APT

Lazarus Group Uses the DLL Side-Loading Technique (mi.dll)

Oct 06 2022

While tracking the Lazarus attack group, the ASEC analysis team discovered that the attackers were using the DLL Side-Loading attack technique (T1574.002) by abusing legitimate applications in the initial compromise stage to achieve the next stage of their attack process.

https://attack.mitre.org/techniques/T1574/002/

The DLL Side-Loading attack technique saves a legitimate application and a malicious DLL in the same folder path to enable the malicious DLL to also be executed when the application is run. In other words, it is a malware execution technique that allows the malicious DLL to be executed first by changing its name to the filename of the normal DLL located in a different path that the legitimate program refers to.

The list of legitimate processes abused by the Lazarus group is as follows. wsmprovhost.exe and dfrgui.exe are all normal MS files.

- wsmprovhost.exe (Host process for WinRM plug-ins)
- dfrgui.exe (Microsoft Drive Optimizer)

According to AhnLab's ASD (AhnLab Smart Defense) infrastructure, the attackers used an old version of the Initech process (inisafecrosswebexsvc.exe) through which they distributed the backdoor malware (scskapplink.dll) used for the initial compromise.

rundll32.exe	scskapplink.dll [object Object]	N/A	Creates executable file	Creates executable file	Target wsmprovhost.exe
inisafecrosswebexsvc.exe	N/A	N/A	Creates executable file	Creates executable file	Target scskapplink.dll

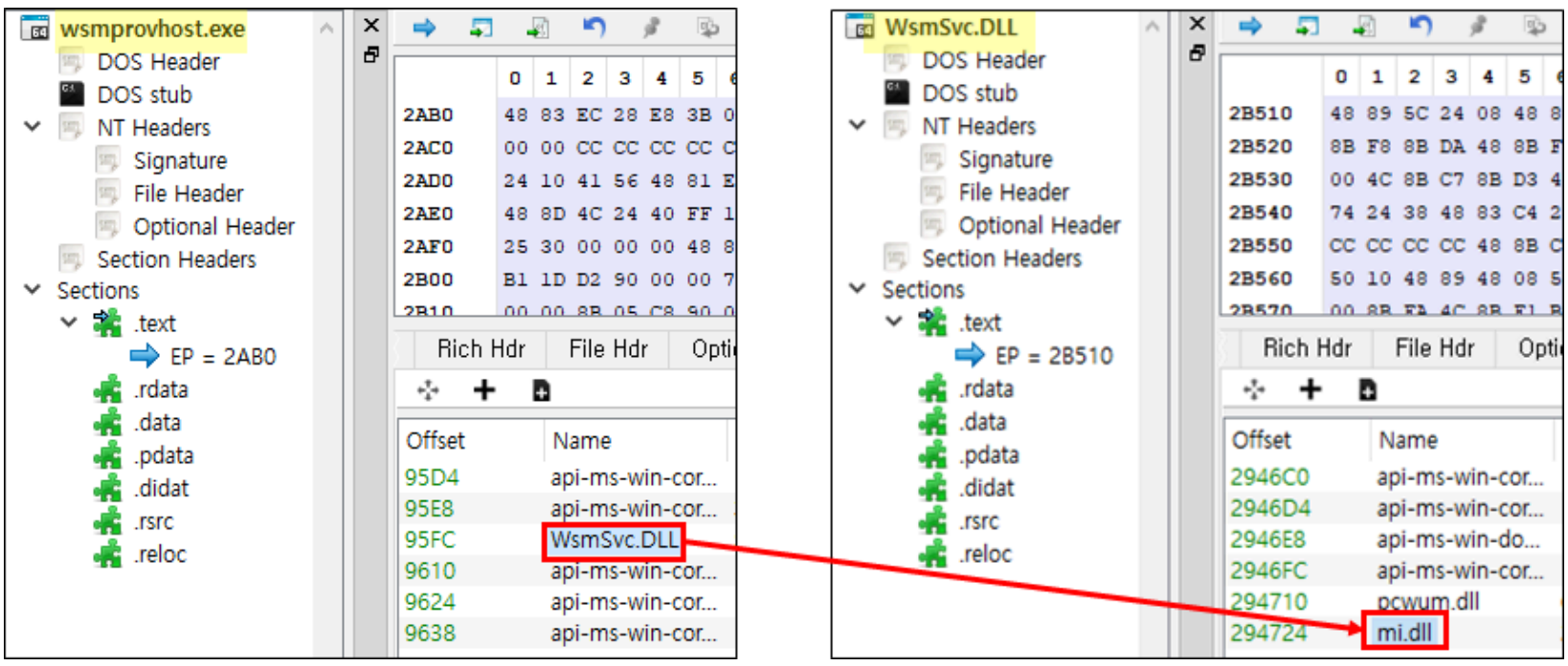
Afterward, it is likely that the executed backdoor malware created wsmprovhost.exe and executed an additional DLL Side-Loading payload. The grounds for the suspected use of the DLL Side-Loading technique lie in the fact that an additional malicious DLL named "mi.dll" was found in the folder path where wsmprovhost.exe was created in the infected PCs. The following is the file path information of mi.dll that was in the same path as wsmprovhost.exe.

