

CoinMiner Malware Being Continuously Distributed via USB

A asec.ahnlab.com/en/91415

ATCP

November 27, 2025



In February 2025, AhnLab SEcurity intelligence Center (ASEC) confirmed in their report “Cases of CoinMiner Being Spread via USB” [1] that CoinMiner malware is being spread via USB in South Korea. In July 2025, Mandiant also released a report on the same attack series and categorized the malware being installed as DIRTYBULK and CUTFAIL [2].

While the overall attack method has not changed significantly, the type of malware used in recent attacks is different from those used in previous attacks. This article will analyze the latest malware strains.

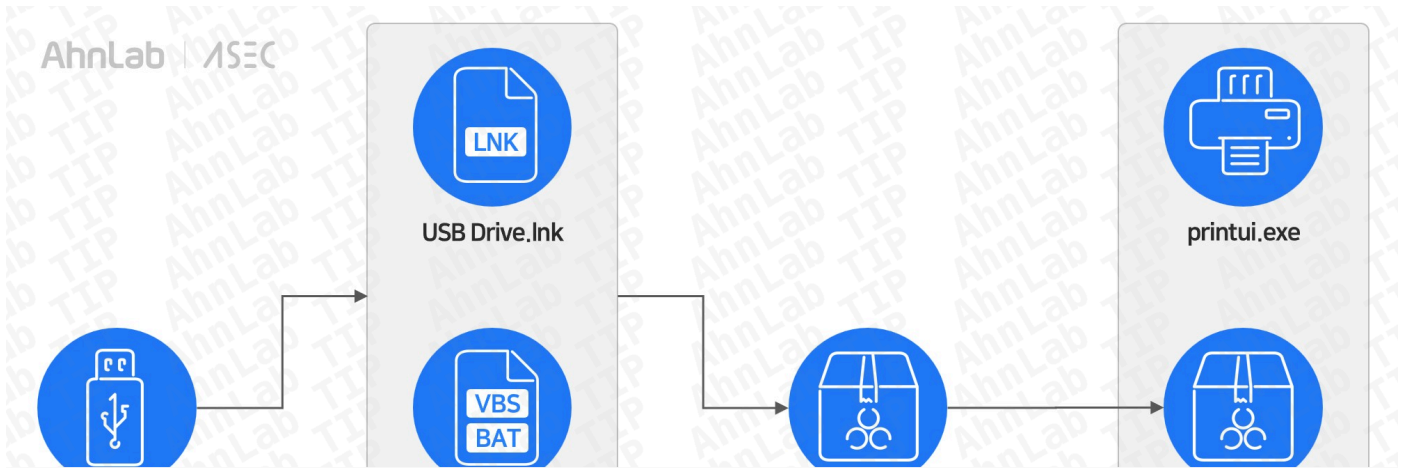


Figure 1. Flowchart

1. Propagation via USB

The infected USB shows the “USB Drive.lnk” file, and there are also “sysvolume” and “USB Drive” folders in hidden attributes. Selecting “Show hidden files, folders, and drives” in the “View” tab of “Folder Options” allows you to view the hidden “sysvolume” and “USB Drive” folders.

Typically, when a user inserts a USB drive and sees the following screen, they would double-click the “USB Drive.lnk” file to execute it. The “USB Drive.lnk” shortcut file executes VBS malware with a name consisting of a random set of six digits starting with “u” like the “u566387.vbs” file in the “sysvolume” folder.

