Monthly Security Report

2021
February

Cover Story

- VPN Traffic Monitoring Scheme in Zero Trust Environment
- Cyber Squatting
- Solarwinds and Malware
- IGLOO Security's Management Security Methodology
  2) ID.BE Business Environment

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. 2021. All rights reserved

Cover Story

1. IGLOO Threat Insight

- Summary
- Monthly security threat trend and analysis
- Detailed analysis of attack pattern
- Indicator of compromise(IOC)
- Detection policy

2. Monthly Security Issue

- Security Issue

3. SIEM Guide (SPiDER TM V5.x)

- VPN Traffic Monitoring Scheme in Zero Trust Environment

4. Tech Note

- Tech Note : Cyber Squatting
- IGLOO Analysis Report : Solarwinds and Malware

5. Focus On IGLOO

- IGLOO Security's Management Security Methodology
  2) ID.BE Business Environment

Copyright © IGLOO Security, Inc. 2021. All rights reserved

Cover Story

CHAPTER 1

IGLOO Threat Insight

1. Summary

2. Monthly security threat trend and analysis

01. Monthly attack pattern
02. Monthly vulnerability attack TOP 10
03. Monthly threat IP address TOP 10

3. Detailed analysis of attack pattern

4. Indicator of compromise(IOC)

5. Detection policy

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Summary

Monthly Hot Issue

Change can easily be found at world-renowned conferences. At MWC and CES, automobiles are emerging as a key tool to show off their technology, and the world's largest commercial vehicle companies set up booths and participate in them. Now, automobiles are changing from a representative product of mechanical engineering born in the industrial revolution to a representative of IT technology. However, as there is a shadow when there is light, with the development of automobile IT technology, automobiles have begun to be exposed to external hacking risks. Unlike information leakage due to general hacking, car hacking can make the driver and the surroundings dangerous. Fortunately, the government and industry are rapidly developing standards and technologies, as well as research on related security. If this is the trend, we believe that general users will not have to worry about security issues from the time autonomous driving is commercialized. Now, many security industry officials, including IGLOO SECURITY, seem to have to think more about how to protect a new security target such as automobiles, not only from a technology point of view, but also from the process. In the not far future overcoming COVID-19, we hope that humans can ride safely and comfortably to their hometown in autonomous vehicles.

Monthly Statistics Analysis

- This month, as in the previous month, system vulnerabilities accounted for the highest percentage of attack types. This is confirmed as the effect of the increase in the vulnerability related to Command Injection.
- In order to prevent network scan (Nmap, masscan, OpenVas), it is recommended to establish firewall policy and close unused service ports so that only authorized users can access major services.
- The security administrator must periodically manage the part of applying the latest patch and checking updates to all servers that are internally managed and used.

※ Statistical data used in this report was prepared based on data collected through SIEM at IGLOO SECURITY, INC.'s Security Operation Center.

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

2 Monthly security threat trend and analysis

In order to predict cyber threats, the IGLOO SECURITY's Security Operation Center collects and analyzes the monthly attack type, the number and rate of attacks by vulnerability and source IP.

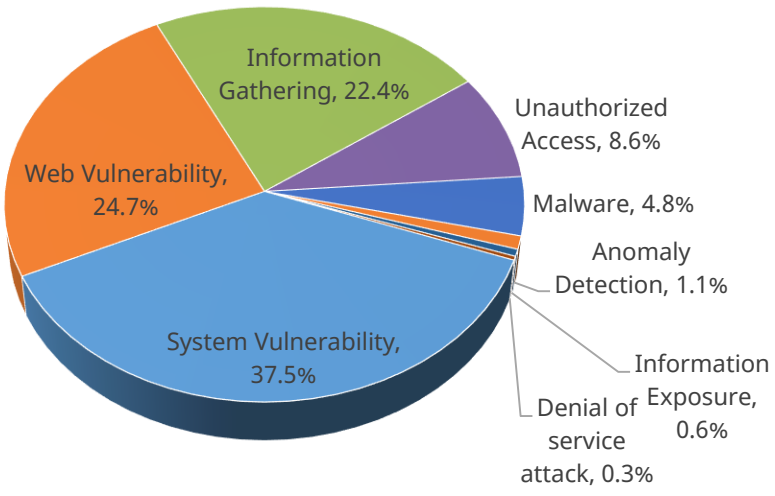
01. Monthly attack pattern

※ Based on the IGLOO Security's SOC report

Pattern	Counts	Ratio(%)	Fluctuation
System Vulnerability	3,209	37.5	-
Web Vulnerability	2,108	24.7	-
Information Gathering	1,913	22.4	-
Unauthorized access	738	8.6	-
Malware	411	4.8	-
Anomaly Detection	92	1.1	-
Information Exposure	49	0.6	-
Denial of service attack	27	0.3	-
Total	8,547	100	-

[Table1-1] Monthly Attack Patten

As a result of checking the monthly attack type in February 2021, you can see the same ranking results as in the previous month. System vulnerability accounts for the largest percentage of monthly attack types, and this is confirmed by the impact of command injection-related vulnerabilities among the top 10 monthly vulnerabilities. After that, Web Vulnerability and Information Gathering accounted for the ratio in order.



Copyright © IGLOO Security, Inc. 2021. All rights reserved

2 Monthly security threat trend and analysis

02. Monthly vulnerability attack TOP 10

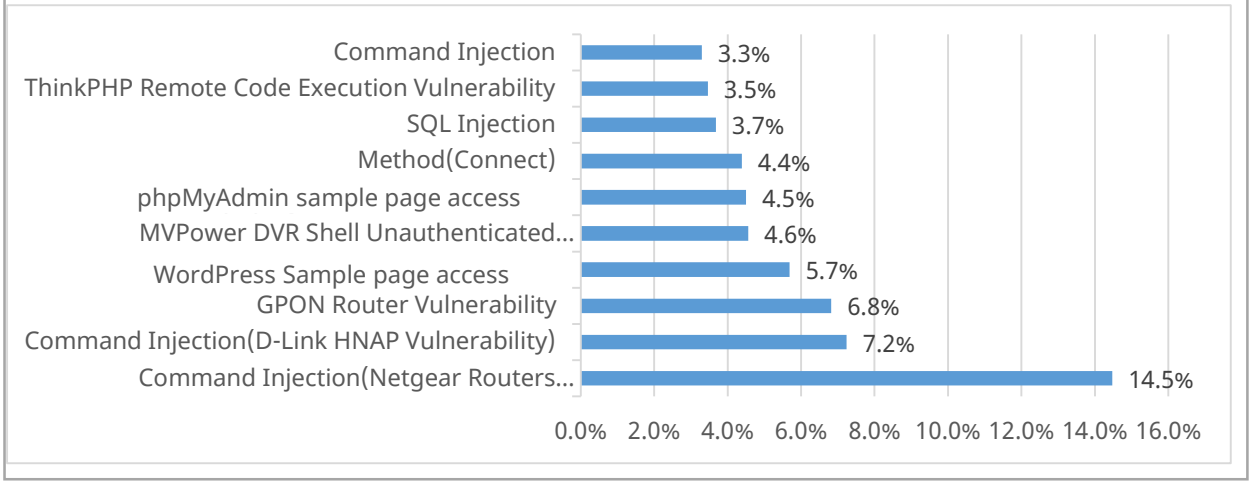
As a result of checking the top 10 monthly vulnerability attacks in February 2021, SQL Injection and ThinkPHP Remote Code Execution Vulnerability newly entered the Top 10. In addition, GPON Router Vulnerability, phpMyAdmin sample page access ranking decline, and WordPress sample page access vulnerability rapidly rise.

※ Based on the IGLOO Security's SOC report

Rank	Detection Name	Counts	Ratio(%)	Fluctuation
1	Command Injection (Netgear Routers Vulnerability)	1,237	14.5	-
2	Command Injection (D-Link HNAP Vulnerability)	619	7.2	▲1
3	GPON Router Vulnerability	583	6.8	▼1
4	WordPress Sample Page Access	486	5.7	▲6
5	MVPower DVR Shell Unauthenticated Command Execution	390	4.6	▲2
6	phpMyAdmin Sample Page Access	385	4.5	▼2
7	Method(Connect)	375	4.4	▲2
8	SQL Injection	315	3.7	NEW
9	ThinkPHP Remote Code Execution Vulnerability	296	3.5	NEW
10	Command Injection	282	3.3	▼2
	Total	4,968	58.1	-

Total Threats In SOC

Top 10 and percentage of vulnerability events that were detected and responded to intrusion reports by the IGLOO Security SOC.



[Table1-2] Monthly vulnerability attack TOP 10

Copyright © IGLOO Security, Inc. 2021. All rights reserved

2 Monthly security threat trend and analysis

03. Monthly threat IP address TOP 10

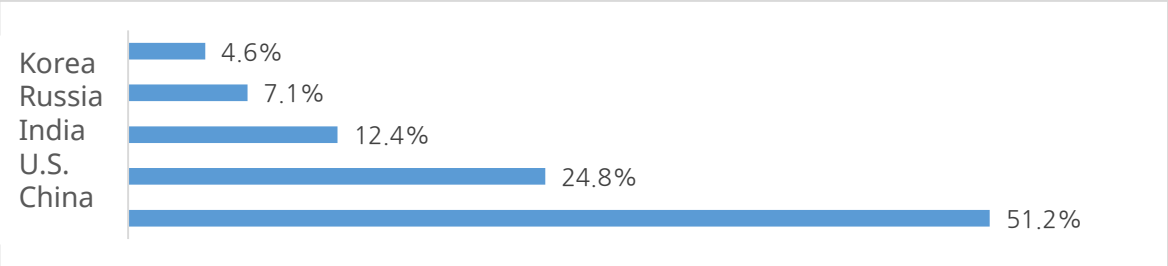
As of February 2021, as a result of confirming the top 10 source IPs, the IP from China occupies the majority and holds the highest market share. After that, it was identified in the order of Russia, India, the United States, and China. The harmfulness of the source IP is the result of checking in IGLOO_CTI, OSINT information, etc.
It is recommended to block the firewall or other security devices by referring to the table below.

※ Based on the IGLOO Security's SOC report

Rank	Threat IP	Country	IGLOO_CTI	Attack Information
1	45.155.205.108	RU	14/114	ThinkPHP Remote Code Execution Vulnerability
2	89.248.170.31	GB	6/114	ThinkPHP Remote Code Execution Vulnerability
3	199.19.226.67	US	19/114	Web Scanner(ZmEu)
4	89.248.162.235	GB	8/114	Web Scanner(ZmEu)
5	43.229.62.95	AU	2/114	Network Scanner(masscan)
6	97.74.229.113	US	4/114	Admin page access
7	103.78.208.100	ID	9/114	Network Scanner(masscan)
8	89.248.168.108	GB	21/114	Restriction Method(limited method)
9	211.211.195.105	KR	0/114	XML External ENTITY Injection
10	72.251.228.101	US	11/114	SIP Vulnerability Scanner(Sipvicious)

Total Countries

This month's attack IP, country ranking detailed Top 10 table and ratio



Rank	Source IP	Country
1	45.155.205.108	RU
2	89.248.170.31	GB
3	199.19.226.67	US
4	89.248.162.235	GB
5	43.229.62.95	AU

Rank	Source IP	Country
6	97.74.229.113	US
7	103.78.208.100	ID
8	89.248.168.108	GB
9	211.211.195.105	KR
10	72.251.228.101	US

[Table1-3] Monthly source IP address TOP 10

Copyright © IGLOO Security, Inc. 2021. All rights reserved

3 Detailed analysis of attack pattern

We introduce detailed analysis results according to attack patterns, focusing on the TOP 10 of the vulnerability patterns that occurred in February.
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 result
Command Injection (Netgear Routers Vulnerability)	A vulnerability that occurs when the web server in the NetGear DGN series router does not authenticate some URLs. You can execute arbitrary commands by using the "syscmd" function of the "setup.cgi" script.
Command Injection (D-Link HNAP Vulnerability)	Due to the vulnerability in the HNAP (Home Network Administration Protocol) related script used when installing D-Link products, it is possible to bypass authentication and execute commands such as service stop and backdoor installation. The attacker inserts a command after the Domain/HNAP1/GetDeviceSettings/ path and tries to execute it using the SOAPAction field.
GPON Router Vulnerability	A vulnerability found in Dasan GPON home routers. It is a vulnerability that can pass the authentication process by entering the string '?images' into the URL of the device. By exploiting this vulnerability, an unauthenticated attacker can remotely execute commands on the device and modify DNS settings.
WordPress Sample page access	This event accesses sensitive sample pages such as wp-login.php, wp-admin.php, and wp-config.php, which are WordPress login pages, and is mainly used to check the existence of the page.
MVPower DVR Shell Unauthenticated Command Execution	When processing an HTTP request, validation of the user-supplied input is insufficient, so a remote attacker can execute arbitrary system commands in a query string by using the \'shell\' file in the web interface.
phpMyAdmin sample page access	phpMyAdmin is an open source tool written in PHP for the purpose of managing MySQL on a web server. It searches for vulnerabilities in the My-SQL server, creates/deletes a database, creates/deletes a table, creates/deletes a field, executes SQL statements, and has permissions. It is an attack that can execute management functions. If this vulnerability exists, it has a vulnerability that can execute system commands by inserting an arbitrary function using the `?` argument in the script/setup.php file of phpMyAdmin.
Method (Connect)	Try to access the inside through HTTP TLS (Transport Layer Security) tunneling using the Connect Method. For this, the Connect Method is used, and if there is a vulnerability, it may be used as an intermediate stop for an attack.
SQL Injection	SQL Injection attack can occur when the input value is used in the query statement without filtering the characters used in the query such as special characters, Union, and Select in the web page. The attacker can acquire, modify, delete and access the system by using various queries within the privileges of the account connected to the DB.
ThinkPHP Remote Code Execution Vulnerability	This is a vulnerability that could lead to a remote code execution attack by calling an inappropriate controller class due to ThinkPHP's vulnerable character filtering. By calling the \think* classes, the vulnerable object could allow an attacker to execute arbitrary PHP code and system commands.
Command Injection	If the input value including the system command does not go through an appropriate verification procedure, the received command may be executed. If a vulnerability exists, an attacker can directly transmit commands to the system, so additional damage may occur through file browsing, downloading, and execution.

