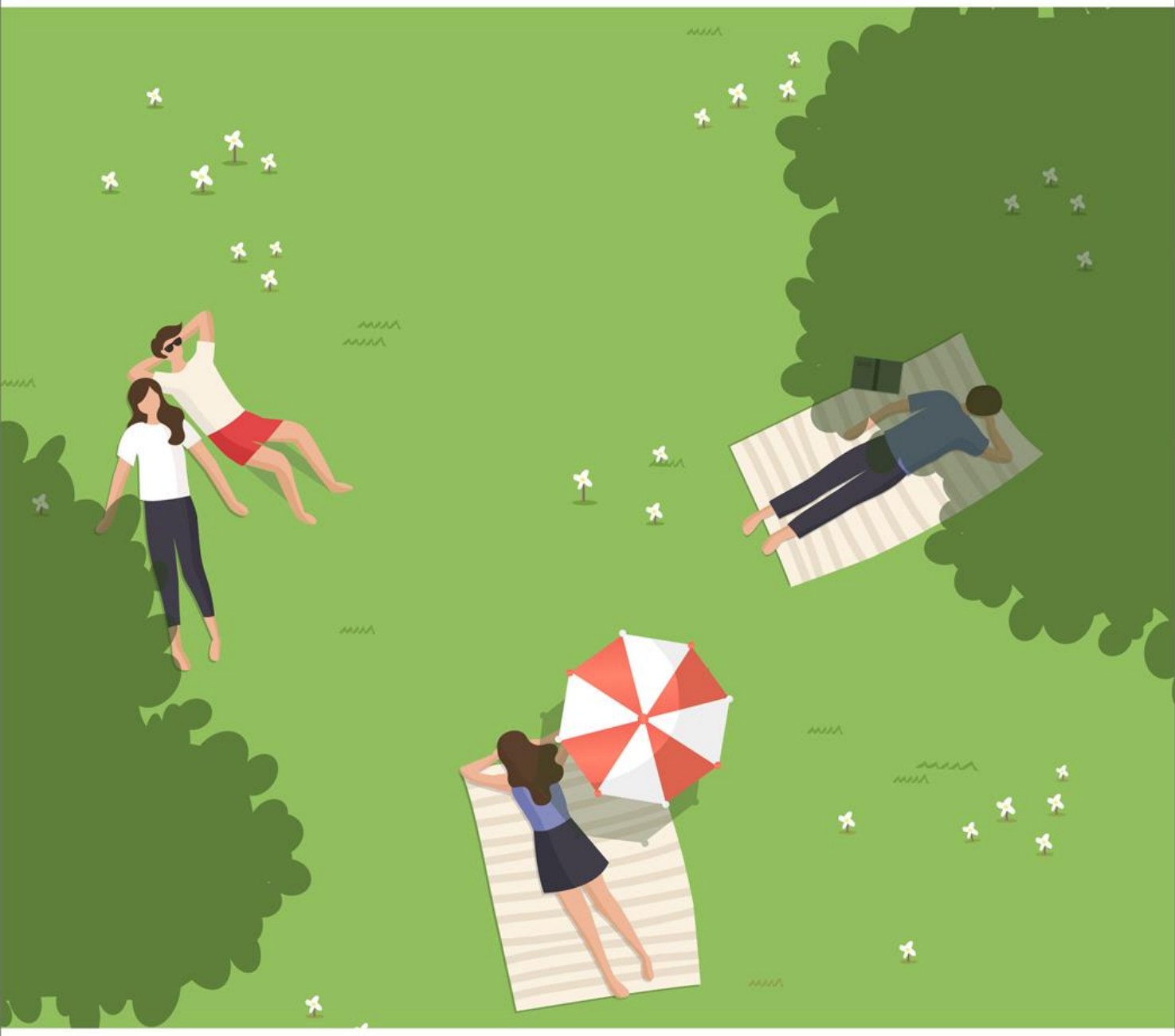
Monthly Security Report

2020
May



Cover Story

- System monitoring through general log collection
- Security issues and countermeasures due to untact work system
- Ransomware of industrial control system as an example

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. SIEM Guide (SPiDER TM V5.x)

- System monitoring through general log collection

4. Tech Note

- Security issues and countermeasures due to untact work system

5. Special Column

- Ransomware of industrial control system as an example

6. Focus On IGLOO Security

- This month’s IGLOO Security

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

CHAPTER 1

Monthly Security Issue

1. Security issue

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

1 Security Issue

'Zoom' member information and hacking method found on the dark web… Requires user attention

- In the dark web, a hacking method for the video conferencing solution “Zoom” has been traded, so user attention is required.
- According to IntSights, a threat intelligence agency, the Dark Web has revealed a database containing more than 2,300 Zoom account and password combinations.
- In addition, a number of zoom hacking methods have been found that attempt to log in to Zoom using existing leaked user account information, collect only successful accounts, and re-release them on the Dark Web or infect malware on the PC and steal zoom account information.
- The United States, Taiwan, Germany, Australia, and Singapore have banned the use of “Zoom” because of concerns about security issues such as so-called zoom bombing attacks and privacy leaks, which are terrorist attacks on security loopholes.
- According to the US media ‘The Burgess’, the zoom call is given a randomly generated 9-11 digit access number.
- In addition, Zoom explained that they applied AES-256 encryption technology to his solution, but it turns out that he used AES-128, which is rarely used because of the lack of encryption.

Zoom impersonation attack soaring

- As the popularity of video conferencing solution “Zoom” has skyrocketed due to the increase in the introduction of remote work and education, attacks that exploit it are rapidly increasing.
- According to the security company Webroot, malicious files, including zoom in the file name, increased by 2000% in March compared to February. As the amount of zoom is rapidly increasing, it is analyzed that the attention of hackers is focused on zoom users.
- Security experts predict that attacks targeting specific usage-intensive solutions, such as Zoom and Microsoft Teams, will increase rapidly as the worldwide COVID-19 spreads.

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

1 Security Issue

Warning for threatening spam emails requiring Bitcoin

- Threatening spam e-mails are being distributed asking for bitcoin by threatening 'to spread the use of pornography.' This is to increase fear by specifying the user account password that appears to have been leaked in the subject and body of the mail.
- According to AhnLab, the attacker ‘obtained all PC information and SNS contact information. If you do not send Bitcoin, you will disseminate pornography access records and watch videos as contacts in your address book. '
- Given that there is no date and time of pornography access and video capture images in the body of the mail, it is presumed that the attacker sent an intimidating message using the account information previously leaked, regardless of whether the user accessed the pornography or not.
- Security experts are advised to change the passwords of all website accounts that use these passwords to prevent further damage, if the usual passwords are included in these threatening emails.

Malicious files disguised as mask-related information documents are also found

- In COVID-19, another malicious file disguised as a mask-related information document was discovered.
- According to East Security, the malicious file was distributed under the name of guidance. If you open the document, malicious code can be installed and the main information can be stolen.
- The attack is believed to have been the result of a hacker organization called "Konni," which has been conducting intelligent persistent threat (APT) attacks over the past few years based on the support of a specific government.

COVID-19 Vaccine Research Institute Injured Target of Hacking

- With the spread of Corona 19, cyber attacks targeting the Corona 19 vaccine laboratory are increasing. The United States Federal Bureau of Investigation (FBI) has pointed to a government-supported hacking organization behind the attack.
- Tanya Yugoretz, deputy general manager of the FBI Cyber Department, says attackers are attempting to steal research results and information by focusing on medical institutions externally known for conducting research related to COVID-19.
- Since the early days of COVID-19, there have been concerns about hacking to steal Corona 19 treatment and vaccine information. In March, two government-supported hacking groups were caught trying to hack into the World Health Organization (WHO), and cyber attacks aimed at the pharmaceutical industry are also known to deepen.

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

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

In the top 10 of vulnerability attacks collected during the month of May 2020, many attacks using the DrayTeck Vigor RCE (CVE-2020-8515) vulnerability and phpMyAdmin and WordPress pages were found.

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

Rank	Pattern	No. of cases	Ratio(%)	Fluctuation
1	DrayTek Vigor RCE (CVE-2020-8515)	1,710	29.40%	NEW
2	phpMyAdmin sample page access	625	10.75%	NEW
3	MVPower DVR Shell Unauthenticated Command Execution	607	10.44%	NEW
4	ThinkPHP Remote Code Execution Vulnerability	505	8.68%	NEW
5	WordPress sample page access	445	7.65%	NEW
6	Netlink GPON Router Remote Code Execution	442	7.60%	NEW
7	SQL Injection	356	6.12%	NEW
8	GPON Router Vulnerability	302	5.19%	NEW
9	Network Scanner(masscan)	282	4.85%	NEW
10	Command Injection (Netgear Routers Vulnerability)	274	4.71%	NEW
Total		5,816	100.00%	-

[Table2-1] TOP 10Top 10 monthly vulnerability attacks

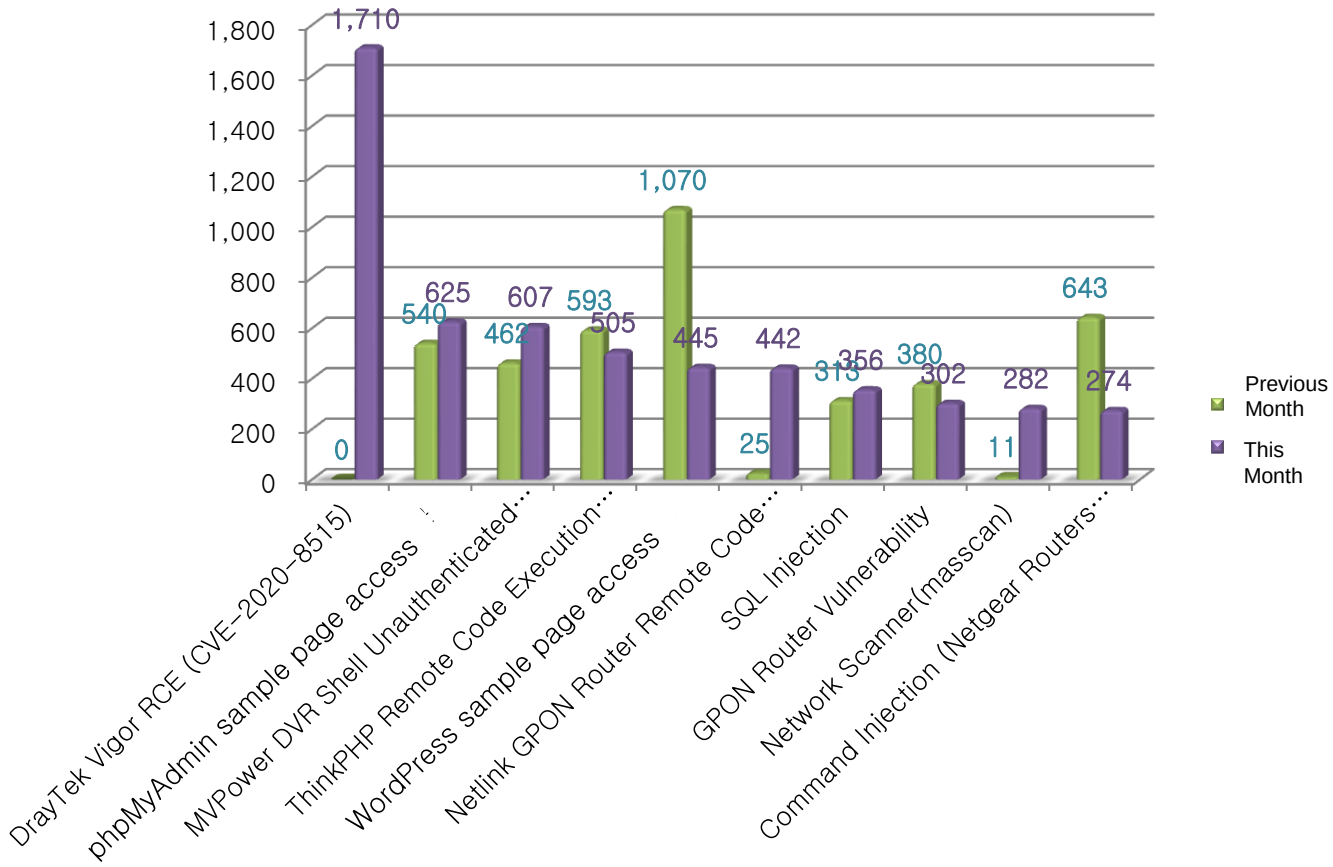
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

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

As a result of analyzing vulnerability events collected for a month in May 2020, a number of attacks using the RayTek Vigor RCE (CVE-2020-8515), discovered as a new vulnerability in 2020, were detected. Vulnerabilities exist in DrayTek's routers and switches, and remote code execution attacks using them are possible. If you are using DrayTek's products, the latest firmware update is required. Subsequently, RCE attacks using web framework vulnerabilities such as IoT and ThinkPHP to form BotNet have been strong.



