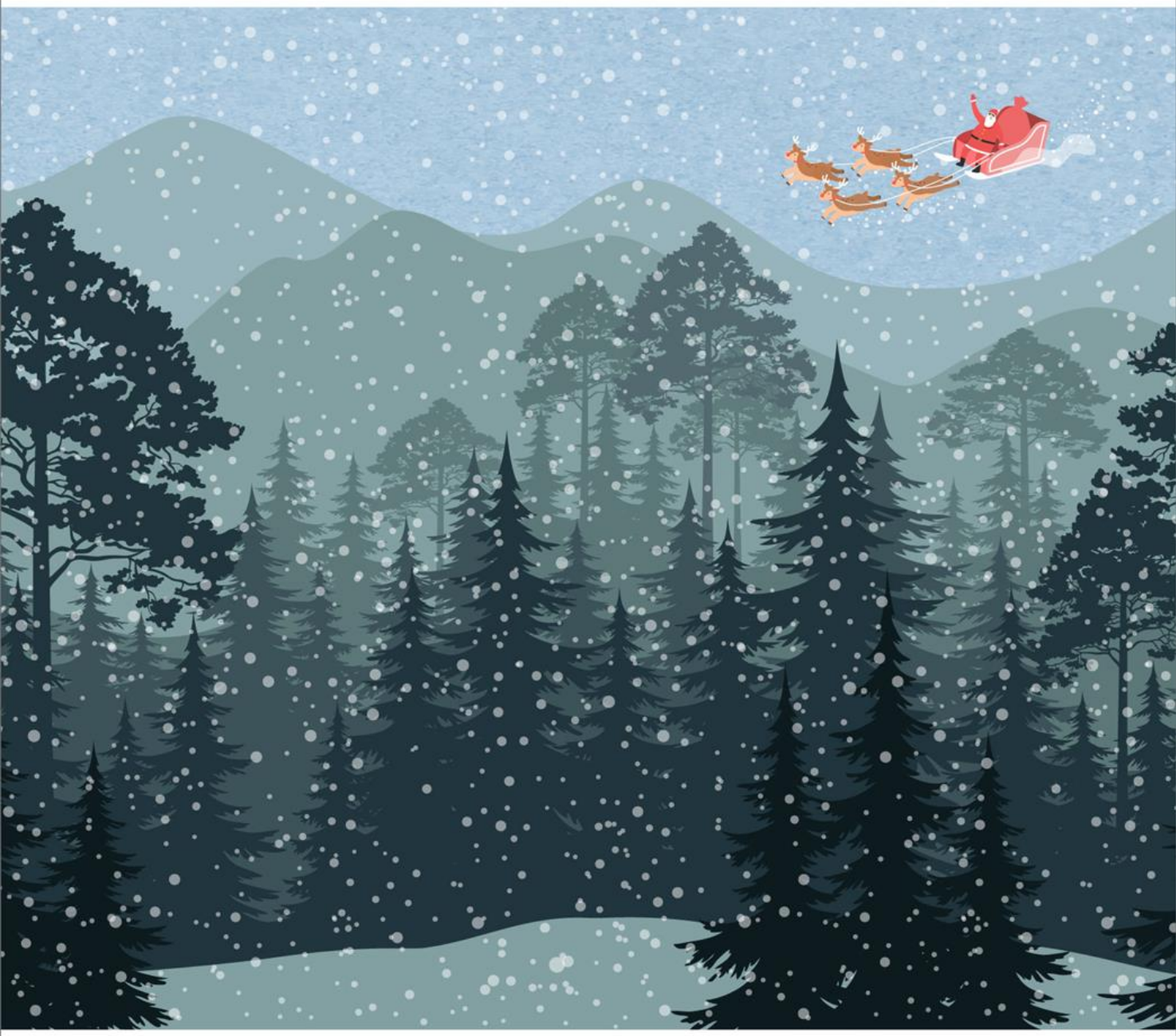
Monthly Security Report

2019
December



Cover Story

Data usage using user-defined statistics
Understanding of Linux PAM module
Cyber security threat and it's countermeasures in the blockchain era

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

- Security Issue

2. IGLOO Statistics

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

3. SIEM Guide (SPiDER TM V5.x)

- Data usage using user-defined statistics

4. Tech Note

- Understanding of Linux PAM module

5. Special Column

- Cyber security threat and it's countermeasures in the blockchain era

6. Focus On IGLOO Security

- This month's IGLOO Security

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

CHAPTER 1

Monthly Security Issue

1. Security issue

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

1 Security Issue

'Ransomware attack is on going in December..'…Warning for ransomware attacks at end of year

- Careful attention should be given as ransomware attacks continue during the year-end and New Year holidays.
- Security companies said they detected a new ransomware, called "Antefrigus", similar to Sodinokibi in early November. Anteprigus encrypts folders and files in drives D, E, and F, except Drive C, and changes the extension to .qrja.
- They also found ransomware mail that allegedly spread by VenusLocker organizations. If you download the compressed file attached to this email disguised as a recruitment support email, Nemty Ransomware will be installed.
- Security experts stressed the need for a more thorough security posture at the end of the year events such as new employee bonds, business plans, and year-end parties..

'We love K-POP!'… Indonesian hackers threw photos of Korean idol groups after hacking deface

- Indonesian hackers are continuing their deface attacks to target websites around the world. They are changing websites screens with photos of Korean idol groups as if they are fans of K-POP.
- Security experts suggest that a defaced attack indicates that the website is vulnerable, and that the website is regularly checked and the vulnerability is managed so that the defaced attack does not recur.

'should be doubt the mail sent at Monday'… Corporate email breach (BEC) attacks, mostly happens at Monday

- Security company Barracuda Networks recently analyzed 1.5 million spear phishing e-mails, and corporate e-mail breach (BEC) attacks have the following characteristics:
- 91% of BEC attacks occur during the week. In particular, most attacks occur on Mondays and Tuesdays.
- The BEC attack is targeting 6 employees in a company per average.
- Attacks based on thorough investigation of the target company.
- Many e-mails included words such as emergency, urgency, and request for help in the subject, or disguised as bosses or executives in order to prevent the employees who receive the e-mails from making rational judgments.
- About 30% of users who received BEC mail opened the email, but not all sent money according to the instructions of the culprit.
- Security experts stress that attackers are creating highly elaborate, personalized emails targeted to target BEC attacks that require a higher price than typical spear phishing.

'No one can trust..'…Expecting for cloud attack increase through third party service providers

- According to the 2020 Security Forecast Report published by Trend Micro, cloud attacks through third-party service providers will increase. As more and more companies are moving to cloud environments, third-party companies are becoming more involved.
- Specifically, code injection attacks (SQL injection, cross-site scripting, etc.) are likely to target corporate data stored in the cloud or DDoS attacks using botnets against cloud service providers.
- As more companies using the DevOps culture use third-party code, the related risks are expected to increase.
- Security experts recommend that regular third-party vendors perform vulnerability and risk assessments.

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

1 Security Issue

Account information for over 4,000 Disney + users traded on the Dark Web

- After launching the Disney Plus streaming service, which was highly anticipated by Disney fans, began to capture account information and credentials of over 4,000 users on the Dark Web. Username, password, subscription type, and subscription expiration information were being traded.
- Security experts predicted that an attack aimed at Disney Plus, which is expected to join tens of millions of people, would point out that Disney did not introduce a dual or multiple authentication option and did not obfuscate user IDs and passwords.
- Since the hackers have taken over their accounts and changed their email or passwords, the social media has been constantly updating the victims' complaints.
- Security experts believe that attackers are likely to hijack some of their accounts through brute force attacks.

'Increase attack costs with active vulnerability management'…Average severity of vulnerabilities discovered between 2016 and 2018 is getting lower

- Research has shown that it is possible to increase the cost of attack by cyber attackers through continuous observation and active inspection..
- According to security firm Synack, the average severity of vulnerabilities discovered between 2016 and 2018 is decreasing as companies actively identify vulnerabilities through automated technology and periodic penetration testing. In 2016, the average CVSS score was 6.41, but in 2018 it was 5.95.
- Cynack said that security efforts have been effective in that △vulnerabilities are becoming less and less severe, △ the time it takes for attackers to find vulnerabilities to use in the attack is longer.
- HackerOne, a bug bounty management platform, recently analyzed four major data breaches and found that known vulnerabilities had been exploited. It also emphasized that if the vulnerability was checked and patched in advance, the problem could be solved at a much lower cost.

43% of PaaS targets MS, PayPal, DHL and Dropbox

- Recently, cybercriminals use phishing as a service (PaaS), and 43% of them are targeting MS, PayPal, DHL and Dropbox users.
- According to Akamai, cybercriminals have recently been stealing user credentials in a multi-level way that leads to phishing pages via pages that mimic multiple legitimate websites.
- Cybercriminals target prestigious global companies and their users, and work on organized and sophisticated phishing kits. According to Akamai's monitoring, Microsoft has 21.88% (3,897 domains, 62 variant kits), PayPal 9.37% (14 variant kits), DHL 8.79% (7 variant kits), and Dropbox 2.59%(11 variant kits).
- Phishing attackers continue to develop new bypass methods to avoid detection for as long as possible. 60% of the phishing kits observed were set to activate only for up to 20 days.
- Security experts call attention to the fact that phishing as a service that exploits corporate trust will continue over the long term.

