Monthly Security Report

2020
July

Cover Story

How to use the new add on dashboard of SIEM

Multimedia steganography

IGLOOSECURITY

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

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

Cover Story

1. Monthly Security Issue

- Security Issue

2. IGLOO Statistics

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

3. SIEM Guide (SPiDER TM V5.x)

- How to use the new add on dashboard of SIEM

4. Tech Note

- Multimedia steganography

5. Focus On IGLOO Security

- This month's IGLOO Security

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

Cover Story

CHAPTER 1

Monthly Security Issue

1. Security issue

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

1 Security Issue

A shopping mall pretending to be a phishing attack

- As the mask became popular, a phishing attack appeared, impersonating the shopping mall W that sold it. When using a phishing site, caution is required because personal information may be leaked and money may be stolen.
- According to EST Security, a phishing site that copied W, a famous mask shopping mall that recorded a mask out-of-stock after Corona 19, was caught..
- The phishing site captured this time was made to look like a normal site domain without careful attention, with only one letter changed among the normal site domains.
- The attacker induces infection by registering false postings impersonating mask-related information several times in a domestic portal site cafe and distributing phishing site domains.
- This site looks like a normal site, but when users sign up for membership on this site, their personal information is immediately passed on to the attacker.
- Security experts say that through the fake site, which is almost the same as the normal site, the threat of stealing personal information and money is increasing.

Malicious code advisory disguised as a product activation tool

- Recently, malicious code targeting users who want to use software illegally has been distributed.
- According to Ahn Lab, the malicious code “Vidar” disguised as an illegal activation tool for MS products is being distributed.
- Attackers spread malicious executable files disguised as'KMSAuto' or'KMSPico', which are illegal activation tools for MS products, through various channels such as P2P sites and illegal download sites.
- When the user executes the malicious executable file, the password input window appears. If you enter the password provided by the attacker and click the OK button, the illegal activation tool and Vidar malware will be installed at the same time.
- Vidar malware can leak key information from the infected PC to the outside, and even download other malicious codes afterwards to perform additional malicious actions.
- Security experts say that information that is stolen by an attacker can be exploited for various crimes such as money theft or account theft in the future, and it is recommended that users use regular software and refrain from using suspicious websites or P2P.

Massive DDoS attacks on U.S. ICT companies

- A recent DDoS attack targeting major ICT companies in the United States appears to be continuing.
- Forbes cited data from a communication monitoring site, DownDetector, and explained that there was a phenomenon in the eastern and midwestern United States.
- Targets of attack include mobile carriers (T-Mobile, Verizon, AT&T, Sprint), SNS operators (Facebook, Instagram, Twitter, Snapchat), video streaming service providers (Netflix, Hulu), game companies (Fortnight), financial companies (Chase Bank, Bank of America).
- Nothing is known about the attack behind. While global hacking group Anonymous pointed to China behind the attack, security expert Marcus Hutchins said it was unlikely to be an attack on the United States.

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

1 Security Issue

Sprinkle ransomware on YouTube-Guide to recovery method with Tor browser

- Ransomware malware that encrypts files in the user's PC has recently been distributed through various paths such as YouTube and Tor Browser, which requires special attention from the user.
- According to the Korea Internet & Security Agency's “Quarterly Report on Ransomware in the 1st Quarter,” about 50 types of ransomware were identified, including 30 new ransomware.
- Some of the notable attacks are :
  -In March, a case of ransomware was discovered through YouTube channel of 120,000 subscribers. This YouTuber launched an attack by inserting a ransomware executable file aimed at users who want to install pirated software. The YouTuber demanded 0.02 bitcoin at the cost of decryption, and threatened that recovery was impossible after 48 hours.
  -Of these, some variants of the ‘Ako’ ransomware, first discovered in January of this year, required victims to install a Tor browser to access specific sites to check data recovery methods and decryption costs.
  - Also known as “Snake” ransomware targeting the Industrial Control System (ICS). This ransomware is written in Go, a programming language developed by Google, and is considered to be a ransomware targeting ICS in terms of terminating the process used in ICS.

Cyber attacks aimed at cloud apps for telecommuting

- In order to prevent the spread of Corona19, the number of cyber attacks targeting cloud-based apps, such as video conferencing and collaboration tools, has increased by more than six times as the remote work spread worldwide.
- According to a report that McAfee surveyed 30 million McAfee customers, it was analyzed that the number of remote attacks targeting cloud-based services increased by 630% from January to April.
- Attackers were conducting attacks by buying large amounts of login credentials that users use to log in to cloud-based services or by indiscriminately substituting existing leaked credentials.
- Due to the nature of cloud-based apps that allow users to log in from anywhere, cyber attacks can be suspected when access is made from locations where there is no login history or multiple login attempts to the same account occur at short intervals.
- Security experts say that attacks targeting cloud-based services, which are increasingly used by Corona 19, are also on the rise, and emphasized that a security response system should be prepared for this by introducing multi-factor authentication.

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

Cover Story

CHAPTER 2

IGLOO Statistics

1. Monthly attack service and trend analysis

   01. Top 10 monthly vulnerability attacks

   02. Event by vulnerability compared to previous month

   03. Top 10 monthly attack service(port)

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

   05. Top 10 monthly attack service patterns

   06. Monthly attack service incident patterns compared to previous month

2. Detailed analysis according to different patterns

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

1 Monthly attack service and trend analysis

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

01. Top 10 monthly vulnerability attacks

In the TOP 10 of vulnerability attacks collected during the month of July 2020, access to WordPress sample pages and web attacks such as SQL Injection are strong. On the other hand, the RCE attack of DrayTek Vigor Remote Code Execution (CVE-2020-8515) was greatly reduced.

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

Rank	Pattern	No. of cases	Ratio(%)	Fluctuation
1	WordPress Sample Page Access	1,072	18.41%	▲4
2	Zyxel Remote Code Execution (CVE-2020-9054)	916	15.73%	▼1
3	SQL Injection	723	12.42%	▲3
4	ThinkPHP Remote Code Execution Vulnerability	565	9.70%	▼1
5	phpMyAdmin Sample Page Access	547	9.39%	▼1
6	Command Injection (Netgear Routers Vulnerability)	462	7.93%	▲3
7	MVPower DVR Shell Unauthenticated Command Execution	415	7.13%	▲1
8	Method(Connect)	395	6.78%	NEW
9	URL extension access control	397	6.82%	▼2
10	DrayTek Vigor Remote Code Execution (CVE-2020-8515)	331	5.68%	▼8
	Total	5,823	100.00%	-

[Table2-1] TOP 10 monthly vulnerability attacks

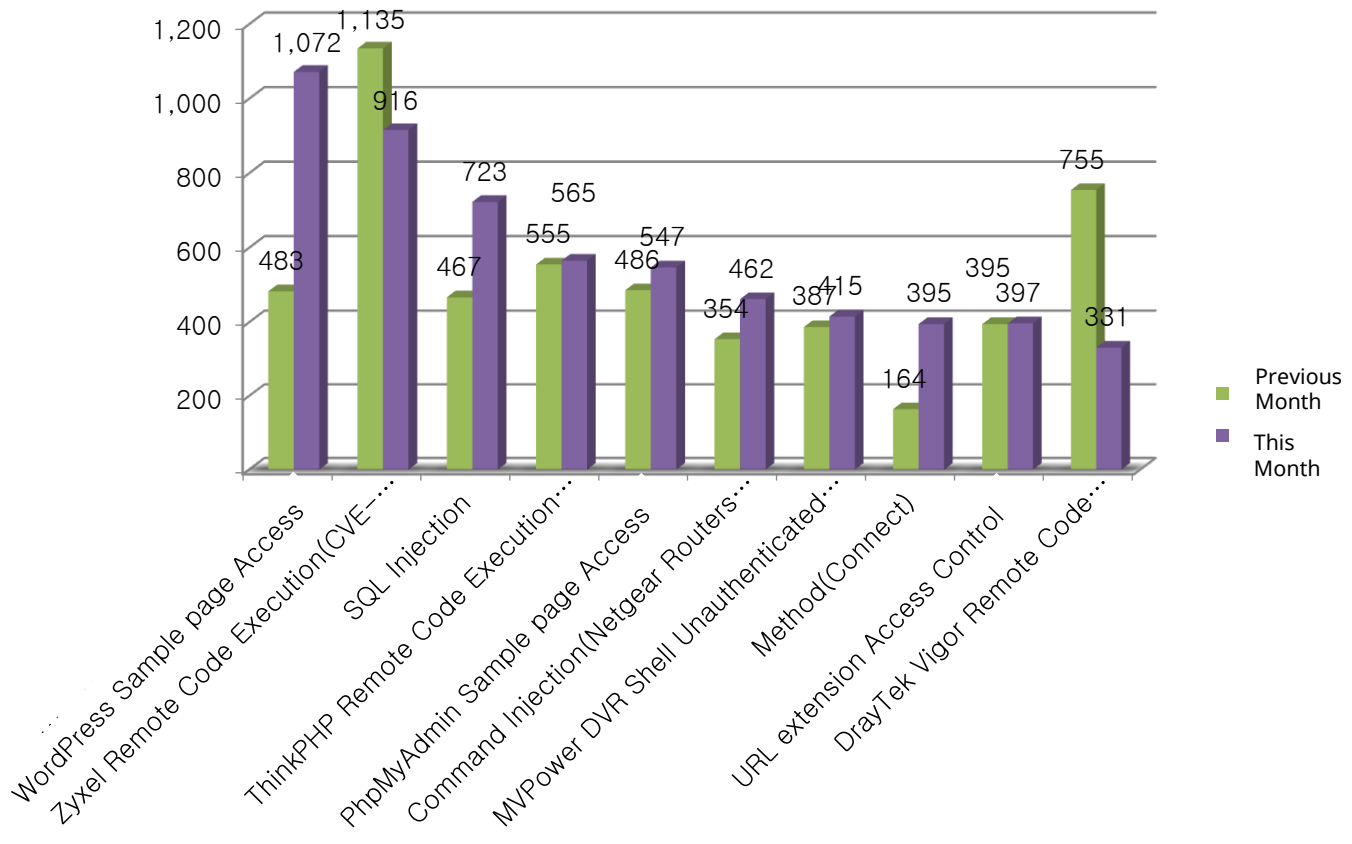
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

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

02. Event by vulnerability compared to previous month

As a result of analyzing vulnerability events collected for one month in July 2020, WordPress sample page access and SQL Injection attacks increased significantly compared to the previous month. Hold it and need attention from security personnel. And the Method(Connect) event has entered the top 10. If an attacker uses the Connect method, it is possible to use the method as an intermediate way for attack, so it is recommended to limit the methods that are not required for work.



