XMRig Malware - what it is, easy signs to spot, and how to clean and prevent it

Gridinsoft Help Center

What it is

XMRig malware is a cryptominer that sneaks onto your PC and secretly mines the Monero (XMR) cryptocurrency using your CPU/GPU. You'll notice slower performance, hot fans, and higher power bills while attackers collect the coins. It often arrives through fake installers, cracks, or sneaky scripts on hacked sites. Cleanup tips and examples: https://gridinsoft.com/xmrig

Why it matters

Mining eats your hardware and electricity, making games and apps lag. Miners also open the door for more malware and can run even when you think the PC is idle.

How it works

- Infect: bundled with "free" software, email attachments, or browser drive-bys.
- Hide: drops into user folders, adds startup tasks, and may disable security.
- Mine: connects to a mining pool and maxes out CPU/GPU to earn Monero.
- Persist: auto-restarts if you kill the process or reboot.

Red flags

- Fans roar and the PC is slow even with no apps open.
- CPU/GPU at 90-100% in Task Manager for an unknown process.
- Power bills jump; laptop battery drains fast and runs hot.
- New scheduled tasks or startup items with random names in AppData/Temp.

Do it right

- Uninstall shady apps/extensions; run a full scan with reputable anti-malware.
- Check Task Manager, Startup, and Task Scheduler; remove unknown entries.
- Update Windows, drivers, and browsers; avoid cracks and "activators."
- In browsers, disable unwanted extensions and reset settings.
- After cleanup, change important passwords from a known-clean device.