XMRig Miner Malware Analysis 2026: Understanding Threats

By Gridinsoft LLC

Archived: 2026-04-05 16:57:00 UTC

XMRig Miner Malware

Everything is poison, and everything is medicine. XMR mining tool, that was originally designed to make mining more convenient and easy-to-deploy, became an ever-loved tool of cybercriminals that chase crypto profits. It is now known as XMRig – tremendously widespread miner trojan.

The XMRig trojan is a miner malware – one that parasites on its victim's hardware to mine cryptocurrencies, particularly Monero (XMR). Being based on a **legitimate open-source** crypto mining application, it employs anti-analysis and detection evasion techniques that can render legacy anti-malware software significantly less effective. Nonetheless, the visible effect of XMRig activity – **an overloaded processor** – is hard to confuse with that of any other malware. As it targets any kind of system, the unfortunate opportunity to witness your computer being rendered nearly useless can occur both at work and at home.

Another notable detail XMRig can boast of is the wide variety of delivery methods it exploits, and its association with numerous other malware types, including ransomware and spyware. Such associations have influenced the malware in a way that some of its samples can perform spyware-like actions – which is particularly concerning given its long-term activity. Since the basis for this miner is an open-source tool, XMRig likely has the largest number of variants – other malicious miners that, however, feature some alterations in their codebase.

Read also: Almoristics Application: What It Is & How to Remove Virus Miner

Why Do Hackers Choose Monero?

Cryptocurrencies based on the Proof-of-Work (PoW) protocol utilize computational power to validate transaction hashes. Each successful validation rewards the operator with a commission fee. Monero is among these currencies and is engineered for a simplified hash calculation, significantly quicker than those of **Bitcoin** or **Ethereum**. This

efficiency drastically shortens transaction times and enables mining on low-power systems while still maintaining sufficient efficiency to earn commissions. Consequently, this provides an ideal scenario for cybercriminals: to create a botnet that utilizes its CPU power (instead of traditional GPU-based mining farms) for mining cryptocurrencies – resulting in a steadily growing wallet.

The darknet infrastructure has fostered another layer of convenience for illicit activities, enabling criminals to obscure their ill-gotten gains. Cryptomixers conduct transactions not in the traditional wallet-to-wallet manner but by breaking down the amount into dozens of smaller parts and funneling it through a series of unrelated wallets, making the crypto transfer hard to trace. XMR is particularly suited for this purpose, as its rapid transactions facilitate the completion of transfers within just a few hours. Other cryptocurrencies might require days to accomplish a similar level of obfuscation.

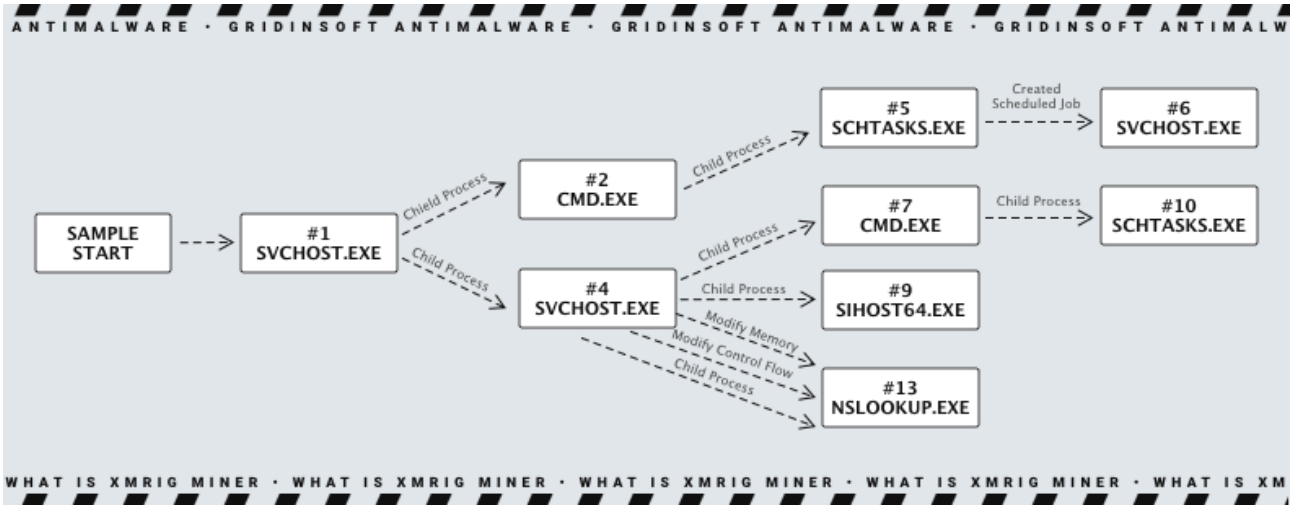
How Does XMRig Spread?

