

Sliver C2 Being Distributed Through Korean Program Development Company

ASEC asec.ahnlab.com/en/55652/

By Sanseo

August 1, 2023

In the past, AhnLab Security Emergency response Center (ASEC) had shared the **“SparkRAT Being Distributed Within a Korean VPN Installer” [1]** case post and the **“Analysis of Attack Cases: From Korean VPN Installations to MeshAgent Infections” [2]** case post which covered the SparkRAT malware being distributed through a Korean VPN service provider’s installer.

ASEC has recently identified similar malware strains being distributed while being disguised as setup files for Korean VPN service providers and marketing program producers. Unlike the past cases where SparkRAT was used, Sliver C2 was used in the recent attacks [3] and techniques to evade detection were employed.

As of now, most websites of the affected companies provide normal setup files available for download. It is therefore uncertain whether the malware strain has been distributed as installers in official websites before being rectified like in past cases, or if there are other distribution paths. However, an investigation of the malware strains involved revealed that they were all related to the software provided by the same program development company. Most malware samples had certificates disguised as valid ones from this company. There were also multiple samples signed with valid certificates.

Malicious installers are still uploaded on the software download website provided by this company, so users may be unaware of this fact and install the file in question. In light of these facts, it seems that the threat actor attacked the development company and distributed installers with malware strains. Such types of attacks are steadily being launched from the first half of 2023.