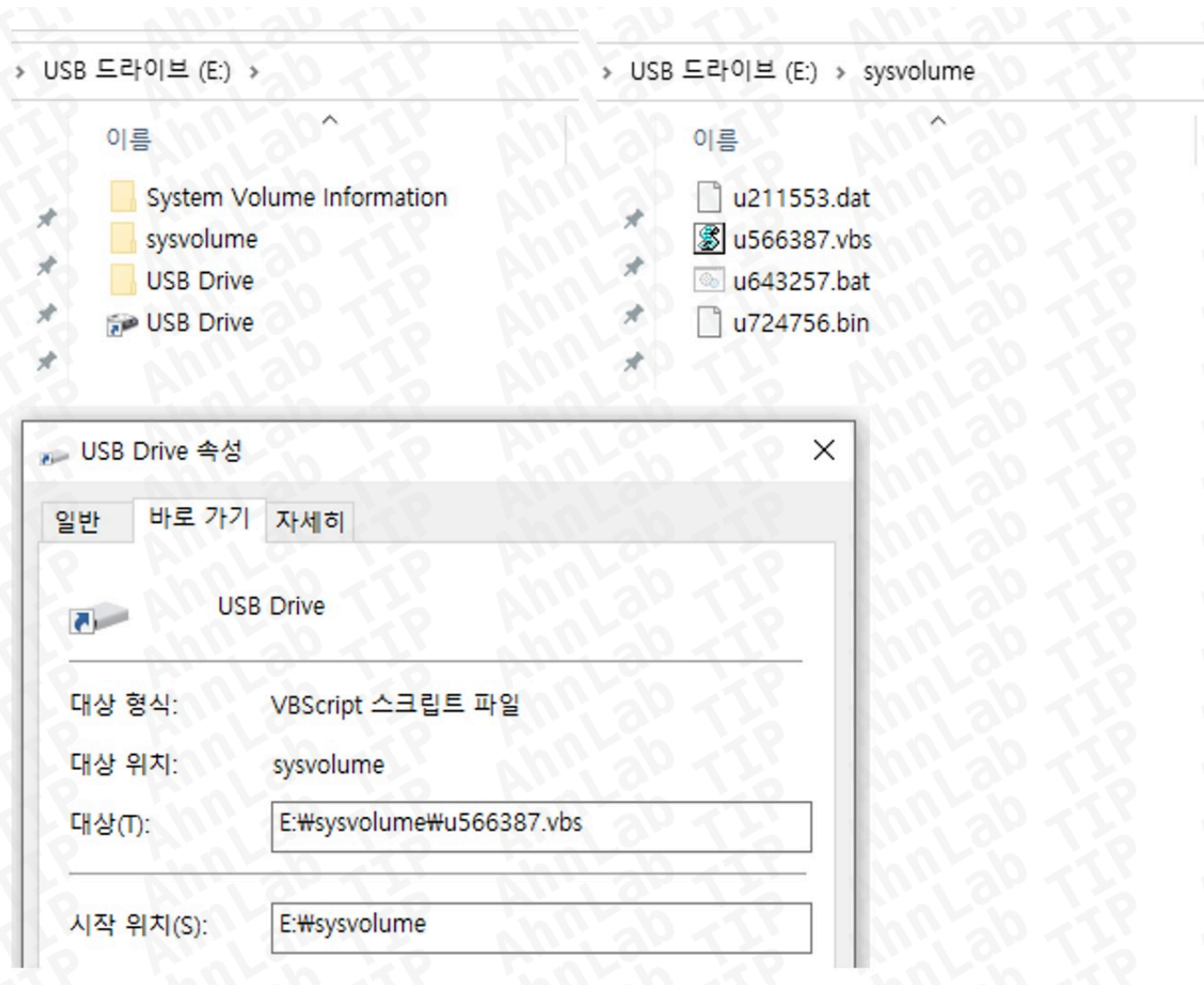


Figure 2. Files inside the infected USB

The VBS malware is responsible for executing BAT malware with the same name (“u643257.bat”) in the same directory. The BAT malware opens the “USB Drive” folder, which contains the original files that were on the USB. As a result, users can use the USB normally, and it may be difficult to identify the malware infection. Additionally, the BAT malware creates a folder with a space in its name (e.g., “C:\Windows \System32\”) and copies the “u211553.dat” dropper malware into it, renaming it as “printui.dll”. It then copies the “printui.exe” file that is in the “%SystemDirectory%” folder into the “C:\Windows \System32\” folder before executing it. This allows the “printui.dll” (i.e., “u211553.dat”) malware to be loaded and executed by the legitimate “printui.exe” program.

```

If Not WScript.Arguments.Named.Exists("elevated") Then
    Set sh = CreateObject("Shell.Application")
    sh.ShellExecute "wscript.exe", Chr(34) & WScript.ScriptFullName & Chr(34) & " /elevated",
        "", "runas", 1
    WScript.Quit
End If
Set fs = CreateObject("Scripting.FileSystemObject")
pp = fs.GetParentFolderName(WScript.ScriptFullName)
bp = pp & "\u643257.bat"
If fs.FileExists(bp) Then

```

Figure 3. Malware installation scripts

2. Dropper

printui.dll is a dropper that is responsible for creating and executing another malware internally in the "%SystemDirectory%\svcinstry64.exe" path. svcinsty64.exe is also a dropper that creates and executes the "svctrl64.exe" file in the "%SystemDirectory%" path. It also creates a configuration file named "wlogz.dat" in the "%SystemDirectory%\wsvcz" folder. Afterward, it executes "svctrl64.exe" as a child process.

svctrl64.exe is also a dropper that ultimately creates a DLL with the same name as "u826437.dll" in the "%SystemDirectory%" folder and registers it with the DcomLaunch service.

