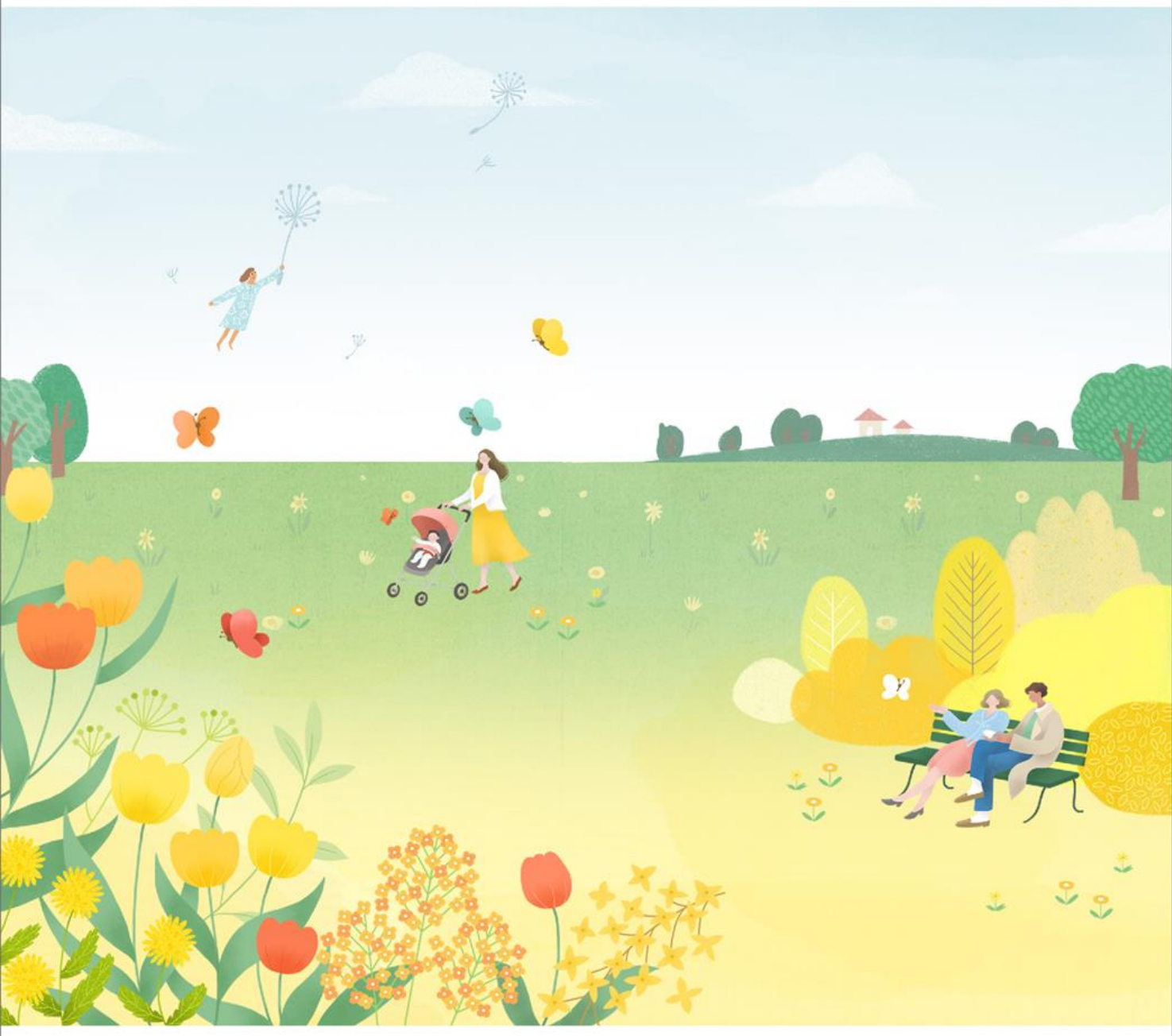
Monthly Security Report

2019
May



Cover Story

Email-based spear phishing attack log analysis and CTI-based detection

File Content Disclosure on Rails (CVE-2019-5418)

Artificial Intelligence in Cyber Security

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. 2019. All rights reserved.

Cover Story

1. Monthly Security Issue

- Monthly security issue

2. IGLOO Statistics

- Monthly Attack Service and Trend Analysis
- Detailed Analysis According to Different Patterns

3. SIEM Guide (SPiDER TM V5.x)

- Email-based spear phishing attack log analysis and CTI-based detection

4. Tech Note

- File Content Disclosure on Rails (CVE-2019-5418)

5. Special Column

- Artificial intelligence from a cyber security point of view

6. Focus On IGLOO Security

- Japan IT Week Spring 2019
- 2019 Partner Day launch

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

CHAPTER 1

Monthly Security Issue

1. Monthly Security issue

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

1 Monthly Security Issue

‘It’s the end phase of lung cancer.’ …Medical examination result, it turns out that was manipulated by hacker

- A research report say that It is possible to manipulate medical records by using AI technology , which can lead physicians to make false diagnoses.
- Researchers at the Ben Gurion University in Israel conducted an experiment to manipulate the 3D scan image of a patient after implanting a malicious code created through deep learning technology into a hospital. In fact, the researchers showed a manipulated 3D scanned image to three radiologists. And none of the three could find out whether it was manipulated.
- Security experts say hospital systems are becoming increasingly sophisticated and automated, but the majority of hospital-generated medical data is distributed without security devices such as encryption and digital signatures. It is likely to become a serious threat in the future.
- Particularly, in the case of radiology such as 3D CT, X-ray and MRI, special care is required because more hospitals are evaluating the results by applying AI technology.
- Security experts are now emphasizing that many hospitals use closed networks that are difficult to access from outside, but should prepare a defense strategy that is optimized for medical data in case future telemedicine or cloud adoption will spread.

’Did you get BTS concert tickets?’ … Malicious bots, pretending to be human being, aim for ticketing services and medical services

- the technology of automated programs which pretend as a human being and access the web-site is developing into serious problem.
- According to security company Distil Networks, the largest number of high-end bots are found, especially in ticketing businesses and medical health organizations.
- Of course, there are good bots that automatically scan ports or collect price information, but malicious bots that are used for online fraud, such as substituting leaked passwords and user names, or manipulating product evaluation scores, are likely to be a big problem.
- The high-end bots acting like human account for around 21% in the malicious bots.
- It is analyzed that 28% of ticketing in ticket sites were made by malicious bots. These robots were using tools make allowing human-like mouse point moving and malware-infected PCs.
- In the medical health business, which has a lot of sensitive personal information, there were many high-end bots collecting personal identification information and obtaining false insurance or issuing fake prescriptions.

‘Don’t touch machines thoughtlessly?’… may be exposed to ransomware risk

- Research has shown that the longer the life cycle of the equipment, the more likely the manufacturer is to be exposed to threats.
- According to Trend Micro's research, manufacturing is more likely to be infected with cryptocurrency mining tools, Ransomware, etc. due to the high percentage of older OSs and poor security updates compared to other businesses.
- Most manufacturers have been using equipment for a long time in accordance with the unwritten rule of "Don't touch a working machine if it works fine" Many of the older equipment are not compatible with the latest software, and little support has been provided for security updates.

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

1 Monthly Security Issue

‘What is the malicious code that will take over the throne?’ …Warning! Malicious codes disguised as an episode of a popular American drama.

- Cyber criminals are believed to be inducing infection through malicious code distribution disguised as the latest episode of a popular U.S. drama. The attackers were especially fond of dramas such as games of the throne, walking dead, and Arrow.
- According to the Kaspersky Lab report, there were about 20,000 users who were attacked in 2018 disguised as games of the throne. The most frequently used episode in the attack was "The Beginning of Winter," the first episode of the game of throne season 1.
- Security experts say cybercriminals are exploiting people's anxiety and loyalty and recommend not to download pirated content that is likely to be infected with malware.

‘Don’t expose my booking information’ …Personal information is leaking from hotels around the world

- When making hotel reservations by online, it appears that the customer’s personal information is leaking easily.
- According to a survey by SIMENTEC, personal information related to reservations (name, address, contact number, passport number, last four digits of credit card) is leaking out to third-party advertising agencies, social media websites, etc. from businesses ranging from small hotels to large five-star hotels.
- In a survey of more than 1,500 hotels in 54 countries, 67% of hotels were not aware that they were handed over to the partner with a reference code associated with the reservation. Partners could log in to the hotel reservation system to view customer details in detail and cancel the reservation.
- In addition, 57% of the hotels were sending confirmation emails without a login, including a link to view booking details. If the attacker hacked the e-mail in the majority of the places where the link was not encrypted, the key information could be bypassed.
- Security experts advised that companies that provide online booking services must ensure that the link to verify booking details is encrypted, that credentials are exposed, and that sensitive information is being passed on to third parties.

‘Cryptocurrency mining and prevent PC booting !’ …Warning! Malicious Cryptocurrency mining code for MBR modulation

- Cryptocurrency mining malicious code that modifies PC’s master boot record(MBR) and prevent PC booting. It is spreading out in Korea since mid-March.
- According to Ahnlab, this malicious code appears to have the ability to mine the Monero (XMR) while modifying the master boot records, a hard disk area associated with booting.
- If this malicious code is infected, the malicious shell code is first executed in the MBR area, which downloads and executes a malicious file on the PC that mines Monero through communication with the outside.

The European Union said it had no problem with Kaspersky's products.

- The European Commission has found no evidence of any potential risks in using the Kaspersky Lab's products, which have been suspected of being linked to Moscow's intelligence gathering activities, and concludes that each member country can decide whether to use the Kaspersky product or not.
- Until now, Britain, the Netherlands and Lithuania have refrained from using Kaspersky products, and the U.S. has banned the use of Kaspersky products in government agencies.
- President Trump and Caspersky Lab have yet to make an official statement on this conclusion.

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

1 Monthly Security Issue

'Prepare for the sea turtle'…DNS hijacking attack targeting certain organizations was found

- Team TALOS in Cisco announce that a DNS high-jacking campaign targeting 40 organizations in 13 countries to access and manipulate DNS records by a hacking group supported by a nation.
- The Talos team named the campaign "Sea Turtle." It is inferred that most of the organizations hit by the Sea Turtle were related to national defense and national security for cyber reconnaissance purposes.
- Attackers have been stealing information by bypassing users to other malicious servers by using remote code execution vulnerabilities, or by launching a spoofing email attack to infiltrate the network, and then manipulating DNS records by stealing the criticality to gain access to DNS records.
- Security experts emphasize that practical measures should be taken to protect DNS, which is an important and perhaps most vulnerable element of the Internet infrastructure.

'A hero or a criminal?' …Marcus Hutchins who operated 'wannacry killswitch', is convicted of malware creation.

- Marcus Hutchins, a star in the security industry, has recently been found guilty of making malware. Even he launched a killswitch that blocks Wannacry Ransomware, which swept the world in 2017.
- Marcus Hutchins was arrested for creating and distributing banking malware Kronos between July 2014 and 2015.
- Marcus Hutchins says he regrets what had done before he started working in the security industry. However, regardless of the time of the his behaviors, he admits all responsibility for such mistakes.

Exploit attack increases for MS product vulnerabilities ... 80% or more of the vulnerabilities are related to administrator rights.

- More and more cyberattacks are taking issue with Microsoft products. Microsoft continues to enhance product security, but it seems not work well.
- According to BeyondTrust, 189 of the 700 vulnerabilities patched by Microsoft last year are at risk of being lethal.
- 81% of MS product vulnerabilities found in 2018 were related to administrator rights, and there was a high risk of mitigating if the organization properly adjusted and managed administrator rights. Security experts stress that Microsoft cannot release products that do not have administrator rights, so it needs to be managed by the company itself to set up and change the administrator's rights for all systems with Windows installed.

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

CHAPTER 2

IGLOO Statistics

1. Monthly Attack Service and Trend Analysis

01. Monthly Attack Service(Port) TOP 10

02. Monthly Attack Service(Port) cases compared to last month

03. TOP 10 Monthly Attack Service patterns

04. Monthly Attack Service Incident patterns compared to last Month

2. Detailed Analysis According to Different Patterns

Copyright © IGLOO Security, Inc. 2019. 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..

01. Monthly Attack Service(Port) TOP 10

This month's (May. 2019) collected data shows that the HTTPS (TCP/443), IUA(TCP/9900) have increased and Microsoft-DS(TCP/445), SNMP(UDP/161) have decreased compared to last month. The events NETBIOS(UDP/137)have newly entered the rankings.

