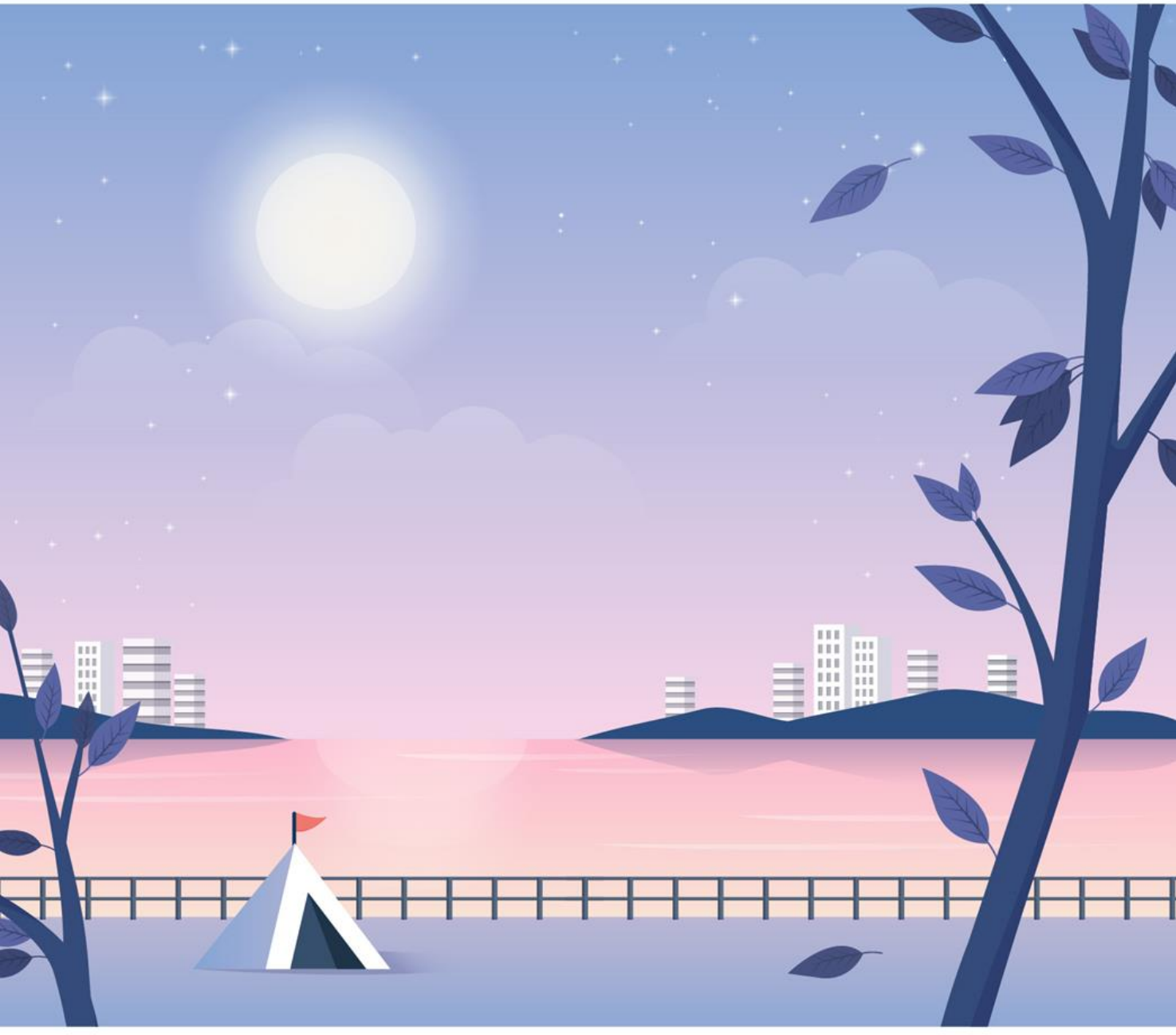
Monthly Security Report

2020
June



Cover Story

Enhancement of infringement response capacity through IP blocking function

webshell pattern collection, inspection script execution and analysis method by type

IGLOOSECURITY

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

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

Cover Story

1. Monthly Security Issue

- Security Issue

2. IGLOO Statistics

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

3. SIEM Guide (SPiDER TM V5.x)

- Enhancement of infringement response capacity through IP blocking function

4. Tech Note

- webshell pattern collection, inspection script execution and analysis method by type

5. 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

Microsoft's GitHub account hacked and 500GB developer data leaked

- It turns out that someone has successfully hacked into Microsoft's GitHub account and took 500 GB of data.
- It is known that the leaked data are Microsoft's development information and confidentiality, which is shocking the industry.
- A hacking organization that identified itself as Shiny Hunters released 1 GB of data and screenshots to the Dark Web forums and media outlets, claiming that they had infiltrated Microsoft's GitHub account.
- There was also a voice of suspicion that they were making false claims, but when they looked at the code samples, experimental projects, and various e-book information they released, opinions seemed to be convinced that the Microsoft account was hacked.
- GitHub is a software development and code sharing platform favored by about 40 million developers, acquired by Microsoft in October 2018 for $7.5 billion.
- Microsoft has not yet announced its official position.

Money laundering targeted for COVID-19 unemployed

- An attempt was made to launder hacking funds using people who lost their jobs due to the recession caused by COVID-19.
- According to security firm Fish Labs, the situation has been caught by cyber attackers sending emails saying that they will "make $5,000 a month through remote work" against Americans and Canadians.
- When the recipient of the mail responded to this, the hacker appeared to be offering an illegal money transfer method to receive money from the hacking victim and deliver it to the hacker.
- Other forms of e-mail have also been found that impersonate US financial firm Wells Fargo to provide jobs where both remote and external work can be provided. Likewise, it was sent to recruit illegal funds.
- The United States' Federal Bureau of Investigation (FBI) says it is trying to recruit illegal money carriers using unemployment anxiety and fear.

RSAC 2021, postponed to May 2020... Due to COVID-19 pandemic

- The RSA conference, the world's largest security event held in February every year, will be held in May next year.
- The RSA conference announced that it decided to hold the RSA 2021 on May 17, taking into account the continued occurrence of COVID-19 infection worldwide.
- In the case of RSA 2020 held this year, it was held as an offline event. Two participants from the participating companies appeared after the event.

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

1 Security Issue

Qatar's COVID-19 tracking app leaks of more than 1 million citizen’s personal information

- Security vulnerabilities in Qatar's COVID-19 tracking app “Eteraz” resulted in the leakage of personal and sensitive information from more than 1 million Qatari citizens.
- Experts pointed out that the authority required by the app is more than necessary, but the Qatar government has made it mandatory for all citizens to install the app.
- According to an investigation by the Amnesty International, it is unknown how long the vulnerability has existed and how many people have accessed this information.
- Although the Amnesty International has said that various privacy measures have been taken since the vulnerability was discovered and resolved, there are concerns that the central server does not have an information protection device and can track users' real-time location.

Ransomware attacks after data is extracted

- The number of cases where ransomware attacks are carried out after data is extracted is increasing rapidly. This is a method to achieve the desired purpose by threatening'to release information to the whole world' when victims do not pay the decryption cost requested by the attacker.
- Recently, a personal information of some employees leaked after a ransomware attack from Magellan Health, an insurance company that is a Fortune 500 company.
- According to the results of Magellan's investigation to Mandiant, the attackers sent a phishing email impersonating a customer and infiltrated it, revealing that they ran a ransomware attack after first extracting some employee data.

Phishing attack advisory disguised as a videoconferencing platform

- Phishing attacks that exploit videoconferencing platforms occur as COVID-19 continues to prolong.
- According to the checkpoint, phishing attacks disguised as video conferencing services such as Zoom, and Microsoft (MS) teams are rapidly increasing.
- Malicious emails disguised as requesting attendance are also spreading rapidly. This email, sent with the subject ‘You have been added to a team in Microsoft Teams’, contains the ‘Open Microsoft Teams’ icon, which can be downloaded by clicking on it.
- Security experts warn that the number of malicious domains and emails associated with COVID-19 and videoconferencing continues to increase.

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 of Vulnerability Attacks collected in June 2020, attacks using the Zyxel Remote Code Execution (CVE-2020-9054) vulnerability and RCEs such as DrayTek Vigor Remote Code Execution (CVE-2020-8515) and ThinkPHP Remote Code Execution Vulnerability The attack was found.

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

Rank	Pattern	No. of cases	Ratio(%)	Fluctuation
1	Zyxel Remote Code Execution (CVE-2020-9054)	1,135	21.30%	NEW
2	DrayTek Vigor Remote Code Execution (CVE-2020-8515)	755	14.17%	▼1
3	ThinkPHP Remote Code Execution Vulnerability	555	10.41%	▲1
4	phpMyAdmin sample page access	486	9.12%	▼2
5	WordPress sample page access	483	9.06%	-
6	SQL Injection	467	8.76%	▲1
7	URL extension access control	395	7.41%	NEW
8	MVPower DVR Shell Unauthenticated Command Execution	387	7.26%	▼5
9	Command Injection (Netgear Routers Vulnerability)	354	6.64%	▲1
10	Network Scanner(masscan)	312	5.85%	▼1
Total		5,329	100.00%	-

[Table2-1] TOP 10 monthly vulnerability attacks

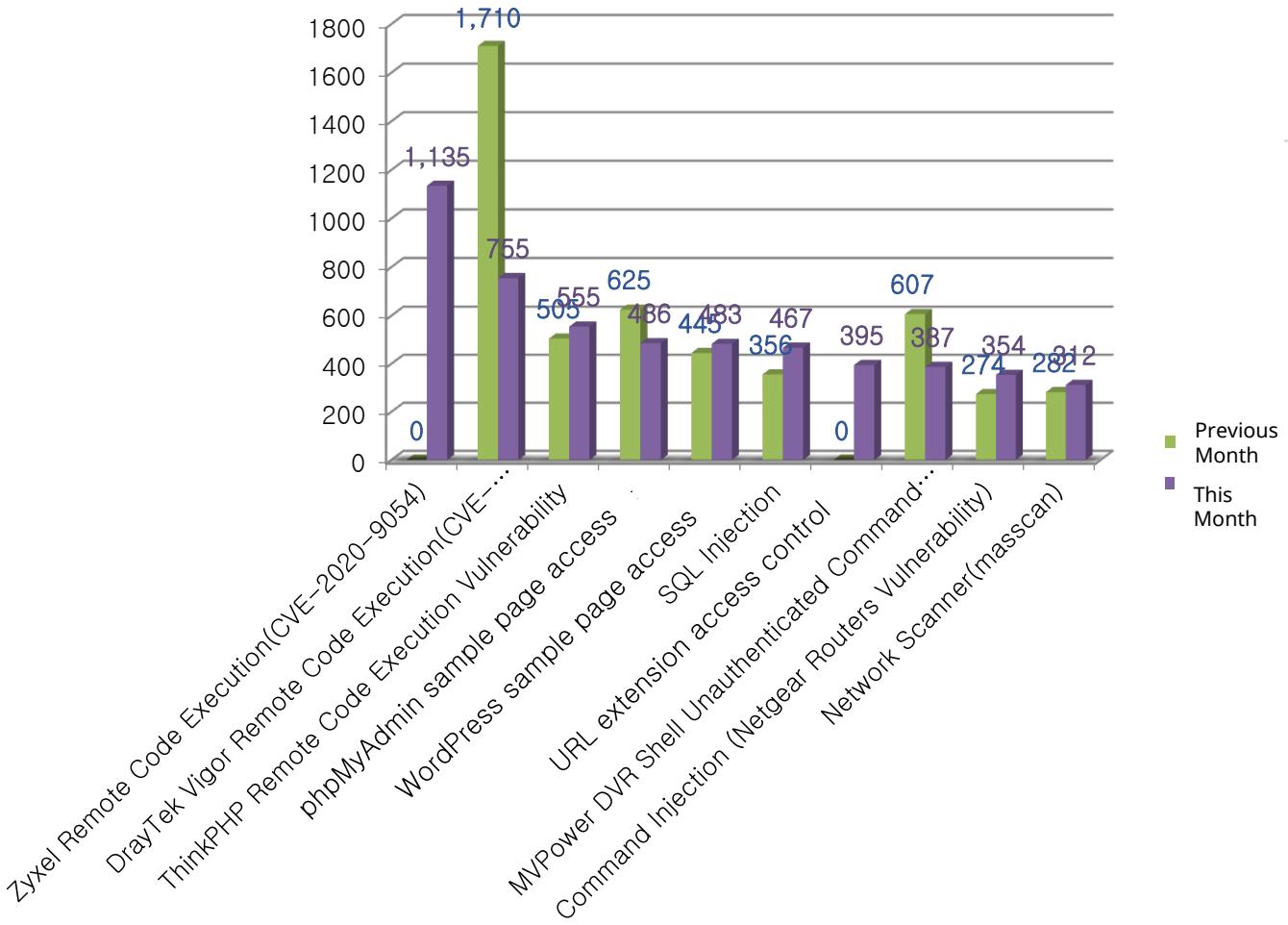
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