[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)

In the top 10 service ports collected for a month in May 2020, events using the Unsigned (TCP/9900) port rose compared to the previous month, SNMP (UDP/161), Telnet (TCP/23), MSSQL (TCP/1433), Unsigned (TCP/7178) showed a downward trend compared to the previous month.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of Cases	Ratio(%)	Fluctuation
1	HTTPS(TCP/443)	1,142,799,491	36.78%	-
2	DNS(UDP/53)	1,017,031,888	32.73%	-
3	Microsoft-DS(TCP/445)	274,003,291	8.82%	-
4	HTTP(TCP/80)	210,393,370	6.77%	-
5	Unsigned(TCP/9900)	165,302,101	5.32%	▲5
6	ICMP(0/ICMP)	93,431,858	3.01%	-
7	SNMP(UDP/161)	93,075,768	3.00%	▼2
8	Telnet(TCP/23)	43,219,602	1.39%	▼1
9	MSSQL(TCP/1433)	39,604,322	1.27%	▼1
10	Unsigned(TCP/7178)	28,589,772	0.92%	▼1
	Total	3,107,451,463	100.00%	-

[Table2-2] TOP10 monthly attack patterns

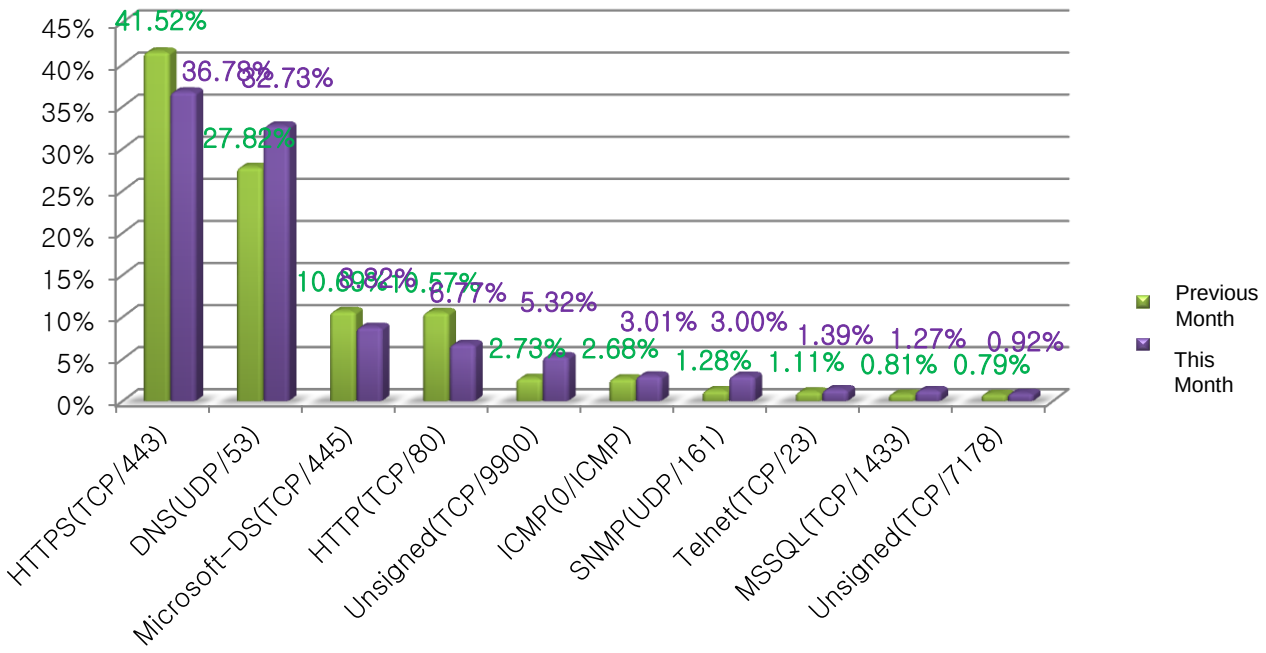
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

1 Monthly attack service and trend analysis

The IGLOO Security SOC collects data on attacks according to the 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 analyzing the events collected during the month of May 2020, the total number of cases decreased slightly, and it is confirmed by the effect of the decrease in the use of HTTPS (TCP / 443) ports. In addition, the number of unsigned (TCP / 9900) cases increased 477% from the previous month, and unknown service ports are changed by using a specific service as a random port, or due to an attacker's attempt to scan for vulnerabilities of unknown services. Therefore, in the case of an externally exposed server, it is recommended to check the open ports through periodic service use checks and establish a policy to limit them.



[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 May 2020, the ranking of Ack Port Scan (F/W Scan) and HTTP Login Brute Force events rose slightly, and it was confirmed that the ranking of Ack Storm and Multi Packet Inspection events fell. Other TLS Malformed Handshake DoS, DNS BIND version request, and HEAD/HTTP (Http server vuffer overflow) events have been newly entered.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of Cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	1,572,294,814	97.67%	-
2	ACK Port Scan(F/W Scan)	10,359,796	0.64%	▲1
3	Ack Storm	10,136,810	0.63%	▼1
4	HTTP Login Brute Force	4,653,216	0.29%	▲2
5	Dcom_TCP_Sweep(MSBlaster Worm Messenger)	4,471,586	0.28%	-
6	Multi Packet Inspection	4,353,200	0.27%	▼2
7	Netbios Scan (Messenger RPC Dcom My Doom) (UDP-137)	2,126,292	0.13%	-
8	TLS Malformed Handshake DoS	900,428	0.06%	NEW
9	DNS BIND version request	298,824	0.02%	NEW
10	HEAD / HTTP (Http server buffer overflow)	265,590	0.02%	NEW
	Total	1,615,141,884	100.00%	-

[Table 2-3] TOP10 monthly attack pattern

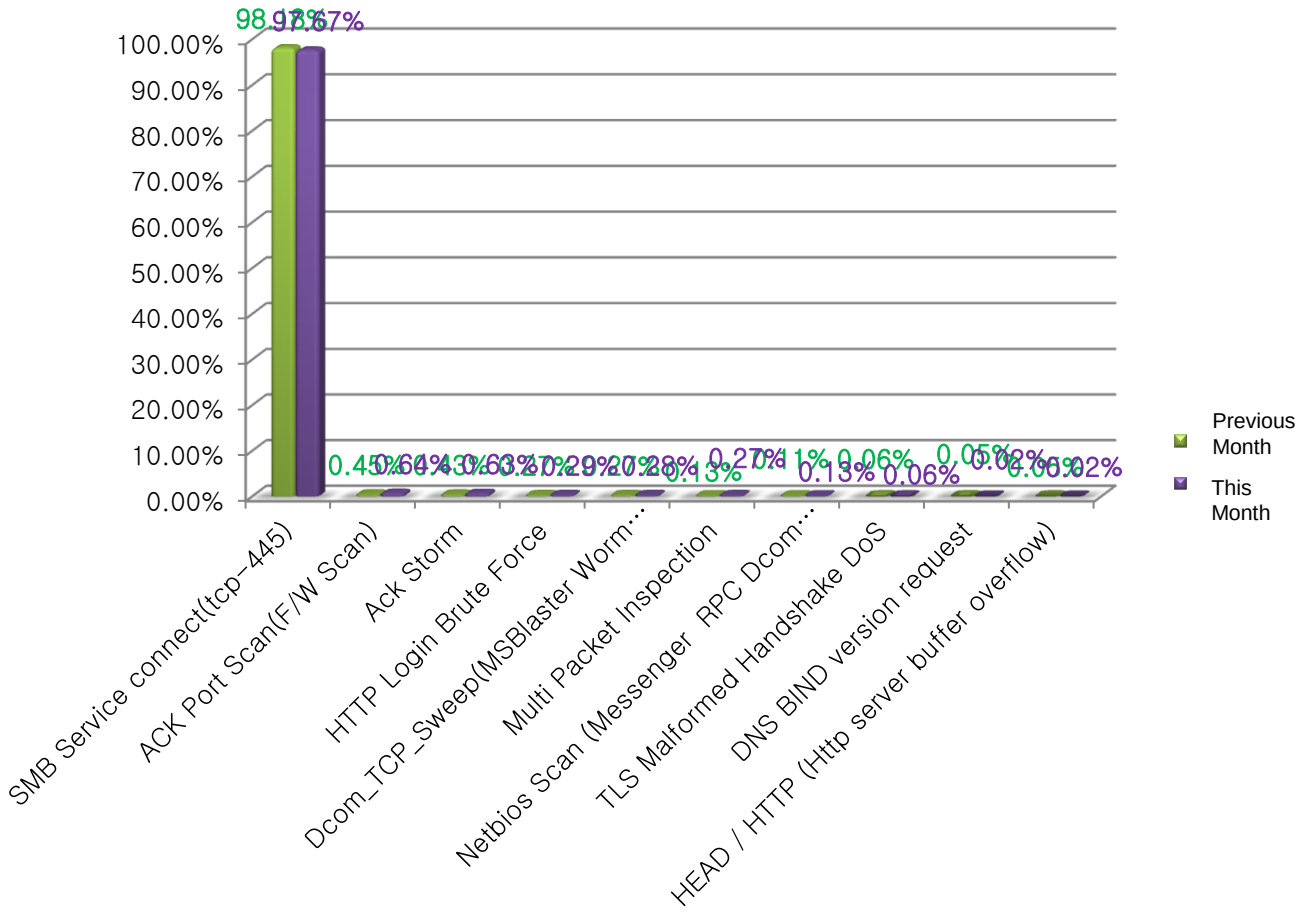
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

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

As in the previous month, scanning attempts to find SMB services are continuously occurring, so it is necessary to continuously manage access control to SMB and Netbios service ports. Scanning events are included in the Top 10, and DNS BIND version request, HEAD/HTTP (http server buffer overflow) events, which are newly identified in the ranking, are also related to scanning. Recommended action to change the named.conf configuration.



[Figure 2-3] TOP10 monthly attack pattern

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

2 Detailed analysis according to different patterns

The results of detailed analysis according to the attack patterns will be introduced, focusing on the TOP 10 among the attack patterns that occurred in May.
The vulnerability of the system should be corrected in advance by referring to the detailed analysis result for each detection pattern.

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 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.
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.
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).
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.
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.
Netbios Scan (Messenger RPC Dcom 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.
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.
DNS BIND version request	The DNS BIND version request attack is an information gathering attack for a malicious user to find out the BIND version, which is one of the DNS server programs.
HEAD / HTTP (Http server buffer overflow)	HEAD requests, similar to HTTP GET requests, are commonly used when using a scanner or when a malicious user is collecting information.

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

CHAPTER 3

SIEM Guide (SPiDER TM V5.x)

System monitoring
through general log collection

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

System monitoring through general log collection

SPiDER TM V5.0 is an integrated security management solution that integrates igloo security's security monitoring experience and big data utilization capability, and increases the agility and efficiency of the control work through a centralized monitoring environment configuration from the first detection to log/network packet analysis.

Technical Support Center
Tech. 1 Team

01. Overview

Today, our SIEM can collect / utilize all logged events, including security events from systems and solutions. However, most customers are using only security-specific solutions that set policies based on security events and use them for analysis when infringement incidents occur.

However, as much as the strengths shown in the area of security monitoring, the methods used to manage systems and solutions are endless. In this issue, let's take a look at how to prevent management and service failures using logging of systems and solutions.

02. SIEM general log

In SPiDER TM V5.0, the log for each process is left in text form, and this is analyzed and used as a trouble shooting when the process operates normally or when a failure occurs.

The table below shows the log location for each process, the log file name, and a brief description of the process.

Location	File	Description
~*Sparrow installed path*/sparrow/logs	indexer.log	Original log parsing and File DB event saving Action log
~*Sparrow installed path*/sparrow/logs	searcher.log	Log search, caching related log
~*TM installed path*/SpDbReader/logs	SpDbReader_js *filename*.log	Integrated device quarry status check log
~*TM installed path*/sptm4/virgo_gm/logs/tm	analyreport.log protection.log sis.log	Real time event analysis, event history analysis Single and correlation analysis statistics and DB insert
~*TM installed path*/sptm4/virgo_sender/logs/tm43	analysis.log statsR.log	Real time raw log transfer to analysis engine(Real time) Create raw log statistics(R process)
~*TM installed path*/SPiDERmwX/logs	spider-x_log.txt spider-x_error_log.txt	WAS, Sparrow, RDBMS communication relay role GM – LM relay role
~*TM installed path*/sptm4/link/logs	statsCheck.log riskcalc.log	Collected/Saved log volume check Risk level calculation module
~*TM installed path*/sptm4/was/logs	siem_app.log siem_error.log spidertm_yyyymmdd.log	SPiDER TM Supervisor (Supervisor page)

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

System monitoring through general log collection

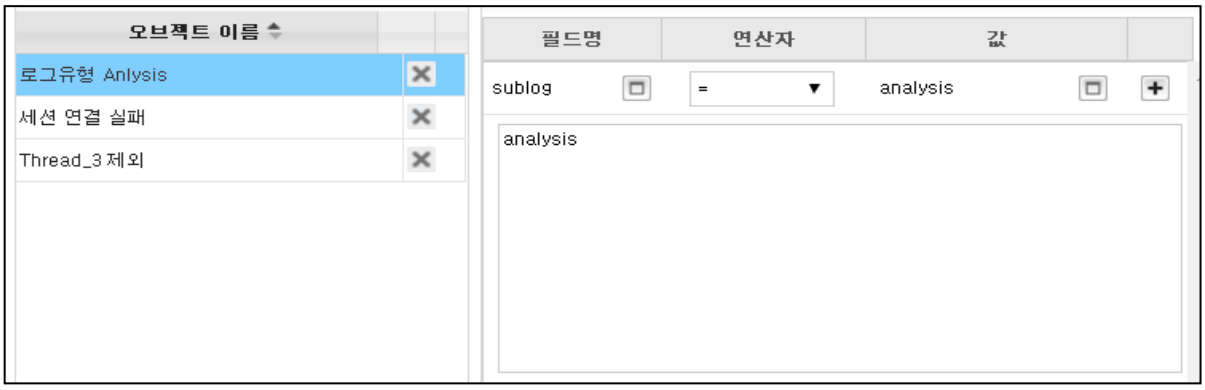
03. SIEM process monitoring

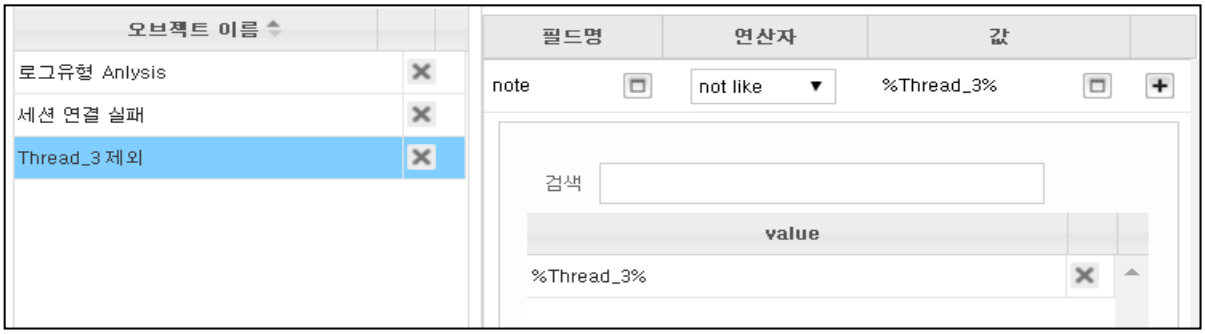
1) Connection fail single alert setting in Virgo GM/LM

상태	룰이름	위험도	발생주기	발생건수	로그소스	조건정의
	Virgo_gm/lm 연결 실패	Medium	1 min	1	로그소스(1)	로그유형 Anlysis,세션 연결 실패,Thread

Set single alert by using connection fail object between Virgo GM and LM Virgo.