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

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

1 Monthly attack service and trend analysis

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

03. Top 10 monthly attack service(port)

In the top 10 service ports collected for a month in July 2020, events using SNMP (UDP/161) and MSSQL (TCP/1433) ports increased compared to the previous month, ICMP (0/ICMP), Telnet (TCP/23), Unsigned (TCP/7178) showed a downward trend compared to the previous month.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of cases	Ratio(%)	Fluctuation
1	HTTPS(TCP/443)	1,074,639,060	38.34%	-
2	DNS(UDP/53)	993,961,603	35.46%	-
3	Microsoft-DS(TCP/445)	242,814,598	8.66%	-
4	HTTP(TCP/80)	175,503,559	6.26%	-
5	SNMP(UDP/161)	92,555,319	3.30%	▲1
6	ICMP(0/ICMP)	91,792,102	3.28%	▼1
7	MSSQL(TCP/1433)	36,071,606	1.29%	▲2
8	Telnet(TCP/23)	35,797,714	1.28%	▼1
9	Unsigned(TCP/7178)	31,903,423	1.14%	▼1
10	Unsigned(TCP/9900)	27,689,281	0.99%	-
	Total	2,802,728,265	100.00%	-

[Table 2-2] Monthly attack service (port) TOP 10

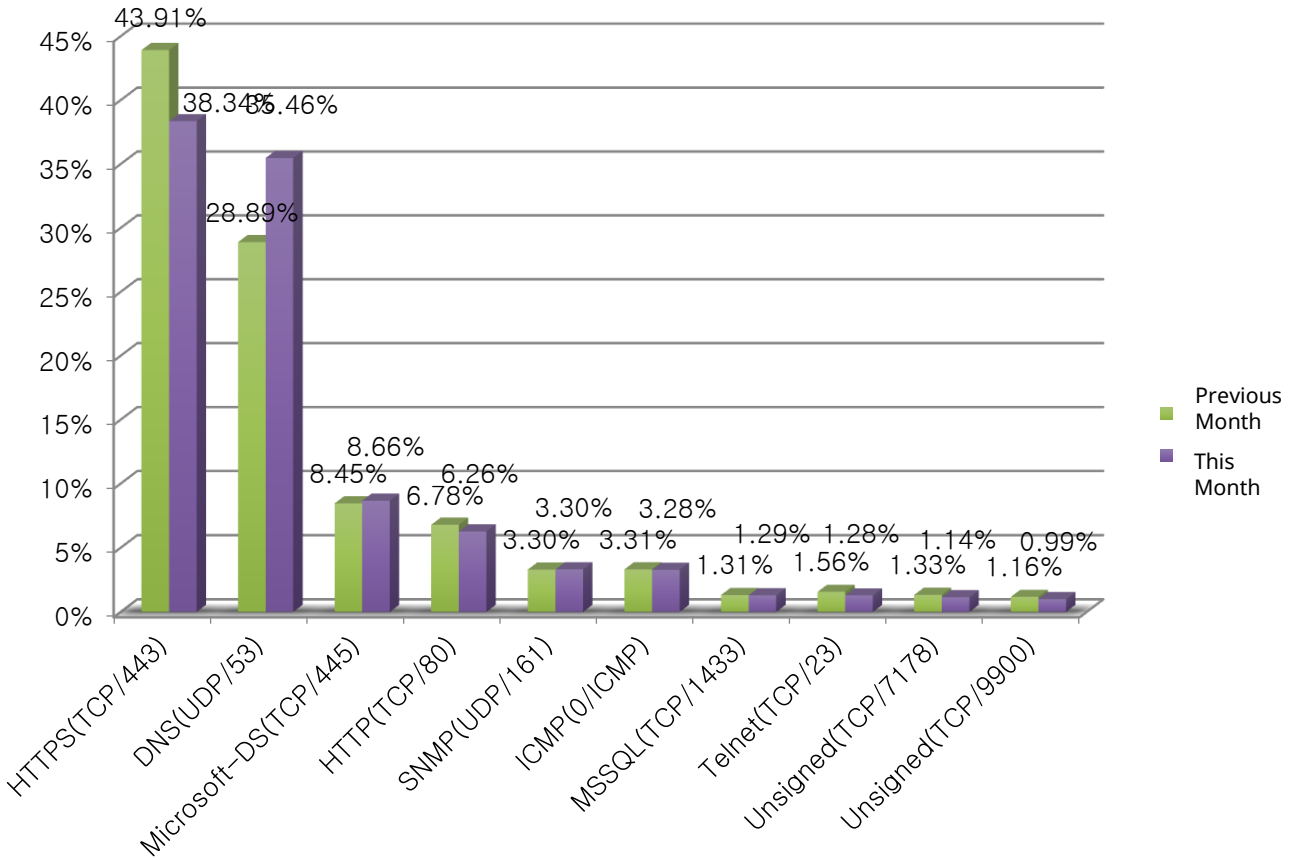
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

1 Monthly attack service and trend analysis

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

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

As a result of event analysis collected for one month in July 2020, HTTPS and DNS service ports continue to have a high share, and most of the lower-ranking service ports of the top 10 monthly attack services this month are service ports not specified in Well-Known Port Was confirmed. Among the unclear service ports, there are service ports used by each company, but it is most likely not. It is recommended to check access to undefined service ports and control access through firewall policy establishment.



[Figure2-2] TOP10 monthly attack port

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

1 Monthly attack service and trend analysis

The trend of attack patterns detected by IGLOO SECURITY SOC can be used to identify the trend of the latest attacks.

05. Top 10 monthly attack service patterns

The ACK Port Scan (F/W Scan), Dcom_TCP_Sweep (MSBlaster Worm Messenger...), and Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137) event rankings rose slightly in the attack pattern TOP10 in July 2020. , HTTP Login Brute Force, Multi Packet Inspection event rankings are confirmed to have fallen. Other POP3 Login Brute Force events have entered the rankings.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	1,685,637,030	97.69%	-
2	Ack Storm	18,650,804	1.08%	-
3	ACK Port Scan(F/W Scan)	6,682,282	0.39%	▲1
4	Dcom_TCP_Sweep(MSBlaster Worm Messenger...)	3,640,786	0.21%	▲2
5	Netbios Scan (Messenger RPC Dcom MyDoom...) (UDP-137)	2,938,786	0.17%	▲2
6	HTTP Login Brute Force	2,913,746	0.17%	▼3
7	TLS Malformed Handshake DoS	1,989,628	0.12%	▲1
8	Multi Packet Inspection	1,107,578	0.06%	▼3
9	POP3 Login Brute Force	1,067,322	0.06%	NEW
10	FIN Port Scan	780,922	0.05%	-
	Total	1,725,408,884	100.00%	-

[Table 2-3] TOP10 monthly attack pattern

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

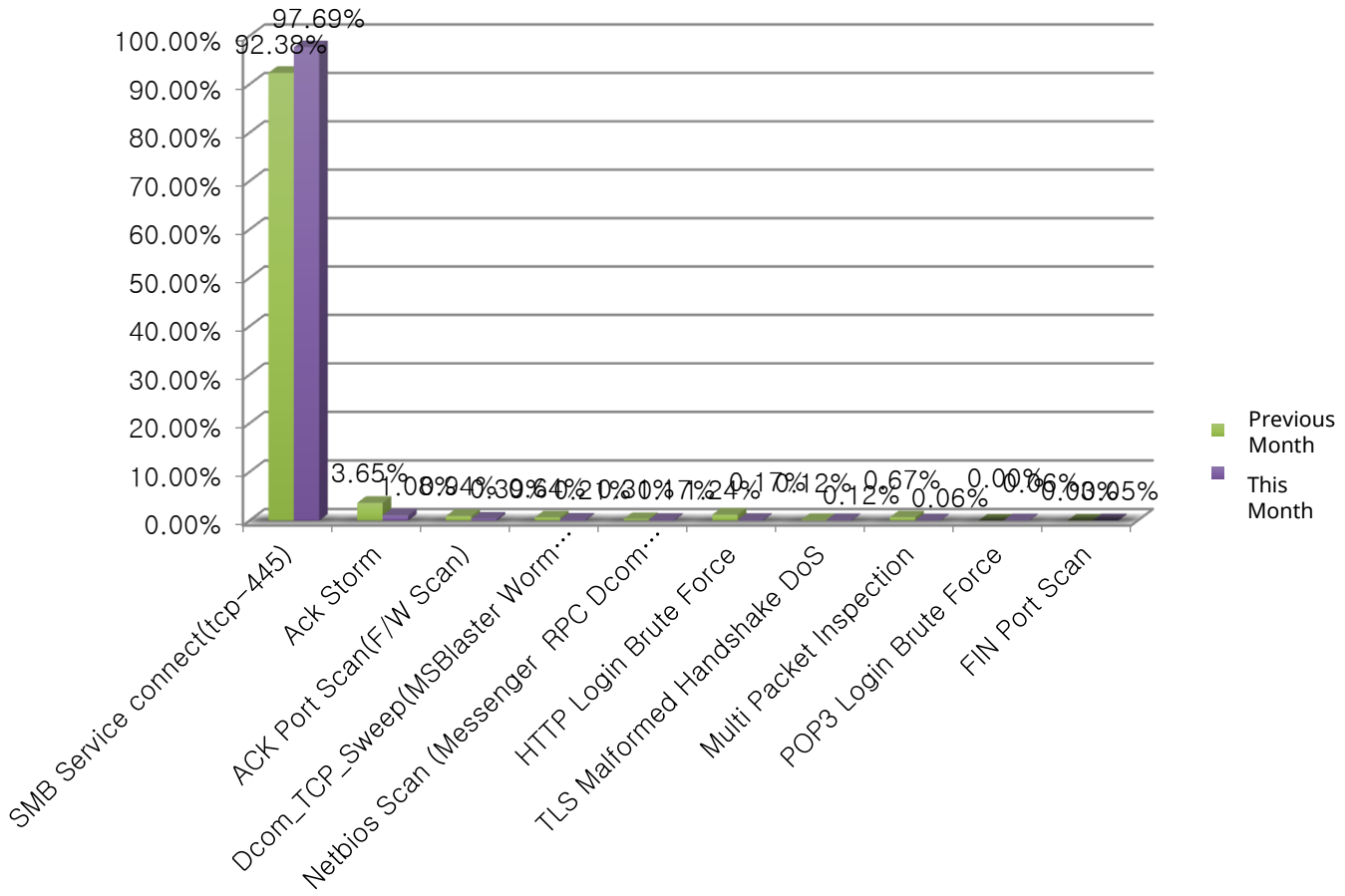
1 Monthly attack service and trend analysis

The attack pattern rankings detected by IGLOO SECURITY SOC can be used to identify the latest trends of attacks.