[Table 1-4] Detailed Analysis of the Top 10 Monthly Vulnerability Attacks

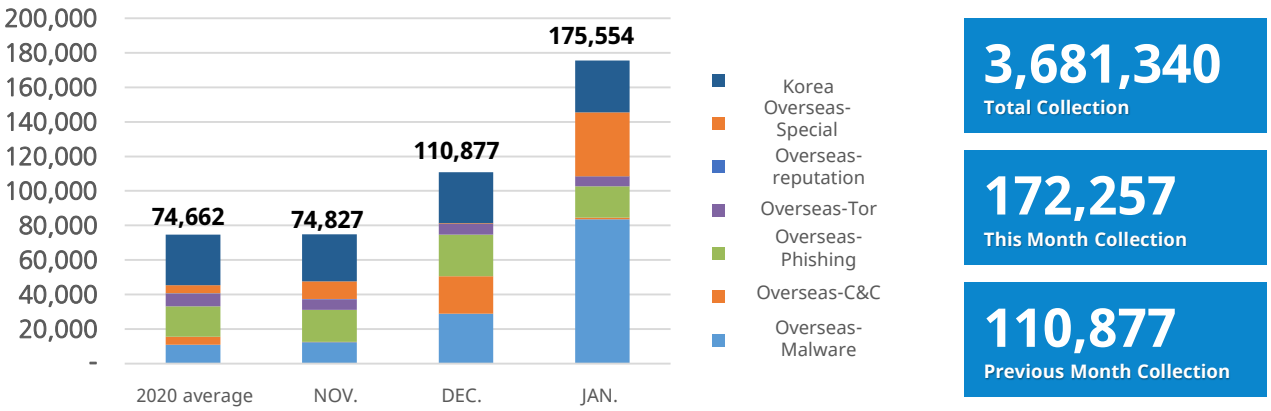
Copyright © IGLOO Security, Inc. 2021. All rights reserved

4 Indicator of compromise(IOC)

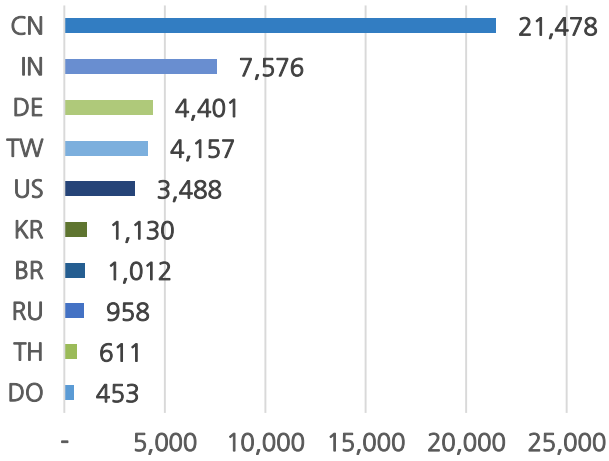
IGLOO Security continues to share security threat information collected by worldwide companies and organizations in order to prevent cyber attacks in advance and to help quickly identify attackers when an attack is detected. It selects and provides detailed information related to the customer company among the collected threat information to enable a preemptive response by detecting the context and purpose of the attack against the security threat that the customer targets the organization.

▶ Monthly threat information collection statistics

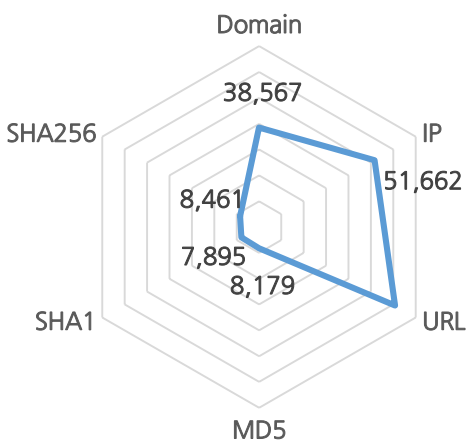
Looking at data for one month in January 2021, [Overseas-Malware (▲54,700)] collection is showing strong performance, followed by [Overseas-Special (▲36,663)].[Korea (▲596)] The data rose slightly from the previous month.



[Figure 1-1] Counts of threat information collection in the last 3 months



[Figure 1-2] Threat IP Country Status



[Figure 1-3] Collection Status by IoC

* Detailed information is available through IGLOO CTI (Cyber Threat Intelligence).

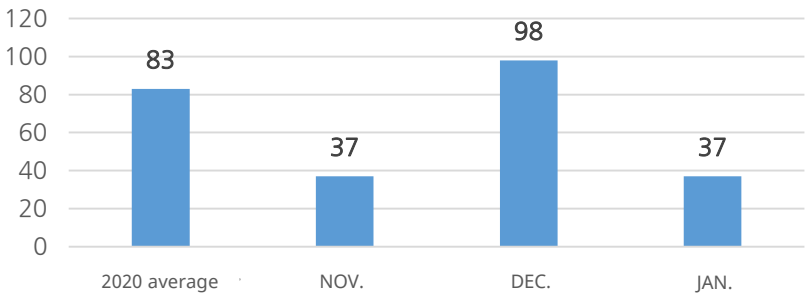
Copyright © IGLOO Security, Inc. 2021. All rights reserved

5 Detection Policy

IGLOO Security continues to share cyber threat detection policies collected or self-produced by companies and institutions so that cyber attacks can be quickly identified. The cyber threat detection policy is provided in the form of a Snort Rule so that cyber attacks can be efficiently detected and responded to, and quickly applied to the security operation center, and the security of the organization is kept up to date by applying it to the security device with the provided detection pattern.

▶ Monthly Cyber Threat Detection Policy Statistics

In January 2021, 37 cyber threat detection policies were shared during the month. During the month of January, detection policies for Solarwinds-related (CVE-2020-10148), CISCO (CVE-2020-26085) vulnerabilities, BumbleBee Webshell, and Trickbot Malware were released.



[Figure 1-4] Counts in the last 3 months

4,819
Total Count

37
This Month Count

98
Previous Month Count

[Figure 1-5] Monthly Counts

Code	Detection Policy	Description	Tag
IGRSS.10.04820	alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.10.04820 SolarWinds, Orion API, CVE-2020-10148 , Web Application Attack"; flow:to_server,established; conten t:"i18n.ashx"; fast_pattern:only; http_uri; content:"&v="; noc ase; http_uri; sid:1004820;)	Policy to detect web application authentication bypass attacks that exploit the CVE-2020-10148 vulnerability of SolarWinds Orion API	SolarWinds, Orion API, CVE-2020-10148
IGRSS.2.04831	alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"IGRSS.2.04831 Cisco, Jabber, CVE-2020-26085, Attempte d User Privilege Gain"; flow:to_server,established; content:"/ CLIENT_REQUEST"; fast_pattern:only; http_uri; content:"onan imationstart"; nocase; http_client_body; sid:204831;)	Policy to detect attempts to steal user privileges that exploit Cisco Jabber's CVE-2020-26085 vulnerability	Cisco, Jabber, CVE-2020-26085
IGRSS.8.04837	alert tcp $EXTERNAL_NET $FILE_DATA_PORTS -> $HOME_NET any (msg:"IGRSS.8.04837 Webshell, BumbleBee, A Network T rojan was detected"; flow:to_client,established; file_data; con tent:"<%if(Ntody(Request.QueryString[|22|parameter|22|]) ==|22|"; fast_pattern:only; sid:804837;)	BumbleBee Webshell's policy to detect network communication	Webshell, BumbleBee
IGRSS.8.04844	alert tcp $EXTERNAL_NET any -> $SMTP_SERVERS 25 (msg:"I GRSS.8.04844 Malware, Trickbot, A Network Trojan was detec ted"; flow:to_server,established; file_data; content:"|2C E7 6 A B3 CE 43 A8 23 3F 8B BF 86 1B 6B 78 4D DA 8C 38 2B A4 F5 26 27 0B 1E 6D DF 70 85 8B FC|"; fast_pattern:only; sid:80484 4;)	Trickbot Malware's policy to detect network communication	Malware, Trickbot

[Table 1-5] Monthly Major Cyber Threat Detection Policies

Copyright © IGLOO Security, Inc. 2021. All rights reserved

Cover Story

CHAPTER 2

Monthly Security Issue

1. Security issue

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 Security Issue

Warning for distribution of malicious apps through illegal adult sites

- A situation in which a malicious app disguised as a chat service is being distributed on an illegal adult site was caught. Attackers appear to have created apps for Android and iOS respectively.
- According to East Security, malicious apps are being distributed through the site, and even when the site is blocked, it is warned that it is still being distributed through new addresses.
- When infected with this malicious app, user information such as phone number and contact list is stolen, and there is a high risk of cyber threats such as phishing in the future.
- Currently, access to the website where this malicious app is distributed is blocked, but the situation of other malicious apps disguised as camera apps is also founded, requiring special attention.
- Security experts say that many cyber attackers are attempting to steal smartphone information with a lot of private and personal information, and recommend that you install the app through the official app store and avoid illegal site access.

US Department of State establishes “Bureau of Cyberspace Security and Emerging Technologies”

- The US State Department announced that it will establish a Cyberspace Security and Emerging Technologies (CSET) to strengthen diplomatic efforts to respond to cyber threats from North Korea, China, and Russia.
- According to local US media, US Secretary of State Mike Pompeo has finally approved the establishment of the Cyberspace Security and Emerging Technologies (CSET) in accordance with the recent Solarwinds crisis.
- At the end of last year, the US State Department, along with major government departments, was infected with SolarWinds software, which contains backdoors. The U.S. government is investigating the Solarwinds crisis, seeing the Russian government as a strong background.
- The State Department said that national security challenges from China, Russia, Iran, North Korea and other competitors and enemies continued to increase, and that the need to reorganize diplomatic capabilities in the field through the establishment of CSET became important.
- Unlike the existing Cyber Infrastructure Security Administration (CISA) under the U.S. Department of Homeland Security, which plays a role in protecting the public and public from cyber attacks, the CSET is expected to focus more on diplomacy in the field of cybersecurity.

Most phishing attacks pretending to be MS

- According to the ‘Phishing Report for Q4 2020,’ released by Checkpoint, ‘Microsoft (MS)’ was the most common cyber attackers impersonated for phishing attacks in the fourth quarter of last year.
- Checkpoint analyzed that the spread of remote work due to the COVID-19 pandemic had an effect on the ranking of impersonation agencies. In fact, it appears that there has been an explosion of fake email attacks on employees who are working from home or remotely, asking them to reset their MS 365 account.
- In the fourth quarter of last year, attempts to steal user accounts by disguised as MS-related login screens accounted for 43% of all phishing attacks. Logistics delivery company DHL (18%), social platform LinkedIn (6%), online shopping malls Amazon (5%) and Rakuten (4%) followed.
- Security experts say you should always be cautious when entering personal data or accounts into corporate business applications, and urge you to take a closer look before opening emails that appear to come from Microsoft and Google.

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

Cover Story

CHAPTER 3

SIEM Guide (SPiDER TM V5.x)

VPN Traffic Monitoring Scheme
in Zero Trust Environment

Copyright © IGLOO Security, Inc. 2021. All rights reserved

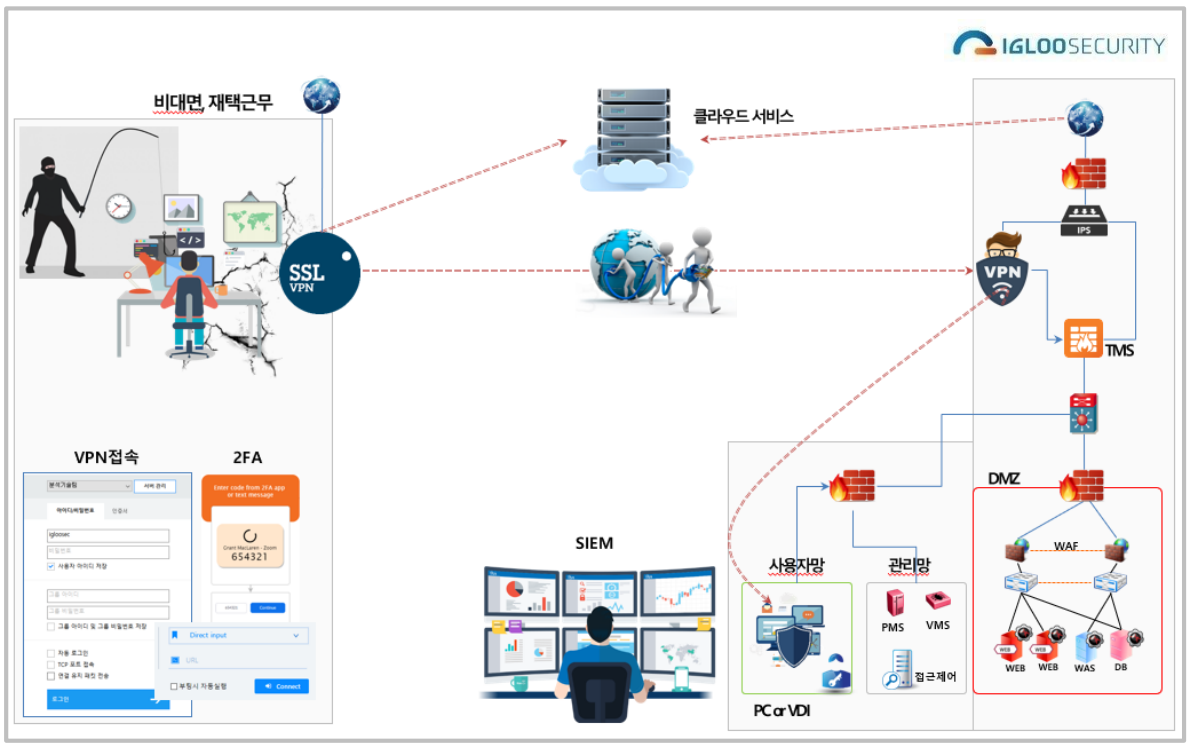
VPN Traffic Monitoring Scheme in Zero Trust Environment

SPiDER TM V5.0 is an integrated security management solution that combines IGLOO SECURITY's security monitoring experience and big data utilization capabilities. It increases the agility and efficiency of the monitoring business through the unified environment configuration from initial detection to log analysis.

Technical Support Center
Analysis Technology Team

01. Non-face-to-face, Remote work

It is said that due to the spread of COVID-19, the number of companies and institutions that work from home has increased more than four times. Companies are actively using remote access security technologies such as SSL VPN to work from home. VPN is a long-established technology, providing remote workers with a secure passage to corporate networks in the past. In this SIEM guide, we would like to present a plan on how internal employees can use SIEM to monitor security in order to continuously use a secure VPN.



[Figure 3-1] Telecommuting VPN environment

Copyright © IGLOO Security, Inc. 2021. All rights reserved

VPN Traffic Monitoring Scheme in Zero Trust Environment

02. Establishment of scenarios for security monitoring of telecommuters

As shown in [Figure 3-1], telecommuters can access the company system or network through the VPN device. There are two main types of this approach.

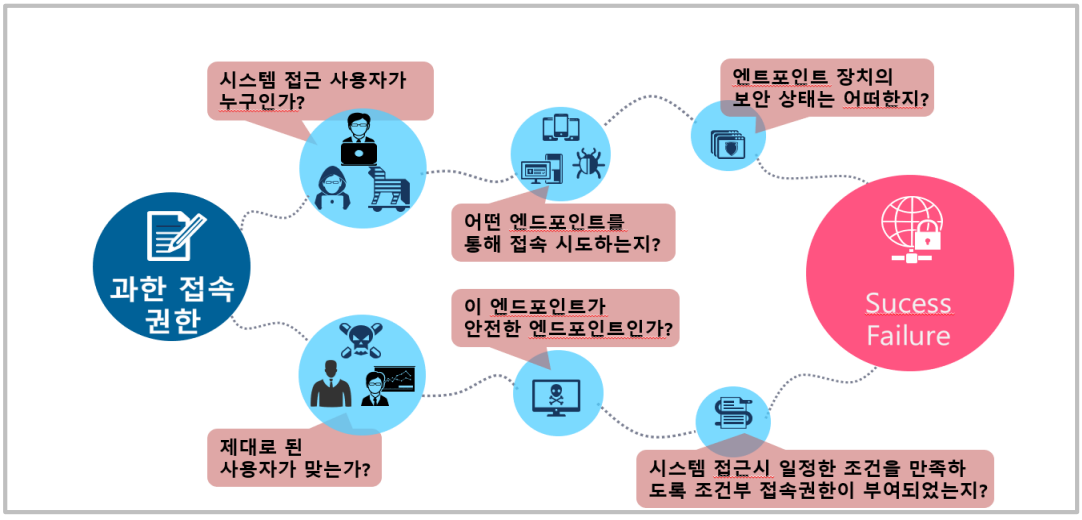
The first method : home workers can work in the existing way by accessing only their own PC, which is affected by the company's security policy.