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 vulnerability event analysis collected for one month in June 2020, many attacks using Zyxel Remote Code Execution (CVE-2020-9054) and DrayTek Vigor Remote Code Execution (CVE-2020-8515) registered as new vulnerabilities in 2020 were detected. done. The Zyxel Remote Code Execution (CVE-2020-9054) attack is a new vulnerability that enables RCE attacks using the vulnerability in the weblogin.cgi file of the Zyxel NAS device.
The latest security update is released, and when using the device. So, firmware update is required.



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

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

1 Monthly attack service and trend analysis

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

03. Top 10 monthly attack service(port)

In the top 10 service ports collected in June 2020, events using ICMP (0/ICMP), SNMP (UDP/161), Telnet (TCP/23), and Unsigned (TCP/7178) ports rose from the previous month, and Unsigned (TCP/9900) ports are showing a decreasing trend compared to the previous month.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of cases	Ratio(%)	Fluctuation
1	HTTPS(TCP/443)	1,245,119,926	43.91%	-
2	DNS(UDP/53)	819,055,672	28.89%	-
3	Microsoft-DS(TCP/445)	239,714,297	8.45%	-
4	HTTP(TCP/80)	192,385,059	6.78%	-
5	ICMP(0/ICMP)	93,873,041	3.31%	▲1
6	SNMP(UDP/161)	93,442,641	3.30%	▲1
7	Telnet(TCP/23)	44,205,535	1.56%	▲1
8	Unsigned(TCP/7178)	37,581,961	1.33%	▲2
9	MSSQL(TCP/1433)	37,108,994	1.31%	-
10	Unsigned(TCP/9900)	33,012,848	1.16%	▼5
	Total	2,835,499,974	100.00%	-

[Table2-2] TOP10 monthly attack patterns

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

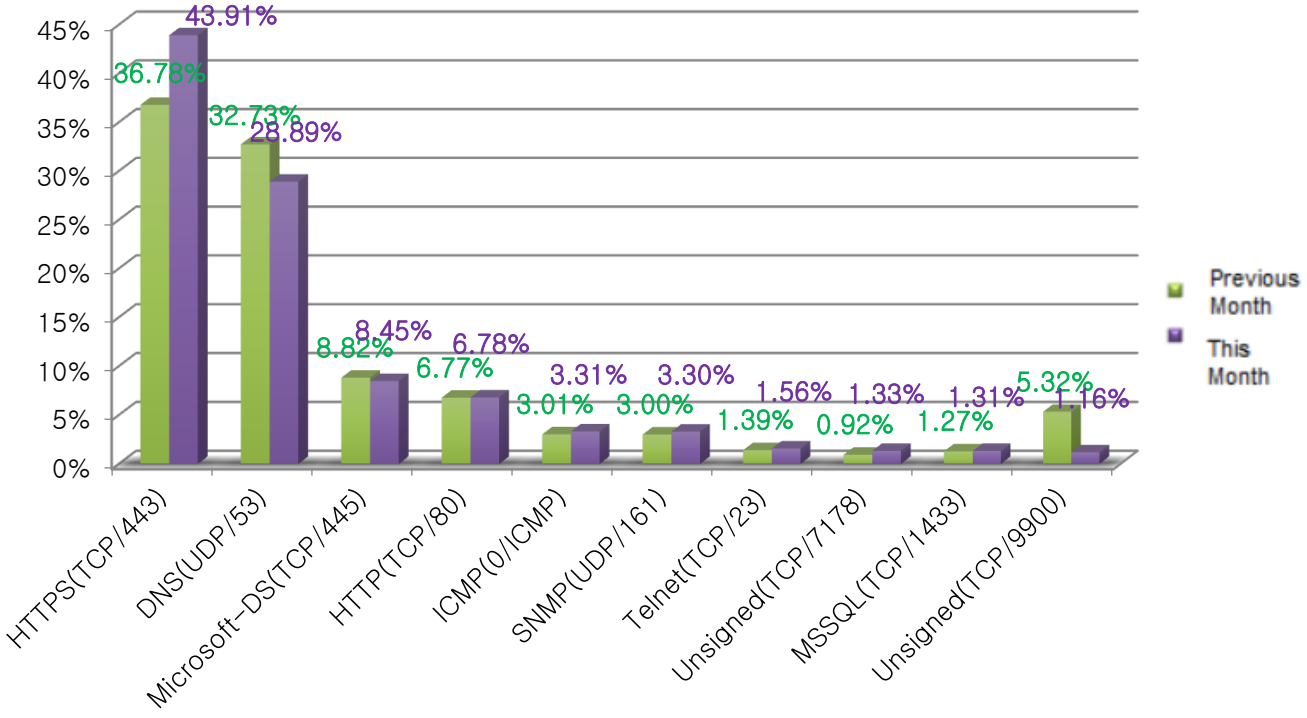
1 Monthly attack service and trend analysis

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

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

The analysis of the events collected in June 2020 confirms that the total number of cases decreased slightly from the previous month.

Events using ICMP (0/ICMP), SNMP (UDP/161), Telnet (TCP/23), and Unsigned (TCP/7178) ports increased from the previous month. Among them, it is recommended to disable ICMP configuration of security equipment and manage information not to be exposed through reply/request packet so that ICMP event is a protocol that is likely to be used for Sniffing, ICMP Redirection, and Spoofing attacks.



[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

Ack Storm, HTTP Login Brute Force, and Multi Packet Inspection event rankings rose slightly in the TOP10 attack patterns in June 2020, and the rankings of ACK Port Scan (F/W Scan) and Dcom_TCP_Sweep (MSBlaster Worm Messengr) events were confirmed to have decreased. Other UDP Tear Drop and FIN Port Scan events have entered the rankings.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	647,966,292	92.33%	-
2	Ack Storm	25,611,722	3.62%	▲1
3	HTTP Login Brute Force	8,680,504	1.23%	▲1
4	ACK Port Scan(F/W Scan)	6,609,726	0.93%	▼2
5	Multi Packet Inspection	4,726,052	0.67%	▲1
6	Dcom_TCP_Sweep (MSBlaster Worm Messenger)	4,514,050	0.64%	▼1
7	Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	2,167,696	0.31%	-
8	TLS Malformed Handshake DoS	876,310	0.12%	-
9	UDP Tear Drop	478,046	0.07%	NEW
10	FIN Port Scan	195,780	0.03%	NEW
	Total	707,647,602	100.00%	-

[Table 2-3] TOP10 monthly attack pattern

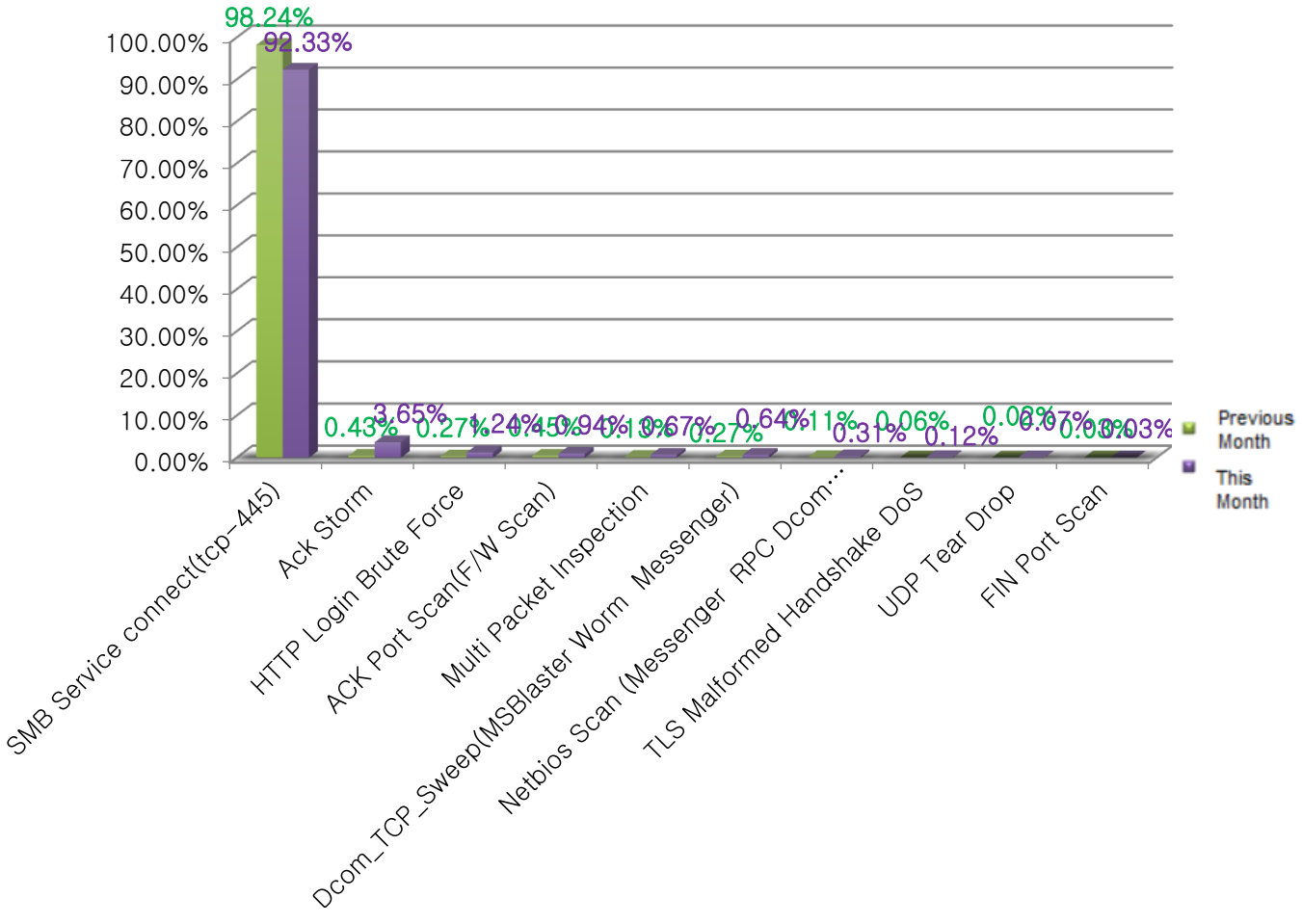
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

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

The number of SMB Service connects (tcp-445) compared to the previous month dropped significantly in the Top 10 Attack Patterns in June 2020, but it is still the No. 1 attack pattern that requires continuous access control management for SMB and Netbios service ports. The UDP Tear Drop and FIN Port Scan patterns are newly identified in the rankings, and most of the attacks in the TOP 5 ranking this month are confirmed to be scanning events such as Scan and Brute Force. We recommend security precautions such as grasping the status of unused ports accessible to the company and checking the password complexity of various devices and servers.



