Cobalt Strike Being Distributed to Vulnerable MS-SQL Servers

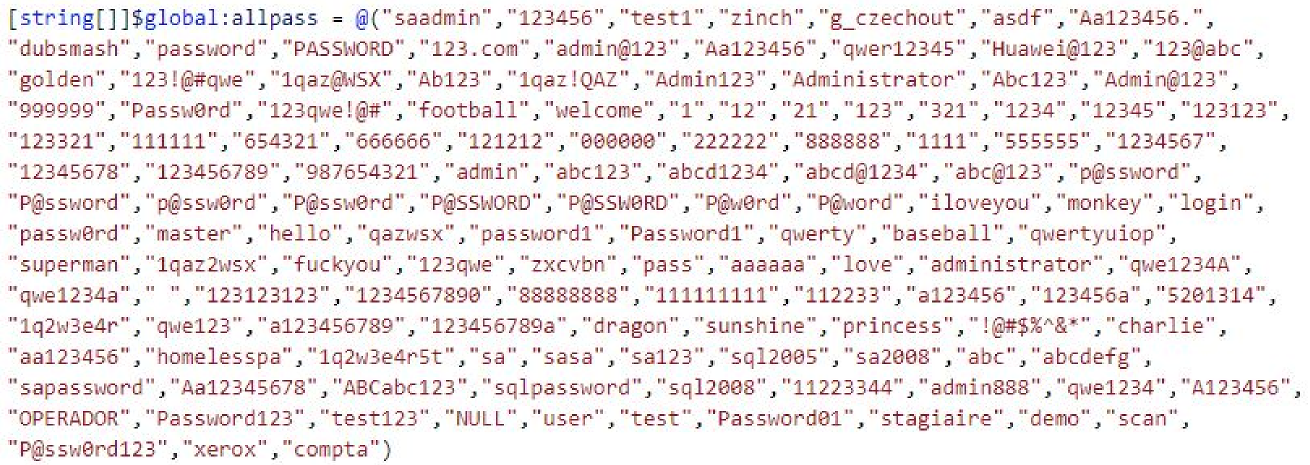
asec.ahnlab.com/en/31811/

February 21, 2022

The ASEC analysis team has recently discovered the distribution of Cobalt Strike targeting MS-SQL servers that are vulnerable to malware attacks.

MS-SQL server is a typical database server of the Windows environment, and it has consistently been a target of attack from the past. Attacks that target MS-SQL servers include attacks to the environment where its vulnerability has not been patched, **brute forcing,** and **dictionary attack** against poorly managed servers.

The attacker or the malware usually scans port 1433 to check for MS-SQL servers open to the public. It then performs brute forcing or dictionary attacks against the admin account, a.k.a. **"sa" account** to attempt logging in. Even if the MS-SQL server is not open to the public, there are types such as Lemon Duck malware that scans port 1433 and spreads for the purpose of lateral movement in the internal network.