06. Monthly attack service incident patterns compared to previous month

The attack pattern event using SMB Service connect (tcp-445) accounted for 97% of all attacks in the Top Attack Pattern in July 2020. This is an increase of about 1,040,000,000 compared to the previous month, which is very high. Accordingly, it is considered that special attention is required for the SMB port.

After identifying whether the SMB service is used in the internal network, it is recommended to block external SMB access through the firewall policy and to prevent malicious code or unnecessary access from other client PCs using the anti-virus program and firewall function.



[Figure 2-3] Monthly event comparison by Attack(Pattern)

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

2 Detailed analysis according to different patterns

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

Attack Pattern	Detailed Analysis Results
SMB Service connect (tcp-445)	Microsoft Windows uses SMB protocol to share files and printer resources with other computers. Sharing resources using SMB in older versions (95, 98, Me and NT) of Windows used TCP port 137 and 139 and UDP port 138 by executing NETBIOS with NETBIOS over TCP/IP. On older versions of Windows 2000/XP, it was possible to run SMB directly through TCP/IP on TCP port 445. If the files are shared with easily guessable password or passwords are not set, they can suffer from secondary attacks.
Ack Storm	Attacker sends a large amount of TCP / IP Ack signal to the target server, and the target server is an attack method that creates unnecessary load and delays normal service. This attack is also used to Hijacking the packet in which the Session is made.
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 worm that spreads by using the DCOM RPC Buffer Overflow vulnerability. The worm checks whether the TCP / 135 port is enabled and infects the system when it is found. The infected system activates TCP / 4444 port, downloads malicious files from the host server, registers them in the registry, and in this process, traffic from the infected system may increase.
Netbios Scan (Messenger RPC D com MyDoom...) (UDP-137)	NetBios checks each other's information through UDP port 137, establishes a session with TCP 139, and exchanges data through TCP 138. An attacker can use this UDP port 137 to establish a session with the target system and scan information about the folders and networks shared on the target system.
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).
TLS Malformed Handshake DoS	TLS Malformed Hadnshake DOS attack is a type of DOS attack using a maliciously manipulated TLS packet. It occurs during the handshake of a maliciously manipulated TLS client. It is an attack that a remote attacker can cause a load on the victim system by sending a maliciously crafted TLS packet to the affected system.
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.
POP3 Login Brute Force	By accessing POP3 (110/tcp), the attacker attempts to log in manually or through a program using a list of IDs and passwords previously created. An attacker can obtain the system user's account and gain access.
FIN Port Scan	This method can be used as a faster alternative to the normal TCP port scan. It scans by observing the host's response to the TCP FIN packet to find the TCP port it is listening on. The target host uses the property of sending a response only when it is sent to the non-listening port when there is no response when the FIN is sent to the listening port. The port is checked without actually initiating a TCP connection.

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

Cover Story

CHAPTER 3

SIEM Guide (SPiDER TM V5.x)

How to use the new add on dashboard of SIEM

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

How to use the new add on dashboard of SIEM

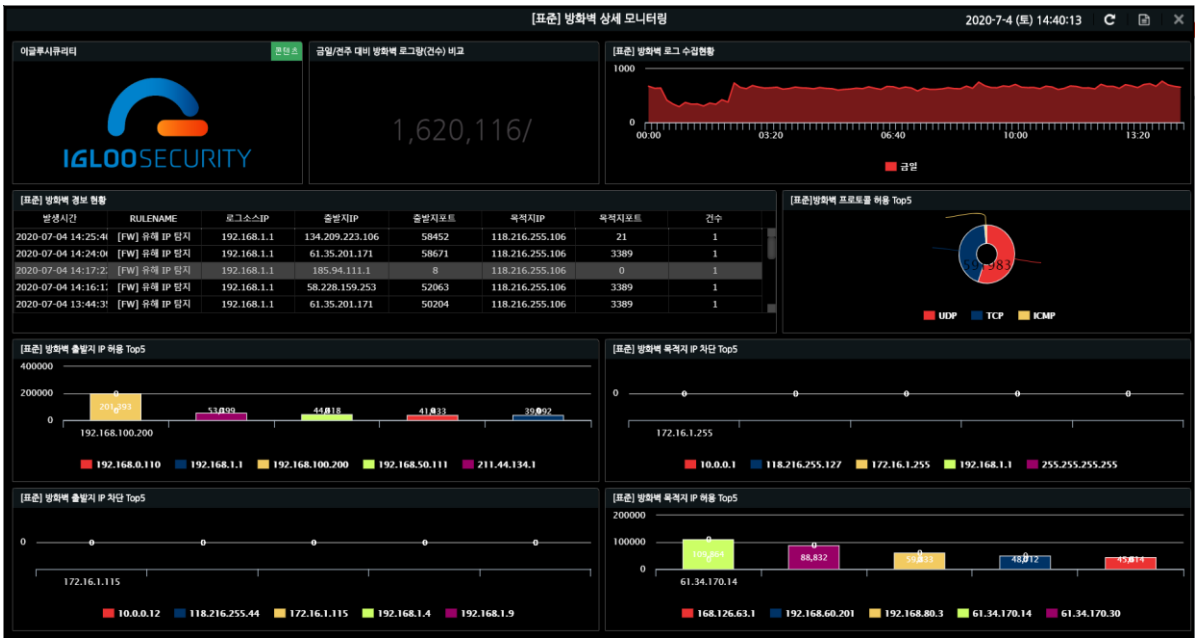
Technical Support Center
Analysis Tech. Team

01. Overview

What are the conditions for a good “dashboard”? The conclusion from the search on multiple sites is that “if you can give users insight beyond the data within 5 seconds”, that is a good dashboard.

SPiDER TM, our big data analysis solution, provides user-defined dashboards to collect and present various data. The dashboard provides a flexible screen suitable for various security device and other systems by combining widgets of table, circle, bar, linear, and text.

Below is the basic screen of the user-defined dashboard currently in use. If you ask about the screen to monitor the TopN status and the alert status of the firewall or whether you can give insight within 5 seconds, it seems that it is somewhat insufficient. To solve this problem, we introduced a product called **Unified Dashboard**. Let's see how you can use the new dashboard.



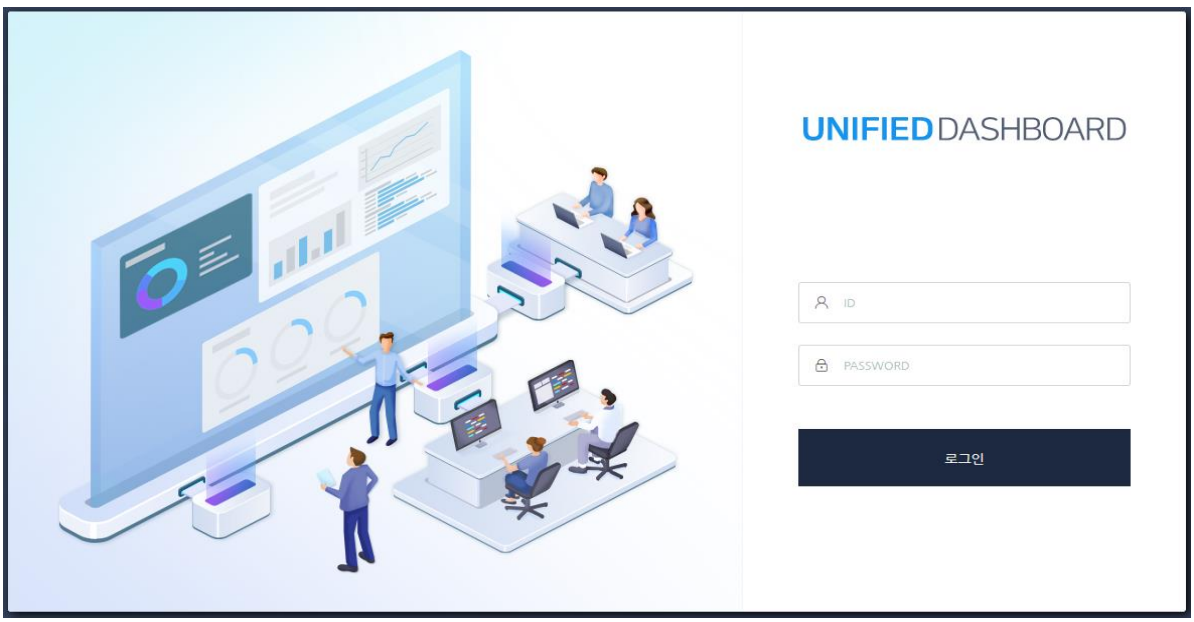
[Figure 3-1] User-defined Dashboard

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

How to use the new add on dashboard of SIEM

02. UNIFIED DASHBOARD

The new dashboard name of SPiDER TM is **UNIFIED DASHBOARD**, and the integrated dashboard can be applied to most of our solutions using API.



[Figure 3-2] UNIFIED DASHBOARD Main Screen

03. New widget of UNIFIED DASHBOARD

The new dashboard provides **various widgets** and secures visibility and readability of the dashboard. Through various widgets, various data collected in SIEM can be displayed.