- In case, the log type is analysis during the Virgo process
- In case, the result : false sentence is included in analysis.log
- Exclude “Thread_3” phrase in analysis.log



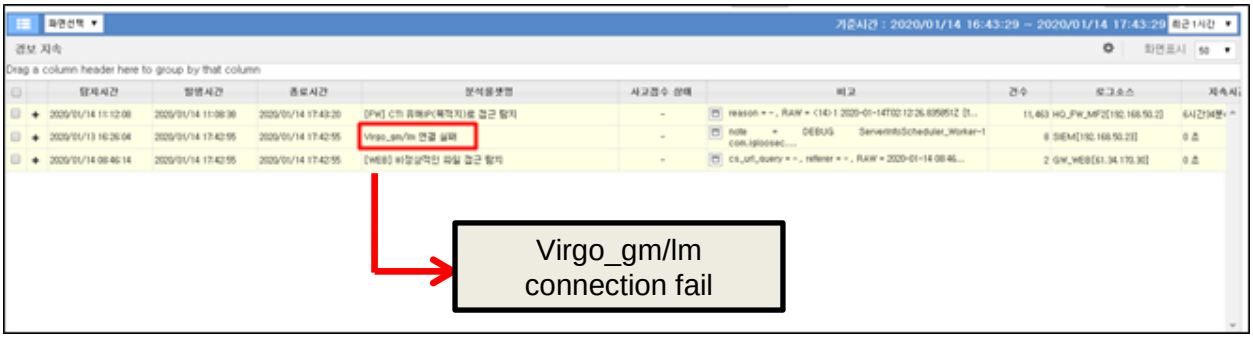


Copyright © IGLOO Security, Inc. 2020. All rights reserved.

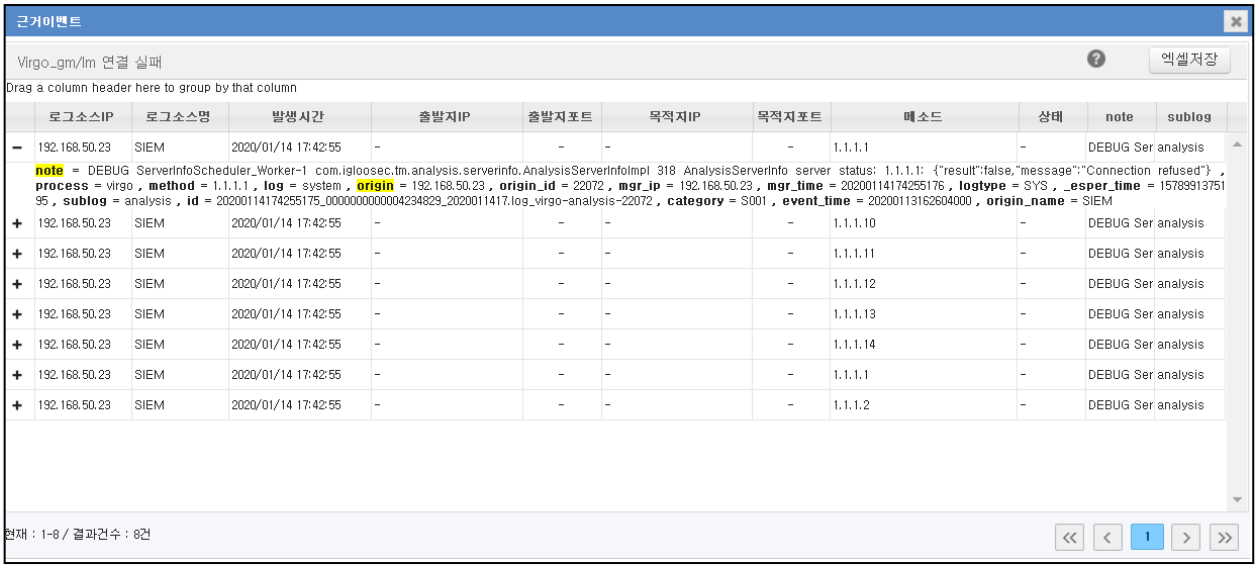
System monitoring through general log collection

▶ Alert occur and analysis

When the session connection between Virgo GM and LM fails, an alert occurs as shown in the figure below.



Evidence event for the generated alert can be checked with [Alert name-click with mouse].



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

System monitoring through general log collection

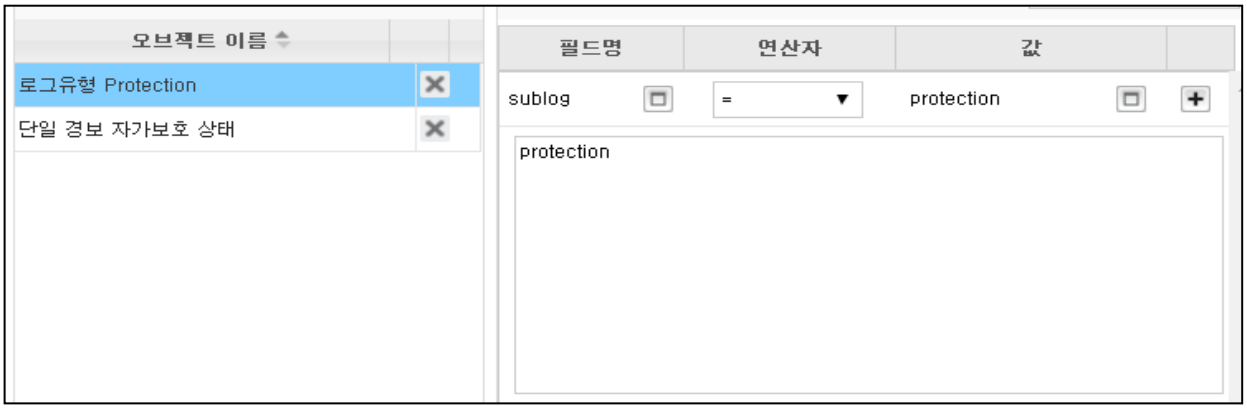
03. SIEM process monitoring

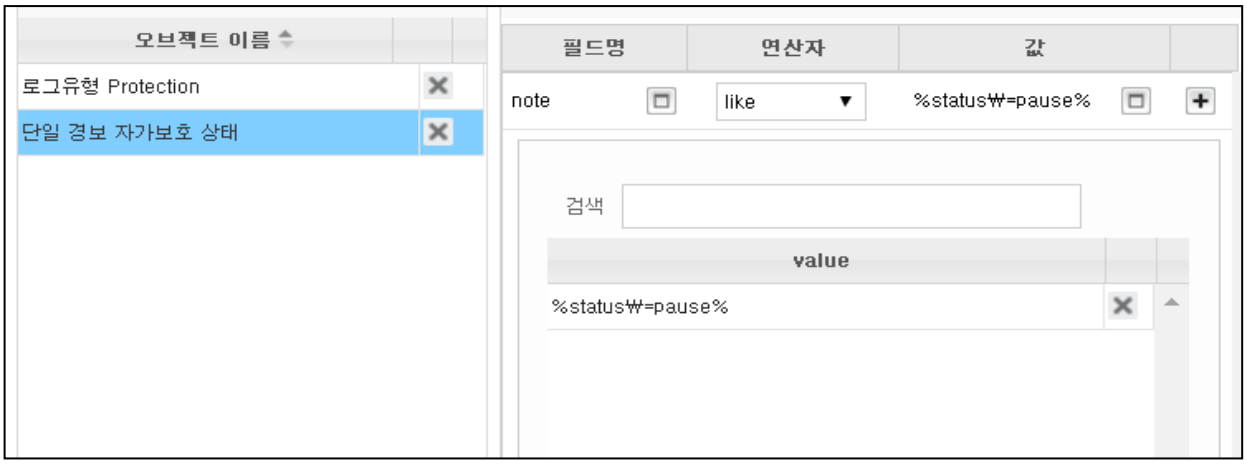
2) Virgo process self-protection single alert setting

상태	룰이름	위험도	발생주기	발생건수	로그소스	조건정의
	Virgo_protection 경보중지 발생	Medium	1 min	1	로그소스(1)	로그유형 Protection,단일 경보 자가보호

The Virgo analysis engine sets a single alert for the policy changed to self-protection due to rule load.

- In case, the log type is protection during the Virgo process
- In case, protection.log log contains status = pause statement





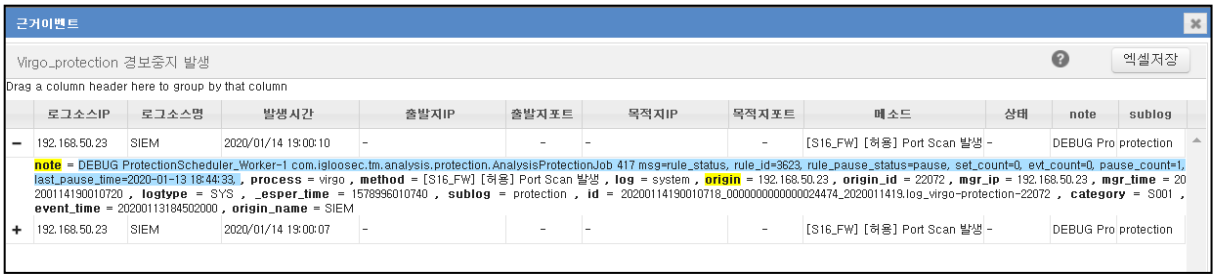
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

System monitoring through general log collection

▶ Alert occur and analysis

When the alert is stopped due to the actual rule load, an alert is generated as shown in the figure below.

Evidence event for the generated alert can be checked with [Alert name-click with mouse].



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

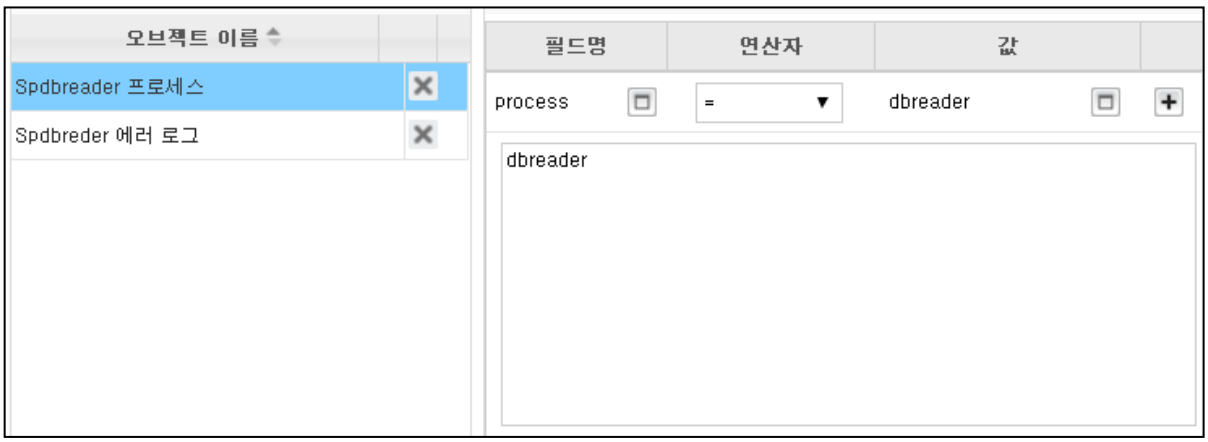
System monitoring through general log collection

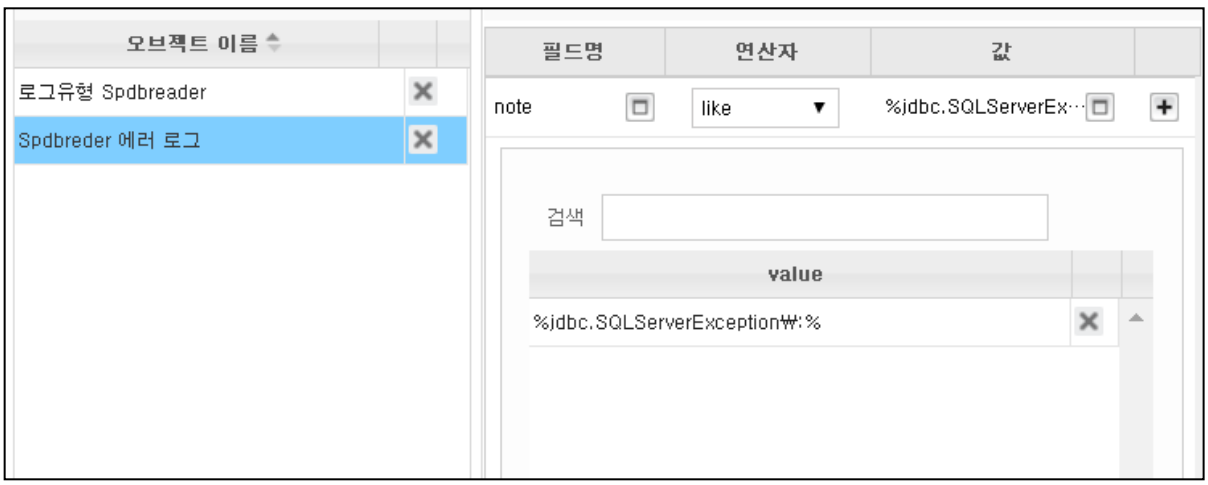
03. SIEM process monitoring

3) SpDbReader error single alert setting

When using SpDbReader process, set a single alert for connection problems with the database.

- In case, The process is SpDbReader
- In case, the jdbc.SQLServerException statement is included in the SpDbReader_error_alyac.js.log log



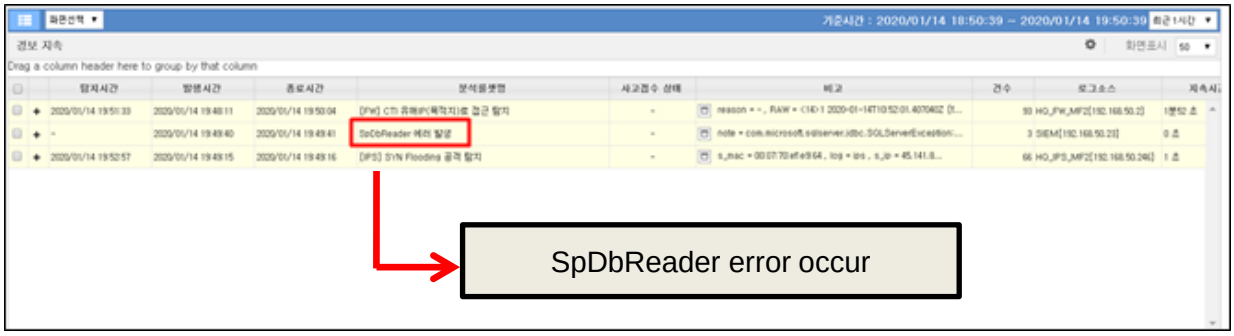


Copyright © IGLOO Security, Inc. 2020. All rights reserved.

System monitoring through general log collection

Alert occur and analysis

If a connection problem with the database occurs while the SpDbReader process is running, an alert will occur as shown in the figure below.



Evidence event for the generated alert can be checked with [Alert name-click with mouse].