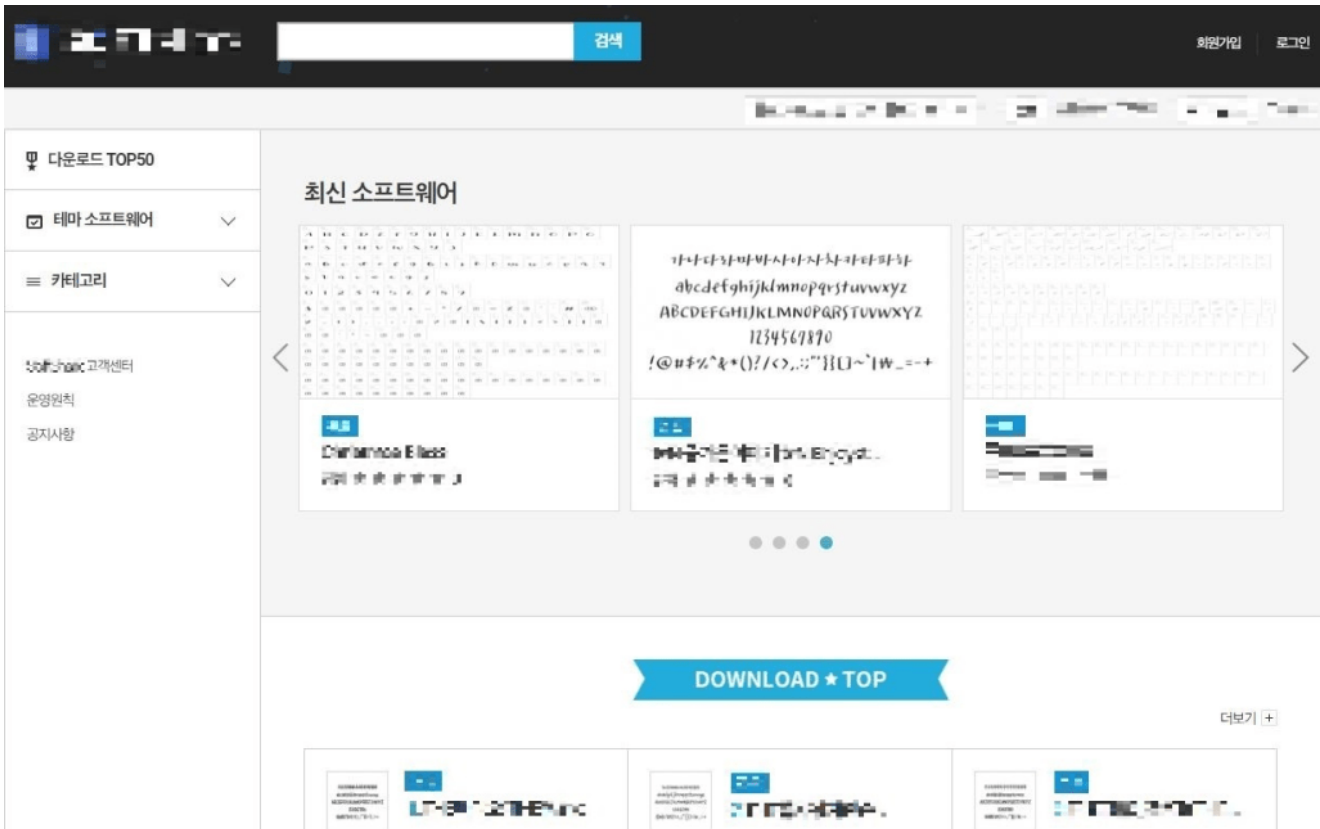


Figure 1. Software download website of the company used for malware distribution

1. Past Attack Cases

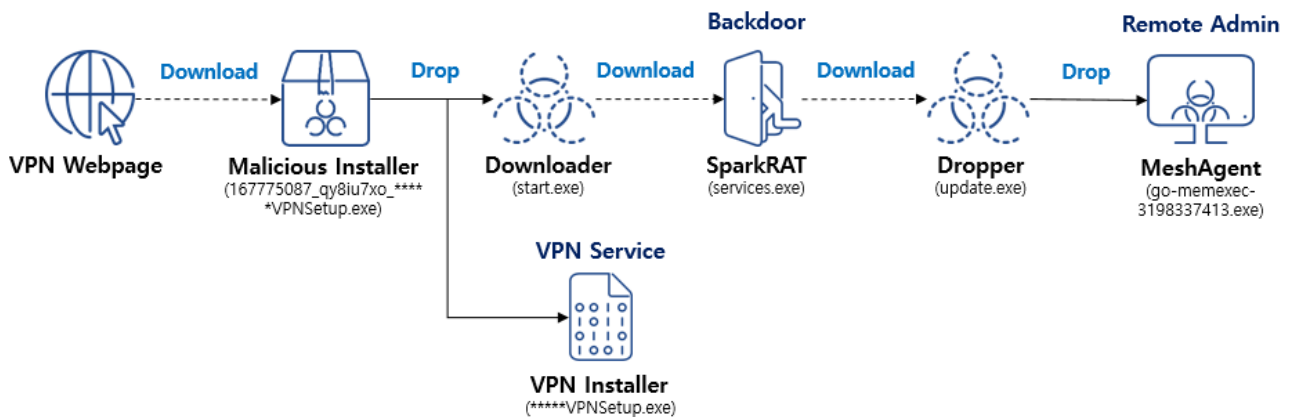


Figure 2. Past attack flow

Examining past cases show that a malicious setup file is uploaded to the website of a Korean VPN service provider instead of the normal installer. Accordingly, users may mistakenly think that they have executed a normal setup file, but a malware strain is also installed in the system and executed. The malicious installer in the initial attack was developed in .NET which simply created and executed the normal installer and the SparkRAT malware. SparkRAT is an open-source RAT type malware developed in Go lang. It provides features to control the infected system such as executing commands, exfiltrating information, and controlling processes and files.

Malware files continued to be uploaded to the website of this VPN company afterward. To prevent the malware from being detected, the tactic changed from directly dropping the malware strain to installing SparkRAT through a downloader. After SparkRAT (backdoor) was installed in the infected system, MeshAgent from MeshCentral was additionally installed to be used for remote desktop features.

2. Analysis of the Malware Currently Used in Attacks

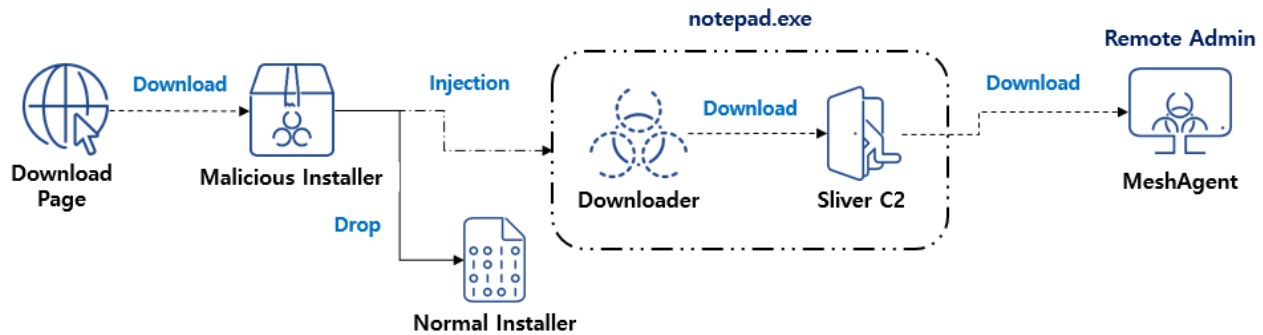


Figure 3. Current attack flow

Unlike the malicious installers of the past which were droppers that simultaneously installed the malware strain, the currently used type is both a downloader and injector type malware. All malware strains used in the attacks including the installer were developed in Go lang and were all obfuscated. SparkRAT, which was used by the threat actor in the past, is also a backdoor developed in Go lang. Dropper and downloader type malware types developed in Go lang were also used in subsequent attack stages. Sliver C2 which is being detected recently is also developed in Go lang. As such, it appears that the threat actor prefers the Go language for development.

```

00806C40 47 76 6F 38 2E 51 48 58 4C 72 48 7A 4E 51 50 6A Gvo8.QHXLrHzNQPj
00806C50 45 00 6D 62 38 32 52 63 62 2E 4D 4F 78 68 67 6B E.mb82Rcb.MOxhgk
00806C60 34 39 6B 6A 74 00 6E 36 35 36 35 4A 2E 58 61 7A 49kjt.n6565J.Xaz
00806C70 31 48 6C 6D 5F 4B 57 34 5B 2E 2E 2E 5D 00 6D 62 1Hlm_KW4[...].mb
00806C80 38 32 52 63 62 2E 28 2A 50 72 6F 63 65 73 73 29 82Rcb. (*Process)
00806C90 2E 4E 61 6D 65 00 6E 36 35 36 35 4A 2E 4C 70 38 .Name.n6565J.Lp8
00806CA0 69 54 67 41 5B 2E 2E 2E 5D 00 6D 61 69 6E 2E 43 iTgA[...].main.C
00806CB0 59 47 49 66 71 57 73 35 34 00 4B 4D 4D 48 79 4A YGIIfqWs54.KMMHyJ
00806CC0 75 7A 74 2E 45 72 53 77 4A 4D 00 6D 61 69 6E 2E uzt.ErSwJM.main.
00806CD0 28 2A 7A 55 39 4C 49 59 79 50 46 29 2E 41 66 74 (*zU9LIYyPF).Aft
00806CE0 65 72 00 75 73 75 31 49 49 2E 58 6F 76 74 57 4D er.usulII.XovtWM
00806CF0 00 5F 53 6D 4B 74 6F 69 68 34 49 79 2E 44 42 68 ._SmKtoih4Iy.DBh
00806D00 59 5A 66 36 30 7A 00 5F 53 6D 4B 74 6F 69 68 34 YZf60z._SmKtoih4
00806D10 49 79 2E 28 2A 49 65 56 30 58 7A 29 2E 4D 75 73 Iy. (*IeV0Xz).Mus
00806D20 74 46 69 6E 64 50 72 6F 63 00 00 00 00 00 00 tFindProc.....

