C

CoinMiner Detection: Malware Signs, Removal, and False Positives

CoinMiner is a generic detection for cryptocurrency-mining software. Learn how to distinguish approved mining from cryptojacking, remove persistence, and validate false positives.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
6 min

CONTENTS

In this guide

01 Authorized mining vs CoinMiner malware
02 How CoinMiner malware gets installed
03 Signs of unauthorized cryptomining
04 What the detection path can tell you
05 How to remove CoinMiner malware
06 Why CoinMiner keeps coming back
07 Could CoinMiner be a false positive?
08 Prevention
09 Frequently asked questions
10 References

CoinMiner is a generic security-detection name for software that uses a computer's CPU or GPU to mine cryptocurrency. Mining software is not automatically malware: an owner may install and configure it intentionally. It becomes cryptojacking or coin-mining malware when it runs without informed authorization, is delivered by an attacker, hides itself, persists after removal, or sends the proceeds to someone else.

The detection name alone does not identify one malware family. Products may label a known miner, a modified mining client, a script that launches it, or behavior associated with unauthorized mining. The file path, parent process, installer, wallet or pool configuration, and persistence method determine what happened.

01 Authorized mining vs CoinMiner malware

Expected mining	Likely unauthorized mining
The device owner approved the software and resource cost	The user cannot explain when or why it appeared
Installed from the documented project or vendor source	Arrived with a crack, fake utility, exploit, document, or compromised server
Pool, wallet, schedule, and startup settings are known	Configuration is hidden, encrypted, or points to an unfamiliar wallet
Resource limits match an approved policy	Mining runs when the device is idle or throttles when monitoring starts
Security exclusions are narrow and documented	Defender, firewall, or broad exclusions were changed unexpectedly
Uninstalling the miner ends the workload	A service, task, script, or remote actor recreates it

Do not restore or allow a CoinMiner detection merely because the underlying mining engine is open-source. Legitimate tools such as XMRig can be repackaged or launched by malware.

02 How CoinMiner malware gets installed

- Cracked software, key generators, game cheats, fake codecs, and unofficial installers.
- Poisoned search results or cloned download sites impersonating popular utilities.
- Malicious documents, scripts, archives, browser extensions, or fake updates.
- Exploited public servers, weak remote-access credentials, or exposed cloud services.
- A loader that later downloads a mining client selected for the victim's CPU or GPU.
- Compromised websites that run browser-based mining scripts without meaningful consent.

Microsoft documented a 2026 campaign that used poisoned search results, fake utility downloads, DLL side-loading, remote management software, process hollowing, multiple persistence methods, and dynamically selected GPU miners. This illustrates why deleting only the visible miner may leave remote access and persistence behind.

03 Signs of unauthorized cryptomining

- High CPU or GPU use while the computer should be idle.
- Fans run continuously, temperatures rise, battery drains quickly, or performance drops.
- A process stops or reduces activity when Task Manager or an analysis tool opens.
- Unfamiliar mining-pool domains, wallet strings, command-line parameters, or outbound connections appear.
- Scheduled tasks, services, startup entries, or scripts recreate the detected file.
- Security exclusions, firewall rules, or update settings change unexpectedly.
- Cloud usage, electricity cost, or infrastructure bills increase without an approved workload.

High CPU or GPU use is not proof of mining. Games, rendering, AI workloads, updates, indexing, backup, and hardware diagnostics can be intensive. Confirm the owning process, executable path, signer, parent, command line, network destinations, and persistence.

04 What the detection path can tell you

Location	Likely question to investigate
Downloads or an archive	Was the suspicious installer or crack ever opened?
Browser cache	Did a site or extension deliver a script, or is the cached object inert?
Temporary or AppData folder	Which process created it, and is a task or loader relaunching it?
Program folder for an approved miner	Do the owner, wallet, pool, and policy match authorized use?
Windows or system-looking path	Is it masquerading as a trusted component or injected into one?
Server web root or cloud instance	Was an internet-facing service or credential compromised?

05 How to remove CoinMiner malware

1. **Disconnect or isolate the device.** This stops pool communication, additional downloads, and remote control while you investigate.
2. **Record the alert.** Preserve the name, path, hash, time, user, parent process, command line, and security action.
3. **Leave the item quarantined.** Do not add an exclusion until ownership and intent are proven.
4. **Run a full updated scan.** Remove the miner, its loader, and any additional detections. Use an offline scan if malware interferes with normal protection.
5. **Check persistence.** Review scheduled tasks, services, startup entries, WMI subscriptions, browser extensions, remote-management tools, and scripts.
6. **Undo malicious security changes.** Remove unauthorized exclusions and restore firewall, update, proxy, and DNS settings.

7. **Patch and rotate access.** If a server or remote account was exploited, close the exposure and reset affected credentials and tokens from a clean system.
8. **Validate after restart.** Confirm that the process, network connection, alert, and abnormal resource use do not return.

For an enterprise server or cloud instance, also review identity logs, new keys, containers, startup metadata, cron jobs, orchestration changes, and billing. Unauthorized mining proves that an attacker obtained execution; it does not prove mining was the only objective.

06 Why CoinMiner keeps coming back

- A downloader or remote-access tool reinstalls it.
- A scheduled task, service, login script, or container restarts it.
- A synchronized folder or shared drive restores the file.
- The vulnerable server or stolen credential remains exposed.
- Only the mining executable was removed, not the initial infection.

Use the creation time and parent process of each new copy. Repeated deletion without finding the creator can hide the real compromise while allowing it to continue.

07 Could CoinMiner be a false positive?

Mining utilities are frequently classified as potentially unwanted applications even when intentionally installed, because they consume resources and are widely abused. Validate a possible false positive by confirming the official source, digital signature or published hash, approved owner, expected path, wallet, pool, command line, and change record.

If it is authorized, use the security product's narrowest documented exception for the exact file or managed deployment. Do not exclude an entire Downloads, Temp, user-profile, or system folder.

08 Prevention

- Enable potentially unwanted application protection and tamper protection.
- Download utilities only from verified vendor sites, not advertisements or mirrors.
- Patch browsers, servers, VPNs, management tools, and exposed applications.
- Require MFA and restrict administrative and remote-management access.
- Use application control and monitor new services, tasks, exclusions, and RMM tools.
- Alert on sustained unexplained CPU/GPU use and connections to mining pools.

09 Frequently asked questions

Is CoinMiner always a Trojan?

No. CoinMiner is often a generic detection or PUA label. It is malicious when installation or use was unauthorized, deceptive, or part of a larger intrusion.

Can a miner damage hardware?

Modern hardware normally throttles at high temperatures, but constant load increases heat, fan wear, power consumption, and instability. Unsafe overclocking or failed cooling raises the risk.

Why does CPU use drop when Task Manager opens?

Some miners pause to avoid discovery, but normal workloads can also change. Correlate the behavior with process and network telemetry rather than relying on this symptom alone.

10 References

- Microsoft Defender for Endpoint: Coin miners
- Microsoft: 2026 GPU mining campaign

- Microsoft Support: Protect against unwanted software

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com