Monero CoinMiner Being Distributed via Webhards

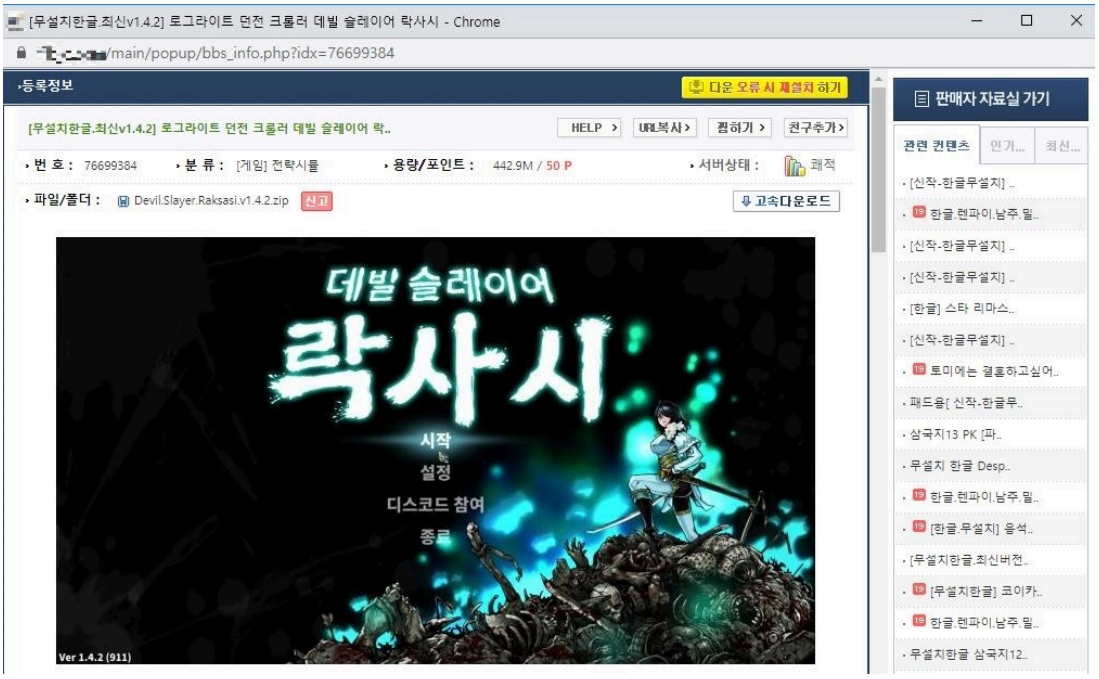
By ATCP

Published: 2022-07-31 · Archived: 2026-04-05 22:48:17 UTC

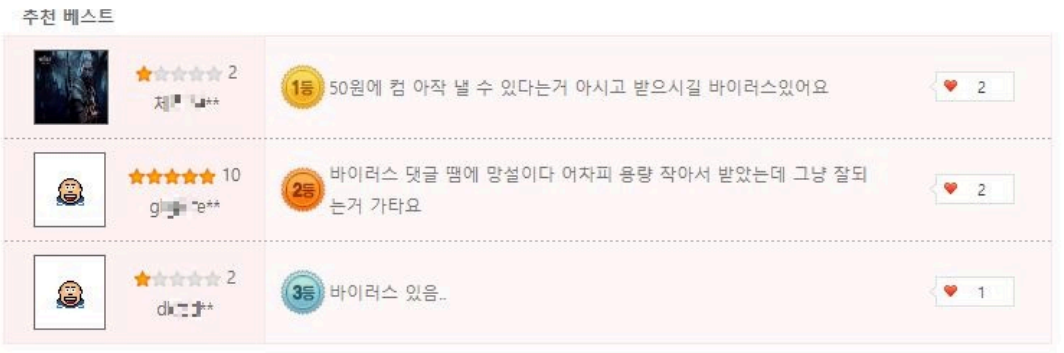
Webhards are the main platforms that the attackers targeting Korean users exploit to distribute malware. The ASEC analysis team has been monitoring malware types distributed through webhards and uploaded multiple blog posts about them in the past.

Generally, attackers distribute malware with illegal programs such as adult games and crack versions of games. Those who use webhards as a distribution path typically install RAT type malware such as njRAT, UdpRAT, and DDoS IRC Bot.

