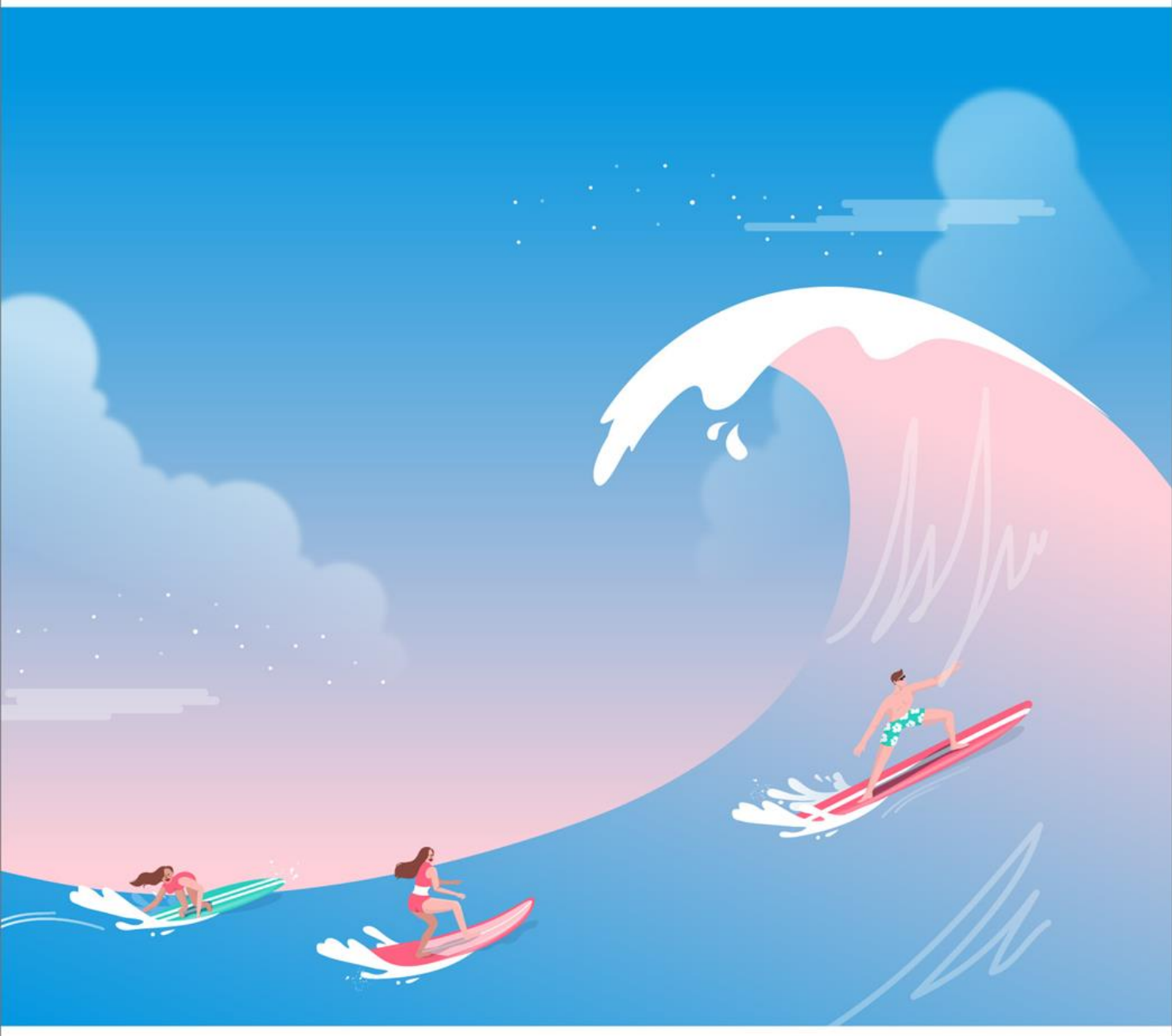
Monthly Security Report

2019
August



Cover Story

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

Enhance the accuracy and speed of security monitoring beyond managing the vulnerability of internal assets

OS Command Injection using SHELLING

How to ensure Container Security, between user convenience and security

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

Monthly security issue

2. IGLOO Statistics

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

3. IGLOO Analysis Report

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

4. Special Column

How to ensure Container Security, between user convenience and security

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

CHAPTER 1

Monthly Security Issue

1. Monthly Security issue

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

1 Monthly Security Issue

‘Delivery is delayed due to incorrect customs declaration’… Malicious mail alert for overseas shoppers

- Users are cautioned as malicious emails are spreading under the name of DHL Express service, stating that delivery is delayed due to wrong customs declaration. It seems like that hackers recognize about frequently delayed delivery from overseas.
- This email contains a message stating that the shipment has been delayed due to incorrect customs declaration and that you should check with the attached document as soon as possible and contact related employees. However, if you execute the zip file (DHL Customs Declaration.zip) attached to this email, you will be infected with malicious files.

‘Warning…’ Cryptocurrency Mining Malware in Smartphone

- As the price of cryptocurrency including Bitcoin has soared recently, cryptojacking malware, which uses IT device resources to secretly mine cryptocurrencies, is on the rise. Recently, the number of malware targeting Android smartphones is increasing as well as PCs, so be careful when installing mobile applications.
- Recently, AhnLab discovered a cryptocurrency app disguised as an Android game app. When mining malware, smartphone CPU usage increases rapidly, reducing performance, but it is difficult for users to know that even malicious apps exist because they think that game apps are running.

‘Please check the E-Ticket from OO airlines’… The distribution of malicious mail aimed at the holiday season

- Recently, malicious mail disguised as a domestic airline's e-ticket ticket confirmation has been spreading, so users need to pay special attention. Written in native language and attached with a file disguised as an PDF icon and extension, users are more likely to click without a doubt.
- According to East Security, this email contains a compressed file called 'e-Ticket Verification_95291015.iso' that is uncompressed and clicked on the attached 'e-Ticket Verification_66016630.pdf.scr' file. Connected to a C & C server that downloads and runs the code. Attackers have used a variety of source email addresses to make blocking and tracking difficult.
- East Security estimates that the Russian-based “TA505” organization behind Kloop Ransomware in the first half of this year is behind the attack.

‘Your account has been blocked’...Warning for account stealing phishing mail

- The phishing e-mail, which was previously distributed under the title of 'Your Account Has Been Hacked', is now spreading again in world.
- Attackers are attracting users with the title `` Your account has been blocked, '' and then trying to enter certain account information by allowing them to access a specific site. “If you do not update your account information, account, it could be permanently disabled" and trigger tensions, and include "audit, security team, terms of use / privacy policy" in your email, Disguised as if sent out from them.
- Security experts advise not to click on the hyperlink but immediately report it to the company's security team.

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

CHAPTER 2

IGLOO Statistics

1. Monthly Attack Service and Trend Analysis

01. Monthly Attack Service(Port) TOP 10

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

03. TOP 10 Monthly Attack Service patterns

04. Monthly Attack Service Incident patterns compared to last Month

2. Detailed Analysis According to Different Patterns

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

1 Monthly Attack Service and Trend Analysis

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

01. Monthly Attack Service(Port) TOP 10

In the top 10 service ports collected during the month of August 2019, events using IUA (TCP / 9900) rose by two steps compared to the previous month and events using SNMP (UDP / 161) and ICMP (0 / ICMP) have declined by one step.
Other Unassigned (TCP / 37215) and DNS (TCP / 53) events are newly identified in the ranking.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Service(Port)	No. of Cases	Ratio(%)	Fluctuation
1	HTTP(TCP/80)	1,530,560,831	49.12%	-
2	DNS(UDP/53)	562,957,139	18.07%	-
3	HTTPS(TCP/443)	329,242,727	10.57%	-
4	Microsoft-DS(TCP/445)	279,938,948	8.98%	-
5	IUA(TCP/9900)	117,349,239	3.77%	▲2
6	SNMP(UDP/161)	97,898,417	3.14%	▼1
7	ICMP(0/ICMP)	92,902,033	2.98%	▼1
8	Telnet(TCP/23)	42,822,267	1.37%	-
9	Unassigned(TCP/37215)	35,205,543	1.13%	NEW
10	DNS(TCP/53)	27,098,024	0.87%	NEW
	Total	3,115,975,168	100.00%	-