※ Based on IGLOO SECURITY SOC SIEM data collection

Rank	Service(Port)	No. of Cases	Ratio(%)	Fluctuation
1	HTTP(TCP/80)	2,278,282,889	54.30%	-
2	DNS(UDP/53)	718,421,448	17.12%	-
3	HTTPS(TCP/443)	372,907,501	8.89%	▲1
4	Microsoft-DS(TCP/445)	321,345,654	7.66%	▼1
5	ICMP(0/ICMP)	143,912,535	3.43%	-
6	IUA(TCP/9900)	121,739,555	2.90%	▲1
7	SNMP(UDP/161)	114,867,997	2.74%	▼1
8	Telnet(TCP/23)	54,259,057	1.29%	-
9	NTP(UDP/123)	36,324,228	0.87%	-
10	NETBIOS(UDP/137)	33,423,207	0.80%	NEW
	Total	4,195,484,071	100.00%	-

[Table2-1] TOP 10 Monthly Attack Ports

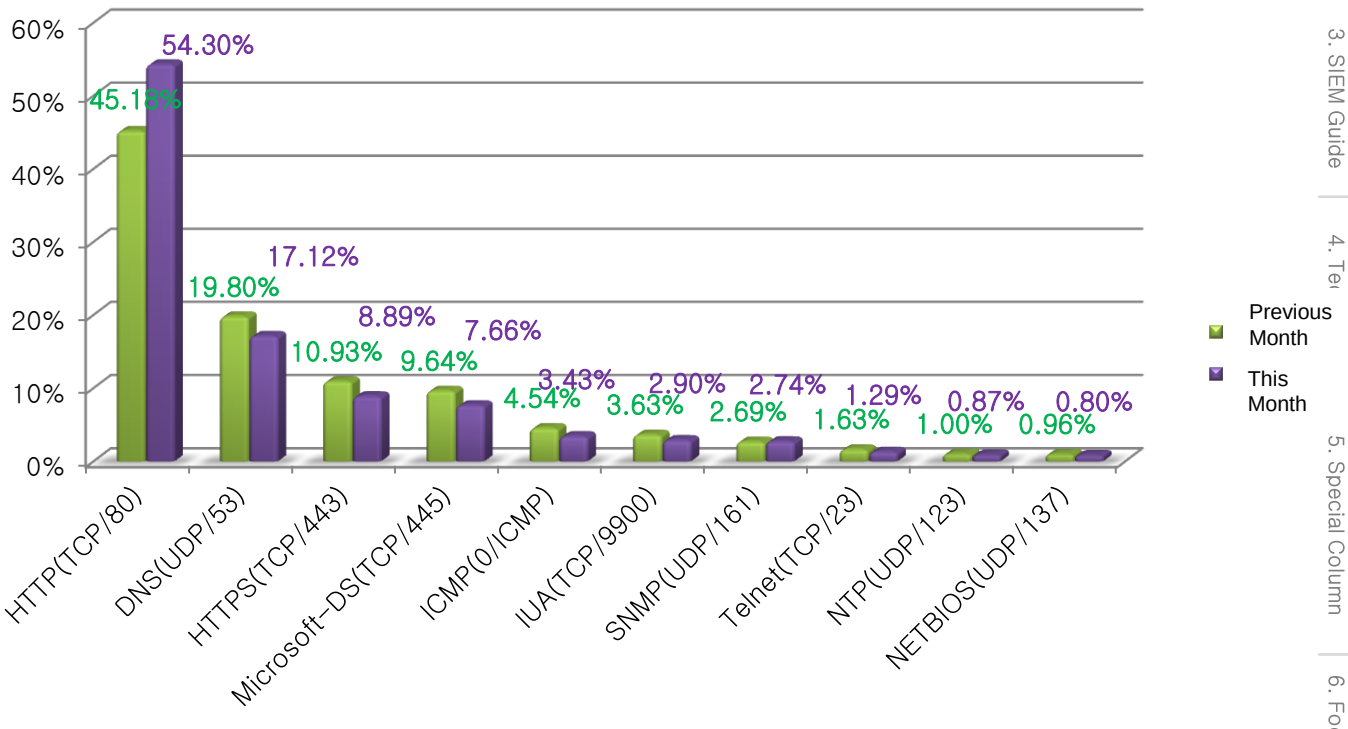
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

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..

02. Monthly Attack Service(Port) cases compared to last month

According to analysis of events by attack service port in May 2019, there is slight change in ranking of TOP, but number of events has not increased significantly compared to rate of variation, so it is estimated that there will be no particular information. HTTP ports have increased by 9%, accounting for more than 50% of the total. The number of events increased by 5 million compared to the previous month, and HTTP Login Brute Force Attack attacks were also found to have increased. Recently, there have been frequent attacks on Brute Force Attack using HTTP (TCP/80) service ports, and a variety of other attacks using other vulnerabilities continue to occur. Periodic security checks, such as pre-inspection and vulnerability patches, are recommended for prevention of security accidents.



[Figure2-1] Monthly Attack Port TOP 10

Copyright © IGLOO Security, Inc. 2019. 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 a ranking process, future cyber threats become predictable.

03. TOP 10 Monthly Attack Service Patterns

The results from this month's (May. 2019) attack event analysis indicate that HTTP Login Brute Force event have increased in rank and that FIN Port Scan, Multi Packet Inspection event has fallen in rank. The events UDP Tear Drop, Netbios Scan have newly entered the rankings.

※ Based on IGLO SECURITY SOC SIEM data collection

Rank	Pattern	No. of Cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	240,899,618	48.15%	-
2	ACK Port Scan(F/W Scan)	108,378,322	21.66%	-
3	SYN Port Scan	74,692,826	14.93%	-
4	MySQL-Server Login Brute force	27,171,032	5.43%	-
5	HTTP Login Brute Force	13,227,180	2.64%	▲1
6	FIN Port Scan	11,126,664	2.22%	▼1
7	UDP Tear Drop	9,098,110	1.82%	NEW
8	Multi Packet Inspection	6,517,312	1.30%	▼1
9	MS WINS Server Registration Spoofing Vuln-1[Req](UDP-137)	4,885,798	0.98%	
10	Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	4,308,910	0.86%	NEW
Total		500,305,772	100.00%	-

[Table 2-2] TOP 10 Monthly Attack Patterns

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

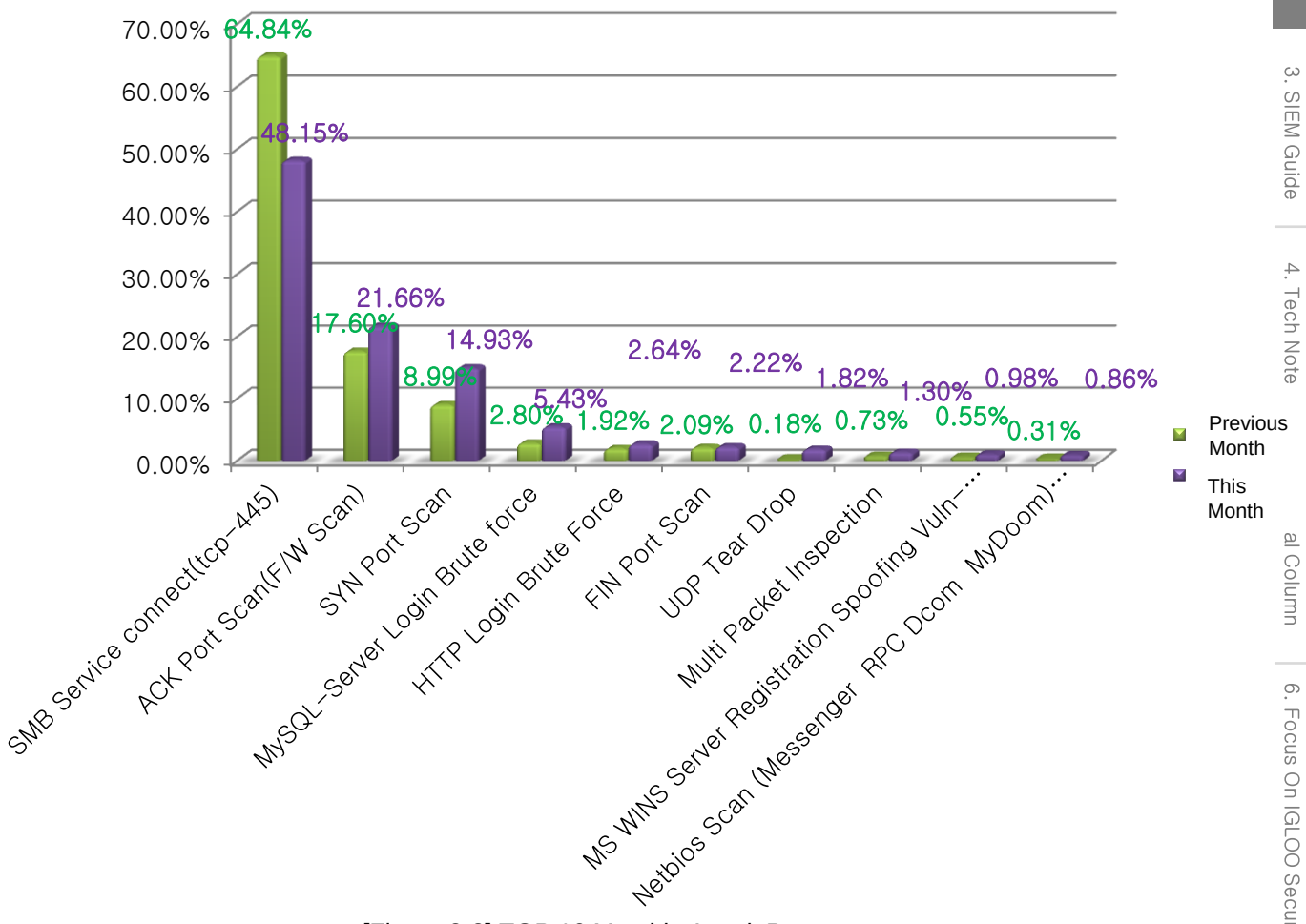
1 Monthly Attack Service and Trend Analysis

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 Incident Patterns Compared to Last Month

The results from this month's (May. 2019) attack event analysis indicate that the ratio of SMB Service Connect(tcp-445) event detection have been decreased significantly and the number of event occurrences also have been decreased.

Newly identified UDP Tear Drop this month is a type of DOS attack that loads target servers by over-fragmentation through manipulation of IP packet data. In order to prevent such as from occurring, it is advised that the security manager periodically check their systems.



[Figure 2-2] TOP 10 Monthly Attack Patterns

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

2 Detailed Analysis According to Different Patterns

IGLOO Statistics introduces results of an integrated analysis of the TOP 10 attack patterns which occurred in May. Each vulnerability needs to be dealt with in advanced in accordance with the integrated analysis results of each attack pattern.

Attack Pattern	Integrated Analysis Results
SMB Service Connect (tcp-445)	Microsoft Windows uses SMB protocol to share files and printer resources with other computers. Sharing resources using SMB in older versions (95, 98, Me and NT) of Windows used TCP port 137 and 139 and UDP port 138 by executing NETBIOS with NETBIOS over TCP/IP. On older versions of Windows 2000/XP, it was possible to run SMB directly through TCP/IP on TCP port 445. If the files are shared with easily guessable password or passwords are not set, they can suffer from secondary attacks.
ACK Port Scan (F/W Scan)	ACK Port Scan (F/W Scan) is a type of scanning attack targeting vulnerable ports which are allowed to be accessed by firewall policy. Attackers can collect information on vulnerable ports by analyzing the returned packet as a response to the packet sent in advance. These attacks are not intended to destroy the system but to collect information for planning a scenario for secondary attack.
SYN Port Scan	In order to hacking the computer (server), the targeted computer sends SYN sequentially or infrequently from port number 0 to 65,535 ports to check the SYN/ACK that the server responds to as a way to find out if the target computer opens the port of TCP/IP to service.
MySQL-Server Login Brute force	A brute force attack can be launched against an user account in MySQL. MySQL replies with success/error based on supplied credentials and time required for the verification is almost the same in either cases. Hence, an attacker can launch brute force attack against a MySQL user account at a rapid rate and can try many different passwords.
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).
FIN PORT SCAN	This method can be used as a faster alternative to a typical TCP port scan, which is scanned by observing the host's response to TCP FIN packets to find a TCP port that is listed. The port is actually scanned without initializing the TCP connection, using a property that does not respond when the FIN is sent to the Listening port and sends a response only when it is sent to the Non-Listening port.
UDP Tear Drop	A common form of denial of service attack. In which the perpotrator overbears a network by exploiting datagram fragmentation mechanisms.
Multi Packet Inspection	A Multi Packet Inspection is a rule that occurs within the IPS of a specified company and detects using the automated pattern learning defense mechanism set-up within the IPS. It denies access for a certain amount of time if a packet, which exceeds the bytes PPS set-up by the IPS, is injected.
MS WINS Server Registration Spoofing Vuln-1 [Req](UDP-137)	This attack occurs while a name is being registered on the Windows WINS server and the NetBIOS is not inspected thoroughly enough. Through this vulnerability, the attacker is capable of redirecting the victims internet traffic through web proxy spoofing to a specified domain.
Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	A network scanner tool that scans all computers in the IP addresses range you choose, using NetBIOS protocol. For every computer located by this NetBIOS scanner, the following information is displayed: IP Address, Computer Name, Workgroup or Domain, MAC Address, and the company that manufactured the network adapter (determined according to the MAC address). NetBScanner also shows whether a computer is a Master Browser. You can easily select one or more computers found by NetBScanner, and then export the list into csv/tab-delimited/xml/html file.