[Figure 2-3] TOP10 monthly attack pattern

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

2 Detailed analysis according to different patterns

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

Attack Pattern	Detailed Analysis Results
SMB Service connect(tcp-445)	Microsoft Windows uses SMB protocol to share files and printer resources with other computers. Sharing resources using SMB in older versions (95, 98, Me and NT) of Windows used TCP port 137 and 139 and UDP port 138 by executing NETBIOS with NETBIOS over TCP/IP. On older versions of Windows 2000/XP, it was possible to run SMB directly through TCP/IP on TCP port 445. If the files are shared with easily guessable password or passwords are not set, they can suffer from secondary attacks.
Ack Storm	Attacker sends a large amount of TCP / IP Ack signal to the target server, and the target server is an attack method that creates unnecessary load and delays normal service. This attack is also used to Hijacking the packet in which the Session is made.
HTTP Login Brute Force	This attack accesses the HTTP WEB service port(80) and repetitively inserts random strings through a Tool-Kit in order to find out the password for a specific ID(root, guest etc). Passwords which are easy to guess or are in an alphabetic/symbolic order are more prone to this attack. This attack can be prevented by using IDs and passwords over 6 letters and by Filtering data from the HTTP port(80/TCP).
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.
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.
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.
Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137)	NetBios checks each other's information through UDP port 137, establishes a session with TCP 139, and exchanges data through TCP 138. An attacker can use this UDP port 137 to establish a session with the target system and scan information about the folders and networks shared on the target system.
TLS Malformed Handshake DoS	TLS Malformed Hadnshake DOS attack is a type of DOS attack using a maliciously manipulated TLS packet. It occurs during the handshake of a maliciously manipulated TLS client. It is an attack that a remote attacker can cause a load on the victim system by sending a maliciously crafted TLS packet to the affected system.
UDP Tear Drop	If fragmentation occurs when the packet is normally transmitted, the offset value is added for accurate assembly during reassembly. This pattern is a type of DoS attack technique that paralyzes system functions by overflowing beyond the range by adding a value larger than the normal offset value using UDP.
FIN Port Scan	This method can be used as a faster alternative to the normal TCP port scan. It scans by observing the host's response to the TCP FIN packet to find the TCP port it is listening on. The target host uses the property of sending a response only when it is sent to the non-listening port when there is no response when the FIN is sent to the listening port. The port is checked without actually initiating a TCP connection.

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

Cover Story

CHAPTER 3

SIEM Guide (SPiDER TM V5.x)

Enhancement of infringement response capacity through IP blocking function

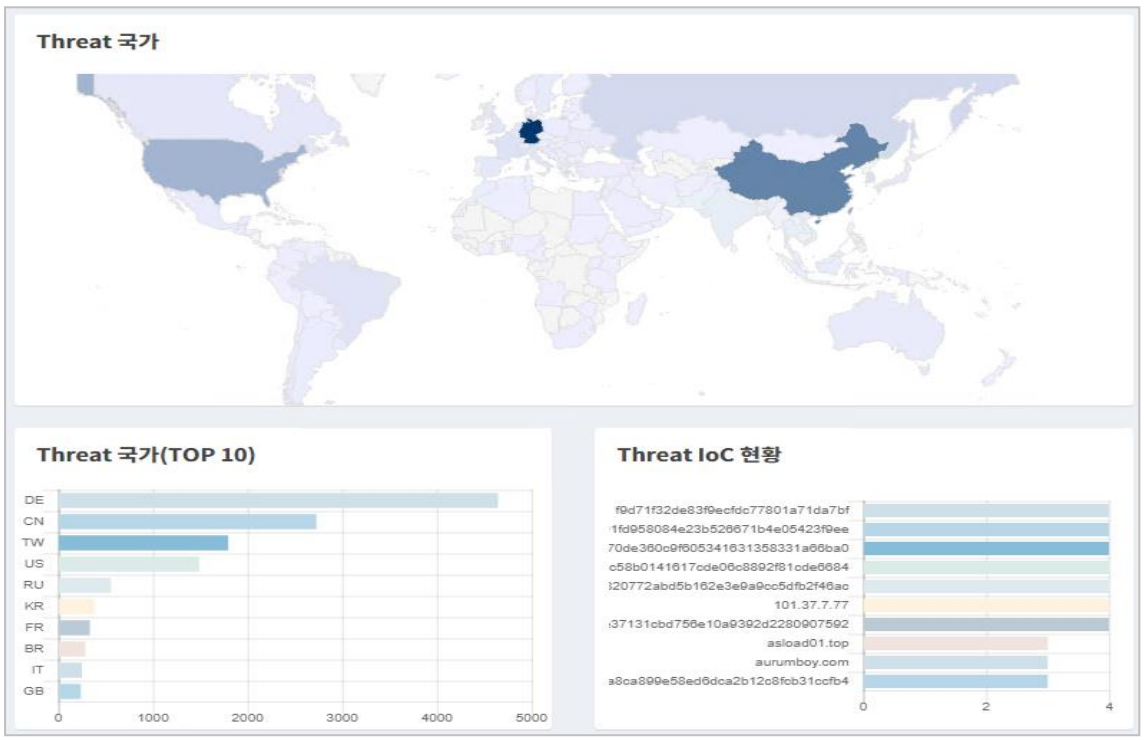
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Enhancement of infringement response capacity through IP blocking function

Technical Support Center
Analysis Technology Team

01. Overview

As major APT attack groups use new social engineering techniques in recent years, it is necessary to further strengthen the information sharing system to proactively respond to cyber threats. However, the cybersecurity center is struggling to block dozens or hundreds of IPs every day in order to respond to the increasing threat IPs. Our integrated security control system SPiDER TM V5.0 provides firewall blocking IP function to respond to intelligent and advanced cyber threats. Let's take a look at how to reduce the amount of security monitoring work using these functions.



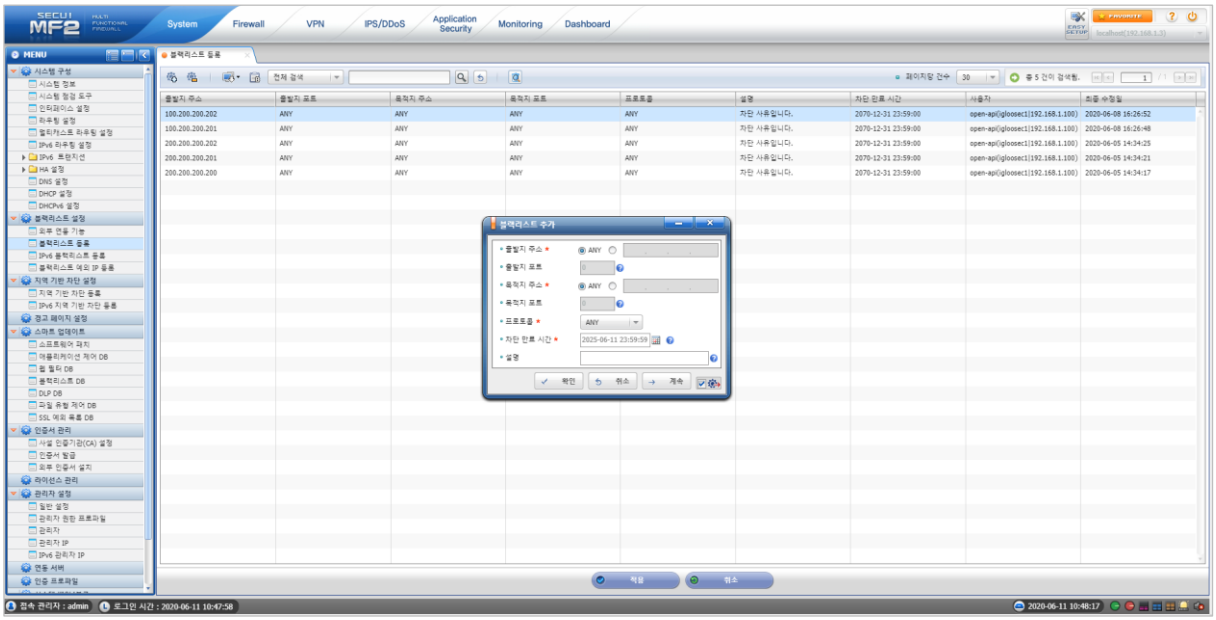
[Figure 3-1] IGLOOSEC Cyber Threat Intelligence

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

Enhancement of infringement response capacity through IP blocking function

02. What if possible in an integrated security monitoring system from detection to analysis and blocking?

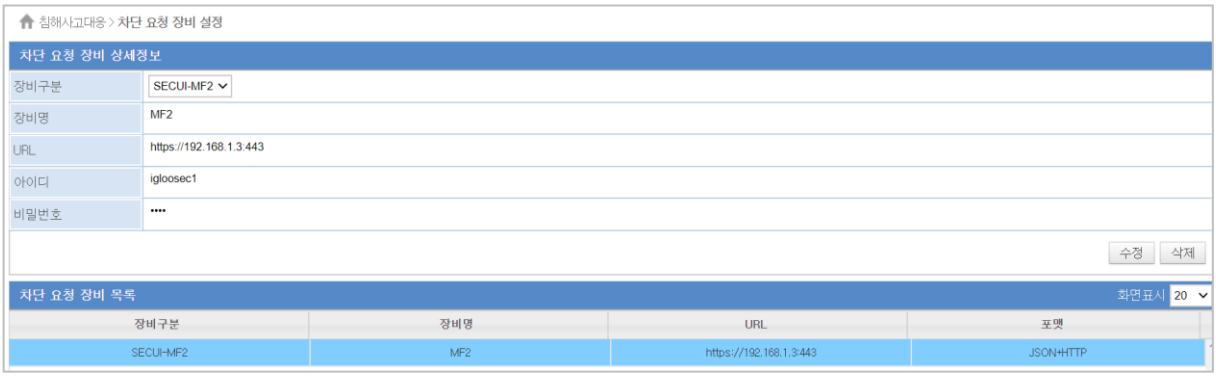
In the past, IP blocking of network devices had to be registered by individually accessing the firewall GUI in each network. However, as the number of firewalls increases, it takes a considerable amount of time to register harmful IPs in the firewall.