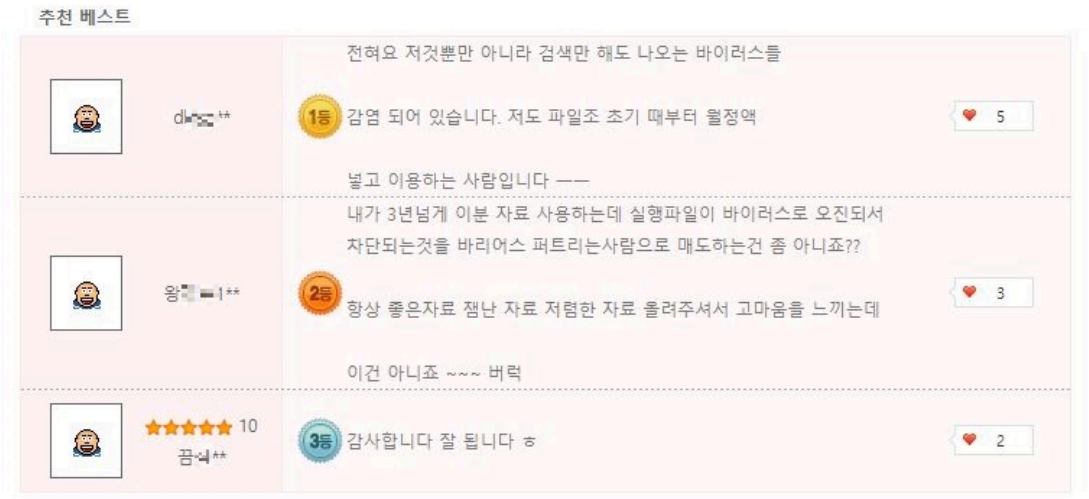
The team has recently discovered the distribution of XMRig, also known as Monero CoinMiner, through webhards and will discuss it in this post. After checking the path where the malware was distributed, the team found that compressed files disguised as game installers were uploaded to certain webhards.



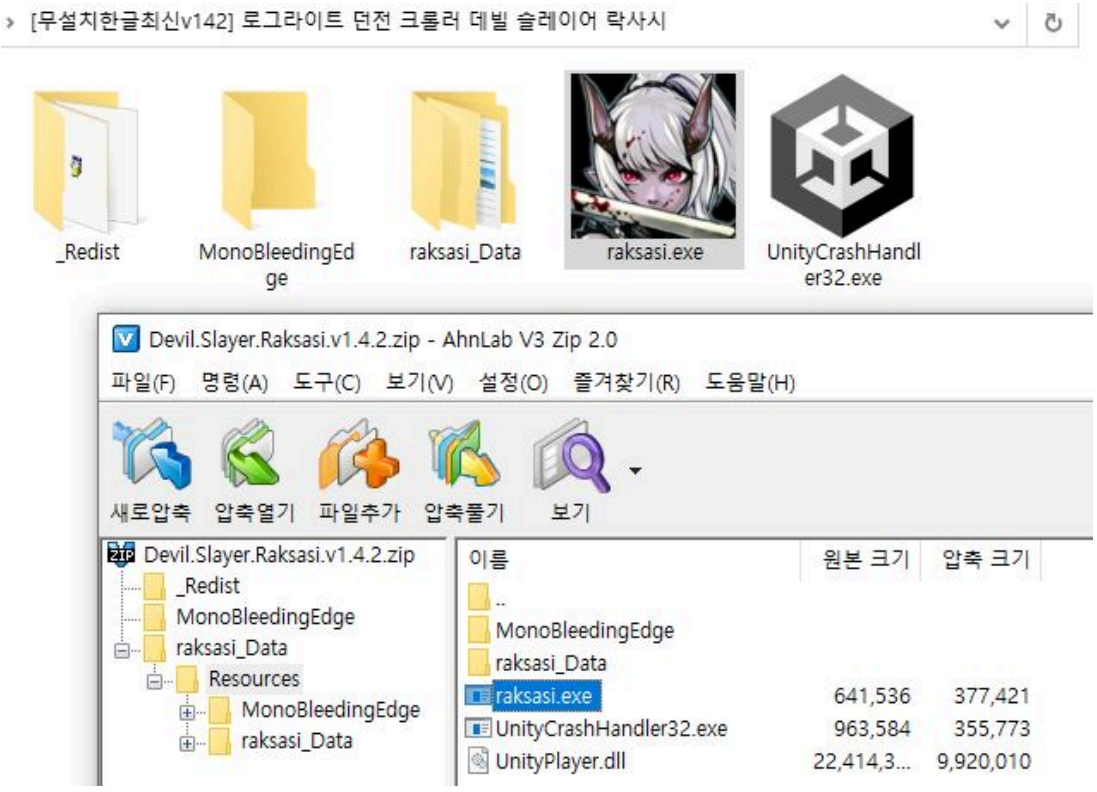
There are many users in the reply section of the above posts who have confirmed the existence of malware inside the files after a scan was carried out by their respective anti-malware programs during the installation process.