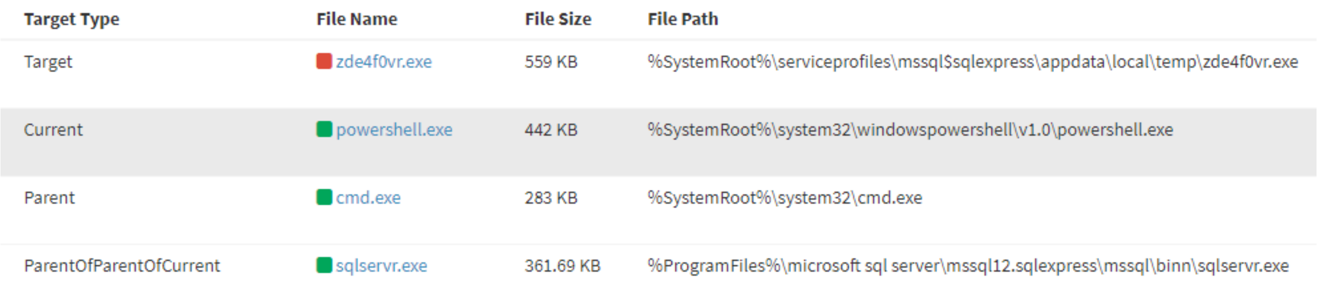


```
[string[]]$global:allpass = @("saadmin","123456","test1","zinch","g_czechout","asdf","Aa123456.",
"dubsmash","password","PASSWORD","123.com","admin@123","Aa123456","qwer12345","Huawei@123","123@abc",
"golden","123!@#qwe","1qaz@WSX","Ab123","1qaz!QAZ","Admin123","Administrator","Abc123","Admin@123",
"999999","Passw0rd","123qwe!@#","football","welcome","1","12","21","123","321","1234","12345","123123",
"123321","111111","654321","666666","121212","000000","222222","888888","1111","555555","1234567",
"12345678","123456789","987654321","admin","abc123","abcd1234","abcd@1234","abc@123","p@ssword",
"P@ssword","p@ssw0rd","P@ssw0rd","P@SSWORD","P@SSW0RD","P@w0rd","P@word","iloveyou","monkey","login",
"passw0rd","master","hello","qazwsx","password1","Password1","qwerty","baseball","qwertyuiop",
"superman","1qaz2wsx","fuckyou","123qwe","zxcvbn","pass","aaaaaa","love","administrator","qwe1234A",
"qwe1234a"," ","123123123","1234567890","88888888","111111111","112233","a123456","123456a","5201314",
"1q2w3e4r","qwe123","a123456789","123456789a","dragon","sunshine","princess","!@#$%^&*","charlie",
"aa123456","homelesspa","1q2w3e4r5t","sa","sasa","sa123","sql2005","sa2008","abc","abcdefg",
"sapassword","Aa12345678","ABCabc123","sqlpassword","sql2008","11223344","admin888","qwe1234","A123456",
"OPERADOR","Password123","test123","NULL","user","test","Password01","stagiaire","demo","scan",
"P@ssw0rd123","xerox","compta")
```

F**igure 1. List of Passwords for Dictionary Attack Used by LemonDuck**

Managing admin account credentials so that they're vulnerable to brute forcing and dictionary attacks as above or failing to change the credentials periodically may make the MS-SQL server the main target of attackers. Other malware besides Lemon Duck that target MS-SQL server includes CoinMiner malware such as Kingminer and Vollgar.

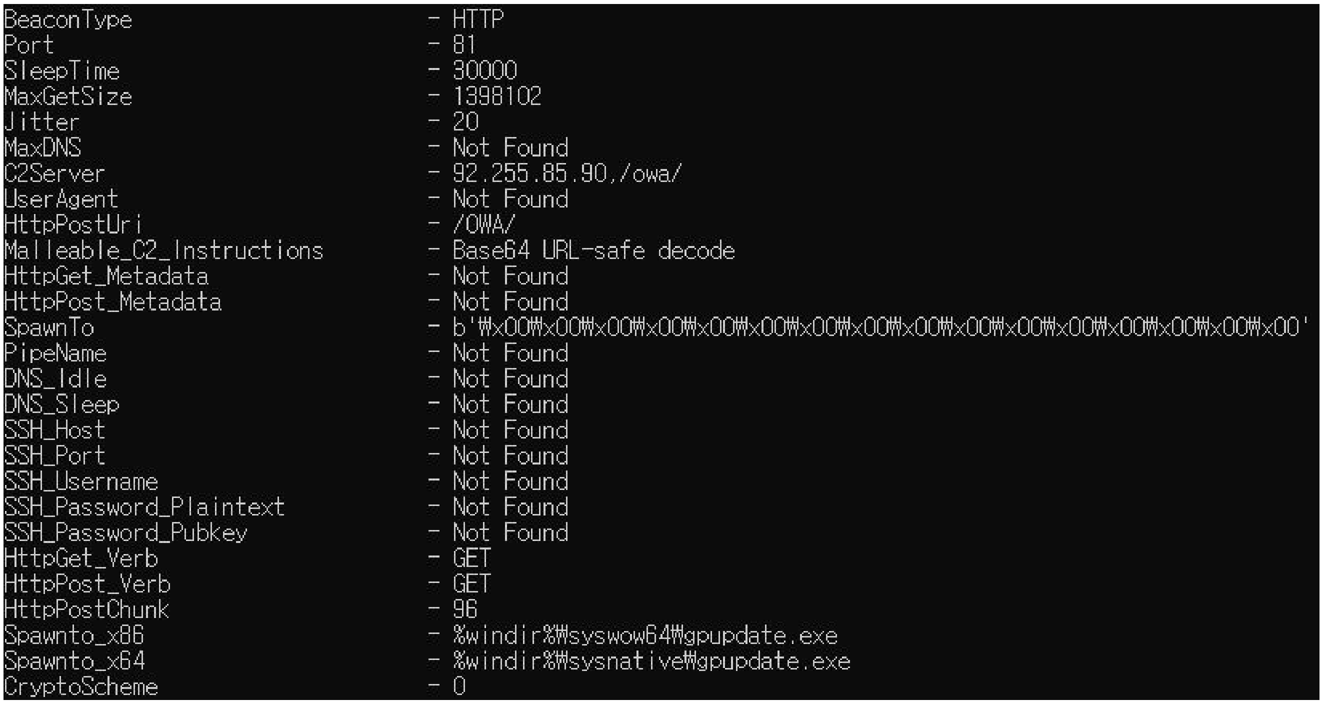
If the attacker succeeds to log in to the admin account through these processes, they use various methods including the xp_cmdshell command to execute the command in the infected system. Cobalt Strike that has recently been discovered was downloaded through cmd.exe and powershell.exe via the MS-SQL process as shown below.