```

Figure

4. Obfuscated Go binary

The malicious installer connects to the C&C server and downloads encrypted configuration data. When conditions match, Sliver C2 is downloaded. Notepad (notepad.exe), a normal program, is executed before Sliver C2 is injected into this. Because these processes are

carried out simultaneously with the task of creating and executing the normal setup file, users may think the file is normal.

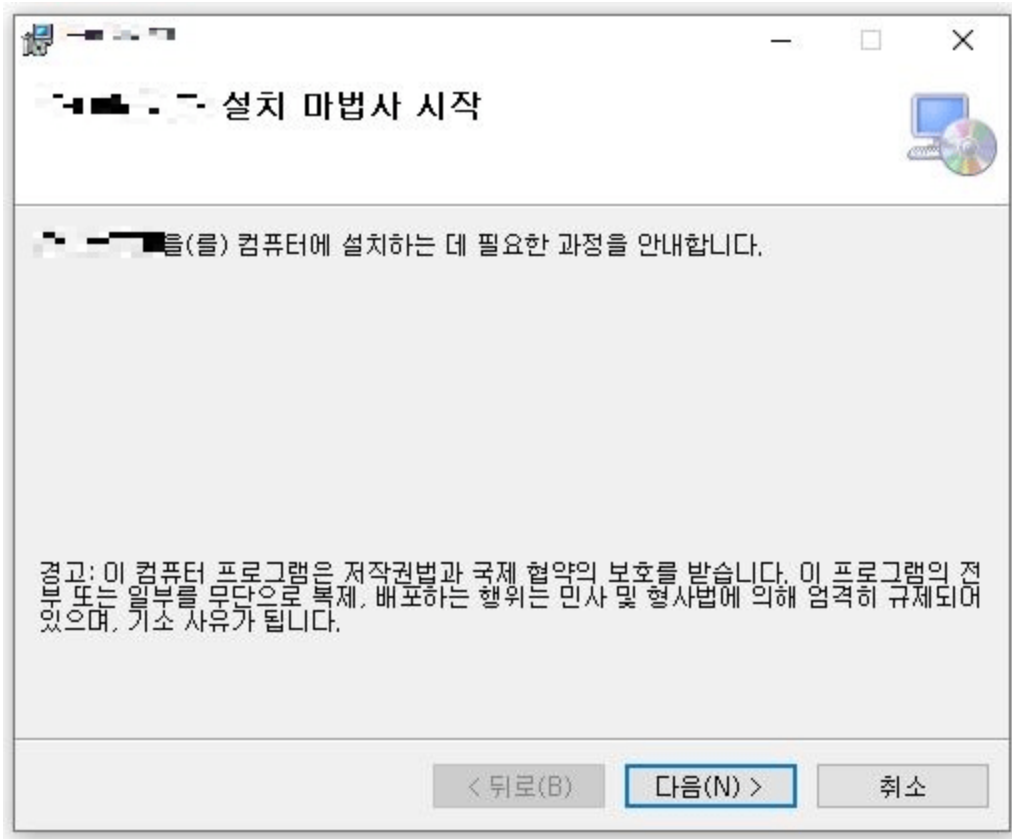


Figure 5. Normal

installer created by the malicious file

The malicious installer also includes an anti-sandbox feature. The list of currently running processes is looked up and injection is only performed when a certain process is running. The list of processes to check for is encrypted at the following URL. The malware strain downloads this and decrypts it to use it for checking the conditions.

Configuration download URL: [hxxps://status.devq\[.\]workers.dev/](https://status.devq[.]workers.dev/)