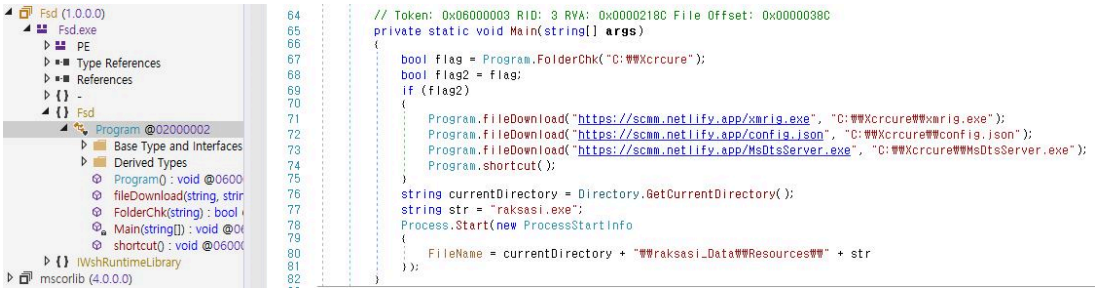
However, the team could not confirm whether the uploaders of these files were the ones who actually created the malware or not. This is because the files can be uploaded to other webhards after they are initially uploaded on certain torrents or webhards due to the characteristics of such game installers.



The following files are shown after decompressing the downloaded file. Therefore, users will run the “raksasi.exe” program that is disguised as the game icon. However, the file is actually a malware strain that installs XMRig CoinMiner. The actual game program is inside the Resources folder within raksasi_Data.



This malware has a very simple structure. First, it downloads the Monero mining malware (xmrig.exe), XMRig config file (config.json), and XMRig launcher malware (MsDtsServer.exe) in the path “c:\Xcrcure\”. It then creates a shortcut called “NewStartUp.lnk” in the startup folder that executes the XMRig launcher. This causes Monero to be launched after the next reboot. Finally, it executes the actual game inside the Resource folder to make it seem like the user launched the game normally.



After XMRig is installed through this process, it reads the config.json file in the same path whenever the computer is rebooted to perform the mining process. The following figure shows the addresses of the mining pool and of the attacker's wallet that exist inside the json file.


```
"log-file": null,
"donate-level": 1,
"donate-over-proxy": 1,
"pools": [
    {
        "algo": null,
        "coin": null,
        "url": "gulf.moneroocean.stream:10128",
        "user": "438wFRXdmiEQfgfhK4XhSMSNaFNd8EdJzPhj5PcXtomEaKcNJuBoZaC32TSdGpnFUxRANRiQdsWxGdvM7bDgLJHZR9FKFSF",
        "pass": "x",
        "rig-id": null,
        "nicehash": false,
        "keepalive": false,
        "enabled": true,
        "tls": false,
        "tls-fingerprint": null,
        "daemon": false,
        "socks5": null,
        "self-select": null,
        "submit-to-origin": false
```


– Mining pool address: gulf.moneroocean[.]stream:10128
– Monero wallet address: 438wFRXdmiEQfgfhK4XhSMSNaFNd8EdJzPhj5PcXtomEaKcNJuBoZaC32TSdGpnFUxRANRiQdsWxGdvM7bDgLJHZR9FKF

As shown in the examples above, the malware is being distributed actively via file-sharing websites such as Korean webhards. As such, caution is advised when running executables downloaded from a file-sharing website. It is recommended to download products such as utility programs and games from the official websites.

AhnLab's anti-malware software, V3, detects and blocks the malware above using the aliases below.

[File Detection]
– Trojan/Win.FY.C5155016 (2022.06.02.02)
– Trojan/Win64.XMR-Miner.R226842 (2019.12.11.01)
– CoinMiner/Text.Config (2022.08.01.02)
– Trojan/Win.Launcher.C5217400 (2022.08.01.02)

MD5

2f4650b01f8943f577abad9869429d1a

35370cd5222ade95f77c8db5e39bcd64

c717c47941c150f867ce6a62ed0d2d35

d5d51ebb4ab6dc97d7e5557476526547

f3227fc9ecc270d49e4b24eedfbdfdf2

Additional IOCs are available on AhnLab TIP.

URL

https[:]//scmm[.]netlify[.]app/MsDtsServer[.]exe

https[:]//scmm[.]netlify[.]app/config[.]json

https[:]//scmm[.]netlify[.]app/xmrig[.]exe

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/37526/