[Figure 3-2] MF2 Firewall Blocking IP Registration Screen

03. IP blocking function in SPiDER TM V5.0

If you enter only the device name, URL, ID, and PW information of the firewall, the integration setup is complete. (Multiple registrations are possible depending on the number of devices)



[Figure 3-3] SPiDER TM V5.0 blocking request device setting screen

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

Enhancement of infringement response capacity through IP blocking function

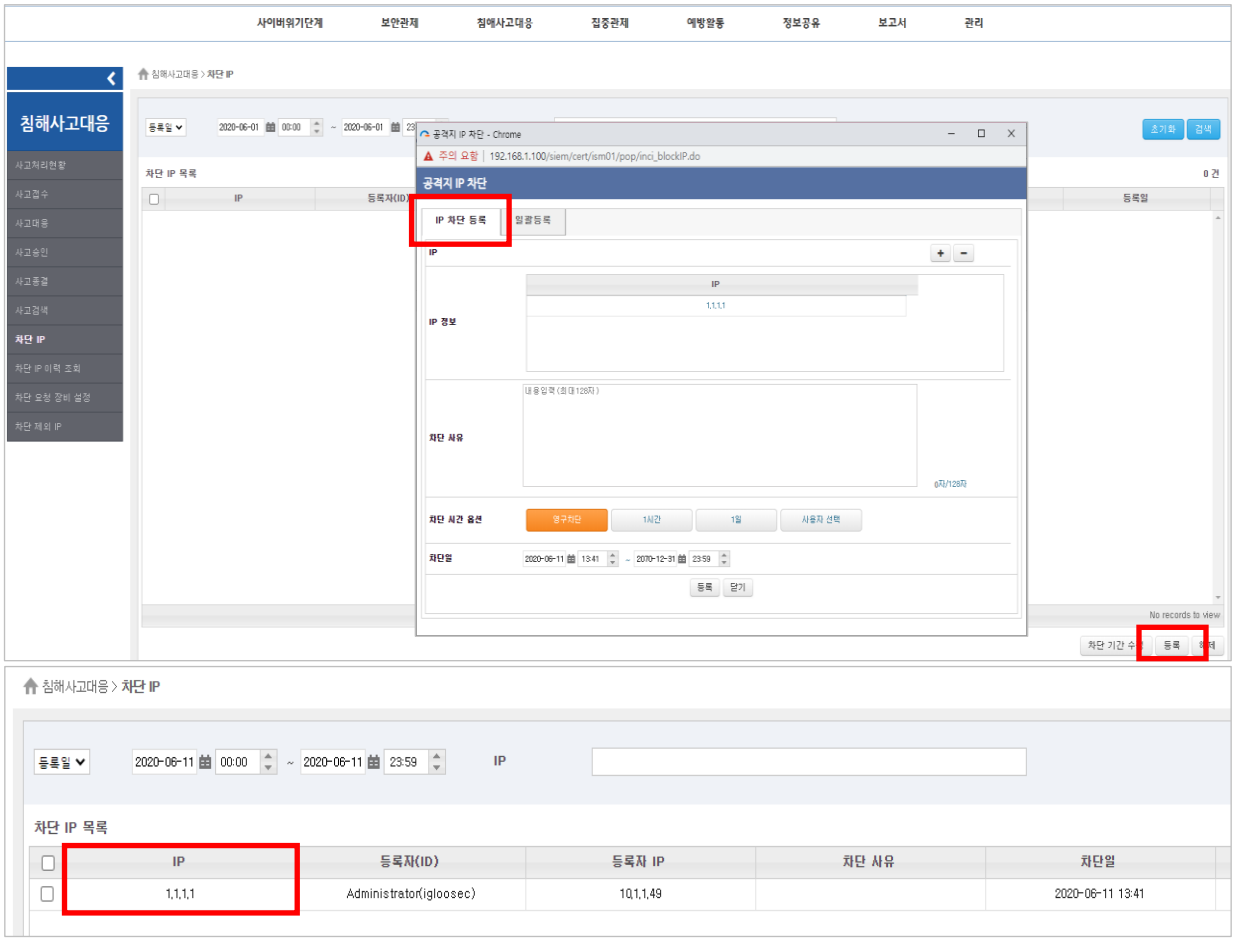
1) Single block IP function

Response to infringement incidents → Block IP → Register → Register IP Block

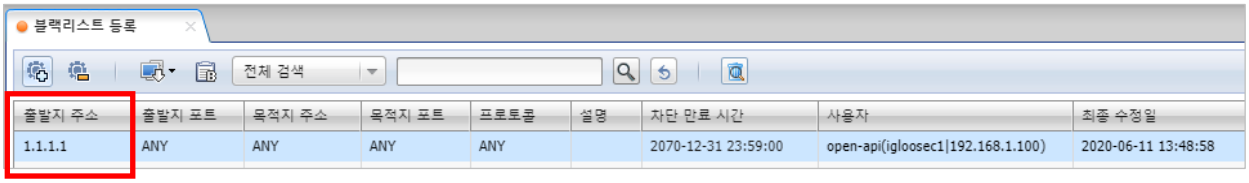
① IP: Block IP registration (band IP cannot be registered)

② Reason for blocking

③ Blocking time option: permanent (~2070.12.31), 1 hour, 1 day, user defined



[Figure 3-4] SPiDER TM V5.0 blocking IP registration and results



[Figure 3-5] Blacklist normal input result after accessing firewall UI

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

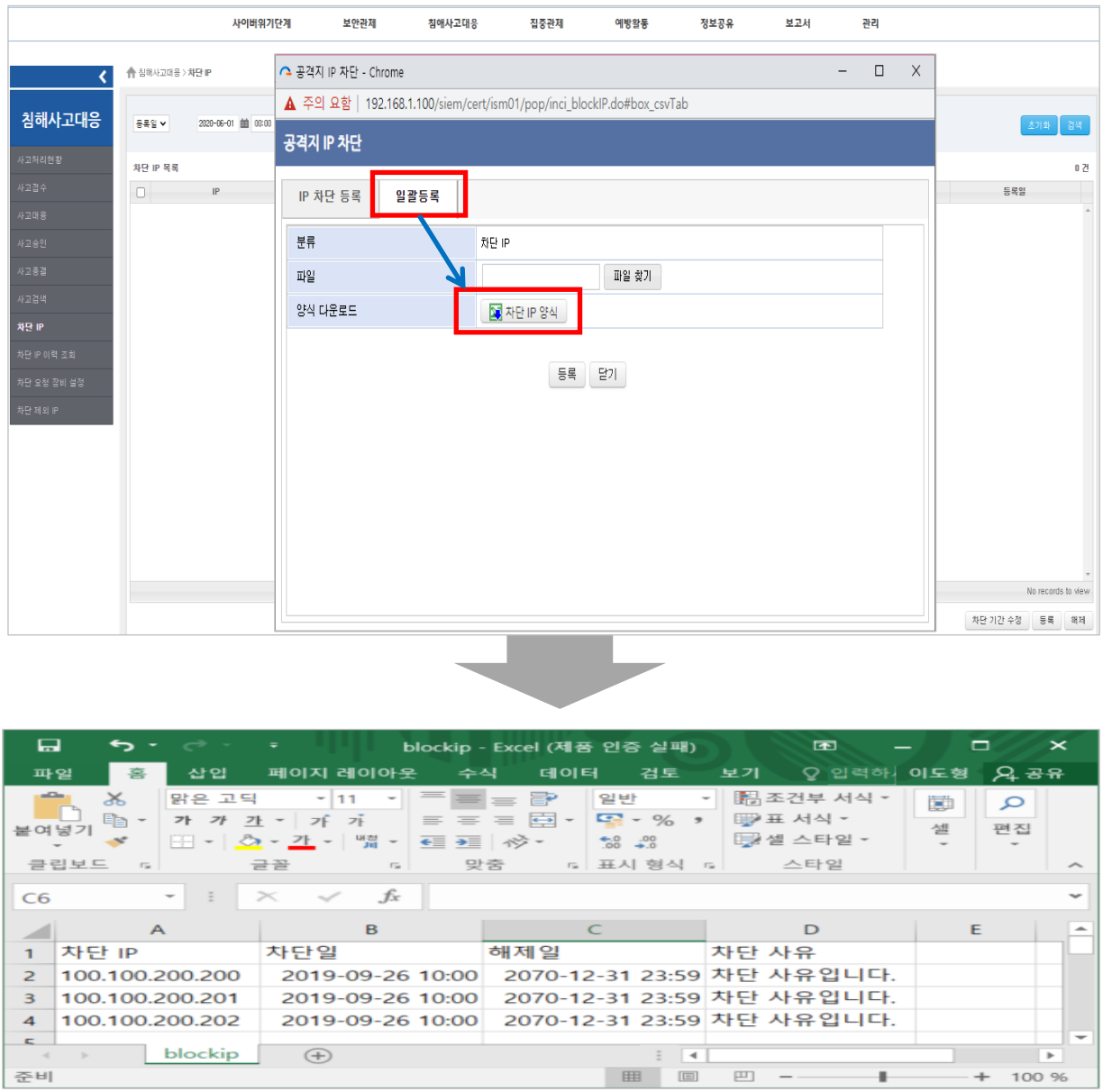
Enhancement of infringement response capacity through IP blocking function

2) Block IP batch registration function

Response to infringement incident → Block IP → Registration → Batch registration

To block multiple IPs rather than a single IP, download the “Block IP Form” and enter the information

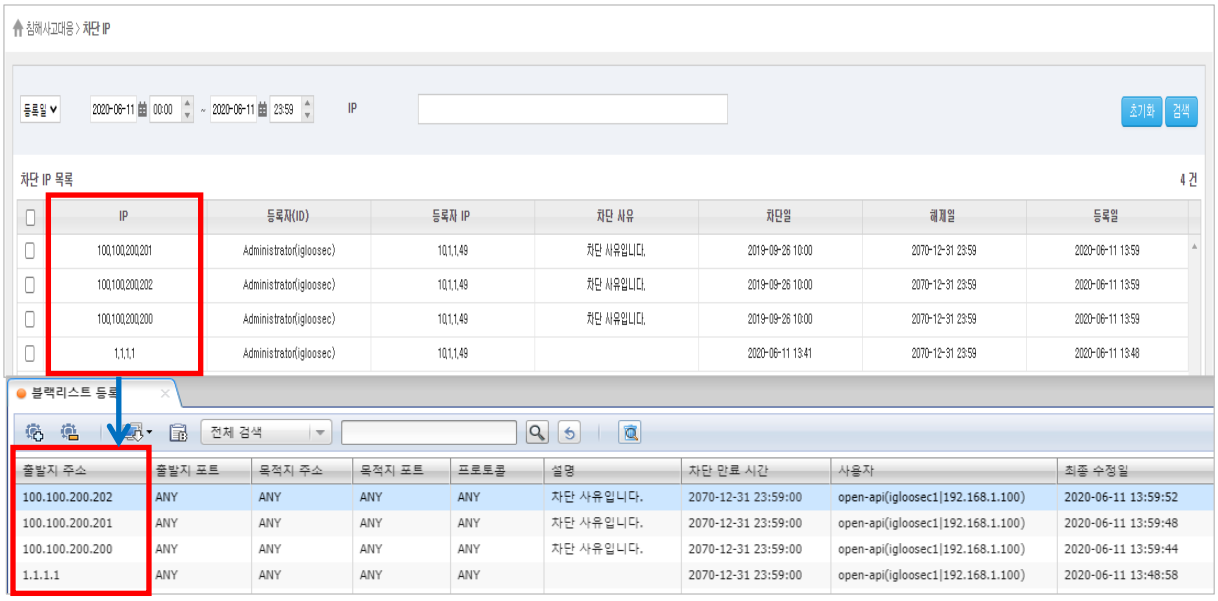
(Block IP, blocking date, unblocking date, reason for blocking) → Batch registration is possible by uploading the input CSV file



