XMRig CoinMiner Installed via Game Hacks - ASEC

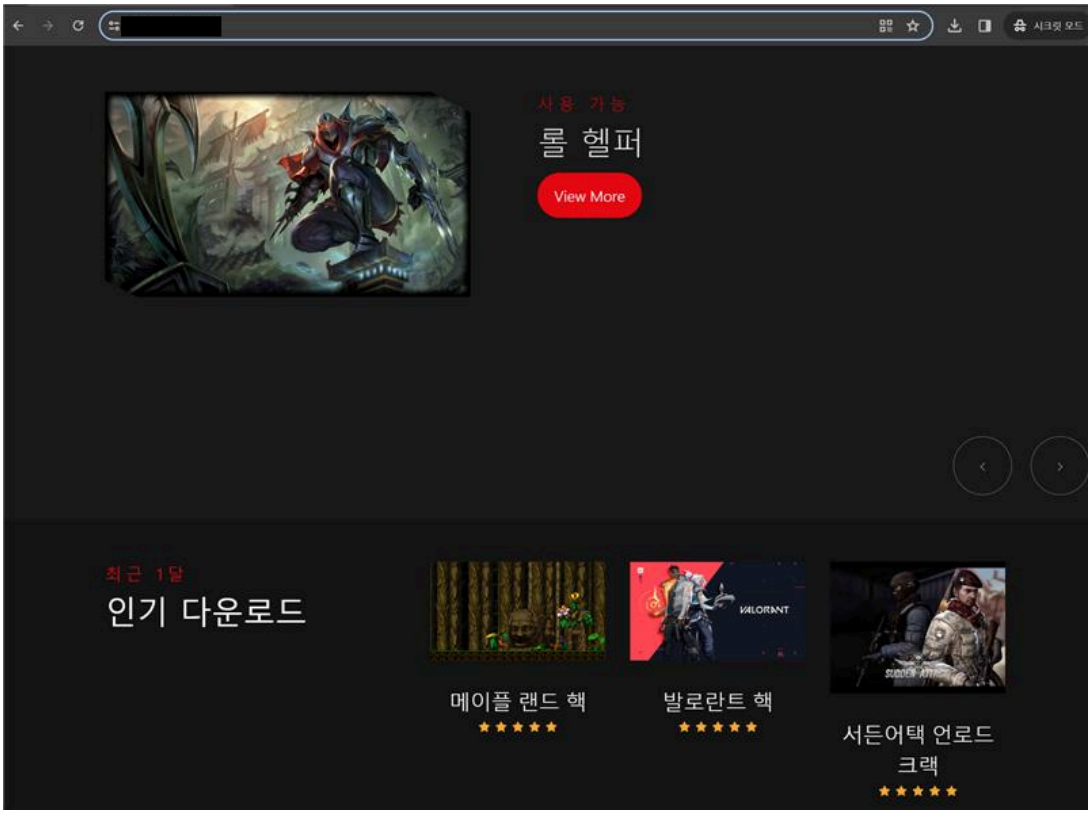
By ATCP

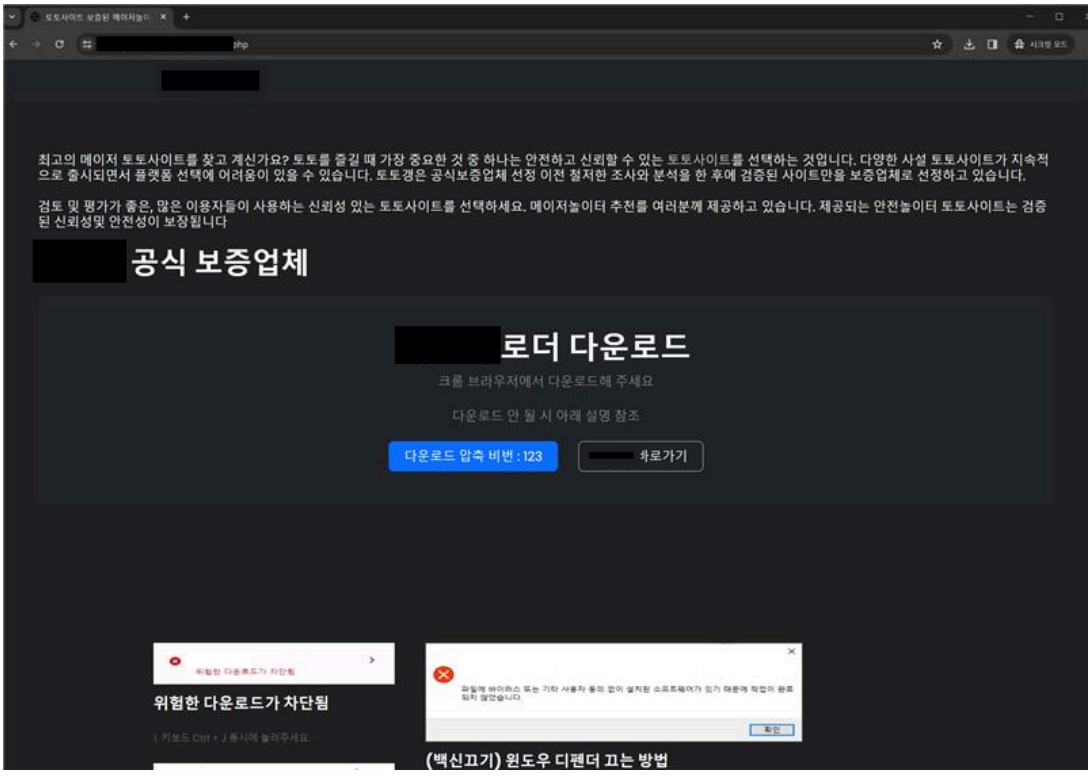
Published: 2024-01-18 · Archived: 2026-04-05 14:27:55 UTC

AhnLab SEcurity intelligence Center (ASEC) recently found that XMRig CoinMiner is being distributed through game hacks. The process is similar to previously covered cases where file-sharing platforms were used to distribute XMRig CoinMiner [1] [2].

