retains the logs only for about one month. It would be good if the good detection rules can identify all attacks within one month, but it would be difficult to find the cause of exploitation with only the host logs provided by the EDR. Therefore, the following event log setting is recommended for all Windows systems in an enterprise. The size of the log should be as large as possible in the environment, and the system audit policy should be modified or added to be compatible with the internal security policy.

[Table 3] Minimum Recommended Setting of Event Logs

| Type | Settings |
|---|---|
| Event Log Size | ● Main event logs (system, security, and application program): Increase to 1–4 GB<br>● Other logs that help to respond to exploitations: Increase to 100 MB or more<br>ㄴ Powershell–related logs<br>ㄴ RDP–related logs<br>ㄴ Storage unit–related logs<br>ㄴ Wired/wireless connection–related logs |
| Strengthening of System Audit Policy | ● Account logon<br>ㄴ Kerberos authentication service audit (success, failure)<br>ㄴ Kerberos service ticketing audit (success, failure)<br>● Account management<br>ㄴ Computer account management audit (success)<br>ㄴ User account management audit (success)<br>● Detailed tracking<br>ㄴ Process creation audit (success)<br>ㄴ Process termination audit (success)<br>● Logon/logoff<br>ㄴ Logon audit (success, failure)<br>ㄴ Logoff audit (success, failure) |

Sysmon [3] It is recommended to enhance the event log by installing Sysmon if it is available. Although Sysmon offers many benefits, some enterprises are cautious of it because of the need to install additional drivers in the host.

3) https://docs.microsoft.com/en–us/sysinternals/downloads/sysmon

The default size of the Sysmon event log is 64MB, and it is necessary to increase its size after the installation of Sysmon. Detection of Sysmon patterns according to the attack pattern can substitute the detection function of the EDR. However, not setting the exception handling would generate too much noise to make it difficult to identify events, and it is necessary to modify the configuration file. Refer to the following open source for Sysmon settings.

● Sysmon-modular, https://github.com/olafhartong/sysmon-modular

If Sysmon is not available, one must use the audited event logs to detect the events related to targeted attack techniques. The following table shows examples of detecting events related to targeted attacks.

[Table 4] Examples of Using Event Logs to Detect Events Related to Targeted Attacks

| Event Log | Detection Measures |
|---|---|
| Security.evtx | Detection of abnormal logons using the logon event type, account, process, and network address |
| | Detection of abnormal account generation and account privilege modification |
| | Detection of malicious processes running using the image path, PID, and PPID of the created and terminated process |
| | Detection of security log delete events |
| System.evtx | Detection of the system time changing events |
| | Detection of the event log delete events (logs excluding security logs) |
| Windows PowerShell.evtx | Detection of the trace of attack script running using PowerShell |
| Application-Experience%4 Program-Telemetry.evtx | Detection of malware running that has the compatibility problem |
| TerminalServices*.evtx | Detection of using remote access protocols (port change, port forwarding, reverse connection, etc.) |
| WMI-Activity%4 Operational.evtx | Detection of attack behaviors using the WMI command |

If it is difficult to monitor various events, it should be possible to detect at least the "event log delete" events. The attack usually deletes the system event logs to remove its trace before moving to another internal system. Therefore, even only monitoring event log deletion can increase the possibility of identifying the attacker before it achieves its purpose. Refer to the following open source for identifying the attack technique through event logs.

● EVTX-ATTACK-SAMPLES, https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES

What is necessary with the event detection is to find the cause of the event generation and track and delete it from the enterprise systems and to manage accumulated TTP to establish the strategy to cope with re-attacks by the same attacker.

### 5) Conclusion

This section briefly reviewed the strategy of detecting targeted attacks in the host. It is difficult to detect targeted attacks with static rules since they vary widely according to the target environment. Therefore, it is necessary to understand the techniques used by targeted attacks and to distinguish them from normal behaviors in the business environment of the organization.

When a distinguished event is detected, it is necessary to analyze the cause and remove the cause to enhance the security control, instead of initializing the detected system. Initialization may be beneficial right away, but it makes it more difficult to detect the attack in the long-term, since the attack can be more cautious and use a bypass path.

We know our security environment more than anyone outside. Likewise, since targeted attacks change according to the security environment, we can implement the strategy of detecting and responding to the attacks against our security environment better than anyone. We must take action before it is too late.