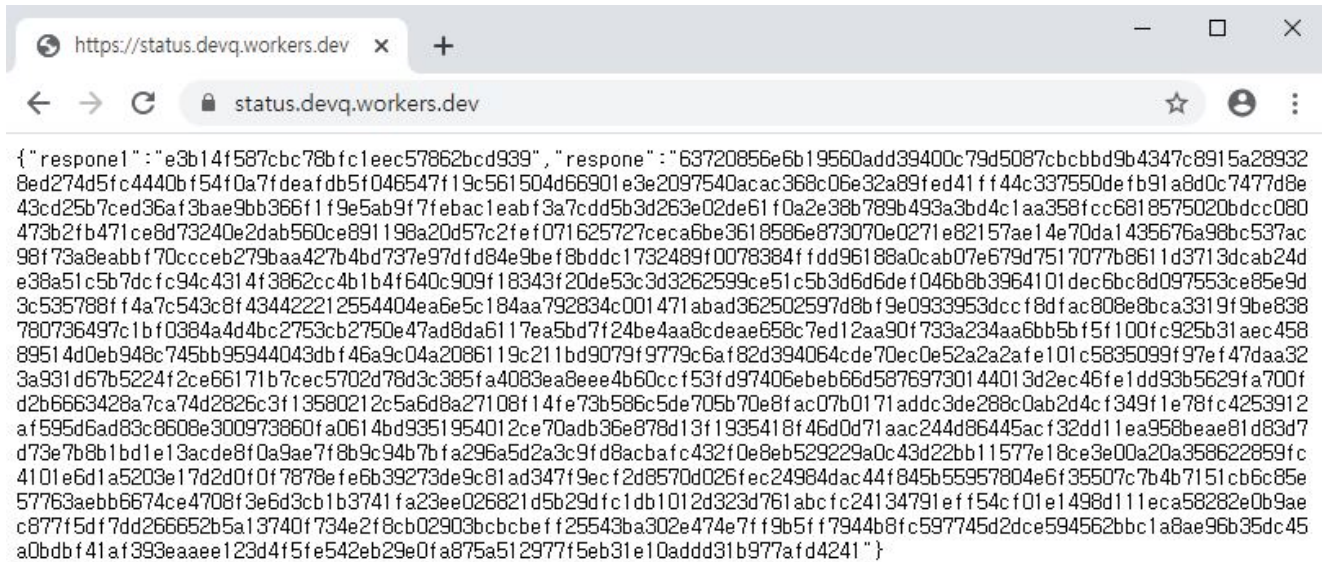


Figure 6. Encrypted condition

주소	Hex	ASCII
000000C0001BE960	44 69 73 63 6F 72 64 2E 65 78 65 00 00 00 00 00	Discord.exe.....
000000C0001BE970	64 69 73 63 6F 72 64 2E 65 78 65 00 00 00 00 00	discord.exe.....
000000C0001BE980	4E 65 78 6F 6E 50 6C 75 67 2E 65 78 65 00 00 00	NexonPlug.exe...
000000C0001BE990	6E 65 78 6F 6E 70 6C 75 67 2E 65 78 65 00 00 00	nexonplug.exe...
000000C0001BE9A0	4F 50 2E 47 47 2E 65 78 65 00 00 00 00 00 00 00	OP.GG.exe.....
000000C0001BE9B0	6F 70 2E 67 67 2E 65 78 65 00 00 00 00 00 00 00	op.gg.exe.....
000000C0001BE9C0	71 71 2E 65 78 65 00 00 6C 69 6E 65 2E 65 78 65	qq.exe..line.exe
000000C0001BE9D0	51 51 47 75 69 6C 64 2E 65 78 65 00 00 00 00 00	QQGuild.exe.....
000000C0001BE9E0	71 71 67 75 69 6C 64 2E 65 78 65 00 00 00 00 00	qqguild.exe.....
000000C0001BE9F0	51 51 50 72 6F 74 65 63 74 2E 65 78 65 00 00 00	QQProtect.exe...
000000C0001BEA00	71 71 70 72 6F 74 65 63 74 2E 65 78 65 00 00 00	qqprotect.exe...
000000C0001BEA10	54 72 61 66 66 69 63 50 72 6F 2E 65 78 65 00 00	TrafficPro.exe..
000000C0001BEA20	74 72 61 66 66 69 63 70 72 6F 2E 65 78 65 00 00	trafficpro.exe..
000000C0001BEA30	57 65 43 68 61 74 41 70 70 45 78 2E 65 78 65 00	WeChatAppEx.exe.
000000C0001BEA40	77 65 63 68 61 74 61 70 70 65 78 2E 65 78 65 00	wechatappex.exe.
000000C0001BEA50	57 65 43 68 61 74 50 6C 61 79 65 72 2E 65 78 65	WeChatPlayer.exe
000000C0001BEA60	77 65 63 68 61 74 70 6C 61 79 65 72 2E 65 78 65	wechatplayer.exe
000000C0001BEA70	61 6E 79 64 65 73 68 2E 65 78 65 00 00 00 00 00	anydesk.exe.....
000000C0001BEA80	68 61 68 61 6F 74 61 6C 68 2E 65 78 65 00 00 00	kakaotalk.exe...
000000C0001BEA90	6C 64 70 6C 61 79 65 72 2E 65 78 65 00 00 00 00	ldplayer.exe.....
000000C0001BEAA0	6C 6F 67 69 62 6F 6C 74 2E 65 78 65 00 00 00 00	logibolt.exe....
000000C0001BEAB0	6F 62 73 36 34 2E 65 78 65 00 00 00 00 00 00 00	obs64.exe.....
000000C0001BEAC0	73 68 79 70 65 2E 65 78 65 00 00 00 00 00 00 00	skype.exe.....
000000C0001BEAD0	74 65 6C 65 67 72 61 6D 2E 65 78 65 00 00 00 00	telegram.exe....
000000C0001BEAE0	77 65 63 68 61 74 2E 65 78 65 00 00 00 00 00 00	wechat.exe.....
000000C0001BEAF0	77 68 61 6C 65 2E 65 78 65 00 00 00 00 00 00 00	whale.exe.....

Figure 7.

Decrypted conditional string

Process Name

Discord.exe, discord.exe, NexonPlug.exe, nexonplug.exe, OP.GG.exe, op.gg.exe, qq.exe, line.exe, QQGuild.exe, qqguild.exe, QQProtect.exe, qqprotect.exe, TrafficPro.exe, trafficpro.exe, WeChatAppEx.exe, wechatappex.exe, WeChatPlayer.exe, wechatplayer.exe, anydesk.exe, kakaotalk.exe, ldplayer.exe, logibolt.exe, obs64.exe, skype.exe, telegram.exe, wechat.exe, whale.exe

Table 1. List of processes used as conditions

These strings are the names of programs that are likely to be installed in ordinary user PCs. Because VPN services are mainly used by users to have unrestricted Internet access in China, many Chinese messenger names are also included. When conditions match, the malware downloads an encrypted Sliver C2 from an external source and decrypts it. Then it launches Notepad, a normal program, and injects Sliver C2 into this process.

Sliver C2 Download URL: hxxps://config.v6[.]army/sans.woff2

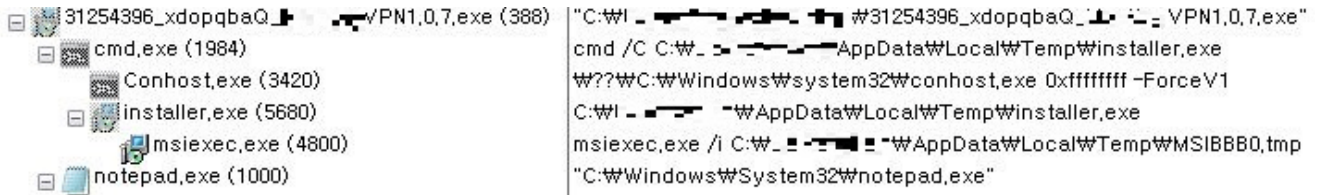


Figure 8. Process tree

Sliver C2 is an open-source penetration testing tool published on GitHub. Penetration testing tools are used for the purpose of checking the security vulnerabilities within the network and systems of companies and institutes. They can potentially be used for malicious purposes if placed in the hands of threat actors as they generally provide various features for each penetration testing stage. Major commercial penetration testing tools include Cobalt Strike and the open-source Metasploit. Recently, there have been multiple identified cases where Sliver C2 was used.