The second method : granting authority by setting policies for each company system accessible to telecommuters through VPN equipment.

The first method can be monitored by the existing security operating environment. But, In this issue, we will look at the security monitoring method for telecommuters for the second method, which is the most used. VPN is a security technique based on the concept of network perimeter. Telecommuters or remote workers are authorized via VPN, but what these employees do to company systems should be monitored. By applying the Zero Trust security model, you can start with the premise that "there is no one to trust in the world."

▶ The scenario for security monitoring of telecommuters is as follows. IGLOOSECURITY	
1. Are there any excessive access rights in the VPN policy?	6. Is this terminal in a safe state?
2. Can identify who the system access user is?	7. Was conditional access granted to satisfy certain conditions when accessing the internal system?
3. Can check whether the user is authorized or not	8. If you have access to the internal system, can you identify working hours, non-work hours, weekends, holidays and nights?
4. What terminal do you try to connect to, such as a PC, cell phone, or pad?	9. What actions (commands, file transfers, etc.) do you do if you are connected to the server?
5. What is the security status of the terminal device?	

In addition, there will be various monitoring items. Recently, many teleworking guides have also been published. Above all, it is essential to establish a monitoring plan suitable for the company environment.



[Figure 3-2] Access scenario

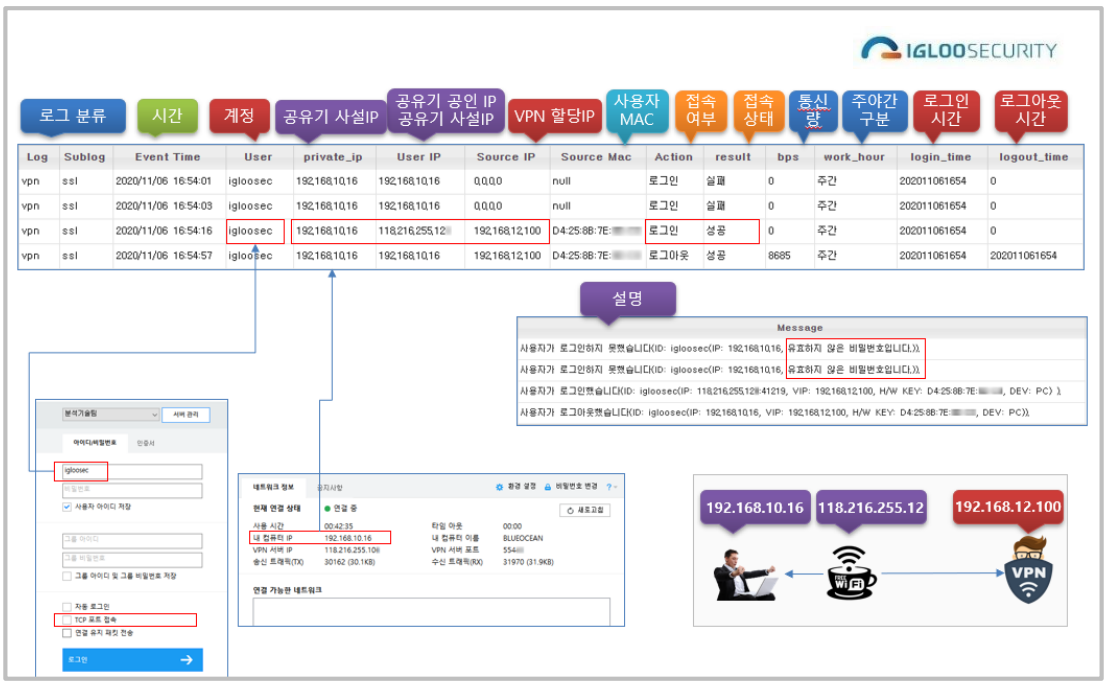
Copyright © IGLOO Security, Inc. 2021. All rights reserved

VPN Traffic Monitoring Scheme in Zero Trust Environment

03. Security equipment log characteristics & analysis

1) SSL VPN authentication log

To monitor the behavior of telecommuters, let's first look at the SSL VPN authentication log. The USER field is the VPN access account of the home worker. IP has 3 fields. The Private IP field is the private IP of the router. User IP is the public IP of the router. When you log in to the VPN normally, the public IP remains, but when the login fails or logs out, the router's private IP remains. Through User IP, it is possible to identify where users of the same account access from and whether they are connecting to multiple terminals at the same time. And, the source IP is assigned an IP to be used in the corporate network when the VPN is normally logged in. In other words, the log left in FW, IPS, WEB server, etc. is the Source IP. In addition, there are MAC addresses that can distinguish user terminals, login success/failure, day/night classification, and access time.



[Figure 3-3] SSL VPN authentication log

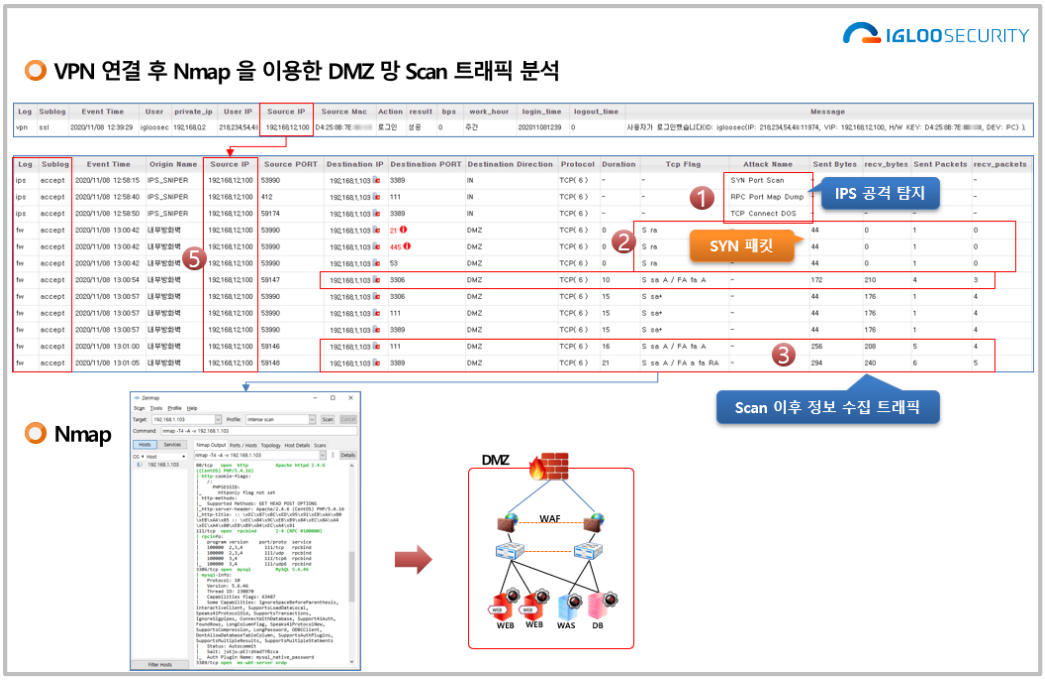
2) Analysis of abnormal behavior log after VPN connection

After the VPN connection, mock training was preceded to monitor the behavior of home workers. The premise is that a home worker's PC is infected with a malicious code, and a hacker can remotely control it. [Figure 3-4] is the log analysis content that occurs when a hacker scans with the Nmap tool to collect information through the company's DMZ network while connected to the VPN.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

VPN Traffic Monitoring Scheme in Zero Trust Environment

192.168.12.100 IP connects to VPN normally, and after that, you can see logs detected by ①SYN Port Scan, RPC Port Map Dump, and TCP connect DOS policy in IPS by Nmap Scan.
In the FW log, for ports that do not respond by service scan, you can see ②TCP flag'S ra', 44 bytes for Sent bytes, and 0 bytes for recv bytes.
If the service port is open, there will be data in the response packet like ③recv byte 176byte.
If you collect information after checking the service port, you can see the size changed to ④Sent bytes 256 bytes and recv bytes 208 bytes.
And, it can be confirmed that the IP assigned from the VPN remains the same as ⑤ the origin IP in the FW and IPS for the perimeter security equipment.
The part to be pointed out here is VPN communication, but depending on where the VPN device is located, whether or not it is affected by the policies of the internal perimeter security devices varies. And, it may be natural, but it can be said that the VPN communication environment is the same that I have in the company's network.



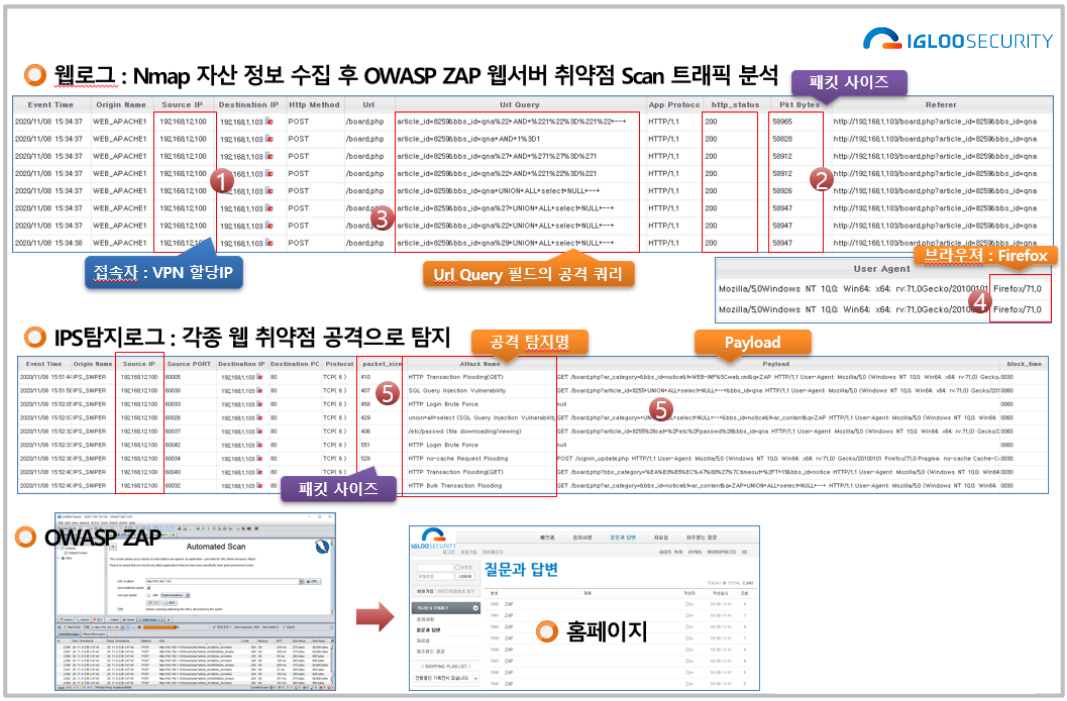
[Figure 3-4] SSL VPN authentication log

Once the web server information has been collected through the DMZ area, now we will simulate the web vulnerability scan through the OWASP ZAP tool while connected to the VPN. [Figure 3-5] It can be seen that the VPN allocated ① departing IP from 192.168.12.100 to web server 192.168.1.103 repeatedly accesses ② packet 5897 of a certain size in POST method. And, you can see that the attack code "~UNION+ALL+select+NULL+--+", which is the most important ③URL Query, attacks with a slight change, and ④User Agent remains as Firefox/71.0. Of course, User Agent can be changed.

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

VPN Traffic Monitoring Scheme in Zero Trust Environment

The telecommuter IP 192.168.12.100 was detected by a number of web vulnerability attacks such as ⑤SQL Query Injection, union+all+select, etc. in the IPS device by the OWASP ZAP tool vulnerability Scan attack. As such, it would be good to consider that depending on the location of the VPN device, it may be influenced or bypassed by the policies of internal security devices.



[Figure 3-5] OWASP ZAP Web Vulnerability Scan Result

3) Remote desktop traffic analysis

This is the traffic screen when connecting from a telecommuter PC to the internal PC of the company ① from ISP environment and ② from VPN environment to remote desktop. When connecting in a general Internet environment, the source IP is public IP, and it can be confirmed that it is ③TCP communication. However, in the VPN environment, it can be confirmed that it is the VPN assigned IP and ④UDP communication. VPN is a basic UDP communication.

[Figure 3-6] Remote Desktop Traffic

Copyright © IGLOO Security, Inc. 2021. All rights reserved

VPN Traffic Monitoring Scheme in Zero Trust Environment

4) SSH connection traffic analysis

There are cases where the home worker is a server administrator or an application administrator and has access to internal systems such as a web server. The problem is, the story will be different if a home worker PC with such privileges is infected with malware and is in the hacker.

When the terminal is connected to port 22 for server management, it remains as [Figure 3-6]. In the firewall log, the Duration field is the session connection ESTABLISHED time. In other words, you can see how long the hacker has been connected to the web server. However, the regrettable point is that the timing of logs to be left differs depending on the firewall manufacturer. There are cases where the connection is left when the connection is attempted, when the connection is terminated, and both are left, so it is important to understand the characteristics well.

In addition, the fields that are important for analysis are the Sent bytes field and the recv bytes field to determine the amount of data transmission/reception traffic. If data such as a file is uploaded, the Sent bytes field is large, and if the data is downloaded, the recv bytes field is large.

If the recv bytes field is large in the server, it can be predicted that internal information has been downloaded, and if the Sent bytes field is large when communicating over the Internet, it should be suspected of external leakage.

These features are the same when analyzing remote desktop traffic.

[Figure 3-7] SSH connection traffic analysis

5) System keylogging

If the hacker accessed the management server through the home worker's PC, it is important to analyze what actions (commands) were performed on the server. As shown in the log in [Figure 3-8], after ① login to the server and grasping the basic system structure, ③wget command was used to download and install additional malicious codes from outside.