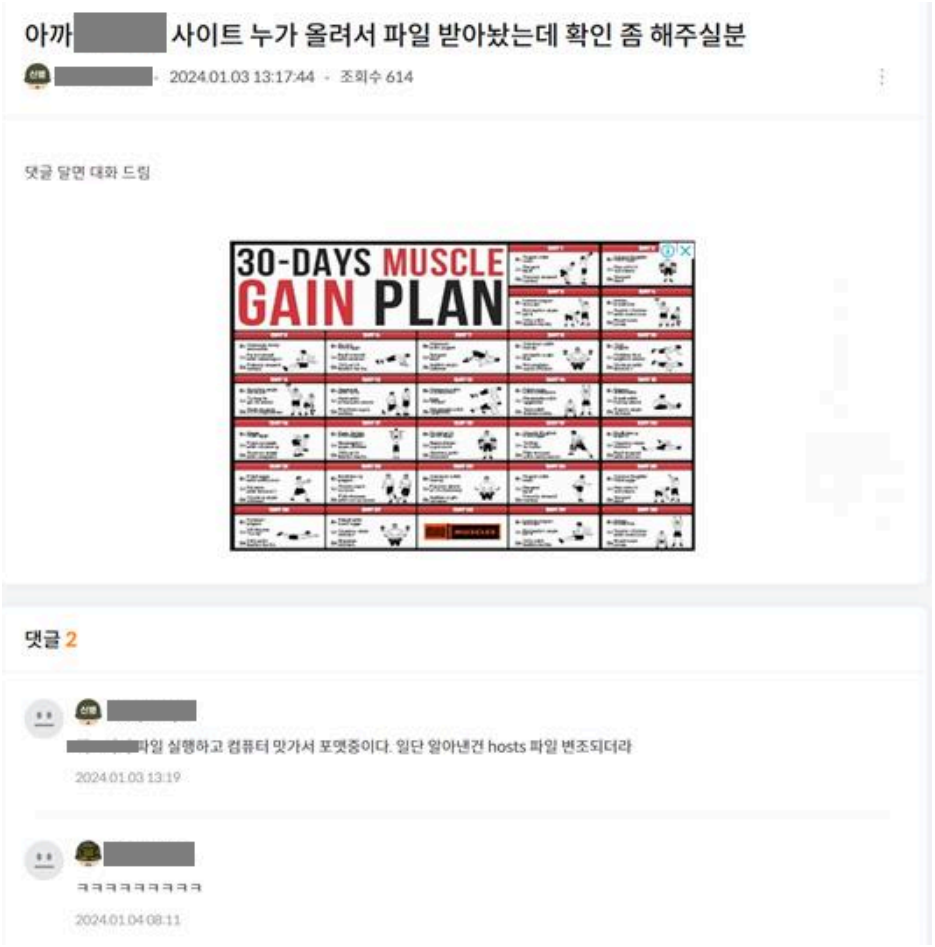
1. Distribution Channel

The CoinMiner's distribution channel was found to be a website that distributes game hacks for famous games. On this website, multiple compressed files disguised as hacks for famous games are uploaded. In order to prevent the download from being blocked by browsers and anti-malware software, it prompts users to install the malware by detailing how to disable the browser from blocking downloads and how to shut down anti-malware software.