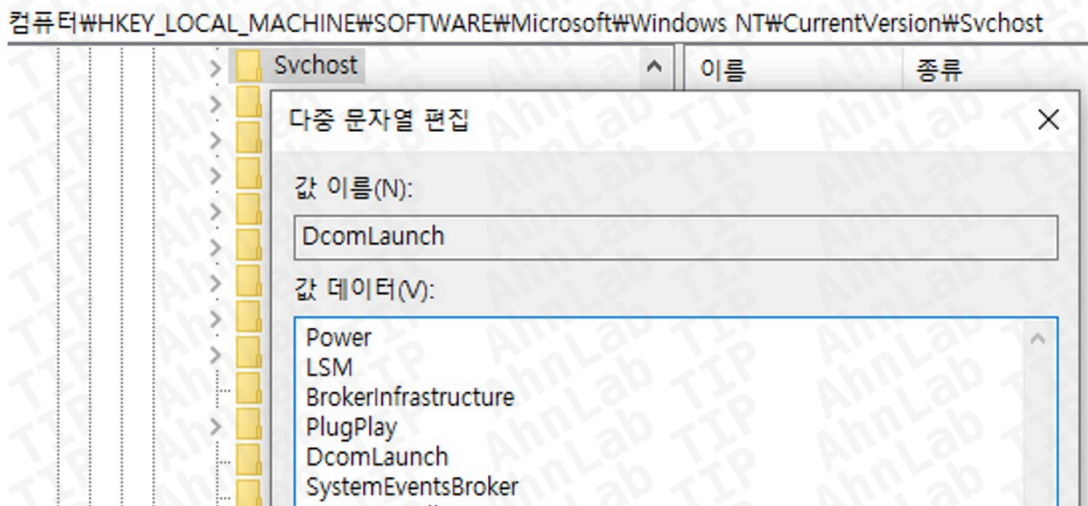


Figure 4. Malware registered to the DcomLaunch service

3. PrintMiner

The malware executed by the DcomLaunch service is categorized as PrintMiner. PrintMiner registers the installation path as an exception folder in Windows Defender and adjusts the power settings to prevent the system from entering sleep mode. It then finds the C&C server's address and transmits information about the infected system, such as the CPU and GPU. Afterward, it installs additional payloads, including XMRig, in the "%SystemDirectory%\wsvcz" folder. The downloaded files are encrypted, so a decryption process is also carried out.

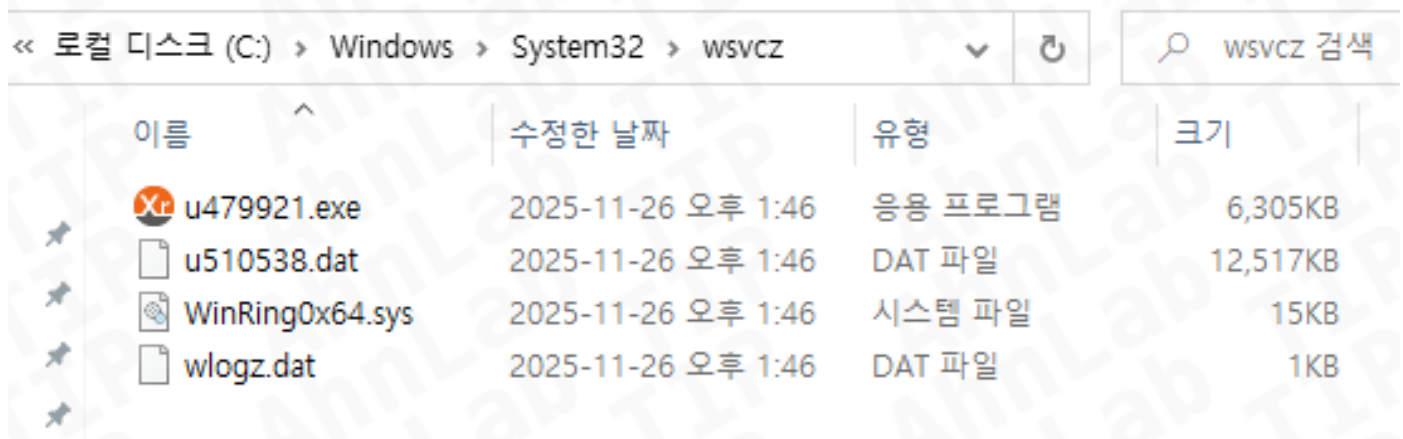


Figure 5. Decrypted installation files

Additionally, the configuration file located in the “%SystemDirectory%\wsvcz\wlogz.dat” path is updated to include information such as the IP address of the C&C server, mining information, and the path of the installed malware.