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 previous month

   03. Top 10 monthly attack service patterns

   04. Monthly attack service incident patterns compared to previous 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. TOP 10 monthly attack service(port)

Event analysis collected during the month of December 2019 shows that events using Microsoft-DS (TCP / 445), DNS (TCP / 53), and MS-SQL-S (TCP / 1433) ports are on the rise compared to the previous month. event history using Oracle (TCP / 1521) and HTTPS (TCP / 443) decreased compared to the previous month. The overall number of events has decreased, and in particular, the number of HTTPS (TCP / 443) ports has dropped sharply.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of Cases	Ratio(%)	Fluctuation
1	HTTP(TCP/80)	1,423,464,457	49.53%	-
2	DNS(UDP/53)	578,673,864	20.13%	-
3	Microsoft-DS(TCP/445)	308,046,491	10.72%	▲1
4	HTTPS(TCP/443)	243,791,291	8.48%	▼1
5	ICMP(0/ICMP)	99,678,268	3.47%	-
6	SNMP(UDP/161)	92,301,539	3.21%	-
7	Telnet(TCP/23)	46,057,755	1.60%	-
8	DNS(TCP/53)	29,047,637	1.01%	▲1
9	MS-SQL-S(TCP/1433)	26,889,543	0.94%	▲1
10	Orcale(TCP/1521)	26,153,048	0.91%	▼2
	Total	2,874,103,893	100.00%	-

[Table2-1] TOP10 monthly attack patterns

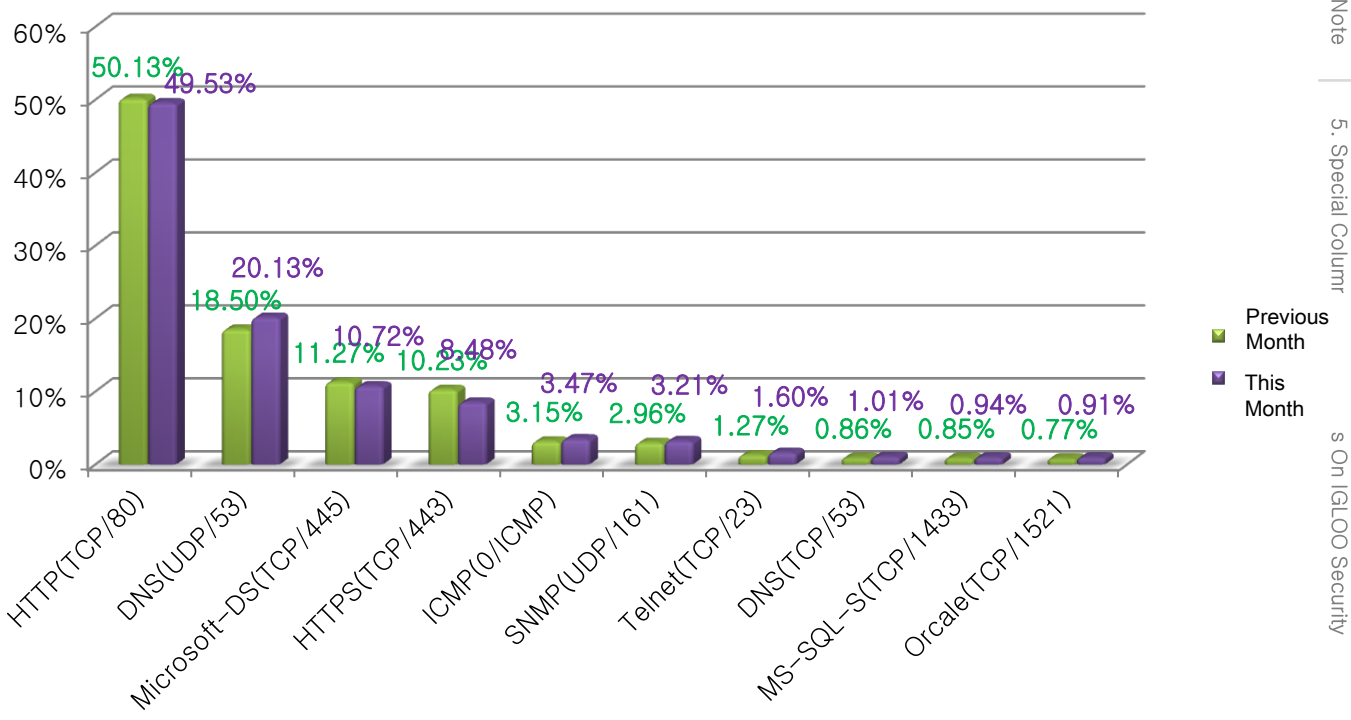
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

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 previous month

As a result of event analysis by attack service port, HTTP and DNS service ports continue to show a high share, and the majority of events seem to decrease compared to the previous month, but DNS service is slightly increased. This may be due to an increase in DRDoS attacks that recently exploited the protocol characteristics of DNS (UDP / 53). In order to prepare for DRDoS using the DNS protocol, it is recommended to check the DNS server response setting and adjust the threshold of abnormal traffic blocking of security equipment.



[Figure 2-1] TOP10 monthly attack port

Copyright © IGLOO Security, Inc. 2019. 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.

03. TOP 10 monthly attack service patterns

The ranking of the HTTP Login Brute Force event has fallen significantly in the December 2019 attack pattern TOP10, and another HTTP POST Session Exhaustin Attack (By rudy) event is newly confirmed. The Brute Force event saw a temporary increase in the previous month, and the number of denial-of-service attacks such as rudy and slowloris increased significantly this month.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of Cases	Ratio(%)	Flunctuation
1	SMB Service connect(tcp-445)	999,477,436	96.29%	-
2	HTTP POST Session Exhaustion Attack(By rudy)	6,924,722	0.67%	NEW
3	ACK Port Scan(F/W Scan)	5,802,174	0.56%	-
4	HTTP Connection Limit Exhaustion Attac k(By Slowloris)	5,354,208	0.52%	▲4
5	Dcom_TCP_Sweep(MSBlaster Worm Me ssenger)	5,136,002	0.49%	▼1
6	Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	3,965,512	0.38%	-
7	Multi Packet Inspection	3,669,244	0.35%	▼2
8	MS WINS Server Registration Spoofing V uln-1[Req](UDP-137)	3,455,272	0.33%	▼1
9	HTTP Login Brute Force	2,920,954	0.28%	▼7
10	HP Data Protector Client EXEC_CMD wit h Directory Traversal-1	1,307,088	0.13%	-
Total			100.00%	-

[Table 2-2] TOP10 monthly attack pattern

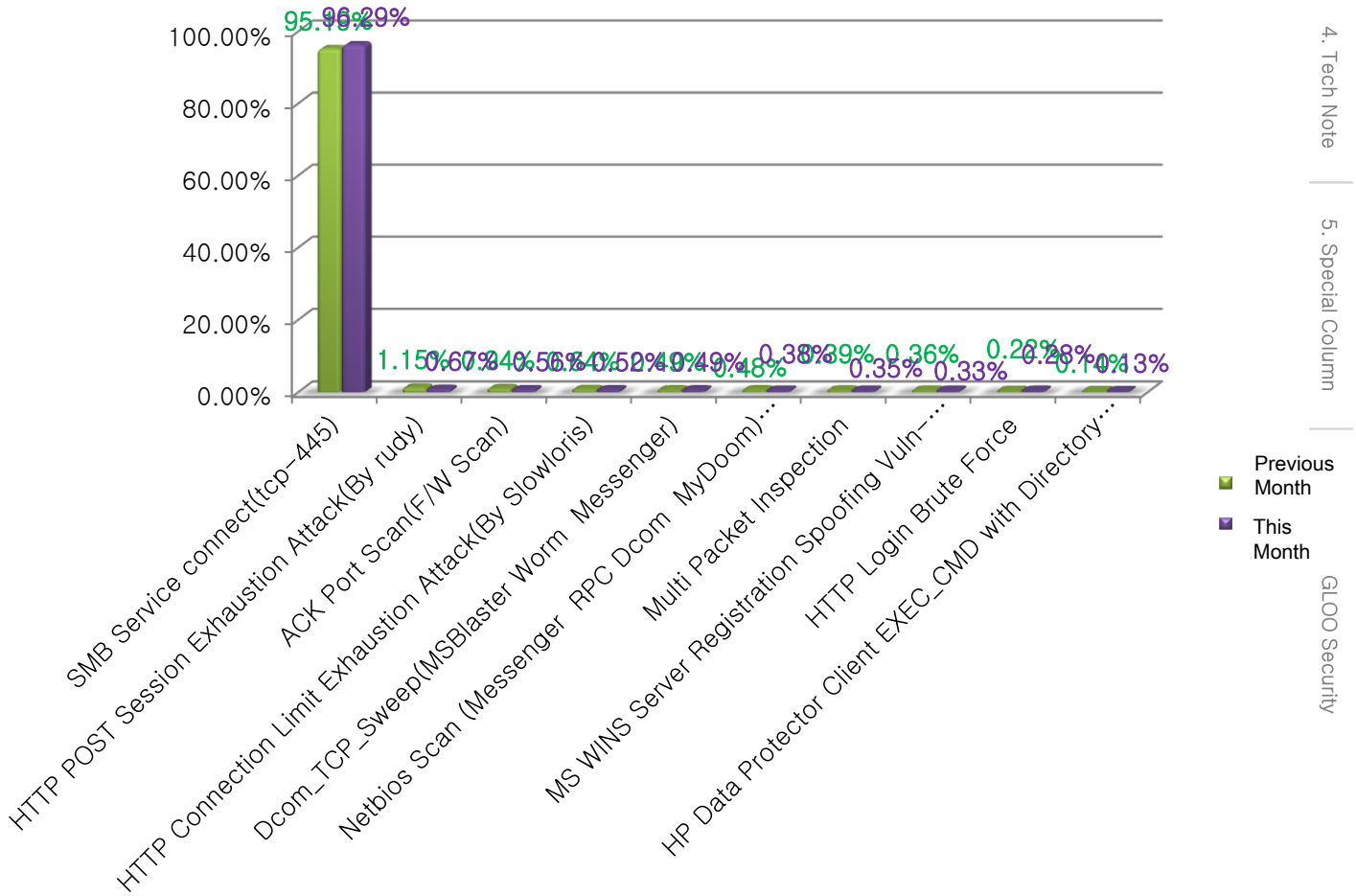
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

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.

04. Monthly attack service incident patterns compared to previous month

The HTTP POST Session Exhaustion Attack (By rudy) and HTTP Connection Limit Exhaustion Attack (By Slowloris) events increased sharply compared to the previous month. oth events are a type of denial-of-service attack that exhausts server resources. It is recommended to specify a session timeout to establish a policy that blocks connections from hosts that are overly occupying sessions.



[Figure 2-2] TOP10 monthly attack pattern

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

2 Monthly attack service and trend analysis

IGLOO SECURITY introduce the detailed analysis results according to the attack pattern centering on the TOP 10 among the attack patterns that occurred in December. 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 POST Session Exhaustion Attack(By rudy)	R.U.D.Y stands for "R-U-Dead-Yet" and is a connection resource depletion type Denial of Service tool using HTTP's POST method. Incomplete HTTP headers and fragmented data are used to generate a large number of non-terminating connections, exhausting the connection resources of the target system.
ACK Port Scan(F/W Scan)	ACK Port Scan (F/W Scan) is a type of scanning attack targeting vulnerable ports which are allowed to be accessed by firewall policy. Attackers can collect information on vulnerable ports by analyzing the returned packet as a response to the packet sent in advance. These attacks are not intended to destroy the system but to collect information for planning a scenario for secondary attack.
HTTP Connection Limit Exhaustion Attack (By Slowloris)	Slowloris is an attack tool that maintains a TCP connection by sending an abnormal HTTP request to a web server, unlike 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 user requests.
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)	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.
Multi Packet Inspection	A Multi Packet Inspection is a rule that occurs within the IPS of a specified company and detects using the automated pattern learning defense mechanism set-up within the IPS.It denies access for a certain amount of time if a packet, which exceeds the bytes PPS set-up by the IPS, is injected.
MS WINS Server Registration Spoofing Vuln-1 [Req](UDP-137)	NetBios checks each other's information through UDP port 137, establishes 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 with the target system.
HTTP Login Brute Force	This attack accesses the HTTP WEB service port(80) and repetitively inserts random strings through a Tool-Kit in order to find out the password for a specific ID(root, guest etc). Passwords which are easy to guess or are in an alphabetic/symbolic order are more prone to this attack. This attack can be prevented by using IDs and passwords over 6 letters and by Filtering data from the HTTP port(80/TCP).
HP Data Protector Client EXEC_CMD with Directory Traversal-1	This vulnerability occurs in the HP Data Protector Client. Directory Traversal is an attack which uses a bypass attack. It is an attack in which an unauthorized user sends maliciously manipulated input values to EXEC_CMD. If the attack is successful, the attacker can execute arbitrary codes with system level permissions. Prevention is possible by installing the latest patch released from vendors.