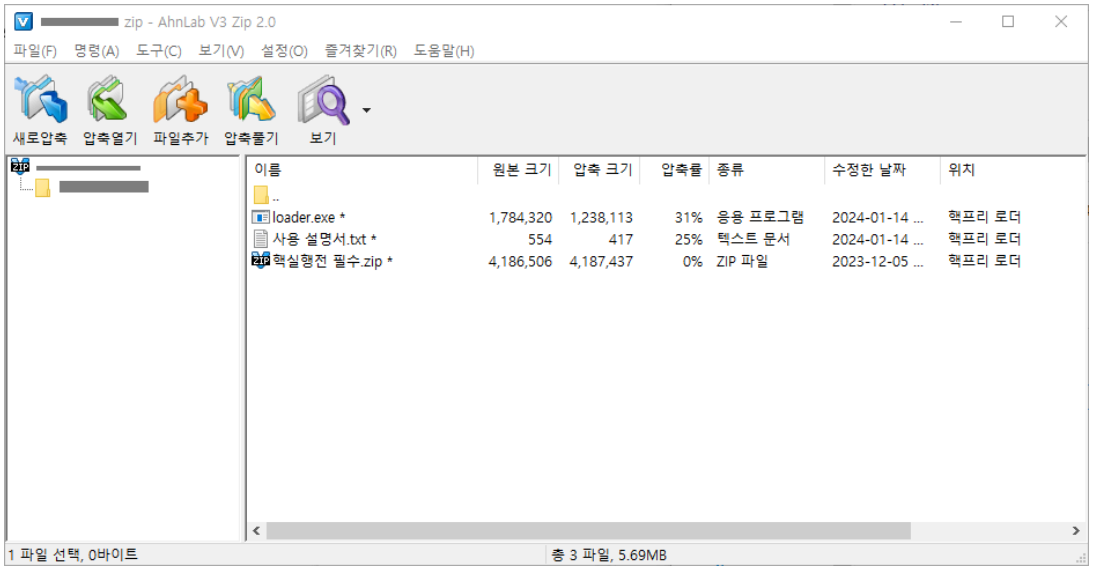


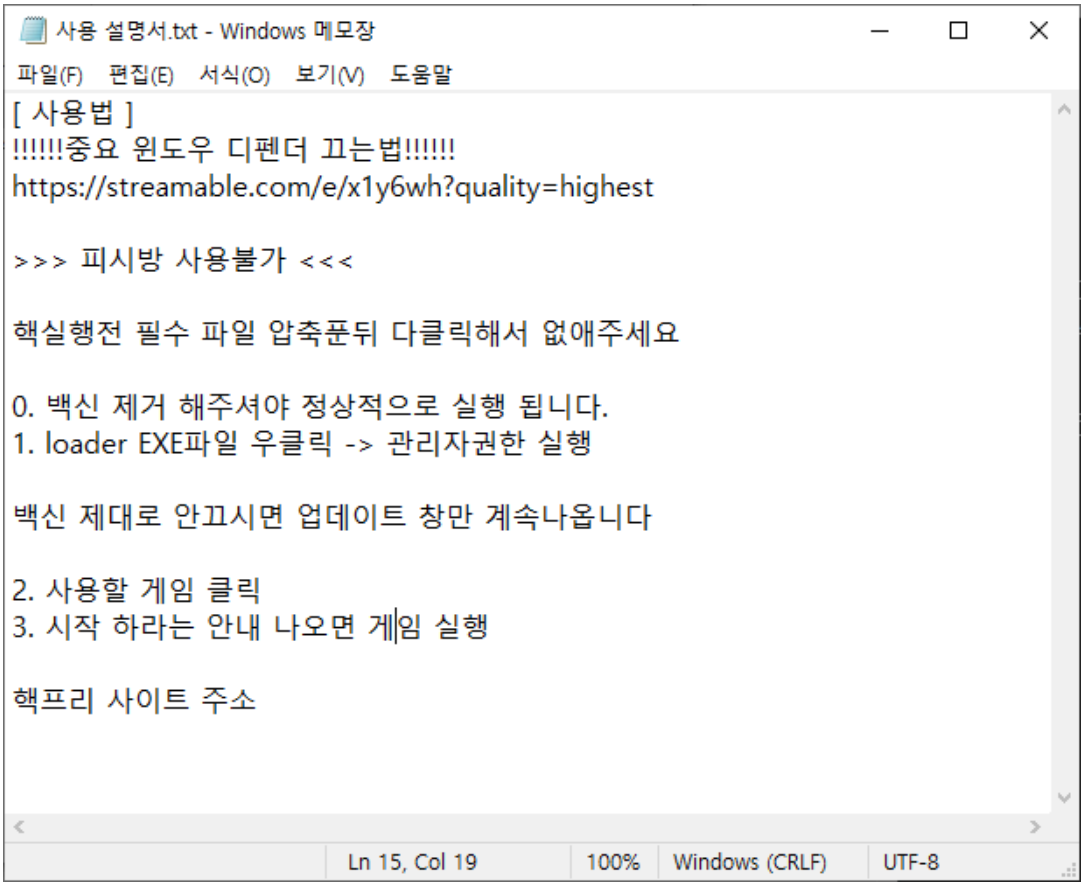
When searching for the programs in an actual gaming community, there are multiple comments from users who are aware that these programs contain malware.



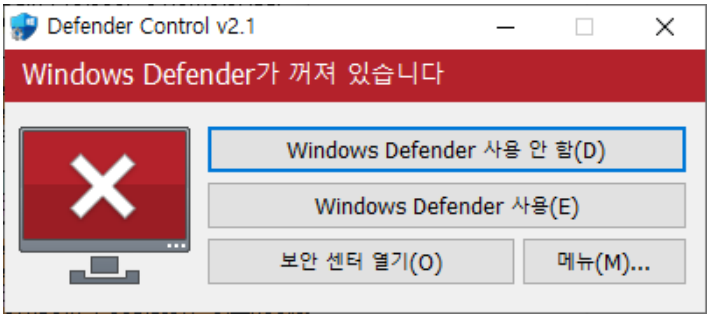
2. Bypassing Detection

The uploaded compressed file has a downloader that installs the CoinMiner and malware that shuts down anti-malware software. The threat actor guides the users to shut down the anti-malware software with the manual that is included in the compressed file, making it much harder for users to be aware of the damage caused by malicious activities.