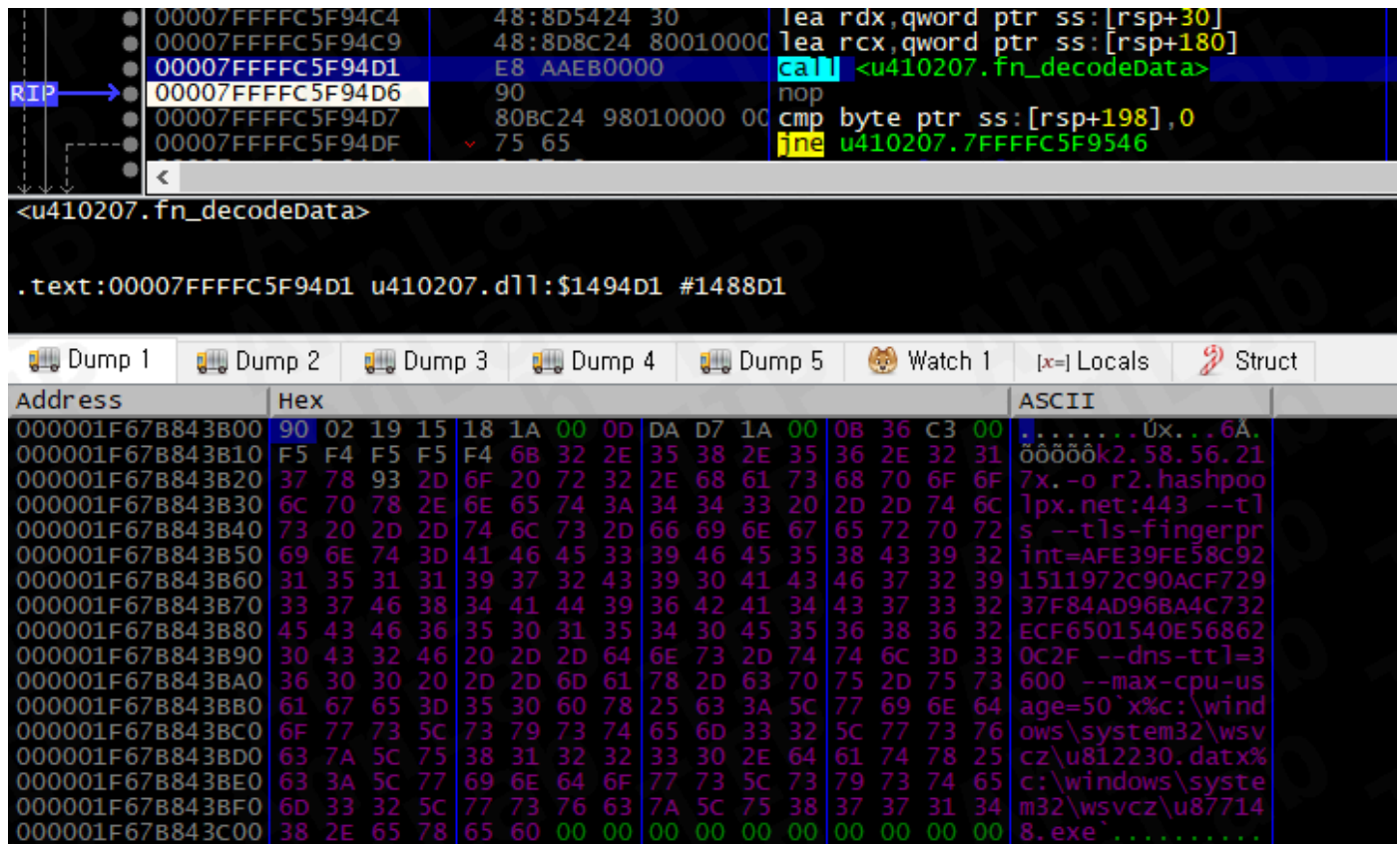


Figure 6. Updated configuration data

Afterward, it creates threads responsible for USB and XMRig execution. As mentioned above, the thread responsible for the USB creates the “USB Drive.lnk” shortcut file, generates malware for the USB worm and VBS/BAT, and moves the user’s files to the “USB Drive” folder in the “sysvolume” directory.