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

CHAPTER 3

SIEM Guide (SPiDER TM V5.x)

Email-based spear phishing attack log analysis and CTI-based detection

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

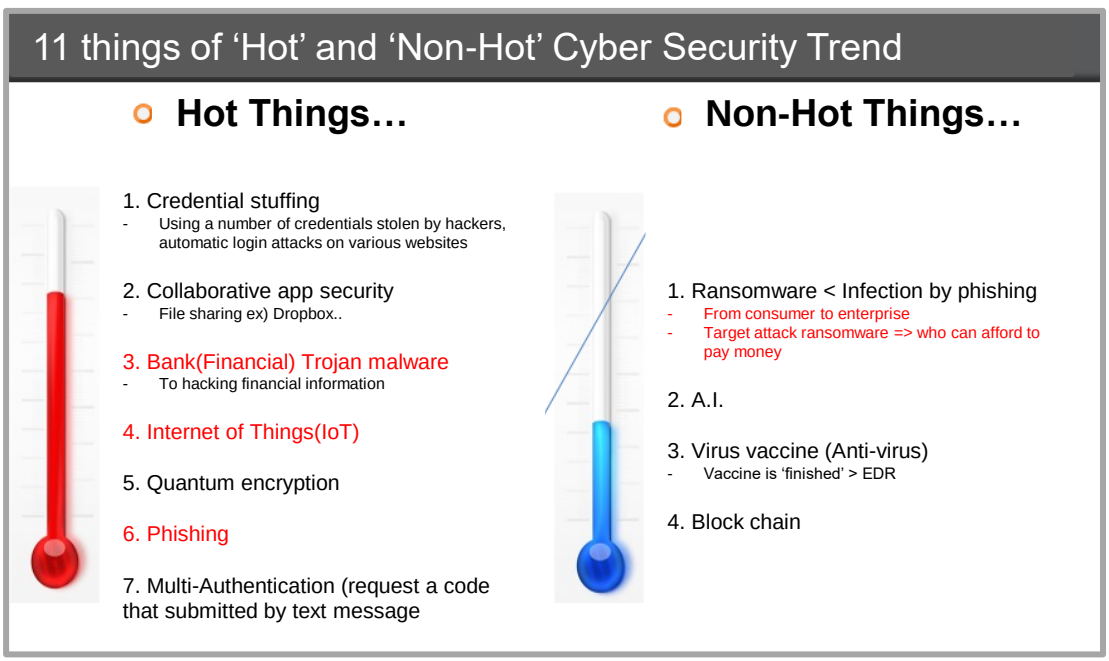
Email-based Spear phishing attack log analysis and detection scheme

SPiDER TM V5.0 is an integrated security management solution that integrates Igloo security 's security monitoring experience and big data utilization capability. It improves the agility and efficiency of security monitoring work through unified monitoring environment configuration from initial detection to log / network packet analysis, The visibility of the first half can be secured.

Technical Support Center
Analysis Technology Team

01. 91% of corporate / institutional target attacks are spear phishing

Most spear phishing attacks are initiated via e-mail, and not sophisticated attacks are made on a wide range of targets, but rather sophisticated attacks in the form of customized attacks targeting specific targets in the form of intelligent target attacks. Although it is a specific target, anyone can be the target of an attack. If the sender of the received message is an acquaintance familiar with the customer, employee, family member or the like, the link or attachment of the mail body will be clicked without doubt. The average person will open 3% of spam and 70% of spear phishing emails within an hour of receiving an email.

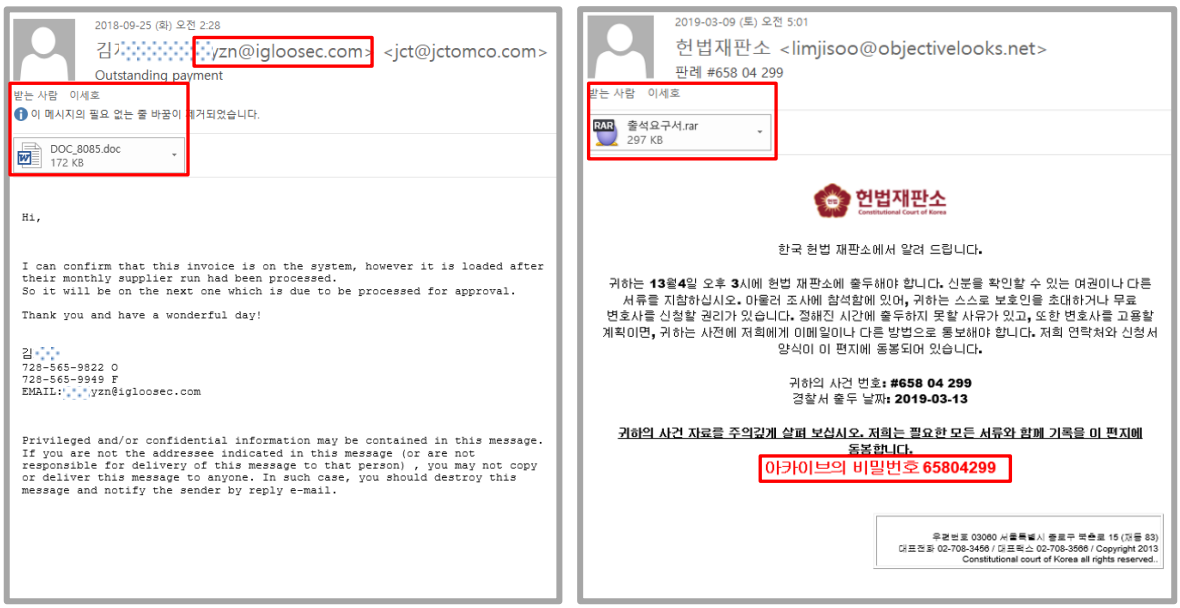


[Figure 3-1] Changes in phishing attacks (Source : www.itworld.co.kr/news/118748)

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

Email-based Spear phishing attack log analysis and detection scheme

Spear phishing e-mail attacks are based on mutual trust, so they are as effective as attacks. Ransomware, which has been widely and indiscriminately distributed using e - mail in recent years, is usually attacking enterprises for money. This trend is the same in Korea. Recently, many phishing e-mails have been received rapidly by our mail server. [Figure. 3-2] is the phishing or spear phishing e-mails that we received in our e-mail account. The right-hand phishing e-mail is an email impersonating the Constitutional Court, attaching an event request named "Attendance Request" to attract the recipient's attention. This has led to the execution of malicious files, and in order to pretend enhancing security, have set passwords in compressed attachments and are kindly described by email. The left-hand phishing email is an unpaid invoice (invoice) email impersonating a colleague of the same company, and request to check it. In this issue of the SIEM Usage Guide, we will look at CTI-based log analysis and detection methods to determine if there are internal users who have run attachments through these malicious emails.



[Figure 3-2] Phishing emails impersonating invoices and the Constitutional Court

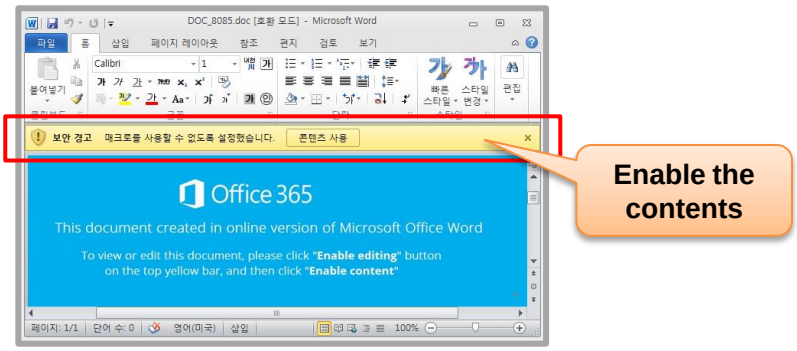
02. Log analysis about spear phishing mail's malicious code attachment

1) Execution malicious attachments on user's PC

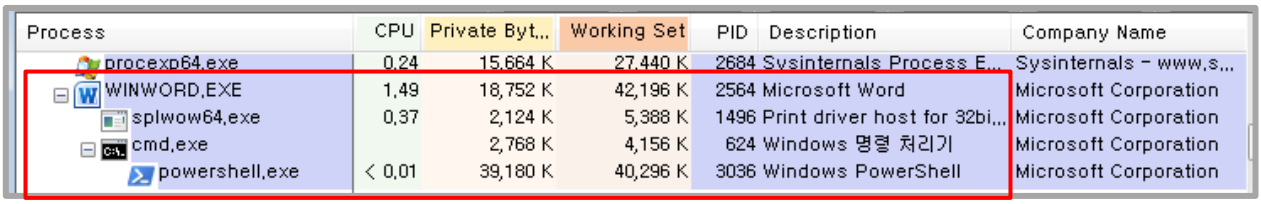
We will execute the document file attached to the left sphere phishing e-mail in [Figure 3-2] and analyze the malicious file of the PC, and we will look at logs generated from the infrastructure and security equipment based on it. [Figure 3-3] When an internal user executes a document with an embedded malicious script (VB, Macro) attached to an e-mail, a "Use Content" box appears with a security warning notification. As soon as we click "Use content", we can see that WINWORD.EXE → cmd.exe → powershell.exe is executed automatically as in [Figure 3-4].

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

Email-based Spear phishing attack log analysis and detection scheme



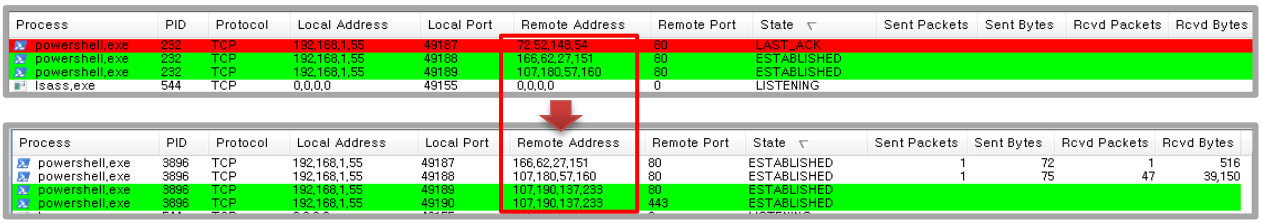
[Figure 3-3] Encourage clicks on enable the contents



Process	CPU	Private Byt...	Working Set	PID	Description	Company Name
procexp64.exe	0.24	15,664 K	27,440 K	2684	Sysinternals Process E...	Sysinternals - www.s...
WINWORD.EXE	1.49	18,752 K	42,196 K	2564	Microsoft Word	Microsoft Corporation
splwow64.exe	0.37	2,124 K	5,388 K	1496	Print driver host for 32bi...	Microsoft Corporation
cmd.exe		2,768 K	4,156 K	624	Windows 명령 처리기	Microsoft Corporation
powershell.exe	< 0.01	39,180 K	40,296 K	3036	Windows PowerShell	Microsoft Corporation

[Figure 3-4] Automatically execute 'powershell.exe'

The attached document runs normally without any problems, but in the background it communicates with the external C & C server by the powershell.exe script execution. As shown in [Figure 3-5], you can see that powershell.exe communicates with four IP : 72.52.148.54, 166.62.27.151, 107.180.57.160, and 107.180.137.233. When a document is executed, it can not be assumed that it is a malicious act because external communication is performed. In this situation, **CTI (Cyber Threat Intelligence information)** is helpful for quick judgment. These IPs are all malicious code distribution sites.

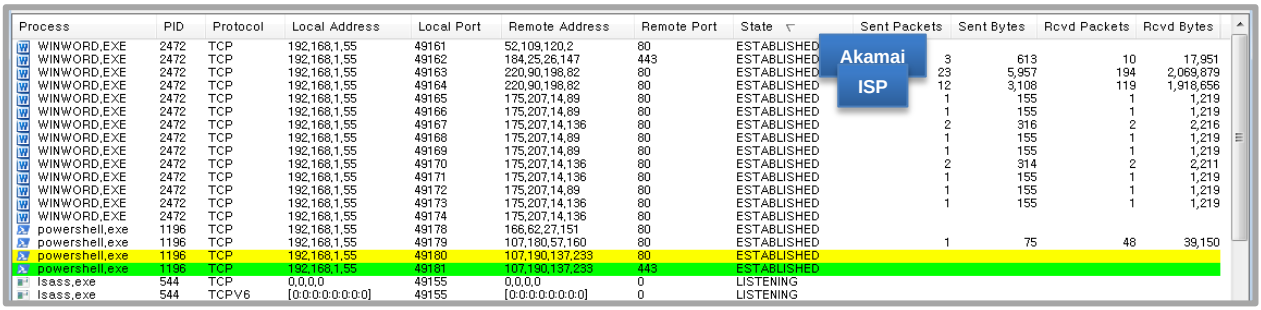


Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
powershell.exe	232	TCP	192.168.1.55	49187	72.52.148.54	80	LAST_ACK				
powershell.exe	232	TCP	192.168.1.55	49188	166.62.27.151	80	ESTABLISHED				
powershell.exe	232	TCP	192.168.1.55	49189	107.180.57.160	80	ESTABLISHED				
lsass.exe	544	TCP	0.0.0.0	49155	0.0.0.0	0	LISTENING				

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
powershell.exe	3896	TCP	192.168.1.55	49187	166.62.27.151	80	ESTABLISHED	1	72	1	516
powershell.exe	3896	TCP	192.168.1.55	49188	107.180.57.160	80	ESTABLISHED	1	75	47	39,150
powershell.exe	3896	TCP	192.168.1.55	49189	107.190.137.233	80	ESTABLISHED				
powershell.exe	3896	TCP	192.168.1.55	49190	107.190.137.233	443	ESTABLISHED				

[Figure 3-5] External C&C communication by malicious script(Powershell.exe) execution

When the document file is executed, communication with many external service providers such as Akamai may occur for CDN (Content Delivery Network) communication as in [Figure 3-6]. It seems that we should not make a mistake and block the firewall.



Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State	Sent Packets	Sent Bytes	Rcvd Packets	Rcvd Bytes
WINWORD.EXE	2472	TCP	192.168.1.55	49161	52.109.120.2	80	ESTABLISHED				
WINWORD.EXE	2472	TCP	192.168.1.55	49162	184.25.26.147	443	ESTABLISHED	3	613	10	17,951
WINWORD.EXE	2472	TCP	192.168.1.55	49163	220.90.198.82	80	ESTABLISHED	23	5,957	194	2,069,879
WINWORD.EXE	2472	TCP	192.168.1.55	49164	220.90.198.82	80	ESTABLISHED	12	3,108	119	1,918,656
WINWORD.EXE	2472	TCP	192.168.1.55	49165	175.207.14.89	80	ESTABLISHED	1	155	1	1,219
WINWORD.EXE	2472	TCP	192.168.1.55	49166	175.207.14.89	80	ESTABLISHED	1	155	1	1,219
WINWORD.EXE	2472	TCP	192.168.1.55	49167	175.207.14.136	80	ESTABLISHED	2	316	2	2,216
WINWORD.EXE	2472	TCP	192.168.1.55	49168	175.207.14.89	80	ESTABLISHED	1	155	1	1,219
WINWORD.EXE	2472	TCP	192.168.1.55	49169	175.207.14.89	80	ESTABLISHED	1	155	1	1,219
WINWORD.EXE	2472	TCP	192.168.1.55	49170	175.207.14.136	80	ESTABLISHED	2	314	2	2,211
WINWORD.EXE	2472	TCP	192.168.1.55	49171	175.207.14.136	80	ESTABLISHED	1	155	1	1,219
WINWORD.EXE	2472	TCP	192.168.1.55	49172	175.207.14.89	80	ESTABLISHED	1	155	1	1,219
WINWORD.EXE	2472	TCP	192.168.1.55	49173	175.207.14.136	80	ESTABLISHED	1	155	1	1,219
WINWORD.EXE	2472	TCP	192.168.1.55	49174	175.207.14.136	80	ESTABLISHED				
powershell.exe	1196	TCP	192.168.1.55	49178	166.62.27.151	80	ESTABLISHED				
powershell.exe	1196	TCP	192.168.1.55	49179	107.180.57.160	80	ESTABLISHED	1	75	48	39,150
powershell.exe	1196	TCP	192.168.1.55	49180	107.190.137.233	80	ESTABLISHED				
powershell.exe	1196	TCP	192.168.1.55	49181	107.190.137.233	443	ESTABLISHED				
lsass.exe	544	TCP	0.0.0.0	49155	0.0.0.0	0	LISTENING				
lsass.exe	544	TCPV6	[0:0:0:0:0:0:0:0]	49155	[0:0:0:0:0:0:0:0]	0	LISTENING				

[Figure 3-6] Phishing mail pretending to be invoice mail and Constitutional Court

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

Email-based Spear phishing attack log analysis and detection scheme

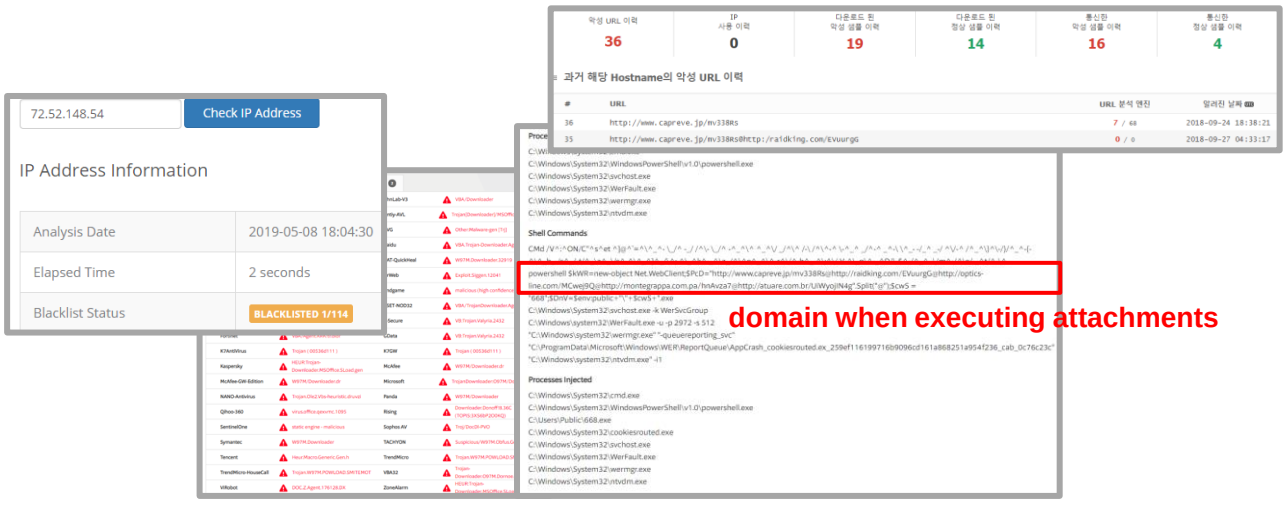
Even if you try to open the attachment, look carefully at the "Security Warning Macro is disabled. [Enable contents]" section, and you do not use it, you can avoid the infection by not executing the script.

2) Analysis of harmful IP / URL using SIEM's CTI information

Even if we are not an expert, we can analyze the reversing level of malicious files by using the CTI information that has been opened to the attached document. In [Figure 3-5], when the attached document is executed, information of IP which communicates with external C&C server by executing malicious script by Powershell.exe can be obtained. In order to judge whether suspicious IP is malicious or not, we can easily check malicious activity and activity history by checking SIEM → Blacklist Management→ Blacklist IP/URL menu. 72.52.148.54, 166.62.27.151, 107.180.57.160, 107.180.137.233 All four IPs are malicious IPs with history of malware distribution.

[Table 3-7] Malicious IP inquiry result screen of prevention activity (CTI)

In addition, we can check these information from various web-site such as ipvoid, malwares, virustotal. Since the information provided form each site is slightly different, it may be useful to complement each other with necessary information.

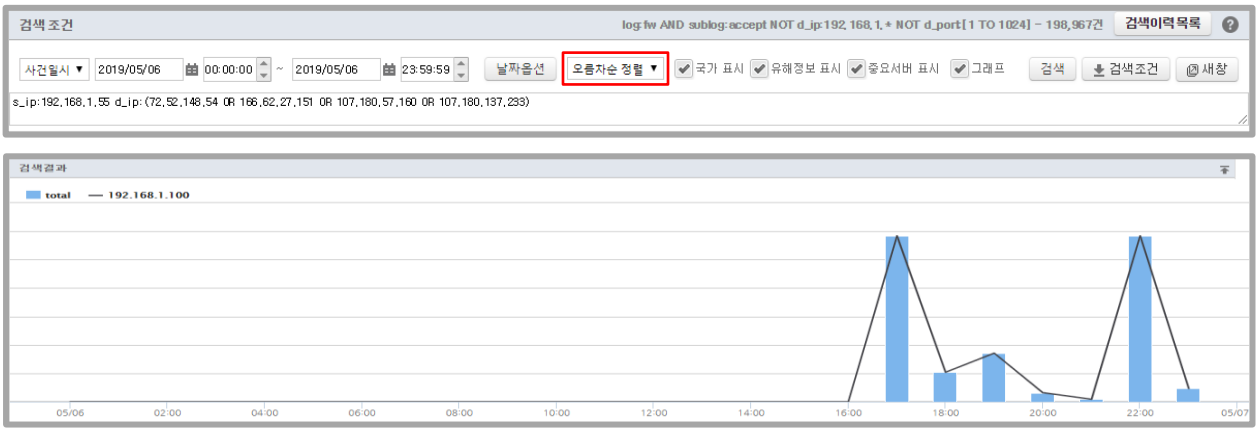


[Figure 3-8] Cyber Threat information providing sites

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

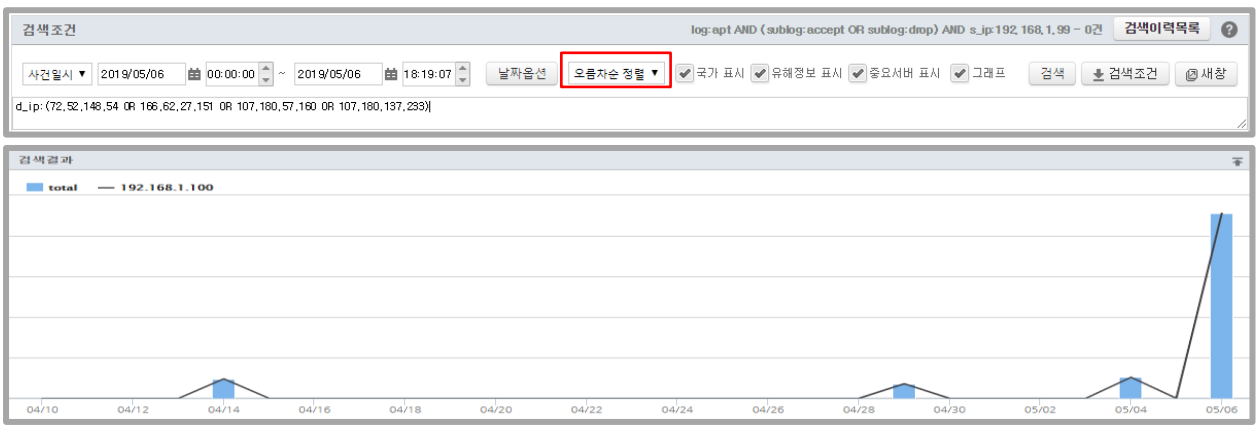
3) SIEM TimeLine log analysis

We will analyze the traffic generated by the PC at the endpoint that executed the document containing the malicious script through the logs of the network edge security devices collected by SIEM. If we want to analyze the behavior of the suspicious terminal PC in time order, use "ascending sort" in the search condition to help log analysis. If the suspicious IP of the global infection is 192.168.1.55, it can search "s_ip: 192.168.1.55", and the search results screen sorted in batch time can be seen from all collected logs. If you add an infected destination here (d_ip: (72.52.148.54 OR 166.62.27.151 OR 107.180.57.160 OR 107.180.137.233)), TimeLine analysis is available for 24 hours from when it was infected. In the search results, 192.168.1.55 IP is infected at 17:00, and it can be seen that the malicious site is accessed.



[Figure 3-9] Ascending Search and TimeLine Analysis

If you know the C&C IP and you want to find the infected PC of our institution, you can find it at the same time with "d_ip: (72.52.148.54 OR 166.62.27.151 OR 107.180.57.160 OR 107.180.137.233) . Through the TimeLine analysis, another source IP is already infected on April 14, and intuitively can see the history of access to the C2 server.



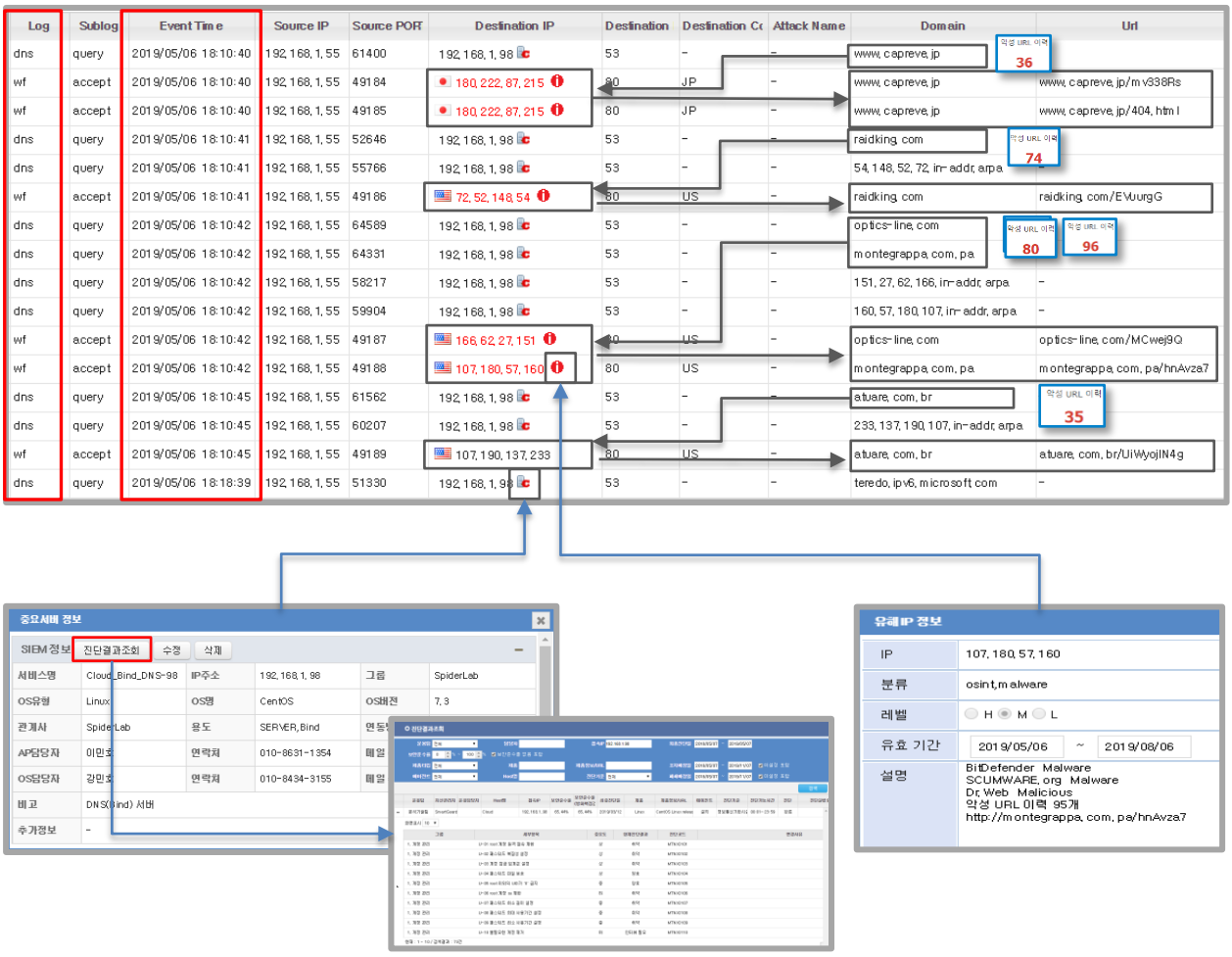
[Figure 3-10] Analysis about all internal users accessing C2 server TimeLine