[Table2-1] TOP10 monthly attack patterns

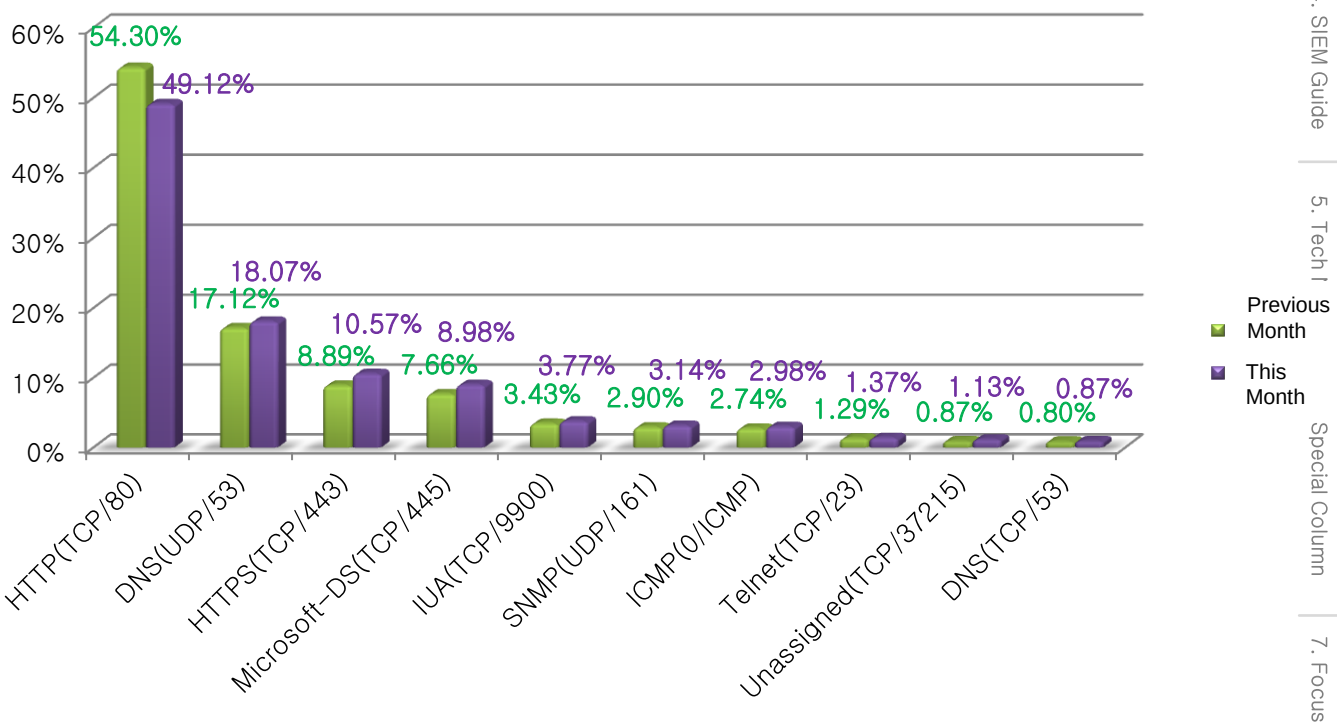
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

1 Monthly Attack Service and Trend Analysis

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

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

As a result of the event analysis by attack service port in August, detection rate of HTTP service port decreased slightly. In addition, unassigned (TCP / 37215) and DNS (TCP / 53) service ports entered the top 10 this month. The newly identified Unassigned (TCP / 37215) port is identified as a port that has been exploited for Huawei HG532 routers remote code execution vulnerability and satiori malware infection Unknown service ports, such as Unassigned (TCP / 37215), may cause traffic to be caused by an attacker's attempt to scan a given service for vulnerabilities. Therefore, if the server is exposed to the outside, it is recommended to check the open ports through periodic service usage check and establish a policy that can limit them.



[Figure 2-1] TOP10 monthly attack port

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

1 Monthly Attack Service and Trend Analysis

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

03. TOP 10 Monthly Attack Service Patterns

According to the analysis of attack events in August 2019, the top 10 rankings fluctuated, but the total number of event occurrences did not increase significantly compared to the rank change rate, and the number of SMB Service connect (tcp-445) event occurrences decreased significantly. Multi Packet Inspection The ranking of the multi-packet inspection and other events increased compared to previous month, while the MySQL-Server Login Brute force and Ack Storm events declined.

※ Based on IGLOO Security SOC SIEM data collection

Rank	Pattern	No. of Cases	Ratio(%)	Fluctuation
1	SMB Service connect(tcp-445)	514,818,568	88.13%	-
2	ACK Port Scan(F/W Scan)	46,926,312	8.03%	-
3	Multi Packet Inspection	6,624,874	1.13%	▲2
4	Netbios Scan (Messenger RPC Dcom MyDoom) (UDP-137)	3,707,456	0.63%	▲3
5	MS WINS Server Registration Spoofing Vuln-1[Req](UDP-137)	3,481,396	0.60%	▲1
6	Dcom_TCP_Sweep(MSBlaster Worm Messenger)	3,092,582	0.53%	▲3
7	MySQL-Server Login Brute force	1,633,846	0.28%	▼4
8	HTTP Login Brute Force	1,444,146	0.25%	-
9	HP Data Protector Client EXEC_CMD with Directory Traversal-1	1,315,486	0.23%	▲1
10	Ack Storm	1,103,096	0.19%	▼6
	Total	584,147,762	100.00%	-

[Table 2-2] TOP10 monthly attack pattern

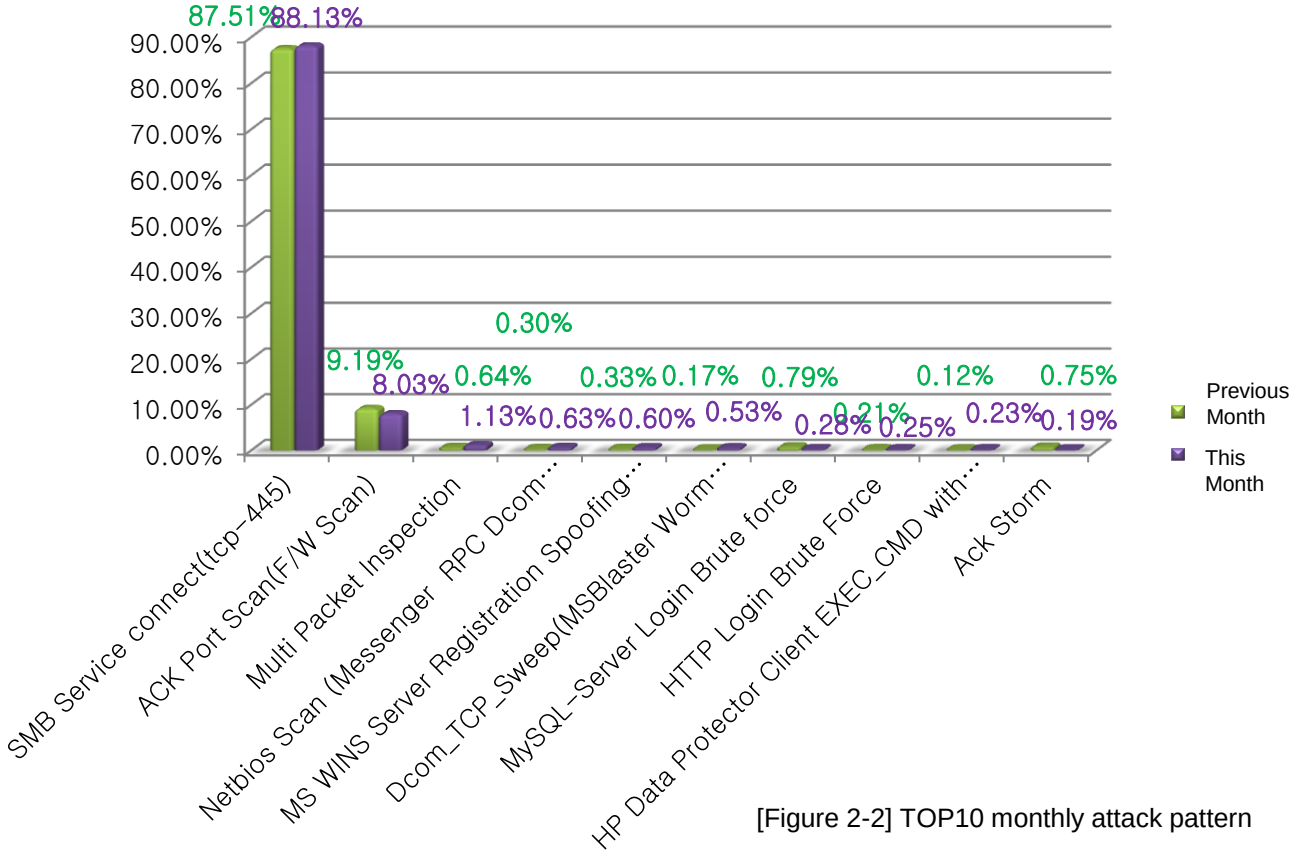
Copyright © IGLOO Security, Inc. 2019. All rights reserved.

1 Monthly Attack Service and Trend Analysis

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

04. Monthly Attack Service Incident Patterns Compared to Last Month

SMB Serivice Connect (tcp-445) still ranks high at 88% in the top 10 attacks in August 2019. Since ransomware malware exploited SMB service vulnerabilities for multiple infections in the network, access to 445 service ports continues to be at the top. A slight increase compared to the previous month, and still high, proves that many attackers are seeking financial gain from ransomware. Due to the nature of ransomware, which may lose important data for a moment, vulnerabilities are being actively patched, and the value of virtual currency that an attacker can obtain greatly decreases attack attempts on SMB service ports. Risks are unlikely to decrease as the increase and the disclosure of network equipment vulnerabilities require constant attention to the internal network.



[Figure 2-2] TOP10 monthly attack pattern

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

2 Detailed Analysis According to Different Patterns

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

Attack pattern	Detailed Analysis Results
SMB Service Connect (tcp-445)	Microsoft Windows uses SMB protocol to share files and printer resources with other computers. Sharing resources using SMB in older versions (95, 98, Me and NT) of Windows used TCP port 137 and 139 and UDP port 138 by executing NETBIOS with NETBIOS over TCP/IP. On older versions of Windows 2000/XP, it was possible to run SMB directly through TCP/IP on TCP port 445. If the files are shared with easily guessable password or passwords are not set, they can suffer from secondary attacks.
ACK Port Scan (F/W Scan)	ACK Port Scan (F/W Scan) is a type of scanning attack targeting vulnerable ports which are allowed to be accessed by firewall policy. Attackers can collect information on vulnerable ports by analyzing the returned packet as a response to the packet sent in advance. These attacks are not intended to destroy the system but to collect information for planning a scenario for secondary attack.
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.
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.
MySQL-Server Login Brute force	A brute force attack can be launched against an user account in MySQL. MySQL replies with success/error based on supplied credentials and time required for the verification is almost the same in either cases. Hence, an attacker can launch brute force attack against a MySQL user account at a rapid rate and can try many different passwords.
HTTP Login Brute Force	This attack accesses the HTTP WEB service port(80) and repetitively inserts random strings through a Tool-Kit in order to find out the password for a specific ID(root, guest etc). Passwords which are easy to guess or are in an alphabetic/symbolic order are more prone to this attack. This attack can be prevented by using IDs and passwords over 6 letters and by Filtering data from the HTTP port(80/TCP).
HP Data Protector Client EXEC_CMD with Directory Traversal-1	This vulnerability occurs in the HP Data Protector Client. Directory Traversal is an attack which uses a bypass attack. It is an attack in which an unauthorized user sends maliciously manipulated input values to EXEC_CMD. If the attack is successful, the attacker can execute arbitrary codes with system level permissions. Prevention is possible by installing the latest patch released from vendors.
Ack Storm	An Ack Storm is the a hacker sends a large amount of TCP/IP Ack signals to the target server, causing an unnecessary load on the target server. It is an attack method which delays normal services. It is a technique which attacks using loopholes of the TCP/IP protocol. This attack is also used to perform hijacking on the packets which contain sessions. .