# 3. Advance prevention of cyberattacks through simulated training of response to cyber threats

Internet Security Response Team, KISA
Kang Tae-woo, Senior Researcher

The Training Group of Korea Internet & Security Agency (KISA) received an urgent call. "We are experiencing a huge volume of DDoS attack traffic into our web server." The staff at the Training Group got busy as soon as they received the call. Afterward, the skillful actions by the enterprise and KISA defended the DDoS attack flawlessly, and the attack subsided quickly.

This is part of a simulated training for response to cyber threats, not an actual attack, jointly carried out by KISA and enterprises to inspect the readiness to cyberattacks and increase the awareness of security.

KISA conducts the joint simulated training of cyber threats with various private sector enterprises three times each year.

## 1) Purpose of simulation training

KISA strives to enhance security in the private sector. Although the response to cyber intrusion is important, enhancing the awareness of security in enterprises before the incident and inspecting the response capability to enhance the ability to cope with the incident flexibility is crucial. As such, KISA conducts the joint simulated training of cyber threats with private sector enterprises three times each year. We work with a wide range of enterprises that have suffered from exploitation and those that are targets of recent cyberattacks to help them to prepare for cyberattacks. The training is divided into the three areas of APT training, DDoS response training, and website simulated exploitation.

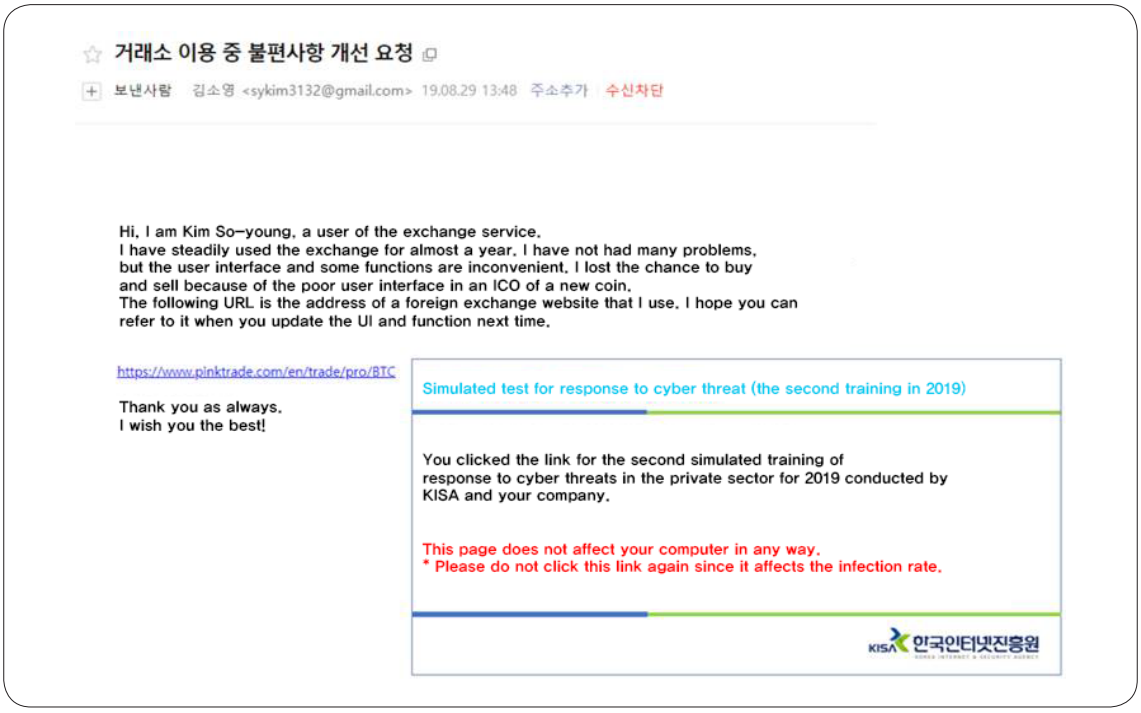
## 2) Areas of simulated training

The simulated training of the response to cyber threats is conducted jointly with a wide range of enterprises, including telecommunication carriers, vaccine developers, manufacturers, and others.

Moreover, KISA conducts the training with the enterprises that recently suffered from or have been targeted by cyberattacks to prevent or reduce the possibility of re-attacks. In 2019, virtual currency trading companies participated in the training to prevent recently active cyberattacks related to virtual currency.