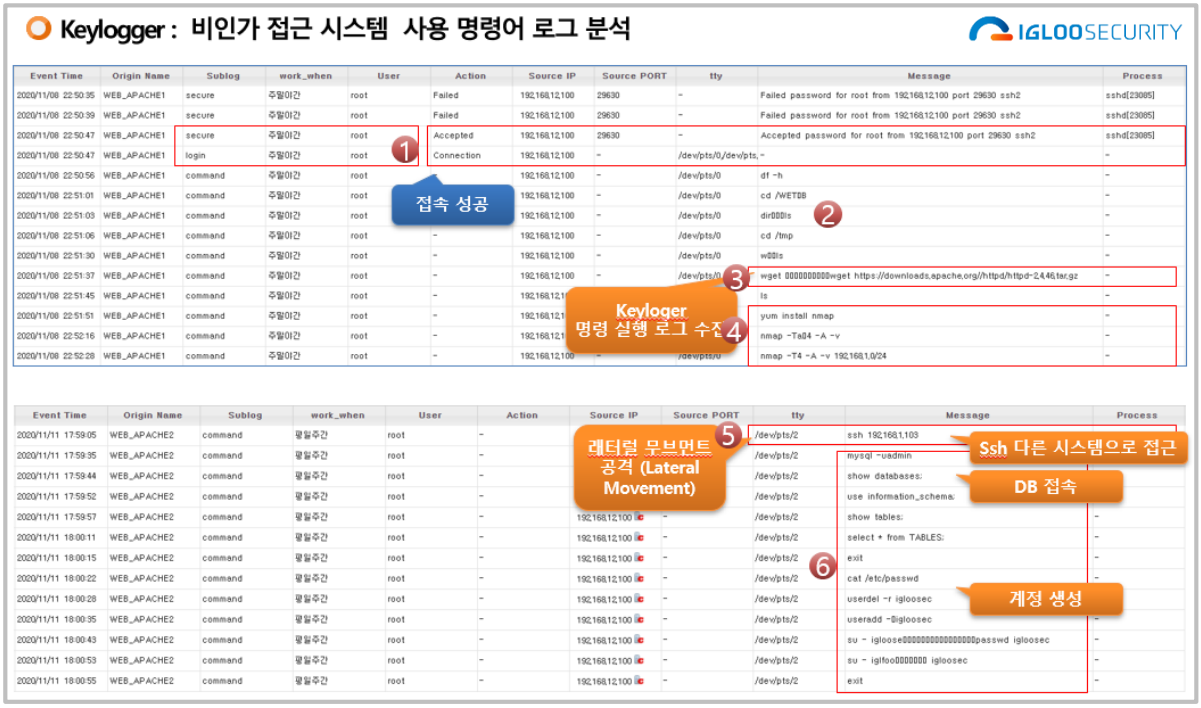
And, after installing nmap through ④yum, the information was collected by scanning the same band.

Then, after logging in to the DB server discovered through the ⑤ Lateral Movement attack, various DB information was collected. And, it can be seen that ⑥ even a general account for additional attacks is created.

In this way, it is possible to shorten the response time by immediately detecting and analyzing unauthorized access when all logs generated in the server can be collected in detail.

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

VPN Traffic Monitoring Scheme in Zero Trust Environment



[Figure 3-8] SSH connection traffic analysis

04. Custom interactive dashboard

1) VPN access status monitoring and analysis dashboard

Up to now, you can monitor and analyze the logs one by one, but if you view the entire log required for intrusion analysis on one screen, you can secure visibility and shorten the analysis time further. This can be done through the unified dashboard.

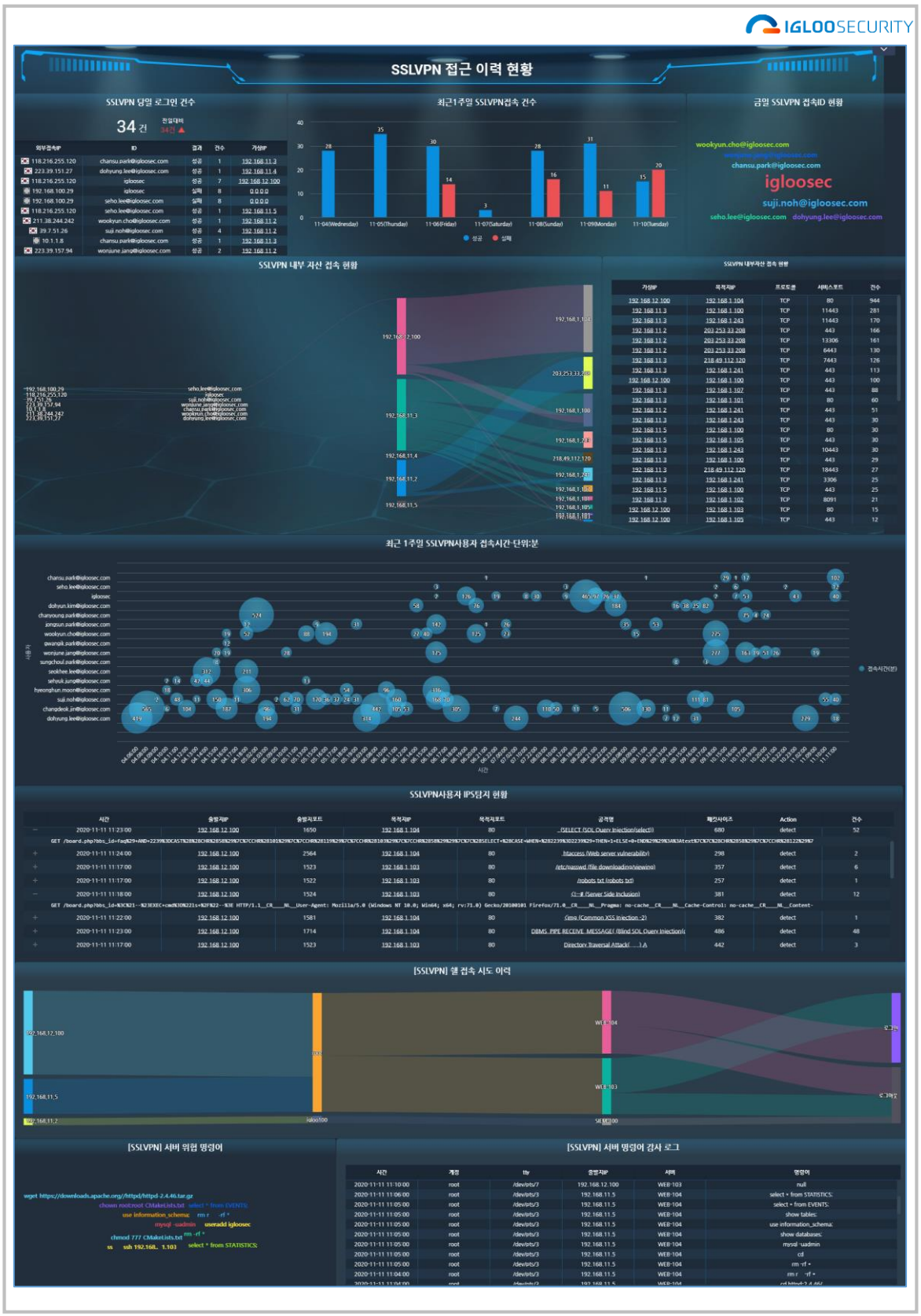
Until now, the dashboard has been used for simple briefings or status boards, but various configurations on one screen include threat information, asset information, detection trend, detection by major security equipment in infrastructure, and detailed logs of the security equipment required for analysis by attack type.

Of course, as mentioned above, the log collection required for intrusion analysis by attack type has the highest priority. Even in threat hunting, if you establish a hypothesis and define a log of signs that fit the hypothesis and configure it as a dashboard, you will be able to find threats more easily. The breach response rate will vary depending on how you use the security equipment and functions you have from different perspectives.

[Figure 3-9] Through the monitoring and analysis dashboard for SSL VPN connection status, visibility and monitoring by service became possible. In other words, real-time VPN access monitoring by telecommuters and filtering and outputting when abnormal behavior is detected by the IPS among VPN users will enable centralized management by separating them from external threats.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

VPN Traffic Monitoring Scheme in Zero Trust Environment



[Figure 3-9] SSL VPN connection status monitoring and analysis dashboard

Copyright © IGLOO Security, Inc. 2021. All rights reserved

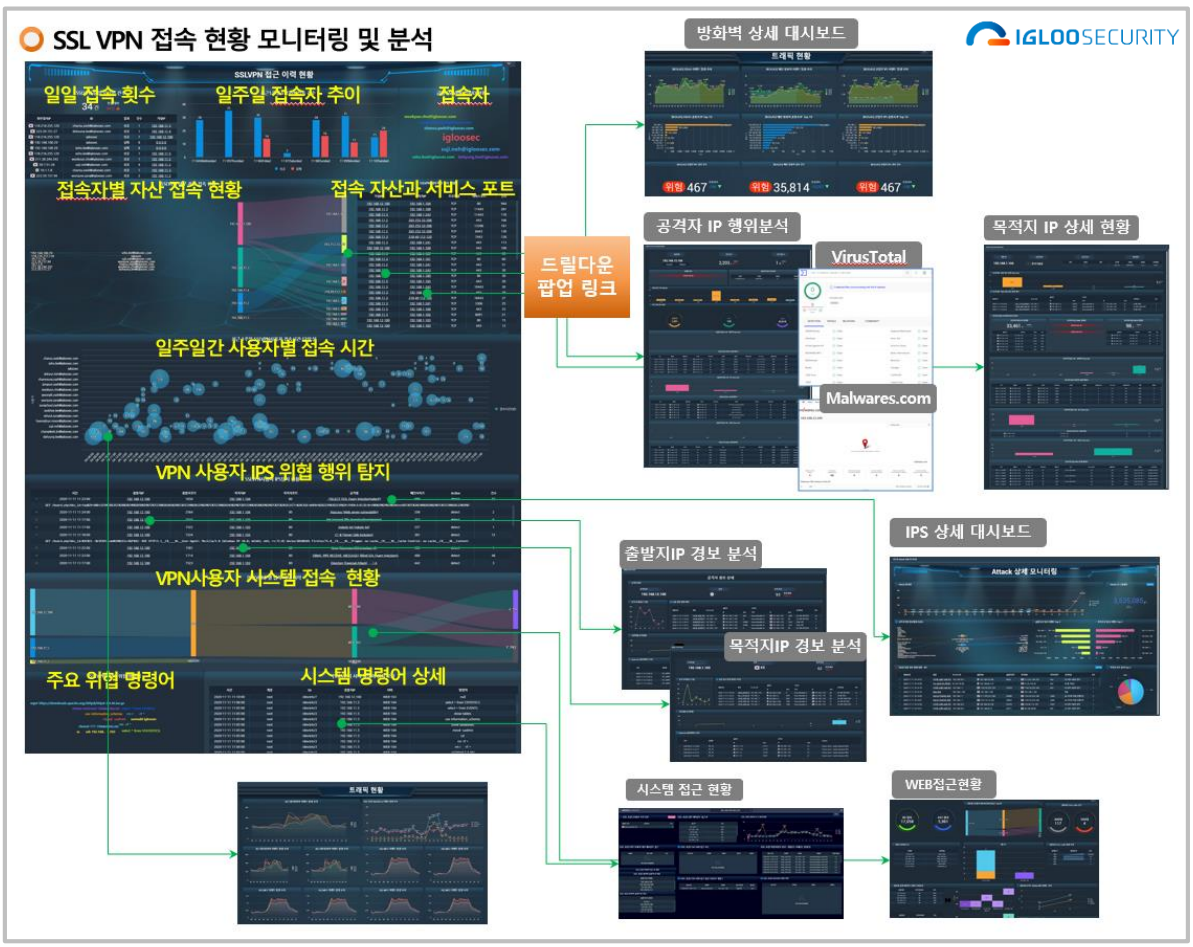
VPN Traffic Monitoring Scheme in Zero Trust Environment

In addition, when connecting to a management server or a web server among VPN users, the access system and service port for each user can be expressed in charts to understand at a glance. In other words, it is possible to immediately identify which asset inside the VPN connection was accessed. After accessing the system, it is possible to grasp which commands are executed, and among them, only threatened commands can be output separately to monitor abnormal behavior immediately.

[Figure 3-10] is an easy one-click dashboard configuration by expanding from the SSL VPN connection status monitoring dashboard. Unlike the past-generation dashboard, it can be configured to allow drill-down analysis of information necessary for additional analysis for each item.

In particular, it is possible to configure a dashboard that can analyze all logs of infrastructure security equipment for one hour or one month for the source IP. From the detection history, it takes an average of 1 hour to analyze each log of single security devices such as FW, IPS, and WEB. If you define these actions in advance and configure the dashboard required for analysis, you can view all logs at a glance in seconds with just one click.

If you create scenarios, define necessary logs, and organize them into dashboards, you will be able to improve fast and high response rates.



[Figure 3-10] One-Click Analysis-Pop-up Link Dashboard

Copyright © IGLOO Security, Inc. 2021. All rights reserved

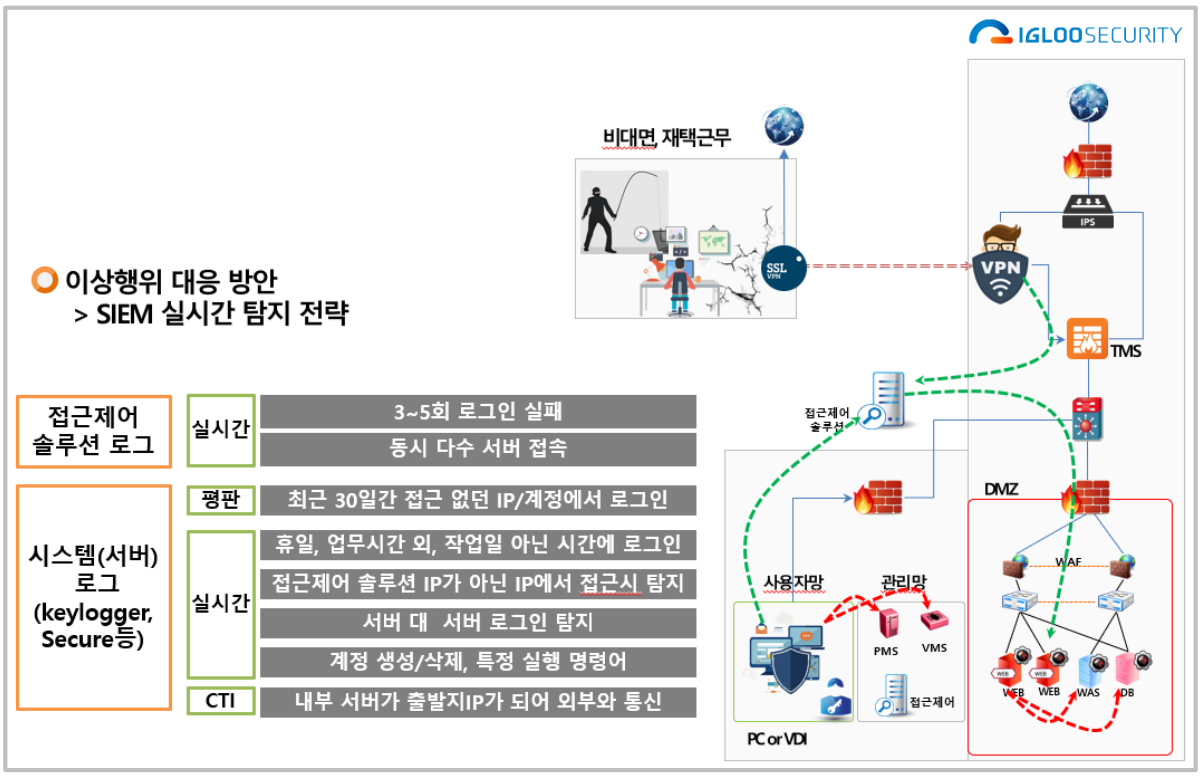
VPN Traffic Monitoring Scheme in Zero Trust Environment

05. VPN connection abnormal behavior detection plan

1) SIEM detection strategy

Real-time monitoring of the abnormal behavior described above is good, but since continuous monitoring is not possible, it is possible to automatically detect abnormal behavior by scenario.
[Figure 3-11] is a scenario configuration diagram of a detection strategy when unauthorized access to the server among VPN users. There is a detection method when a threat command is executed after access control solution logs are collected in real time and the number of login failures or multiple simultaneous servers are accessed in a short time. In addition, the following threats can be detected through the server log and the log collection of the keylogger function of the SIEM Agent.