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

Email-based Spear phishing attack log analysis and detection scheme

4) Detailed log analysis by SIEM

If you have confirmed the time of infection through time line analysis, the next analysis process is the detailed log analysis at that time. Let's take a look at Figure 3-11. You can start analyzing from a Zero-Trust network connection point of view. After executing the document, querying "www.capreve.jp" to the DNS server and receiving "180.222.87.215" IP response and attempting to connect with "http://www.capreve.jp/mv338Rs", it was converted to 404.html error page It looks like the page is missing from the point. Next, We inquired the DNS server "raidking.com" and tried to access "http://raidking.com/EVuurgG" after receiving the information of "72.52.148.54" IP and "optics-line.com" to "166.62.27.151" / MCWEJ9Q "," 107.180.57.160 "," montegrappa.com.pa/hnAvza7 ", and" 107.190.137.233 "are connected to" atuare.com.br/UiWyojIN4g/ " However, the page is deleted and the malicious code is not distributed (Drive-by download). It is a recent trend to use the DNS domain of web hosting, not IP direct communication, and to use several distribution servers. The malicious site can be immediately determined through the harmful IP information.



[Figure 3-11] DNS and Web filter log, identification information about IP

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

As shown in [Figure 3-11], if the source IP and the destination IP are registered in the preventive activity 166.62.27.151 displayed in red color, When clicked, harmful information is provided in a popup window to help quick judgment. If it is an internal asset, 192.168.1.98 it is represented by the server icon next to the IP field and displays the same information in a popup window. If SmartGuard from Igloo Security is installed, it will show the vulnerability information together. That is, the attacker's information and asset information necessary for the infringement analysis can be immediately seen.

If you check the communication status of the tcp_flag field in the firewall traffic log in [Figure 3-12], you can see that it is "S sa A / FA a fa RA" and "S sa A / RA". Therefore, HTTP 80 communication with the malicious code distribution server is normally performed. In other words, some servers are hosted on a web server and a web hosting company server which are recovered by hacking, and it seems that IP is not blocked and continues to operate normally when the distribution server is operated.

Log	Sublog	Event Time	Source IP	Source POR	Destination IP	Destinatior	Destinatic	Protoco	Tcp Flag	Duration	Sent Bytes	Rcvd Bytes
fw	accept	2019/05/06 18:10:50	192.168.1.55	49184	180.222.87.215	80	JP	TCP(6)	S sa A / fa A FA a	10	283	603
fw	accept	2019/05/06 18:10:50	192.168.1.55	49185	180.222.87.215	80	JP	TCP(6)	S sa A / fa A FA a	10	420	12335
fw	accept	2019/05/06 18:10:52	192.168.1.55	49186	72.52.148.54	80	US	TCP(6)	S sa A / fa A FA a	10	281	749
fw	accept	2019/05/06 18:10:56	192.168.1.55	49190	107.190.137.233	443	US	TCP(6)	S sa A / RA	11	873	5610
fw	accept	2019/05/06 18:10:56	192.168.1.55	49189	107.190.137.233	80	US	TCP(6)	S sa A / RA	11	285	625
fw	accept	2019/05/06 18:10:56	192.168.1.55	49188	107.180.57.160	80	US	TCP(6)	S sa A / RA	14	807	40362
fw	accept	2019/05/06 18:10:56	192.168.1.55	49187	166.62.27.151	80	US	TCP(6)	S sa A / RA	14	336	1204
fw	drop	2019/05/06 18:18:06	192.168.1.55	138	192.168.1.255	138	-	UDP(17	null	-1	229	-1

[Figure 3-12] Firewall traffic log

03. SIEM Detection Scheme

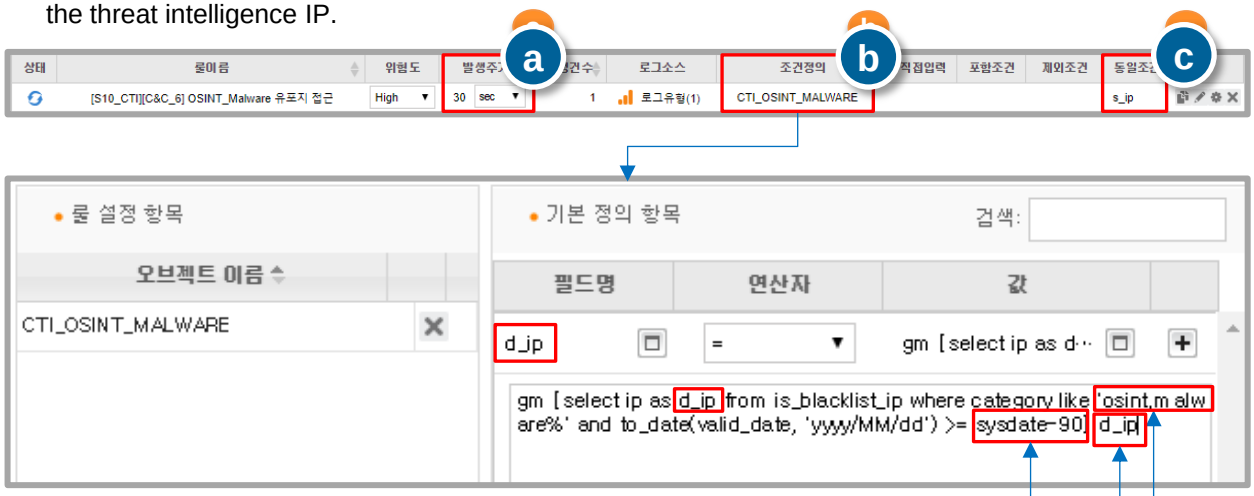
1) Detection using CTI:Cyber Threat Intelligence

Using logs collected from the SIEM perspective, PCs infected with malicious e-mail can be detected in two ways. After executing the first attachment file, it can be detected by using Cyber Threat Intelligence (CTI) when accessing malicious code distribution server. If you have an infection, there is a way to detect it on the IPS and vaccine devices and detect a long session on the firewall log. Even with network connection monitoring from the Zero-Trust perspective, it is impossible to analyze and monitor all of the many traffic. It is also difficult to distinguish malicious codes from C & C server because it is a normal web server access traffic. So, Effectiveness of CTI is determined whether it could identify who the contact is and who the destination IP is. If SIEM is already established, Threat Intelligence information is provided from the CGI server of Igloo Securities through the preventive activity function, and a single alert detection rule is also provided based on threat intelligence information.

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

2) Single rule detail setup using cyber threat intelligence

The "Single Alert Management → S10 Cyber Threat Intelligence (CTI)" rule group is an associated rule group that utilizes threat intelligence. As shown in [Figure 3-13], various rules have already been registered. It can classify the collection destination and malicious code type in the threat database registered in the preventive activity, and detect the real time by putting the harmful IP in memory according to the condition at the valid period. Modifying detection condition can be done in ⓑ Change condition definition object ("gm [select ip as d_ip from is_blacklist_ip where category like 'osint, malware%' and to_date (valid_date, 'yyyy / MM / dd')> = sysdate-90] d_ip). If we want to change the attacker (origin) or infected person (destination) of harmful IP, you can modify ①. Through the classification part ②, it is possible to classify and collect threat information collection destinations and malicious code types (tor, malware, c & c). ③ can set the validity period of threat information, that is, define whether threat information registered in the threat database a few days ago will be used as detection information. ⓐ, ⓒ part is a setting that allows the same source IP to be detected with only one access. In case of detection of 1 gun, the occurrence period is 30 seconds in consideration of continuous alert. Even if it is set to 30 seconds, if the number of occurrences is one, an alert occurs immediately upon detection. Therefore, It is detected in 0 seconds and generates an alert. In the case of a log source, you can select a log source as to whether it will be detected in the firewall log, TMS, IPS, or whether the detected device will generate an alert if the threat detected as a threat matches the threat intelligence IP.



[Figure 3-13] Single alert rule setting

[Figure 3-14] Prevention activities (CTI)

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

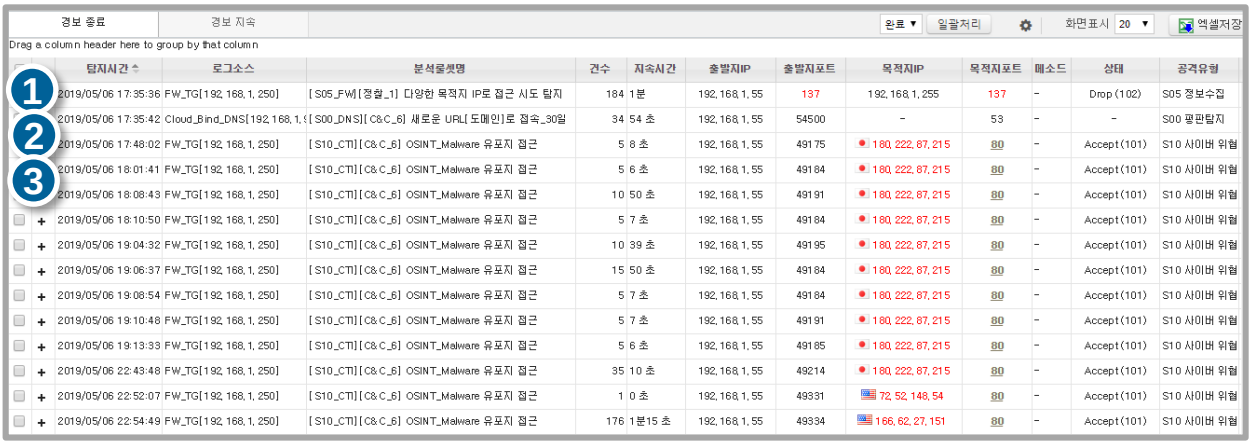
Email-based Spear phishing attack log analysis and detection scheme

3) Analysis of detection results

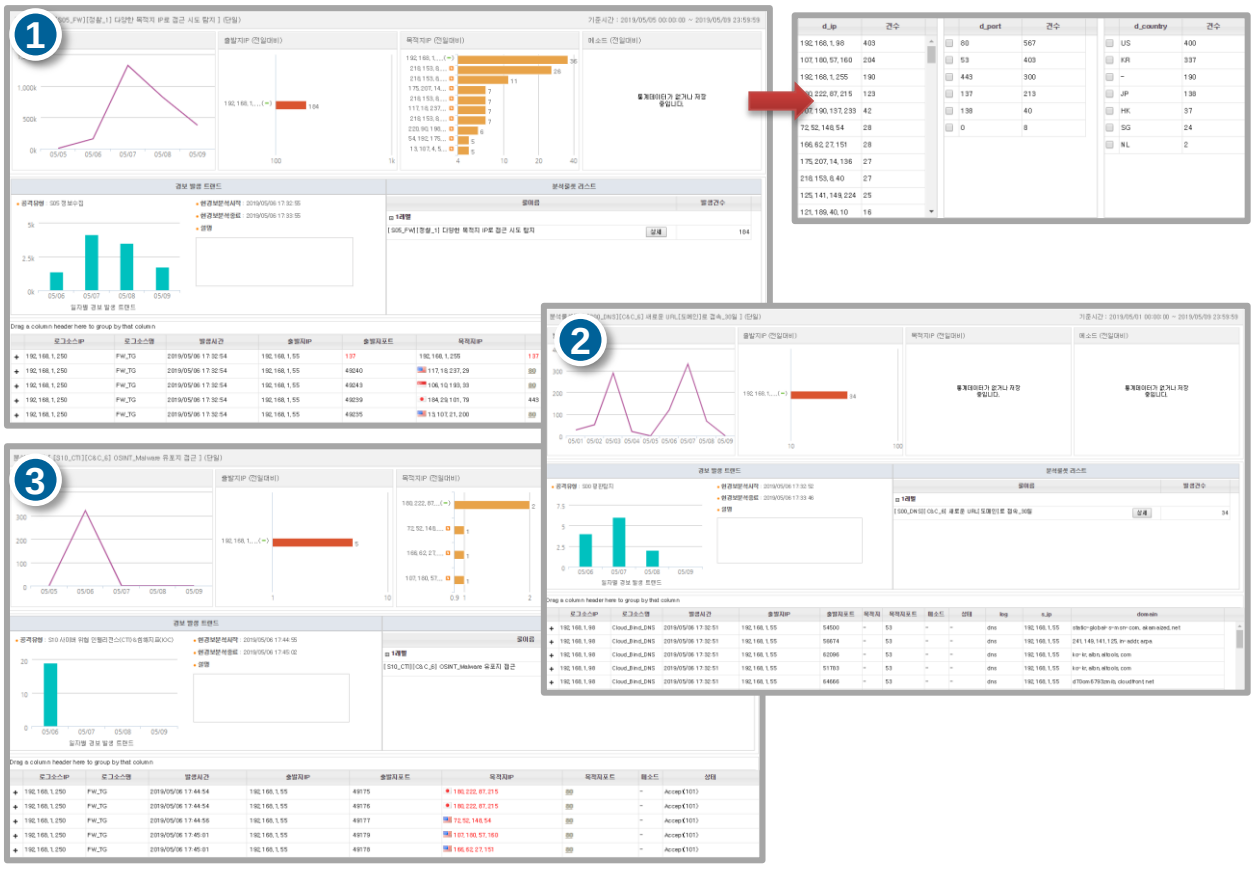
The following figure is the result screen detected on the PC when malicious attachment is executed.