Target Type	File Name	File Size	File Path
Target	🟥 zde4f0vr.exe	559 KB	%SystemRoot%\serviceprofiles\mssql$sqlexpress\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.sqlexpress\mssql\binn\sqlservr.exe

Figure 2. Process Tree

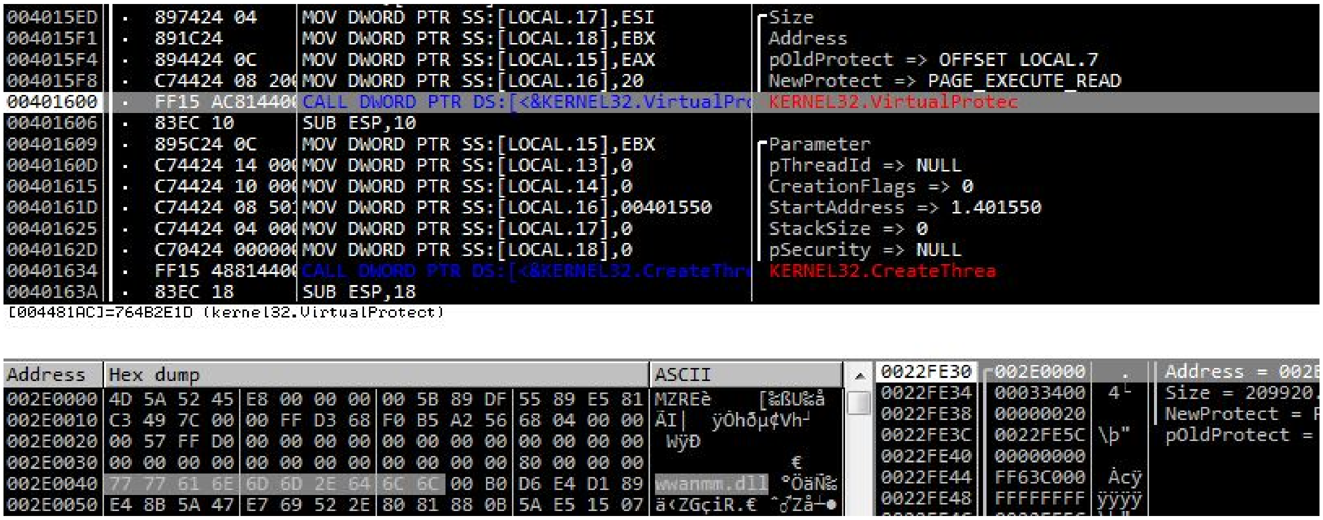
Cobalt Strike is a commercial penetration testing tool, and it is recently being used as a medium to dominate the internal system in the majority of attacks including APT and ransomware. Malware that has recently been discovered is an injector that decodes the encoded Cobalt Strike inside, and executes and injects the normal program MSBuild.exe.



```
BeaconType                    - HTTP
Port                          - 81
SleepTime                     - 30000
MaxGetSize                    - 1398102
Jitter                        - 20
MaxDNS                        - Not Found
C2Server                      - 92.255.85.90,/owa/
UserAgent                     - Not Found
HttpPostUri                   - /OWA/
Malleable_C2_Instructions     - Base64 URL-safe decode
HttpGet_Metadata              - Not Found
HttpPost_Metadata             - Not Found
SpawnTo                       - b'₩x00₩x00₩x00₩x00₩x00₩x00₩x00₩x00₩x00₩x00₩x00₩x00₩x00₩x00₩x00₩x00'
PipeName                      - Not Found
DNS_Idle                      - Not Found
DNS_Sleep                     - Not Found
SSH_Host                      - Not Found
SSH_Port                      - Not Found
SSH_Username                  - Not Found
SSH_Password_Plaintext        - Not Found
SSH_Password_Pubkey           - Not Found
HttpGet_Verb                  - GET
HttpPost_Verb                 - GET
HttpPostChunk                 - 96
Spawnto_x86                   - %windir%₩syswow64₩gpupdate.exe
Spawnto_x64                   - %windir%₩sysnative₩gpupdate.exe
CryptoScheme                  - 0
```