Instead of SparkRAT which was previously used, the threat actor employed Sliver C2 in attacks. probably because Sliver C2 supports more features than SparkRAT, a simple backdoor. Sliver C2 supports most features supported by the ordinary backdoor and RAT malware types such as process and file-related tasks, executing commands, uploading/downloading files, and capturing screenshots. It also provides various features needed for gaining control over internal networks such as privilege escalation, process memory dump, and lateral movement.

- **Sliver C2 Name:** PRETTY_BLADDER
- **Sliver C2 C&C URL:** hxxps://panda.sect[.]kr

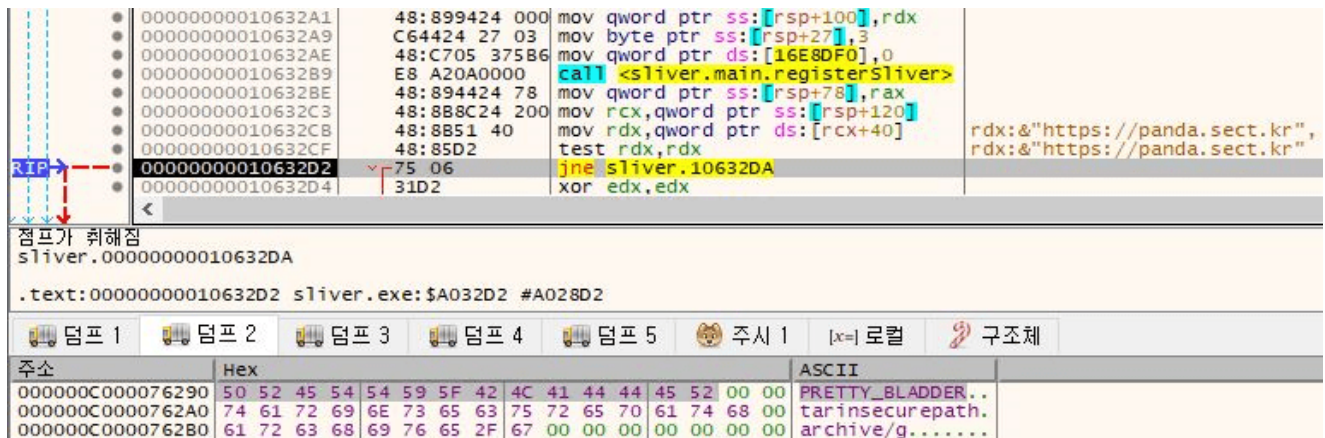





Figure 9. Sliver C2 settings data

3. Analysis of Additional Malware

While the malware strain used in the attacks was changed from SparkRAT to Sliver C2, the threat actor ultimately used the same MeshAgent in the end. Using Sliver C2 injected into notepad, the threat actor installed MeshAgent under the “%PROGRAMFILES%\Microsofts\Microsofts\preMicrosoft.exe” path.

Target Type	File Name	File Size	File Path ⓘ
Current	 premicrosoft.exe	3.33 MB	%ProgramFiles%\microsofts\microsofts\premicrosoft.exe
Parent	 cmd.exe	283 KB	%SystemRoot%\system32\cmd.exe
DropperOfCurrent	 notepad.exe	196.5 KB	%SystemRoot%\system32\notepad.exe







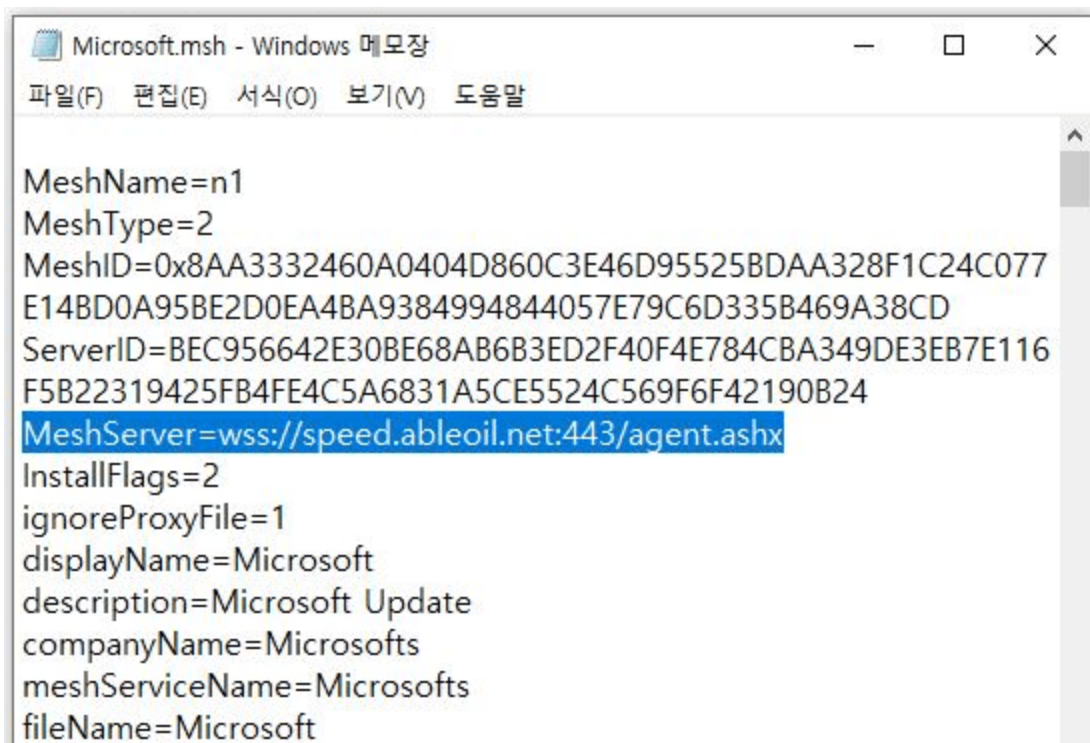
Process	Module	Target	Behavior	Data
 premicrosoft.exe	N/A	N/A	Registered DLL/driver as service	system\controlset001\services\microsofts
 notepad.exe	N/A	N/A	Creates executable file	 premicrosoft.exe
 cmd.exe	N/A	 premicrosoft.exe	Creates process	N/A
 services.exe	N/A	N/A	Registered DLL/driver as service	system\controlset001\services\microsofts