[Figure 3-6] SPiDER TM V5.0 blocking IP batch registration

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

Enhancement of infringement response capacity through IP blocking function

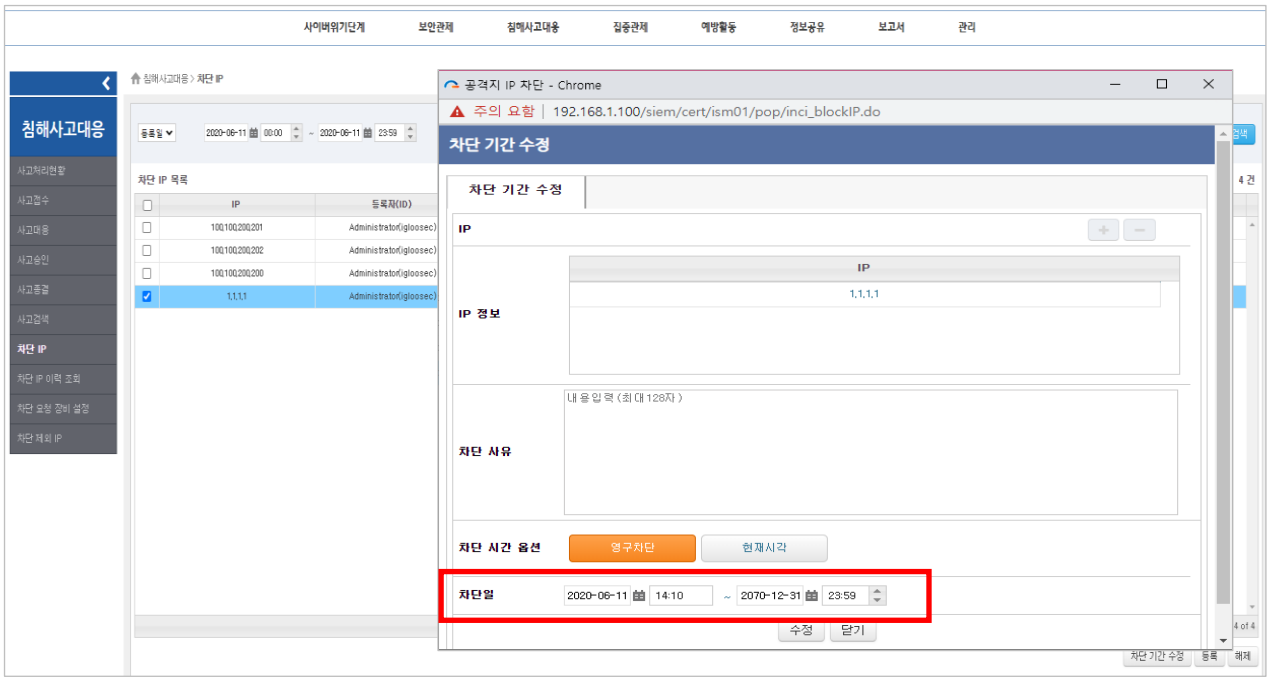


[Figure 3-7] SPiDER TM V5.0 Firewall Blocking IP Registration Result

3) Modify the IP blocking period

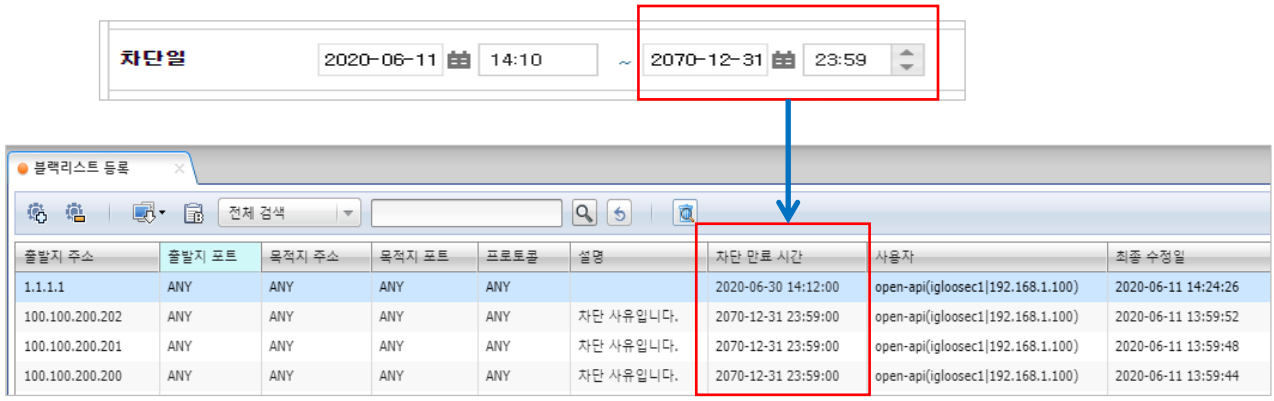
Response to infringement incidents → Blocking IP → Modifying blocking period

If the IP blocking date needs to be changed, it can be reflected in real time by modifying the blocking period (blocking date ~ unblocking date)



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

Enhancement of infringement response capacity through IP blocking function

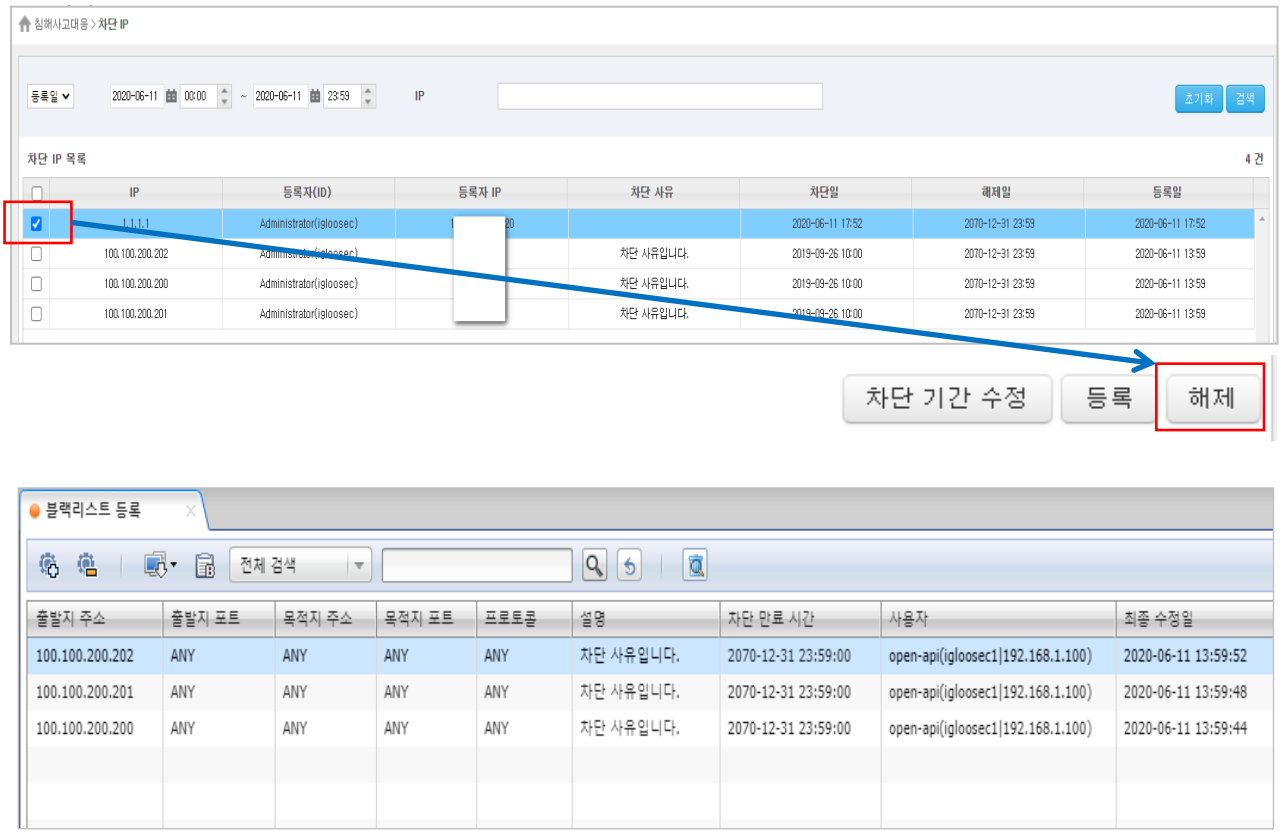


[Figure 3-8] SPiDER TM V5.0 blocking IP blocking date modification result

4) Unblock IP

Response to infringement incidents → Block IP → Unblock

Check the desired IP in the list of registered blocked IPs and click the unblock button to



[Figure 3-9] SPiDER TM V5.0 Firewall unblocking IP

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

04. Conclusion

In the meantime, despite blocking hundreds of thousands of IPs, we are entering a policy to block hundreds of thousands of IPs every day. If you estimate the time required for such an operation, the following figures will appear.

Malicious IP(n) x the required time (around 5 mins) x Networks(No. of firewalls) = Total required working hours

Apart from the existing work method, through the IP blocking function of the integrated security control system, it will be possible to more quickly and accurately process multiple network boundaries to increase work efficiency. In addition, in order to strengthen infringement response capability, it is necessary to actively collect information necessary for preemptive response, and it is recommended to actively utilize Cyber Threat Intelligence (CTI) information provided by igloo security.

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

Cover Story

CHAPTER 4

Tech Note

- webshell pattern collection, inspection script execution and analysis method by type

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

webshell pattern collection, inspection script execution and analysis method by type

Infrastructure Business Department
Management Division

01. Overview

The webshell is created to execute commands from the web page to the server using a simple server script (jsp, php, asp ..). These scripts are uploaded through a vulnerability in the web server to obtain the server's administrator privileges.

Even if the web is running on the server, if the vulnerability does not exist, the webshell will not work. Even if the webshell is uploaded, if it does not have execute permission, it will not run. However, when the vulnerability and execution authority of the webshell exist, the scope of the infringement can be widened by executing commands inside the server to leak key information, check source code, and falsify the homepage.

According to the Korea Internet & Security Agency (KISA), webshells were found in more than 90% of hacked servers.

Let's take a look at how to collect webshell patterns that can check these webshells, write and run inspection scripts, and analyze each websehll type.

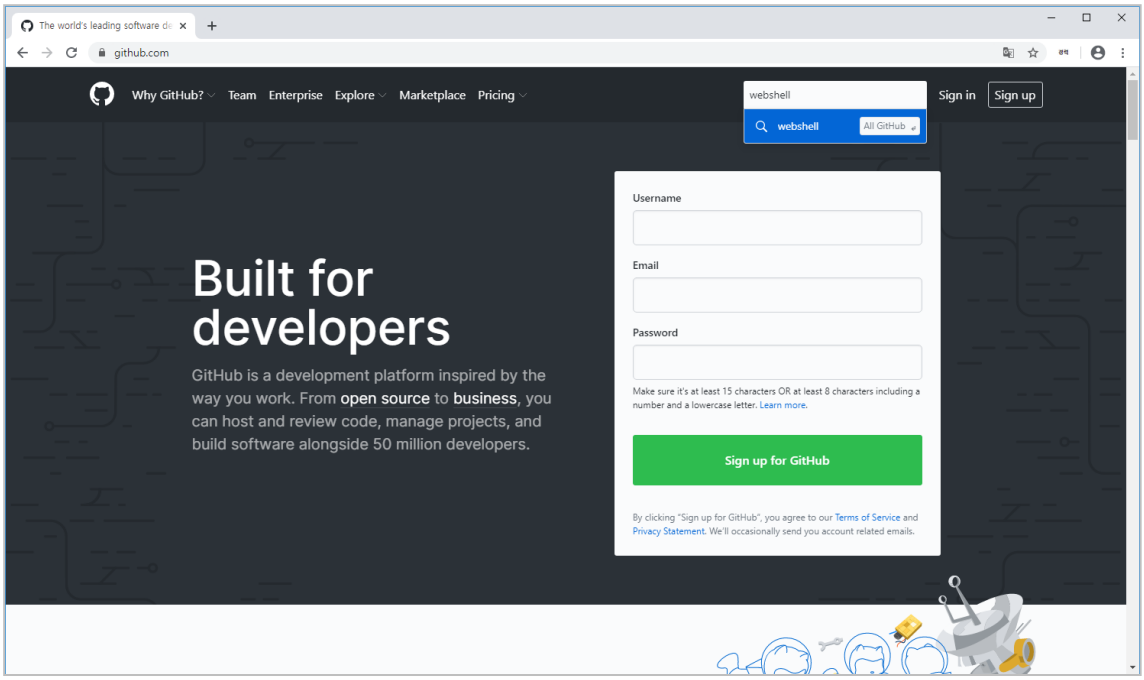
02. Collecting webshell search pattern

1) webshell keyword search

The company that performed the webshell inspection has a webshell pattern. However, if the inspection is performed for the first time, access the developer open community (https://github.com), enter webshell in the search keyword, and perform the search.