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

CHAPTER 3

IGLOO Analysis Report

Ransomware trends for the first half of 2019

(Part 1. CLOP/Sodinokibi)

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

Security Monitoring Center
Security Analysis Team

01. Synopsis

Cyber attacks using ransomware are constantly occurring. GandCrab creators, who ended their service in June of this year, said the revenue from ransomware services for two years was $ 2 billion.

Ransomware encrypts files on the system when infected, making the system unusable. Attackers demand cryptocurrency by using decryption key (key to return to normal file) of encrypted file.

In order to prevent damages in advance, ransomware infections cause considerable damage, and the risks and prevention methods are known through various media recently, but attackers are increasingly sophisticated, and the damage is increasing every year.

Therefore, the IGLOO Analysis Report examines four ransomwares (CLOP, Sodinokibi, GandCrab, and Crysis (Dharma)) that suffered a lot in the first half of 2019. In the first half of this year's <Ransomware Trends in 1H19> Part 1, Sodinokibi, which is being distributed in a similar form to CLOP and GandCrab, which has been distributed to Active Directory (AD) servers since early this year, was analyzed. Subsequently, GandCrab and Crysis (Dharma) will be covered in Part 2 of the next issue of IGLOO Analysis Report <1H20 Ransomware Trends>.

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

Top 10 most common families of ransomware Trojans

	Name	Verdicts*	Percentage of attacked users**
1	WannaCry	Trojan-Ransom.Win32.Wanna	26.25
2	(generic verdict)	Trojan-Ransom.Win32.Phny	18.98
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	12.33
4	(generic verdict)	Trojan-Ransom.Win32.Crypmod	5.76
5	Shade	Trojan-Ransom.Win32.Shade	3.54
6	(generic verdict)	Trojan-Ransom.Win32.Encoder	3.50
7	PolyRansom/VirLock	Virus.Win32.PolyRansom	2.82
8	(generic verdict)	Trojan-Ransom.Win32.Gen	2.02
9	Crysis/Dharma	Trojan-Ransom.Win32.Crusis	1.51
10	(generic verdict)	Trojan-Ransom.Win32.Cryptor	1.20

** Statistics are based on detection verdicts of Kaspersky Lab products. The information was provided by Kaspersky Lab product users who consented to provide statistical data.*

*** Unique Kaspersky Lab users attacked by a particular family of Trojan cryptors as a percentage of all users attacked by Trojan cryptors.*

[Figure 3-1]Top 10 Ransomware for the first half of 2019 (Resource : Kaspersky)

▶ Major features of ransomware : CLOP, Sodinokibi, GandCrab, Crysis(Dharma)

Classification	GandCrab	CrySiS	Clop	Sodinokibi
Period	2018.01. ~ 2019.06	2016.02. ~ Current	2019.02. ~ Current	2019.04. ~ Current
Distribution Type	· Malware distribution · Spear Phishing · Malvertising · Worm(Bondat) · Watering hall	· Malware distribution · Spear Phishing · RDP Protocol	· Advance attack (Targeting specific server)	· Spear Phishing · vunlerability
encryption extension	· .CRAB (v1~v3) · .KRAB (v4) · .[rand] (v5)	· .id-[id].[email].[rand] · .[email].dharma	· .[rand]	· .[rand]
encryption Key management	· Network communication · Registry storage	· Encrypted file	· Save in infected file	· Registry storage
main Malicious behavior	· File encryption · Process termination · System Information Takeover · Delete Shadow Copies	· File encryption · Delete Shadow Copies	· File encryption · Service registration · Shared Drive File Encryption · Specific country language infection excluded	· File encryption · Shared Drive File Encryption

[Table 3-1] Behavior summery

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

02. CLOP Ransomware

1) Synopsis

The CLOP ransomware estimates that the attack was going against an **Active Directory (AD) server** that had been taken over by the **TA505 group**. When infected, the file extension is changed to * .Clop (CLOP) or * .Ciop (CIOP) and the file is encrypted. Use batch files to delete all shadow copy files, identify processes that interfere with ransomware's behavior (primarily antivirus processes), and recently disseminate clop ransomware directly if certain antivirus (older versions) are installed do.

※ The details of the pre-attack of the TA505 group are discussed in detail in the **04. TA505 Group Pre-attack (CLOP) Detailed Analysis**.

Classification	Contents
Process	- Operate after being registered as service
File	- File encryption and extension change (* .Clop (CLOP), * .Ciop (CIOP) - Delete specific program and check process - Create and run batch file (shadow file deletion) - Systems that use a language in a specific country do not proceed with infection

[Table 3-2] Behavior summery

2) Detailed Behavior analysis

CLOP ransomware runs after being registered as a service. The registered service name differs depending on the sample.

```
ServiceStartTable.lpServiceName = L"TaskNetProcess";
ServiceStartTable.lpServiceProc = (LPSERVICE_MAIN_FUNCTIONW)sub_40E1C0;
```

[Figure 3-2] Perform the main behavior using the service

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

Once the language of a particular country is identified, it will no longer be malicious.

```
v1 = (unsigned __int16)GetKeyboardLayout(0);
if ( (unsigned __int16)v1 <= 0x437u )
{
  if ( (unsigned __int16)v1 != 0x437 )          // Georgian
  {
    switch ( v1 )
    {
      case 0x419u:                              // Russian
      case 0x422u:                              // Ukrainian
      case 0x423u:                              // Belarusian
      case 0x428u:                              // Tajik
      case 0x42Bu:                              // Armenian
        return 1;
      default:
        return v0;
    }
    return v0;
  }
  return 1;
}
if ( v1 > 0x82C )
{
  if ( v1 != 0x843 )                            // Uzbek
    return v0;
  return 1;
}
if ( v1 == 0x82C )                              // Azerbaijani
  return 1;
if ( v1 >= 0x43F )                              // Kazakh
{
  if ( v1 > 0x440 && v1 != 0x442 )              // Kyrgyz, Turkmen, Swahili
    return 0;
  return 1;
}
return v0;
```

[Figure 3-3] Performing Main Behaviors Using Services

Checking languages
Georgian, Russian, Ukrainian, Belarusian, Tajik, Armenian Uzbek, Azerbaijani, Kazakh, Kyrgyz, Turkmen, Swahili

[Table 3-3] excluded system languages

Make sure that certain processes are currently running (the process name you see depends on the sample)

```
if ( SearchProcess_403630(L"SBAMSvc.exe")
  || SearchProcess_403630(L"MCSHIELD.EXE")
  || SearchProcess_403630(L"naPrdMgr.exe")
  || SearchProcess_403630(L"WRSA.exe")
  || SearchProcess_403630(L"MCSACORE.EXE")
  || SearchProcess_403630(L"MCSUHOST.EXE")
  || SearchProcess_403630(L"QHACTIVEDEFENSE.EXE")
  || SearchProcess_403630(L"masvc.exe")
  || SearchProcess_403630(L"SBAMSvc.exe")
  || SearchProcess_403630(L"VipreAAPSvc.exe")
  || SearchProcess_403630(L"QHSAFETRAY.EXE")
  || SearchProcess_403630(L"SBPIMSvc.exe")
  || SearchProcess_403630(L"SBAMTray.exe") )
```

[Figure 3-4] Checking if processes are running

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

Create a mutex to prevent duplicate execution (the mutex name varies from sample to sample)

```
v5 = CreateMutexA(0, 0, "^_-HappyLife^_-");
```

[Figure 3-5] Create mutex

Create a batch file in any path.

```
GetCurrentDirectoryA(0x104u, &Buffer);
wsprintfA(&FileName, "%s\\upwindowsetsecurity.bat", &Buffer);// 특정 경로에 upwindowsetsecurity.bat 생성
```

[Figure 3-6] Create batch file

Identify the drive type (removable drive / hard drive, etc.) and perform file encryption.

```
void __stdcall __noreturn sub_403E70(LPVOID lpThreadParameter)
{
  int v1; // eax@2
  WCHAR String1; // [sp+4h] [bp-38h]@1

  lstrcpyW(&String1, lpThreadParameter);
  Sleep(0x64u);
  while ( 1 )
  {
    v1 = CheckDrive_402AF0();
    sub_401D70(&String1, L"*.*", off_417104, v1, 1);
    Sleep(0x493E0u);
  }
}
```

[Figure 3-7] Check drive type

Check the drive name from A to Z (including uppercase letters only) and search for an infection. The part where the file is encrypted runs as a thread.

```
do
{
  wsprintfW(&RootPathName, L"%c:", (v6 + 65));// A~Z : 드라이브 확인
  v9 = GetDriveTypeW(&RootPathName);
  _mm_storel_epi64(v5, 0i64);
  sub_405640(v5, &RootPathName, 8);
  if ( v9 == 3 || v9 == 2 )
  {
    CreateThread(0, 0, sub_403E70, v5, 0, 0);
    Sleep(0x3E8u);
  }
  Sleep(0x64u);
  ++v6;
}
while ( v6 < 26 );
```