### 2-1) APT training

The Advanced Persistent Threat (APT) malicious email training reflects the latest cyber threat issues. It conducted responses to APT malicious email training using the email statements that targeted enterprise employees and simulated stealing of information from users by inducing them to download malware or click malicious links. Moreover, it sent a malicious email specifically to each enterprise group to induce them to open the email and click the link. For example, it sends a malicious email related to actual issues such as corporate line usage or quality inquiry to a telecommunication carrier, a product quotation inquiry to a manufacturer, and a virtual currency trading website problem to a virtual currency exchange.




[Figure 27] Malicious Email for APT Training

The above figure shows a malicious email sent to the employees of a virtual currency trading company in 2019. We sent an email requesting improvement of UI to exchange employees with a fake account. The attached link is a malicious link disguised as a foreign virtual currency exchange. When the receiver of the email clicks the link, personal information such as the user's IP address and user name is stolen to identify the infected user. It displays a popup window to inform the infected user that it was an email for training and notifies the security team.

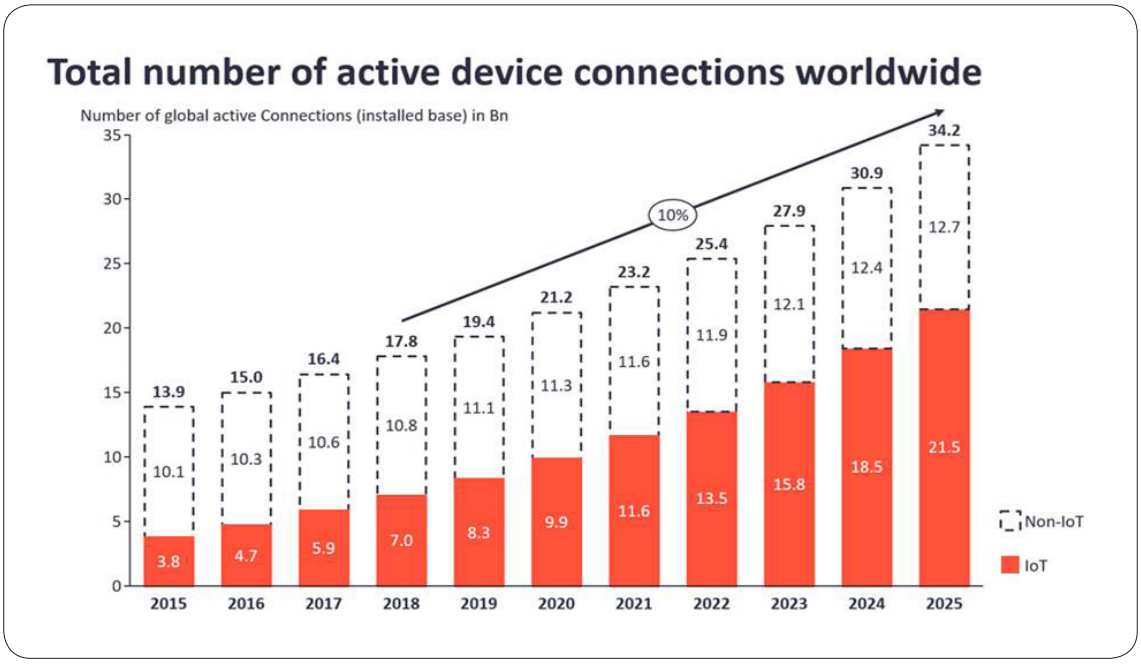
APT email training is conducted as follows:

- KISA is notified when a malicious email is found.
- The number of emails, number of infected users, and the follow-up measures in each enterprise are sent to KISA.
- The information on the attack against the enterprise is delivered by assuming a specific cyber incident situation.
- The countermeasures to the cyberattack are established and delivered to KISA.
- The information collecting site and malicious email distribution site used in the cyberattack are blocked.

### 2-2) DDoS defense training

A DDoS attack shuts down the targeted Internet service by generating a large volume of traffic that the service cannot handle. It creates a zombie BotNet worldwide and generates the attack traffic simultaneously against a specific target. DDoS attacks using IoT devices have been increasing as more IoT devices are distributed. For example, the 1.2TB attack that targeted a large DNS service company Dyn is known to have mobilized 50,000 IoT devices, including IP cameras and DVRs.