1. Reputation detection: Login from an IP/account that has not been accessed for the last 30 days
2. Realtime Detection
   - Log in on holidays, outside business hours, or during non-working days
   - Detect when accessing from an IP other than the access control solution IP
   - Server-to-server login detection, account creation/deletion
   - Detect specific threat execution commands
3. Comparison with CTI threat information: Detected when the internal server becomes the source IP and communicates with the outside



[Figure 3-11] VPN User Server Unauthorized Access Detection Strategy Scenario

Copyright © IGLOO Security, Inc. 2021. All rights reserved

VPN Traffic Monitoring Scheme in Zero Trust Environment

2) Correlation analysis detection setting

[Figure 3-12] is a rule setting that detects visitors on holidays and nights outside of working hours among VPN traffic. And, these are detection policies that can detect when sending and receiving large amounts of data outside of business hours.

In addition, by collecting the reputation of the usual server connection, it is possible to detect a login attempt, an attempt to access an account without a history of access within 30 days, an account creation, and a change in a period other than the time of password change.

With only logs, you can detect a variety of strange threats.

[Figure 3-12] Strange threat behavior detection settings

3) Automatic blocking of attack IP (available upon the user environment)

If a VPN accessor performs strange threats at a time when security activities are weak such as night time, it is possible to automatically block according to certain conditions through the automatic blocking integration function between SIEM and firewall.

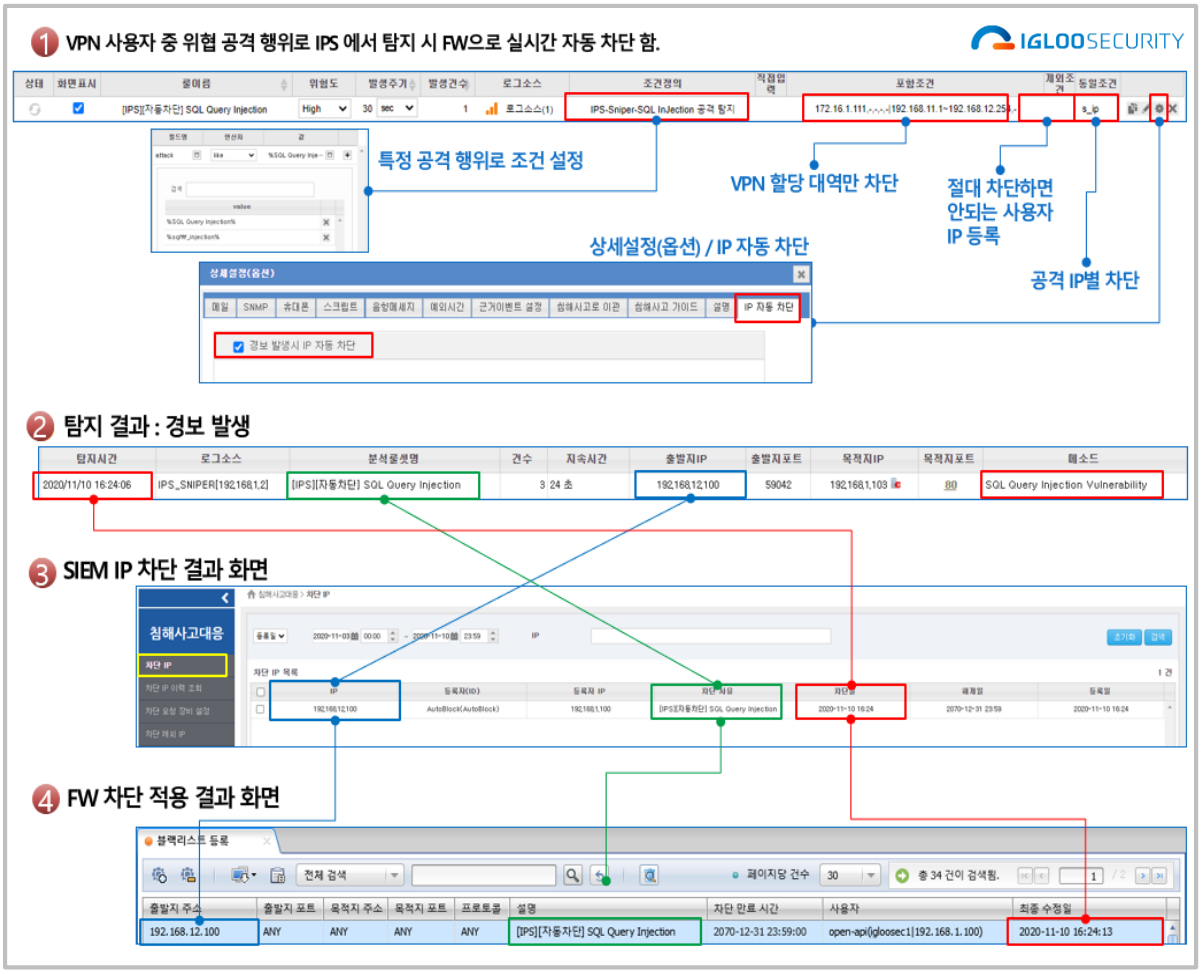
In the case of [Figure 3-13], a correlation analysis detection rule was set in SIEM as a condition of a specific threat attack behavior in the IPS among ①VPN users and a traffic condition destined for a specific destination. In addition, an automatic IP blocking option was set when an alarm occurs as an automatic response. User IPs that should never be blocked can be registered in the exclusion condition.② If an alarm occurs due to the correlation analysis condition, the corresponding source IP is ④ Blocked by firewall.

At the same time, it is registered in the ③Infringement accident response> Blocking IP menu, and the blocking history management is automatically performed. Blocked IP list information includes blocking IP, registrant, blocking reason, blocking date, and release date.

The time required to block the firewall after the alarm is triggered is less than 10 seconds, which is quickly blocked. Of course, you need to be cautious about automatic blocking, but you can set up a safe condition and set up a safety device by registering a white list.

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

VPN Traffic Monitoring Scheme in Zero Trust Environment



[Figure 3-13] Strange threat behavior detection settings

05. Conclusion

In the non-face-to-face era of COVID-19, we looked at ways to monitor VPN traffic using SIEM to ensure a safe environment for employees working in various places.

If you understand, collect, detect, and visualize logs generated in the infrastructure as much as possible through SIEM, you will be able to improve the security response rate by creating an easy security monitoring environment.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

Cover Story

CHAPTER 4

Tech Note

1. Tech Note
   : Cyber Squatting

2. IGLOO Analysis Report
   : Solarwinds and Malware

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[Tech Note]

1 Cyber Squatting

Security Operation Center
Security Analysis Team

01. Overview

In the post-covid era, many changes have occurred in society. In companies, the work environment changes from the 'face-to-face' method of performing tasks represented by the existing office to the ‘non-face-to-face' method, while in the financial industry, the deposit amount through the non-face-to-face channel is 40% a year. In addition, the number of Internet banking and mobile banking transfers has increased by 10% compared to the previous year, and non-face-to-face transactions are rapidly increasing.

It's not just this. Due to the long-lasting social distancing, the 'online environment' without time and space limitations is rapidly becoming active. The consumption pattern of middle-aged people who mainly consume offline has begun to change with online shopping, and the number of views of Home training videos exercising at home is steadily increasing. In addition, singers hold online concerts, and ‘online environment' has become deeply established in our daily lives.

However, as the online market expands, various attack surfaces are exposed to more attackers, and cyber threats are expected to increase accordingly. In addition, social engineering attacks that exploit human error or carelessness are increasing, rather than hacking using vulnerabilities in hardware or software, and online users are concerned about damage.

A representative social engineering attack is a 'phishing' attack. The main purpose of phishing is to steal personal or corporate important information (personal information, credit information, etc.) or monetary gain by disguised as deceptive content or content that may be mistaken as real through phone, text, e-mail, or fake sites. , To perform attacks such as system paralysis. Phishing attacks are classified into general phishing and spear-phishing depending on the attack target, and according to attack techniques, squatting, watering holes, email spoofing (phishing mail), voice phishing.

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

[Tech Note]

1 Cyber Squatting

▶ Various phishing attacks

Compared to general phishing attacks against an unspecified number of people, spear phishing is performed after collecting information about the target of attack in advance, such as employees of a specific company (organization) and users visiting a specific site. The biggest difference from general phishing is that it focuses on corporate internal documents and system paralysis rather than simply stealing personal information, and is used as a precursor before committing it.

Classification	Attack Target	Features
General Phishing	Unspecified	• Performing attacks through social issues that users may be dazzling • Use for the purpose of stealing important personal information (personal information, credit informati on), financial fraud, etc.
Spear-Phishing	Specified	• Performing an attack after collecting information on the target • It is widely used as a precursor to APT attacks such as corporate internal documents and system paralysis.
Whaling	Celebrities (CEO, Politician, etc.)	• Kind of spear phishing • Attacks against government officials or senior executives within a company

[Table 4-1] Features of attack characteristics according to the attack target

Phishing has a wide variety of attack methods, such as △ attack through the web, △ attack through email, and △ attack through phone or text. In this issue, we are going to look into 'Cyber Squatting', which uses an address similar to an actual domain address to perform secondary attacks such as credential stuffing and malicious code distribution.

Attack Path	Attack Type	Description
Web	Squatting	• Using domain addresses similar to normal domain addresses to trick users
	Watering-hole	• After collecting sites history frequently visited by t argets, malicious scripts are inserted into the site t o perform malicious actions when the targets revi sit the site.
Email	Email spoofing (Phishing mail)	• Disguises the email sender information to trick the recipient as if it was sent by someone other than an attacker, such as a colleague or business partner.
	Replica phishing	• Deception of recipients as if they were normal mail by making the contents of normal mail sent in the past similar
Voice/Text	Voice phishing	• Deceive users via phone or voice message
	Smishing	• Deceive users via text message

[Table 4-2] Phishing attack description

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[Tech Note]

1 Cyber Squatting

02. What is the Cyber squatting?

Cybersquatting is a compound word of 'Cyber' and 'Squat(to settle without permission, to occupy illegally)'. It refers to the act of registering an Internet address (domain) prior to the legitimate owner with the name, product name, or characteristic of a famous company or organization for the purpose of 'financial gain (sale)'.

In the United States, there is a case where "www.wallstreet.com," which an individual registered for $70 in 1994, was sold for $1 million in 1999.

Cases	Description
wallstreet.com	the domain "www.wallstreet.com" registered for $70 by an individual was traded for $1 million.
McDonalds.com	Renowned franchise McDonald's donated about $35,000 to a public school to obtain a domain in the name of a company.

[Table 4-3] Cases of Cyber Squatting

Originally, cybersquatting was a speculative act in which a domain of a company's representative name or trademark was unauthorized and then sold back to a company to gain financial gain. It is used as a means of malicious actions such as hijacking.

Moreover, as the public's activities have been reduced due to the recent increase in social distancing in the aftermath of the COVID-19, the amount of Internet usage increased by about 33.8% compared to the previous year, and the damage caused by cybersquatting continued.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[Tech Note]

1 Cyber Squatting

These cybersquatting can be divided as follows.

1. **'Typo-Squatting' which a user's misspelling causes them to access a fake domain**
2. **'Combo-Squatting' that tricks users who access fake domains by using similar words that are often confusing or representative of a company.**

1) Typo-Squatting

Typo-squatting refers to connecting to a fake domain due to a user input mistake (typo) such as missing some letters or changing the order of the actual domain. Attackers register fake domains based on 'String', which is a common mistake by users, and then attack users who access the domain as secondary attacks such as credential stuffing and malicious code distribution.

For example, if the target to be disguised is 'igloosec.com', typos that users can commonly cause are as follows, and all of them can be fake domains.

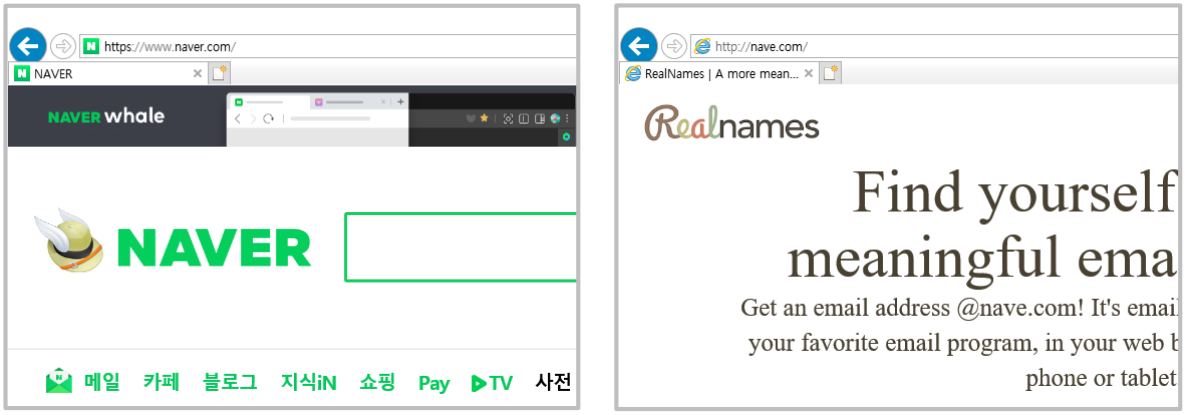
- igloo-sec.com
- igloo**es**c.com
- **e**gloosec.com
- gloosec.com

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[Tech Note]

1 Cyber Squatting

The figure below is the representative Korean portal site, Naver (www.naver.com) and a similar domain (nave.com).



[Figure 4-1]Naver (www.naver.com) / Nave(nave.com)

※ Similar domains are only examples and may be domains that are actually serviced normally

2) Combo-Squatting

Combo squatting refers to creating a fake domain that the user might be mistaken for, such as replacing it with a word very similar to the real domain or another higher domain (.com, .co.kr, .org, etc.) to disguise it as a real domain.

For example, if the target to be disguised is 'igloosec.com', fake domains that may confuse users are as follows.

- igloosecurity.com
- igloo-TM.com
- igloosec.co.kr

The following are the actual Korea Internet & Security Agency (www.kisa.or.kr) domains and similar domains (www.kisa.co.kr, kisa.com).