[Figure 3-8] Drive File Verification and Thread running

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

After checking whether the file to be infected is included in the target of infection exclusion, if not, the file is encrypted by a thread.

```
else
{
  if ( FindFileData.dwFileAttributes & 0x10
    || !lstrcmpW(FindFileData.cFileName, L"..")
    || !lstrcmpW(FindFileData.cFileName, L".")
    || sub_402F90(FindFileData.cFileName, L".CIop")
    || sub_402F90(FindFileData.cFileName, L"CIopReadMe.txt")
    || sub_402B70(FindFileData.cFileName)
    || sub_402CA0(FindFileData.cFileName) )
  {
    v9 = a5;
  }
  else
  {
    v7 = FindFileData.nFileSizeHigh;
    v8 = FindFileData.nFileSizeLow;
    sub_406140(&String2, 0, 520);
    v31 = &v27;
    wsprintfW(&String2, L"%%%%%?%%%s", &v27);
    Sleep(0xDu);
    sub_406140(&Parameter, 0, 2408);
    lstrcpyA(&Parameter, a3);
    lstrcpyW(&v21, FindFileData.cFileName);
    lstrcpyW(&v20, &String2);
    v22 = v8;
    v23 = v7;
    v34 = 0;
    v33 = 0;
    if ( a5 == a4 )
    {
      v9 = 1;
      v10 = CreateThread(0, 0, RAN_StartAddress, &Parameter, v33, v34);
      WaitForSingleObject(v10, 0xFFFFFFFF);
    }
```

[Figure 3-9] Confirmation of infection exclusion

All files except the extensions and file names corresponding to the table below are encrypted.
(The file name and extension may vary depending on the ransomware version.)

File name
desktop.ini, autorun.inf, ntuser.dat, iconcache.db, bootsect.bak, ntuser.dat.log, thumbs.db, DESKTOP.INI, AUTORUN.INF, NTUSER.DAT, ICONCACHE.DB, bootsect.bak, NTUSER.DAT.LOG, THUMBS.DB, boot.ini, BOOT.INI, ntuser.ini, AUTOEXEC.BAT, autoexec.bat, NTDETECT.COM, ntdetect.com, CIopReadMe.txt, ntldr, NTLDR

[Table 3-4] Infection Excluded File Names

Extension
.CIop, .dll, .DLL, .exe, .EXE, .sys, .SYS, .OCX, .ocx, .LNK, .lnk

[Table 3-5] Infection Excluded extension

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

03. Sodinokibi Ransomware

1) Sysnopsis

Sodinokibi (Sodin, REvil) ransomware has been deployed in various ways since the end of April this year, including **attachments, vulnerabilities, exploit kits, fort scanning and RDP brute force attacks**. It also has a feature that stores information such as keys used for encryption and extensions that are changed in **the registry**. It has been distributed in much the same way as the method for distributing GandCrab ransomware, but there are additional cases of exploiting **zero-day and one-day vulnerabilities**.

Classification	Contents
File	- File encryption and extension (random value) change
Network	- Attempts to communicate the collected data to a specific C2 server
Registry	- Stores key used for file encryption, changed extension, etc.

[Table 3-6] Behavior summery

2) Distribution type

The same methods are used as the previous GandCrab ransomware was distributed, but if there is anything unusual, attackers are using the vulnerability to spread the ransomware and execute it directly with a Powershell command after the attack. Because of these methods, victims can be infected by vulnerable systems even if they do not run ransomware.

The distribution methods confirmed to date are as follows.

Distribution methods	Contents
Spear Phishing	**- Distribution through attachment of various impersonated emails** ex) Application form, impersonation of financial company, spam blacklist, bank, sex crime, constitutional court, request for quotation, original image, etc.
Vulnerability	- CVE-2019-2725 (WebLogic vulnerability) - CVE-2019-2729 (WebLogic vulnerability) - CVE-2018-8453 (Windows permission elevation vulnerability)
others	- RIG Exploit Kit - Malvertising

[Table 3-7] Ransomware Distribution Method

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

3) File Type

The types that are distributed directly to users are often distributed through **attachments in impersonated emails**. Various file types are used to disguised as normal attachments.

File format		Contents
Compressed file	Link file (*.lnk)	- Disguised as an icon of a file that is impersonating (ex. A document icon) - Linked ransomware file is executed when execution
	Execution file (*.exe)	- Mostly hidden and not visible on the user's PC unless the folder option is changed - Linked to LNK file and the file is executed when the link file is executed
Java script (*.js)		-

4) Uniqueness

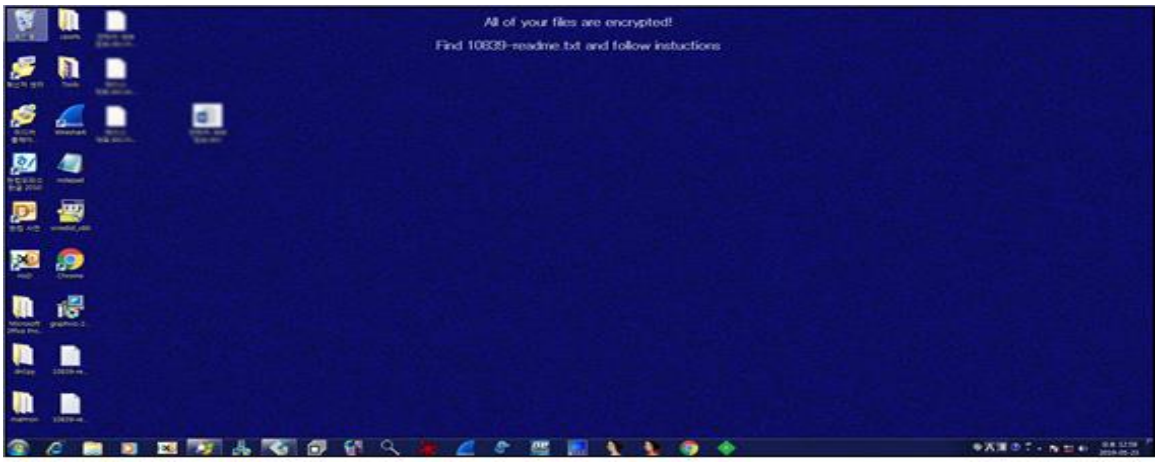
It is distributed in a manner very similar to Gandcrab Ransomware (Spear Phishing, Malvertizing, etc.). However, the attack by exploiting various zero-day vulnerabilities differs from the way GandCrab ransomware is distributed. Recent variants use **Heaven's Gate** to evade detection of antiviruses, are encrypted with complex algorithms and currently have no decryption tools.

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

5) Detailed behavior analysis

When the infection is completed, the desktop changes as follows.



[Figure 3-10] Changed Desktop after Infection

Mutex is created to prevent duplicate execution, and the mutex name is different for each sample.

```
signed int makeMutex_40471B()
{
  signed int v0; // esi@1
  int v2; // [sp+4h] [bp-58h]@1
  __int16 v3; // [sp+5Ah] [bp-2h]@1

  decoding_text_404C82(&unk_41CC30, 153, 7, 86, &v2);// EAX=0021F744, (UNICODE "Global\6CAC559B-02B4-D929-3675-2706BBB8CF66!")
  v3 = 0;
  v0 = 0;
  CreateMutexW_Return_41D45C = CreateMutexW_41CA7C(0, 0, &v2);// Global\6CAC559B-02B4-D929-3675-2706BBB8CF66
  if ( CreateMutexW_Return_41D45C && RtlGetLastWin32Error_41CAA4() == 183 )
    v0 = 1;
  return v0;
}
```

[Figure 3-11] Creating a Random Mutex

Delete the shadow copy using the following command.

```
de_text_404C63(&unk_41CBE8, 0x578, 15, 14, &v3);// cmd.exe
v4 = 0;
de_text_404C63(&unk_41CBE8, 0x180, 8, 292, &v1);// EAX=001BFC84, (UNICODE "/c vssadmin.exe Delete Shadows
                                                // /All /Quiet & bcdedit /set
                                                // {default} recoveryenabled No & bcdedit /se")
```

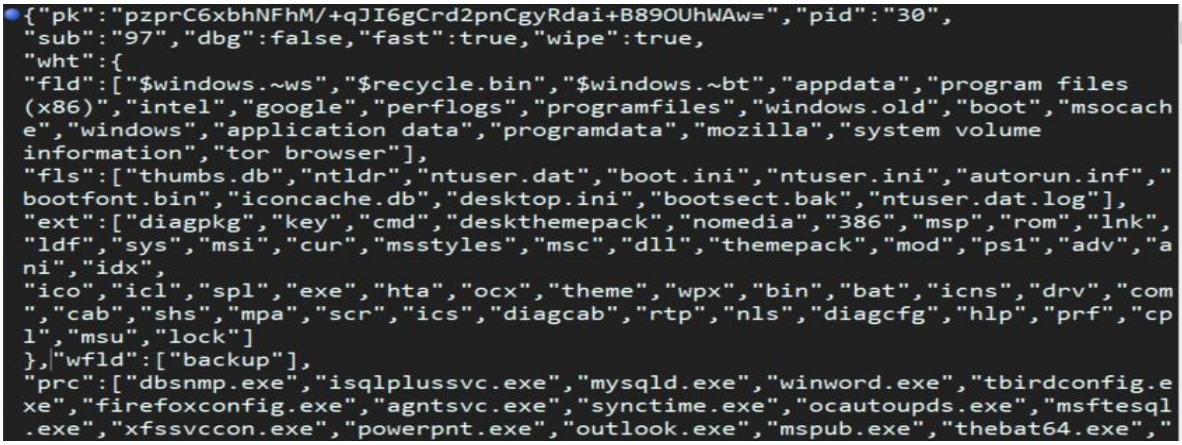
Command
cmd.exe /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /se

[Table 3-9] Shadow Copy Delete Commands

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

The data used for file encryption is loaded into memory and then decrypted using an arbitrary decoding routine. The decrypted data contains information such as what is excluded from infection, PK, infection exclusion extension, etc.