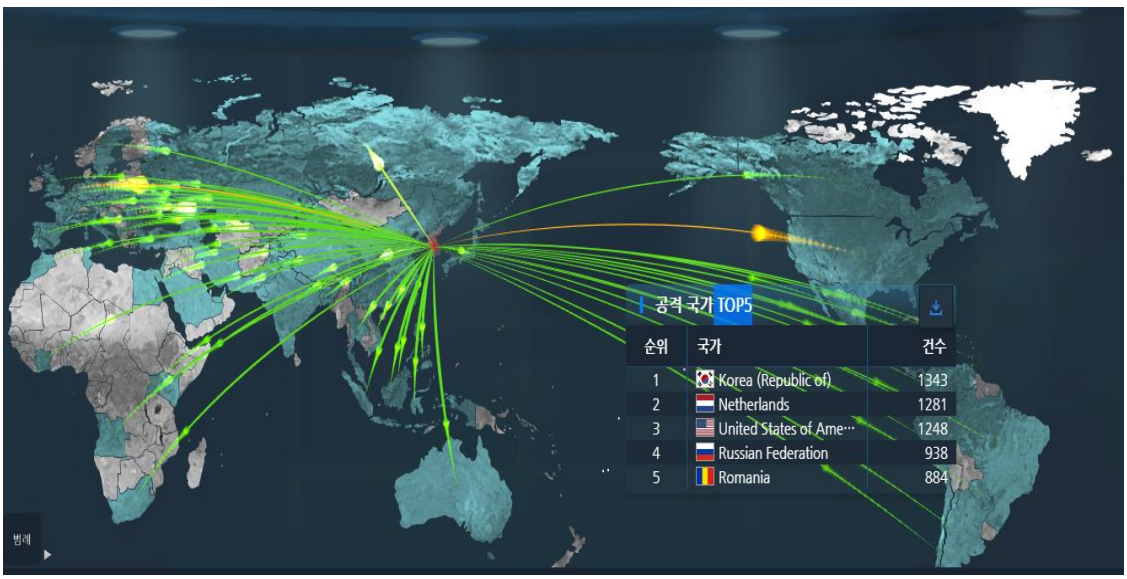
[Figure 3-3] Widgets of UNIFIED DASHBOARD

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

How to use the new add on dashboard of SIEM

04. 3D Visualized Dash board

UNIFIED DASHBOARD supports 3D visuals and can be used for **briefing based on SIEM data**. As shown in the figure below, it can be used as a world map and a globe, so it is possible to grasp at a glance how many events are coming based on the data coming from SIEM.



[Figure 3-4] 3D World Map in Dashboard

[Figure 3-5] 3D Globe in Dashboard

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

How to use the new add on dashboard of SIEM

05. Use of dashboard

1) For Briefing

It is very important for security officers in the field to have a briefing dashboard to check the status at a glance. [Figure 3-6] and [Figure 3-7] below are briefing dashboards applied to actual sites. The cyber safety center dashboard is more intuitive and cyan than the existing user-defined dashboard, so you can grasp the status of the site at a glance.

[Figure 3-6] Dashboard for briefing (1)

[Figure 3-7] Dashboard for briefing (2)

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

How to use the new add on dashboard of SIEM

05. Use of dashboard

2) For Practical work-1

The practical dashboard is the expression of the event processing data or event relationship that is considered to be an important task in the actual security monitoring center. Examples of data that can be applied in SIEM are as follows.

1. Detection of abnormal response packet-causing IP from web server through reputation detection
2. Based on reputation detection, blacklist IP (CTI) is used to detect the access base
3. IP detection accessing 443 ports from the log blocked by 80 ports from the IPS device through reputation detection

[Figure 3-8] Monitoring dashboard using reputation detection function (1)

Item 1 monitors by checking the IP of the overseas departure originating the 400~500 abnormal response code among the web server's response codes, and examines whether or not it is blocked through the number of attempts.

Item 2 is examining whether to block by checking the IP accessing into the monitoring area through the CTI function of igloo security.

Item 3 was created for the purpose of storing the blocked data from the IPS to 80 ports through the reputation function and blocking when the stored IP accesses 443. In case 3, 80 ports can be managed and blocked in IPS, but 443 packets could not be blocked, which was used as a method to block the same attack of 443 of the web server.

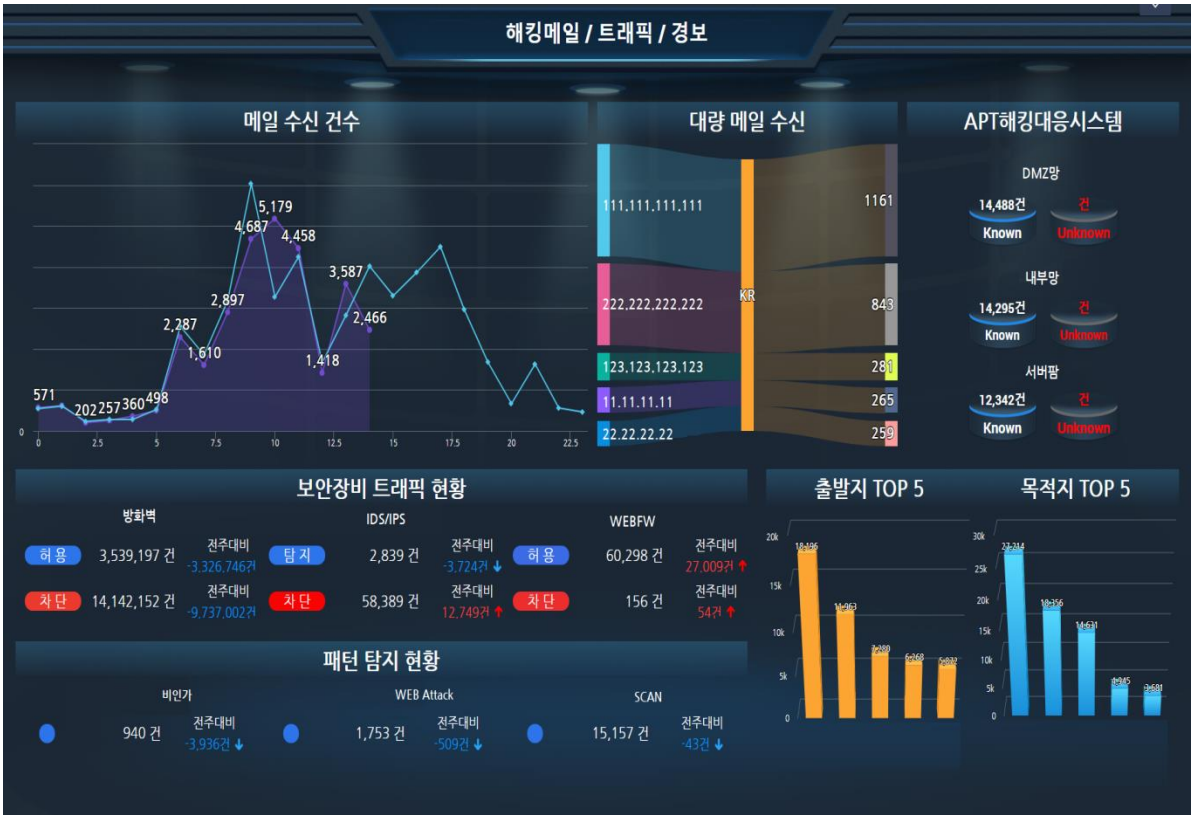
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

How to use the new add on dashboard of SIEM

05. Use of dashboard

3) For Practical work-2

This dashboard is equipped with mail-related widgets that are viewed as important data on the actual security monitoring site, and it analyzes and blocks advertisement mail in suspicion. A dashboard for analyzing and analyzing unknown patterns other than the known patterns of the APT response system is applied, and it is a dashboard of widgets that express the TOPN of the basic security device traffic status and alarm IP standards where important patterns were detected.



[Figure 3-9] Monitoring dashboard using reputation detection function (2)

Through the dashboard, the monitoring agent checks the mass-received IP, etc., and blocks the firewall when an ad-mail is generated. When an unknown attack of the APT device is detected, the system immediately accesses the system to check and process the event.

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

How to use the new add on dashboard of SIEM

06. Conclusion

Unlike the existing user-defined dashboard, **the UNIFIED DASHBOARD**, which was introduced this time, is expected to secure visibility through various widgets and improve readability, thereby helping not only in briefing but also in practice. It can be said to be a dashboard that can express the expression "Insight in data within 5 seconds" that I mentioned earlier.

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

Cover Story

CHAPTER 4

Tech Note

Multimedia steganography

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

Multimedia steganography

Security Monitoring Center
On-Site Monitoring Team

01. Overview

Steganography is a secret method of hiding secrets in visible places such as images and videos. It has been used as a way to send and receive secret messages since ancient Greece. Steganography was used worldwide when Osama bin Laden exchanged messages with terrorists during the 9/11 attacks.

Steganography has moved into the digital world and has evolved in many ways. In particular, hackers are using steganography techniques to hide malicious code in addition to simply sending a secret message.

In the past, steganography used a method of concealing data by manipulating it in photos. Recently, data is concealed using video or audio to hide large data. Moreover, with the development of multimedia, even the general public can easily make ultra-high-definition videos, and the capacity of the video itself is also large, so it can hide the problem that the file size is larger than the apparent message that was the biggest weakness of steganography.

Therefore, video steganography is used as the most suitable hiding place when the data to be hidden is large.
Let's summarize how to create a video steganography by creating a virtual volume without additional equipment and how to infer it.

Video steganography has traditionally used a space-based method and a frequency-based method, and requires a thoroughly prepared video and time to perform the method. Therefore, the probability of detection was small, but practical use was difficult without a professional user.

Method	Description
Space Steganography	Production of steganography images using pixel values of images Modulate the least significant bit (LSB) in the spatial domain using the limits of the human eye
Frequency Steganography	A technique that hides data by manipulating the least significant bit (LSB) that has undergone quantization after DCT (discrete cosine transform) during JPEG compression. A typical video steganography technique that is achieved during JPEG compression.