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

CHAPTER 3

SIEM Guide (SPiDER TM V5.x)

Utilizing Data through User-defined Statistics

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

Utilizing Data through User-defined Statistics

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

Technical Support Team,
Technical Support Center

01. Overview

1) Utilizing SIEM through User-defined Statistics

Modern IT services, such as 5G networks, IoT devices, and the cloud, use R, a big data analysis tool, to analyze huge amounts of big data. R is a popular data analysis program that is easy to use and popular with users.
SPiDER TM V5.0 can increase efficiency of big data analysis through user-defined statistics menu, which is based on R program. In this topic, we will consider how to utilize the created/loaded data efficiently using the user-defined statistics menu.

* User-defined statistics feature is provided as UI from TM 5.0.1.36 or later

02. User-defined Statistics

1) Concept of User-defined Statistics

- Statistical data can be generated based on user defined conditions.
- The data generated by user-defined statistics is stored in RDB, which can be used to organize custom dashboard content and use it as a single alert.

User-defined Statistics

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

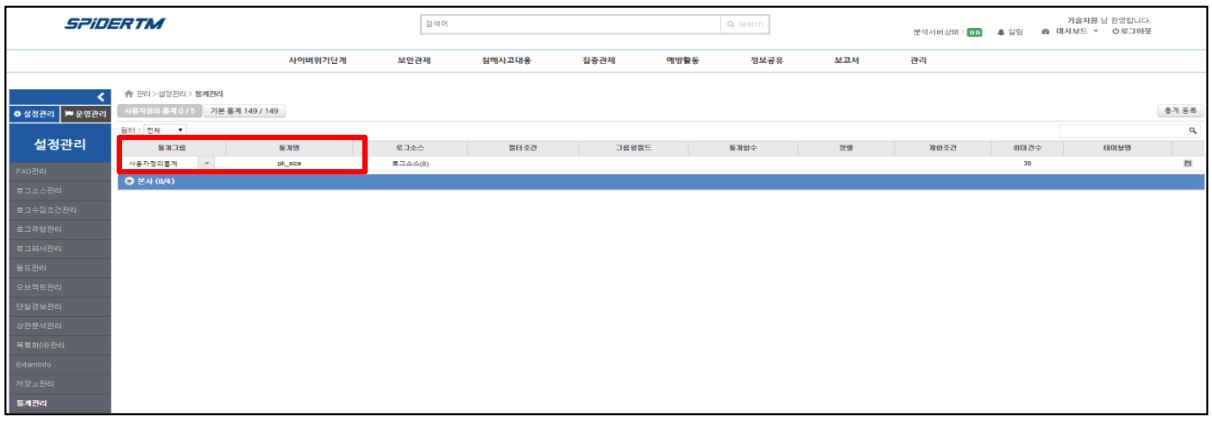
Utilizing Data through User-defined Statistics

2) User-defined Statistics Creation

SPiDER TM 5.0 UI - Admin > Configuration > Statistics Management

- User-defined statistics data can be created by selecting **"Statistics Registration"** menu at the top of statistics management menu.
- Let's learn how to create a user-defined statistics that stores the sum of outgoing bytes in firewall's allow log to a table in the stats.

① Set statistics group and statistics name

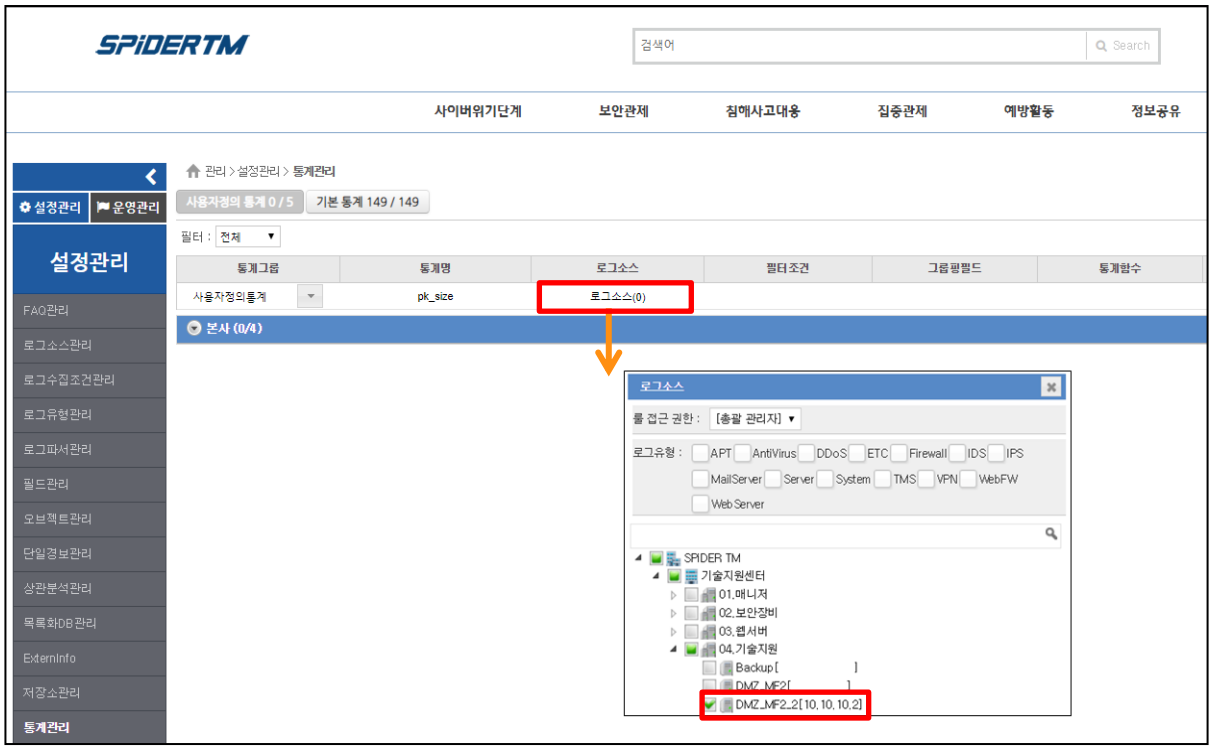


- Select statistics registration menu and assign statistics group and statistics name that are not duplicated with others.

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

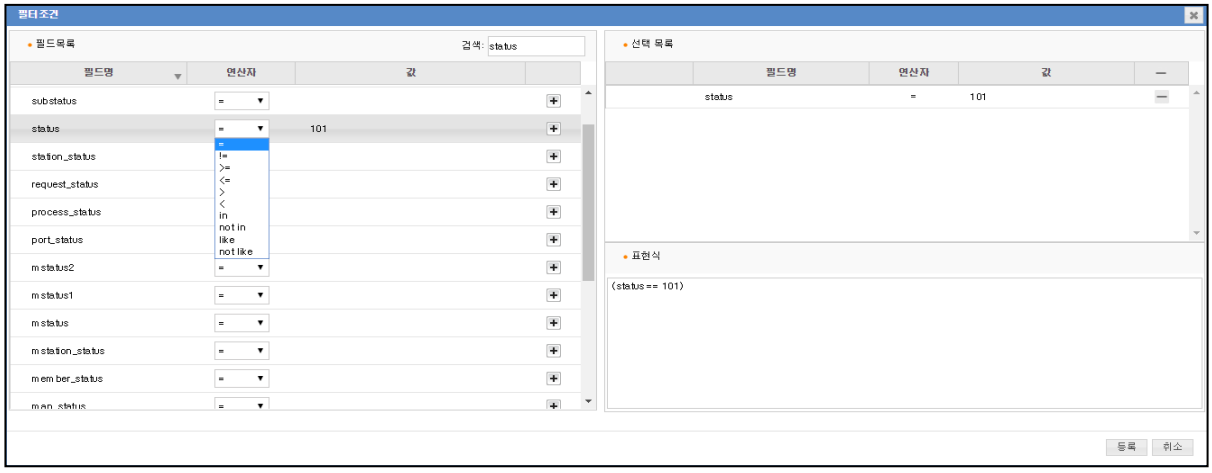
Utilizing Data through User-defined Statistics

② Log source



- Select log source menu and specify the target device for generating statistics.
- When log type is selected, all target devices registered in the log type are subject to statistics generation.