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

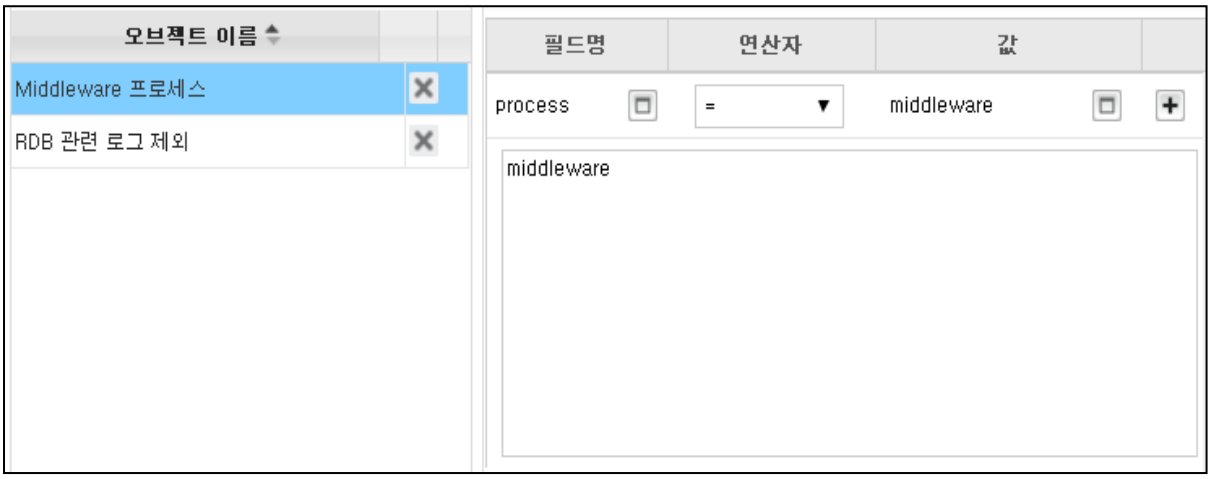
System monitoring through general log collection

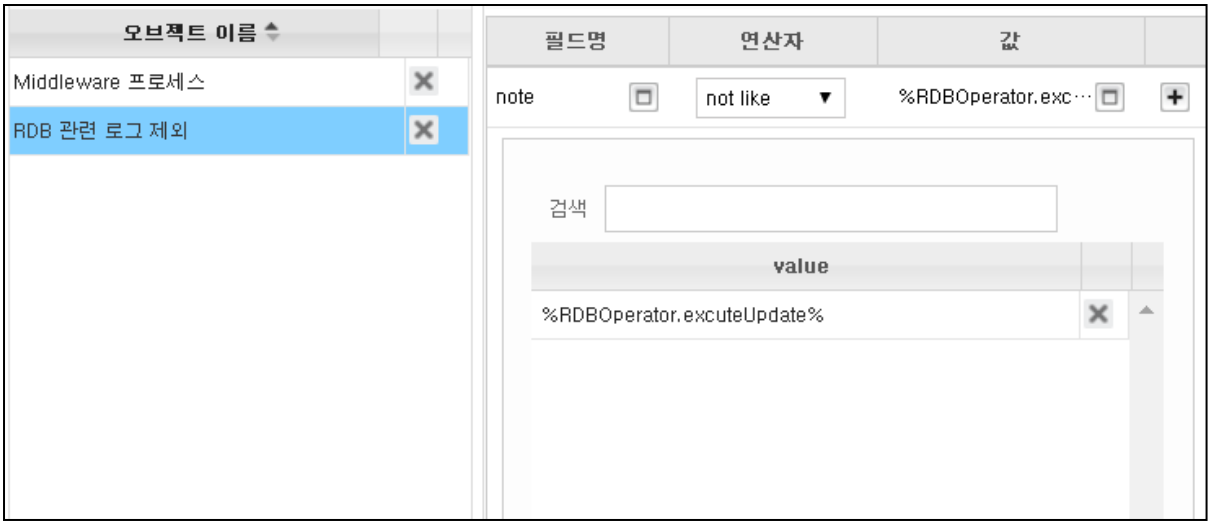
03. SIEM process monitoring

4) Middleware error single alert setting

Set a single alert for multiple problems while using the middleware process.

- In case, The process is middleware
- Exclude RDB related log in spider-x_error_log.txt



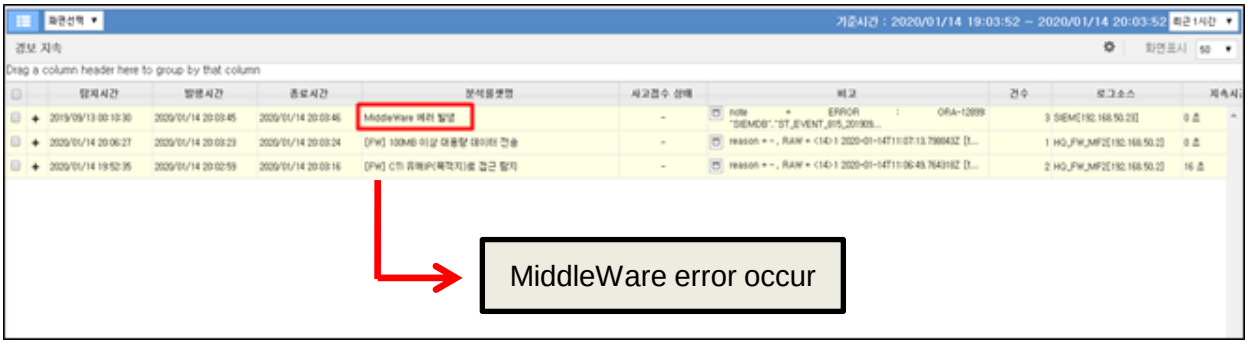


Copyright © IGLOO Security, Inc. 2020. All rights reserved.

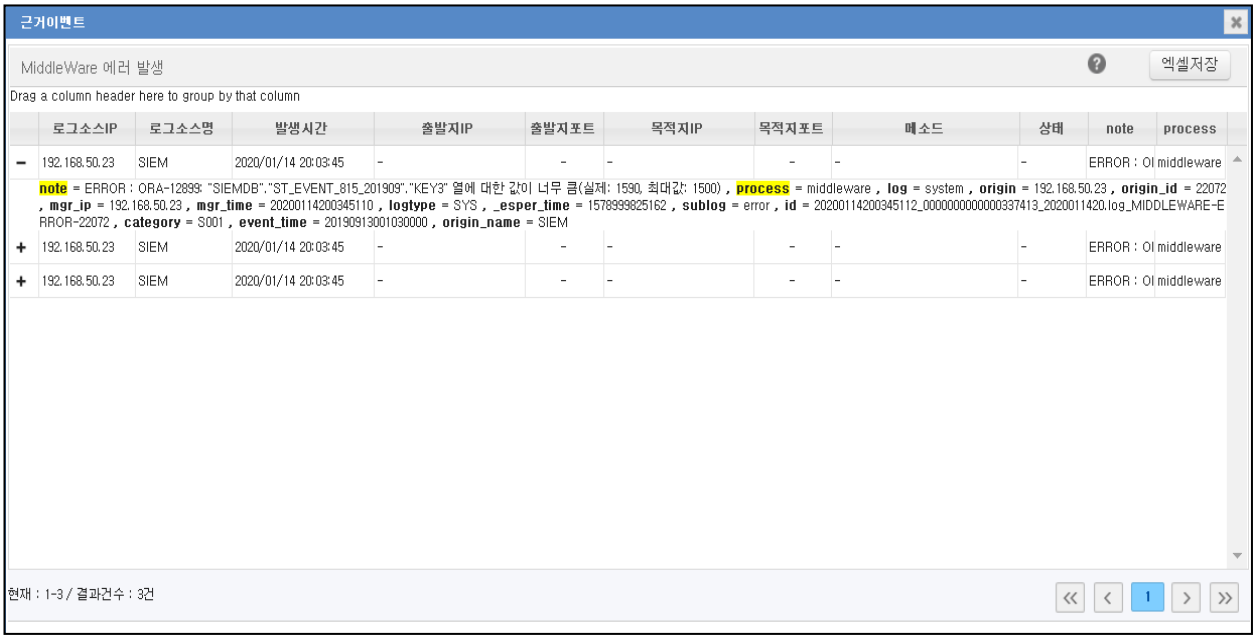
System monitoring through general log collection

▶ Alert occur and analysis

If an error other than RDB appears while the middleware process is running, an alert occurs as shown below.



Evidence event for the generated alert can be checked with [Alert name-click with mouse].



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

System monitoring through general log collection

04. Conclusion

So far, we have examined how to collect and utilize logs required for process management used in SPiDER TM V5.0.

It is composed of the most basic contents, but I think the practical use in the field is endless. Most of the solutions are analyzed and fault response using the log left in case of abnormal operation and error.

The engineer in charge of the solution analyzes and responds based on the log when the problem occurred. Through such collection of logs and policy setting, it is possible to check the anomalies of the solution in advance and to collect practical information according to the generated problem so that a faster response is possible when a failure occurs.

If there is a product that causes difficulties or frequent obstacles to management, I think it is also beneficial to put together a management control using the log of the solution itself.

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

CHAPTER 4

Tech Note

Security issues and countermeasures due to untact work system

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

Security issues and countermeasures due to untact work system

Security Monitoring Center
Security Analysis Team

01. Overview

As the corona virus (COVID-19) spreads around the world, many companies are pursuing an untact work system as part of a “social distance” to reduce the possibility of infection. The introduction of remote collaboration tools and VPNs in the form of software as a service (SaaS) is also increasing to realize a untact work system that can maintain business continuity even when working from home.

In order to convert the work system more conditions than expected should be considered, such as communication among employees, management of work history, and possibility of information leakage.

△ Video conference solution that supports communication between conference participants through voice and screen

△ Messenger that supports rapid opinion exchange and file sharing using text

△ Work-sharing solutions for work issues, processing status, etc. among employees are the solutions that have emerged due to untact work systems.

It is also characterized by using cloud-based PaaS or SaaS rather than being implemented in an internal system to support most various operating systems and working environments.

However, not all business systems can always introduce an external Internet network or cloud environment. Since personal information is stored, or security and important information in the company must still be built in the internal network, a VPN that can safely access the internal network from the outside is also emerging. Telecommuters can secure work efficiency and safety at remote locations through a VPN.

Changes in the work system are not only changing the work paradigm, but also the security issues caused by the new work environment are emerging. Starting with the security issue of Zoom, which has recently been spotlighted as a video conferencing solution, some of the solutions have been restricted due to the emergence of security issues of remote collaboration tools. Therefore, in this issue, we are looking into security issues and countermeasures due to the spread of untact work systems.

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

Security issues and countermeasures due to untact work system

02. Security Issues of Remote Col-work Tools

The introduction of the untact work system does not mean just a change of work place, but a change of the overall process for work. It is the remote co-work tool that supports this change in business processes.

The flexibility of the work type, which was difficult to settle through the 52-hour work system and flexible work system, has been regained by the corona virus, and many companies are seducing users by explaining their advantages and methods of use. We are trying to compete on the platform by providing unlimited chats and repositories, expanding conference participants, and occupying a competitive advantage, and expanding the market share by providing 3rd party product linkage, file storage capacity support, and business management efficiency as a separate license.

Type	Characteristic	Video Conference	Messenger	Work sharing
Microsoft Teams	Unlimited Chat&Video call Team file storage up to 10GB Real-time co-work in Microsoft Office	○	○	○
Zoom	Up to 100 participants in a video conference 40 minutes of meeting Unlimited meetings count Group co-work function	○	○	○
Cisco Webex	Up to 100 participants in a video conference Unlimited meetings duration Webex Teams (Co-work tool)	○	○	○
Slack	Access to 10,000 messages from the team, File storage up to 5GB 1: 1 voice and video calls		○	○
Trello	Unlimited boards Cards can be created Automated application through a rule creation tool called Butler			○

[Table 4-1] Comparison of support functions by remote collaboration tool solution (Support service : ○)

Many companies and organizations are responding quickly to establishing a untact working system due to the expansion of telecommuting, but the security issues that arise after one another have been a chance to reconsider the impact of not considering security when building the environment. .

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

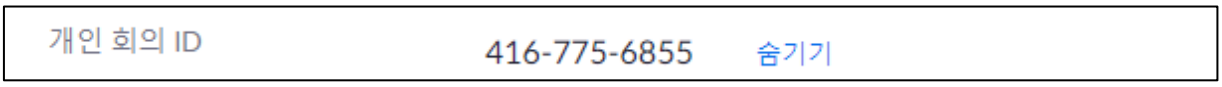
Security issues and countermeasures due to untact work system

1) Video conference

As the business form was changed to untact work system, business processes based on mutual communication were greatly affected. Due to this problem, many companies or institutions have adopted video conferencing solutions, and among them, an application called 'Zoom (Zoom Cloud Meetings)' has been noticed.

Zoom has 100 users free of charge, provides 40 minutes of meeting time, and when used in a PC environment, the video conferencing is possible in a browser environment without installing a separate program. So, Over 200 million people use this solution in march 2020. However, during a video conference using Zoom, a third party attends the conference room, resulting in a video conference solution due to a 'Zoombombing' attack that interferes with the normal conference due to racial discrimination, religious remarks, or sharing pornographic videos. Controversy over the safety of the people is constantly on.

The zoomboming attack is possible by generating IDs randomly through a brute-force attack using a structure in which conference rooms are created using IDs consisting of 9 to 10 digits given when joining Zoom. When the conference room is found, any user can participate in the active conference room.