[Table 4-1] Video Steganography methods

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

Multimedia steganography

02. Multimedia steganography

1) VeraCrypt

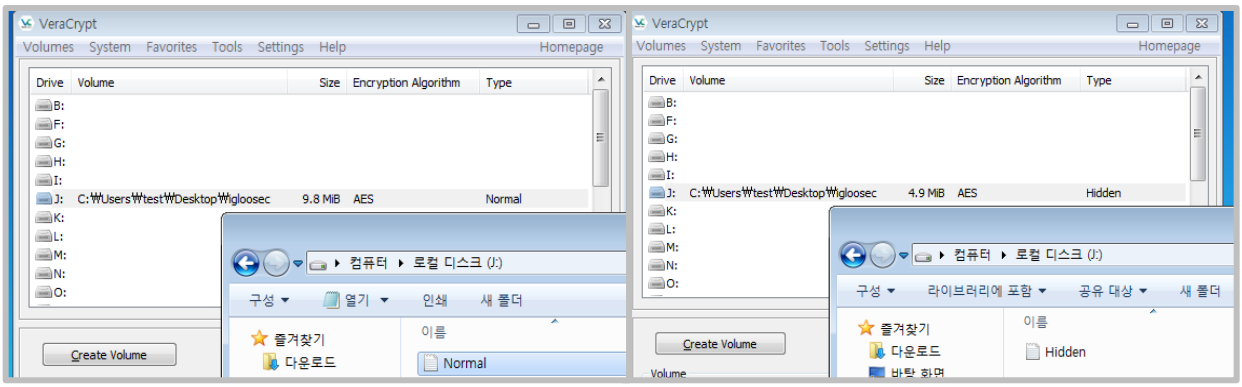
It is an encryption program that protects the data stored in the volume by creating an encrypted virtual volume. VeraCrypt software is required to access the data stored in the volume with VeraCrypt, and the password created at volume creation is entered and mounted.

Among the functions of VeraCrypt, the hidden volume refers to an additional hidden volume in addition to the existing encrypted volume. As shown in [Figure 4-1], a normal volume means an encrypted volume without a hidden volume, and as shown in [Figure 4-2], the hidden volume is an encrypted volume in addition to the normal volume space. The advantage of a hidden volume is unknown, because in the absence of a hidden volume, the area is filled with random data, and the hidden volume and random data cannot be distinguished.

VeraCrypt attempts to decrypt by receiving the password, and if the password fails, decrypts the hidden volume. The normal volume is set to a moderately difficult password with Decoy, and the hidden volume can be successfully hidden by increasing the password strength.

[Figure 4-1] Normal Volume Structure

[Figure 4-2] Hidden Volume Structure



[Figure 4-3] Normal Volume & Hidden Volume mount

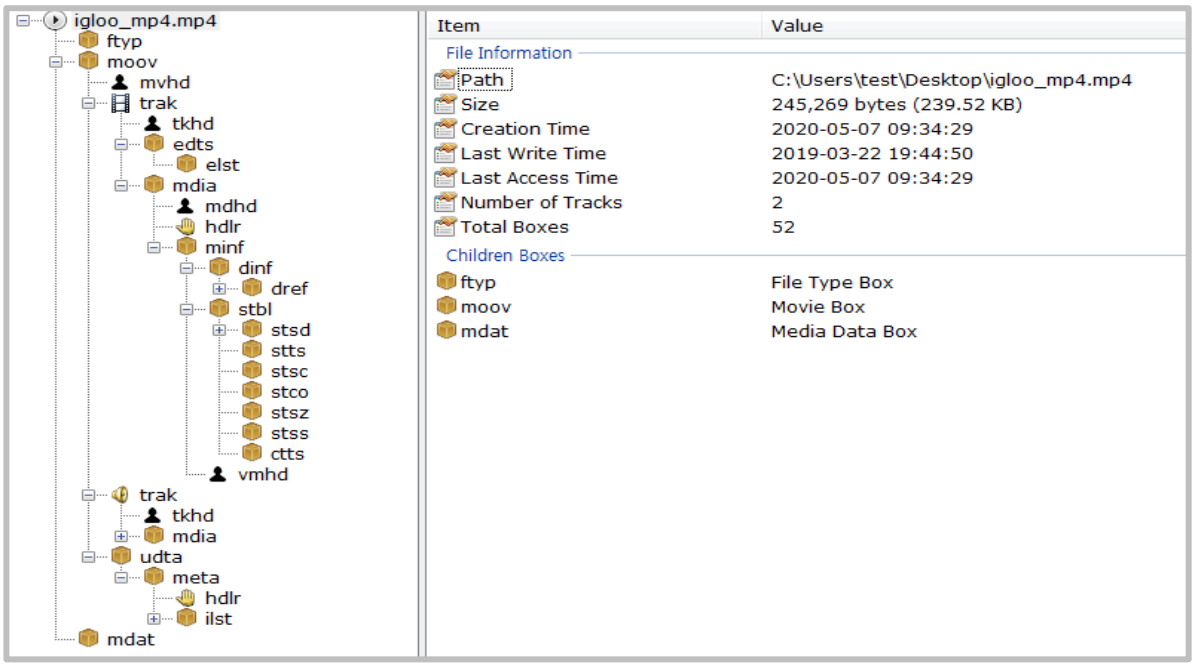
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Multimedia steganography

02. Multimedia steganography

2) MP4 file steganography principle

The official name of MP4 is MPEG-4 part 14, a media container format standard, and is a technology that stores and plays high-definition video at a high compression rate. The MP4 file format is largely composed of a header, media data, and media header, and the file structure is composed of a data and metadata box structure.



[Figure 4-4] MPEG-4 file data structure (Boxes/Atoms)

Header	Description
ftyp	File type box to check file compatibility
moov	Movie box that stores all of the media's metadata
mvhd	Movie header box
mdat	Media data box that store actual media
trak	Meta information of specific media
stsd	Codec information required for decoding a track (sample description box)
stts	Time of sample (time-tosample box)
stsz	Size of sample in chunk (sample size box)
stsc	Count of sample in chunk (sample to chunk box)
stco	Location of chunk (chunk offset box)

[Table 4-2] MPEG-4 file format header

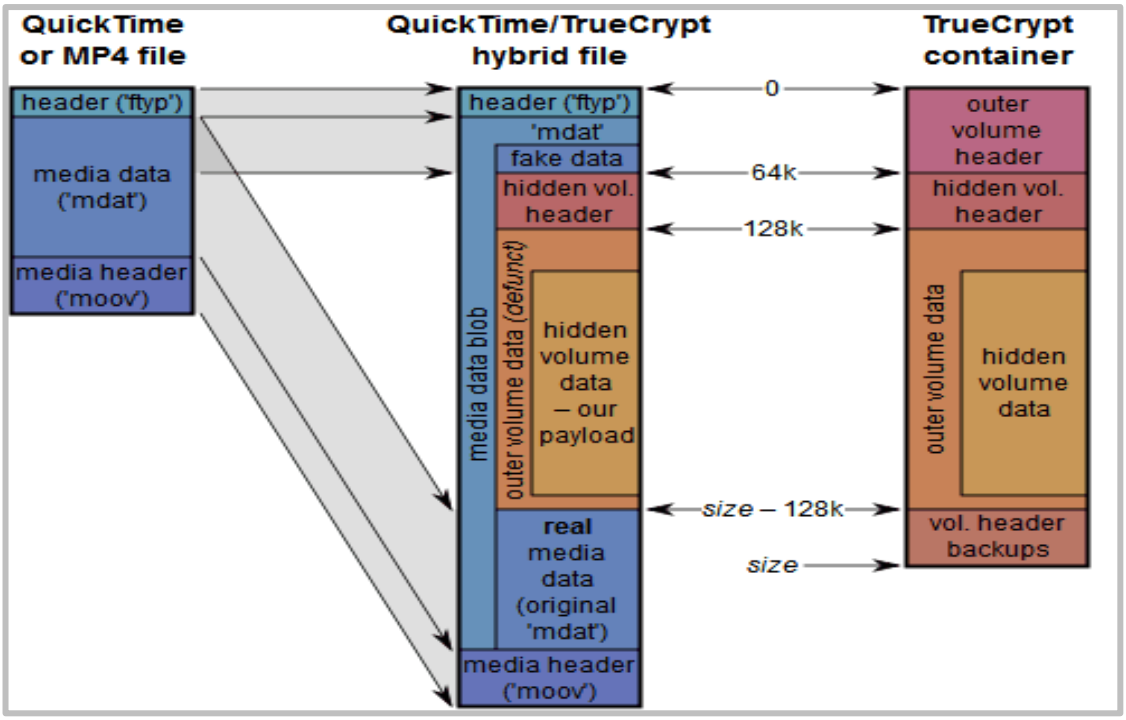
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Multimedia steganography

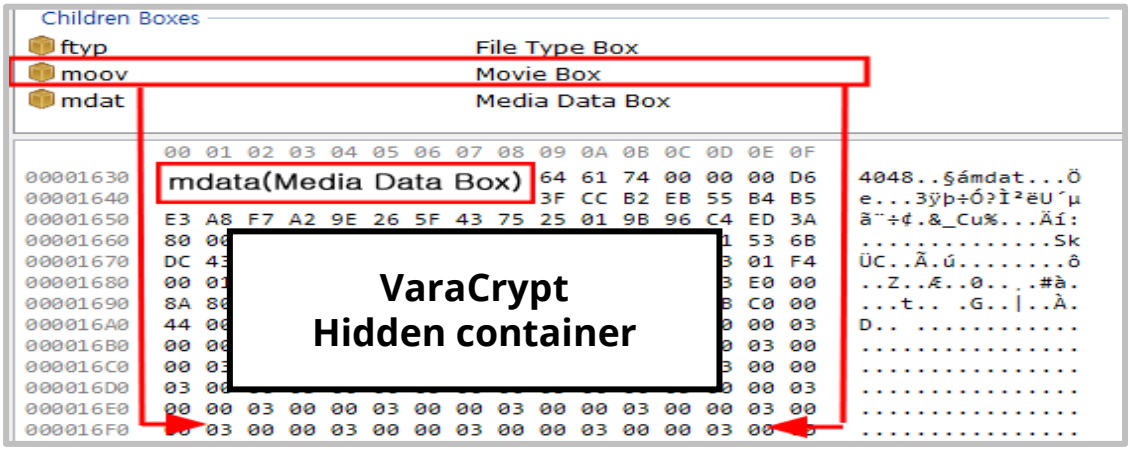
02. Multimedia steganography

3) VeraCrypt steganography

The media data area of the MP4 file structure is modified to hide the data. Delete the external volume header and header backup area from the container file created with VeraCrypt and insert it into the media data area of mp4. In order to normally execute the existing media data in the media data area, fake data is added before the hidden volume header.