① Alarms are the result of detection of anomalous activities that approach abnormal destinations. You can see the detection result when accessing the harmful IP corresponding to CTI.

② The detection result is the result of using the DNS log, but detecting the access to the domain that the 55th IP is not normally accessed. DNS logs can be used to detect when accessing a domain / URL.



[Figure 3-15] SIEM correlation analysis detection result screen



[Figure 3-16] Correlation analysis → detailed view by rule

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

③ Alarm is the result of detection when accessing IP registered in IP of CTI Malware. It is a detection setting based on the departure point, and even if the same IP accesses various harmful IPs, only one alarm occurs. If an internal user PC wishes to generate an alert each time it accesses by noxious IP, it can be set to s_ip and d_ip under the same condition of single alarm. Then, the alarm is generated by subdivision, but the number of alarms also increases. On the other hand, if d_ip is set, it is possible to detect internal IPs accessed by each infection site separately.

04. Conclusion

We have used the threat intelligence information (CTI) provided by SIEM to see how internal users can analyze and detect malicious e-mails when infected. And even if you are not an expert, I have also looked at the Open threat information sites to find out if the attachment is malicious and if IOC indicators are dangerous. In other words, if the threat information is used well, I think that we can set up a threat analysis and detection policy like the experts.

If you conclude, you can use the threat information provided by CTI Server and parent organizations of Iglooo Security to manage the harmful IP and URL / Domain through the activities.

In the next issue, we will look at more active prevention activities using threat information, asset information, and vulnerability information.

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

CHAPTER 4

Tech Note

File Content Disclosure on Rails

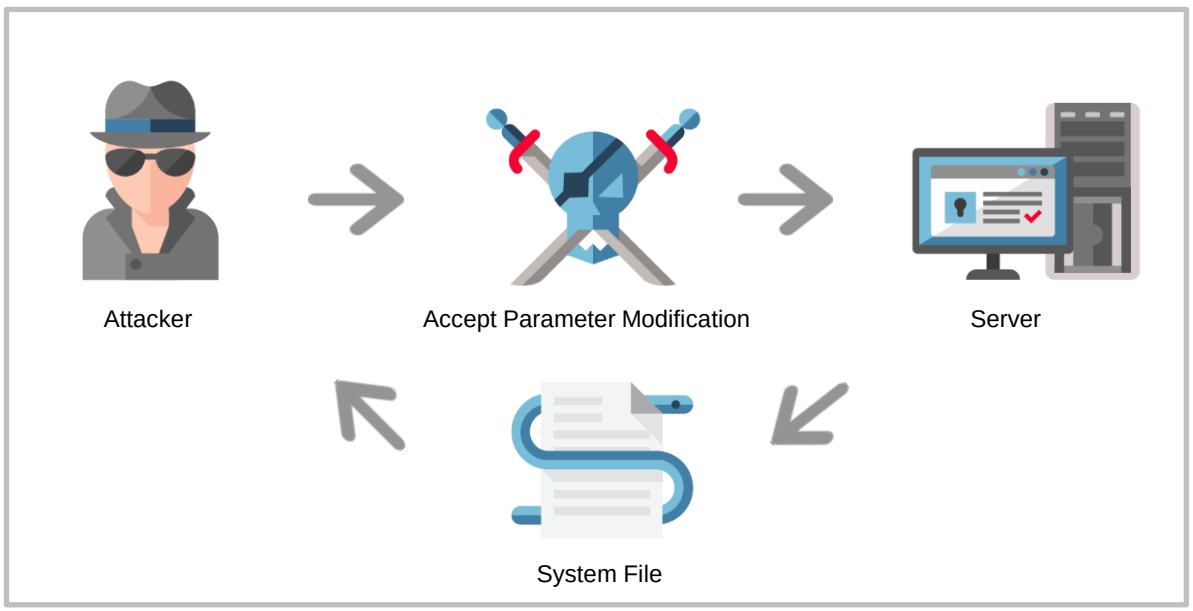
(CVE-2019-5418)

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

File Content Disclosure on Rails (CVE-2019-5418)

Overseas Department
Overseas Tech Team

01. Synopsis



[Figure 4-1] Vulnerability operation summary

There have been reports on 2 cases of vulnerabilities(File Content Disclosure : CVE-2019-5418, DOS : CVE-2019-5419) in the Ruby based web application framework Rails(Ruby on the Rails) this March. Both vulnerabilities are estimated to have high threat leels and this Month's Security Report will explore the CVE-2019-5418, which is able to carry out RCE attacks.

The CVE-2019-5418 carries out an attack through an internal processing method utilizes the file factors of the render function which is a Controller function of the MVC. When the render function of the rails searches for the requested file, the attacker can execute files which are not present in the web server directory. Rails was first released in 2004 and in march of 2019, its the first time a vulnerability was detected in the render function of the Controller.

CVE	Affected Versions	Criticality	Security Patch Version
CVE-2019-5418	<5.2.2.1, <5.1.6.2, <5.0.7.2, <4.2.11.1	High	4.2.11.1 , 5.0.7.2 , 5.1.6.2 , 5.2.2.1 , 6.0.0.beta3

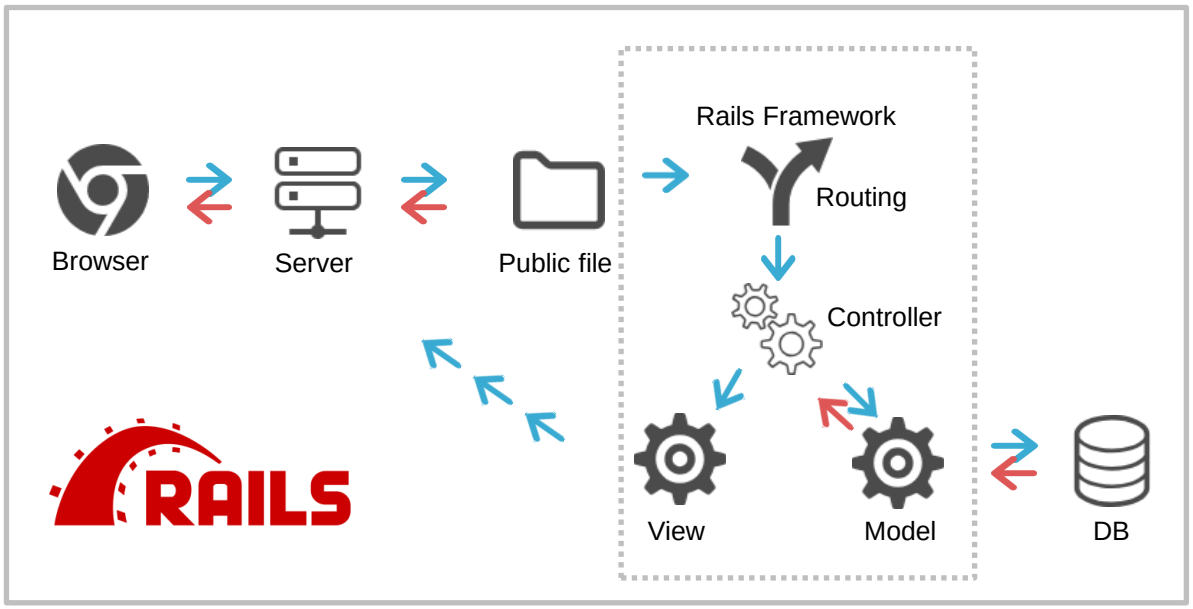
[Figure 4-1] Vulnerability information

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

File Content Disclosure on Rails (CVE-2019-5418)

02. Rails(Rails on Ruby)

▶ Where does the Rails vulnerability occur?



[Figure 4-2] Rails structure

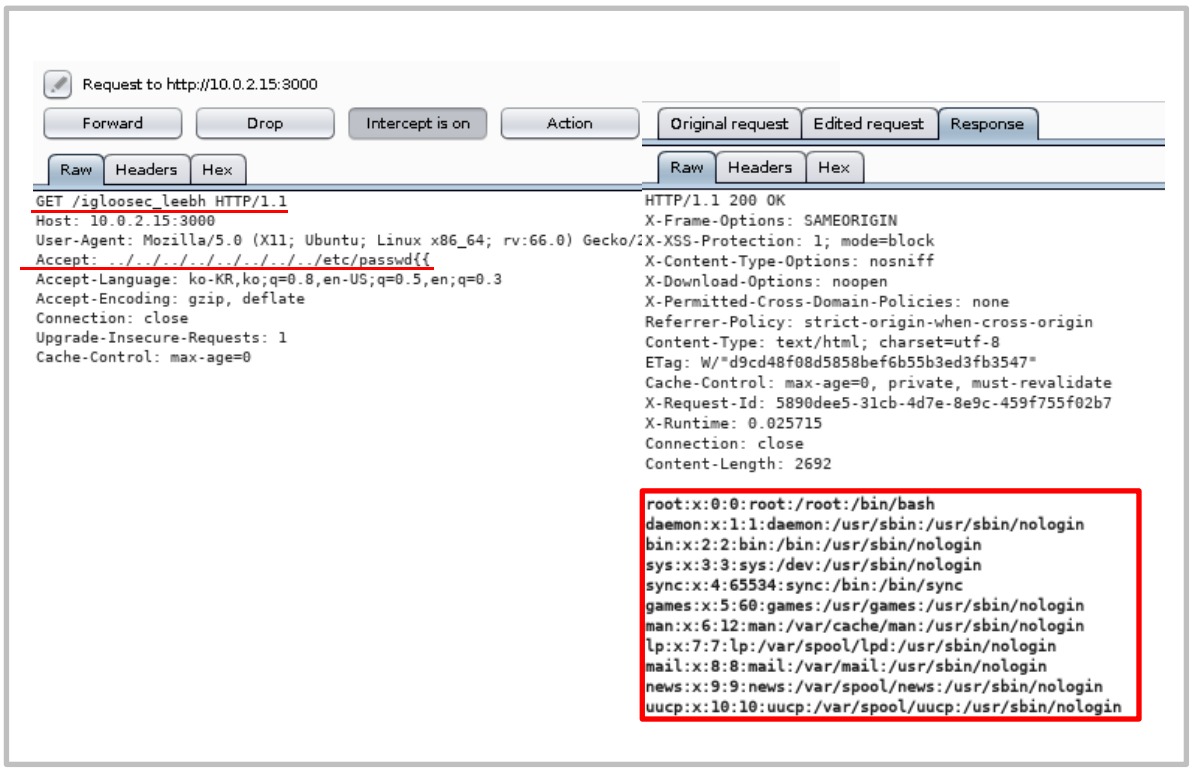
Rails is a web application frame work which utilizes the script language Ruby and aids in efficiently carrying out web programing. Rails allows for a more efficient code creation by separating the function screens utilizing the MVC(Model, View, Controller) design patterns. The vulnerability which was detected occurred in the Controller process of the MVC.

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

File Content Disclosure on Rails (CVE-2019-5418)

03. Vulnerability demonstration

▶ Attack demonstration



[Figure 4-3] Vulnerability operation synopsis

The vulnerability can generate the contents of a requested file if 'file directory+{{' is inserted into the Accept parameter of the HTTP header when the Controller is requested. However, the attack is set to generate specific files when the Controller is requested in the Application Controller.
In order to demonstrate the attack, the environment consisted of Rails below the 5.2.1 version and Ruby below version 2.5.1p57.