XMRig miner is operated by numerous cybercriminal groups, each employing their unique method to disseminate this malware. As such, **there is no single, unified approach to its distribution** – making it an even more formidable threat. To counteract this, one must consider virtually every possible method, a task that can be overwhelming. Fortunately, certain techniques – typically associated with the most active criminal groups utilizing XMRig – are encountered more frequently than others.

- **Dropper malware** is utilized in attacks against networks of computers that were already compromised. It proves especially effective for infiltrating corporate networks, which tend to have stronger security measures. Botnets driven by droppers (or backdoors with dropper capabilities) are also common in single-user systems. In specific instances, XMRig has been delivered alongside **other malware**, such as ransomware and spyware, making it a preferred method for spreading infections to these systems.
- **Cracked and untrustworthy software** serves as a façade for a broad spectrum of malware, with XMRig being one example. Software becomes malicious after being cracked, that is, once its license verification has been bypassed. Those who crack software often aim for monetization, and deploying malware is one of the ways to achieve this. Moreover, using cracked software is illegal, leaving individuals open not only to malware risks but also to legal repercussions for copyright infringement.
- **Untrustworthy software** is explicitly designed to carry a malicious payload. Browser plugins, driver updaters, and system cleaning tools – all potentially harboring questionable intent. While not all software in these categories is malicious, those offered as part of a bundle, **or through an unexpected ad**, are usually suspect. They might perform their advertised functions but operate malicious activities in the background – akin to a browser plugin harboring a miner.
- **Email spam** is a widely recognized method for malware dissemination on a broader scale. XMRig is not exempt – with some variants spread via this method. A noteworthy aspect of such campaigns is the employment of the outdated double-extension trick, exploiting default settings in Windows file manager. Files named *important-document.docx.exe* appear as *important-document.docx* on systems with hidden file extensions, leading unsuspecting victims to execute what they believe to be a legitimate document.

XMRig Malware Analysis

Similar to their distribution methods, the XMRig samples are extensively modified by various cybercrime groups to suit their specific needs. Therefore, we've chosen to focus on some of the common features found in most XMRig samples circulating in the wild. In general, malicious miners share several tricks that are prevalent across this type of malware.



Scheme of the XMRig infection chain

Upon reaching the target computer, the malware begins by decrypting itself and establishing persistence. The decryption process is standard: the malware unpacker uses a hardcoded key to eliminate RC4 encryption. It then allocates memory through the *VirtualAlloc* function, transfers the decrypted data to this memory, and initiates execution from there. The static part of the decrypted data is typically stored in the *AppData\Local\Temp* directory, often under a name mimicking a system process.

The result of this initial decryption is a PE file containing the actual miner and all necessary components for the malware’s operation. It ensures its persistence in the victim's environment by creating tasks in the Task Scheduler using a console command. This task is designed to start the mining process immediately after the user logs in.

```
/c schtasks /create /f /sc onlogon /rl highest /tn "svchost" /tr '"C:\Users\RDhJ0CNFevzX\AppData\Loc
```

The name of the malware file, *svchost.exe*, is not consistently used and can vary from one case of infection to another, ranging from mimicking the names of system processes to simple numerical sequences.