[Figure 3-12] Data Used for Infection

Folder name
$windows.~ws, $recycle.bin, $windows.~bt, appdata, program files (x86), intel, google, perflogs, programfiles, windows.old, boot, msocache, windows, application data, programdata, mozilla, system volume information, tor browser

[Table 3-10] Excluded Folder Names

File name
thumbs.db, ntldr, ntuser.dat, boot.ini, ntuser.ini, autorun.inf, bootfont.bin, iconcache.db, desktop.ini, bootsect.bak, ntuser.dat.log

[Table 3-11] Infection Excluded File Names

File extension
diagpkg, key, cmd, deskthemepack, nomedia, 386, msp, rom, lnk, ldf, sys, msi, cur, msstyles, msc, dll, themepack, mod, ps1, adv, ani, idx, tico, icl, spl, exe, hta, ocx, theme, wpx, bin, bat, icns, drv, com, cab, shs, mpa, scr, ics, diagcab, rtp, nls, diagcfg, hlp, prf, cpl, msu, lock

[Table 3-12] Infection Exclusion File Extensions

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

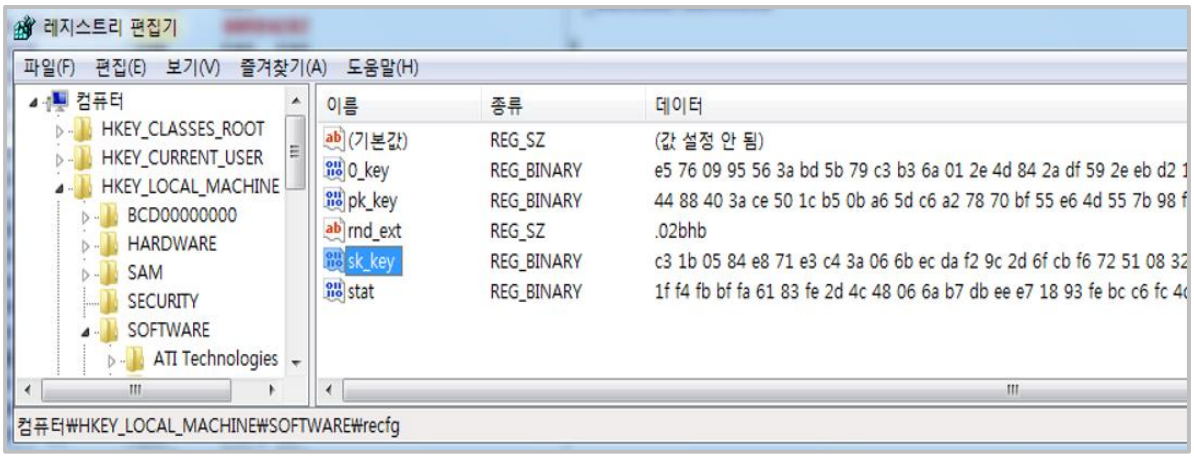
Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

The values used for encryption are created through specific routines, stored in specific registry keys, and each value is retrieved and used. The values stored in the registry key are as follows.

(Regisryr key route : HKEY_LOCAL_MACHINE\SOFTWARE\recfg)

Creation value	Contents
0_key	Used to encrypt files (encryption related keys)
pk_key	
sk_key	
rnd_ext	File extension to be changed after file encryption on the PC (Random value)

[Table 3-13] Keys and Their Contents Stored in the Registry



[Figure 3-13] Key Values Stored in the Registry

After checking the drive status, search for the drive name from A to Z and infect it.

(If the shared folder is held by drive, it gets infected together)

```
de_text_404C63(&unk_41CBE8, 1113, 5, 14, &v3);// EAX=001BFDA8, (UNICODE "₩₩?₩A:₩x")
v4 = 0;
sub_404FBC(v2, &v3);
while ( *(v2 + 8) <= 0x5Au )
{
  if ( (GetDriveTypeW_41CAAC(v2) - 2) <= 2 )// return 2 : 이동형 저장장치(DRIVE_REMOVABLE)
    folder_find_4060F0(v2, a1);             // A:₩부터 알파벳을 한글자씩 올려가면서 동작
  ++*(v2 + 8);
  *(v2 + 14) = 0;
}                                           // A~Z 드라이브까지 탐색
sub_403B66(v2);
result = 1;
```

[Figure 3-14] Check Drive Information

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

Check the network drive connected to your PC. At this time, if a network drive exists, it is infected together.

```
int __cdecl searchNetDrive_4064E2(int a1, int a2)
{
  int v3; // edi@3
  int v4; // eax@5
  unsigned int v5; // ebx@6
  _DWORD *v6; // esi@7
  int v7; // ST0C_4@15
  int v8; // [sp-8h] [bp-18h]@3
  int v9; // [sp+0h] [bp-10h]@5
  int v10; // [sp+4h] [bp-Ch]@3
  int v11; // [sp+8h] [bp-8h]@1
  int v12; // [sp+Ch] [bp-4h]@3

  if ( WNetOpenEnumW_41CA74(2, 1, 0, a2, &v11) )// 컴퓨터가 접속한 원격드라이브 포함
    return 0;
  v12 = -1;
  v10 = 0x4000;
  v3 = sub_403B3A(0x4000);
```

[Figure 3-15] Network Drive Search

Collect various system information. (PC name, language used by the PC, etc.)

```
02bhb_41D6C8 = regKey_rnd_ext_401B7B(1);        // return .02bhb(확장자)
asdfasd_41D6D8 = sub_404220();                  // return asdfasd
if ( !asdfasd_41D6D8 )
  asdfasd_41D6D8 = sub_405036(&v91);
dword_41D6DC = sub_403D62();                    // return WIN-P985HP16QH3
if ( !dword_41D6DC )
  dword_41D6DC = sub_405036(&v91);
dword_41D6E0 = reg_Domain_403EC8();             // return WORKGROUP
if ( !dword_41D6E0 )
  dword_41D6E0 = sub_405036(&v91);
dword_41D6E4 = reg_localName_404017(1);         // return ko-KR
```

[Figure 3-16] Checking Drive Information

The collected information is sent to a number of domains with arbitrary values including: The number of domains used is more than 1000.

```
"dmn":"mundo-pieces-auto.fr;mind2muscle.nl;atrgroup.it;eksperdanismanlik.com;lidkopingsnytt.nu;bd2fly.com;teamsegeln.ch;leopoldineroux.com;gardenpartner.pl;theintellect.edu.pk;malevannye.ru;bychowo.pl;eatyoveges.com;aheadloftladders.co.uk;bjornvanvulpen.nl;global-migrate.com;jefersonalessandro.com;adterium.com;chainofhopeeurope.eu;biodentify.ai;nicksrock.com;yourhappyevents.fr;forskolinslimeffect.net;heuvelland-oaze.nl;krishnabrawijaya.com;klapanvent.ru;lunoluno.com;hostingbangladesh.net;hensleymarketing.com;weddingceremonieswithtim.com;carolynfriedlander.com;bendel-partner.de;baikalflot.ru;edrickennedymacfoy.com;alabamaroofingllc.com;n-newmedia.de;vapiano.fr;test-teleachat.fr;memphishealthandwellness.com;rino-gmbh.com;orchardbrickwork.com;zorgboerderijravensbosch.nl;etgdogz.de;racefietsenblog.nl;a-zpaperwork.eu;ox-home.com;cymru.futbol;bcabattoirs.org;janellrardon.com;schroederschoembs.com;log-barn.co.uk;trevi-vl.ru;pansionatblago.ru;quitescorting.com;arthakapitalforvaltning.dk;utilisacteur.fr;rentsportsequip.com;brannbornfastigheter.se;saint-malo-developpement.fr;oscommunity.de;autoteamlast.de;grupoexin10.com;banksrl.co.za;triavlete.com;towelroot.co;ruggestar.ch;oexebusiness.com;bagaholics.in;aciscomputers.com;mariannelemenestrel.com;agencewho-aixenprovence.fr;angeleyezstripclub.com;ykobbqchicken.ca;advesa.com;ingresosextras.online;crestgood.com;gavelmasters.com;p-ride.live;martha-frets-ceramics.nl;bodymindchallenger.com;c-sprop.com;matteoruzzaofficial.com;netadultere.fr;koncept-m.ru;promus.ca;internalresults.com;nbva.co.uk;arabianmice.com;rubyaudiology.com;tellthebell.website;webforsites.com;cleanroomequipment.ie;oro.ae;the-beauty-guides.com;linkbuilding.life;shortsalemap.com;shortysspices.com;aoyama.ac;adabible.org;atelierkomon.com;gratiocafeblog.wordpress.com;napisat-pismo-gubernatoru.ru:443;alisodentalcare.com;tilldeeke.de;protoplay.ca;gbk-tp1.de;subquercy.fr;gosouldeep.com;fbmagaz
```

[3-17] Checking Drive Information

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

04. Detailed Analysis of Pre-attack (CLOP) fromTA505 Group

The TA505 group is a hacking group that is believed to be supported by the Russian government, and has been distributing malware through various impersonation emails for a number of domestic companies and financial sectors since February 2019. The attack vectors covered in this part were drawn from the collected samples from February to June 2019.