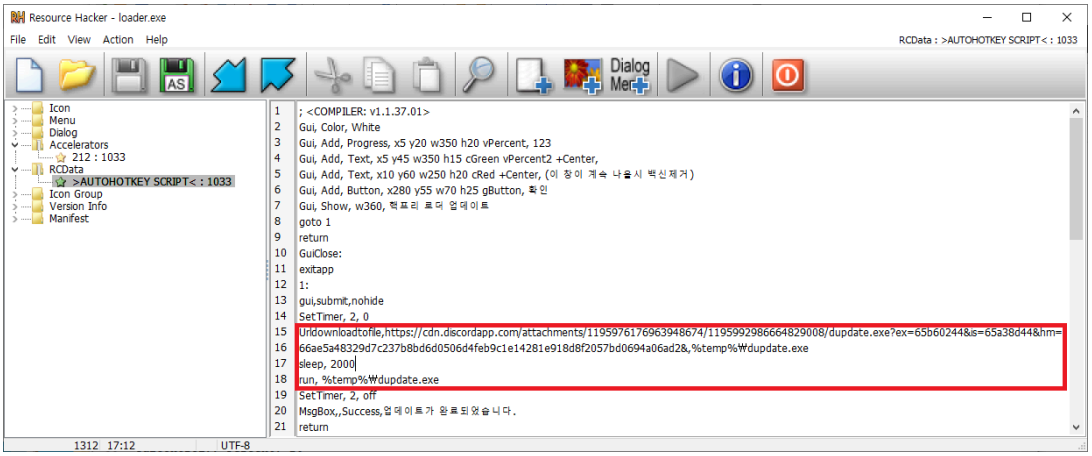


The program used to shut down the anti-malware software is the Windows Defender management program dControl.exe, which disabled Windows Defender.



3. CoinMiner Installed via Downloader

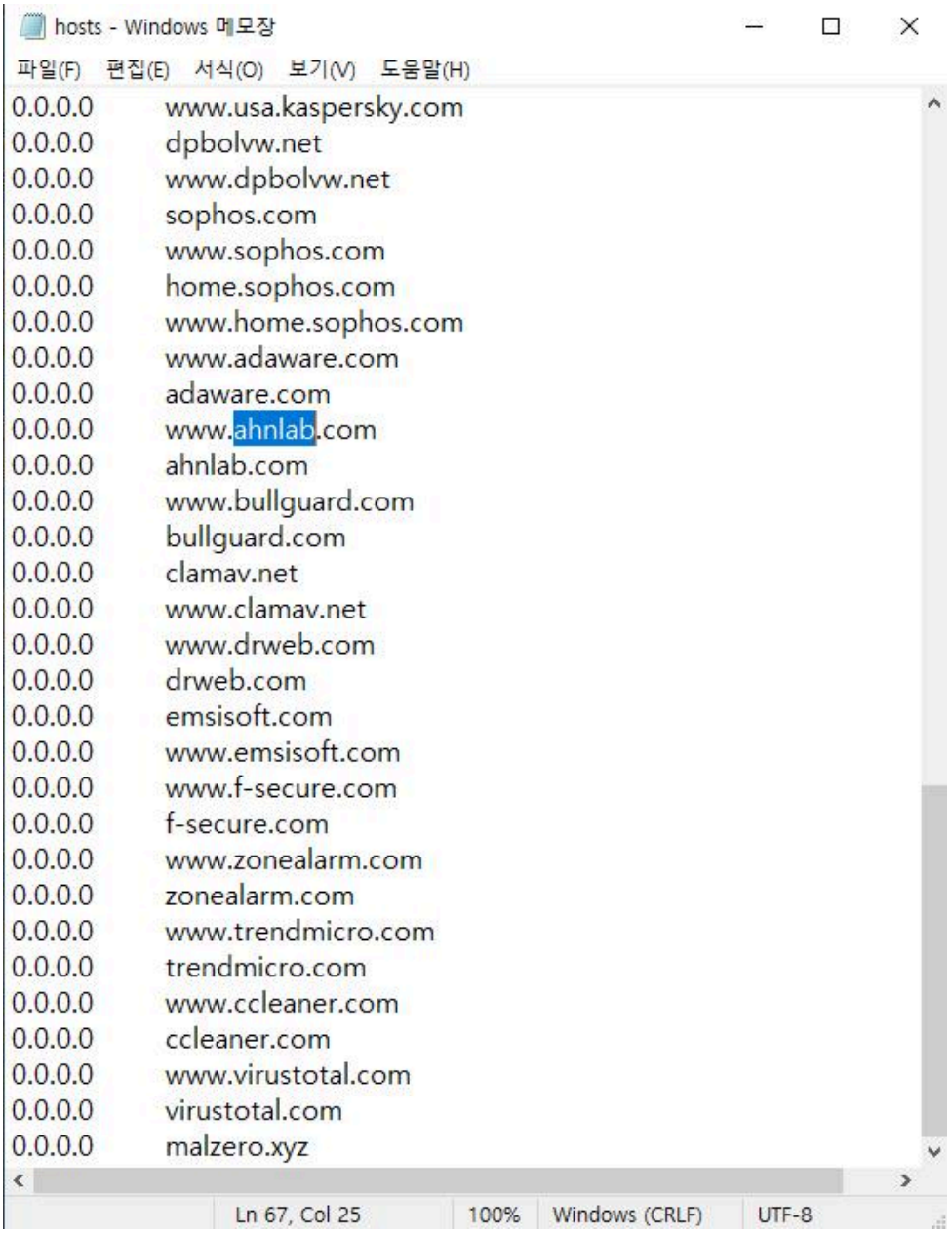
When the preparation to execute the CoinMiner is complete, the CoinMiner is downloaded through loader.exe. The initial downloader is a program made with AutoHotkey, and it installs and executes the CoinMiner in the ‘%temp%\’ folder path.