Figure 3. Cobalt Strike settings data

Cobalt Strike that is executed in MSBuild.exe has an additional settings option to bypass detection of security products, where it loads the normal dll wwanmm.dll, then writes and executes a beacon in the memory area of the dll. 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.



```
004015ED  .  897424 04      MOV DWORD PTR SS:[LOCAL.17],ESI           ┌Size
004015F1  .  891C24         MOV DWORD PTR SS:[LOCAL.18],EBX           │Address
004015F4  .  894424 0C      MOV DWORD PTR SS:[LOCAL.15],EAX           │pOldProtect => OFFSET LOCAL.7
004015F8  .  C74424 08 20(  MOV DWORD PTR SS:[LOCAL.16],20            │NewProtect => PAGE_EXECUTE_READ
00401600  .  FF15 AC81440(  CALL DWORD PTR DS:[<&KERNEL32.VirtualPr(  KERNEL32.VirtualProtec
00401606  .  83EC 10        SUB ESP,10
00401609  .  895C24 0C      MOV DWORD PTR SS:[LOCAL.15],EBX           ┌Parameter
0040160D  .  C74424 14 00(  MOV DWORD PTR SS:[LOCAL.13],0             │pThreadId => NULL
00401615  .  C74424 10 00(  MOV DWORD PTR SS:[LOCAL.14],0             │CreationFlags => 0
0040161D  .  C74424 08 50:  MOV DWORD PTR SS:[LOCAL.16],00401550      │StartAddress => 1.401550
00401625  .  C74424 04 00(  MOV DWORD PTR SS:[LOCAL.17],0             │StackSize => 0
0040162D  .  C70424 00000(  MOV DWORD PTR SS:[LOCAL.18],0             │pSecurity => NULL
00401634  .  FF15 48814400  CALL DWORD PTR DS:[<&KERNEL32.CreateThr(  KERNEL32.CreateThrea
0040163A  .  83EC 18        SUB ESP,18
[004481AC]=764B2E1D (kernel32.VirtualProtect)
```

```
Address   Hex dump                                         ASCII              0022FE30  ┌002E0000  .     Address = 002E
002E0000  4D 5A 52 45|E8 00 00 00|00 5B 89 DF|55 89 E5 81  MZREè    [‰ßU‰å    0022FE34  │00033400  4┘    │Size = 209920.
002E0010  C3 49 7C 00|00 FF D3 68|F0 B5 A2 56|68 04 00 00  ÃI|  ÿÓhðµ¢Vh┘     0022FE38  │00000020        │NewProtect = P
002E0020  00 57 FF D0|00 00 00 00|00 00 00 00|00 00 00 00   WÿÐ               0022FE3C  │0022FE5C  \þ"   pOldProtect =
002E0030  00 00 00 00|00 00 00 00|00 00 00 00|80 00 00 00              €      0022FE40  00000000
002E0040  77 77 61 6E|6D 6D 2E 64|6C 6C 00 B0|D6 E4 D1 89  wwanmm.dll °ÖäÑ‰   0022FE44  FF63C000  Àcÿ
002E0050  E4 8B 5A 47|E7 69 52 2E|80 81 88 0B|5A E5 15 07  ä‹ZGçiR.€ ˆ♂Zå┴●   0022FE48  FFFFFFFF  ÿÿÿÿ
```