Figure 10. MeshAgent installation log

Provided by MeshCentral, MeshAgent allows various system control commands such as command execution and file download, as well as remote desktop features such as VNC and RDP. Ordinary users may use these services to remotely manage the system, but the features can also be used for malicious purposes. The threat actor in this case probably used MeshAgent for remotely controlling the infected system.

MeshAgent C&C URL: speed.ableoil[.]net:443



```

Microsoft.msh - Windows 메모장
파일(F) 편집(E) 서식(O) 보기(V) 도움말

MeshName=n1
MeshType=2
MeshID=0x8AA3332460A0404D860C3E46D95525BDAA328F1C24C077
E14BD0A95BE2D0EA4BA9384994844057E79C6D335B469A38CD
ServerID=BEC956642E30BE68AB6B3ED2F40F4E784CBA349DE3EB7E116
F5B22319425FB4FE4C5A6831A5CE5524C569F6F42190B24
MeshServer=wss://speed.ableoil.net:443/agent.ashx
InstallFlags=2
ignoreProxyFile=1
displayName=Microsoft
description=Microsoft Update
companyName=Microsofts
meshServiceName=Microsofts
fileName=Microsoft

```

Figure 11.

MeshAgent used for the attack

The threat actor installed Sliver C2 and MeshAgent to seize control over the infected system. Afterward, the attacker was able to perform various malicious behaviors such as exfiltrating user information saved in the PC or installing additional malware strains. According to the AhnLab Smart Defense (ASD) logs, the threat actor used MeshAgent to install an additional malware strain titled “m.exe”. The file “m.exe” is a malware type that captures webcam feeds and is also available publicly on GitHub. Like other malware strains, it is developed in Go lang. Using this malware type, the threat actor can capture images of the user in systems with webcam access.