[Figure 4-5] MP4 steganography (Source : MP4 Steganograpy:Analyzing and Detecting TCSteg)



[Figure 4-6] MP4 steganography

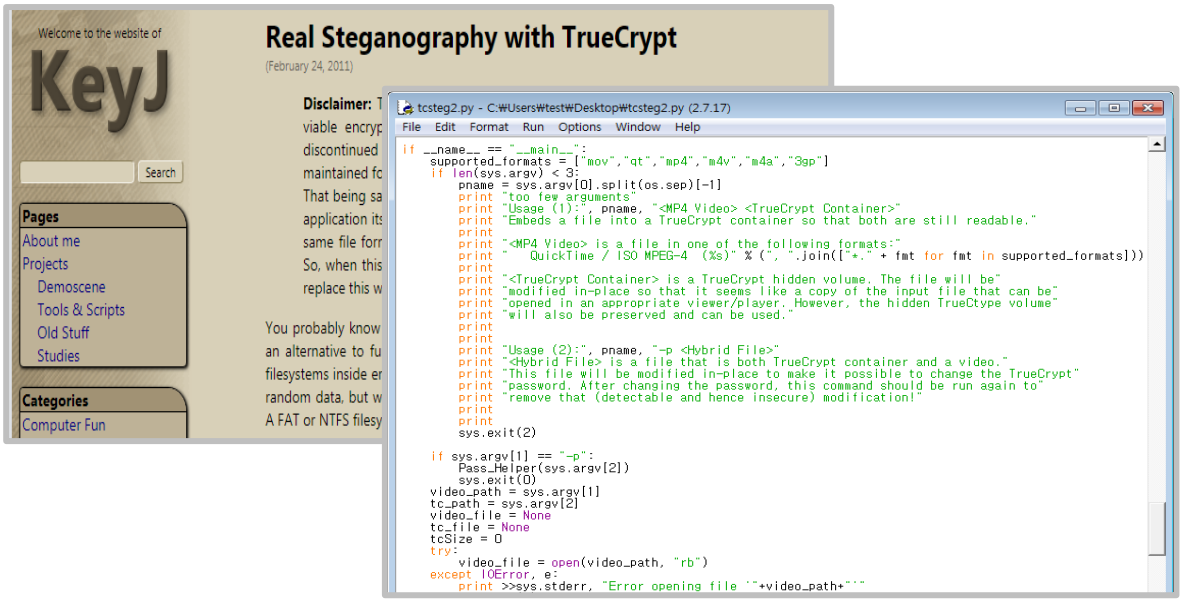
Copyright ⓒ IGLOO Security, Inc. 2020. All rights reserved

Multimedia steganography

02. Multimedia steganography

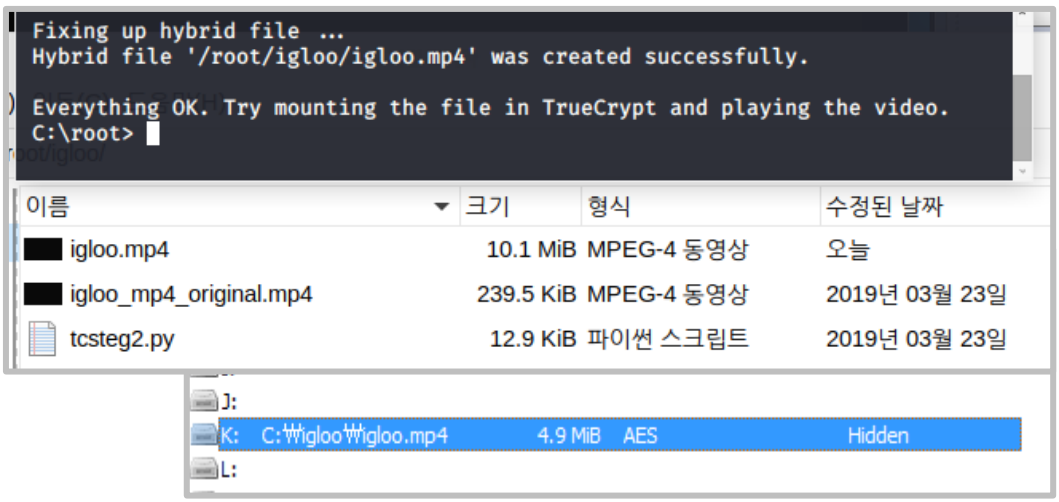
4) Create VeraCrypt steganography

The media data area of the MP4 file is modified to insert data. I used tcsteg2.py, a python script that is currently open to create a steganography file that plays.



[Figure 4-7] tcsteg2.py creator and source code (Source : keyj.empy.de)

The volume increased by the size of the volume as shown in [Figure 4-8] by inserting the 10MB file created with VeraCrypt into the prepared video. The created video plays the same as the original video, and can be mounted with VeraCrypt.



[Figure 4-8] Create steganography and recognize hidden volume

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

Multimedia steganography

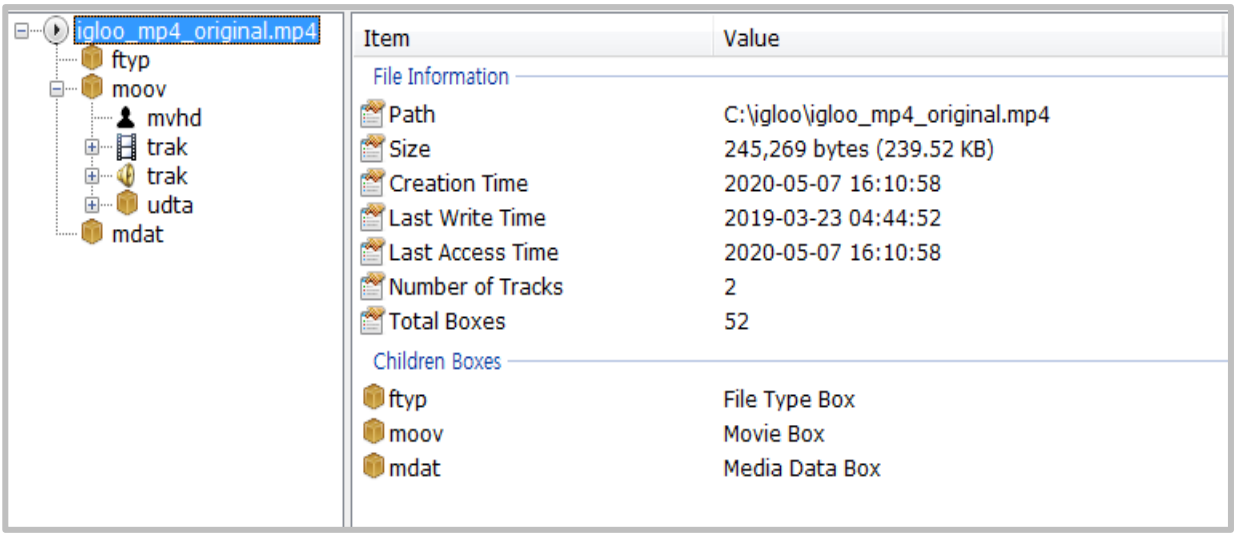
02. Multimedia steganography

5) Analyze VeraCrypt steganography

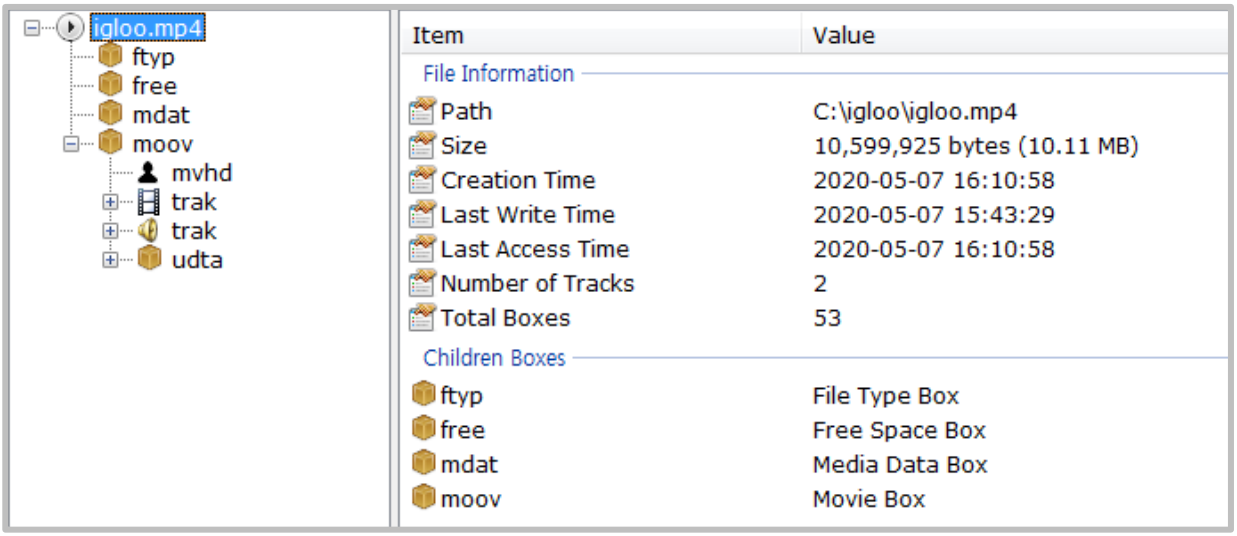
The overall comparison of MPEG-4 files and data structures (Boxes/Atoms) were compared and analyzed using the MP4 Inspector tool.

When comparing the original video file and the steganography file, both files have the signature in MP4 format and show the same playing time and image quality.