[Figure 4-1] ID provided from Zoom

Attack code for brute-force attack can be easily implemented. Enter a random number in the User ID field at the URL address for attending the meeting ('https://zoom/us/wc/join/[user ID]), and if the meeting exists, you can attend.

```
while istrue == 'true':
    rand=random.uniform(0, 1)
    if rand > 0.5:                                          ⓐ
        id=random.randrange(100000000, 999999999, 6)
    else:
        id=random.randrange(1000000000, 9999999999, 6)
    joinid='https://zoom.us/wc/join/' + str(id)             ⓑ
    print("trying code " + str(id))
    browser.get((joinid))                                   ⓒ
    if len(browser.find_elements_by_id('inputname')) > 0:   ⓓ
        print('Code ' + str(id) + ' works!')
```

[Figure 4-2] Zoomboming attack code

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

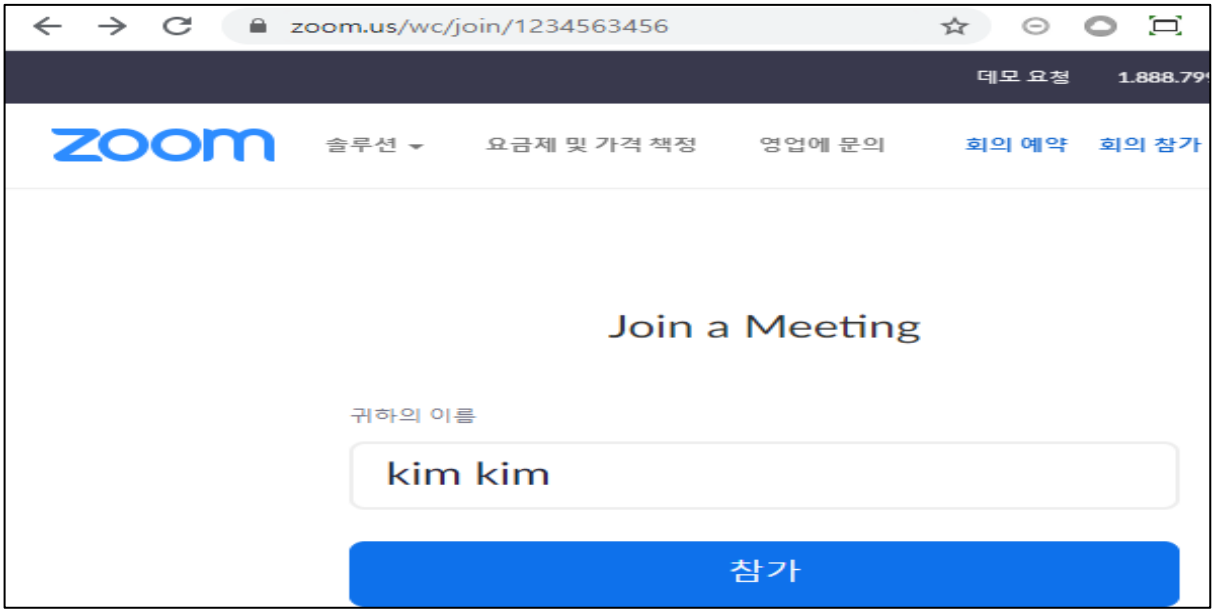
Security issues and countermeasures due to untact work system

ⓐ IDs consisting of 9 to 10 digits are randomly generated.
ⓑ A randomly generated ID is added to the URL for joining the conference room.
ⓒ Try to access the meeting room with the URL you combined in ⓑ.
ⓓ Check whether or not the combined URL access in ⓑ

[Figure 4-3] Zoomboming attack process

[Figure 4-4] shows the result of finding an active meeting room after attempting to access the meeting room with a randomly generated ID.

[Figure 4-4] Successful search of conference rooms activated through randomly generated ID



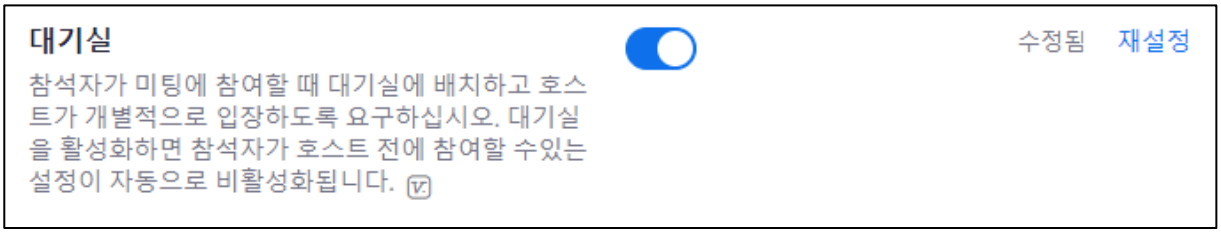
[Figure 4-5] URL to enter the active conference room after entering the ID

Division	Conference room URL
Meeting room URL with no password	https:/ zoom.us/j/12 327
Meeting room URL with password	https://us04web.zoom.us/j/4167756855? pwd=R2NvTnVEelZHK2NwQXUvWTlLcFlTdz09

[Figure 4-6] Meeting room URL with password

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

Security issues and countermeasures due to untact work system



[Figure 4-7] Waiting activation in the setting page

Besides the zooming attack, Zoom had vulnerabilities such as executing arbitrary commands with the Universal Naming Convention (UNC) UNC Path Injection in the zoom client. A patched version of the vulnerability (4.6.19253.0401) has been released, and in the case of a zooming attack, a password has been added to the meeting room access URL. In addition, by using the waiting room function, the number of people entering the room before the video conference starts is gathered in the waiting room and then the presence of a third party can be confirmed.

2) Messenger

Slack, a messenger tool, exists for each channel and can post messages for each channel. The vulnerability creates a link that can be posted to the channel in Slack, which can manipulate the default Download Location within the user's settings into the attacker's SMB shared folder.

[Figure 4-8] Slack structure : ⓐ channel ⓑ message ⓒ feed (resource : Slack official web page)

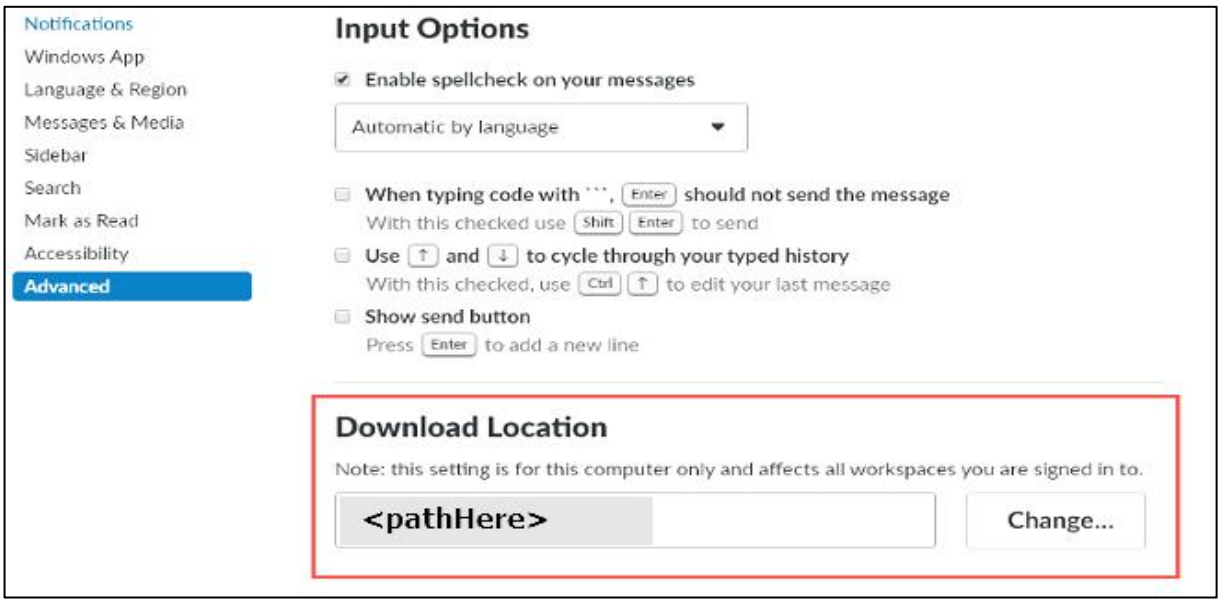
All settings of Slack can be checked in the Settings-Resucer.ts module, and the download path can be changed using the “PrefSSBFileDownloadPath” setting. All settings can be configured via the slack:// settings link. Since ":" (colon) cannot be included in the Slack://link, it can be bypassed through SMB sharing.

```
slack://setting/?update={'PrefSSBFileDownloadPath':{'<pathHere>'}
```

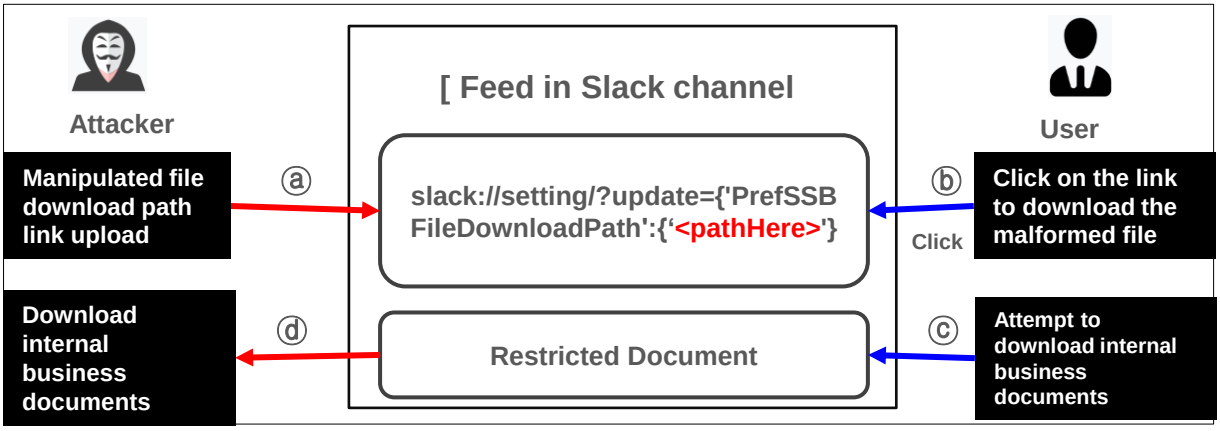
[Figure 4-9] Basic download path manipulation syntax

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

Security issues and countermeasures due to untact work system



[Figure 4-10] Setting value changed by the path operation syntax (Resource : https://medium.com/)



[Figure 4-11] Slack Messenger's default download path manipulation attack process

ⓐ The attacker posts a message to the slack channel containing a link to the user's default download path manipulation.
ⓑ Default download path changes when user clicks a link in a message.
ⓒ After that, the user tries to download the “Restricted document” for the job.
ⓓ ‘Restricted document’ is downloaded to the attacker according to the changed user's default download path.

[Figure 4-12] Slack Messenger's basic download path manipulation attack description

In addition to this method, hyperlinks can be created using the attachment function when posting to a channel. After adding the attachment parameter to the message post request packet on the channel and adding the link in [Figure 4-13], the disguised hyperlink is posted as shown in [Figure 4-14]. When the user clicks the link, the default download path is manipulated.

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

Security issues and countermeasures due to untact work system


```
[{"title":"http://google.com", "title_link":
"slack:\/\/settings/?update={'PrefSSBFileDownloadPath':'<pathHere>'}"}]
```

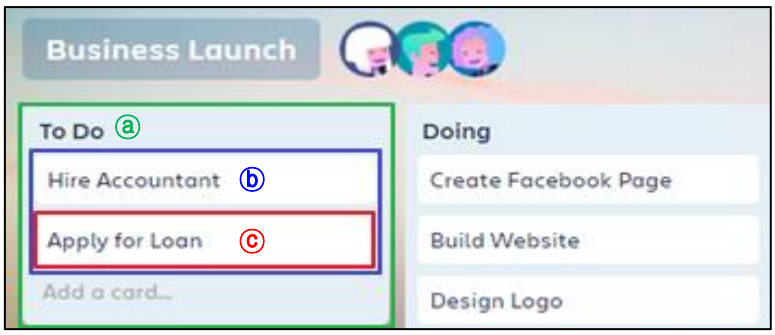
[Figure 4-13] Attack syntax disguised as http://google.com link

[Figure 4-14] Slack feed with attack phrase disguised as a link to http://google.com (Resource : https://medium.com/)

The vulnerability has been patched in Slack version 3.4.0. The user should be careful not to open an unknown link as shown in [Figure 4-14] when using a remote collaboration tool such as a messenger.

3) Work-sharing

Trello, a collaboration tool, is a method of creating a board based on a project, creating a list for each stage and part, and registering progress details as a card. The user can set the board to two types: Private (only open to members) and Public (open to all). Users exposed sensitive information on the board in a public setting, causing information disclosure.



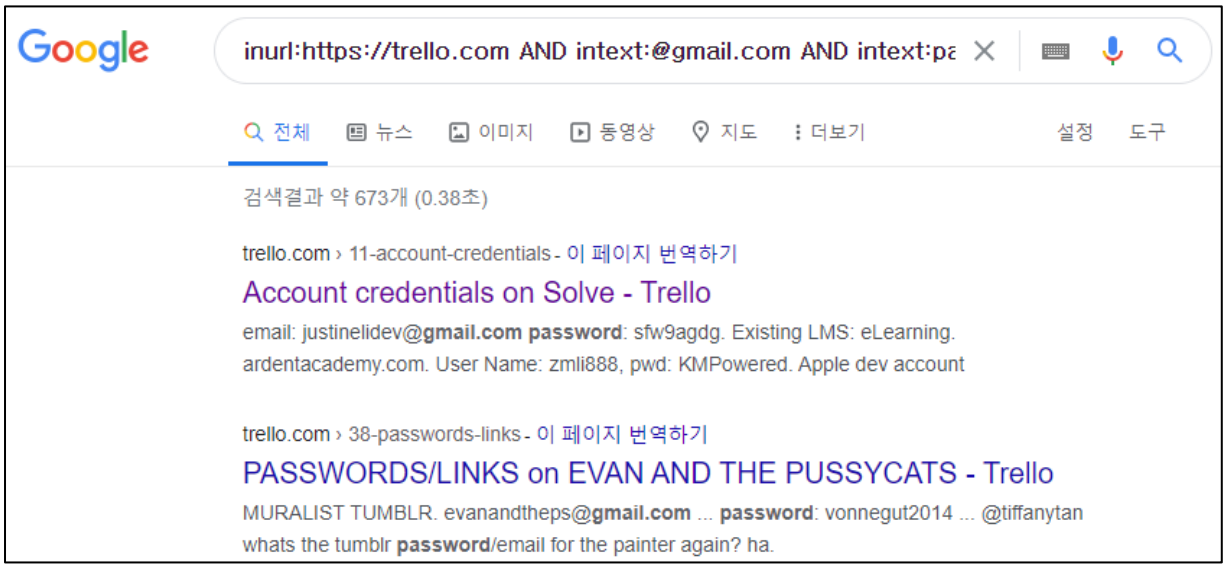
[Figure 4-15] Trello structure : ⓐ board ⓑ list ⓒ card (resource : Trello official web page)

```
inurl:https://trello.com AND intext:@gmail.com AND intext:password
```

[Figure 4-16] Search for information published on the board using Google Dork (google hacking)

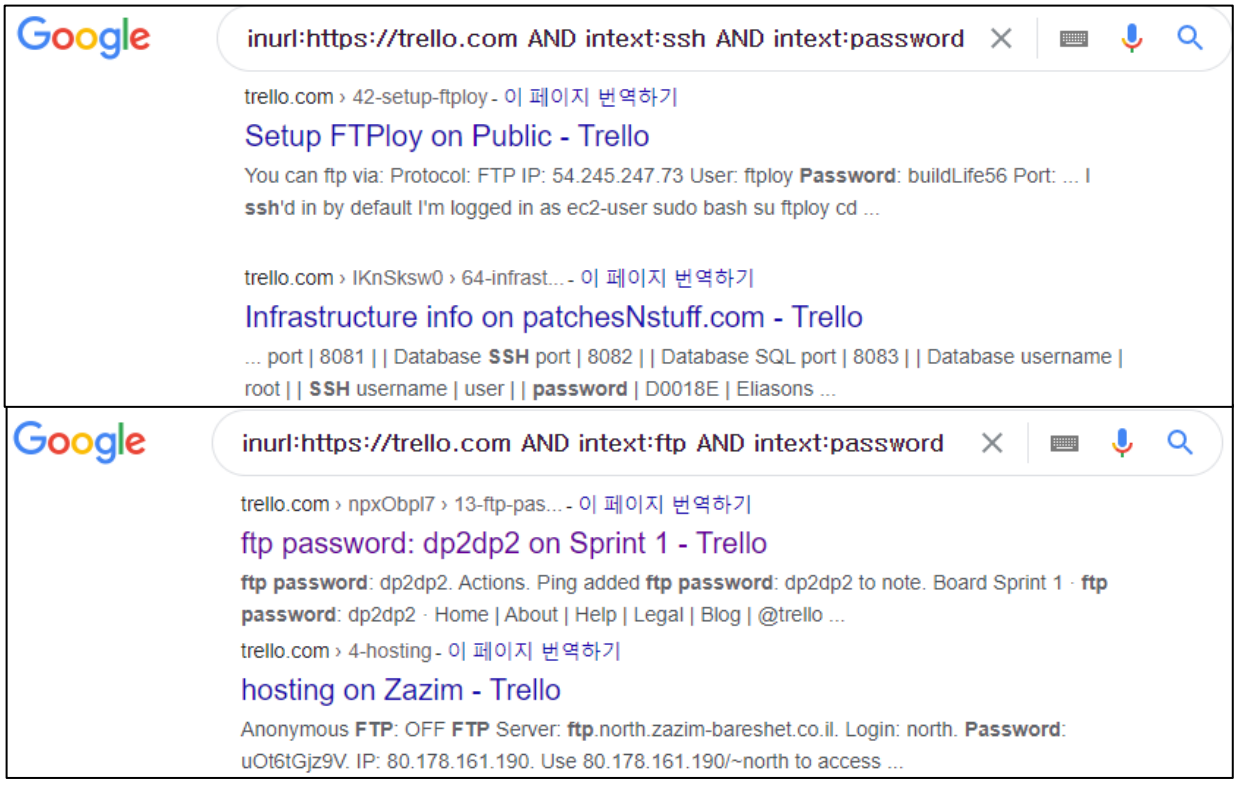
Copyright © IGLOO Security, Inc. 2020. All rights reserved.