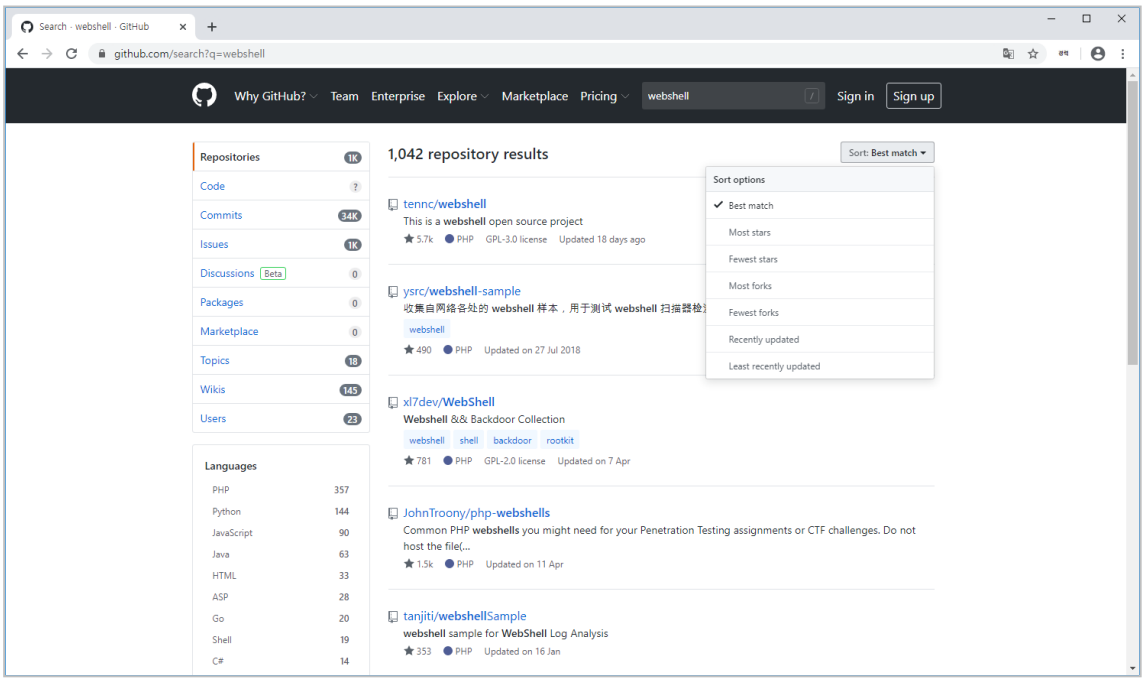
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

webshell pattern collection, inspection script execution and analysis method by type



[Figure 4-1] webshell keyword search

When searching, the search option can check the results corresponding to the best match.

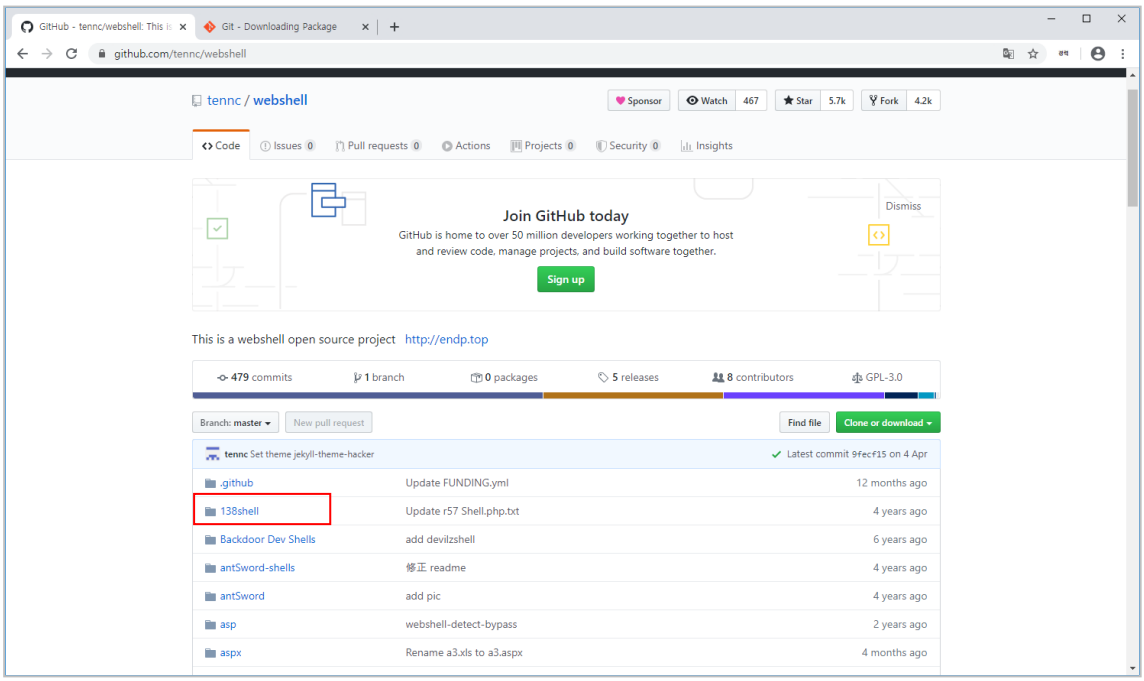


[Figure 4-2] webshell keyword search result check

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

webshell pattern collection, inspection script execution and analysis method by type

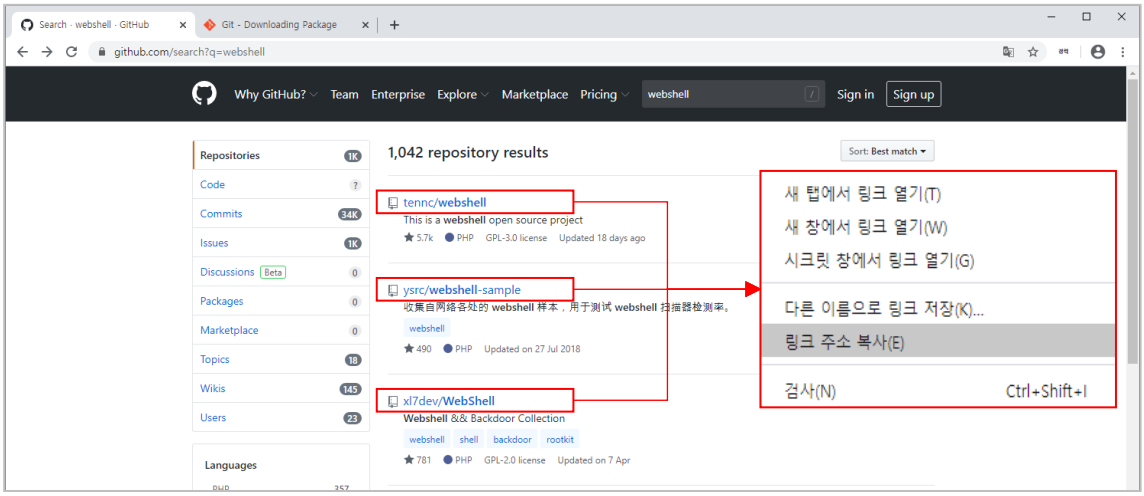
After directly accessing one link of the result (eg, tennc / webshell), check the source code and extract the string that determines the webshell from within the code.



[Figure 4-3] Extraction of strings judged by webshell from source code

2) Using the Git program

Since it takes a lot of time to check the string judged by webshell by checking the source code in each link, you can use the Git program to download multiple result links in bulk through link copy.



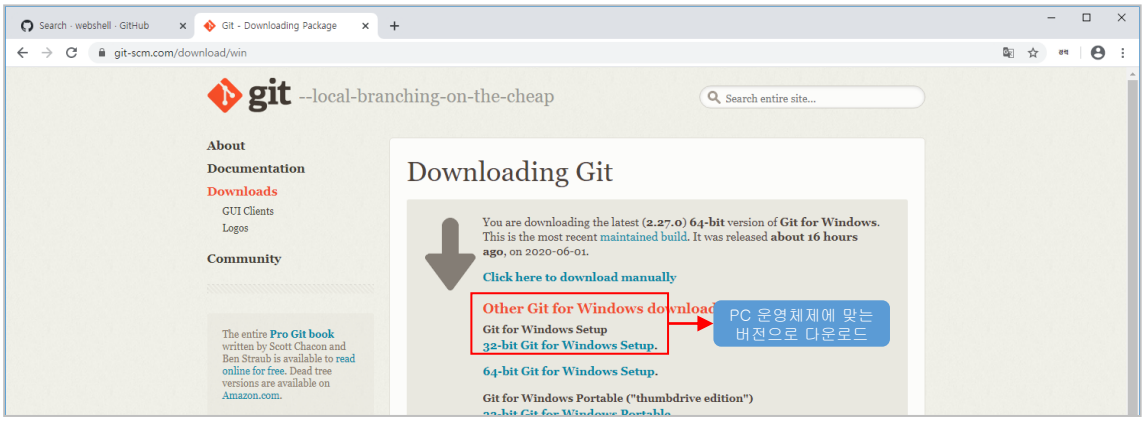
[Figure 4-4] Copy link address for the result link

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

webshell pattern collection, inspection script execution and analysis method by type

Download and install the Git program according to the operating system version from the link below.

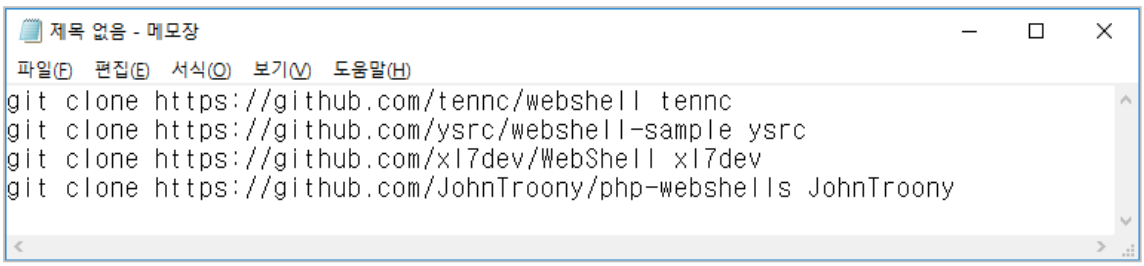
<Download path: https://git-scm.com/download/win>



[Figure 4-5] Git program download method

After installing the Git program, let's learn how to use the run command.

① Save the copied path in notepad as git command
- command : git clone [copied link address] [saved directory name]



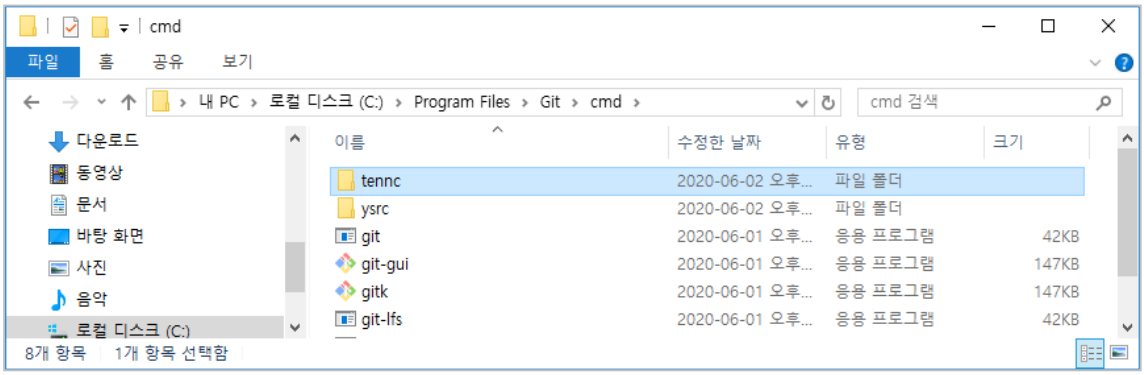
[Figure 4-6] Save the copied path in notepad as git command

② Go to the directory where the program is installed and execute the contents of Notepad with git command

[Figure 4-7] Notepad contents are executed with Git command

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

After executing the Git command, you can confirm that the directories for multiple output links have been created.