As such, KISA needs to work with enterprises to help them to respond better when a DDoS attack occurs. DDoS response training is conducted with enterprises that have a web server or DNS server. The simulated DDoS attack is generated at the same level as the actual attack traffic using a traffic generation and distribution server constructed in KISA. In the first half of 2019, 23 enterprises participated in the DDoS response training that generated up to 20 GB of attack traffic. The attacked enterprise notifies KISA of the attack in real-time and responds to it. The enterprises familiarize themselves with the series of procedures regularly to prepare for actual attacks.




[Figure 28] IoT Device Distribution Rate 〈Source : Akamai 2019 Report〉

DDoS response training is conducted as follows:

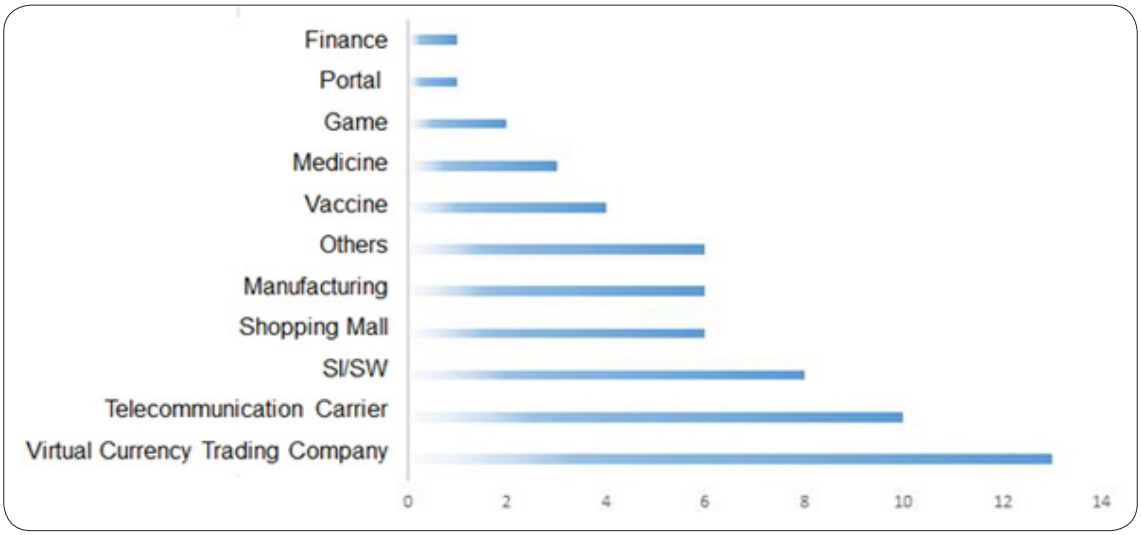
- The DDoS attack traffic is identified.
- The defense against the attack is performed, and the attack is reported to KISA.
- The attack type and attack IP are secured.
- The normalization of the attacked service is confirmed after the attack is extinct.
- The follow-up results of each enterprise are submitted to KISA.

### 2-3) Simulated exploitation training

The simulated exploitation training is conducted to check the web vulnerabilities of enterprises operating websites. KISA works with white hackers to attack the websites and identify the vulnerabilities. The simulated exploitation training provides training for the response to incidents such as web tampering caused by website vulnerability and prevents future cyber accidents by detecting and acting on vulnerabilities in advance. The training in the first half of 2019 recruited white hackers who received awards in "Hack The KISA" to identify and act on various vulnerabilities of the participating enterprises.