③ Filter condition

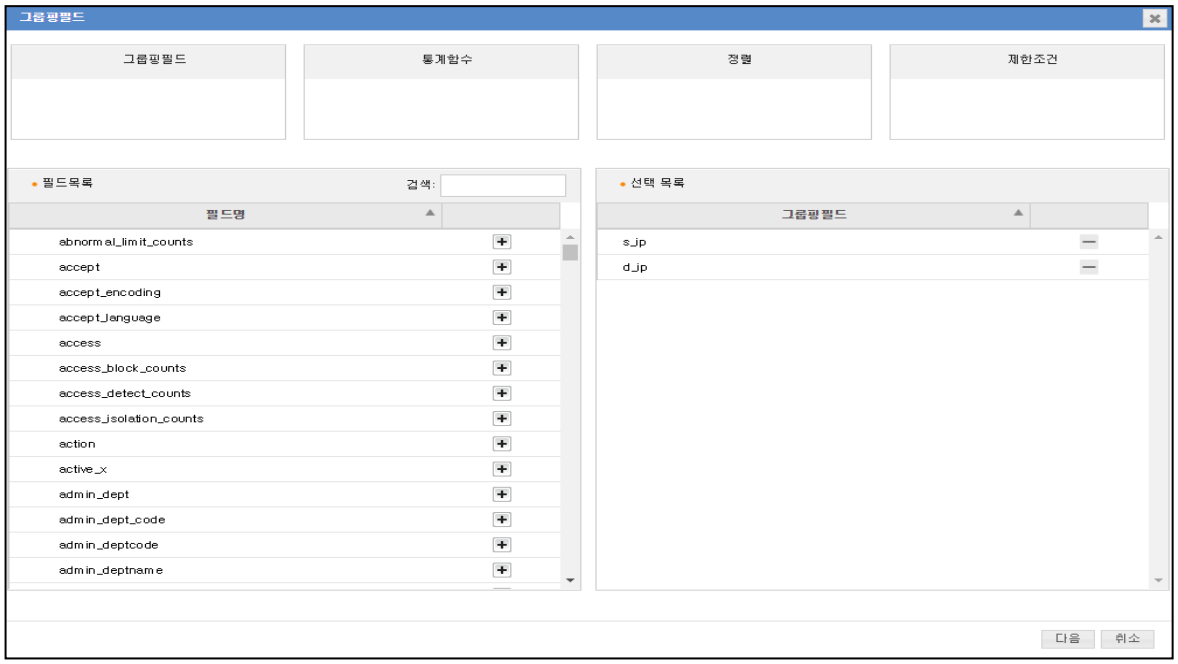


- This part defines conditions before generating statistics.
- When multiple fields are selected, the relationship between the fields is applied by AND condition.
- status=101 condition means that the status value of firewall log is allowed.
- Available operators : =, !=, >, >=, <, <=, like, in, not like, not in

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

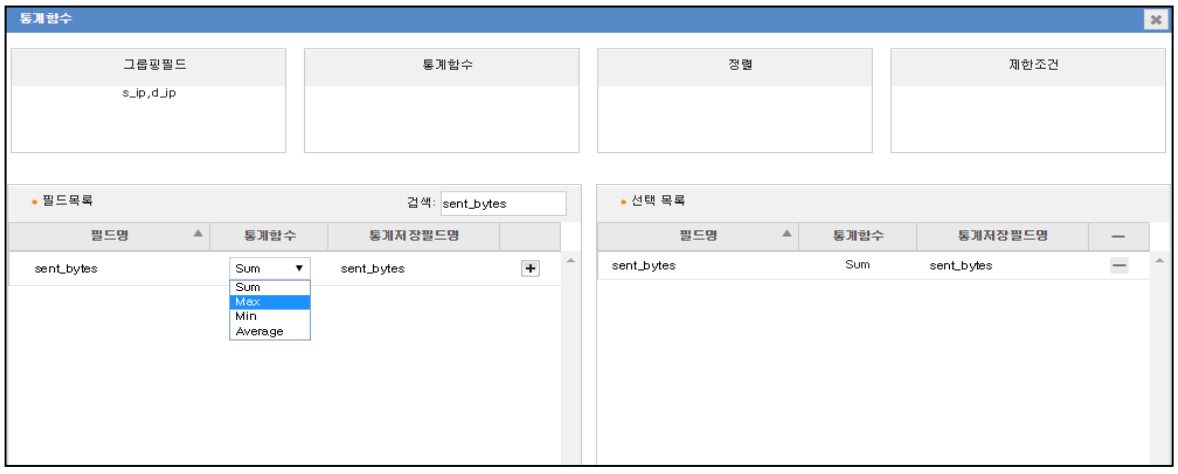
Utilizing Data through User-defined Statistics

④ Grouping field



- Specify a field to ‘group by’ the collected data for 1 minute.
- Fields specified as grouping fields are created as columns of user-defined statistics table. Specify source IP(s_ip) and destination IP(d_ip) fields.

⑤ Statistical function

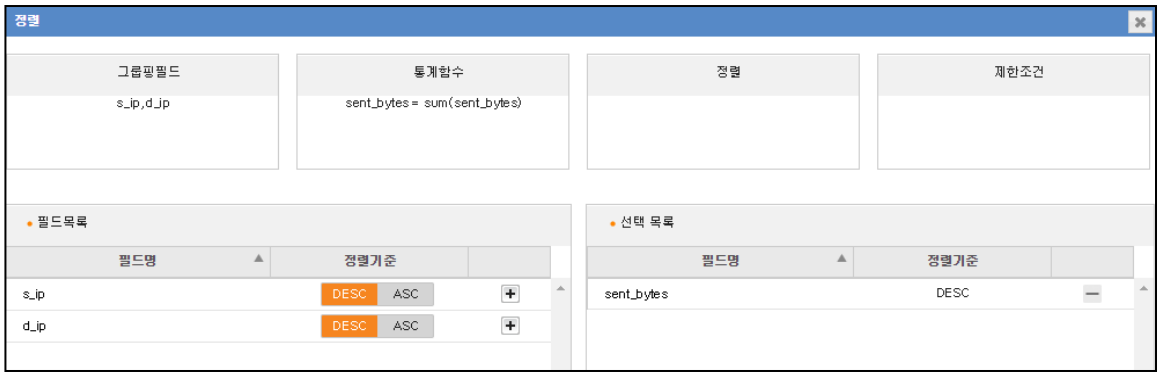


- Specify a field to perform statistical function.
- Specify "sent_bytes" field containing the information of sending bytes of target firewall.
- Collection cycle is 1 minute and data is saved after performing calculation on the collected data for 1 minute.
- Available operators : sum, max, min, average

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

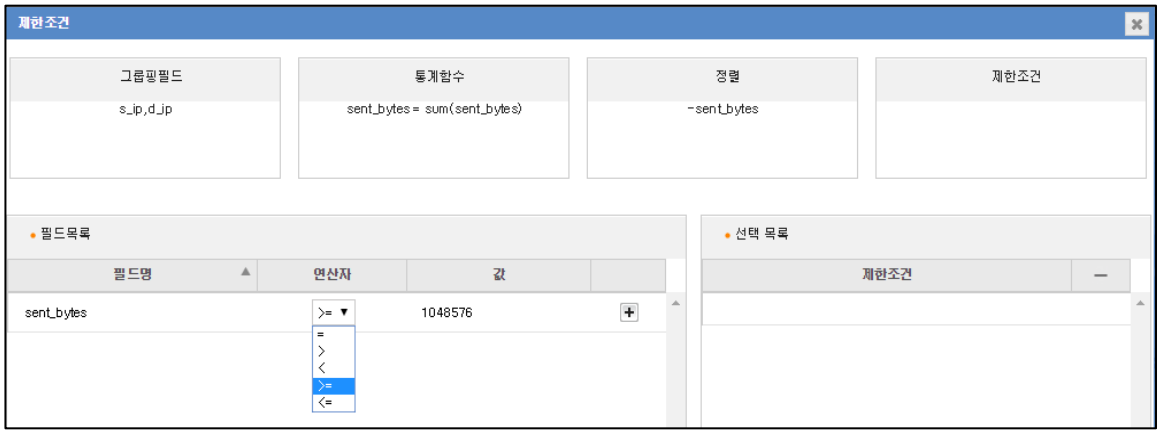
Utilizing Data through User-defined Statistics

⑥ Sorting



- When storing data in a table, specify the sort criteria field.
- DESC: descending order, ASC: ascending order

⑦ Exclusion criteria



- Exclusion value for each field can be set. For example, the transmission bytes per minute generates only the data of more than 1MB to store the statistics.

⑧ Table name

- Enter the name of table to store user-defined statistics data. It is automatically created when user-defined rules are activated.
- The fields specified in the grouping field and the statistics function area are registered as columns.

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

Utilizing Data through User-defined Statistics

⑨ Data search

```
select s_ip, d_ip, sent_bytes from US_STATSR order by idate desc
```

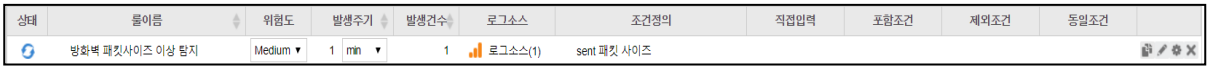
S_IP	D_IP	SENT_BYTES
105.253.123.110	192.168.135.100	153,251,018
103.108.108.254	211.44.134.209	5,598
103.108.105.253	175.193.100.25	6,550
122.216.80.211	175.190.90.47	199,922
175.223.65.120	58.140.111.35	856
1.222.82.214	192.168.100.221	1,685
150.216.20.13	118.216.62.51	8,500
1.221.130.150	220.153.112.10	450
135.52.150.130	211.44.134.209	9,805

- It can be checked that statistical data is stored in the created user-defined table.

03. Single Alert with User-defined Statistics

1) Alert analysis using R statistical data

1. Single alert registration



- An object using sent_bytes field of user-defined statistics table can be created and used as a single alert.
- If the data stored in RDB is larger than the average sent_bytes value for 1 minute using DB query function, the condition is defined.
- Detects packet anomalies through the corresponding alert.

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

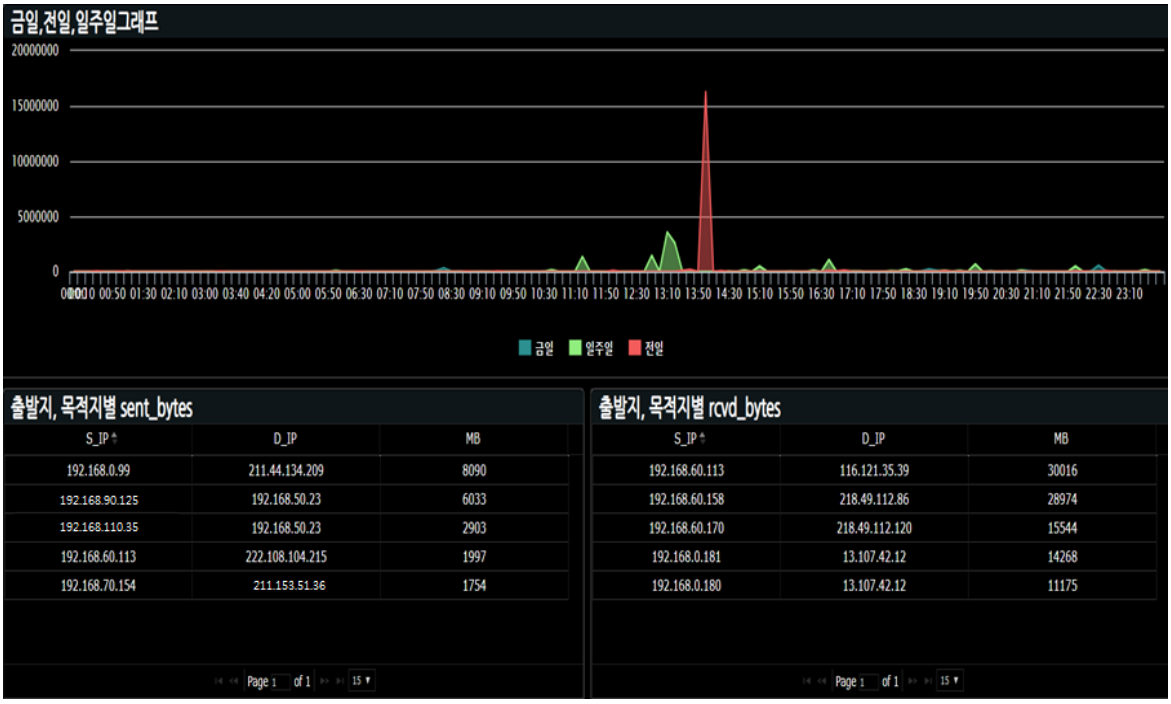
Utilizing Data through User-defined Statistics

04. Dashboard using User-defined Statistics

1) Visualization using R Statistical Data

▹ **Dashboard**

It is possible to compose a dashboard screen using Area Chart, Grid Chart, etc. provided in “User-defined Dashboard” by using the data created through user-defined statistics function.