[Figure 4-2] KISA(www.kisa.or.kr) / KISA similar domain 1(www.kisa.co.kr), 2(kisa.com)

※ Similar domains are only examples and may be domains that are actually serviced normally

Copyright © IGLOO Security, Inc. 2021. All rights reserved

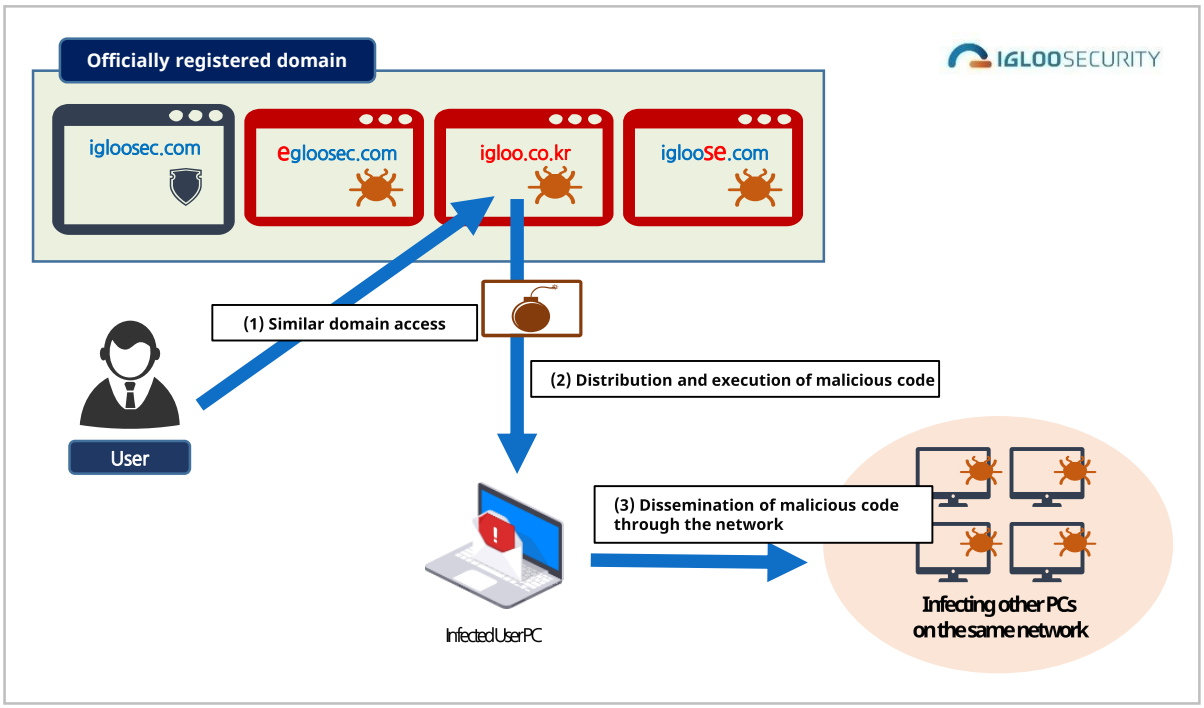
[Tech Note]

1 Cyber Squatting

03. Cyber Squatting Attack Scenario

The attack scenario of cyber squatting is as follows.

1. The attacker registers a domain similar to the real domain with the domain registrar and creates a phishing site with content that the user might mistake as the real domain.
2. A user connects to a fake domain created by an attacker due to a typing mistake or confusion with the upper domain (.com, co.kr, .org, etc.), and the malicious code is automatically downloaded.
3. The downloaded malicious code is executed on the user's PC and infects all the user's PCs in the same network.



[Figure 4-3] Expected Cyber Squatting Scenario

The above scenario is the simplest example, and let's assume that a user has been attacked by cybersquatting in the corporate network. At a small level, it seems that personal PCs are infected with malicious code, but this small ember can lead to leakage of confidential documents in the company or service paralysis due to malicious code infection of the server, and all systems in the enterprise are infected with ransomware, etc.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[Tech Note]

1 Cyber Squatting

04. Difficulty in detecting/recognizing attack damage

Looking at the cybersquatting attack process, it is so simple and ridiculous that the question arises, 'Can the attack be successful?' However, according to Palo Alto Networks, there are an average of 450 squat domains registered every day, many of which are found to be used to distribute malicious code.

There are three reasons why cybersquatting attacks, which cause more attacks and damage than expected, are inevitable and difficult to prevent.

1) Fake domain (officially registered)

Most of the fake domains registered by the attacker without permission are domains registered through ‘official domain registrars'. Anyone can easily apply for domain registration, and it is also a problem that the standards for domain registration are not strict.

2) HTTPS communication

Sites created by attackers (similar domains), not actual corporate sites, use HTTPS communication, known as a secure encryption network protocol, so it is difficult for general users to easily determine whether they are normal or malicious sites. When visiting a site using the HTTP protocol, a security warning appears in the browser address bar, saying 'This site does not use a secure connection (HTTPS)', whereas in the case of HTTPS, a secure connection is used with a 'lock' shape. It is a problem that the user's suspicion is somewhat relieved as the phrase appears.

3) When malicious behavior is not detected

Most security equipment analyzes the pattern of an attack and detects an attack using a signature-based method for the attack and an behavior-based method that detects when an activity different from the normal behavior occurs. Therefore, if there is malicious activity on the site created by the attacker (site accessed through a similar domain), it is possible to respond appropriately with security equipment such as blocking access, but simply requesting account information to steal personal information or purchase false goods. In the case of a domain that induces a security device, it is difficult to distinguish between a normal behavior and a malicious behavior.

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

[Tech Note]

1 Cyber Squatting

05. Countermeasures

For company

First of all, companies can prevent the damage of an attack by registering a similar domain before an attacker by listing a list of typos that can occur when a user enters their domain address and a string that can be easily mistaken by the user.

In addition, the security officer should periodically check whether a domain similar to the company's own domain exists, and if malicious behavior is detected in a similar domain, notify the service users in advance so that damage does not occur, such as posting the content on the homepage.

Also, even if there is no malicious activity, if an illegal activity using an image or trademark of a company that users may confuse is detected, a response is required, such as requesting dispute mediation with the Internet Address Dispute Mediation Committee and canceling similar domains.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[Tech Note]

1 Cyber Squatting

06. Conclusion

Currently, as the digital economy is revitalized by COVID-19, the digital transformation is accelerating. As a result, cybercrime is expected to increase rapidly, and social engineering attacks such as phishing attacks are also expected to increase. Moreover, as the rate of telecommuting increases, phishing emails targeting employees are still on the rise, so companies and users are encouraged to read the following security rules to prevent accidents.

Company	User
✓ Hardening security device detection policy	✓ Do not click suspicious mail, attachment and link
✓ Monitoring	✓ Financial transaction should be double checked
✓ Account MGMT. at least once per quarter	✓ Genuine software
✓ Illegal SW check at least once per half-year	✓ Periodical back-up
✓ Security training for employees	✓ Activate EDR or AV
✓ Malicious mail mock training	✓ Keep maintain the latest version of OS and other S/W
✓ Management care	

07. Reference

[1] Non-face-to-face transactions increase 40% in one year..."Now is the Golden Time for Digital Innovation“
https://www.sedaily.com/NewsVIew/1Z46CMLRXJ
[2] Financial Services Commission, Financial Glossary'Cyber Quoting’
https://www.fsc.go.kr/know/wrd_list.jsp?menu=7420000&bbsid=BBS0026&sword=&s=7&e=8&page=18
[3] Internet Address Dispute Resolution Committee, 2016 Domain Name Dispute White Paper.pdf
[4] Card news to prevent damage such as cyber fraud
https://spam.kisa.or.kr/customer/sub2_R.do?boardNo=1021
[5] Google safe browsing
https://transparencyreport.google.com/safe-browsing/overview

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

[IGLOO Analysis Report]

2 Solarwinds and Malware

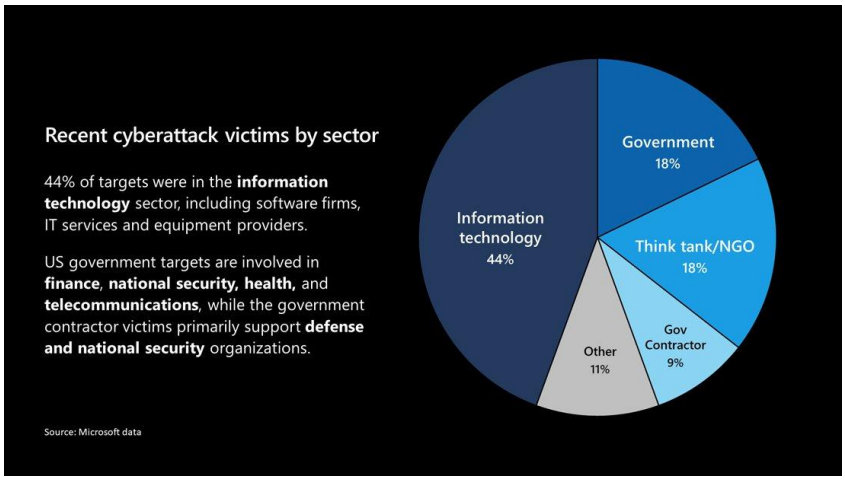
Security Operation Center
Security Analysis Team

01. Overview

On December 13, 2020, through CISA, it was revealed to the world that the supply chain of SolarWinds Orion products, a network management solution, was attacked by unidentified hackers, and some versions of the product were used as backdoors. SolarWinds Orion is used by more than 400 of the Fortune 500 companies and 33,000 of SolarWinds' 300,000 customers. Attackers attacked by targeting places that could steal information with high attack value among companies infected with malicious code. The percentage of damage disclosed by Microsoft is △IT-related fields (44%), △Government agencies (18%), △Think tanks and NGOs (18%), △Government contractors (9%), △Others (11%). The U.S. government agencies attacked include the U.S. Department of Defense, U.S. Department of Homeland Security, U.S. National Institutes of Health, U.S. Treasury and U.S. Department of Commerce.

According to the results of the investigation so far, SUNSPOT and SUNBURST (Solorigate) malware was used in the SolarWinds supply chain attack. FireEye names the group behind the attack as UNC2452, and Volexity as Dark Halo, and four US security agencies pointed to Russia as the country behind the attack. Kaspersky said that the SUNBURST malware is similar to the backdoor KAZUAR used by the Russian APT group Turla.

In this report, we would like to investigate the solarwinds supply chain hacking incident and the SUNBURST malware used in the attack.



[Figure 5-1] Solarwinds Orion Supply Chain Attack Damage Ratio (Source: Microsoft)

Copyright © IGLOO Security, Inc. 2021. All rights reserved

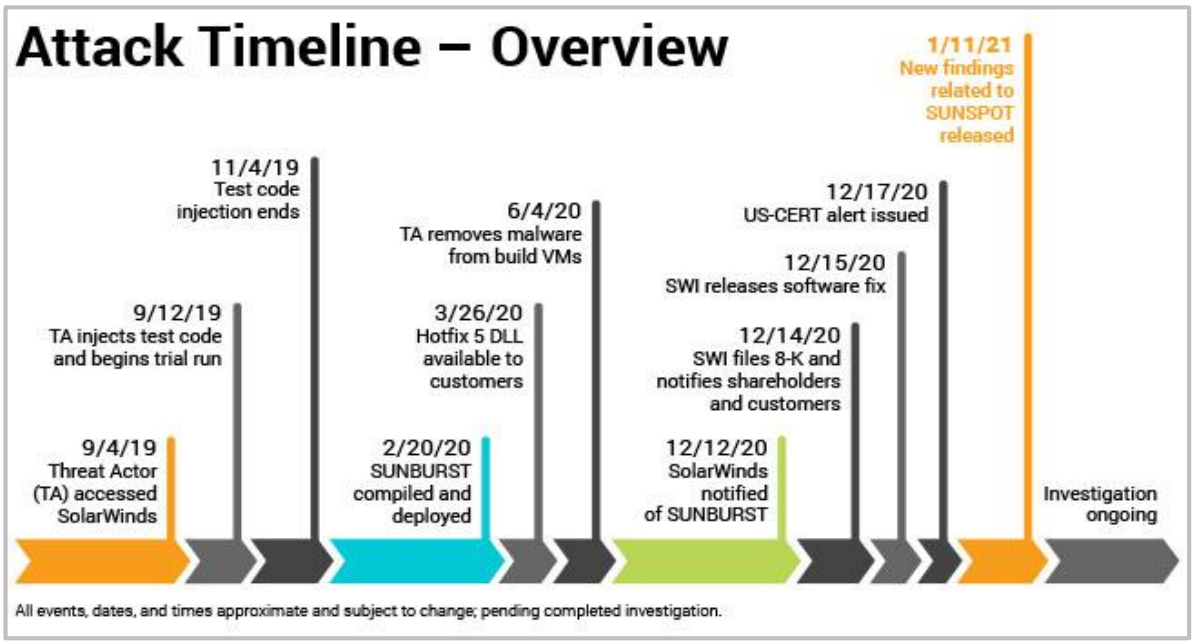
[IGLOO Analysis Report]

2 Solarwinds and Malware

02. Attack

1) Solarwinds and Supply Attack

Supply chain attack refers to an attack in which a hacker infiltrates a company's development environment and creates a problem. In supply chain attacks, the malicious code altered in the development/distribution stage is distributed to the normal update server of the software company, so the user cannot easily recognize that the updated file is a file altered by an attacker. Therefore, when an attack occurs, the user's point of view is inevitable, and the company's point of view continues to distribute malicious code until the attack has occurred. Due to the nature of these supply chain attacks, the damage is inevitably large, and the frequency of supply chain attacks by attackers has increased since several years ago. Hackers who attacked the SolarWinds supply chain also aimed at the nature of this supply chain attack. Attacks that began in September 2019 were not revealed until January 2021.



[Figure 5-2] SolarWinds Supply Chain Attack Timeline (Source: SolarWinds orangematter)

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[IGLOO Analysis Report]

2 Solarwinds and Malware

2) Affected target

Targets affected by malicious code are shown in [Table 5-1]. All versions prior to 2019.4.HF 4 are not affected by SUNBURST, but all SUPERNOVA using the vulnerability (CVE-2020-10148) are affected.

SUPERNOVA

SUPERNOVA is a malicious code discovered during the investigation of the SolarWinds supply chain attack incident, and **Microsoft sees it as the act of an attack group other than the group that attacked the supply chain**. SUPERNOVA uses the zero-day vulnerability to install malicious code. The installed malicious code is a web shell developed with .NET, and is a backdoor targeting a web server.

No.	Affected Orion Platform version	SUNBURST	SUPERNOVA	Latest version
1	2020.2.4	X	X	Latest version
2	2020.2.1HF2	X	X	2020.2.4
3	2020.2.1 HF 1	X	O	
4	2020.2.1	X	O	
5	2020.2 HF 1	O	O	
6	2020.2	O	O	
7	2019.4.2	X	X	Latest version
8	2019.4 HF 6	X	O	2020.2.4 or 2019.4.2
9	2019.4 HF5	O	O	
10	2019.4 HF 4	X	O	

[Table 5-1] Affected Orion Platform Version (Source: Solarwinds)

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[IGLOO Analysis Report]

2 Solarwinds and Malware

03. Malware used in attack

1) SUNSPOT

According to CrowdStrike's analysis, the attackers used the main malware SUNBURST backdoor in the supply chain with a malicious code called SUNSPOT. The malware was named “taskhostsvc.exe” and ran on the software build server of Solarwinds Orion. SUNSPOT checks whether MsBuild.exe, which is used for building among Microsoft Visual Studio development tools, is currently building Orion software. When it was confirmed that the build was in progress, SUNSPOT hijacked the build operation to add the SUNBURST backdoor code to the Solarwinds Orion software, and added the backdoor code to check whether an error occurred during build. Until now, the IOC of the sample has been disclosed, but since the sample has not been disclosed, direct analysis was not possible.

2) SUNBURST

It is a backdoor malware included in Solarwinds Orion software modulated by SUNSPOT. FireEye's name is SUNBURST, and Microsoft's name is Solorigate. SUNSPOT steals the victim's information through actions such as △ domain name change using DGA (Domain Generation Algorithms), △ check security product related services and check whether reversing and forensic tools are running, △ C2 communication, etc. The attack was conducted using additional malicious code (TEARDROP). In this report, an analysis was conducted on SUNBURST, in which the sample was released.