The thread responsible for executing XMRig examines the currently running processes, and only executes XMRig when specific processes are not running, then terminates XMRig when it is already running. Among the processes examined, there are process inspection tools such as Process Explorer, TaskMgr, System Informer, and Process Hacker. These are likely used to conceal the execution status of XMRig when users check the currently running processes. There are also many game client processes included, which may be due to the performance impact that may occur if a coin miner is executed alongside a game that requires high performance.

```
// "Taskmgr.exe"  
// "SystemInformer.exe"  
// "Processhacker.exe"  
// "procexp64.exe"  
// "procexp.exe"  
// "Adobe Premiere Pro.exe"  
// "AfterFX.exe"  
// "vegas190.exe"  
// "vegas200.exe"  
// "aces.exe"  
// "ACMirage.exe"  
// "ACOdyssey.exe"  
// "ACOrigins.exe"  
// "ACS.exe"  
// "RustClient.exe"  
// "s1_sp64_ship.exe"  
// "s2_mp64_ship.exe"  
// "s2_sp64_ship.exe"  
// "SanAndreas.exe"  
// "SCUM.exe"  
// "sdhdship.exe"  
// "sekiro.exe"  
// "ShadowOfWar.exe"  
// "ShippingPC-BmGame.exe"
```

```
// "Shivers-Win64-Shipping.exe"
// "ShooterGame.exe"
// "Bodycam.exe"
// "Sifu.exe"
// "Sifu-Win64-Shipping.exe"
// "SkaterXL.exe"
// "sniper5_dx12.exe"
// "sniperelite5.exe"
```

Figure 7. Part of the process being checked

XMRig execution parameter: "-o r2.hashpoolpx[.]net:443 -tls -tls-fingerprint=AFE39FE58C921511972C90ACF72937F84AD96BA4C732ECF6501540E568620C2F -dns-ttl=3600 -max-cpu-usage=50"



Figure 8. Process tree

5. Conclusion

USB drives are still being used to propagate malware, but unlike in the past when the autorun.inf feature was exploited, the recent cases involve methods that prompt users to execute the malware. In the above case, the malware is hidden in a folder, and only a shortcut file named "USB Drive" is visible. When a user opens the shortcut file, they are able to see not only the malware but also the files belonging to the previous user, making it difficult for users to realize that they have been infected with malware.

The threat actor used multiple techniques to bypass antivirus programs and installed XMRig to mine Monero coins. XMRig is configured to not raise suspicions, such as being terminated if the user is playing a game. It also checks for process monitoring tools, making it difficult for ordinary tools to detect that XMRig is running.

Users must apply the latest security patches for their operating system and installed software, and keep V3 products up to date to block known attacks.

[V3 Diagnosis]

- Trojan/Win.SelfDel.R734002 (2025.11.08.01)
- Trojan/Win.Evo-gen.R731187 (2025.10.20.00)
- CoinMiner/Win.Agent.R735221 (2025.11.13.00)
- CoinMiner/Win.Agent.R5805841 (2025.10.18.00)
- Trojan/Win.Miner3.R512976 (2022.08.31.01)
- Trojan/BAT.RUNNER.S3110 (2025.11.27.03)
- Trojan/VBS.RUNNER.S3111 (2025.11.27.03)

MD5

1cf4a8bfd59d5f04be313d2fa3af5f5a

248eed41f083c5de46a15c2b9f30303e

4bf6fe55240267398bef02703f1a6182

916eac9c0e83da08819d49be32afa182

b88b2c61844a49fcc54727105ae9abac

Additional IOCs are available on AhnLab TIP.

URL

http[:]//2[.]58[.]56[.]13/inf[.]dat

http[:]//2[.]58[.]56[.]13/utl/xmr[.]dat

http[:]//2[.]58[.]56[.]13/utl/xmrsys[.]dat

FQDN

r2[.]hashpoolpx[.]net

umnsrx[.]net

IP

2[.]58[.]56[.]13

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