Program	Name	Version
Language	Ruby	2.5.1p57
FrameWork	Rails	5.2.1

[Table 4-2] Vulnerability demonstration environment

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

File Content Disclosure on Rails (CVE-2019-5418)

04. Vulnerability analysis

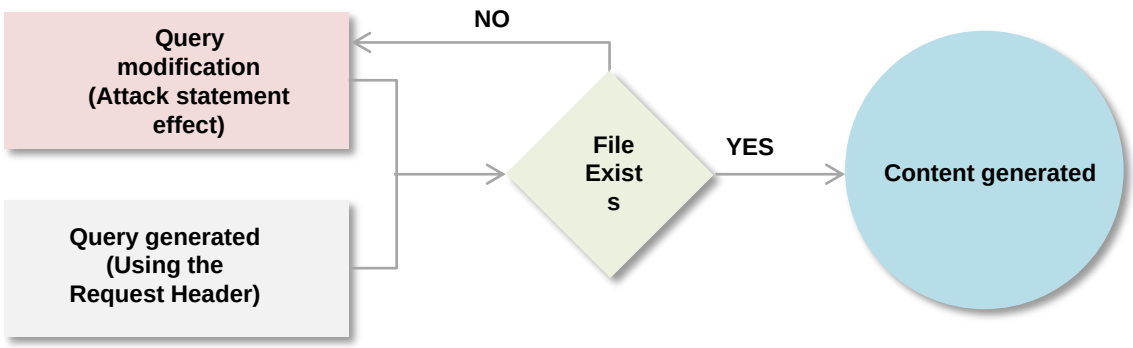
1) Vulnerability occurrence code

```
class IgloosecLeebhController < ApplicationController
  def index
    render file: "#{Rails.root}/welcome.txt"

  end

end
```

[Figure 4-4] Source code of the Controller, where the vulnerability occurs

Above is the source code of the Controller and when said Controller is called, the statement inside the index is executed. The source code is the render function in the File option "{Rails.root}/welcome.txt" and generated the directory file.

2) Vulnerability operation flow chart



[Figure 4-5] Vulnerability operation flow chart

When Controller is executed and Render File function is requested, it compiles Header information of request and creates a query and checks whether file the exists. After the search fails, the query is modified. In this process, the Accept header is used to when checking for file existence. The internal operation method performs the file search with the Accept sentence. As a result, the corresponding file is retrieved and the contents are output.

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

File Content Disclosure on Rails (CVE-2019-5418)

3) Analyzing the query modification function

```
def build_query(path, details)  path: home/twoicefish/CVE-2019-5418/demo/v
  query = @pattern.dup  query: nil

  prefix = path.prefix.empty? ? "" : "#{escape_entry(path.prefix)}\\1"
  query.gsub!(/:prefix(\/)?/, prefix)

  partial = escape_entry(path.partial? ? "_#{path.name}" : path.name)
  query.gsub!(/:action/, partial)

  details.each do |ext, candidates|
    if ext == :variants && candidates == :any
      query.gsub!(/:#{ext}/, "*")
    else
      query.gsub!(/:#{ext}/, "{#{candidates.compact.uniq.join(',')}}")
    end
  end

  File.expand_path(query, @path)
end
```

[Figure 4-6] The build_query function, where vulnerability occurs

Above is the content of the query modification function that causes the vulnerability. When the first query sentence fails to search the file, it enters. The file path is verified and modified through the escape_entry function, and the query statement is replaced with the Ruby method gsub to complete the query. In this process, the existing query and the Accept statement are used.

4) Query analysis

```
+ "/etc/passwd{{},}{+{},}{.{raw,erb,html,builder,ruby,coffee,jbuilder},}"
```

[Figure 4-7] Query generated by the vulnerability

[Figure 4-7] is a query made with the modified Accept in the query modification process of [Figure 4-6] and is used to search files. In the case of a normal query, "welcome.txt" is exposed at the front but in the process of query modification, the previous part is deleted by "../../../../" and it starts with "/ etc / passwd" part.

The query is used to search for the path ("/ etc / passwd"). This attack query is characterized by inserting "{{", closing the right square bracket to prevent screen output error. As a result, the file contents of the corresponding path are responded to.

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

File Content Disclosure on Rails (CVE-2019-5418)

05. Countermeasures

1) Web server log verification

```
Started GET "/igloosec_leebh" for 10.0.2.15 at 2019-04-09 11:17:39 +0900
Cannot render console from 10.0.2.15! Allowed networks: 127.0.0.1, ::1, 127.0.0.0/127.255.255.255
Processing by IgloosecLeebhController#index as HTML
  Rendering welcome.txt within layouts/application
  Rendered welcome.txt within layouts/application (16.2ms)
Completed 200 OK in 539ms (Views: 537.7ms | ActiveRecord: 0.0ms)
```

[Figure 4-8] Web server Puma normal console log

This is the normal console log for the default web server Puma used by Rails. It records the status of the user's connection requests and results. Then, the Controller records the file format requested by Accept and the response result thereof. [Figure 4-8] is a normal console log that shows the welcome.txt file when sending a response request in an HTML format to igloosec_leebh Controller.

```
Started GET "/igloosec_leebh" for 10.0.2.15 at 2019-04-08 09:19:27 +0900
Cannot render console from 10.0.2.15! Allowed networks: 127.0.0.1, ::1, 127.0.0.0/127.255.255.255
Processing by IgloosecLeebhController#index as ../../../../../../../../etc/passwd{{
  Rendering /etc/passwd
  Rendered /etc/passwd (0.5ms)
Completed 200 OK in 16ms (Views: 14.5ms | ActiveRecord: 0.0ms)
```

[Figure 4-9] Web server Puma abnormal console log

[Figure 4-9] requests igloosec_leebh Controller to output the file format ../../../../../../../../ etc / passwd {{ and a console log showing the / etc / passwd file in response to the server response. If you check the accept parameter after as in the console log of the web server, you can see whether the attack parameter has been attacked.

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

File Content Disclosure on Rails (CVE-2019-5418)

2) Inserting the MIME filter phrase

```
79                else
80                  [Mime[:html]]
81                end
82  +
83  +             v = v.select do |format|
84  +               format.symbol || format.ref == "*/*"
85  +             end
86  +
87                set_header k, v
88              end
89            end
```

[Figure 5-10] MIME-limited source code addition

The directory to the file is actionpack / lib / action_dispatch / http / mime_negotiation.rb, and add the source code that limits the MIME type under line 81 of the source code. The code checks the registered MIME type or * / * format. You can avoid the Accept attack syntax by adding the statement in the server-side source code.

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

File Content Disclosure on Rails (CVE-2019-5418)

3) Performing updates

[Figure 4-11] Rails security patch notice

Above is the vulnerability uploaded on March 13, 2019 through a version update. Since the release of Rails in 2004, the vulnerability was first reported in the Controller's Render file in March 2019, so all previous versions are vulnerable. In order to prevent the vulnerability, update to 4.2.11.1, 5.0.72, 5.1.6.2, 5.2.2.1, 6.0.0.beta3 where security patches have been performed.

06. Reference

[1] [rails] 레일즈란? https://jinbroing.tistory.com/18
[2] Rails 4.2.11.1, 5.0.7.2, 5.1.6.2, 5.2.2.1, and 6.0.0.beta3 have been released!
https://weblog.rubyonrails.org/2019/3/13/Rails-4-2-5-1-5-1-6-2-have-been-released/
[3] Ruby on Rails 路径穿越与任意文件读取漏洞分析 - 【CVE-2019-5418】
https://xz.aliyun.com/t/4448
[4] CVE-2019-5418 - File Content Disclosure on Rails, Github https://github.com/mpgn/CVE-2019-5418

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

CHAPTER 5

Special Column

Artificial intelligence from a cyber security point of view

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

Artificial intelligence from a cyber security point of view

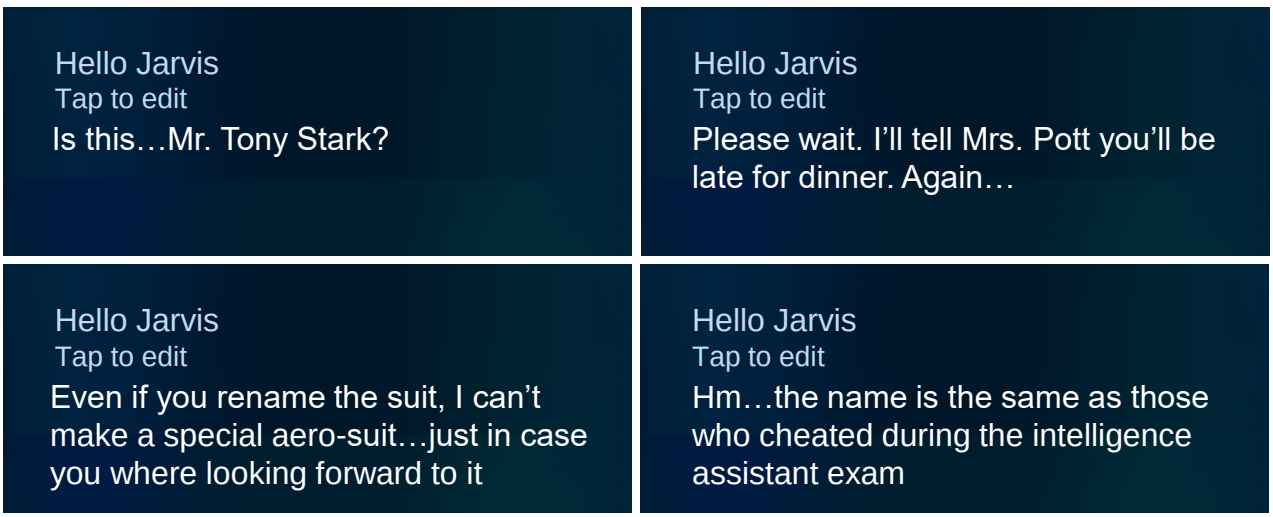
Security Monitoring Center
Security Analysis Team

01. Synopsis

It did not seem possible that Artificial Intelligence would arrive so quickly when Tony Stark was playing around with his AI Assistant Jarvis in the movie Iron Man (2008). Nowadays, "Artificial Intelligence" has become familiar and easy to access through various systems such as smartphones (Shiri, Bixby) and artificial intelligent speakers (Cacao Mini, Naver Clover, etc.).

Artificial intelligence, which we commonly think of, is a highly developed intelligent machine that thinks and acts like in the movies while also threatening humans, or falling in love with them. However, in reality, the technology is not as advanced as we think. This gap is causing much confusion for those studying artificial intelligence.

Artificial intelligence, which is now integrated into our lives, do not think and act like most humans, but solve problems with certain patterns. For example, if you say "Hello Jarvis" to Siri, the AI will respond "Are you Tony Stark?", "Wait a second. Contacting Mrs. Potts...' This is makes it seems like a conversation with artificial intelligence is possible, but in fact it is just an emulation of intelligence using a set of predefined rules.



[Figure 5-1] Examples of Siri's response trough predefined rules

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

Artificial intelligence from a cyber security point of view

▶ Why do we need AI?

At present, artificial intelligence is being actively studied in various fields because it is expected to replace human "labor" rather than to replace "humans" themselves. In other words, there are positive effects such as saving time and money, processing speed is much faster than humans in the areas where correct answers or conclusions are determined, and showing almost same level of processing results.

Due to the amendment of the Labor Standards Law in South Korea, legal working hours have been restricted from 68 hours a week to 52 hours a week. As a result, companies have been burdened with inputting manpower and a culture of Work and Life balance has emerged. Therefore, a tendency to avoid 24 hour shift jobs has followed such as security monitoring jobs, which leads to a higher necessity of artificial intelligence within the cyber security industry. Even in 2025, global data size is projected to increase by about 10 times, and it would be inconvenient to solve massive amounts of data monitoring and processing with limited resources.

In particular, it is safe to say that the introduction of artificial intelligence in the cyber security industry is ultimately for "automated work". Therefore, in order to construct a system that automatically processes the tasks that were priorly performed by a person before the introduction of artificial intelligence, processes which were taken for granted such as event analysis method, (a standardization of the work process) need to be established, the processing of false positives / true negatives / false negatives, report format, reporting hierarchy, thus a "standardization of the work process" needs top be established.

When these series of processes are properly performed, we can think about the artificial intelligence research specialized in the cyber security industry and how to use it.

02. Things to consider when implementing artificial intelligence in cyber security

Have you ever felt that the flavor of vending machine coffees vary depending on the machine? All the coffee may taste the same, but the proportion of coffee in the vending machines is slightly different. While drinking coffee that meets my taste people may think about "What is the ratio of beans, sugar, and prima to that of the coffee maker?", "Why does the vending machine coffee installed in our company taste bad?".

Gangneung coffee street, which is famous for vending machine coffee, is said to have become a famous place for people who have not forgotten the coffee flavor of vending machines installed there since. In fact, the coffee from the vending machine in Gangneung may be more delicious than drinking elsewhere because of the romantic atmosphere of drinking while gazing at the sea or the word of mouth from many people. However, in order to make the coffee taste unique, the Gangreung vending machine coffee's ratio of bean, sugar, and prime could have gone through several times.

Like the coffee being made from a trial and error method to make the best tasting coffee, artificial intelligence research is also similar in that it implements the optimal artificial intelligence algorithm with many studies to get an accurate results. Especially, in the field of cyber security, continuous research on algorithms is very important because 'true positive rate' and 'false positive rate' are different depending on which algorithm is being used.