Security issues and countermeasures due to untact work system



[Figure 4-17] Trello board sensitive information exposed to search engines

As a result of searching on Google using Google Dork (Google Hack) in [Figure 4-16], when Board is set as Public, sensitive information posted on Board is exposed as shown in [Figure 4-17].
Even when searching using other search terms, sensitive information posted on the board was exposed when Board was set to public.

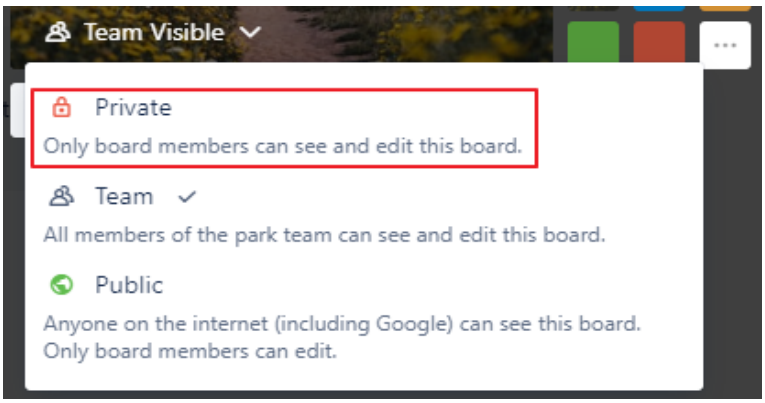


[Figure 4-18] Trello board sensitive information exposed to search engines

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

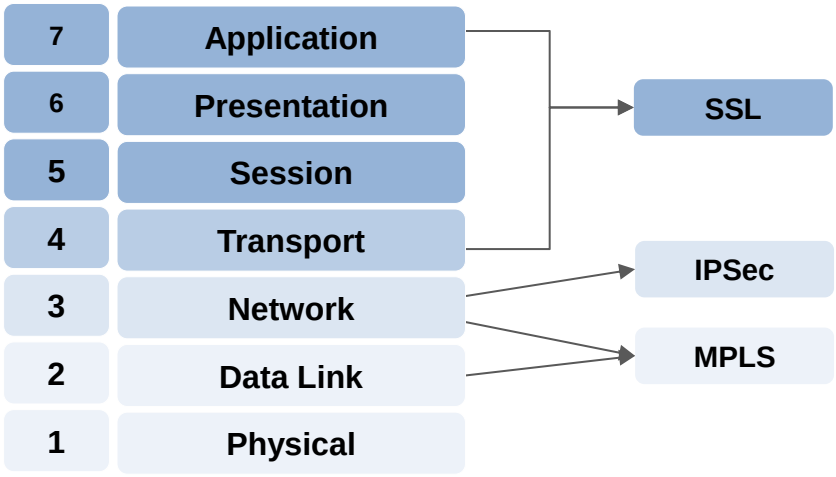
Security issues and countermeasures due to untact work system

When using Trello for work, the user should be careful about exposing sensitive information by setting the public setting of the board to Private.



[Figure 4-19] Trello board visibility setting

03. Security issue of VPN



[Figure 4-20] Each VPN operation layer in OSI layer 7

VPNs include IPSec VPNs that use connection-only clients and SSL VPNs that can access internal networks regardless of the location and type of terminal.There are also MPLS VPNs that provide logically separated VPN networks with little overload.Each company implements telecommuting by building a VPN according to the environment. Among them, we would like to find out the technical and administrative measures required to conduct non-face-to-face work using SSL VPN.

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

Security issues and countermeasures due to untact work system

The following [Table 4-2] shows the known and vulnerable versions of devices that support SSL VPN. The administrator should establish a patch policy through version management of the VPN device currently in use.

Product	CVE vulnerability	Vulnerable version
Pulse Connect Secure	CVE-2019-11510 : Unauthorized attacker can read arbitrary files CVE-2019-11539 : Insert and execute authenticated attacker commands	Pulse Secure Pulse Policy Secure 9.0 Rx Pulse Secure Pulse Policy Secure 5.x Rx Pulse Secure Pulse Connect Secure 8.x Rx Pulse Secure Pulse Connect Secure 9.0 Rx
Fortinet	CVE-2018-13379 : Unauthorized attackers can download system files	Fortinet Fortios 6.0.x, 5.6.x
	CVE-2018-13382 : Unauthorized attackers can modify the user's password	Fortinet Fortios 6.0.x, 5.4.x, 5.6.x
Palo Alto Networks	CVE-2019-1579 : Execute remote code	Paloaltonetworks PAN-OS 8.0.x, 7.1.x, 8.1.x

[Table 4-2] CVE description, vulnerable version

User account management through multi-factor authentication (MFA), which identifies users by verifying two or more things in different authentication bases based on knowledge, possession, and inheritance when connecting to a VPN Is needed. The two-factor authentication (2FA) authentication method, which performs OTP authentication after logging in with ID and PW, can be considered as an example of application of a typical MFA method.

According to the 'Five things you can do right now to stay safer online' announced by Google in February 2019, when setting up 2FA (Two-Factor Authentication), the possibility of someone stealing your account is greatly reduced. In this way, the administrator must perform access control through user authentication. In addition, it is necessary to prevent unnecessary internal system access by allowing an authenticated user to access only the required system, and be careful about information disclosure.

Division	Factor
Knowledge	ID, password, i-pin, password question/answer, etc.
Possession	Token, smart card, OTP, SMS, etc.
Inherence	Fingerprint, face, retina, iris, voice, signature, etc.

[Table 4-3] 3 ways to MFA

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

Security issues and countermeasures due to untact work system

In some enterprises, work was paralyzed because the VPN overload caused by telecommuting was not considered. To avoid this problem

△ VPN access account management, △ Maximum number of concurrent VPN users, △ Capacity and license, △ It is necessary to set policies considering monitoring and log audit methods. In particular, in order to prevent system load due to indiscriminate access, system availability through load management can be secured by terminating the session when communication is not performed for a certain period of time.

Companies should establish and distribute work system response plans for safe work when working from home. Also, you need to distribute the VPN user manual for the OS you are using. The user should grasp whether there are no issues after driving according to the manual in advance. The document says △ Supported OS information, △ Installation environment required in advance, △ Type of application to be installed, △ Contents about VPN execution status, etc. are required.

04. Remote co-work Tools and VPN Checklist

Division	Check list	result
Remote co-work tool	1. Prepare a video conferencing security policy	
	2. When using video conference, use the waiting room function	
	3. Only the people required for the meeting share the access code of the meeting room	
	4. Participate in a video conference using an authenticated terminal	
	5. Prohibit recording of meeting content unless necessary	
	6. Be careful not to expose sensitive information to the screen during a meeting	
	7. Disable when features such as chat, file sharing, and URL sharing are unnecessary	
	8. Do not share files and click URLs of unknown users when using messenger	
	9. When using the work sharing solution, it is necessary to set the scope of project disclosure	
	10. Do not post sensitive information when using a work sharing solution	

[Table 4-4] Remote co-work tool check list

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

Security issues and countermeasures due to untact work system

Division	Target	Check list	Result
VPN	Manager	1.User establishes patch policy through VPN device version management	
		2. Capacity and license need to be expanded considering the maximum number of users	
		3. When connecting to a VPN, apply secondary authentication means other than password	
		4. Requires session expiration settings for VPN users	
		5. Establish and distribute untact work plans within the company	
		6. Distribution of VPN user manual for various OS environments	
	User	1. PC update and antivirus program update	
		2. Do not work through private Wi-Fi or public PC	
		3. Refrain from accessing unnecessary websites when performing business	
		4. Be careful when downloading unnecessary files	

[Table 4-5] VPN Check list

05. Conclusion

Due to the sudden change of the IT environment, it is busy due to the introduction of various solutions and business processes, but most importantly, the IT environment that does not consider security will lose the user's trust. In order to provide users with a reliable remote work environment with security applied, it is necessary to establish a checklist for each security officer and user based on the above-mentioned rules and considerations, and to create a safe environment through distribution.

Due to the remote working environment, virtualization technology is also emerging to manage threats caused by information leakage and shadow IT in addition to the remote collaboration tools or VPNs described above. Desktop virtualization (VDI), a technology that centrally manages each user's PC by utilizing a server in the cloud or a corporate data center as a desktop, not only lowers the risk of data leakage, but is also gaining attention in management. In addition, consideration should be given to post-validation measures through monitoring and evidence log management measures for infringement incidents and audits.

Before applying any security solution or policy, the most important thing is to implement IT governance that fits the current status of the company or institution's assets and business characteristics. If you analyze the pros and cons of remote co-work tools and VPN introduction and establish an implementation plan suitable for the current situation, you will be able to establish a more secure untact working environment.

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

Security issues and countermeasures due to untact work system

06. Reference

[1] Zoom
-https://github.com/DDDASHXD/ZoomBrute.py/blob/master/README.md
-https://thenextweb.com/security/2020/04/06/nyc-classrooms-cancel-zoom-after-trolls-make-zoombombing-a-thing/
-https://devforum.zoom.us/t/force-username-when-entering-meeting-using-browser-zoom-app/1102/4
[2] Slack
-https://medium.com/tenable-techblog/stealing-downloads-from-slack-users-be6829a55f63
-https://slack.com/intl/en-kr/solutions/remote-work
[3] Trello
-https://www.freecodecamp.org/news/discovering-the-hidden-mine-of-credentials-and- sensitive-information-8e5ccfef2724/
-https://trello.com/home
[4] VPN CVE
-https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities
[5] MFA
https://ko.wikipedia.org/wiki/%EB%8B%A4%EC%9A%94%EC%86%8C_%EC%9D%B8%EC%A6%9D
[6] MFA
-https://docs.broadcom.com/doc/passwordless-vip-ig
-https://techcommunity.microsoft.com/t5/azure-active-directory-identity/all-your-creds-are-belong-to-us/ba-p/855124#
-https://www.blog.google/technology/safety-security/five-things-you-can-do-right-now-to-stay- safer-online/
[7] Conclusion
-https://www.krcert.or.kr/data/guideView.do?bulletin_writing_sequence=35319
-https://www.dailysecu.com/news/articleView.html?idxno=107699
-https://blog.lgcns.com/1952

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

CHAPTER 5

Special Column

Ransomware of industrial control system as an example

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

Ransomware of industrial control system as an example

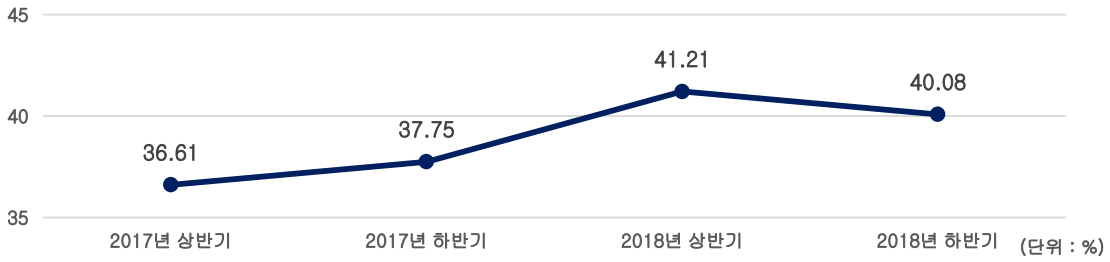
Security Monitoring Center
Security Analysis Team

1. Overview

In 2010, there was a hacking incident that targeted a nuclear facility in Iran, using the worm vulnerability of the network sharing and printer spooler with Stuxnet, a worm virus. Therefore, some functions of the centrifuge were paralyzed. This incident triggered awareness of the impact of the security of the ICS (Industrial Control System) on safety.

Ten years later, as the technological development of the 4th Industrial Revolution, a new security threat is faced due to the combination of existing OT (Operation Technology) and IT (Information Technology). Looking at the recent cyber attacks, the Saudi Aramco hacking incident in 2012, the paralysis of the Ukrainian power grid in 2015, and the attack on energy industries such as nuclear power plants, nuclear facilities, nuclear power, water resources, etc.

Of the cyber attack detection rate of ICS among the cyber attack detection rates surveyed by Kaspersky in 2018 in [Figure 5-1], the average attack rate was 3.5% in one year from 37.18% in 2017 to 40.65% in 2018. Considering that the figure was calculated based on the ICS standard installed with Kaspersky's solution, it can be seen that the number of attack detections increased significantly in one year.

