X

XMRig Miner: Legitimate Tool or Malware?

XMRig is a legitimate open-source cryptocurrency miner, but attackers often install modified or unauthorized copies for cryptojacking. Learn how to tell expected mining from compromise and remove an unwanted miner completely.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 What does XMRig do?
02 When is XMRig unsafe?
03 Signs of an unauthorized XMRig miner
04 How unauthorized XMRig gets installed
05 How to remove an unwanted XMRig miner
06 Frequently asked questions

XMRig is a legitimate, open-source cryptocurrency mining application. Its official project describes it as a cross-platform CPU and GPU miner supporting algorithms such as RandomX. A copy that you deliberately downloaded, configured, and authorized is not

automatically malware. However, criminals frequently deploy XMRig or modified versions without the device owner's consent. That unauthorized use is cryptojacking.

This distinction matters: finding the name `xmrig` does not by itself reveal how it arrived. Source, consent, configuration, persistence, and related activity determine whether it is legitimate mining, a potentially unwanted program, or part of a compromise.

01 What does XMRig do?

Mining software performs repeated calculations and submits valid results to a cryptocurrency mining pool or node. The work can consume substantial CPU or GPU capacity, electricity, cooling, and cloud-compute credits. Authorized operators can configure resource use and the destination wallet or pool. An attacker instead hides those choices and receives the proceeds while the victim pays the cost.

02 When is XMRig unsafe?

Expected use	Likely unauthorized use
You installed it from the official project and chose its configuration	It appeared after a crack, fake fix, exposed server, script, or unknown installer
The process, folder, pool, wallet, and startup method are documented	Names and paths are disguised, or the process restarts after termination
Resource use matches an approved schedule	CPU or GPU use rises while the device should be idle
Security exclusions were approved and narrowly scoped	Protection, firewall rules, or exclusions changed unexpectedly
The owner receives the mining proceeds	An unfamiliar wallet or pool receives the work

Security products may flag even an official mining binary as riskware or a potentially unwanted application because the same program is widely abused. Do not create an exclusion until you can verify the file and business purpose.

03 Signs of an unauthorized XMRig miner

- Sustained CPU or GPU use, heat, fan noise, lag, battery drain, or unexpected cloud costs.
- An `xmrig` process, a renamed executable, or an unknown container consuming resources.
- Connections to mining-pool domains or ports that the organization did not approve.
- New scheduled tasks, services, cron jobs, startup scripts, containers, or SSH keys.
- The process stops when monitoring tools open and returns later.
- Unexpected commands, vulnerable internet-facing services, or additional malware detections.

High resource use alone is not proof. Compilers, games, updates, and legitimate workloads can look similar. Confirm the executable path, signer or hash, parent process, launch time, network destination, and owner authorization.

04 How unauthorized XMRig gets installed

Campaigns commonly exploit exposed or unpatched servers, stolen administrative credentials, malicious scripts, cracked software, fake installers, vulnerable web applications, and an earlier malware foothold. On servers, the miner may run inside a container or under a service account. On Windows, persistence may use a service, scheduled task, startup entry, or script. The delivery mechanism changes across campaigns, so deleting a file called `xmrig.exe` does not repair the original access path.

05 How to remove an unwanted XMRig miner

1. **Isolate the device** if compromise is suspected, especially a server or cloud workload.
2. **Preserve evidence:** record the process command line, executable path and hash, parent process, pool address, wallet, user, startup item, and detection time.
3. **Stop mining safely** through incident-response or endpoint tools. Do not rely only on Task Manager; a watchdog may restart it.

4. **Run a full security scan** and investigate services, tasks, cron entries, containers, startup scripts, SSH keys, security exclusions, and recently created accounts.
5. **Close the entry path:** patch exploited software, remove exposed administration, rotate compromised credentials and tokens, and enable MFA.
6. **Rebuild when trust is lost.** Reimage an internet-facing or privileged system if the attacker had administrative access or the full chain cannot be established.
7. **Monitor after recovery** for renewed pool traffic, resource spikes, or recreated persistence.

06 Frequently asked questions

Is XMRig itself a virus?

No. The official project is mining software, not a self-replicating computer virus. An unauthorized installation can still be malicious, and a modified download may include other malware.

Why does antivirus detect an XMRig copy I installed?

Miners are commonly abused, so security tools may classify them as coinminers, riskware, or potentially unwanted software. Verify the download, hash, configuration, and authorization before considering a narrowly scoped exception.

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