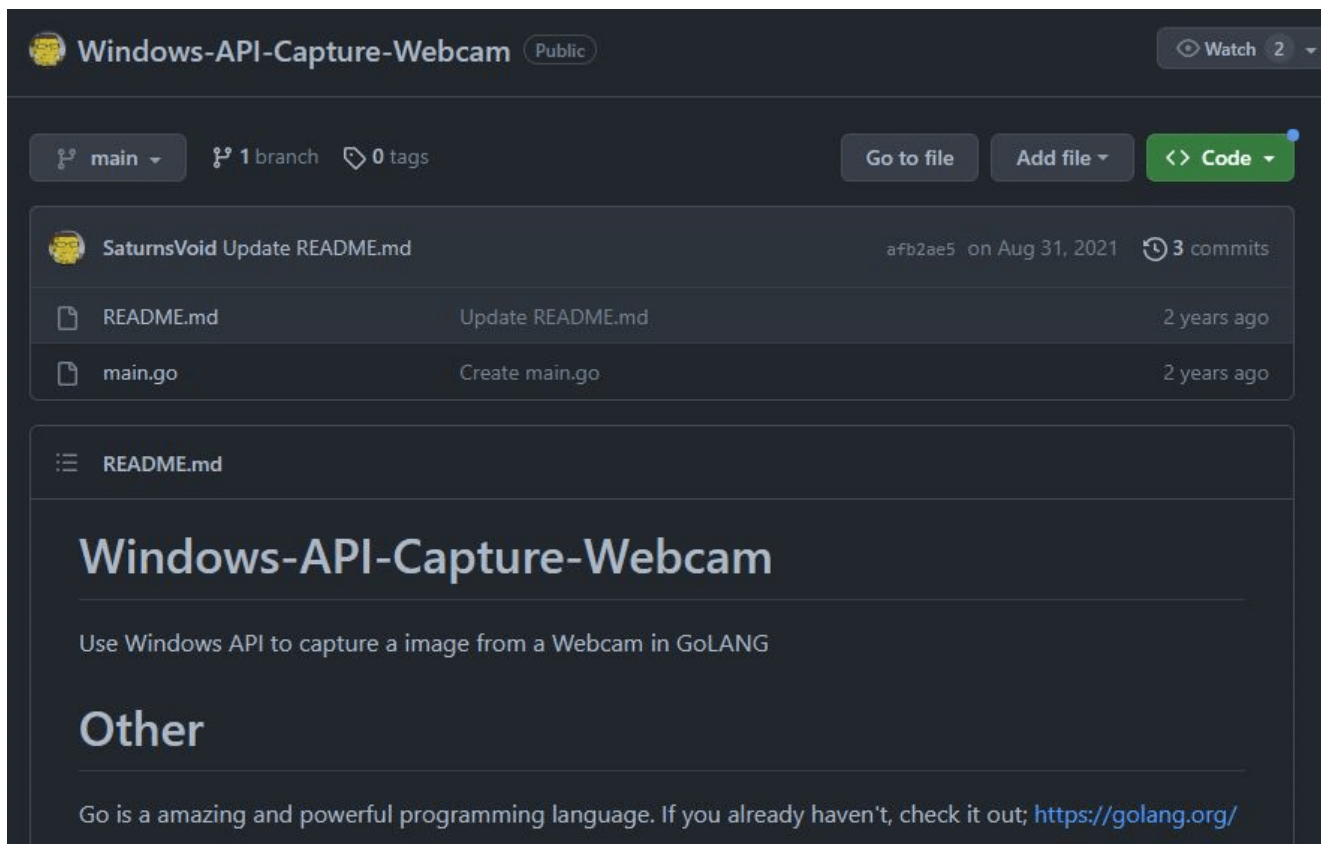


Figure 12. Open-source webcam capturing malware used by the threat actor

4. Installers Used in Attacks

Currently, most VPN and marketing program provider websites hold only normal setup files, but there are companies who have not yet fully taken appropriate measures. In the case of a particular VPN company, a normal setup file is downloaded from the download link on the official website, but the website still contains a malicious installer that can be downloaded.

- [31254396 U8JCSPqf](#) - VPN1.1.0.exe
- [31254396 YVwThDQM](#) - VPN1.0.8.exe
- [31254396 hzcZVMfW](#) - VPN1.1.1.exe
- [31254396 tR62V4Nn](#) - VPN1.0.8.exe
- [31254396 tv2wflgz](#) - VPN1.0.8.zip
- [31254396 xdopqbaQ](#) - VPN1.0.7.exe
- [31254396 zUVwpB05](#) - VPN1.0.7.zip
- [32254396 xdopqbaQ](#) - VPN1.0.7.exe
- [3555450761 DbLgvEqF](#) - VPN1.0.9.exe
- [3555450761 gpmErFPv](#) - VPN1.0.9.zip

Figure 13. Malware uploaded on the

website of a certain VPN company

There are also malicious installers being distributed from the following software download site, which was found to be another website of the same program development company. The files are supposed to be font files, but they are actually malicious installers.

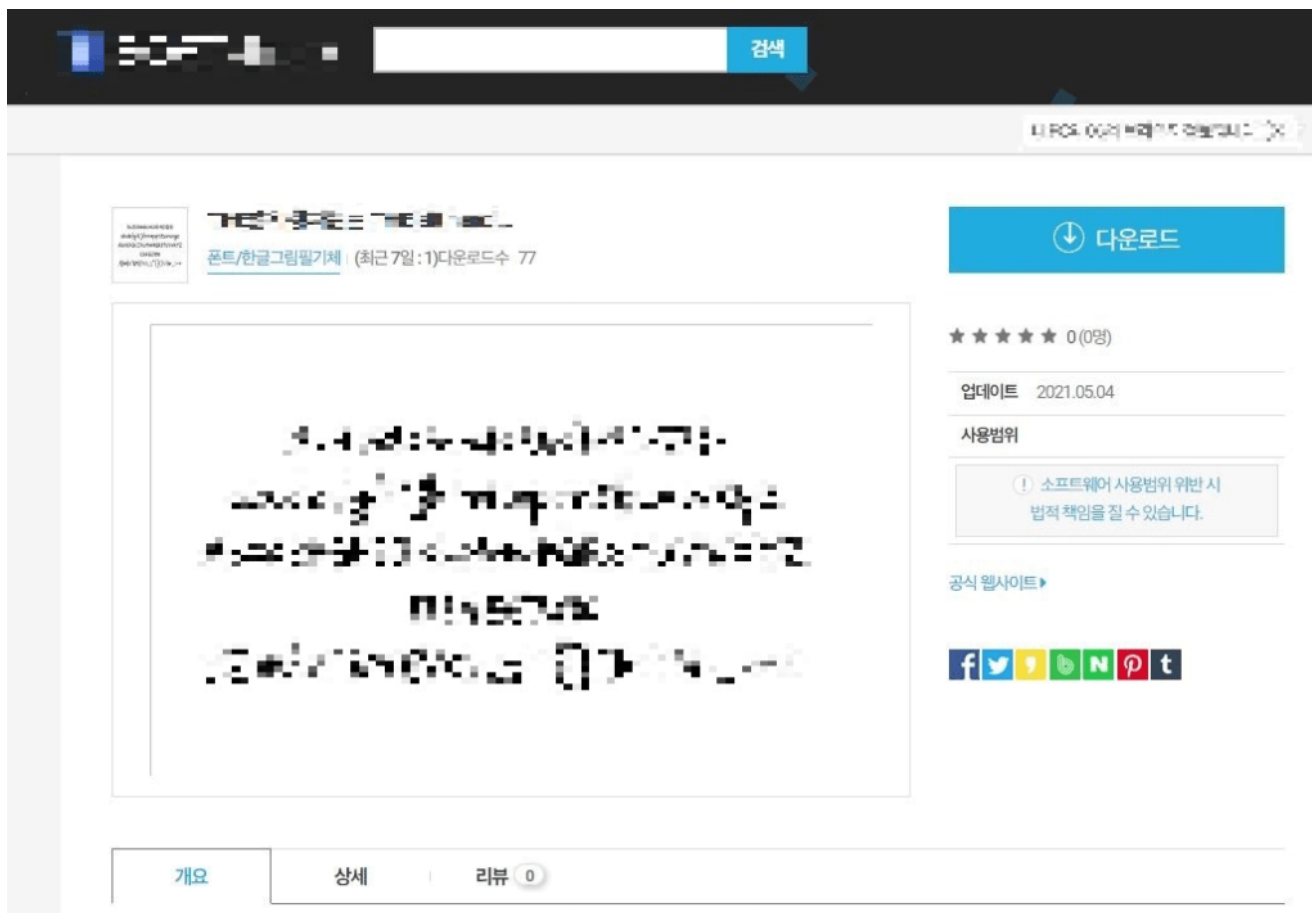


Figure 14. Website still containing downloadable malware strains

The above malware types are all signed with invalid certificates, stolen by the threat actor to disguise the files as installers. However, there are also multiple malware strains signed with a valid certificate from the appropriate program developer. Malware strains with valid signatures vary from malicious setup files disguised as those for various services, VPN execution files, and MeshAgent.