The execution of XMRig continues with the malware contacting its command and control (C2) server to fetch configuration files. These configurations dictate the mining method and the wallet address to use. It retrieves this information from the C2 server and adjusts the system's network settings accordingly. To achieve this, it employs *nslookup.exe*, the default DNS configuration utility in Windows, executing the following command:

```
--cinit-find-x -B --algo="rx/0" --asm=auto --cpu-memory-pool=1 --randomx-mode=auto --randomx-no-rdms
```

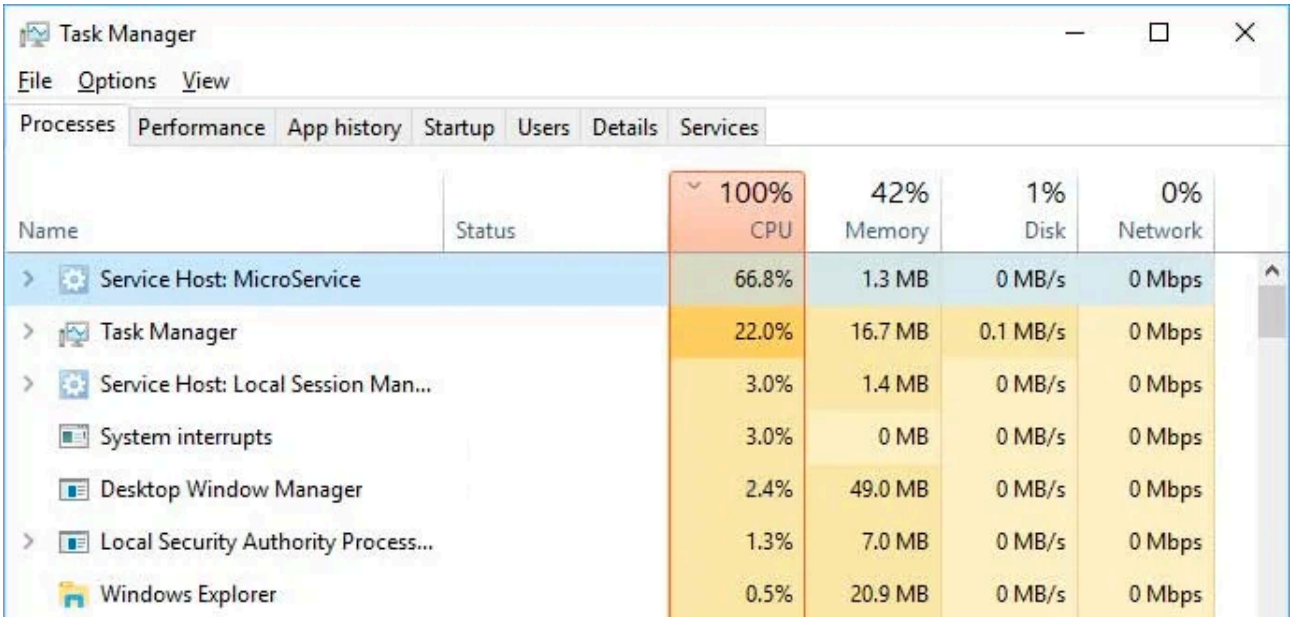
This step concludes the preparations, and the malware is now ready for operation. **The communication with the C2 server by XMRig is not particularly remarkable**—after initialization and receiving configurations, it

operates based on them unless directed otherwise by the C&C server to change settings or cease operation. Additionally, the malware gathers some information about its host system, simply to allow its C&C to distinguish it from others.

Read also: StaryDobry Malware Hides in Pirated Games, Deploys XMRig

The Effects of XMRig

Unlike most malware, which corrupts files by locking them or leaking them to a command server, XMRig's primary function is to utilize the computational power of an infected PC for cryptocurrency mining. This should not be underestimated—such exploitation can severely harm your computer. In contrast to voluntary mining, where loads can be managed, malicious mining disregards the well-being of the host system's hardware. **Cybercriminals often configure the CPU load to 80%**, which might be sustainable for a robust system. However, laptops or poorly maintained computers might experience throttling; associated components, especially those linked to the processor or its heatsink, could also be affected. High temperatures can shorten the lifespan of any electronic component.



Processes that overload the CPU can be detected by opening the Task Manager.

Setting aside pessimistic forecasts, **an overloaded computer is undesirable**. Lesser-powered systems may barely respond to user inputs, while more capable computers will remain functional but suffer from degraded performance even in basic applications. Fortunately, this behavior is distinct enough not to be mistaken for other issues, making diagnosis straightforward. Nonetheless, living with this issue is inadvisable, and removing the malware should be a priority. However, the system overload complicates immediate use of anti-malware software. A targeted approach for XMRig removal is necessary, involving booting the system into Safe Mode with Networking.

How to Protect Yourself from XMRig Malware?