The executed CoinMiner uses PowerShell to disable Windows Defender from scanning .exe extensions in the ‘ProgramData’ path and removes Windows Malicious Software Removal Tool (MSRT) update, Windows Update, and other similar services. It also attempts to bypass detection by editing the hosts file.

At the same time, it replicates itself in the %ProgramData%\Google\Chrome path with the file name updater.exe and maintains persistence by registering with the service name GoogleUpdateFile.

- Add-MpPreference -ExclusionPath @($env:UserProfile, $env:ProgramData) -ExclusionExtension ‘.exe’ -Force
- cmd.exe /c wusa /uninstall /kb:890830 /quiet /norestart
- sc.exe stop UsoSvc
- sc.exe stop WaaSMedicSvc
- sc.exe stop wuauserv
- sc.exe stop bits
- sc.exe stop dosvc
- sc.exe create “GoogleUpdateFile” binpath=”C:\ProgramData\Google\Chrome\Updater.exe” start=”auto”



- id : zajpavgygytczlbw
- wallet : 4824qBU4jPi1LKMjUrkC6qLyWJmnrFRqXU42yZ3tUT67iYgrFTsXbMmiupfC2EXTqDCjHrjtUR8oHVEsdSF2DErrCipV
- Mining pool : xmr.2miners[.]com:12222
- cinit-stealth-targets : Taskmgr.exe,ProcessHacker.exe,perfmon.exe,procexp.exe,procexp64.exe

4. Conclusion

As malware is being distributed actively via games or game hacks, users need to take caution. As for game hacks, there is a potential risk of getting infected by other malware apart from the CoinMiner introduced in this blog post, as the user needs to periodically execute a downloader like loader.exe. As such, caution is advised when running executables downloaded from unreliable file-sharing websites. It is recommended to download programs such as utilities and games from the official websites. This type of malware is diagnosed by AhnLab as follows.

[File Detection]
Downloader/Win.Agent.C5574989 (2024.01.16.03)

CoinMiner/Win.Agent.C5574932 (2024.01.16.02)
HackTool/Win.DefenderControl.R443408 (2021.10.07.03)

[Behavior Detection]
Execution/MDP.Cmd.M4789

MD5

58008524a6473bdf86c1040a9a9e39c3

7698fe6bd502a5824ca65b6b40cf6d65

db98d8d6c08965e586103b307f4392fb

Additional IOCs are available on AhnLab TIP.

SHA2

66ae5a48329d7c237b8bd6d0506d4feb9c1e14281e918d8f2057bd0694a06ad2

Additional IOCs are available on AhnLab TIP.

URL

https[:]//cdn[.]discordapp[.]com/attachments/1195976176963948674/1195992986664829008/dupdate[.]exe?ex=65b60244&is=65a38d44&hm=66ae5a48329d7c237b8bd6d0506d4feb9c1e14281e918d8f2057bd0694a06ad2

Additional IOCs are available on AhnLab TIP.

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

Source: https://asec.ahnlab.com/en/60845/