05. Conclusion

Now we have gone through how to take advantage of user-defined statistics capabilities in SPiDERTM V5.0.

Data storage with user-defined statistics, single alert configuration using stored data, and dashboard expressions using loaded data can be used to visually display and instantly know the user of anomalous behavior.

In order to respond to cyber threats that are becoming more intelligent, users need to continuously monitor and thoroughly supervise using various analysis methods.

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

CHAPTER 4

Tech Note

Understanding of Linux PAM module

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

Understanding of Linux PAM module

Security Monitoring Center
Security Analysis Team

01. Synopsis

If you are diagnosed with a server vulnerability, you will often be guided to "Use the PAM module to fix the vulnerability" in topics such as "Set Account Lockout Threshold" and "Restrict SU Command Usage." However, if you open the PAM configuration file and follow the guide, you will face to failure.

PAM configuration is not just a single line modification, but the result depends on the settings declared on the top and bottom lines. This can make the SU command unusable or cause you to suddenly be unable to log in.

Therefore, in this Tech note, We will find out about PAM, including what PAM is and how it works.

2. What is the PAM(Pluggable Authentication Modules)?

PAM is a 'Pluggable Authentication Modules' used in Linux system to control the user's permission to the application (service).

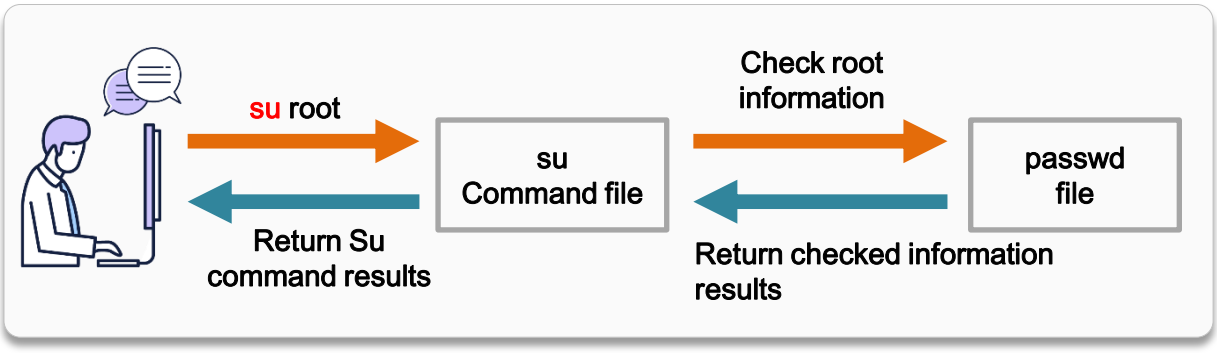
Before using PAM, Linux systems implemented their own logic in each application to authenticate users. In particular, when authenticating through the user information stored in the system, there was a risk of infringement because the application program should have access to the main system file (/etc/passwd) containing the user information. In addition, there are many difficulties in managing the user authentication method for each application.

PAM has emerged to solve this problem, and the operation principle of PAM is as follows.

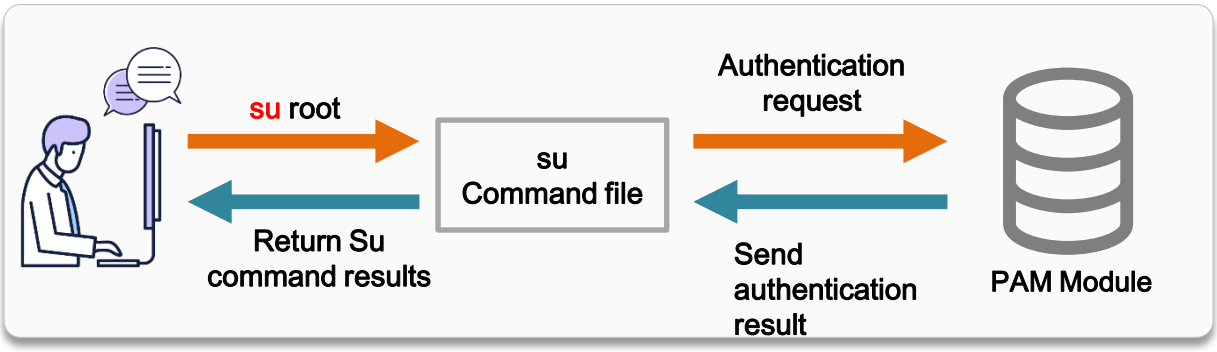
1. An application that requires authentication no longer reads the passwd file and requests user authentication from the 'PAM' module.
2. PAM uses the information of the user who requested the authentication, derives the result and passes it to the application.

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

Understanding of Linux PAM module



[Figure 5-1] The process of authenticating a user by the application itself



[figure 5-2] User Authentication Process with PAM Module

Since the PAM module is designed to separate software development from authentication and secure authorization schemes, when authentication is performed, not only the application logic is directly implemented in the application, but also the development is simplified. The advantage is that you do not have to browse the file. First and foremost, the system operator can control the authentication behavior of the application, allowing the system to operate more securely.

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

Understanding of Linux PAM module

03. PAM component

1) Basic PAM component

· basic component

Module type	Control Flag	Module Name	Module Arguments

· example of basic PAM component

[/etc/pam.d/su]

auth	sufficient	pam_rootok.so
auth	required	pam_wheel.so debug group=wheel
auth	required	pam_wheel.so use_uid
auth	include	system-auth
account	sufficient	pam_succeed_if.so uid = 0 use_uid account
	include	system-auth
Module type	Control Flag	Module Name 및 Module Arguments

2) Module Type

The module type field designates what kind of authentication to use for PAM. Four types of types can be set.

auth	Module that asks the user for a password and checks if the information entered is correct
account	Module to manage access control and account policy for accounts by checking whether specified accounts are valid authentication targets under current conditions
password	Module that manages password renewal so that users can change their credentials
session	Module defining what needs to be done before and after the user is authenticated

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

Understanding of Linux PAM module

3) Control Flag

This field is used to determine what modules should be used in the PAM.

requisite	If authentication fails, end authentication – If authentication result is the succeeds, execute following authentication module(Not reflected in the final certification result) – If authentication result is the failure, immediately return the authentication fails
required	Execute the next authentication regardless of the authentication result –If the authentication result the succeeds, the final authentication result is unconditionally the succeeds. –If the authentication result is the failure, the final authentication result is unconditionally is the failure.
sufficient	If authentication fails, end authentication – If authentication result is the succeeds, immediately return the authentication succeeds. –If the authentication result is the failure, execute following authentication module.(Not reflected in the final authentication result)
optional	Generally, not reflected in the final authentication result However, If there is no clear success/failure of another authentication module, return the result of this module
include	Call another PAM configuration file

In case of “Required” among 5 Control Flags, the next module is executed regardless of the result of the module. Note that even if it fails at "Required", the final authentication result will fail because it has a higher priority than the result of the next module executed.

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

Understanding of Linux PAM module

4) Module Name

This field specifies the path and name of the module you want to use. Most PAM modules are located in the /lib/security or /etc/pam.d directory. The following is a description of the main modules.

pam_rootok	A module that in case of root account, allow unconditionally without additional authentication.
pam_wheel.so	A module used for authentication using SU command and controlling authentication for a specific group (wheel)
pam_ succeed_if.so	A modules that control authentication based on conditions given as arguments
pam_securetty. so	This module is applied only to the root account. If a root exists in the file by referring to the /etc/securety file, the module allows root access to a specific service. (In case of non-root account, authentication success value is always returned.)

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

Understanding of Linux PAM module

5) Module Arguments

Module-arguments represent the arguments passed to the module. Each module has its own arguments. Each module may or may not require arguments.

Debug	Specify to leave debug information in the system log file
No_warn	Specify not to send a warning message to the module
Use_first_pass	An argument that specifies that the user should not be prompted for a password. Authentication fails if the password entered in the previous module does not exist
Try_first_pass	Attempt to authenticate with the password entered in the previous module. If the password entered previously does not exist, the user is prompted for input.

04. Detailed authentication process by PAM

Now let's analyze the authentication process through PAM in detail. In this section, we will analyze the "su" command application program.

1 Attempt to user change in general account(igloo) to "root" account ➡ open /etc/pam.d/su

```
[igloo@localhost ~]$ su root
```

2 Check requester (igloo) is "root" or not ➡ Since it is nor "root", execute next condition

[/etc/pam.d/su]

```
auth        sufficient      pam_rootok.so
auth        required        pam_wheel.so use_uid
auth        include         system-auth
account     sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account     include         system-auth
                    ... 중략 ...
```

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

Understanding of Linux PAM module

3 Check requester(igloo) is “wheel” group member or not → Execute the following conditions regardless of success/failure(required)

[/etc/pam.d/su]

```
auth        sufficient      pam_rootok.so
auth        required        pam_wheel.so use_uid
auth        include         system-auth
account     sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account     include         system-auth
                    ... 중략 ...
```

4 Open /etc/pam.d/system-auth file and ask file open and PW input to users → It the PW input is correct, authentication is closed

[/etc/pam.d/su]

```
auth        sufficient      pam_rootok.so
auth        required        pam_wheel.so use_uid
auth        include         system-auth
account     sufficient      pam_succeed_if.so uid = 0 use_uid quiet
account     include         system-auth
                    ... 중략 ...
```

[/etc/pam.d/ system-auth]

```
auth        required        pam_env.so
auth        sufficient      pam_fprintd.so
auth        sufficient      pam_unix.so try_first_pass
auth        requisite       pam_succeed_if.so uid >= 500 quiet
auth        required        pam_deny.so
                    ... 중략 ...
```

※ try_first_pass

If there is a password input from the previous module, authentication is attempted first with the password. If no password has been entered before, it prompts for a password.