[Figure 4-8] Git command result check

3) Extracting webshell pattern

After reading the source code using a notepad program, etc., the string that can be added as a pattern is manually extracted, and the source code that is most likely to be developed in the form of a web shell is selected and extracted.

When extracting, it should be extracted in a pattern that the general source code developer does not think to use, and it should be noted that the false positive rate of the web shell inspection script may increase depending on which pattern is extracted.

Rank	Pattern type	webshell detection pattern examples
1	Known webshell file name	cmdasp.asp, jFolder.jsp, alihack.php, etc..
2	The specific signature left by the attacker, Email, etc..	h4cked, hacked by, by unknown, etc..
3	Main functions that can perform web shell functions	Script.WShell, eval(gzinflate(base64_, echo exec(..
4	Strings that can be judged by other web shells	File Browser, filemanager, jfileman, etc..

[Table 4-1] Detection pattern by webshell type

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

webshell pattern collection, inspection script execution and analysis method by type

03. webshell inspection script

The webshell inspection script is a program that finds source code with a string matching the webshell pattern defined by the inspector as source code that can be executed on the server using the find command.

Webshell inspection script uses UNIX and WINDOWS series. Here, let's check the contents and operation method of UNIX inspection script.

1) UNIX series script

① The file size is set to 2048 (1M), and the inspection target is set to all files (*.*).

```
#!/bin/sh
# File Size Setting ( size=1024 -> 512K byte, size=2048 -> 1M byte, size=4096 -> 2M byte )
size=2048

# File Extension Setting (Default=all)
file_ext="*.*"
```

Set the file size to 1M byte as a result of inspection

All files (*.*) are set for inspection target files

[Figure 4-9] File size setting and inspection target setting

② For variables : set count, hostname, date, time, and result (3)

```
# Global Variable Setting
LANG=C
export LANG
count=0
hostname=`hostname`
today=`date +%y%m%d`
totime=`date +%H%M%S`
sday=`date +%y.%m.%d`
stime=`date +%H:%M:%S`
result0=shell_"$hostname"
result1="$today"_"$totime"
result2="$hostname"_"$today"_"$totime"
```

[Figure 4-10] Variable setting for use in script

③ Set the automatic decompression script for the webshell pattern file using the if statement

```
if [ -f usig.tar.gz ]
  then
    gzip -d usig.tar.gz
    tar -xvf usig.tar
else
    echo "Not Found File usig.tar.gz!!"
    exit 0
fi
```

[Figure 4-11] Webshell pattern automatic decompression

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

webshell pattern collection, inspection script execution and analysis method by type

④ Create a file folder to save webshell check results

```
53  # Create Folder (Result File & Web shell File)
54  mkdir -p ./"$result0"/"$result1"/file
```

[Figure 4-12] Saving webshell pattern check result

⑤ Set summary information about the inspection target to be output in the result file (result_log.tsv)

```
56  # Script Start Info
57  clear
58  echo "" 2>&1
59  echo " Web Shell Find Script File" 2>&1
60  echo "" 2>&1
61  echo " - Start Time: $sday $stime" 2>&1
62  echo "Start Time: $sday $stime">./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
63
64  echo "Hostname: $hostname" >> ./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
65  ifconfig | grep "inet addr" >> ./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
66
67  echo " - Directory : $1" 2>&1
68  echo "Directory : $1">>./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
69  echo " - File Size : $size" 2>&1
70  echo "File Size : $size">>./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
71  echo " - File Extension: $file_ext" 2>&1
72  echo "File Extension: $file_ext">>./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
73  echo "" 2>&1
74  echo "  File Listing..." 2>&1
75  echo "" 2>&1
76  echo "Webshell Copy File List">>./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
```

[Figure 4-13] result_log.tsv output information

⑥ Set to search webshell pattern string and save the matched result in webshell_list.tsv file

```
78  # Webshell Find
79  find "$1" -type f -exec ls -Ralt {} \;  >> ./"$result0"/"$result1"/"$result2"_file_list.tsv 2>&1
80  find "$1" -type f -size -"$size" -name "$file_ext" -exec fgrep -l -i -f usig /dev/null {} \; >> ./"$result0"/
    "$result1"/"$result2"_webshell_list.tsv 2>&1
```

[Figure 4-14] webshell pattern string search and file creation

⑦ Set the file path in webshell search results and create the file as a txt file

```
85  # Webshell File Copy
86  for filename in `cat ./"$result0"/"$result1"/"$result2"_webshell_list.tsv`
87  do
88      count=`expr $count + 1`
89      cp -p "$filename" ./"$result0"/"$result1"/file/$count.txt
90      echo "$count.txt = $filename">>./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
91  done
92
93  file_num=`find ./"$result0"/"$result1"/file/ -type f | wc | awk '{ print $1}'`
94  file_list=`cat ./"$result0"/"$result1"/"$result2"_file_list.tsv | wc | awk '{ print $1}'`
95  file_512=`find "$1" -type f -size -"$size" | wc | awk '{ print $1}'`
96  copy_dir_size=`du ./"$result0"/"$result1"/file/ | awk '{print $1}'`
```

[Figure 4-15] Create webshell result as txt file

⑧ Result summary file creation (result_log.tsv)

```
98  echo """>>./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
99  echo " - File Count: $file_512 files [all $file_list files]" 2>&1
100 echo "File Count: $file_512 files [all $file_list files]">>./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
101 echo " - File Copy : $file_num files [$copy_dir_size bytes]" 2>&1
102 echo "File Copy : $file_num files [$copy_dir_size bytes]">>./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
103 echo " - Result Dir: $result0/$result1" 2>&1
104 echo "Result Dir: $result0/$result1">>./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
105 echo " - End Time  : `date +%y.%m.%d` `date +%H:%M:%S`" 2>&1
106 echo "End Time  : `date +%y.%m.%d` `date +%H:%M:%S`">>./"$result0"/"$result1"/"$result2"_result_log.tsv 2>&1
```

[Figure 4-16] Result summary file creation

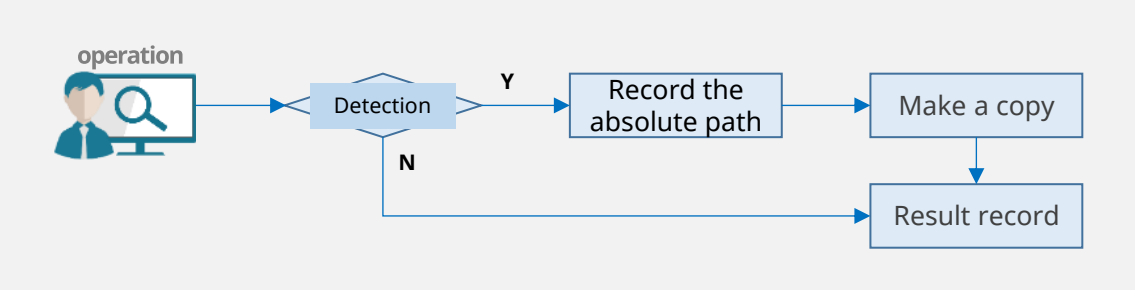
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

webshell pattern collection, inspection script execution and analysis method by type

2) How to run the inspection script

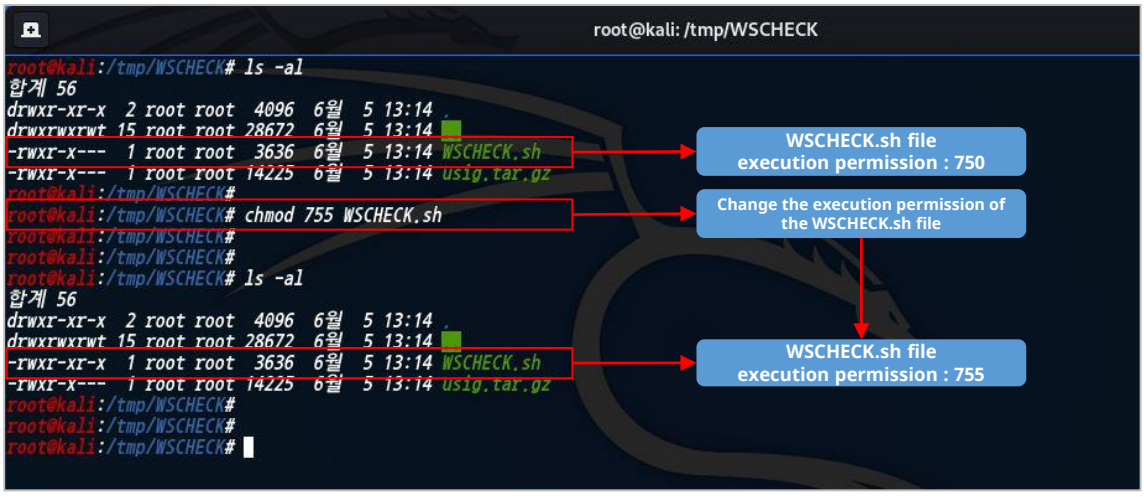
Run by entering the path to the inspection script command parameter, and analyze the contents (source code) of all files under the parameter to check whether the webshell pattern is included (detected).

If a webshell is detected, record the absolute path, then make a copy and record the result.



[Figure 4-17] webshell inspection script operation method

Copy the webshell check script file and pattern file to disk space so that the searched webshell file copy can be saved. On the server to be checked, execute the check by specifying the directory to be checked in the directory by granting execute permission to the script file as root.