1) Types of attack-Distribution of malicious code using attachments of mail

In February 2019, the invoice_xxxx.xls samples were distributed under the pretense of various documents. But at the end of May 2019, they started using a sample that changed the form of attachments from Excel (* .xls) to HTML (* .html) files. When executing HTML file, Excel file is downloaded from a specific server and Excel file of the same routine is downloaded and executed. This seems to circumvent spam processing of emails with Excel files attached, and it is expected that various types of attachments will be used for attacks in the future.

Month	Attachment typr	Title of attachment
2	Microsoft Excel	Invoice_ [number] .xls
3	Microsoft Excel	Certificate.xls, Purchase order4500286249.xls
4	Microsoft Excel	20180423 receipts and payments.xls
5	Microsoft Excel, **HTML**	eTaxInvoice_[number].html, eTaxInvoice_[number].xls
6	Microsoft Excel, **HTML**	Contract_[number].html, [number].xls, 20.06.2019 remittance [number].[number].html, 20.06.2019 remittance [number].[number].htm 20.06.2019 remittance [number].[number].xls

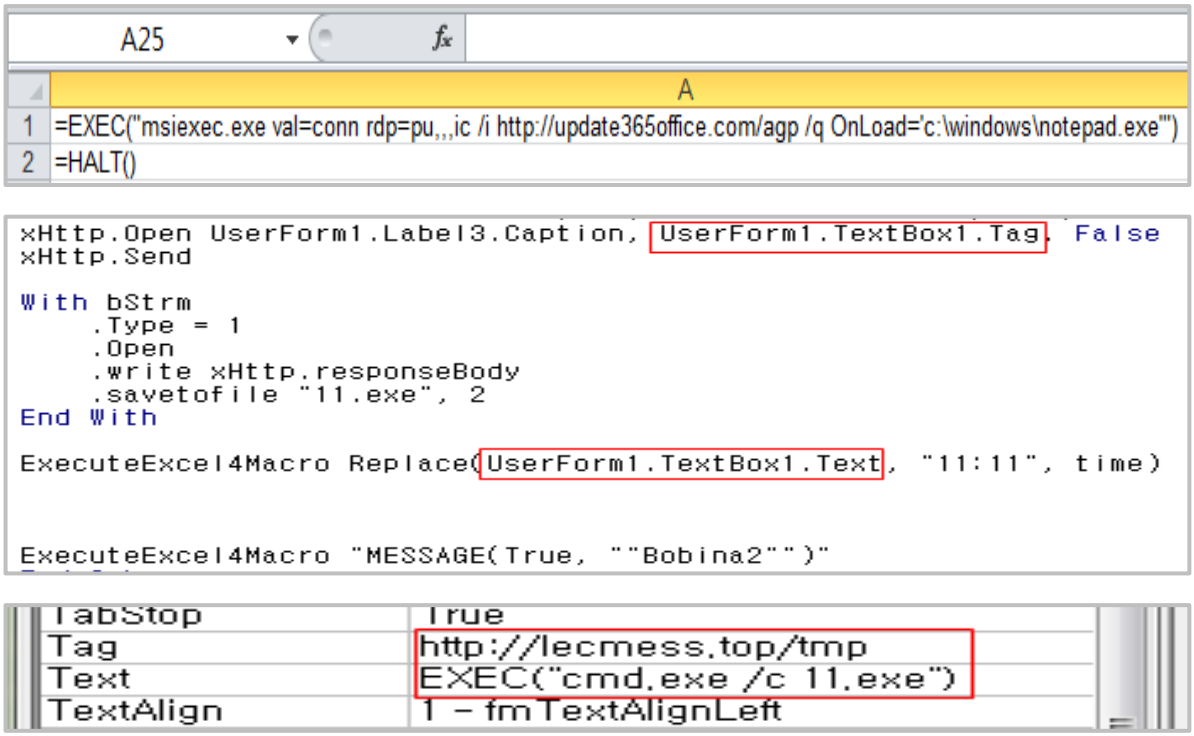
[Table 3-14] Ransomware Distribution Method

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

2) Pre-Attack from TA505 group – excel attachment

Excel attachments used by the TA505 group commonly contain **malicious macros** that attempt to connect to arbitrary C2 servers. In the sample (2019.02) used at the beginning, macros connecting to **C2 # 1 (first C2)** were inserted in the hidden sheet, but in subsequent attacks, data about C2 # 1 was added to the tag and text areas of the form area. Excel attachment is used as a downloader that downloads arbitrary files after connecting to C2 # 1.



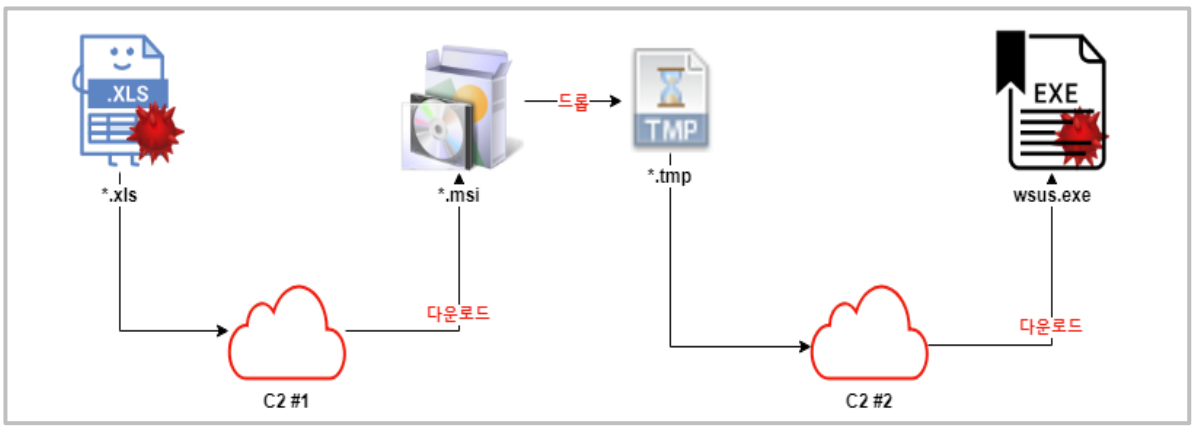
[Figure 3-18] C2 Connection in Various Forms

3) Pre-Attack from TA505 group – Excel to final payload

The Excel malware used by the TA505 group has something in common that macros download additional malware from **C2 # 1** for the next attack. Additional malware downloaded via **C2 # 1** accesses **C2 # 2 (second C2)** and downloads the final payload **wsus.exe.** In the process of downloading the final payload from the Excel file, several changes were observed.

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)



[Figure 3-19] Attack Vector Used in Initial Attack

[Attack Vector 1] – Full Overview (Run-> C2 # 1-> C2 # 2)

(Vector 1.1) The attack vector used in the initial attack is shown in [Figure 3-18]. In the macro of the Excel file, the MSI (Windows Installer) file is downloaded and executed. Drop / execute * .tmp in executed MSI file to access C2 # 2 and download final malware.

(Vector 1.2) Execute ***.tmp** after downloading * .tmp from **C2 # 1** using macro of Excel file. (Skip downloading ***.tmp** using MSI.) Access and download the final malware.

[Attack Vector 2] – (C2 # 2 Approach Process)

(Vector 2.1) When accessing C2 # 2 from * .tmp, check the environment in which malicious code is running using **"net use / domain"** command. After that, if it is not an AD server, terminate the program without accessing C2 # 2.

The final download of **wsus.exe** uses the leaked source **code(Flawed Ammyy)** of the commercial remote control program called **Ammyy Admin**. It collects various information using the backdoor function and sends it to the server. Wsus.exe is disguised as a normal program with a signed certificate.

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

4) Pre-Attack from TA505 group – Comparison with Offshore Target Attack Vectors

The attack routines used by the TA505 group for domestic attacks are changing rapidly. The attack group is attacking not only domestic but also foreign countries, and the attack routines used are showing the following differences with the sample type used in Korea.

	Korea	Overseas country
Mean of attack	malicious mail attachment	malicious mail attachment
File format	MS Excel(*.xls)	MS Excel(*.xls)
First malicious code	**Access and download from malicious code distribution site # 1 using Excel macro (1 file)**	**Access and download from malicious code distribution site # 1 and # 2 using Excel macro (2 file)**
First malicious code File format	**MSI, *.tmp(*.exe)**	**MSI, SFX(*.exe), *exe**
Second malicious code	**After the first malicious code is executed, access the malicious code distribution site # 2 and download it.**	**Drop from SFX type of two downloaded malicious codes**
Second malicious code File format	***.dat, template_[random value]. Random extension**	**SFX(*.exe),** *.exe, i.cmd(*.bat)
Third malicious code	Decrypt **final malware** through random operation in the second malware	**Drop the final malware (winserv.exe) from SFX-type malware among the dropped files**
Third malicious code file format	**wsus.exe**	**winserv.exe**, setting.dat, i.cmd(*.bat), exit.exe
Purpose	Information capture and RAT **(Flawed ammyy)**	Information capture and RAT **(Remote Manipulator System)**
Target	AD server	-

[Table 3-15] Korea / Overseas Attack Vector Comparison

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

05. Countermeasures

Ransomware causes massive damage to the system when infected, and data cannot be recovered if ransomware is infected with a decryption tool. **Therefore, it is important to make sure that infection does not occur first,** and then check and block the route where additional infection can occur.

① Prohibit link / attachment of e-mails received from untrusted senders or organizations

This is the method most widely used by various ransomware and malware distributors. Disseminating mail by pretending to be various organizations and specific people, and the contents of malicious mail are becoming more sophisticated. We recommend that you never execute attachments attached to suspicious emails such as awkward Korean language usage, attachments and link execution, sending to unknown email accounts, hacking threats, or attachments that seem insignificant.