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

Understanding of Linux PAM module

The most important step of the above process is the step "3". In the step "3", the module is executed using the "required" flag, so the next authentication module is executed even if the requester does not belong to the wheel group. Therefore, not only the wheel group members but also all "authentication" requestors go through the "5" level authentication process and all of them will receive the same password input request.

This is where the truth of the "required" flag mentioned earlier appears. The supplicant can be considered simply a password input error because he / she received a password input request even though the authentication failure occurred because he did not belong to the wheel group. This has the advantage that security is very good because the cause of error is not directly expressed.

05. Example of PAM configuration

■ CASE 1

Module-arguments represent the arguments passed to the module. Each module has its own arguments. Each module may or may not require arguments.

```
[ /etc/pam.d/su ]  #1
auth        required        pam_succeed_if.so user=igloo quiet
auth        sufficient      pam_unix.so try_first_pass
```

```
[ /etc/pam.d/su ]  #2
auth        requisite       pam_succeed_if.so user=igloo quiet
auth        sufficient      pam_unix.so try_first_pass
```

Again, the above two configuration files differ only in the control flags, but it should be recalled again that the authentication process and the error messages exposed to the user are completely different. In the case of configuration file # 1, even if the authentication requestor is not "igloo", a password is required, but in configuration file # 2, an authentication failure is immediately returned without requiring a password.

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

Understanding of Linux PAM module


```
[root@localhost pam.d]# su test
암호:
su: incorrect password
```

[Figure 4-3] Result of authentication configuration file #1

```
[root@localhost pam.d]# su test
su: incorrect password
```

[figure 4-4] Result of authentication configuration file #2

■ CASE 2

[/etc/pam.d/su] #1

auth	required	pam_succeed_if.so user=igloo quiet
auth	sufficient	pam_unix.so try_first_pass

[/etc/pam.d/su] #3

auth	sufficient	pam_rootok.so
auth	required	pam_succeed_if.so user=igloo quiet

The following only changes the order of module configuration. The authentication process of configuration file # 1 is as follows.

1. Check that the su command requester is “igloo”
2. Check that the su command Requestor is “root”

But there is a caveat here. Since the control flag of the module that checks whether it is the “igloo” account is required, even if su is used as the root account, authentication failure is eventually returned. Therefore, the above setting allows the su command to be used only by the “igloo” account.

However, for configuration file # 3, the module's control flag is sufficient to verify that it is the “root” account. Unlike configuration file # 1, you can use the su command in two accounts, the "root" account and the "igloo" account. Also, if you use the su command as the root account, PAM does not verify that the requestor is "igloo" and immediately returns successful authentication and terminates the authentication.

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

Understanding of Linux PAM module


```
[root@localhost pam.d]# su test
암호:
su: incorrect password
```

[Figure 4-5] Result of authentication configuration file #1

```
[root@localhost pam.d]# su test
[test@localhost pam.d]$
```

[Figure 4-6] Result of authentication configuration file #2

It may look similar at first glance, but you can see that the actual authentication process and the results are very different from the configuration file # 1. Even if the same setting is changed, the result is completely different, so special attention is required for the PAM setting.

06. Conclusion

User authentication through PAM improves the convenience and security of the system operation, but if it is set incorrectly, it may impair the availability such as allowing access to unauthorized persons and invading confidentiality or blocking the access of authorized users.

Also, there's one more thing to note about using PAM other than the ones discussed earlier: that is, the permission settings of the application itself. Even if PAM is properly set, user authentication itself cannot be performed without the right to execute an application. Therefore, it must not be overlooked that the right to execute the application must be properly provided.

So far, we have looked at the structure and authentication process of PAM. Please read the above carefully to improve the security of your system.

07. Reference

[1] https://www.linux.co.kr/home2/board/subbs/board.php?bo_table=lecture&wr_id=1808
[2] https://ko.wikipedia.org/wiki/%EB%A6%AC%EB%88%85%EC%8A%A4_PAM
[3] https://kimhyun2017.tistory.com/212

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

CHAPTER 5

Special Column

Cyber security threat
and it's countermeasures
in the Block-chain era

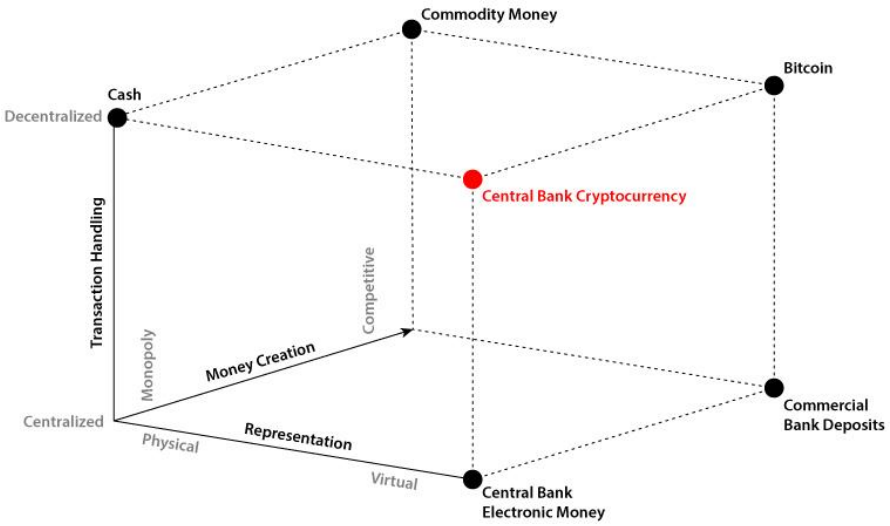
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Cyber security threat and it's countermeasures in the Block-chain era

Security Monitoring Center
Security Analysis Team

01. Synopsis

Unlike centralized system-based money, goods, electronic money and financial investment products, Bitcoin, which can be virtualized and decentralized, built a decentralized system that has secured transaction reliability and stability based on block-chain technology.



[Figure 6-1] Control Structure of Currencies
(Source : The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies)

Money or electronic money, which is commonly used as a legal currency, is guaranteed to be issued or exchanged through a central issuer. Central issuers perform data archiving and verification through centralized ledgers, but blockchain can provide distributed ledger functions through distribution, sealing and verification procedures.

Division	Archiving (Securely manage transaction history)	Validation (Validate if the transaction is abnormal)
Centralization	Store data such as transaction details and reserves among financial transaction targets in the bank server	When requesting a transaction, check whether the double payment is made based on the data stored in the bank server, and check and limit whether the amount exceeding the balance is traded.
Decentralization	Distribute transactions to everyone and seal them so that they can't be modified	Elect validators in a legitimate way, and only benefit from honest methods

[Table 6-1] Comparing Data Archiving and Validation in a Centralized and Decentralized Environment

In this issue, we will look at countermeasures to solve security threats that may occur in block-chain technology applied in various fields such as finance, public and private sectors.

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

Cyber security threat and it's countermeasures in the Block-chain era

2. How to Blockchain

Blockchains are classified into public blockchains, private blockchains, and consortium blockchains based on permissions and consensus algorithms.

Public blockchain is an open blockchain in which anyone, like Bitcoin or Ethereum, participates in the network and shares transactions and various activities that take place on the network.

In contrast, private blockchains do not share transaction details and activities other than participants authorized as closed blockchains, such as NASDAQ's Link (LINQ) or Mijin.

The consortium blockchain combines the characteristics of the public blockchain and the private blockchain, resulting in a semi-centrality based on the allied blockchain such as Corda and Hyperledger Fabric..

Division	Public Blockchain	Consortium Blockchain	Private Blockchain
Consensus Determination	All miners	Selected set of nodes	One organization
Read Permission	Public	Cloud be public or restricted	Cloud be public or restricted
Immutability	Nearly impossible to tamper	Cloud be tampered	Cloud be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Security	• Consensus Mechanism • PoW, PoS	• Pre-approved participants • Voting/multi-party consensus	• Pre-approved participants • Voting/multi-party consensus
Consensus Process	Permissionless	Permissioned	Permissioned
Consensus Core Algorithm	PoW, PoS	DPoS, PBFT, Ripple, Tendermint	DPoS, PBFT, Ripple, Tendermint

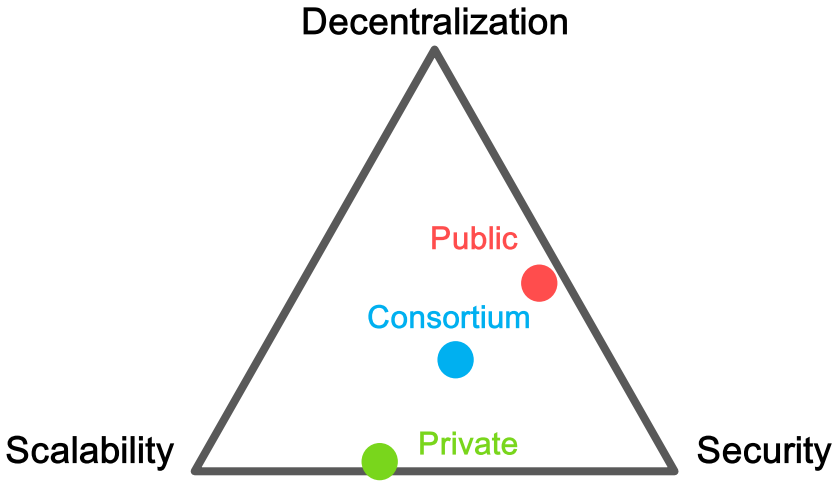
[Table 6-2] Block-chain comparison Public, Consortium, Private

The block-chain platform has evolved to solve problems of △decentralization, △scalability, and △security through Consensus Algorithm or Ledger Data format.

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

Cyber security threat and it's countermeasures in the Block-chain era

2. How to Blockchain



[Figure 6-2] Blockchain Technology based on Blockchain Trilemma

Because blockchain technology checks all ledger data against new ledgers due to distributed ledger structure, transaction processing speed decreases when network expands, which causes problems in scalability. After all, decentralization and calability are contradictory definitions, so satisfying both conditions is not an easy matter.

However, some offer technical alternatives to balance the two conditions of decentralization and scalability. Change the consensus algorithm from PoW (Proof of Work) to PoS (Proof of Stake), ▵ Delegated Proof of Stake (DPoS), ▵ On-Chain and Off-Chain, and ▵ Sharding Proposed but not a perfect alternative.

The decentralization technology of the environment built on the central ledger technology such as financial institutions not only expands, but also causes problems such as double payment, privacy protection, compliance, and cost. Technology and application are needed.