## 3) Overall review of the training results in the first half of 2019

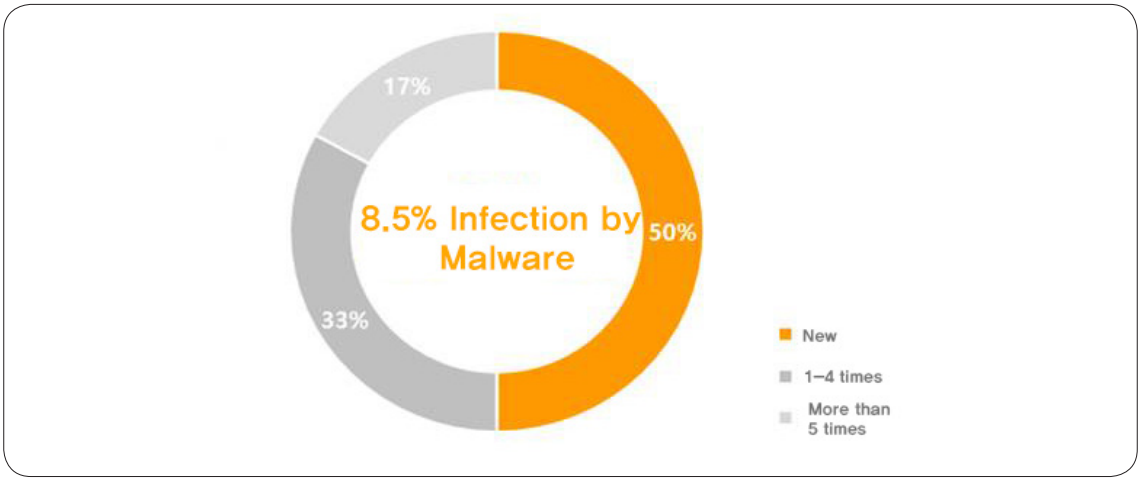
The simulated training for cyber threat response in the first half of 2019 was the historically largest scale of the training program. More than 25,000 people from 60 enterprises participated in the training. The scale was more than twice the training in the first half of last year, in which about 9,200 people participated. The scope was also broadened to telecommunication, vaccine, shopping, medical, and virtual currency trading industries.




[Figure 29] Businesses Participating in Simulated Training in the First Half of 2019

### 3-1) Results of APT malicious email training

The APT training was participated in by 56 companies, and 19 of them (34%) were new participants. The users who were infected by clicking the malicious link contained in the malicious email sent by KISA were 8.5%, of which the new participating enterprises had more users (12%) than the existing participating enterprises (7%). Moreover, the infection rate of SMEs (13.9%) was higher than that of large enterprises (6.5%).



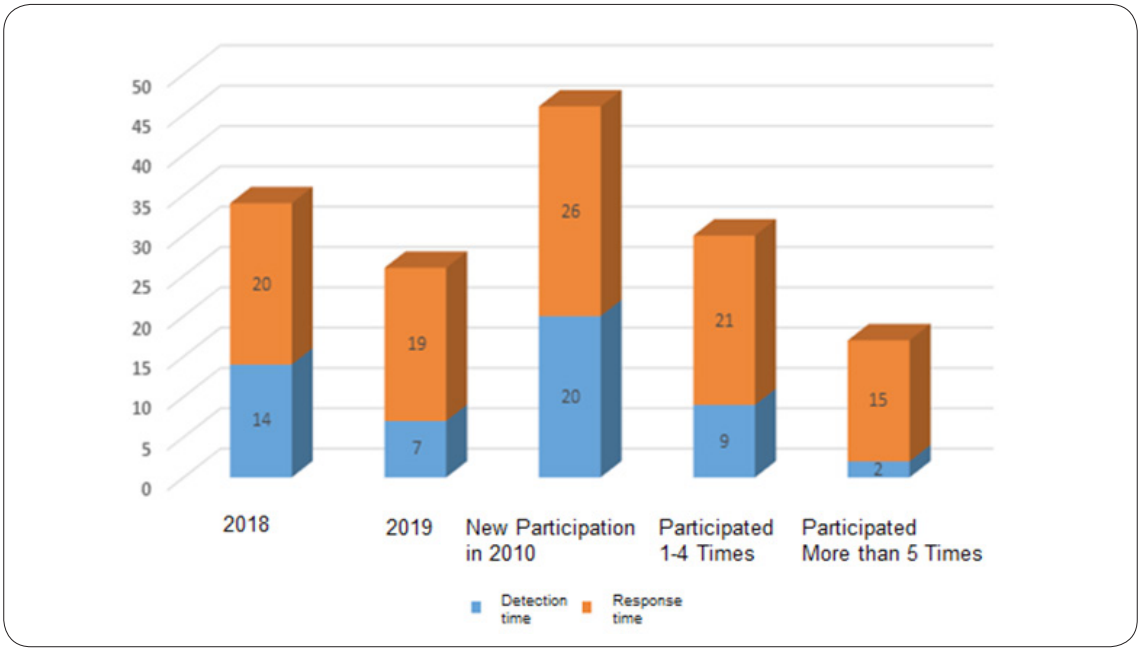

[Figure 30] Malware Infection Rate according to the Number of Participation in Simulated Training

The above results indicate that the continuous training and security education and systematic security education may help to prevent hacking incidents.