To summarize, while the specific circumstances are yet to be revealed, the threat actor is able to sign malware strains with valid certificates from the corresponding program development company. There are multiple identified malicious setup files disguised as being for various services provided by the said company.

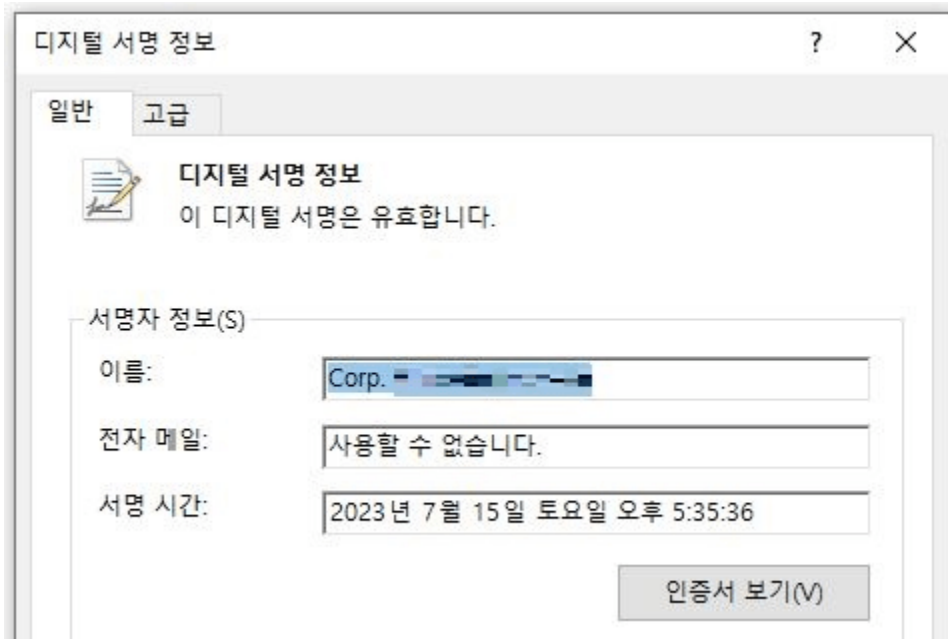


Figure 15. Malware

signed with a valid signature

5. Conclusion

Currently, a malware strain is being distributed through a certain program development company and there are many identified samples that have been signed with a valid certificate from this company. Accordingly, the malware may be distributed from other services provided by this developer. It has been confirmed that malware files are uploaded to the VPN company's download page and the software download website.

The threat actor installed SparkRAT, Sliver C2, and MeshAgent which support features that allow the operator to control infected systems. Accordingly, the threat actor was able to perform various malicious behaviors such as stealing user information saved in the PC and installing additional malware strains.

When users download malicious installers from the website and proceed with the installation, the setup file not only installs malware but also the normal setup file as well, making it difficult to recognize the system has been infected with malware. Users must practice caution and update V3 to the latest version to prevent malware infection in advance.

File Detection

- Trojan/Win.MeshAgent.C5457071 (2023.07.18.03)
- Trojan/Win.MeshAgent.C5459839 (2023.07.24.03)

- Downloader/Win.Agent.C5459845 (2023.07.24.03)
- Downloader/Win.Agent.C5459851 (2023.07.24.03)
- Data/BIN.EncPe (2023.07.25.00)

Behavior Detection

- Persistence/MDP.RunKey.M1038

IOC

MD5

- e84750393483bbb32a46ca5a6a9d253c: Malicious installer
- eefbc5ec539282ad47af52c81979edb3: Malicious installer (31254396_hzczvmfw_....vpn1.1.1.exe)
- 10298c1ddae73915eb904312d2c6007d: Malicious installer (31254396_LO38iuSd_....Setup1.2.1.exe)
- b4481eef767661e9c9524d94d808dcb6: Malicious installer (31254396_a7z34P10_....Install2.1.7.exe)
- 70257b502f6db70e0c75f03e750dca64: Malicious installer (167775112_v17MGr85_167775039_EvimzM59_....VPNSetup1.0.4.4.exe)
- 1906bf1a2c96e49bd8eba29cf430435f: Malicious installer (167774990_A5TinsS6_....VPNInstaller1.0.4_230710.exe)
- 499f0d42d5e7e121d9a751b3aac2e3f8: Malicious installer (31254396_ORZNvfG9_....Fax1.0.0.exe)
- b66f351c35212c7a265272d27aa09656: Malicious VPN program
- ea20d797c0046441c8f8e76be665e882 : Malicious VPN program
- 73f83322fce3ef38b816bef8fa28d37b: Encrypted Sliver C2 (sans.font2)
- 5eb6821057c28fd53b277bc7c6a17465: MeshAgent (preMicrosoft.exe)
- 95dac8965620e69e51a1dbdf7ebbf53a: MeshAgent (Microsoft.exe)
- 23f72ee555afcd235c0c8639f282f3c6: MeshAgent (registrys.exe)
- 27a24461bd082ec60596abbad23e59f2: Webcam capturing malware (m.exe)

Download URLs

- hxxps://status.devq[.]workers.dev : Configuration data
- hxxps://config.v6[.]army/sans.woff2: Encrypted Sliver C2

C&C URLs

- panda.sect[.]kr:443 : Sliver C2
- speed.ableoil[.]net:443 : MeshAgent

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

Categories:[Malware Information](#)

Tagged as:[MeshAgent](#),[Sliver](#)