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

Cyber security threat and it's countermeasures in the Block-chain era

2. How to Blockchain

Division	Generation 1.0	Generation 2.0	Generation 3.0
Keyword	Currencies	Smart Contracts	Blockchain Trilemma
Virtual Currency	Bitcoin, Monero, Dash	Ethereum, Neo, Lisk	Cardano, EOS, IOTA
Characteristic	Distributed Ledger	Smart Contract	Completion of 2.0G block-chain limitation
Decision Making	No self-determination capability	No self-determination capability	self-determination capability
Consensus algorithm	PoW	PoW → PoS	DPOS
Trading speed (Transaction record unit)	Relatively slow	Relatively slow	Superior transaction speed
Security	• SegWit, Lightning network • Brute Force Attack, 50% hash power or gold finger, Wallet Theft, DDoS…	• Raiden network, Sharding, Plasma, TrueBit	• Blockchain Trilemma (Decentralized, Scalability, Security)
Limitation	• Low scalability • Slow transaction speed • Decision-making system difficult to reach agreement	• Decision problems • Hard Fork Proof Method • Transaction capacity limit	• Reliability due to witness contamination • Attack possible due to exposure of representative node

[Table 6-3] Generational Characteristics and Limitations by Block-chain Technology

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

Cyber security threat and it’s countermeasures in the Block-chain era

3. Blockchain Based Security Threat

Blockchain security threats are based on technical issues such as ▵ Transaction or Scalability, ▵ Transaction Finality, ▵ Interoperability, ▵ Lack of Identification and Management. Therefore, in order to solve problems caused by inherent limitations or inadequate implementation, it is necessary to understand each threat.

To this end, Based on the “Security Threats Classification in Blockchains” presented by Cloud State University, I would like to explain the security threats of the blockchain. According to the 'Security Threats Classification in Blockchains', security threats in the blockchain include ▵ Double Spending, ▵ Mining / Pool, ▵ Wallet Threat, and ▵ Network Threat, ▵ Smart Contracts Threats can be classified into five categories and 30 details.

Among all the security threats mentioned, let's take a closer look at actual damage cases and high-risk security threats.

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

Cyber security threat and it's countermeasures in the Block-chain era

3. Blockchain Based Security Threat

Security Threats	Attack Vectors	Cause
Double-Spending Threats	Race Attack	Transaction Verification mechanism
	Finney Attack	Transaction Verification mechanism
	Vector76 Attack	Transaction Verification mechanism
	Alternative History Attack	Transaction Verification mechanism
	51% Attack	Consensus mechanism
Mining/Pool Threats	Selfish Mining/Block-discard Attack	Consensus mechanism
	Block-Withholding Attack (BWH)	Consensus mechanism
	Fork-After-withhold Attack (FAW)	Consensus mechanism
	Bribery Attack	Consensus mechanism
	Pool Hopping Attack	Consensus mechanism
Wallet Threats	Vulnerable signature	ECDSA flaws – Poor randomness
	Lack of control in address creation	Public nature of the blockchain
	Collison & Pre-Image Attack	Flaws in ECDSA, SHA256 & RIPEMD 160
	Flawed key generation	Flaws in implementing ECDSA
	Bugs & Malware	Client design flaws
Network Threats	DDoS Attack	External resources, contracts underpriced operations
	Transaction Malleability Attack	Flaws in blockchain protocols –Transaction ID
	Timejacking Attack	Flaws in blochain protocols – timestamp handling
	Partition Routing Attack	Flaws in Internet routing – routing manipulations
	Delay Routing Attack	Flaws in Internet routing – routing manipulations
	Sybil Attack	Structured P2P network limitation – forge identities
	Eclipse Attack	Flaws in blockchain protocols – outgoing connections
	Refund Attack	Flaws in BIP70 payment protocol –Bitcoin refund policy
	Balance Attack	Consensus mechanism
	Punitive and Feather forking Attack	Consensus mechanism – blacklisting transactions
Smart Contracts Threats	Vulnerabilities in contracts source code	Program design flaws
	Vulnerabilities in EVM Bytecode	EVM design flaws
	Vulnerabilities in Blockchain	Program design flaws
	Eclipse Attack on Smart contract blockchain	EM design flaws
	Low-level attacks	underprice operations

[Table 6 -4] Taxonomy of Blockchain Security Threats (Source : Security Threats Classification in Blockchains)

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

Cyber security threat and it's countermeasures in the Block-chain era

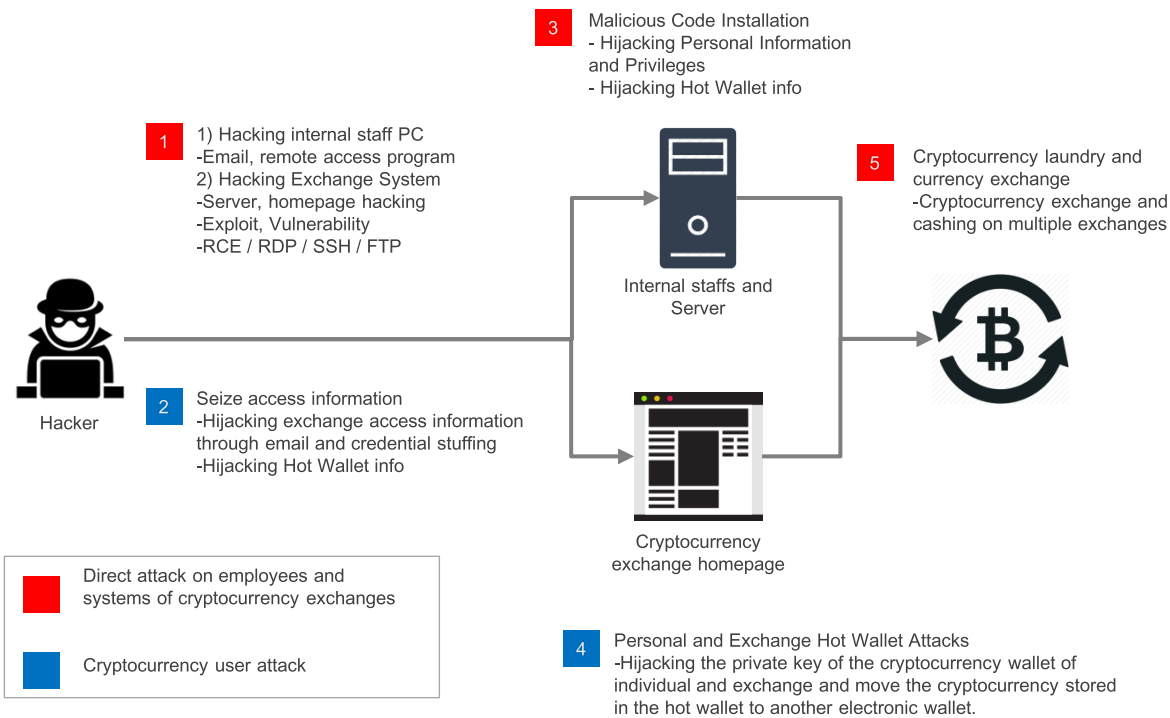
3. Blockchain Based Security Threat

1) Wallet Threats

A cryptocurrency wallet is a software program that manages private keys, public keys, and assets, rather than storing money like the functions of a wallet used in everyday life. Since the public key is the account number owned by the public key, and the private key plays a role similar to that of the account password, owning the private key means all management authority of the asset according to the public key.

Cryptocurrency wallets can be defined as 2 depending on how they work. First, there is a hot wallet that can be used in real time and is used for short-term and small-scale investments, but is likely to be exposed to hacking or writing code. Second, it is a hardware wallet like a USB storage device, which is relatively safe from the risk of hacking, and is used for long-term and large investments, but it is a cold wallet that is hard to find when the device is lost.

The security threat of a cryptocurrency wallet simply depends on the question of how securely a private key can be managed on an individual or cryptocurrency exchange. In the case of individuals, the personal PC or mobile device that stores the private key of the cryptocurrency wallet that stores the cryptocurrency is targeted for attack, or in the case of a cryptocurrency exchange, the server that stores the private key of the cryptocurrency wallet is the target of the attack. The money will be withdrawn.



[Figure 6-3] Flowchart of Cryptocurrency Wallet Attacks by Targets

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

Cyber security threat and it’s countermeasures in the Block-chain era

3. Blockchain Based Security Threat

1) Wallet Threats

Most of the cryptocurrency takeover attacks in major cryptocurrency exchanges were the transfer of the cryptocurrency's right to attackers as the private keys stored in the hot wallet were taken over. In the case of the cryptocurrency exchange in December 2014, the exchange server was attacked and the private key file was leaked, which resulted in the loss of 18,866 bitcoins that existed in the hot wallet.

As the safety issues of cryptocurrency wallets continue to arise, 70% of assets are recommended to be stored in cold wallets when managing cryptocurrency transactions.

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

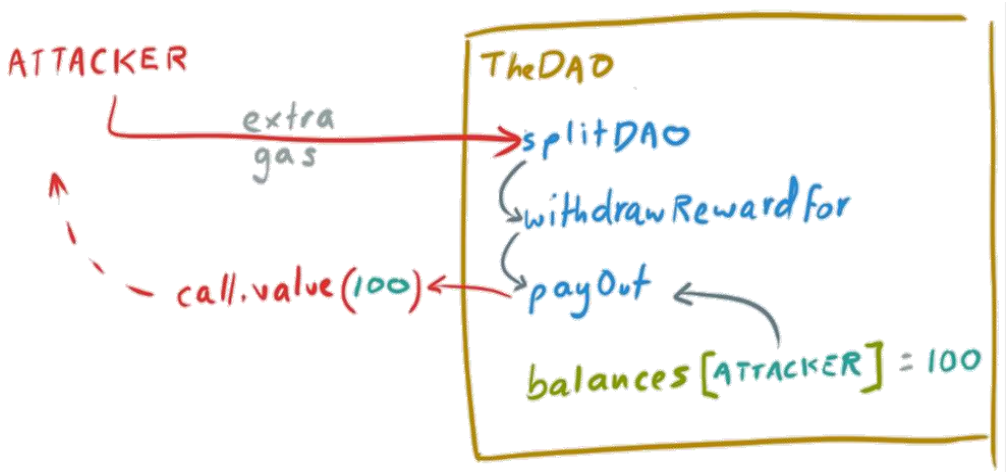
Cyber security threat and it's countermeasures in the Block-chain era

3. Blockchain Based Security Threat

2) Smart Contracts Threats

Smart Contracts is a concept originally proposed by Nick Szabo in 1994, which means 'Automated Self-Enforced Agreements' by using blockchain's Distributed Ledger Technology in P2P without an intermediary.

Representative areas of work include systems that frequently involve mutual transactions and verifications, such as finance, intellectual property, sharing economy, and logistics distribution, and that can automate tasks. Smart contracts have been released due to the reduction in transaction costs associated with existing contracts and trust based on consensus, and various services have been launched, but technical limitations have emerged due to the hacking of the Decentralized Autonomous Organization (DAO) in 2016.