Ransomware that is distributed by disguising as a document file exists, so it is recommended that an attachment with any extension / icon is not executed if it is attached to a suspicious mail.

② Vulnerability patch

Recently, various one-day and zero-day vulnerabilities have been used to infiltrate the system and spread ransomware. Therefore, we recommend that you keep your environment up-to-date.
(Sodinokibi exploited Web Logic Server Vulnerability CVE-2019-2725)

③ Windows OS : RDP(Remote Desktop Protocol) security setting

In the past, ransomware attackers have used RDP-targeted attacks to inject and execute ransomware directly. The attack is carried out by identifying the non-working hours such as night or dawn, and many kinds of ransomware known to date (GandCrab, Sodinokibi, Crysis, etc.) have been infected by the system. Therefore, it is recommended to strengthen the security of the function.

④ Run Anti-virus solution for real time scan and update

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

Ransomware trends for the first half of 2019 (Part 1. CLOP/Sodinokibi)

⑤ Detect and block IoC information at the firewall or IPS (sample used in the report)

Number	File name	
1	CLOP Ransomware	a3ad385444da692d751b9141922ef01e
2		0403db9fcb37bd8ceec0afd6c3754314
3	Sodinokibi Ransomware	72fc67f28e5223b034e357ea7e620d9e
4		13533631b1b82c77ff5bf132771b7724
5	Invoice 12-2-2019.xls	da0dc5e26a4dd2f85c1c56f65999f79b
6	17337ASE.xls	ba29927464fca99980bca1a366a8ce97
7	Invoice-09547593402.xls	7DEB2CBC62ABFF912E4EF03C2B15EF23
8	Daily report 20180423 .xls	C2DBCC176BF6FA9C20F93EF258724C6A
9	C58635.xlsb	6C0D8B03AE466C8142320DAFF9983DBF
10	052719_34D033.xls	6B9CA01960F3D63BF6EA8056D8B52B2D
11	Purchase order 450 0286249.xls	3645C04AD11B617E423EEFB563149ABE
12	C047743.xls	B16E889F912CD8CB4E1349D517C9DA57

[Table 3-16] IOC Information

06. Reference

[1] https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

[2] Checkmal (Clop ransomware infection continually targets companies (2019.5.30)) https://blog.naver.com/PostView.nhn?blogId=checkmal&logNo=221550406092&navType=tl

[3] Checkmal (Sentral selection option included in the Sodinokibi ransomware distribution mail (2019.5.8))http://blog.naver.com/checkmal/221532344042

[4] https://www.krcert.or.kr/data/trendView.do?bulletin_writing_sequence=35018

[5] https://securelist.com/cve-2018-8453-used-in-targeted-attacks/88151/

[6] https://blog.talosintelligence.com/2019/07/rats-and-stealers-rush-through-heavens.html

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

CHAPTER 4

Special Column

How to ensure Container Security,

between user convenience and security

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

How to ensure Container Security, between user convenience and security

Cyber Security Research Lab.

01. Do you have security settings for this service?

As you look back on your IT environment and history, where the day evolves differently, there is a flow that is captured without exception. Many IT industry workers cite security departments and their employees as the main culprit behind the introduction of new innovations. IT workers need to rapidly develop and provide new services that meet the changing needs of their IT environment and customer needs, as security departments and workers in the security industry appear to be disrupted at critical times. Every one is sure that security is important , but they don't want to interfere with what I do.

As new IT technologies emerge, the people around them look at them in different ways. First, IT industry workers pay attention to the convenience and innovation that this technology will bring. Attackers, on the other hand, focus on how to make money by exploiting the loopholes in the technology. And security practitioners between IT and attackers are constantly contemplating what vulnerabilities are in the new technology, whether there are any new security problems by incorporating this technology, and how to apply security elements to the new technology.

“Container” technology, which has quickly emerged as an innovation that can increase the agility of the corporate IT environment, is also a new area of challenge for security practitioners. In this issue, I'll talk about the security areas we are struggling with to make container technology safer.

02. Evolving Container Technology

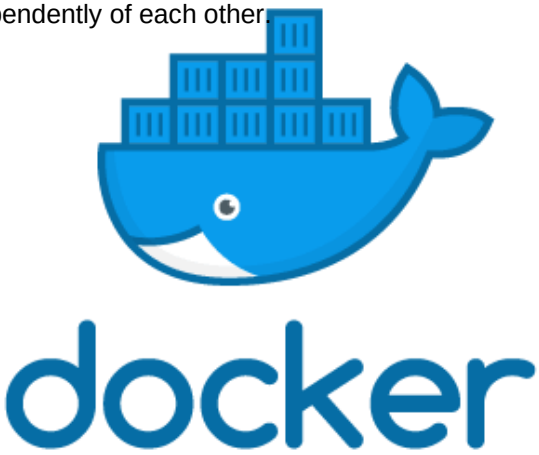
Before we talk about security, let me briefly talk about virtualization technology. Virtualization is a technology that provides independent services by creating multiple virtual machines (VMs) on a single resource (PC, server, etc.). VMs are made in the form of small amounts of the power of many existing infrastructures. Thus, even if some of the infrastructure supporting the VM fails, it is possible to immediately receive the ability from another infrastructure to respond quickly to obstacles and to make efficient use of the infrastructure.

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

How to ensure Container Security, between user convenience and security

Companies around the world have embraced virtualization technologies that can make their infrastructure environments robust. In particular, among many virtualization technologies, hypervisor-based virtualization technology that rapidly creates and utilizes multiple virtual machines on the hypervisor environment has rapidly spread. It is a method of installing and operating a guest OS for executing applications and applications on a VM in which a virtual infrastructure and a host OS are packaged.

Meanwhile, unlike the hypervisor-based virtualization technology, the container virtualization technology that can configure an application while sharing one OS was also introduced. It creates a separate space called a container in the host OS and virtually allocates only resources (CPU, Memory, Storage, Network, etc.) and processes for running the application. This allows each container to use its limited resources more efficiently, and can create an environment in which containers can move independently of each other.



[Figure 6-1] Docker Image (Source: docker.com)

Despite the faster and lighter advantages of hypervisor-based virtualization, container technology has had little impact. This is because the container-based solution that users want is not available. However, Docker, a container-based virtualization solution that appeared like a comet in 2013, has made a big difference across the virtualization market. Similar to workers (dockers) who move and manage containers in ports, they make it easier for users to create, manage, and distribute containers.

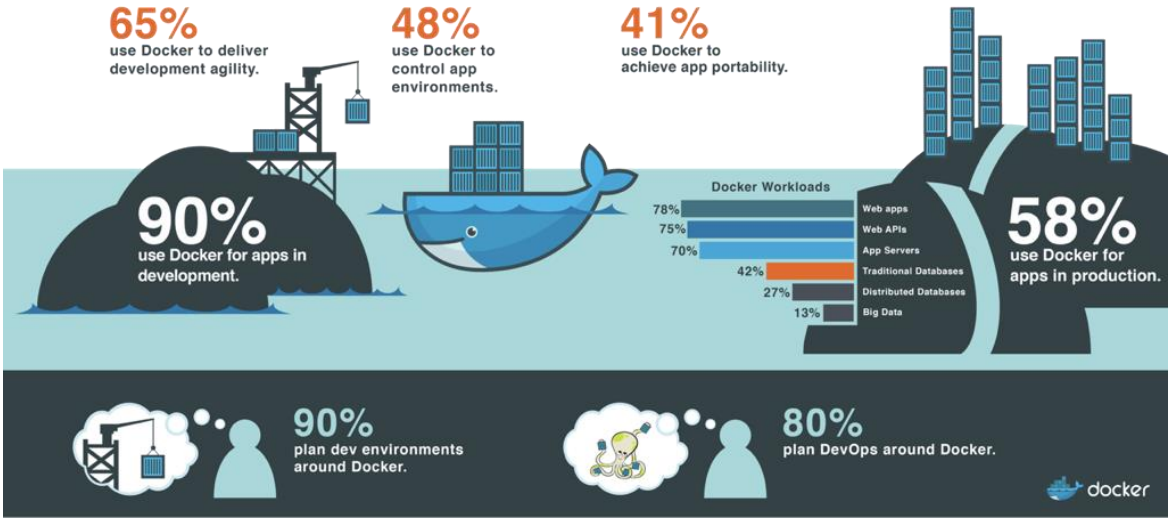
Docker containers use "images" to manage all of the elements necessary to run an application. 'Image' is a value that doesn't change and runs the same regardless of the environment. The value changed while running 'Image' in the container is stored in the container. Users can easily create containers and distribute images using images, without having to install anything. Docker provides a number of Docker images through its “Docker Hub,” and is constantly improving and managing them.

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

How to ensure Container Security, between user convenience and security

Business people can use Docker to streamline application development and operation. Developers can concentrate on development without worrying about the application development environment, and system operators can improve work convenience by not having to pay attention to the components for the development environment.

Since the emergence of the highly popular Docker, container virtualization has begun to become popular. Docker's 2016 survey showed that 58% of respondents were already using Docker for development, and 80% of respondents said they would use Docker in a DevOps environment.