- C:\ProgramData\Microsoft\IdentityCRL\mi.dll
- C:\ProgramData\Microsoft\IdentityCRL\wsmprovhost.exe
- C:\ProgramData\USOShared\mi.dll

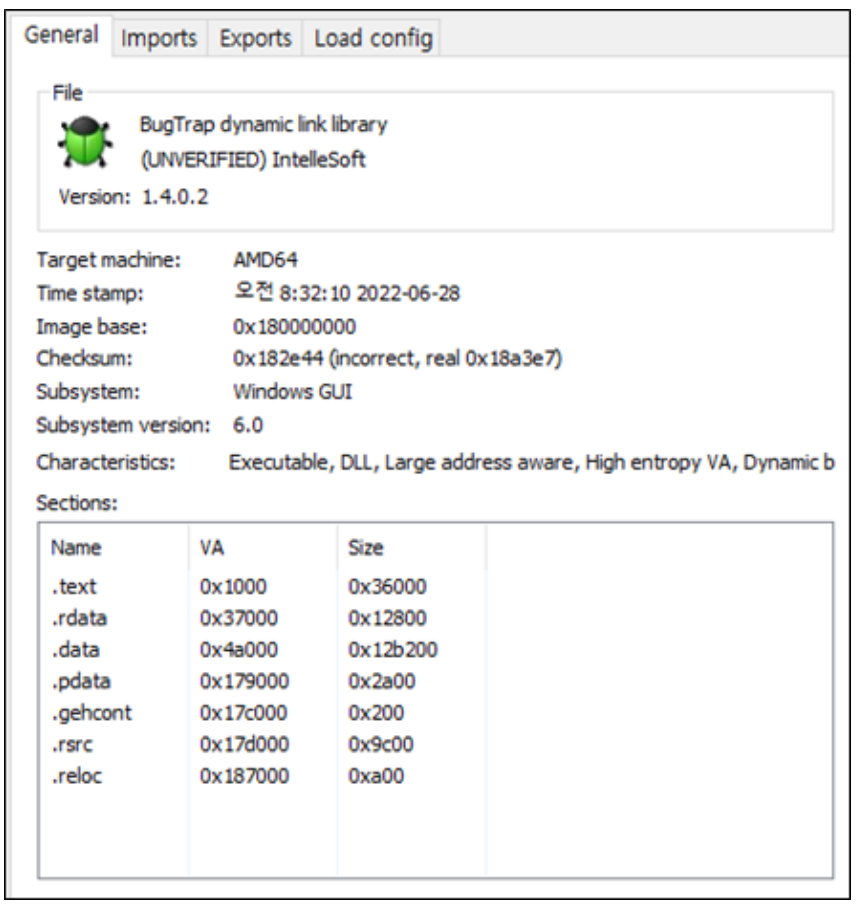
- C:\ProgramData\USOShared\wsmprovhost.exe
- C:\ProgramData\midassoft\mi.dll
- C:\ProgramData\midassoft\wsmprovhost.exe

time	path	rule num
Oct 4, 2022 @ 16:14:33.670	C:\ProgramData\Microsoft\IdentityCRL\mi.dll	5226517
Oct 4, 2022 @ 15:51:29.444	C:\ProgramData\USOShared\mi.dll	5226517
Sep 13, 2022 @ 15:51:25.503	C:\ProgramData\midassoft\mi.dll	5226517

mi.dll is a DLL referenced by wsmprovhost.exe (See Figure 3). Thus, when wsmprovhost.exe is run, mi.dll is loaded in the corresponding process memory.



mi.dll, a normal MS file, exists in the path "c:\windows\system32", but the mi.dll used in this attack was found not in the Windows system path but in another path alongside wsmprovhost.exe. The attackers included the malware in the BugTrap project source code, an open source code on github, to distribute it under the name "mi.dll".



The malicious mi.dll that is executed in the process memory of wsmprovhost.exe includes an additional binary encrypted internally with the AES-128 algorithm, and the moment it is executed, it uses the decryption key transmitted via an argument to decrypt the binary before running an additional malware in the memory.

It has also been identified that the Lazarus group not only executed malware through wsmprovhost.exe but also other normal Windows programs such as dfrgui.exe. Using a DLL that is run in a normal process memory area to perform malicious acts is deemed to be an attempt to bypass the behavior detection of security software.

Recently, the Lazarus group has been using various attack methods, using not only rootkit to disable security software but also performing malicious acts using normal application software as shown in this report to achieve their attack goals. AhnLab is closely watching and responding to this group's attack methods and also detecting the current type of attack using the following aliases.

[Filename, MD5, Detection Name)

– SCSKAppLink.dll (0cc73994988e8dce2a2eeab7bd410fad) Trojan/Win.Lazardoor.C5266363 (2022.09.30.03)

– mi.dll (54b0454163b25a38368e518e1687de5b) – Trojan/Win.LazarLoader.C5226517 (2022.08.22.02)

– dfgui.exe (9caebeda61018e86a29c291225f0319f) – Normal MS file

– wsmprovhost.exe (ff46decb93c6d676a37e87de57bae196) – Normal MS file

[Behavior Detection]

– InitialAccess/MDP.Event.M4242 (2022.09.21.00)

IOC related information

MD5
0cc73994988e8dce2a2eeab7bd410fad
54b0454163b25a38368e518e1687de5b
9caebeda61018e86a29c291225f0319f
ff46decb93c6d676a37e87de57bae196

Previous Post

GlobeImposter Ransomware Being Distributed in Korea

Next Post

Attackers Abusing Various Remote Control Tools