Looking at the largely changed part, the size of the file identified above increased, and a new free box was created, and the total number of boxes increased by one.



[Figure 4-9] Original video MP4 file information



[Figure 4-10] Steganography MP4 File Information

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

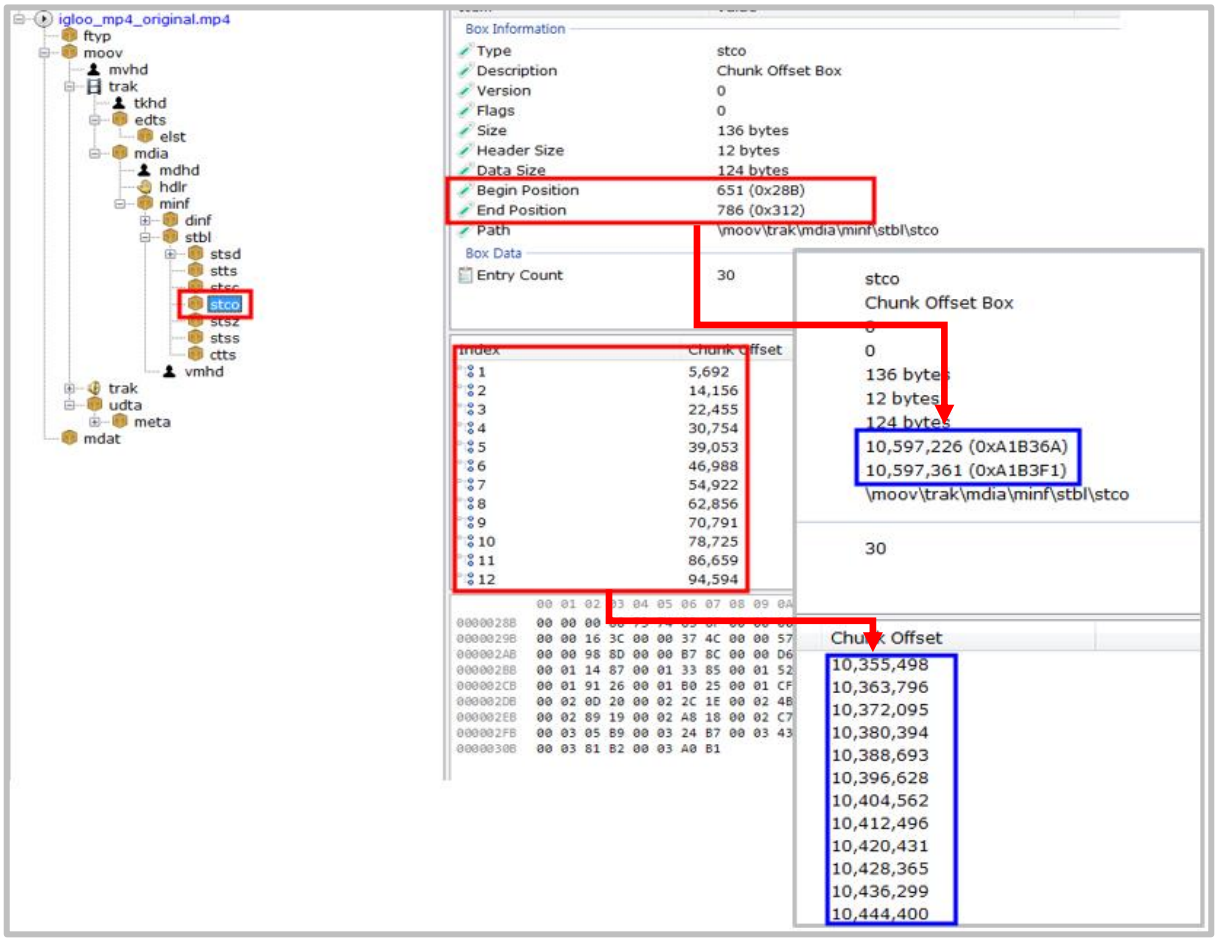
Multimedia steganography

It can be seen that the hidden volume was added to the mdat box due to the increase in the size of the mdat box in the structure.

Item	Value	Item	Value
Box Information		Box Information	
Type	mdat	Type	mdat
Description	Media Data Box	Description	Media Data Box
Size	239,585 bytes	Size	10,594,233 bytes
Header Size	8 bytes	Header Size	8 bytes
Data Size	239,577 bytes	Data Size	10,594,225 bytes
Begin Position	5,684 (0x1634)	Begin Position	32 (0x20)
End Position	245,268 (0x3BE14)	End Position	10,594,264 (0xA1A7D8)
Path	\mdat	Path	\mdat

[Figure 4-11] Increasing mdat size

The stco header is one of the MPEG-4 file formats to be looked at here. stco contains the chunk's location table and is located in the moov (movie box). Since this header maps samples to sequentially reference the location of mdat (media data), the size of the mdat box is increased by steganography, so the offset value referenced by stco is also changed.



[Figure 4-12] Steganography stco value change

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

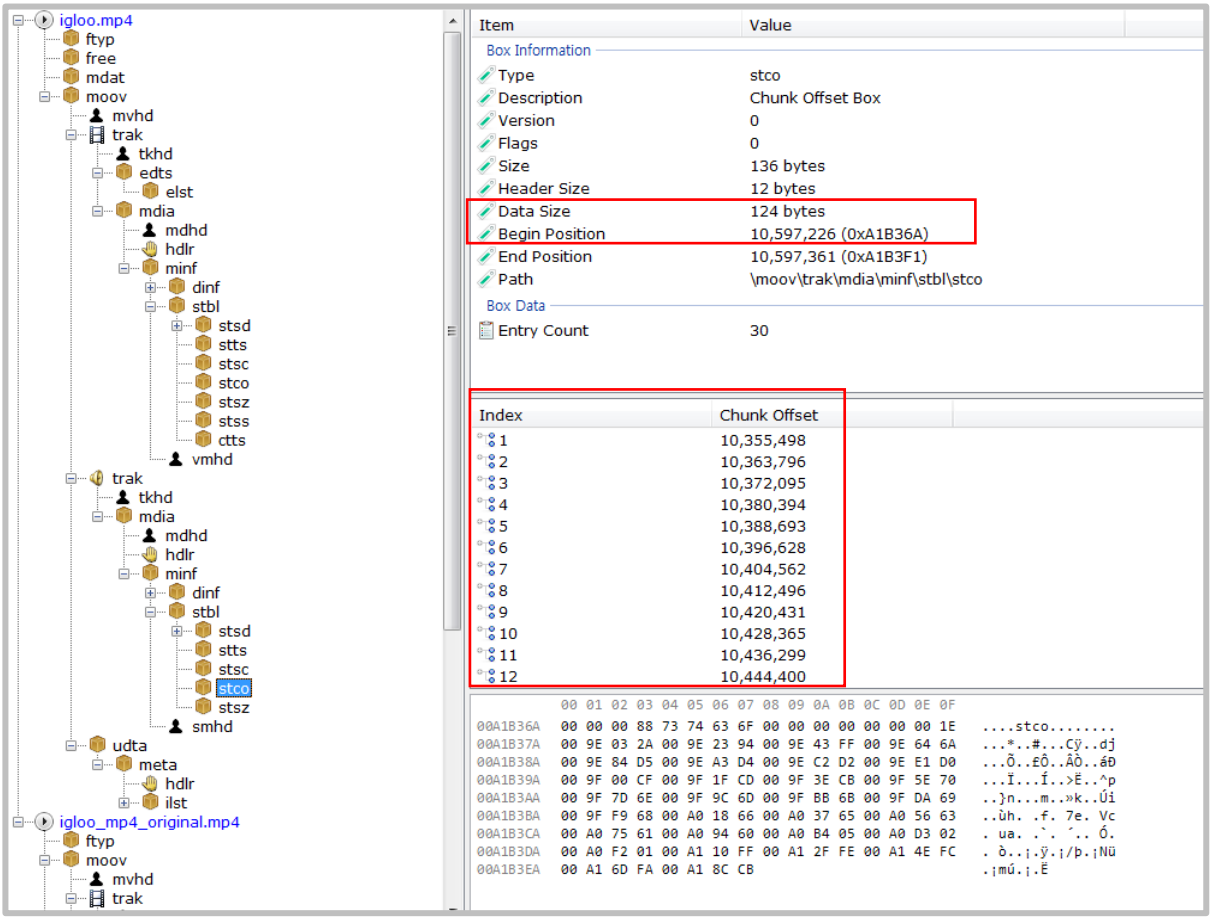
Multimedia steganography

03. Multimedia steganography detection

1) MP4 video steganography detection principle

It is difficult to detect steganography in a video, but there is a way to find the volume hidden in the video through analysis.
As shown in [Figure 4-12], the mdat box changes as the volume is inserted, and you can see that the stco's Chunk Offset value changes to play the video properly.

If the offset start position of a normal video exists between 65536 and 172032, and if the offset start position of stco deviates between 65536 and 172032 as shown in [Figure 4-13], it is necessary to question whether the video is steganography.