[Figure 6-2] The Evolution of the Modern Software Supply Chain (reference : docker.com)

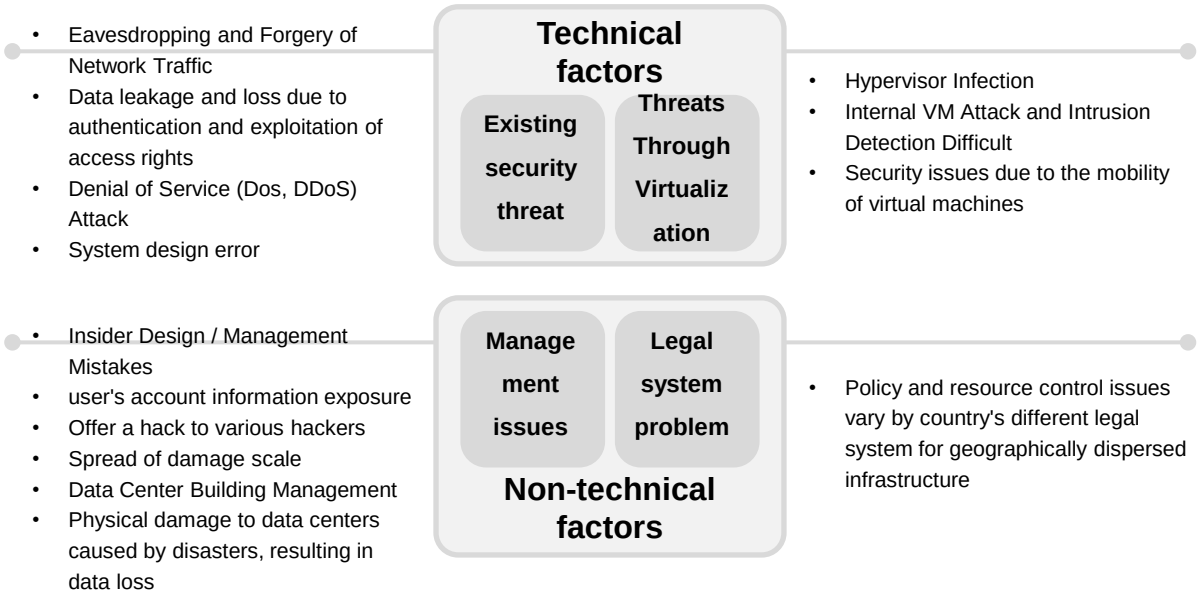
03. Container Security Issue

Just as there is darkness where light exists, technological advances involve security threats. Indeed, with the proliferation of container technology, many companies are facing security issues. According to Tripwire State of Container Security Report (2019), an international security firm, 94% of respondents were concerned about container security, and 60% had container-related security incidents last year. In early 2018, Tesla hacked into Kubernetes' misconfiguration, resulting in a cryptocurrency mining program being installed on an internal system.

What are the main security issues in container environments? First, according to the issue report (2017-006) published by the Software Policy Research Institute (SPRi) in 2017, various security issues that occurred in the existing virtualization environment may appear in the container environment in terms of technical and non-technical aspects. .

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

How to ensure Container Security, between user convenience and security



[Figure 6-3] Reorganization of Cloud Security Threats / (Source: SPRi Issue Report 2017-006)

In addition, attention should be paid to security issues that can only occur in certain container environments. Overseas security company Aqua Security can cause six major security problems for Docker containers, and if the container is operated without countermeasures, security threats can spread to the entire infrastructure. I foresaw.

Container Image Vulnerability	• If a container image is corrupted, it affects all containers that run the image • This issue can lead to more serious problems using unverified open source images.
Image credentials Hard coding	• Storing information such as tokens, passwords, and API keys in an image makes them accessible to unauthorized people • If such data is stored in application code, it can be published through Git.
Large attack exposure	• Docker requires root privileges, and anyone with access will also have root privileges • When an attacker takes over an account on Docker, an attacker can obtain the corresponding privilege
Lack of granular role-based access control (RBAC)	• Docker RBAC provides role-based access control, but issues that can arise due to lack of detailed settings (RBAL: Role based Access Control)
Lack of visibility	• The complexity and short lifespan of Docker containers make it difficult to track containers and manage security
Side network shift	• One Docker host can infect any host connected to the same network • Perimeter security applied by existing firewalls cannot protect it

[Figure 6-4] 6 Docker Security Issues / (Source: blog.aquasec.com Figure 6-4.)

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

How to ensure Container Security, between user convenience and security

04. How to apply security

The security issues of the container environment mentioned above can be subdivided as follows.

1) Security issues due to problems such as configuration error of the container itself
2) security issues of the vulnerability itself within the image

The first security issue can be solved in a similar way to the traditional security issue. Organizations can enhance security by performing thorough access control and account setting management and using the suitable infrastructure security solutions. However, considering the amount of data generated exponentially in real time in a container environment, it is required to apply an advanced detection technique that has been advanced from a general detection technique.

In order to solve the second security issue, integrated and continuous security activities are required, from the creation of containers using images to the visibility of numerous containers. Attackers are attacking malicious deployments of "images" that contain unpatched vulnerabilities or malware, which, if used without question, can lead to infection of many containers.

As an application can consist of hundreds to thousands of containers, it must be able to pinpoint compromise indicators distributed across numerous hosts and quickly correlate them to isolate infected containers. Red Hat emphasizes thorough security activities in areas such as image acquisition, access management, security test integration and deployment automation, and infrastructure protection.

No.	Security items	Contents
1	Image collection	• Are container images signed from trusted sources? • Are the runtime and operating system layers up to date? • How fast and how often are containers updated? • Identify and track known issues?
2	Access management	• What role-based access control is used to manage container images? • Is there a tagging feature that supports image classification? • Can I use the registry to assign and automate policies?
3	Security test integration & Distribution automation	• How to prevent patching of running containers? • Is it possible to use triggers to rebuild my container and replace it with automated updates?
4	Infrastructure protection	• Which containers access each other • How to control access and management of shared resources (network, storage)? • How to monitor container status? • How to manage host updates (such as concurrent updates)?

[Table 6-1] Container Security (Reconfiguration) / (Source: redhat.com)

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

How to ensure Container Security, between user convenience and security

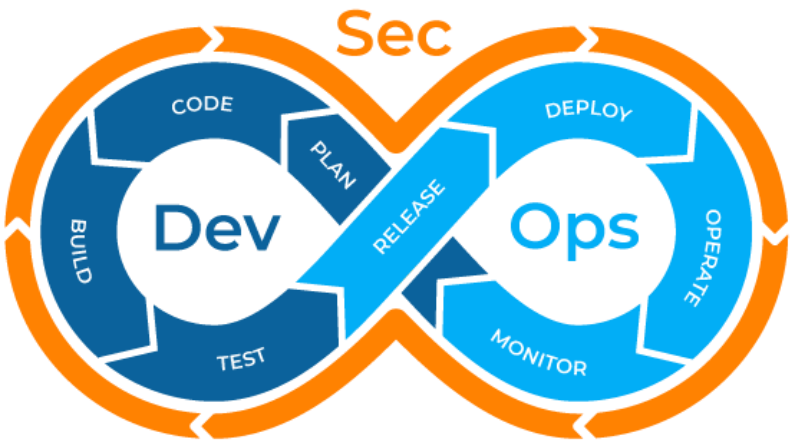
Security personnel can take advantage of proven security solutions for each area. However, introducing a security solution does not eliminate all security threats associated with containers. As with traditional on-premises environments, errors in policy or configuration can be a potential threat to crack hard glass. Enterprises need to build a DevSecOps environment that embeds security into their operational and development environments before introducing optimized security solutions for each domain.

05. Changing the Perspective on Container Security

More and more companies are applying container technology to improve their efficiency and productivity. From the security point of view, the burden of keeping the container safe is considerable. This is because it is an unknown area that does not know what risks are lurking, and when the “image” that contains malicious code is raised due to the characteristics of the container, there is a possibility that the risk may spread more quickly than an external attack.

Security personnel are attempting to control and verify the container-based development and operation stages as closely as possible based on the threat factors and countermeasures currently identified. Perhaps it would be a long day for the security staff to ask, “Did you set up security for this service?” And the operations and development staff who say “I can't work because of security.”

So far, security professionals have been hardening their security against constant changes in the IT environment and the emergence of new attacks. Container technologies that accelerate DevOps adoption are no exception to this flow. Rather, security officials expect to build a more secure DevSecOps environment to ensure security in a convenient container environment.



[Figure 6-4] DevSecOps Diagram / (Source : plutora.com)

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

How to ensure Container Security, between user convenience and security

No.	Contents	
1	Cloud Computing	• Definition: Methodology • Purpose: virtual resource pooling and automation for on demand use • Usage: Provide various user groups with various resources
2	Virtualization	• Definition: Technology • Purpose: create multiple simulation environments on one physical hardware system • Purpose: To provide a specific user with a packaged resource for a specific purpose
3	Hypervisor	• Software called the hypervisor connects directly to the hardware and divides one system into a separate, unique, secure environment called a virtual machine (VM). • VMs operate by using the capabilities of the hypervisor to separate the machine's resources from the hardware and then deploy them appropriately.
4	Container	• Manage each container through the container engine • Containers are constructed using images, which contain the information required by the application (files, settings, executables to run).

[Table 6-3] Cloud computing ,Virtualization
, Hypervisor ,Container terms definition / source : redhat.com

06. Resource

1. Core Issues and Countermeasures of Cloud Security (Software Policy Research Institute, SPRi Issue Report 2017-006)
2. Changes in cloud virtualization technology, container-based cloud virtualization and DevOps (Software Policy Research Institute, SPRi Issue Report 2018-008)
3. Top Docker Security Best Practices(Aqua Security Blog, https://blog.aquasec.com/docker-security-best-practices)
4. Cloud Information Protection Guide (Korea Internet & Security Agency, 2017)
5. Security Guidance for critical areas of focus in cloud computing v4.0(Cloud Security Alliance, 2017)
6. Tripwire State of Container Security Report(Tripwire, 2019)
7. 10 tiers for container security (redhat, 2017)

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

We Know SECURITY!

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

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

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