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

Artificial intelligence from a cyber security point of view

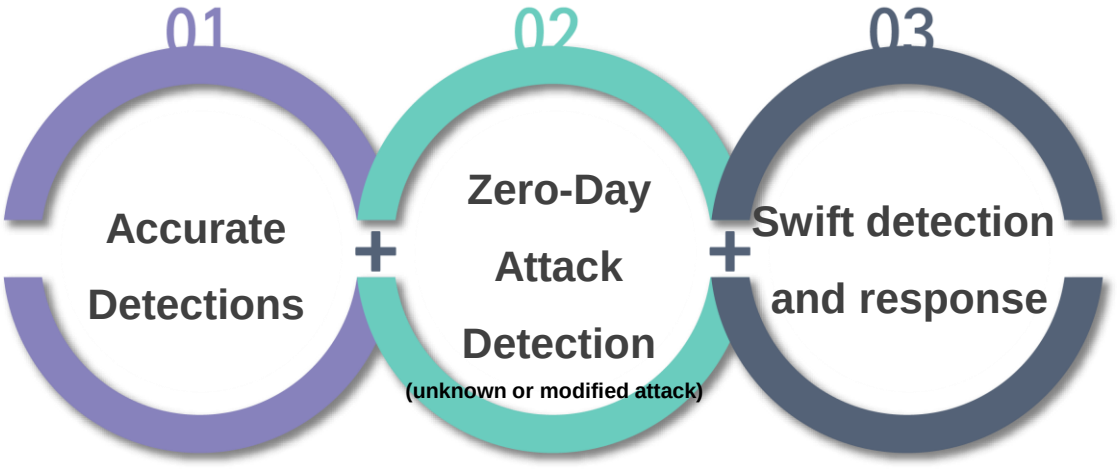
Artificial intelligence algorithms can be classified according to the type of data, how they learn, and the method of deriving the result. There are two ways in which the machine learns. It is called autonomous learning (unsupervised learning) to learn using a data set (hereinafter referred to as learning data) that already knows the result, and learning with data whose result is unknown.

We mainly use the supervised learning algorithm when predicting the result of new data or when judging the kind of data, such as when judging whether a new e-mail sent is spam or not. And we use a lot of supervised learning algorithms to group clusters that have similar characteristics using sample data which we do not know the result of.

Supervised Learning	▪ Learns through provided answers ▪ Utilized on prediction models etc.	SVM
		Artifical Neutral Network
		Naïve Bayes
		Linear regression
Unsupervised Learning	▪ Is not provided with answers ▪ Utilized during clustering	K-means
		DBSCAN

[Table 5-1] Different types of algorithms depending on the method of learning

As mentioned above, in order to complete the delicious coffee, it is necessary to satisfy the following three points: bean, sugar, and prime. Such is the same with cyber security, 3 points have to be satisfied.



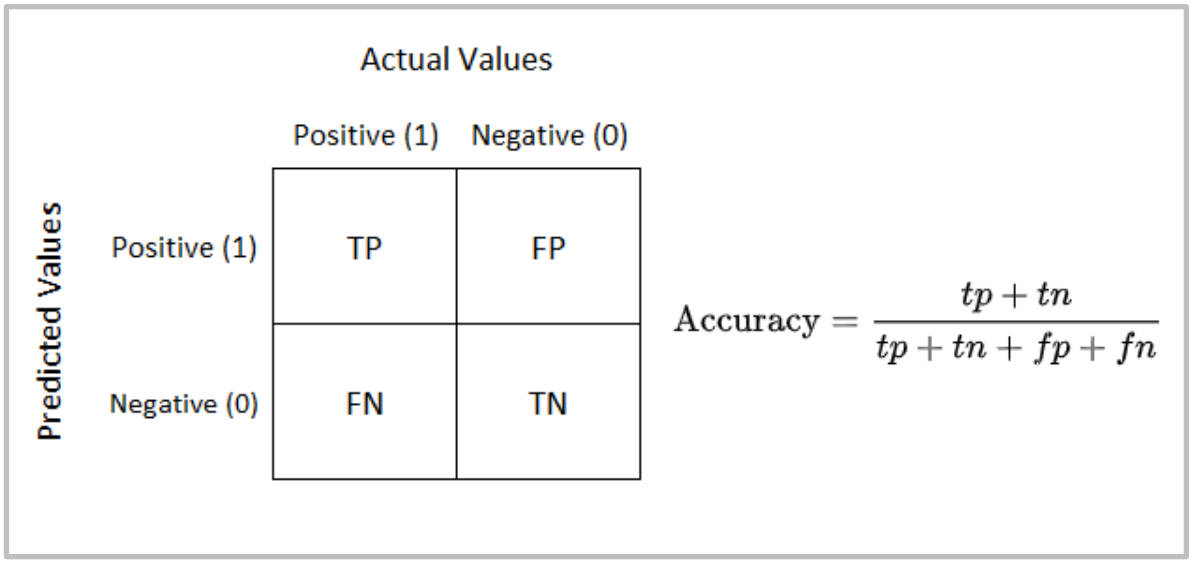
[Figure 5-2] Conditions to implement an AI system

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

Artificial intelligence from a cyber security point of view

▶ Algorithm for accurate detection

Accuracy refers to the probability of detecting an actual attack while not detecting it when it is a normal packet. Therefore, considering the accuracy, it is more desirable to use a learning algorithm that learns data with a clear answer.



[Figure 5-3] How to calculate accuracy

However, there is a possibility that the overlaying phenomenon may occur if the composition ratio of the learning data set (the ratio of the normal data and the abnormal data) is excessively biased to one side. In addition, there is a limitation that a person must directly perform a labeling operation to match a result of a learning data set, and in some cases, a wrong learning result is obtained when learning is carried out with mislabeled learning data.

These problems are basically expected to be overcome if there are enough learning data sets. Most importantly, however, is accurate labeling of prepared learning data sets. These are followed by realistic limitations that require a considerable amount of time, money, and expertise.

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

Artificial intelligence from a cyber security point of view

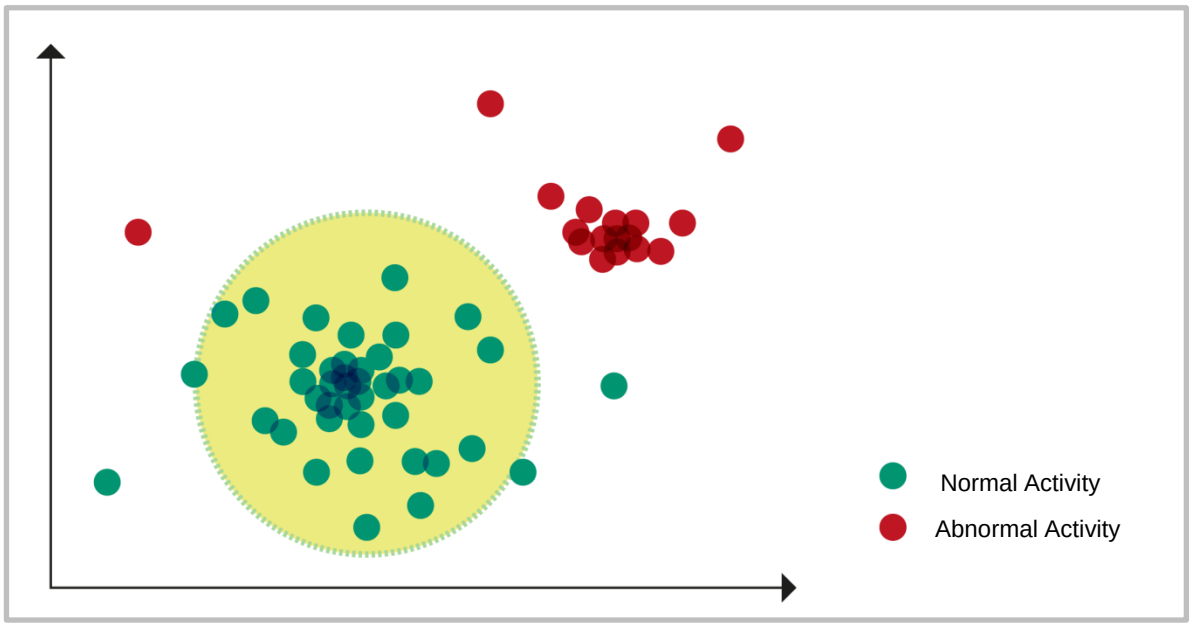
▶ Algorithm for detecting zero-day attacks (unknown or modified attacks)

There are various types of behaviors that are not standardized. The attacks hidden between these activities are difficult to detect through known "signatures". However, using an autonomous learning algorithm that extracts patterns and structural features of data and clusters of behaviors of similar characteristics will be effective in selecting these unknown attacks.

In recent years, there have been a number of security solution products that incorporate autonomous learning algorithms and sandbox technology to efficiently detect zero-day attacks and modified attacks are prevented from being detected by security devices. In particular, when is comes to EDR products detecting abnormal behaviors from servers and normal user devices, not only can cyber attacks such as malicious codes and ransomwares be detected, but also access to file which need a specific authority such as having employee clearance from their PC can be detected as well.

However, the autonomous learning algorithm does not have the answer to true/false, but it is hard to judge whether the bundle belongs to the normal behavior or the abnormal behavior because it bundles data with similar characteristics.

Thus, there is a limitation that normal activities must be preceded in order to effectively distinguish between normal activities and abnormal activities.



[Figure 5-4] Example of clustering

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

Artificial intelligence from a cyber security point of view

▶ Why Rapid Detection and Response is needed

Rapid detection and response is an integral part of cyber security. In the past, when an abnormal behavior was detected by security devices, the analyst analyzes the content to determine whether it is malicious, whether it has infringed, and its influence. If it is determined to be malicious, new detection patterns or signatures are generated based on the analyzed contents and then applied to the security solution. Most of these processes have different managers for each procedure, and time is frequently (unintentionally) wasted when the case is transferred from one manager to another. In addition, there is a possibility that analysis may differ depending on the competence of the analyst.

These problems are expected to be solved naturally if the process becomes "automated". No time will be wasted between procedures. In addition, there is a considerable advantage in temporal shortening, such as simultaneous analysis and simultaneous updating of patterns of new attacks in real time, enabling quick response.

03. Conclusion

Through the study of artificial intelligence, it is questionable whether AI is different from current big data-based detection methods. In terms of detection based on "attack pattern", it may feel that detection through artificial intelligence is not much different from existing detection methods, but "intelligence" is merely the advantage of artificial intelligence. In the past, if the detection pattern and the rule policy had to be manually checked and generated, there would be an "automatic modeling" process in which the detection through AI automatically learned the given pattern data and generated a detection pattern and a policy. There is a big difference between the two. This process can save time and money as well as guarantee efficiency through automation.

Of course, in today's rapidly changing world, "perfect automation" will face many difficulties. However, if continuous investment is made, such as studying advanced algorithms and cultivating professional talent to supervise the technology, one day we may be able to witness the AI we see in movies.

04. Reference

[1] Machine Learning Based Malicious Code Analysis Algorithm Suitability Study, Seoul National University of Science and Technology Industry-Academic Cooperation Foundation, Korea Internet Development Agency_2017

[2] Trends and Future Tasks of Security Management System Based on Artificial Intelligence, Department of Cyber Security, Ajou University_2017

[3] Introducing research on malicious file detection by overseas companies using machine learning, security technology research team_2018

[4] A Comparison of Intrusion Detection Effects Using SVM and Artificial Neural Network, Journal of the Korean Academy of Science Technology, Vol. 17, No. 2_2016

[5] , Machine Learning Infrastructure Infringement Analysis Attack Analysis Study, Gachon University Industry-Academic Cooperation Foundation, Korea Internet Development Agency_2017

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

CHAPTER 6

Focus On IGLOO Security

1. Japan IT Week Spring 2019
2. 2019 Partner Day launch

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

Focus on IGLOO Security

IGLOO Security Co., Ltd participates in Japan IT Week Spring 2019

Igloo Security participated in 'Japan IT Week Spring 2019' which was held in Tokyo Big Sight Aomi Hall from May 8th to the 10th. Japan IT Week Spring is one of the largest IT conferences in Japan with 1180 companies from all over the world and 80,000 visitors from all over the world. This year's event was held twice, and IGLOO Security participated in the second exhibition, which consists of 11 exhibitions.

This exhibition was conducted with IGLOO Secutiy partner Cyber Fortress (CFI), which introduced the SIEM solution SPiDER TM AI edition. Cyber Fortress (CFI) introduced Monitored Security Service (MSS) which received great attention from participants.

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

Focus on IGLOO Security

The 2019 IGLOO Security Co., Ltd Partner Day launched

Igloo Security hosted the 2019 IGLOO Security Partner Day at its headquarters on Thursday, May 9th. Twenty-seven key partners participated in this event to strengthen relationships and identify each others' needs. The event introduced our partners to AI-based SIEM solution SPiDER TM AI edition and Smart [Guard]. Then the participants shared their opinions on the solution.

IGLOO SECURITY emphasized that recent security trends required a control solution with AI/machine learning technology as a practical alternative to overcome the limitation of human resources/technology due to the growing number and intelligence of cyber threats. Finally, the event was finished with a visit to IGLOO Security's SOC.

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

We Know SECURITY!

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

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

Edited by IGLOO SECURITY Marketing Team
© 2019 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.