3) TEARDROP

It is a malicious code that is dropped when certain conditions are satisfied in SUNBURST. It acts as a loader to load Cobalt Strike Beacon on the infected user's PC.

Copyright ⓒ IGLOO Security, Inc. 2021. All rights reserved

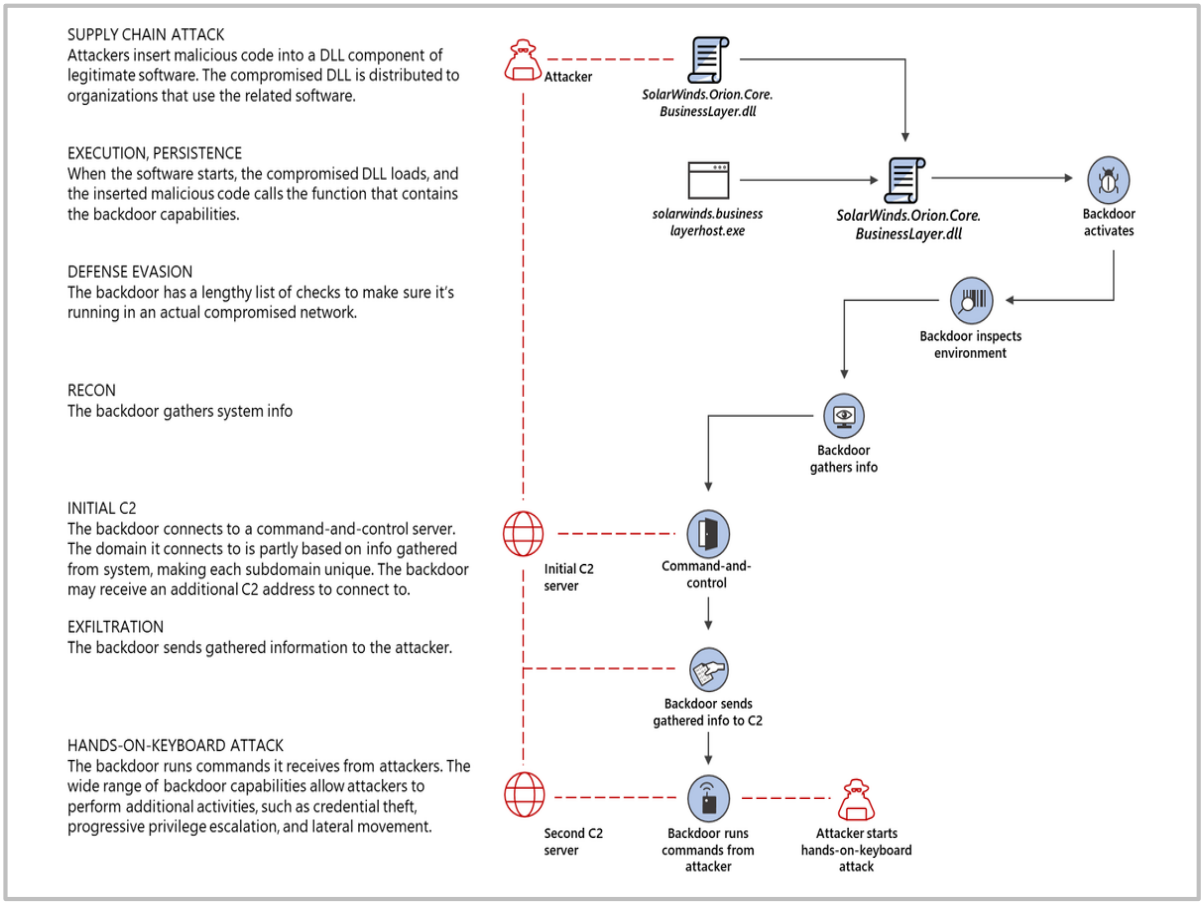
[IGLOO Analysis Report]

2 Solarwinds and Malware

04. SUNBURST

1) Overview

The SUNBURST backdoor spread by the supply chain attack uses the SolarWinds.Orion.Core.BusinessLayer.dll file. Installation is executed through a modified SolarWinds Installer Patch (*.msp) file. After installation, it is loaded by the normal SolarWinds.BusinessLayerHost.exe (or x64), and malicious behavior proceeds.



[Figure 5-3] SUNBURST infection route (Source: Microsoft)

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[IGLOO Analysis Report]

2 Solarwinds and Malware

2) Analysis file information

The samples used in the analysis analyzed in this report were adopted by the malicious code IoC released by FireEye.

No.	File name	MD5
1	CORE-2019.4.5220.20574-SolarWinds-Core-v2019.4.5220-Hotfix5.msp	02af7cec58b9a5da1c542b5a32151ba1
2	Solarwinds Worldwide, LLC	08e35543d6110ed11fdf558bb093d401
3	SolarWinds.Orion.Core.BusinessLayer.dll	2c4a910a1299cdae2a4e55988a2f102e
4	SolarWinds.Orion.Core.BusinessLayer.dll	846e27a652a5e1bfbd0ddd38a16dc865
5	**SolarWinds.Orion.Core.BusinessLayer.dll**	**b91ce2fa41029f6955bff20079468448**
6	OrionImprovementBusinessLayer.2.cs	4f2eb62fa529c0283b28d05ddd311fae
7	app_web_logoimagehandler.ashx.b6031896.dll	56ceb6d0011d87b6e4d7023d7ef85676

[Table 5-2] IoC information of malicious code disclosed by FireEye

No.	Classification	Description
1	File name	SolarWinds.Orion.Core.BusinessLayer.dll
2	MD5	b91ce2fa41029f6955bff20079468448
3	File size	987.34 KB
4	File type	Win32 DLL(.NET)
5	AV detection	53/63 (AV detection : Virustotal 2021/01/11 Standard(UTC))
6	Version	2019.4.5200.9083
7	Compile Time	2020-03-24 08:52:34 (UTC)
8	Signing Time	2020-03-24 08:53:43 (UTC)

[Table 5-3] Analysis file information

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[IGLOO Analysis Report]

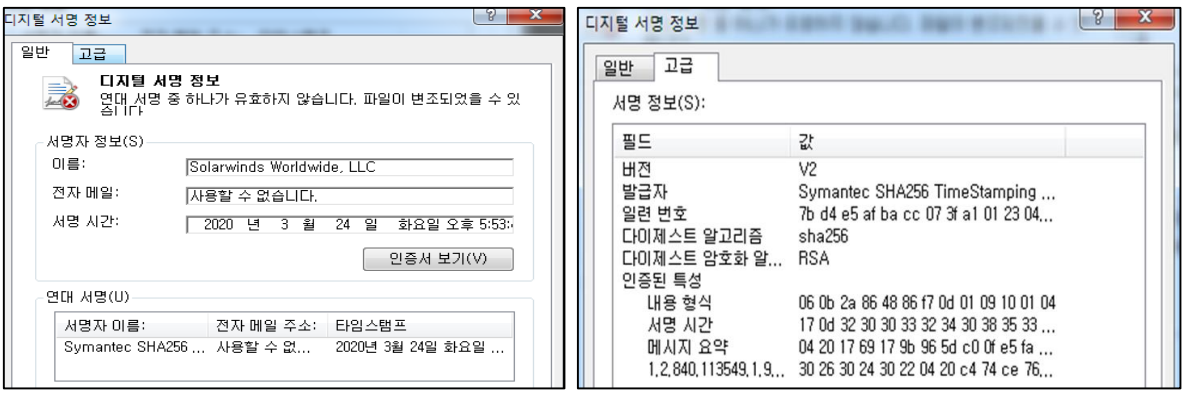
2 Solarwinds and Malware

3) Detailed Analysis

The SolarWinds.Orion.Core.BusinessLayer.dll file is authenticated with a digital signature with a serial number as shown in [Table 5-4], so it is difficult for users to suspect that it is a malicious code.

No.	Classification	Contents
1	Serial Number	0f:e9:73:75:20:22:a6:06:ad:f2:a3:6e:34:5d:c0:ed

[Table 5-4] Certificate serial number



[Figure 5-4] Certificate details

The main malicious behavior is the altered SolarWinds.Orion.Core. It operates through the internal thread of the RefreshInternal method of the BusinessLayer.dll file. The following try/catch statement does not exist in the normal SolarWinds.Orion.Core.BusinessLayer.dll file.

```
internal void RefreshInternal()
{
    if (InventoryManager.log.IsDebugEnabled)
    {
        InventoryManager.log.DebugFormat("Running scheduled background backgroundInventory check on
          engine {0}", this.engineID);
    }
    try
    {
        if (!OrionImprovementBusinessLayer.IsAlive)
        {
            new Thread(new ThreadStart(OrionImprovementBusinessLayer.Initialize))
            {
                IsBackground = true
            }.Start();
        }
    }
    catch (Exception)
    {
    }
    if (this.backgroundInventory.IsRunning)
    {
        InventoryManager.log.Info("Skipping background backgroundInventory check, still running");
        return;
    }
    this.QueueInventoryTasksFromNodeSettings();
    this.QueueInventoryTasksFromInventorySettings();
    if (this.backgroundInventory.QueueSize > 0)
    {
        this.backgroundInventory.Start();
    }
}
```

[Figure 5-5] Inside the modulated RefreshInternal method

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[IGLOO Analysis Report]

2 Solarwinds and Malware

Check whether the name of the currently running parent process is solarwinds.businesslayerhost using the hash value.

```
if (OrionImprovementBusinessLayer.GetHash(Process.GetCurrentProcess().ProcessName.ToLower()) == 17291806236368054941uL)
{
```

[Figure 5-6] Process name check with hash value

The **file/process/service name** used inside the SUNBURST malicious code uses the value obtained by XORing 6605813339339102567 to the hash value calculated by 64bit FNV-1A.

```
// Token: 0x06000057 RID: 87 RVA: 0x00004E7C File Offset: 0x0000307C
private static ulong GetHash(string s)
{
    ulong num = 14695981039346656037UL; 64bit FNV-1A 기본 값
    try
    {
        foreach (byte b in Encoding.UTF8.GetBytes(s))
        {
            num ^= (ulong)b;
            num *= 1099511628211UL;
        }
    }
    catch
    {
    }
    return num ^ 6605813339339102567UL;
}
```

```
Svc = new OrionImprovementBusinessLayer.ServiceConfiguration.Service[]
{
    new OrionImprovementBusinessLayer.ServiceConfiguration.Service
    {
        timeStamp = 1138527537889190660 8UL, // carbonblack
        DefaultValue = 2u
    },
    new OrionImprovementBusinessLayer.ServiceConfiguration.Service
    {
        timeStamp = 1369352587656082728 3UL, // carbonblackk
        DefaultValue = 1u
    },
```

18 1138527537889190660 8:carbonblack

48 1369352587656082728 3:carbonblackk

[Figure 5-7] Function to create a left-hash value / Inside a function that uses a right-hash value

Check the last modified date of the currently running DLL file. Make sure that the last modified date is 12-14 days before.

```
DateTime lastWriteTime = File.GetLastWriteTime(Assembly.GetExecutingAssembly().Location);
// GetLastWriteTime ::파일이 마지막으로 수정된 날짜와 시간 반환
// Assembly.GetExecutingAssembly().Location : 현재 실행되고있는 경로
// 현재 실행중인 파일이 마지막으로 수정된 날짜
int num = new Random().Next(288, 336);
//288 ~ 335중의 난수 발생
if (DateTime.Now.CompareTo(lastWriteTime.AddHours((double)num)) >= 0)
    //12일 ~ 14일 전에 생성된 파일인지 확인
```

[Figure 5-8] Routine to check the modified date

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[IGLOO Analysis Report]

2 Solarwinds and Malware

Set the current status value of the malicious code being executed. When first executed, the value of new(4) is set for the malicious code. After that, the values of Truncate and Append are set according to the condition of the action.

```
// Token: 0x0600096F RID: 2415 RVA: 0x00043154 File Offset: 0x00041354
public static bool ReadReportStatus(out OrionImprovementBusinessLayer.ReportStatus status)
{
    try
    {
        string s;
        int num;
        if (OrionImprovementBusinessLayer.ConfigManager.ReadConfig(OrionImprovementBusinessLayer.
        reportStatusName, out s) && int.TryParse(s, out num))
        {
            switch (num)
            {
            case 3:
                status = OrionImprovementBusinessLayer.ReportStatus.Truncate;
                return true;
            case 4:
                status = OrionImprovementBusinessLayer.ReportStatus.New;
                return true;
            case 5:
                status = OrionImprovementBusinessLayer.ReportStatus.Append;
                return true;
            }
        }
    }
    catch (ConfigurationErrorsException)
    {
    }
    status = OrionImprovementBusinessLayer.ReportStatus.New;
    return false;
}
```

[Figure 5-9] Setting the current status value of the malicious code being executed

Check the domain name on the PC where the malicious code is running. If a domain name exists, check whether the domain name corresponds to the name included in the following [Table 5-5]. If the infected target cannot bring the domain name or has the domain name included in [Table 5-5], the malicious code is terminated.

```
OrionImprovementBusinessLayer.domain4 = IPGlobalProperties.GetIPGlobalProperties().DomainName;
if (!string.IsNullOrEmpty(OrionImprovementBusinessLayer.domain4) && !OrionImprovementBusinessLayer.
IsNullOrInvalidName(OrionImprovementBusinessLayer.domain4))
{
```

[Figure 5-10] Routine to check domain name

Domain name (13 counts)				
swdev.local	swdev.dmz	lab.local	lab.na	emea.sales
cork.lab	dev.local	dmz.local	pci.local	saas.swi
lab.rio	lab.brno	apac.lab	-	-

[Table 5-5] Domain name verified by malicious code

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[IGLOO Analysis Report]

2 Solarwinds and Malware

The malicious code checks drive files, services, and currently running processes to check the security programs installed in the user's PC. Eight security products are checked, and if the services in [Table 5-6] are running, modify the registry and change it to [Disabled].

Security products to check (8 counts)			
Windows Defender	Windows Defender Advanced Threat Protection	Microsoft Defender for Identity	carbonblack
CrowdStrike	FireEye	ESET	f-secure

[Table 5-6] Types of security products identified in malicious code

Process/Service Name (59 counts)					
carbonblack	csfalconservice	epfw	fe_avk	fsdevcon	fsni
carbonblackk	eamonm	epfwwfp	feelam	fsdfw	fsorsp
cavp	eelam	f-secure filter	fekern	fses	fsorspclient
cb	egui	f-secure gatekeeper	fewscservice	fsfw	fssm32
cbcomms	eguiproxy	f-secure gatekeeper handler starter	fnrb32	fsgk32	fsvista
cbstream	ehdrv	f-secure hips	fsaua	fsgk32st	fswebuid
csagent	ekbdflt	f-secure network request broker	fsaus	fsma	microsoft.tri.sensor
csdevicecontrol	ekrn	f-secure recognizer	fsav32	fsma32	microsoft.tri.sensor.updater
csfalconcontainer	ekrnepfw	f-secure webui daemon	fsbts	fsms	msmpeng
sense	windefend	mssense	xagt	xagtnotif	

[Table 5-7] Process/service name identified in malicious code

Check if the tool used for malicious code analysis/forensics, etc. is running on the user's PC. At this time, there are 136 tools to check, and it seems that a lot of effort has been put into preventing malicious code from being analyzed/detected. Among the 136 tools to be checked, various tools such as IDA, ollydbg, x32/64dbg, dnspy, peid, peview, tcpview, tcpdump, and procmon, which are widely used for malicious code analysis, were identified.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[IGLOO Analysis Report]

2 Solarwinds and Malware

The malicious code goes through an intermediate server to connect to the final C2. This intermediate stage server is a server with authority for the avsvmcloud[.]com domain, and in the update method of the malicious code, a sub-domain is created using DGA (Domain Generation Algorithms) for communication with the intermediate stage server. Subdomains are created according to the rules in [Table 5-8]. userId, domain2, domain3, and domain1 refer to the variable names used in the malicious code, and in the case of [domain3], one of the four values is used randomly.

userId	domain2	Domain3 (Random 1)	domain1
Infected PC information	appsync-api	• eu-west-1 • eu-west-2 • us-east-1 • us-east-2	avsvmcloud[.]com

[Table 5-8] Values used for C2 domain creation

[userId] is created by collecting △ physical address, △ domain name, and △ Hardware ID of the infected PC. It is encoded using a routine inside the malicious code, and this information can be decoded to identify the domain infected with the malicious code.

