

# Vulnerable Microsoft SQL Servers targeted with Cobalt Strike

[bleepingcomputer.com/news/security/vulnerable-microsoft-sql-servers-targeted-with-cobalt-strike/](https://bleepingcomputer.com/news/security/vulnerable-microsoft-sql-servers-targeted-with-cobalt-strike/)

Bill Toulas



By

[Bill Toulas](#)

- February 22, 2022
- 01:08 PM
- [0](#)



Threat analysts have observed a new wave of attacks installing Cobalt Strike beacons on vulnerable Microsoft SQL Servers, leading to deeper infiltration and subsequent malware infections.

MS-SQL Server is a popular database management system powering large internet applications to small single-system applets.

However, many of these deployments aren't adequately secured as they are publicly exposed to the Internet with weak passwords, and according to a report by Ahn Lab's ASEC, an unknown threat actor is taking advantage of this.

## Targeting MS-SQL with Cobalt Strike

---

The attacks start with threat actors scanning for servers with an open TCP port 1433, which are likely public-facing MS-SQL servers. The attacker then carries out brute-forcing and dictionary attacks to crack the password. For the attack to work with either method, the target password has to be weak.

Once the attacker gains access to the admin account and logs into the server, the ASEC researchers have seen them drop coin-miners such as Lemon Duck, KingMiner, and Vollgar. Additionally, the threat actor backdoors the server with Cobalt Strike to establish persistence and perform lateral movement.

Cobalt Strike is downloaded via a command shell process (cmd.exe and powershell.exe) onto the compromised MS-SQL and is injected and executed in MSBuild.exe to evade detection.

Target Type	File Name	File Size	File Path
Target	zde4f0vr.exe	559 KB	%SystemRoot%\serviceprofiles\mssql\$ssql\$express\appdata\local\temp\zde4f0vr.exe
Current	powershell.exe	442 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	cmd.exe	283 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	sqlservr.exe	361.69 KB	%ProgramFiles%\microsoft sql server\mssql12.sql\$express\mssql\bin\sqlservr.exe

### Processes that download Cobalt Strike (ASEC)

After execution, a beacon is injected into the legitimate Windows wwanmm.dll process and waits for the attacker's commands while staying hidden inside a system library file.

"As the beacon that receives the attacker's command and performs the malicious behavior does not exist in a suspicious memory area and instead operates in the normal module wwanmm.dll, it can bypass memory-based detection," explains [the report](#) by Ahn Lab's ASEC group.

The screenshot shows a debugger window with the following assembly instructions and parameters:

```

004015ED . 897424 04 MOV DWORD PTR SS:[LOCAL.17],ESI
004015F1 . 891C24 MOV DWORD PTR SS:[LOCAL.18],EBX
004015F4 . 894424 0C MOV DWORD PTR SS:[LOCAL.15],EAX
004015F8 . C74424 08 20 MOV DWORD PTR SS:[LOCAL.16],20
00401600 . FF15 AC814400 CALL DWORD PTR DS:[<&KERNEL32.VirtualProtect
00401606 . 83EC 10 SUB ESP,10
00401609 . 895C24 0C MOV DWORD PTR SS:[LOCAL.15],EBX
0040160D . C74424 14 00 MOV DWORD PTR SS:[LOCAL.13],0
00401615 . C74424 10 00 MOV DWORD PTR SS:[LOCAL.14],0
0040161D . C74424 08 50 MOV DWORD PTR SS:[LOCAL.16],00401550
00401625 . C74424 04 00 MOV DWORD PTR SS:[LOCAL.17],0
0040162D . C70424 000000 MOV DWORD PTR SS:[LOCAL.18],0
00401634 . FF15 48814400 CALL DWORD PTR DS:[<&KERNEL32.CreateThrea
0040163A . 83EC 18 SUB ESP,18

```

Parameters for the CALL instruction:

```

Parameter
pThreadId => NULL
CreationFlags => 0
StartAddress => 1.401550
StackSize => 0
pSecurity => NULL

```

Address: 004481AC1=764B2E1D (kernel32.VirtualProtect)

The screenshot shows a debugger window with the following hex dump and ASCII:

```

Address Hex dump ASCII
002E0000 4D 5A 52 45 E8 00 00 00 00 5B 89 DF 55 89 E5 81 MZREè [ëßUëã
002E0010 C3 49 7C 00 00 FF D3 68 F0 B5 A2 56 68 04 00 00 AI| yôhδμϕVh-
002E0020 00 57 FF D0 00 00 00 00 00 00 00 00 00 00 00 00 wÿÐ
002E0030 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 €
002E0040 77 77 61 6E 6D 6D 2E 64 6C 6C 00 B0 D6 E4 D1 89 wwanmm.dll °ÖäNë
002E0050 E4 8B 5A 47 E7 69 52 2E 80 81 88 08 5A E5 15 07 ä<ZGçiR.€ 7dZâ+•

```

Address = 002E0000

Size = 209920

NewProtect = F

pOldProtect =

### Code and strings used for tainting the dll (ASEC)

Cobalt Strike is a commercial pen-testing (offensive security) tool that is extensively abused by cybercriminals who find its powerful features set particularly useful for their malicious operations.

The \$3,500 per license tool was meant to help ethical hackers and red teams simulate real attacks against organizations that want to boost their security stance, but from the moment cracked versions were leaked, its use by threat actors went out of control.

It's now used by [Squirrelwaffle](#), [Emotet](#), [malware operators](#), [opportunistic attacks](#), [Linux-targeting groups](#), [sophisticated adversaries](#), and commonly by [ransomware gangs](#) when conducting attacks.

The reason why threat actors abuse it so much is its rich functionality which includes the following:

- Command execution
- Keylogging
- File operations
- SOCKS proxying
- Privilege escalation
- Mimikatz (credential-stealing)
- Port scanning

Moreover, the Cobalt Strike agent called the "beacon" is file-less shellcode, so the chances of it being detected by security tools are decreased, especially in poorly managed systems.

AhnLab's data shows that all the download URLs and C2 server URLs that supported the recent attack wave point to the same attacker.

To protect your MS-SQL server from attacks of this type, use a strong admin password, place the server behind a firewall, log everything and monitor suspicious actions, apply available security updates, and use a data access controller to inspect and enforce policies on every transaction.

## **Related Articles:**

---

[Malicious PyPI package opens backdoors on Windows, Linux, and Macs](#)

[Microsoft warns of brute-force attacks targeting MSSQL servers](#)

[Hive ransomware uses new 'IPfuscation' trick to hide payload](#)

[New ChromeLoader malware surge threatens browsers worldwide](#)

[New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps](#)

[Bill Toulas](#)

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.