[Figure 6-4] Recursive Calls Vulnerability attack flow
(Source : Solidity & Systems Programming on the Blockchain)

The vulnerability has the potential to transfer funds infinitely if any function is called before the 'splitDAO()' function, which updates the balance and sum of a particular account, is called again. In other words, if you apply for withdrawal of 500,000 $ from your A account to your account B, you can withdraw your account to your account B before deducting 500,000 $ from your 1 million $ account. In the A account, since a new withdrawal request was made before the 500,000 $ was deducted, 1 million remain intact, and the 500,000 $ withdrawn in the B account is steadily accumulated.

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

Cyber security threat and it's countermeasures in the Block-chain era

3. Blockchain Based Security Threat

2) Smart Contracts Threats

Since this double payment problem is serious enough to discuss the existence of the platform, the lead developer of the DAO project solved the problem through a hard fork, but the value was devalued in that it was a platform separation without technical improvement.

Smart contract refers to code that constitutes a blockchain-based application. Just as an application is built with a programming language such as C or Java, smart contracts are based on programming languages such as Solidity and Go.

Since it is a program implemented by a developer based on a programming language, when developing software such as ▵ input data verification and expression, ▵ security function, ▵ time and status, ▵ error handling, ▵ code error, etc. Security issues that need to be considered are revealed.

To do this, it is necessary to comply with the software development security measures, which means a series of security activities, such as eliminating potential security threats that may exist in software development and designing and implementing functions in consideration of security. In the case of smart contracts, unit testing and auditing are the most important because there are not enough security check tools available in existing programming languages.

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

Cyber security threat and it's countermeasures in the Block-chain era

3. Blockchain Based Security Threat

2) Smart Contracts Threats

Function	Contents
Re-entrancy	• Repeatedly 'Entrancy' certain features to execute code before a certain point in time • DAO hacking incident is a typical example
Message Call and Access Permission	• It is happened by Delegatecall, a Message Call Function of Solidity, which call public controller • Anyone can access when the called controller is set to Public in a contract situation where a delegate call, a kind of message calling function, calls a code of a target address.
Arithmetic Issues	• Problems caused by overflow where a value above the maximum value for integer is entered and underflow that decreases below the minimum value • Smart contracts use OpenZeppelin's SafeMath library to solve the problem.
Short address attacks	• Occurs when the target address in a transaction is short • The Ethereum platform adds a zero to the end of the address instead of invalidating the transaction for a short address, using this to send money that is much larger than the actual balance. • If the data size is short, solve the problem by validating the entered value before exception or remittance
DoS (Denial of Service)	• Attacks that generate unnecessary traffic for service denial

[Table 6-5] Security vulnerability in smart contract

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

Cyber security threat and it's countermeasures in the Block-chain era

4. Blockchain Security Countermeasures

Since blockchain is a foundation technology that can secure data security and reliability in a decentralized environment, it is most important to secure user reliability through security of the technology itself. Therefore, it is absolutely important to recognize and solve problems that may occur in the blockchain, such as intercepting negotiations, abnormal transactions, SW weakness, strengthening key management, and strengthening exchange infrastructure.

This new technology that can gain user trust when security problems that can occur in the blockchain are solved, such as monitoring abnormal participants through validation, storing optional transaction information to improve transaction processing speed, and improving consensus algorithm.

Function		Problem	Solution
Algorithm Enhancement	Intercept	• Control blockchain consensus process by controlling majority of participants	• Abnormal Participant Monitoring • Transaction Verification • Transaction throughput limit
	Abnormal transaction	• Invalid transaction in main chain	• Consensus integration • Validation check
	SW Vulnerability	• Abuse of key theft, agreement operation, etc. due to security weakness of block-chain SW	• Secure Coding • Complement and Improvement of Consensus Algorithm
	Availability degradation	• Poor availability due to blockchain processing speed limitations and increased trading volume	• Validation Participant Restrictions • Save optional transaction information
Attack response ability enhancement	Abnormal Transaction	• Possible transactions such as fraud, money laundering, double payment	• Deal Participant Management
exchange security enhancement	Enhancing key management	• Key hijacking by using cryptocurrency exchange or hot wallet	• Cold-wallet • Multi-factor authentication
	Enhancing exchange infra.	• Ongoing hacking incidents of large cryptocurrency exchanges	• Strengthen basic security rules • Enhanced Security Certification (ISMS-P, ISO27001, etc.) • Store more than 70% of assets in cold wallet

[Table 6-6] Security issues and solutions in blockchain (Source: Financial Security Agency, Blockchain Technology and Security Considerations)

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

So far, we have examined the factors and countermeasures of blockchain security threats based on the blockchain security threats announced as 'Security Threats Classification in Blockchains'. Blockchain is designed on the basis of cryptocurrency with a purpose contrary to the existing financial sector, but its value is recognized in various fields based on distributed environment such as identity verification, document storage, and financial transaction management.

In particular, the financial and public sectors are promoting various projects to revitalize the ecosystem of the blockchain industry. In addition, the company has been making steady efforts to discover new businesses that serve as a bridgehead for overseas market development or combine blockchain technology. Most of us are optimistic about the new market that guarantees the security and reliability of data, but there are some problems that need to be solved such as data processing or compliance for actual application. Careful, long-term, and profitable business perspectives should be used to ensure the effectiveness of the blockchain application.

5. Reference

[1] The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies
https://research.stlouisfed.org/publications/review/2018/02/13/the-case-for-central-bank-electronic-money-and-the-non-case-for-central-bank-cryptocurrencies
[2] Security Threats Classification in Blockchains
https://pdfs.semanticscholar.org/91bb/bb31101cbc2e803726d7210b4100f7b09ac5.pdf
[3] Solidity & Systems Programming on the Blockchain
https://pospi.github.io/talk-solidity-blockchain-intro/#66
[4] Common Vulnerabilities and Exposures
https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures
[5] Financial Security Agency, Blockchain Technology and Security Considerations
https://www.fsec.or.kr/common/proc/fsec/bbs/42/fileDownLoad/1267.do
[6] Virtual Currency Myth and Reality (Extended Version of GFIN Open Seminar)
https://www.slideshare.net/skim71/virtual-currency-myth-and-reality-extended-version-of-gfin-open-seminar-86608238

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

CHAPTER 6

Focus On IGLOO Security

1. IGLOO SECURITY announces '2020 Security Threats and Technology Forecast Report'

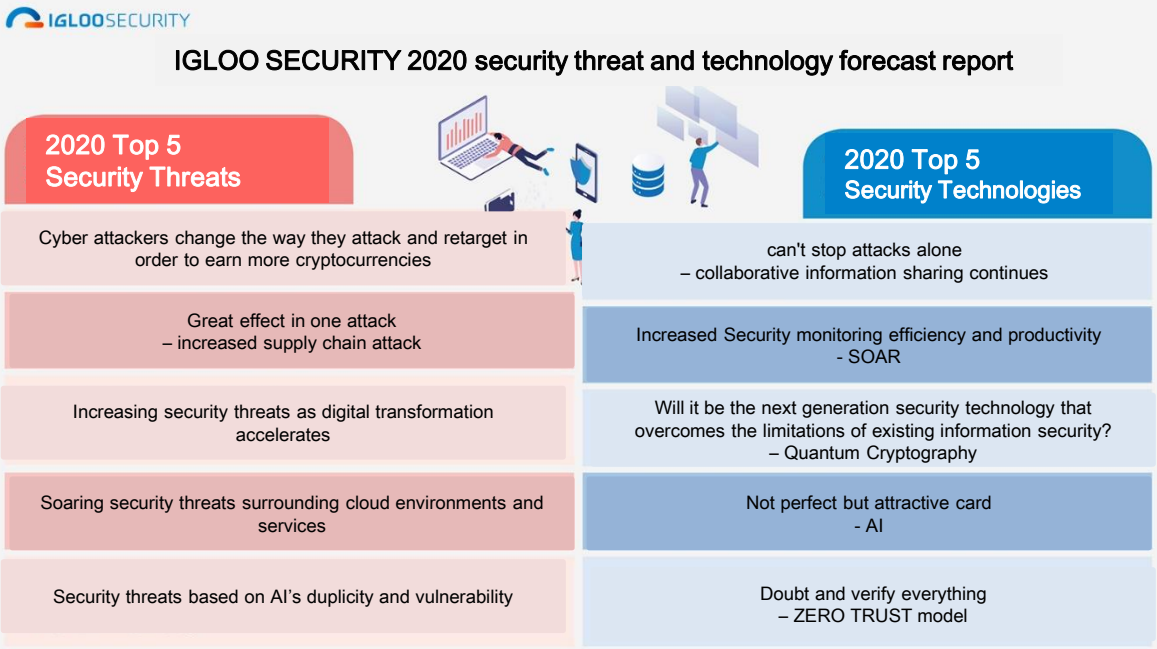
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Focus on IGLOO Security

IGLOO SECURITY announces '2020 Security Threats and Technology Forecast Report'

'2020 Security Threats and Technology Forecast Report'

- Complex threats will grow and spread unprecedentedly… Need to introduce security methodologies and technologies that focus on accurate threat analysis and rapid response
- 'Information Security Mock Test' event on Igloo Security homepage from 5th to 11th



[5th December 2019] Igloo Security Co., Ltd. (CEO Lee, Deuk-Choon, www.igloosec.co.kr/en) unveiled the '2020 Security Threats and Technology Forecast Report,' which contains major forecasts for 2020 security threats. The eighth report, based on the Igloo Security Security Analysis team's forecasts, lists the major cybersecurity threats that will occur in 2020 along with security technologies and methodologies to address them.

The security analyst team predicted that the digital transformation based on next generation IT technologies will accelerate, increasing the number of complex security threats that have not been experienced before. Defenders require active security methodologies and technologies that focus on pinpointing and responding quickly to threats inside and outside the enterprise that an attacker may target.

On the other hand, IGLOO SECURITY held the "Information Security Mock Test" event on Igloo Security Facebook from 5th to 11th in commemoration of the report. Visit the Igloo Security homepage, download a screen saver with 2020 security threats and technology outlooks, and refer to the screen saver contents to answer Mock 2 questions. A total of 50 participants from the event were presented with a gift of Chicken Gifticon. The winners were announced on Igloo Security Facebook on the 13th.

Kim Mi-hee, head of the Iglu-Security Security Analysis Team, said, "With the change of IT infrastructure environment, it is expected that more and more intelligent attacks that cannot be countered by the existing defense system will increase. Defenders will need to respond more quickly and proactively to security threats by leveraging a variety of security technologies and methodologies, including AI (artificial intelligence), security orchestration, automation, and response (SOAR), and threat intelligence. "He emphasized.

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

We Know SECURITY!

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

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