※ Decoder : https://github.com/RedDrip7/SunBurst_DGA_Decode/blob/main/decode.py

```
private static bool GetOrCreateUserID(out byte[] hash64)
{
    string text = OrionImprovementBusinessLayer.ReadDeviceInfo(); //PhysicalAddress
    hash64 = new byte[8];
    Array.Clear(hash64, 0, hash64.Length);
    if (text == null)
    {
        return false;
    }
    text += OrionImprovementBusinessLayer.domain4;
    try
    {
        text += OrionImprovementBusinessLayer.RegistryHelper.GetValue(OrionImprovementBusinessLayer.ZipHelper.Unzip(
        "8/B2jYz38Xd29In3dXT28PRzjQn2dwsJdwxyjfHNTC7KL85PK4lxLqosKMlPL0osyKgEAA=="),
        //HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography
        OrionImprovementBusinessLayer.ZipHelper.Unzip("801MzsjMS3UvzUwBAA=="), "");
        //MachineGuid
    }
```

[Figure 5-11] Inside the function that creates the [userId] value

intermediate Server

FireEye is represented by C2 Coordinator Protocol, and PREVASIO is represented by authoritative DNS server. In this report, it is arbitrarily named as an intermediate server.

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[IGLOO Analysis Report]

2 Solarwinds and Malware

A Record / CNAME Record

- In SUNBURST, it communicates with the C&C server by sending an encoded DNS request. Depending on the transmitted request, the attacker can send a DNS response to A Record or CNAME Record.

During communication, the subsequent actions differ depending on the response of the intermediate server (A Record, CNAME Record). When responding with A Record, check if the IP is included in [Table 5-9]. After checking, switch to the mode suitable for each address family. The disclosed kill switch uses an action that terminates when the IP of the malicious code belongs to Address Family Atm or ImpLink.

No.	IP/Subnet Mask	Address Family	No.	IP/Subnet Mask	Address Family
1	10.0.0.0/255.0.0.0	Atm	12	20.140.0.0/255.254.0.0	ImpLink
2	172.16.0.0/255.240.0.0		13	96.31.172.0/255.255.255.0	
3	192.168.0.0/255.255.0.0		14	131.228.12.0/255.255.252.0	
4	224.0.0.0/240.0.0.0		15	144.86.226.0/255.255.255.0	
5	fc00::/fe00::		16	8.18.144.0/255.255.254.0	NetBios
6	fec0::/ffc0::		17	18.130.0.0/255.255.0.0	
7	ff00::/ff00::		18	71.152.53.0/255.255.255.0	
8	41.84.159.0/255.255.255.0	Ipx	19	99.79.0.0/255.255.0.0	
9	74.114.24.0/255.255.248.0		20	87.238.80.0/255.255.248.0	
10	154.118.140.0/255.255.255.0		21	199.201.117.0/255.255.255.0	
11	217.163.7.0/255.255.255.0		22	184.72.0.0/255.254.0.0	

[Table 5-9] The function that creates [userId] value

When the intermediate stage server responds with CNAME Record, it additionally communicates with HTTP(S)-based C2. Using the command code value received through HTTP(S) C2 communication, various functions inside the JobEngine method are used.

Command				
Idle	Exit	SetTime	CollectSystem Description	UploadSystem Description
RunTask	GetProcessBy Description	KillTask	GetFileSystem Entries	WriteFile
FileExists	DeleteFile	GetFileHash	ReadRegistryValue	SetRegistryValue
DeleteRegistryValue	GetRegistrySubKeyA ndValueNames	Reboot	-	-

[Table 5-10] Command in JobEngine method

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[IGLOO Analysis Report]

2 Solarwinds and Malware

05. MITRE ATT&CK

▶ MITRE ATT&CK for Enterprise(v8.1)

The MITER ATT&CK Techniques for SolarWinds supply chain attack and SUNBURST were disclosed through various media. Among them, only the parts analyzed in this report were summarized separately.

Enterprise tactics	NAME (ID)	Description
Persistence	Create or Modify System Process: Windows Service (T1543.003)	• After searching the service/process for 8 security products, if the service is in operation, the flag is changed to [No operation].
Privilege Escalation	Create or Modify System Process: Windows Service (T1543.003)	• After searching the service/process for 8 security products, if the service is in operation, the flag is changed to [No operation].
Defense Evasion	Obfuscated Files or Information (T1027)	• Malware internal string is compressed/encoded with Deflate + base64 • The names of files, processes, services, etc. used internally use XOR operation value for 64bit FNV-1A hash value.
	Subvert Trust Controls: Code Signing (T1553.002)	• Digital Signature
Discovery	Software Discovery (T1518)	• Search for currently running analysis tools (136 counts)
	Software Discovery :Security Software Discovery (T1518.001)	• Search services/processes for 8 security products (59 counts)
Command and Control	Application Layer Protocol: Web Protocols (T1071.001)	• Additional act using command code value received through C2 communication
	Application Layer Protocol: DNS (T1071.004)	• Different actions using the values received as A Record and CNAME
	Dynamic Resolution: Domain Generation Algorithms (T1568.002)	• Domain creation using DGA algorithm

[Table 5-11] MITER ATT&CK

Copyright © IGLOO Security, Inc. 2021. All rights reserved

[IGLOO Analysis Report]

2 Solarwinds and Malware

06. Reference

[1]https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
[2]https://www.mcafee.com/blogs/other-blogs/mcafee-labs/additional-analysis-into-the-sunburst-backdoor/
[3]https://www.microsoft.com/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/
[4]https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
[5]https://www.picussecurity.com/resource/blog/ttps-used-in-the-solarwinds-breach
[6]https://blog.prevasio.com/2020/12/dns-tunneling-in-solarwinds-supply.html
[7]https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
[8] https://securelist.com/sunburst-connecting-the-dots-in-the-dns-requests/99862/

Copyright © IGLOO Security, Inc. 2021. All rights reserved

Cover Story

CHAPTER 6

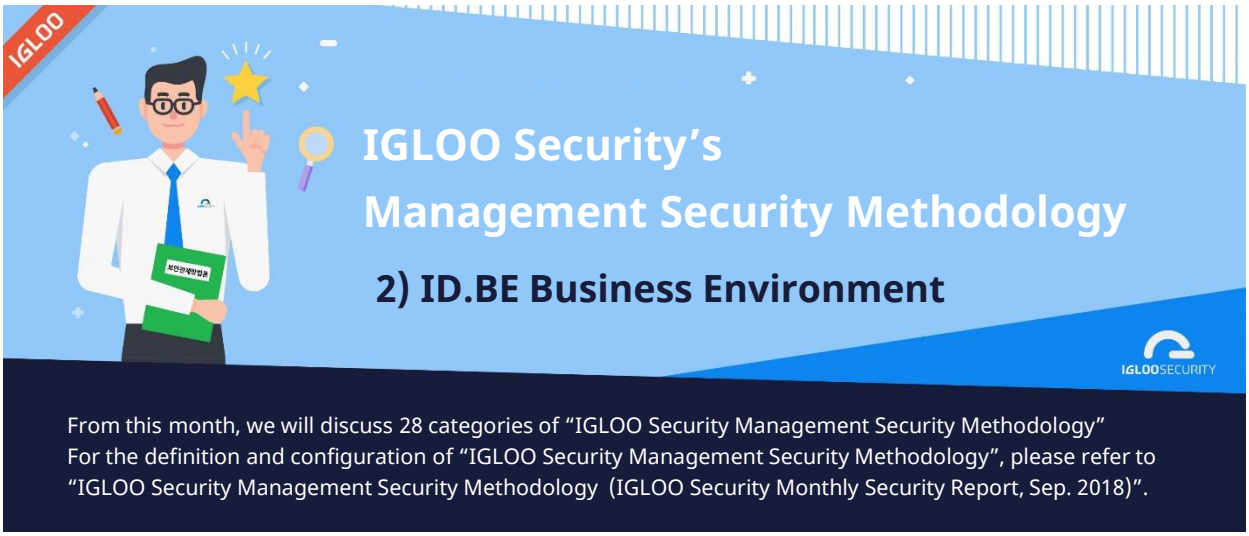
Focus On IGLOO

1. IGLOO Security's
   Management Security Methodology
   2) ID.BE Business Environment

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 IGLOO Security's Management Security Methodology
2) ID.BE Business Environment

Strategic Business Department
Strategic Planning Team



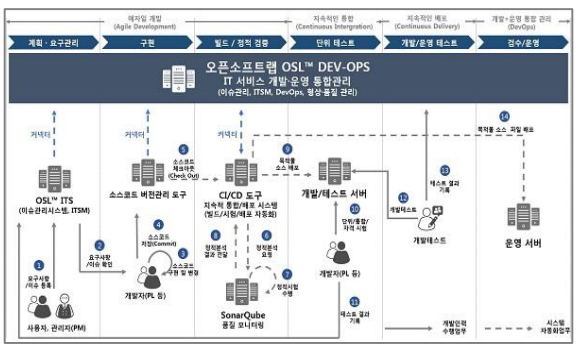
From this month, we will discuss 28 categories of "IGLOO Security Management Security Methodology"
For the definition and configuration of "IGLOO Security Management Security Methodology", please refer to "IGLOO Security Management Security Methodology (IGLOO Security Monthly Security Report, Sep. 2018)".

01. Category : ID.BE Business Environment

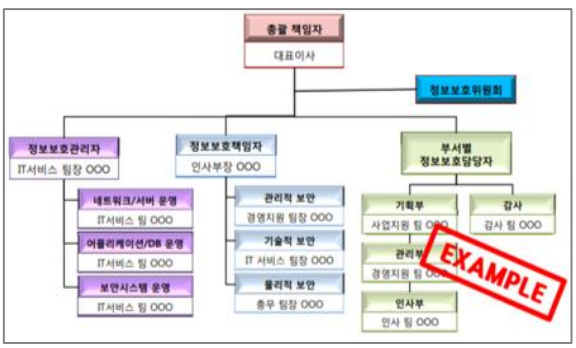
Identify > ID.BE (Business Environment)
: Defining & Prioritizing the task purpose, employees and work scope of SOC. Based on this, the roles and responsibilities of cybersecurity are defined and risk management is performed.

The first function of "IGLOO Security Management Security Methodology" is "Identify" and the second category is "Business Environment (ID.BE, Business Environment)".

Business environment is an extension of the asset management (ID.AM, Asset Management) introduced in January. Security monitoring/control begins with understanding the relationship between the asset to be controlled. Each asset has a person in charge, and most of them are organically integrated to other systems through the network to perform services, so understanding their composition and relationship can accurately define the area of security control. For this, not only the network configuration to be monitored, but also the service configuration diagram is required, and an organization capable of grasping the connection relationship between the organizations managing the controlled system is also required.



[Figure 6-1] Example of information service flow diagram (Source: OpenSoft Lab)



[Figure 6-2] Example of information security organization chart (Source: KISA)

Copyright © IGLOO Security, Inc. 2021. All rights reserved

1 IGLOO Security's Management Security Methodology
2) ID.BE Business Environment

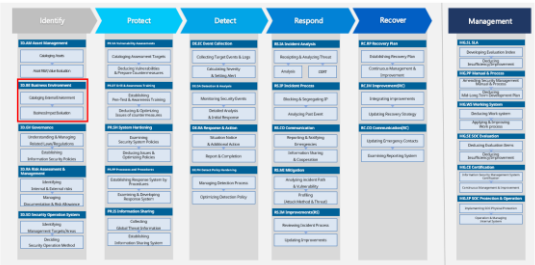
As the remote work system, including the COVID-19 issue, has been continuously strengthened, the working environment has become more connected to the external environment, unlike before. Therefore, grasping this information has also become an important element of security monitoring/control. The elements of business environment analysis identified by the security officer are important elements for identifying the target and scope of security monitoring/control, similar to the asset management stage. In order to clarify such business environment analysis, it is necessary to understand in advance how to connect services of various organizations, such as organizations related to information protection including security operation centers, organizations that operate and manage systems to be monitored, and organizations that connect or use these systems.

This business environment analysis is of course important in the area of "identify"(identifying the monitoring/control targets), but it also plays an important role for "response" and "recovery" in case of any intrusion accident. For example, in the event of an infringement incident, it is necessary to investigate related assets and network configurations to identify it. In addition, after understanding the overall service configuration through the service diagram, the data flow is analyzed, and based on this, it is necessary to analyze how far the intrusion has affected and to predict how far in the future it will be before the recovery can proceed.

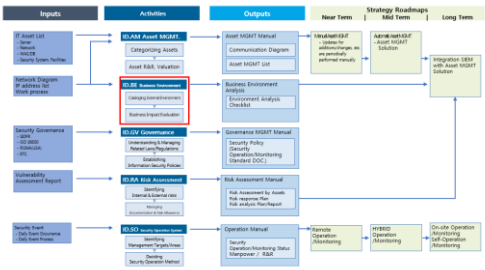
Of course, it is not easy to grasp all of them from the standpoint of security officers. However, there is a difference between recognizing and not applying the importance of these factors and not knowing and not applying them.

02. Location of the detailed activity in the IGLOO SECURITY Management Security Methodology

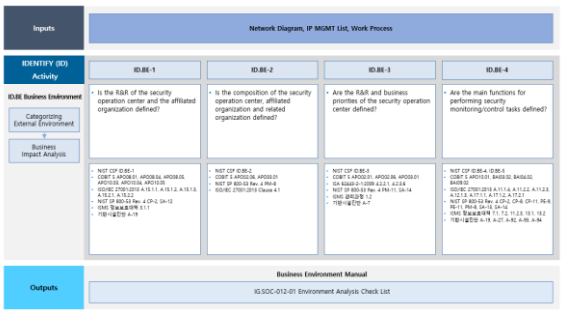
1) Management Security Methodology Process



2) Identify Function Logic Model



3) ID.BE Logic Model



4) Reference

IG.SOC-010 Identification
IG.SOC-012 Business Environment Manual
IG.SOC-012-01 BE Check List
IG.SOC-012-02 MSS description
IG.SOC-012-03 SOC Implementation
IG.SOC-012-04 MSM & Environment Implementation

Copyright © IGLOO Security, Inc. 2021. 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
© 2021 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.