### 3-2) Results of DDoS training

The DDoS response training was conducted in the same way as an actual attack. The training generated attack traffic without warning of the time to the participating enterprises. Moreover, it used composite attacks such as attack traffic using IoT devices and attack traffic using reflectors to disguise it as an actual attack. The participating enterprises detected and defended against the attacks without knowing whether the attack traffic was real or for training.

For the training in the first half of 2019, 23 enterprises participated, and the average attack detection time (7 minutes) decreased by 50% compared to the training in the first half of 2018 (14 minutes). This indicates that, because many enterprises are repeat participants (20 out of 23 enterprises), they have improved the capability to respond to DDoS attacks.




[Figure 31] DDoS Detection and Response Time

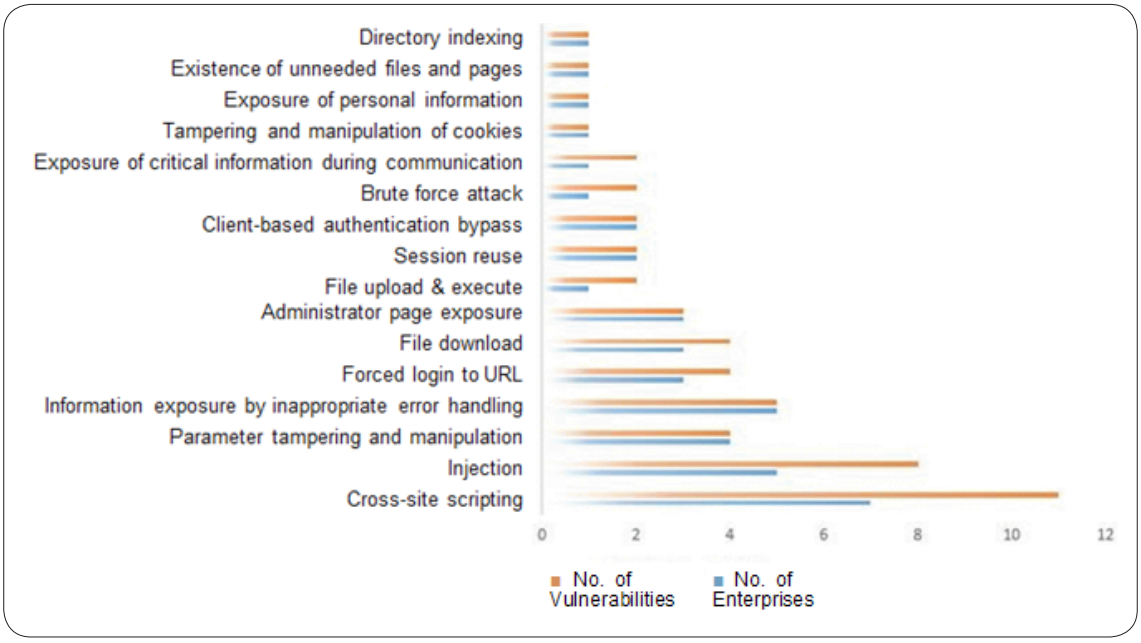
※ Detection time: Time from initiation of the DDoS attack to recognition of the attack by the participating enterprise
※ Response time: Time from initiation of the DDoS attack to response to the attack and reporting by the participating enterprise

### 3-3) Results of simulated exploitation training

KISA worked with white hackers to inspect web vulnerabilities through simulated exploitation training. The white hackers were simulated exploitation specialists and the winners of the "Hack The KISA" contest held by KISA.

Various vulnerabilities were found in simulated exploitation. 16 enterprises among the 23 participating enterprises found 16 types of vulnerabilities (a total of 53 cases).

The training found vulnerabilities that can lead to actual hacking incidents such as stealing of duplicated administrator privileges and leakage of personal information and led to immediate correction.