Figure 4. Shellcode and strings used for wwanmm.dll

Although it is not certain in which method the attacker dominated MS-SQL and installed the malware, as the detection logs of Vollgar malware that was previously mentioned were discovered, it can be assumed that the targeted system had inappropriately managed the account credentials.

AhnLab's ASD infrastructure shows numerous logs of Cobalt Strike over the past month. Seeing that the download URLs and the C&C server URL are similar, it appears that most of the attacks were by the same attacker. IOC of Cobalt Strike over the month is shown in the list below.

AhnLab products are equipped with process memory-based detection method and behavior-based detection feature that can counter the beacon backdoor which is used from the Cobalt Strike's initial invasion stage to spread internally.

[File Detection]
– Trojan/Win.FDFM.C4959286 (2022.02.09.00)
– Trojan/Win.Injector.C4952559 (2022.02.04.02)
– Trojan/Win.AgentTesla.C4950264 (2022.02.04.00)
– Infostealer/Win.AgentTesla.R470158 (2022.02.03.02)
– Trojan/Win.Generic.C4946561 (2022.02.01.01)
– Trojan/Win.Agent.C4897376 (2022.01.05.02)
– Trojan/Win32.CobaltStrike.R329694 (2020.11.26.06)

[Behavior Detection]
– Malware/MDP.Download.M1197

[IOC]
MD5
Cobalt Strike (Stageless)
– ae7026b787b21d06cc1660e4c1e9e423
– 571b8c951febb5c24b09e1bc944cdf5f
– e9c6c2b94fc83f24effc76bf84274039
– 828354049be45356f37b34cc5754fcaa
– 894eaa0bfcfcdb1922be075515c703a3
– 4dd257d56397ec76932c7dbbc1961317
– 450f7a402cff2d892a7a8c626cef44c6

CobaltStrike (Stager)
– 2c373c58caaaca0708fdb6e2b477feb2
– bb7adc89759c478fb88a3833f52f07cf

C&C
– hxxp://92.255.85[.]83:7905/push
– hxxp://92.255.85[.]83:9315/en_US/all.js
– hxxp://92.255.85[.]86:80/owa/
– hxxp://92.255.85[.]90:81/owa/
– hxxp://92.255.85[.]90:82/owa/
– hxxp://92.255.85[.]92:8898/dot.gif

– hxxp://92.255.85[.]93:18092/match
– hxxp://92.255.85[.]93:12031/j.ad
– hxxp://92.255.85[.]94:83/ga.js

Beacon Download URL
– hxxp://92.255.85[.]93:18092/jRQO
– hxxp://92.255.85[.]93:12031/CbCt

Download URL
– hxxp://45.64.112[.]51/dol.exe
– hxxp://45.64.112[.]51/mr_robot.exe
– hxxp://45.64.112[.]51/lion.exe
– hxxp://81.68.76[.]46/kk.exe
– hxxp://81.68.76[.]46/uc.exe
– hxxp://103.243.26[.]225/acrobat.exe
– hxxp://103.243.26[.]225/beacon.exe
– hxxp://144.48.240[.]69/dola.exe
– hxxp://144.48.240[.]85/core.exe

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:BruteForcing, Cobalt Strike, CobaltStrike, Database, Dictionary Attack, MS-SQL, MSSQL