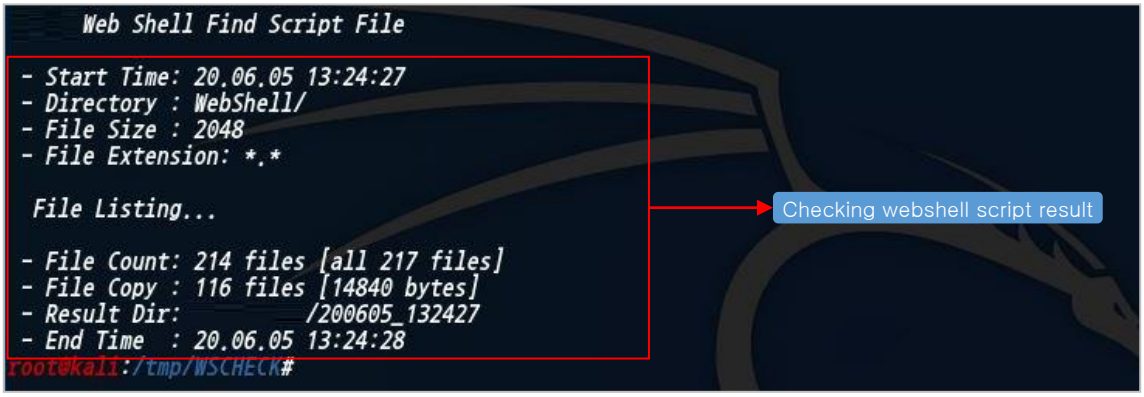


[Figure 4-18] Webshell Script Execution Authority Change

[Figure 4-19] Script execution by specifying the target directory

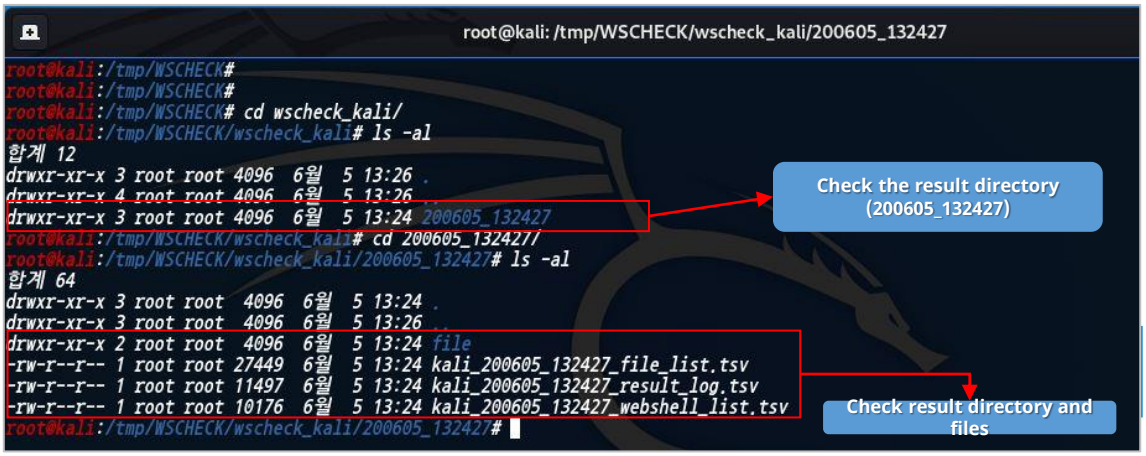
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

webshell pattern collection, inspection script execution and analysis method by type



[Figure 4-20] Checking webshell script result

When the check is completed, the check result folder and 3 result files are created in the directory where the script was executed.



[Figure 4-21] webshell inspection result folder and file

Rank	Folder and file name	Description
1	file	Detected copy of webshell is saved in number.txt format
2	file_list.tsv	Save all file information in the target directory (including subdirectories)
3	result_log.tsv	Store overall information about the script
4	webshell_list.tsv	Save detected web shell file path and web shell file information

[Table 4-2] Webshell inspection result folder and file description

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

04. How to analyze webshell by types

1) Targets can be judged by webshell

When the file extension is confirmed in the source code or in the case of various file browser types, it is judged as a webshell regardless of the extension. Even abnormal files with special characters inserted are judged by webshell regardless of execution.

If the webshell classification for the abnormal file is not clear, it should be regarded as the same level as the webshell and deleted.

```
/project/app/ons/bmsWeb/bms/agd/BmsAgdAInfoListExcel.jsp
/project/app/ons/bmsWeb/bms/com/BmsMyDesk03.jsp
/project/app/ons/bmsWeb/bms/com/BmsMyDesk066.jsp
/project/app/ons/bmsWeb/bms/com/2852cmd.jsp
/project/app/ons/bmsWeb/bms/com/3521cmd.jsp
/project/app/ons/bmsWeb/bms/com/3985cmd.js%70
/project/app/ons/bmsWeb/bms/com/4412cmd.js%70
/project/app/ons/bmsWeb/bms/com/8490cmd.jpg
/project/app/ons/bmsWeb/bms/ord/BmsOrdCardList02L.jsp
/project/app/ons/bmsWeb/bms/ord/BmsOrdCardListHadal.jsp
/project/app/ons/bmsWeb/bms/ord/BmsOrdDisUseInstPreviewList.jsp
/project/app/ons/bmsWeb/bms/ord/BmsOrdInstL.jsp
/project/app/ons/bmsWeb/bms/ord/BmsOrdInstListPortlet.jsp
/project/app/ons/bmsWeb/bms/ord/BmsOrdInstP.jsp
/project/app/ons/bmsWeb/bms/ord/BmsOrdInstResultOnlyV.jsp
/project/app/ons/bmsWeb/bms/ord/BmsOrdInstResultV.jsp
/project/app/ons/bmsWeb/bms/ord/BmsOrdInstV.jsp
/project/app/ons/bmsWeb/bms/ord/BmsOrdOgmInstList.jsp
```

[Figure 4-22] File Name in Date or Time Format

```
<%--
    jsp File browser 1.0
    Copyright (C) 2003,2004, Boris von Loesch
    This program is free software; you can redistribute it and/or modify it under
    the terms of the GNU General Public License as published by the
    Free Software Foundation; either version 2 of the License, or (at your option)
    any later version.
    This program is distributed in the hope that it will be useful, but
    WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or
    FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
    You should have received a copy of the GNU General Public License along with
    this program; if not, write to the
    Free Software Foundation, Inc.,
    59 Temple Place, Suite 330,
    Boston, MA 02111-1307 USA
    - Description: jsp File browser v1.0 -- This JSP program allows remote web-based
                   file access and manipulation.  You can copy, create, move and delete files.
                   Text files can be edited and groups of files and folders can be downloaded
                   as a single zip file that's created on the fly.
    - Credits: Taylor Bastien, David Levine, David Cowan
--%>
<%@page import="java.util.*,
                java.net.*,
                java.text.*,
                java.util.zip.*,
                java.io.*" %>
```

[Figure 4-23] jsp File browser source code

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

2) Who can judge with simple source code

If the format of the file name or the length of the file name with the same extension except for the image file extensions (.jpg, .gif, .bmp, .png, etc.) is confirmed, it is simple because it is created for the purpose of history management during AP development. It can be judged by pattern matching.

```
-rwxr-x---    1 weblogic swgrp          1113 Mar 14 2019  /project/app/WebApp/backup/manual.m
-rwxr-x---    1 weblogic swgrp         52661 Mar 14 2019  /project/app/WebApp/backup/http.m
-rwxr-x---    1 weblogic swgrp           909 Oct  5 2019  /project/app/WebApp/backup/http.m.20191005
-rwxr-x---    1 weblogic swgrp         13322 Dec  3 2019  /project/app/WebApp/backup/http.m.20191203
-rwxr-x---    1 weblogic swgrp          2821 Oct 31 2019  /project/app/WebApp/backup/20191005.xml
-rwxr-x---    1 weblogic swgrp          6857 Dec  3 2019  /project/app/WebApp/backup/wsconfig.20191203
-rwxr-x---    1 weblogic swgrp          1194 Mar 14 2019  /project/app/WebApp/backup/http.m.bak
-rwxr-x---    1 weblogic swgrp          6857 Oct  5 2019  /project/app/WebApp/backup/wsconfig.20191005
-rwxr-x---    1 weblogic swgrp         13622 Mar 14 2019  /project/app/WebApp/backup/wsconfig
```

[Figure 4-24] File Name in Date or Time Format

Basic source code or compiled files (.c, .h, .java, .class) that are commonly used in web containers (jeus, weblogic, tomcat, etc.) or exist in the path where various applications (java, oracle, openssl, etc.) are installed. Etc.) Although the source code required to run the web service cannot be viewed as a webshell, it must be conservatively judged by checking all the contents in the case of open source.

```
-rw-rw-r--    1 weblogic swgrp          2638 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppBisBasicViewCmd.class
-rw-rw-r--    1 weblogic swgrp          2639 Mar 31 2018  /project/app/WebApp/WEB-INF/classes//AppBisLevelViewCmd.class
-rw-rw-r--    1 weblogic swgrp          2701 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppBisSmlViewCmd.class
-rw-rw-r--    1 weblogic swgrp          2905 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppDetailListCmd.class
-rw-rw-r--    1 weblogic swgrp          2408 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppHisDetailListCmd.class
-rw-rw-r--    1 weblogic swgrp          2857 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppPjtDetailViewCmd.class
-rw-rw-r--    1 weblogic swgrp          3154 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppReqCancelUpdCmd.class
-rw-r--r--    1 weblogic swgrp          4647 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppReqListCmd.class
-rw-rw-r--    1 weblogic swgrp          4595 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppReqListCmd.class_061220
-rw-rw-r--    1 weblogic swgrp          2473 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppReqResultViewCmd.class
-rw-rw-r--    1 weblogic swgrp          3112 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppResAgreeCmd.class
-rw-r--r--    1 weblogic swgrp          4651 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppResListCmd.class
-rw-rw-r--    1 weblogic swgrp          4549 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppResListCmd.class_061220
-rw-rw-r--    1 weblogic swgrp          2473 Mar 31 2018  /project/app/WebApp/WEB-INF/classes/AppResResultViewCmd.class
```

[Figure 4-25] Basic source code or compiled file name

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

05. Conclusion

The webshell pattern can be collected sufficiently in the course of a website or infringement response. However, in order to write the inspection script, it is necessary to fully understand the Linux Shell Script and minimize the errors that can occur in the production server through internal tests.

For infringement response, there are limitations in developing rules for detecting and blocking webshells of security device. Therefore, it is a good way to check the webshell on a quarterly basis and periodically check it by registering a schedule in cron when there are few web servers running.

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

Cover Story

CHAPTER 5

Focus On IGLOO Security

1. Igloo Security Inc. acquires 3 patents related to artificial intelligence and security monitoring

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

Focus on IGLOO Security

Igloo Security Inc. acquires 3 patents related to artificial intelligence and security monitoring

- acquires 3 patents related to artificial intelligence and security monitoring

…Focusing on simplify the security monitoring work process from threat detection to response

[20th/May/2020] Igloo Security Co., Ltd. (CEO Lee Deuk-Choon, www.igloosec.co.kr) said, 'Monitoring device and program on how to generate response instructions and analyze application results (Registration No. 10-2111136),'Unsupervised learning-based anomaly detection method and its system (Registration No. 10-2110480)' and 'Machine learning-based frequency security policy generation system and its method (Registration No. 10-2108960)' patents registration was completed. Igloo Security plans to apply three patented technologies to SPiDER TM AI Edition, an AI security monitoring solution.

Igloo Security's three patents aim to shorten the process from threat detection to response based on accurate analysis of cyber attacks that evolve every day. Through the application of the patents registered this time, it is expected to respond in a timely manner to infringement incidents that may affect major IT systems and to increase the efficiency of security control.

Patents on 'Methods for generating response instructions and analyzing application results, monitoring devices, and programs' rank high-risk events that need to be responded first through simulation from a security and operational perspective, and respond with appropriate response times and response methods The focus is on generating instructions. By matching the threat information analyzed through the simulation module with the asset information, and predicting the damage size and recovery cost, and generating a response instruction based on this, it is possible to respond more promptly to attack events that may cause significant damage.

The patent for 'Unsupervised learning-based anomaly detection method and system' learns the prediction model by learning the feedback data provided by security experts about incorrect predictions among the prediction results produced by the deep neural network-based machine learning model through unsupervised learning. In the process of improving, the focus is on supplementing the problem of bias due to the loss of part of the information learned from the past data. Through the technology that selects useful parts of the feedback data and continuously trains the model using it, the learning efficiency of the machine learning model can be improved.

The patent for ‘machine learning based frequency type security policy generation system and method’ is a technology that creates a security policy that reflects the frequency of infringement threats identified through machine learning and its risk and automatically applies this policy to security device. By applying a security control policy that reflects changes in the attack flow in real time, it is possible to increase the visibility of security events that increase exponentially every day and minimize false positives that decrease the effectiveness of security monitoring tasks.

"The application of this patent technology is expected to shorten the process from threat detection to response and improve the effectiveness of security monitoring," said Lee Deuk-choon, CEO of igloo security. "As a leader in AI security monitoring, we will put more emphasis on the development of technology that can increase the response to advanced cyber infringement attempts."

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.