Dealing with miner malware, as previously mentioned, is challenging. Therefore, being prepared to address the issue is less effective than preventing the problem altogether. This advice holds true for nearly all types of malware. The most proactive steps focus on blocking malware from entering your system in the first place, which is relatively straightforward given the common propagation methods we've outlined.

- **Avoid using cracked software and untrustworthy programs.** Even though email spam has become a prevalent method for malware distribution in recent years, cracked software continues to be a popular infection vector targeting individual users. A source may seem safe, and you might have used it multiple times without issue, but this doesn't ensure safety. Additionally, using unlicensed software is illegal and being caught can result in substantial fines or imprisonment.
- **Be wary of untrustworthy programs,** often promoted through various means. Tools for system optimization, keygens, apps for manual software cracking, and browser plugins promising extraordinary features pose significant risks. Most anti-malware solutions identify such software as potentially unwanted programs (PUPs), and disregarding these warnings is ill-advised.
- **Steer clear of email spam.** The sheer volume of emails received daily can make it hard to discern legitimate messages from spam. However, there are clear indicators, such as the sender's email address. Fraudulent messages might mimic reputable companies but sending from a dubious email address reveals the deceit, regardless of the message content.
- **Logic inconsistencies in messages are telltale signs of spam.** Questionable double notifications from courier services or unexpected bills from companies you haven't transacted with are red flags. Rarely do genuine companies send such communications in error, so these are likely spam attempts mimicking routine correspondence.
- Regularly scan your system with high-quality anti-malware software. Malware, whether overt or delivered via droppers, can be effectively detected and removed with specialized tools. Manual detection is challenging, as these threats tend to be as inconspicuous as possible. GridinSoft Anti-Malware can identify and eliminate even the most recent malware strains, leaving no room for resurgence. Its advanced scanning system detects malware not just by its files but also by its behavior, ensuring comprehensive protection.

Use Gridinsoft malware remover to scan for miner virus, review suspicious items, and remove confirmed threats on Windows. If this guide matches what you are seeing on your device, start with a practical cleanup scan.

Download malware remover

XMRig IoC

Hashes

```
SHA256: de5704d6579398a4b51f7458c105759c46096567661a26bffe1159ef11a16eb8
SHA256: ea3eedc043d02375db791cd0d508259dede55a7cffa2f75f813d4e239aa5bf70
SHA256: 3c54646213638e7bd8d0538c28e414824f5eaf31faf19a40eec608179b1074f1
SHA256: 32b617dd0ea32902a18d93fe74b4a8865d23ec398666736ffcb4c4e9dfa9c6ec
SHA256: af421881786af65cf89b28d2a88d37658625f21f9644cf298c438267c7c92572
SHA256: 05e1988f56fe199f7e401c8f4d6ee50bb26ab34fb3f96c22de959c7e5f92de77
```

```
SHA256: f63921129822475dd132a116b11312ebbb0cdc8b54f188aabeb7cf7a8c9065fd
SHA256: 95da91e0a3362fcfb23dd10b50dfb28af074ef11759be5cfd48854572773f989
SHA256: 621a9f892436647a492e3877502454d1783dc0cf4e4ba9f3f459a8c2ac7e6d97
SHA256: f34fc824a6c655bd6320b7818acdad9a5a570b88dd46507fdf73cd254af9b19f
```

```
MD5: 5906ac14bc45a1f39cb9eb790a1d3b27
MD5: 0252b6575abd58fac21130cd75fc42a0
MD5: 2a0d26b8b02bb2d17994d2a9a38d61db
MD5: 52df19b9845a6da6197831525c7a1f01
MD5: 5807efef92e20ffe074bbdc141cfbdad
MD5: 6a292b8ab3ff79cefe5f8e42882885d2
MD5: 22a9265676ffebc71d888f0c57af9fd1
MD5: 47d02cfb4cdbccccbc35d082f5351dd1
MD5: e5e85cc9c86ad7362efc2255612db5c0
MD5: 96c45411bcda48997ead1d0dd2aff484
```

IP addresses

145.14.144.136:443	94.130.165.85:443	142.93.172.227:1389
68.183.165.105:80	62.102.148.152:8618	159.89.182.117
51.250.28.5	150.60.139.51:80	51.250.28.5
150.60.139.51	68.183.165.105	79.134.225.39:6969

Read also: AlrustiqApp.exe Virus (Alrustiq Service)