[Figure 4-13] Running Normal Volume and Hidden Volume

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

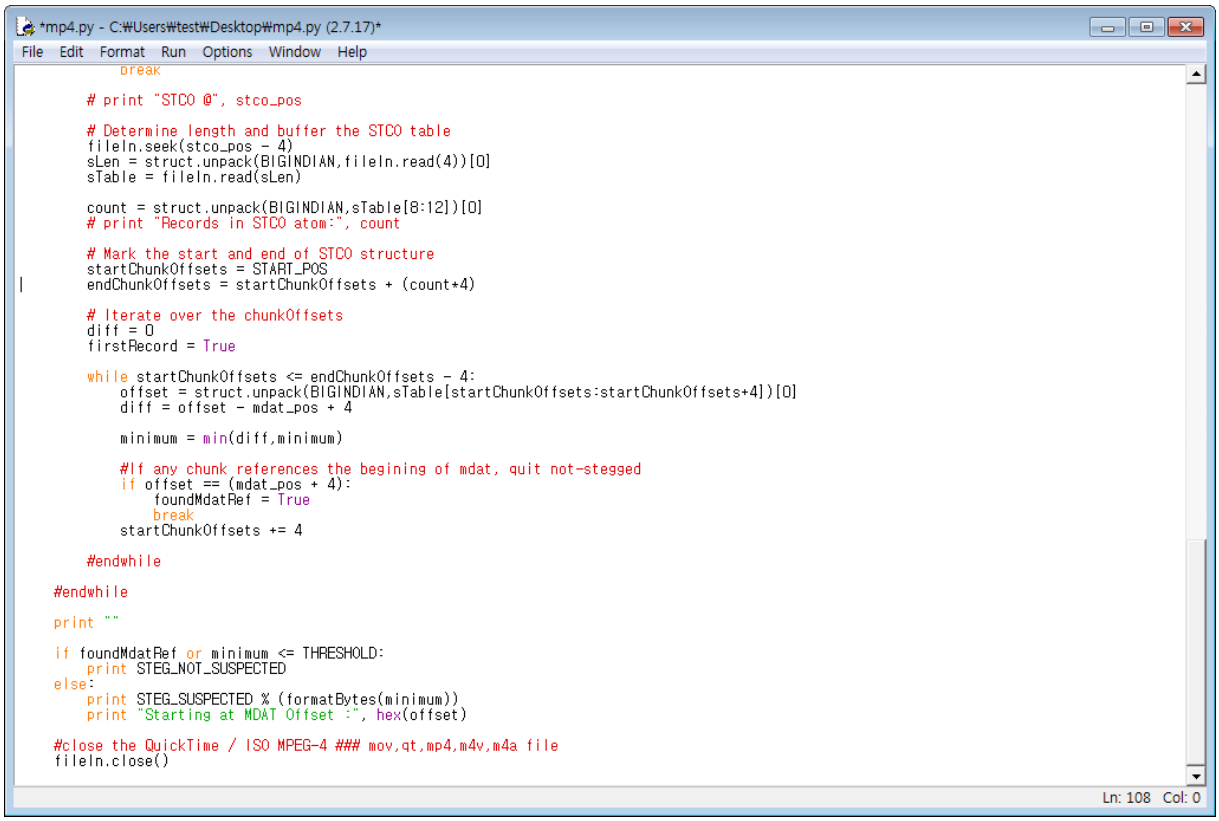
Multimedia steganography

03. Multimedia steganography detection

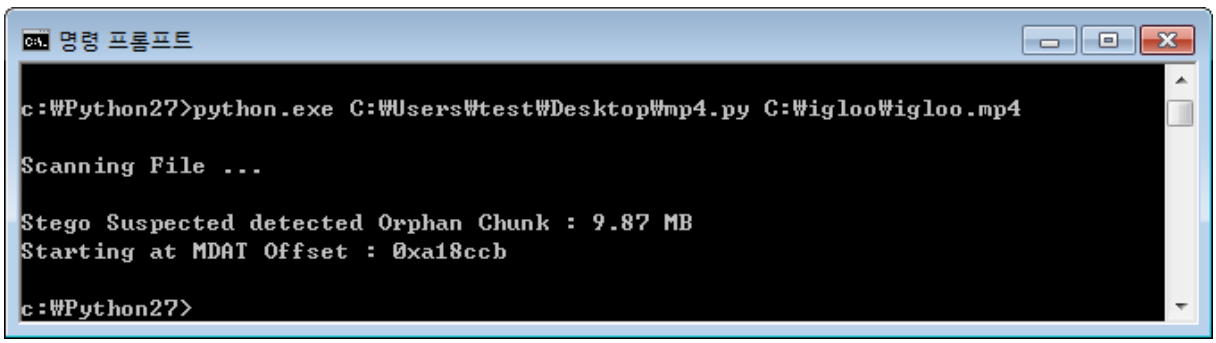
2) MP4 video steganography detection

If the video file structure viewer is not installed, flexible analysis is possible using the open python script.

[Figure 4-15] is a script result screen that finds the offset start position of a video. The used script calculates the starting offset position of mdat and roughly expresses whether steganography is used and the size of hidden data in the video.



[Figure 4-14] python-script-detect-hidden-data source code



[Figure 4-15] python-script-detect-hidden-data result

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

Multimedia steganography

04. Conclusion

As crimes diversify, news about forensics can often be heard. In particular, digital sex crime has become a major social issue in recent years, and it is increasing every year. As these digital crimes have developed intelligently, steganography's interest is growing to collect data without erasing itself.

Steganography has been used since ancient times, but it is currently used in numerous fields such as data encryption, cybercrime, and dissemination of malicious codes.

So far, we have explained how to conceal data directly in a video and browse hidden data. I hope you have a reasonable doubt that your current video may be a steganography file.

05. Reference

[1] MP4 Steganography: Analyzing and Detecting TCSteg
https://dl.acm.org/doi/pdf/10.1145/2978178.2978181
[2] Real Steganography with TrueCrypt
https://keyj.emphy.de/real-steganography-with-truecrypt/
[3] PreviewFilesmp4.py
https://www.forensicmag.com/product-release/2012/01/python-script-detect-hidden-data
[4] VeraCrypt - Documentation
https://veracrypt.codeplex.com/documentation

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

Cover Story

CHAPTER 5

Focus On IGLOO Security

1. IGLOO SECURITY Inc.,
   Cheering COVID-19 medical staff
   #thanks_challenge
2. IGLOO SECURITY Inc.,
   acquired 4 patents related to AI·SIEM

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

Focus on IGLOO Security

IGLOO SECURITY Inc., Cheering COVID-19 medical staff #thanks_challenge

- Mr. Lee Deuk Choon(CEO) participates 'thanks challenge' with his employees

[13rd July 2020] IGLOO Security Inc., (CEO, Lee Deuk-Choon, www.igloosec.co.kr/en) said that they participated in the "thanks_challenge" for staffs dedicated to COVID-19.

The'Thanks Challenge' is a national participatory campaign launched by the Central Disaster Safety Response Headquarters to encourage medical staff and volunteers struggling to protect the health of the people. Posts containing actions that signify respect and a hashtag (#thanks_challenge, #thanks_medical_staff, #thanks_campaign and etc.) that support the action will be posted on the SNS, and will be conducted by pointing to the next challenge participants.

Mr. Lee Deuk-Choon (CEO of IGLOO SECURITY), pointed out by Mr. Kim Jong-wan (CEO of SoNoKong), participated in the campaign with employees. The employees who are protecting information assets of key institutions and companies in all parts of the country are sympathetic to the purpose of the Challenge and joined in unison. Mr. Lee Deuk-Choon (CEO of IGLOO SECURITY) pointed out Mr. Hwang Ho-chan (CEO of Hans Biomed) as the next runner to participate in the Challenge.

Mr. Lee Deuk-Choon (CEO of IGLOO SECURITY) said, "Thank you once again for your sacrifice and hard work. I hope that strong cheers will be delivered to the medical staff and volunteers who are devoted day and night at the forefront of quarantine. IGLOO SECURITY, which is at the forefront of the cyber battlefield, will also strive to protect the nation's cyber safety."

On the other hand, IGLOO SECURITY is committed to proactive measures for cyber safety in the country while focusing on employee safety through preemptive preventive measures in accordance with government guidelines. In order to safely maintain public service and continuity of business without security gaps in the event of an emergency, the security monitoring center is multiplexed and operated, and online-based remote technical support and maintenance services are provided.

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

Focus on IGLOO Security

IGLOO SECURITY Inc., COVID-19 Medical staff cheering #Joining_thanks_challenge

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

Focus on IGLOO Security

IGLOO SECURITY Inc., acquired 4 patents related to AI·SIEM

- IGLOO SECURITY strengthens AI technology competitiveness by continuously securing intellectual property rights

- strengthens AI technology competitiveness by continuously securing intellectual property rights

[30th June 2020] Igloo Security Inc., (CEO Lee Deuk-Choon, www.igloosec.co.kr/en) announced that it has acquired four patents for SIEM (Security Information and Event Management) and AI (Artificial Intelligence). The four patents aim to increase the effectiveness of security control by allowing security control personnel to quickly and accurately identify high-risk events.

'Method, device and program for providing a dashboard of a security device as a mobile device (Registration No. 10-2125428)' is a mobile device through a relay server located in the Internet network that provides dashboard data provided in a closed network environment within a company or institution. It is a safe delivery technology. When requesting to use the mobile dashboard, a QR authentication code is generated, displayed on the user's mobile dashboard, and scanned by a mobile device to perform user authentication.

'Security policy management method and its system (Registration No. 10-2124611)' is a technology that reflects security policy feedback that analyzes security policies currently applied and security events collected in real time based on AI-based technologies, etc. to the security device. By applying the security policy that reflects the latest attack flow in a timely manner, it is possible to speed up the response to threats against high-risk attacks.

The method and apparatus for providing a security control interface (Registration No. 10-2125440) focuses on providing a user-oriented interface (UI) that can intuitively recognize and manage vast security events. It enhances user convenience and work efficiency by expressing security events in semi-circle shapes and changing the number, size and shape according to the number of occurrences and severity.

'Physical security monitoring method using MAC address and its system (Registration No. 10-2125848)' focuses on responding to physical intrusion attempts by analyzing information from the user and the terminal device owned by the user from various angles. It is a method of determining the risk level by checking whether the MAC address of the accessor matches the terminal included in the white list and where the terminal is located, and sends a warning message to the security manager.

"Igloo Security has been focusing on securing intellectual property rights for the development of the AI industry and the protection of new technologies, since I began investing in R&D (AI) in the AI field in 2015. In addition, the job invention system has been expanded to encourage the invention of employees. As a leader in AI security monitoring, we intend to strengthen the competitiveness of AI technology by continuously securing intellectual property rights."

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

We Know SECURITY!

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

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

Edited by IGLOO SECURITY Marketing Team
Translated by IGLOO SECURITY Overseas Business Team
© 2020 IGLOO SECURITY, Inc. All rights reserved.
The copyright of this publication is held by IGLOO SECURITY. It is not permissible to reproduce, copy, or distribute any or all of the contents of this publication in any form or by any means without the prior written consent of IGLOO SECURITY. All information contained in the publication can be changed without prior notice.