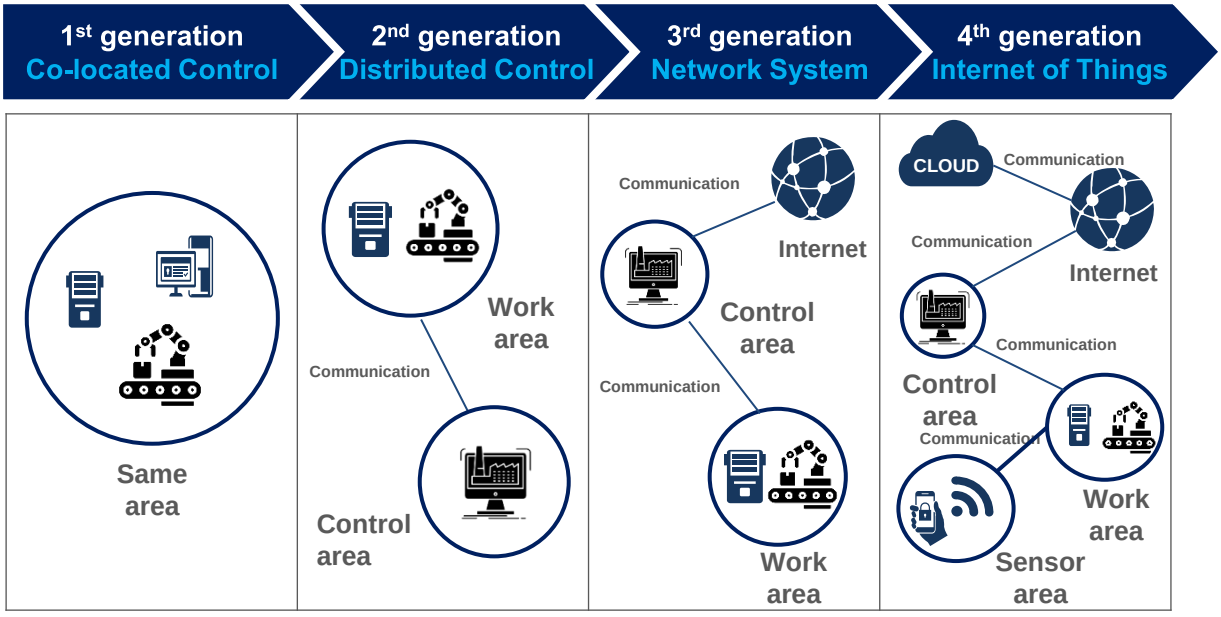


[Figure 5-1] Trend of cyber attacks in ICS (Source: Kaspersky)

In the past, a large number of ICSs operated in the form of closed networks with clear boundaries from external networks. Recently, the efficiency of work is increased as data-based operation is possible by combining IoT with sensors, actuators, etc. However, this resulted in an increase in security threats due to IT linkage. Eventually, the combined IT environment for the purpose of operational convenience and efficiency was combined with the work environment of ERP, SCM, CRM, etc., causing problems that were exploited as external intrusion paths due to USB, email, misconfiguration, etc.

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

Ransomware of industrial control system as an example



[Figure 5-2] Industrial Control System Change Process (Source: SME Technology Roadmap, 2017)

According to the “Small and Medium Business Technology Roadmap Strategy Report” announced by the 2017 Small and Medium Business Technology Roadmap Site, the development trend of industrial control systems has evolved from the 1st generation without network support to the 4th generation with Internet and cloud support. In the OT environment where the embedded base was predominant, as the standard technology environment such as Windows or Unix / Linux spread, the security threat that occurred in the IT environment will be expressed in the ICS environment.

This change in environment has also had a significant impact on the form of the attack. The damages caused by ransomware found in the ICS environment can be seen to show the change of these attacks. Malwares for APT attacks, which were used for information leakage or system paralysis, were transformed into a form in which ransomware and kill disks were combined as seen in the Ukrainian blackout in 2015. Until recently, ICS cyber attacks using ransomware have steadily increased.

In the case of multiple indiscriminate targets, attempts were made to steal money through ransomware. Ransomware attack cases have increased for targeted attacks such as ICS.
In addition, even if money deodorization does not occur due to the ransomware infection, the system has a high impact and it can be considered as a frequent use case because it only causes infection. Therefore, in this issue, we will analyze the damages caused by ransomware in the industrial control system environment and look at countermeasures.

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

Ransomware of industrial control system as an example

2. Attack process aimed at industrial control systems : MITM ATT&CK for ICS Matrix

Looking at the main case, even if the pattern of the attack changed, there were certain rules for the flow of the process and it could be formalized. Based on this, the process for cyber attack and penetration is MITM ATT & CK for ICS. ATT & CK has regularized the attack process for a specific malware or attack group, and if different malicious codes have similar processes, it is considered to be the action of the same attack group or the derivation of a specific malware.

The top 11 categories are Tactics, and each has its own Technology. In order to see a larger picture, 11 tactics are divided into three main categories in the matrix of [Table 5-1]. In the case of ransomware, initial attack, initial access, and lateral movement after infection, and the resulting impact tactics showed a similar attack process. In the middle of the attack process, there may be slight differences due to the inherent characteristics, but the main known ransomware showed similar attack techniques in the following three tactics. Let's analyze the form of ransomware attacking ICS for each tactic

Category	Tactics	Technique
Initial penetration	Initial Access	Drive-by Compromise, External Remote Services, Replication Through Removable Media, Spear-phishing Attachment
Attack	Execution	Change Program State, Command Line Interface, Execution through API, Scripting, User Execution
	Persistence	Hooking, Module Firmware, Program Download, Project File Infection
	Evasion	Rootkit, Masquerading, Exploitation for Evasion
	Discovery	Control Device Identification, I/O Module Discovery
	Lateral Movement	External Remote Services, Exploitation of Remote Services, Remote File Copy, Default Credentials
	Collection	Automated Collection, I/O image, Collection
	Command and Control	Commonly Used Port, Connection Proxy, Standard Application Layer Protocol
	Inhibit Response Function	Denial of Service, Data destruction, Block Serial COM, Manipulate I/O Image
Result	Impair	Brute Force I/O, Change Program State, Masquerading, Program Download
	Impact	Loss of Availability, Loss of View, Loss of Productivity and Revenue

[Table 5-1] Tactics and Techniques Available for Ransomware in ICS (Source: ATT & K)

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

Ransomware of industrial control system as an example

1) Penetration process: initial penetration

There are a total of 10 detailed techniques of initial penetration classified by ATT & CK, and among them, there are four methods that are commonly used when ransomware is distributed. The first method used to access the inside of the system mainly penetrates the inside through the "Replication Through Removable Media" method and the "Spear-phishing Attachment" method. In the case of the drive negotiation method, it is combined with other methods to penetrate inside.

- Drive-by Compromise
- External Remote Services
- Replication Through Removable Media
- Spear-phishing Attachment

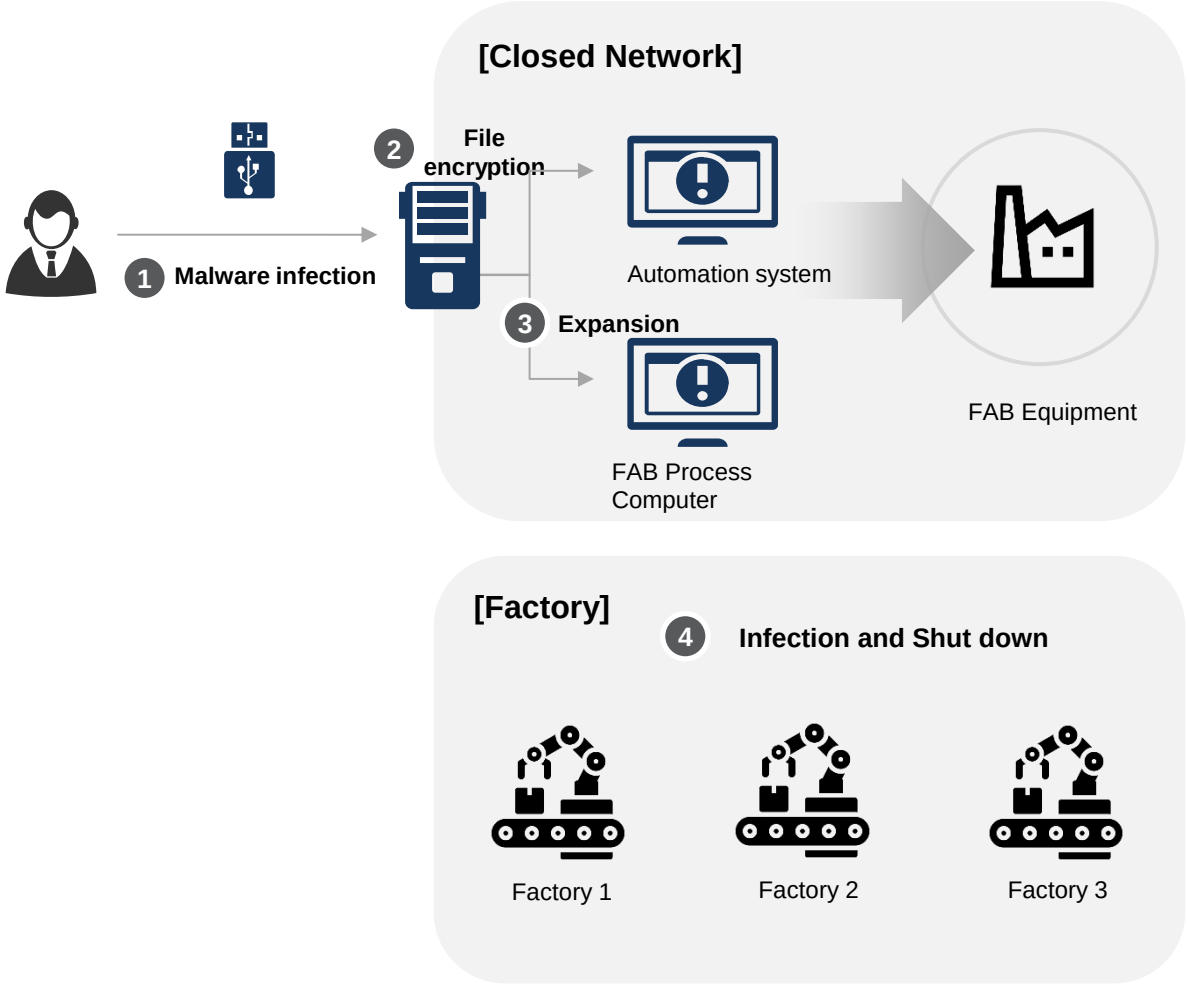
Replication Through Removable Media	Spear-phishing Attachment	External Remote Services	Drive-by Compromise

[Table 5-2] Initial penetration methods

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

Ransomware of industrial control system as an example

In the case of Replication Through Removable Media, the existing ICS is a steady infiltration method, and it is one of the first infiltration methods found in the majority of issues. One recent occurrence is TSMC's ransomware incident in Taiwan in 2018. Through a USB, access to a closed network system that cannot be accessed through the network has affected the production plant.



[Figure 5-3] TSMC Wannacry Ransomware infection process in Taiwan

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

Ransomware of industrial control system as an example

Spear-phishing attachment is one of the most used methods in today's systems. It is one of the most widely used methods of distributing ransomware and uses social engineering techniques. It distributes the attachment file containing the malicious code along with the mail, and follows the user's authority to execute it. An example of an internal system infection through spear phishing was the ransomware infection of the Michigan Water Resources Power Plant in 2016. When an internal employee accidentally read an attachment containing ransomware, file encryption proceeded, and the infection spread to the internal network, eventually suspending the system.

Division	Replication Through Removable Media	Spear-phishing Attachment
How to Distribute	Distributed by specific media	
	Removable disk containing malicious code	Mail with social engineering techniques
Used media	physical media	Attached files in the mail
Major cause	Mistakes made by careless users and managers	
	Use of removable storage device without security check	View attachments in unconfirmed emails
Features	Easy to penetrate inside because it depends on the person who runs it	

[Table 5-3] Attack comparison using replication and spear phishing through removable media

As shown in [Table 5-3], both methods have to be executed by a third party and other media must be used together. However, ICS 'blind spot that cannot penetrate the system even if it detects infection is much easier. It is one of the ways to attack.

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

Ransomware of industrial control system as an example

The External Remote Services method is also one of the methods that have recently occurred as IT and OT are combined and the system can be accessed from outside. It also penetrates internally through vulnerability of the program used and takes system authority and infects ransomware with process-related systems.

Among them, a case of ransomware infection using RAT (Remote Administration Tool), which is one of the tools for facilitating external access, has occurred. According to the Kaspersky Lab 2018 Security Threat Report, about one-third of ICSs using the security product use RAT, and 20% of them contain the function in ICS itself, but the administrator does not know about it. It was also investigated that cases were occurring.

Drive-by Compromise is one of the methods of attacking a watering hole, and it is a method of invading with a specific target and purpose, such as identifying a major website visited by a company to attack a specific industry or company. Drive-by Compromise is also used interchangeably with other infiltration methods. This is done in advance based on research on specific companies.

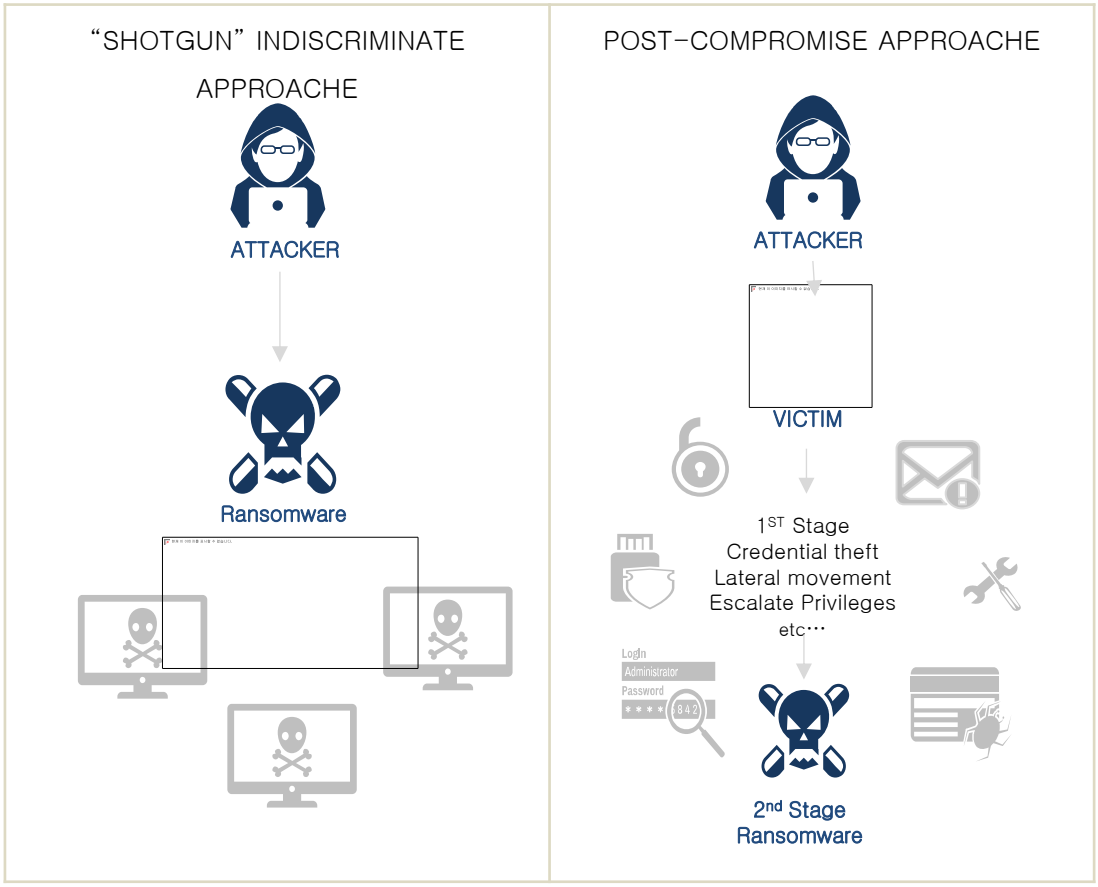
In October 2017, cases of ICS infections in Ukraine, Europe, and Russia infected and spread through the Drive-by Compromise method. When the first infected PC visited a trusted website, it was infected through a dropper disguised as an Adobe flash update. Since then, it has spread to the internal network using unpatched services.