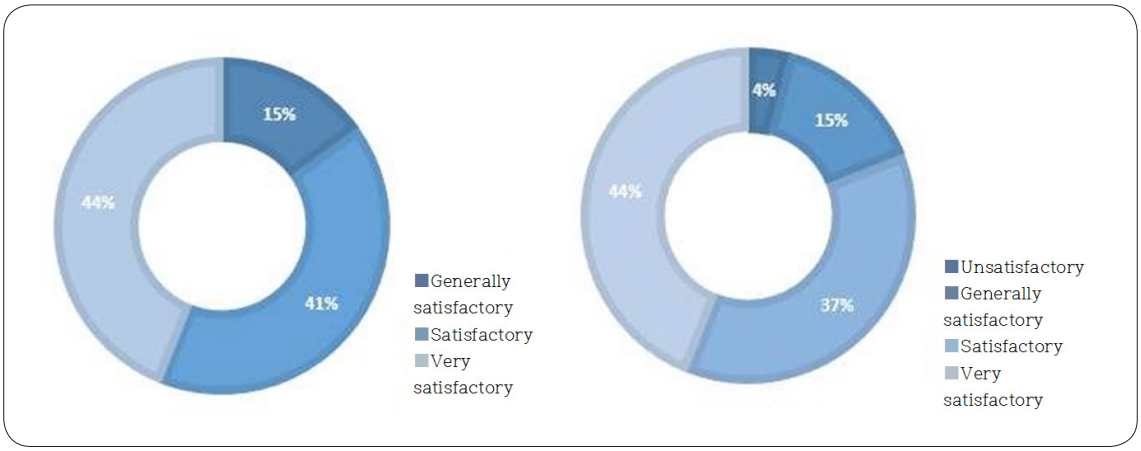



[Figure 32] Vulnerabilities Found after the Simulated Exploitation

### 3-4) Training effect and survey results of participant satisfaction

We conducted an online/offline survey to collect the opinions of participating enterprises after the simulated training and provide a better training opportunity.

89% of participating enterprises answered that the security awareness of their employees had increased, and 81% of the participating enterprises answered that the vulnerable systems and the response system and awareness of internal cyberattack were improved.




[Figure 33] Satisfaction with Preparation of Simulated Training (Left), Satisfaction with Simulated Training Execution (Right)

The satisfaction with the preparation, PR, and briefing of the simulated training was very high at 85%. However, there was a request for better PR to encourage participation from enterprises that were not able to participate in the training. As such, KISA plans to broaden participation by diversifying the PR channels to better advertise the simulated training and encourage new enterprises to participate.

The satisfaction with the time of simulated training and the training program was 81%. As a reason for dissatisfaction, most responded that the content of the malicious email distributed for the APT training was somewhat unrelated to the business of the participating enterprise. As such, KISA is considering the enhancement of the training content by reinforcing customized content beyond the current APT malicious email training, specific to each business type and constructing a database of malicious emails.

### 4) Stories behind the training

As the training in the first half of 2019 was the largest in its history, it generated many interesting stories. One of the examples regarding the APT training email was one that claimed that the receiver violated personal copyright with the attached malicious link.

There was a wide range of responses from employees who received the malicious email. The responses included the "report" type who claimed that he or she never infringed on copyright and felt that his or her personal information was leaked and thus planned to report it to the cyber authority. Others included a "mocking" type, recognizing that it was a spam email and mocked it in reverse, and an "apologizing" type in which the receiver asked which copyright was infringed and asked for forgiveness. There were even abusive responses that embarrassed everyone with verbal harassment, which may be considered as an appropriate response to a malicious email.

Moreover, because the DDoS training was conducted without announcement, it generated various episodes as the participants could not distinguish the training attack from a real attack. As an example, there were several urgent inquiries from participating enterprises that they were experiencing a large volume of DDoS attack and asking whether it was training. We checked the situation and found that KISA did not send the traffic, and an unknown DDoS attacker was actually attacking the calling enterprise. Perhaps, such confusion by the portals and shopping malls, which are routinely subjects of DDoS attacks, is in line with the purpose of the DDoS response training of attacking and defending websites from sudden attacks.

### 5) Conclusion

KISA is expanding and enhancing the training each year to improve the ability of private-sector enterprises to respond to actual cyber incidents.

We plan to continually expand the simulated training of response to cyber threats. Repeated inspections of response procedures through training are a good way to actively secure the capability to respond to cyber incidents. We expect more enterprises to participate in the training to improve their ability to respond to incidents.

# KISA Cyber Security Issue Report : Q3 2019

Printed in October 2019
Published in October 2019

Publisher | KOREA INTERNET & SECURITY AGENCY

IT Venture Tower, 135 Jungdae-ro, Songpa-gu,
Seoul, Korea, 05717

TEL : 82-2-405-5597

# KISA Cyber Security Issue Report : Q3 2019