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

Ransomware of industrial control system as an example

2) Penetration process: the process of attack

The biggest way to spread when ransomware is infected in the internal system was to spread through SMB vulnerability and affect the OT system. This was aimed at promiscuous proliferation and was able to penetrate SMB or remote service activation and unpatched systems. However, in the case of the ransomware used in recent cases, ransomware targeting only the ICS system has been distributed.



[Figure 5-4] Ransomware's indiscriminate distribution method and post-infiltration distribution method process (source: KISA)

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

Ransomware of industrial control system as an example

3) Penetration process: the result of the attack

As the attack form of ransomware evolved to target ICS, the result of the attack also changed. In the case of the recently discovered LokerGoga and SnakeHouse, the same OT Process kill list was confirmed.

```
taskkill /im proficy administrator.exe /f   0x600dec: proficy administrator.exe
taskkill /im ntevl.exe /f                   0x5f224e: ntevl.exe
taskkill /im prproficymgr.exe /f            0x5fa55a: prproficymgr.exe
taskkill /im prrds.exe /f                   0x5f200e: prrds.exe
taskkill /im prrouter.exe /f                0x5f6642: prrouter.exe
taskkill /im prconfigmgr.exe /f             0x5f9ec6: prconfigmgr.exe
taskkill /im prgateway.exe /f               0x5f8552: prgateway.exe
taskkill /im premailengine.exe /f           0x5fb5b1: premailengine.exe
taskkill /im pralarmmgr.exe /f              0x5f905c: pralarmmgr.exe
taskkill /im prftpengine.exe /f             0x5f9dc7: prftpengine.exe
taskkill /im prcalculationmgr.exe /f        0x5fd66e: prcalculationmgr.exe
taskkill /im prprintserver.exe /f           0x5fb617: prprintserver.exe
taskkill /im prdatabasemgr.exe /f           0x5fb4b2: prdatabasemgr.exe
taskkill /im preventmgr.exe /f              0x5f91ac: preventmgr.exe
taskkill /im prreader.exe /f                0x5f7356: prreader.exe
taskkill /im prwriter.exe /f                0x5f6756: prwriter.exe
taskkill /im prsummarymgr.exe /f            0x5faf2a: prsummarymgr.exe
taskkill /im prstubber.exe /f               0x5f7d25: prstubber.exe
taskkill /im prschedulemgr.exe /f           0x5fb7c0: prschedulemgr.exe
taskkill /im cdm.exe /f                     0x5f119e: cdm.exe
taskkill /im musnotificationux.exe /f       0x5fe4d4: musnotificationux.exe
taskkill /im npmdagent.exe /f               0x5f8287: npmdagent.exe
taskkill /im client64.exe /f                0x5f76da: client64.exe
taskkill /im keysvc.exe /f                  0x5f310e: keysvc.exe
taskkill /im server_eventlog.exe /f         0x5fca0b: server_eventlog.exe
taskkill /im proficyserver.exe /f           0x5fb5c2: proficyserver.exe
taskkill /im server_runtime.exe /f          0x5fbfbf: server_runtime.exe
taskkill /im config_api_service.exe /f      0x5feaaa: config_api_service.exe
taskkill /im fnplicensingservice.exe /f     0x5fff0e: fnplicensingservice.exe
taskkill /im workflowresttest.exe /f        0x5fd592: workflowresttest.exe
taskkill /im proficyclient.exe4 /f          0x5fb0fa: proficyclient.exe
```

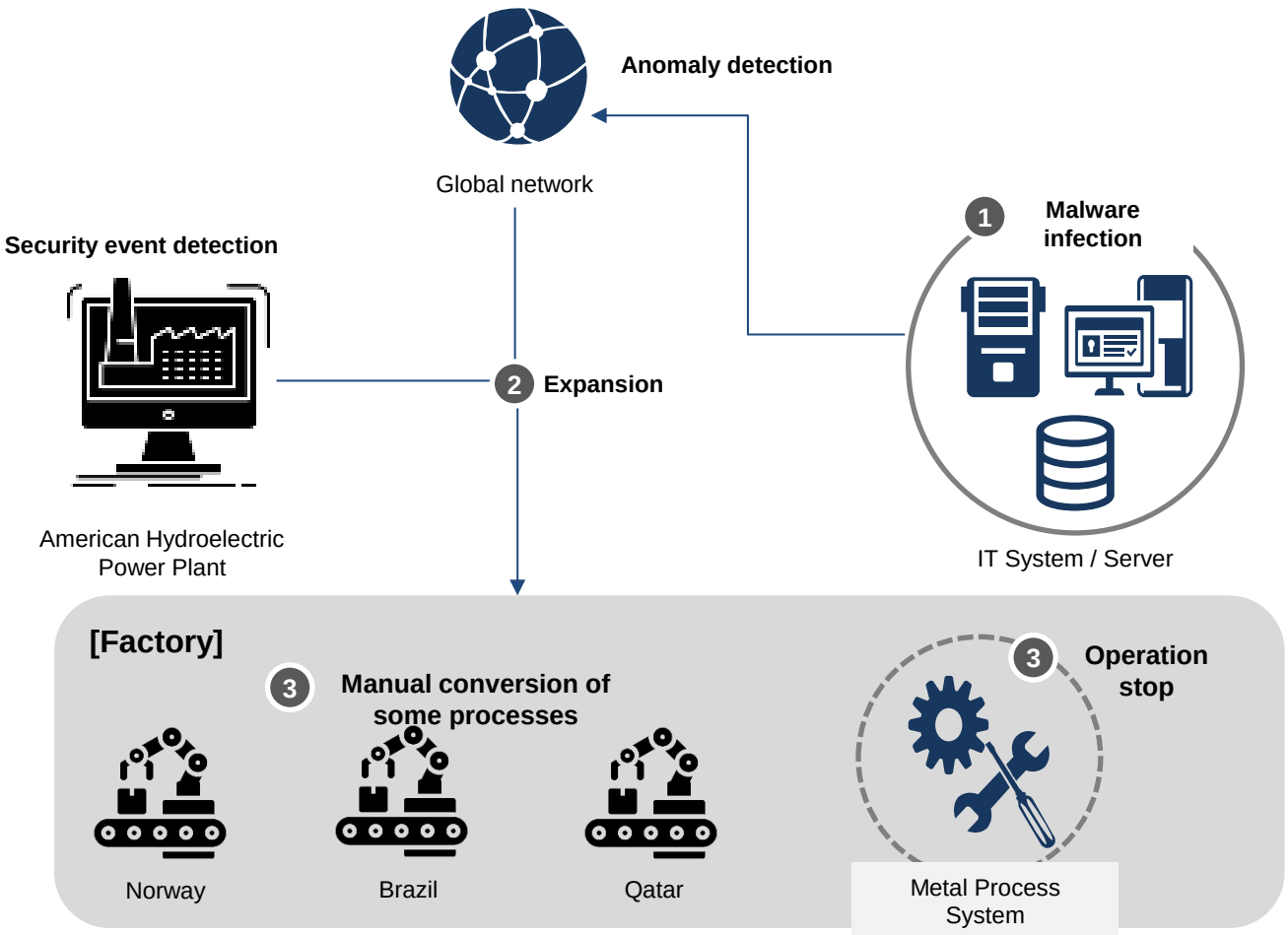
[Figure 5-5] LokerGoga (left) and SnakeHouse (right) process kill list (Source: FireEye)

According to an example of ransomware infection of the OT system of the natural gas compression facility of the Cybersecurity Infrastructure and Security Agency (CISA) in February 2020, the impact was announced to lead to loss of availability due to process-related system shutdown. In addition, the data is encrypted, resulting in loss of view and finally loss of productivity and revenue.

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

Ransomware of industrial control system as an example

In fact, in January 2019, Norker Hydro, a Norwegian aluminum giant, was infected with LokerGoga ransomware and production was suspended. The ransomware issue resulted in about $ 40 million in damage and had a profound impact on productivity and profits.



[Figure 5-6] Norsk Hydro Production Plant Ransomware in Norway

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

Ransomware of industrial control system as an example

3. Conclusion

Through the above examples, it can be seen that ICS ransomware is gradually evolving, and attacks targeting the system itself are increasing. Also, as it evolves into a target type rather than a brute force attack, it aims at companies, institutions, and public institutions that can pay high prices, and the attackers seem to be devoted to attack for a long time.

On the other hand, the overall security technology and awareness of OT systems and ICS seems to be still insufficient. In recent years, many systems or technologies that incorporate security technologies have been revealed, but in the case of equipment that is still in use in the industry, it has been found that old and fixed systems are all. In the case of the system in use, there are many places that use the old OS where the service is terminated, and it is not easy to apply because it can affect the process of the facility when integrating security technology due to industrial characteristics.

However, prevention and countermeasures should be prepared for known security threats. The way to learn from the example above is △ Disable unnecessary services and recognize existing threats, △ IT system security enhancement, △ It can be cited as enhancing security awareness of managers.

Even though there were unnecessary remote connections from the main equipment, the proportion of actual personnel was unaware of this. Disable remote services when not in use, be aware of key services and protocols, and personnel should audit them regularly. The personnel should be interested in what is happening at your facility, and the personnel should be equipped with a process to identify and analyze specific phenomena. Through this, it is important to be aware of the threat of the system in use..

In addition, in the case of major ransomware, there was a case where an infection occurred in a system connected to the outside. When integrated with an OT system, there is a risk of indiscriminate infection such as Wannacry and NotPetya, so IT system security is also important. Since there have been cases of infection through the IT system, the security of the IT system must be strengthened.

In addition, cases due to deliberate acts or mistakes have been found constantly. Threats through removable media or infection through spear phishing were caused by people's inadvertent behavior. To prevent this, it is necessary to improve security awareness of facility managers.

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

4. Resource

[1] ICS targets cyber attacks based on country
http://www.datanet.co.kr/news/articleView.html?idxno=133592
[2] 2017 SME Technology Roadmap_Information Protection
http://smroadmap.smtech.go.kr/02/view/year/2017/m_code/A100/id/1893/idx/1898
[3] Factory security in question, what should I do?
https://blog.lgcns.com/2021?category=604440
[4] Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT
https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html
[5] ATT&CK for Industrial Control Systems
https://collaborate.mitre.org/attackics/index.php/Main_Page

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

CHAPTER 6

Focus On IGLOO Security

1. Igloo Security Co., Ltd. takes AI security monitoring efficiency to the next level by obtaining two patents related to security monitoring

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

Focus on IGLOO Security

Igloo Security Co., Ltd. takes AI security monitoring efficiency to the next level by obtaining two patents related to security monitoring

- It is planned to be applied to SPiDER TM AI Edition, the first AI security monitoring solution in Korea

[April 28, 2020] Igloo Security Co., Ltd. (CEO Lee Deuk-Choon, www.igloosec.co.kr/en) has completed patent registration to increase the accuracy and reliability of security monitoring policies.
1. 'Automatic application system and method of security device control policy based on an infringement incident response instruction (Registration No. 10-2090757)'.
2. 'Security monitoring system and method using block chain technology (registration number 10-2098803)' that guarantees the integrity of log data collected, stored, and processed by security device using blockchain technology.

Various control policies are applied to security device used for security monitoring to effectively detect and block security threats targeting IT assets. In order to quickly respond to serious infringement, it is necessary to add and update various control policies such as signature patterns and Snort Rules from time to time based on accurate analysis to keep it up to date. However, it is true that there are difficulties in effective control policy management because the number of security devices to be managed is increasing and the personnel who perform policy analysis and setting tasks are separated.

Also, in the process of storing and processing logs collected from various security devices, a powerful management function that ensures that these logs have not been tampered with was also required. In general, a method of collecting a log through encrypted communication such as TLS (transport layer security) and generating and managing a hash value for the collected log is applied. However, since encryption and hash generation are performed through an encryption key arbitrarily injected by a security monitoring service provider, it is difficult for the security monitoring service user to trust 100% of the integrity of the log.

The patent for 'Automatic application system and method of security device control policy based on an infringement incident response instruction' is a technology that creates a reliable control policy based on an infringement incident response instruction created during the infringement response process, and automatically applies this policy to security device. Unlike the existing technology, which was applied after validating only the security policy entered based on discretionary judgment, this patent is designed to automatically apply the control policy reflecting the infringement incident response instruction.

The patent for 'Security monitoring system and method using block chain technology' creates the block data using log files collected by the log collection unit and distributes it in the blockchain network to store the integrity of the log data collected by the security monitoring server. By accurately verifying the integrity violation by the security monitoring service provider or the cyber attacker, the reliability of the log, which is the basic data for analyzing the signs of cyber attack and the incident, has been increased.

Igloo Security plans to apply two patented technologies to the SPiDER TM AI Edition, an AI security monitoring solution. By automatically reflecting the control policy based on the infringement incident response instruction, it is expected to shorten the response time for infringement incidents that can have a significant impact on the IT system in the organization and increase security control efficiency. In addition, through the verification of log data integrity using blockchain technology, it is expected that it will be possible to eliminate the possibility of erroneous analysis results based on forged and forged logs.

“Igloo Security is a leading AI security monitoring company, leading the research and development of technologies that can improve the effectiveness of security monitoring. It is expected that the two patent technologies acquired this time will enhance the ability to respond to advanced cyber infringement attempts. ”

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

We Know SECURITY!

Published by IGLOO SECURITY (www.igloosec.co.kr)
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.