GRIDINSOFT
HELP CENTER

OFFICIAL SUPPORT GUIDE

C

Cryptojacking: Symptoms, Detection, and Removal

Learn how unauthorized cryptocurrency mining affects computers, servers, browsers, containers, and cloud accounts—and how to respond safely.

PUBLISHER	UPDATED	READ TIME
Gridinsoft Support	Oct 8, 2026	4 min

CONTENTS

In this guide

01 Cryptojacking vs. crypto malware
02 How cryptojacking happens
03 Common signs of cryptojacking
04 How to detect unauthorized mining
05 How to remove cryptojacking malware
06 Cloud cryptojacking response
07 How to prevent cryptojacking
08 Why killing the miner is not enough

Cryptojacking is the unauthorized use of someone else’s computing resources to mine cryptocurrency. Attackers may run mining software on a personal computer, server, cloud virtual machine, container, or compromised account. The direct goal is usually computing power, but the intrusion may also expose credentials and data.

Cryptocurrency mining is not inherently malicious. It becomes cryptojacking when resource owners did not knowingly authorize it or when malware, stolen credentials, or an exploited service is used.

01 Cryptojacking vs. crypto malware

Cryptojacking specifically steals computing resources for mining. The broader phrase **crypto malware** is ambiguous: it may mean a hidden miner, malware targeting cryptocurrency wallets, or older usage referring to ransomware that encrypts files. Check the detected behavior instead of assuming every “crypto” alert performs the same action.

02 How cryptojacking happens

- A malicious attachment, cracked program, fake update, or bundled installer starts a miner.
- An unpatched Internet-facing application is exploited and launches a mining process.
- Stolen cloud credentials create costly virtual machines or serverless workloads.
- A compromised container image or orchestration account deploys miners across a cluster.
- A website runs mining code in a browser tab without meaningful consent.

Host-based miners often add scheduled tasks, services, startup entries, cron jobs, or modified container definitions so they return after a reboot.

03 Common signs of cryptojacking

Endpoints may show sustained CPU or GPU use while idle, loud fans, heat, reduced battery life, slow applications, crashes, or an unfamiliar process that returns after termination. Servers may have unusual load averages, outbound connections, new services, or workloads running under unexpected accounts.

In cloud environments, the first sign may be a cost spike, quota exhaustion, new regions in use, unfamiliar API activity, or many high-compute instances. These symptoms are not proof by themselves; legitimate rendering, indexing, updates, and scientific workloads can look similar.

04 How to detect unauthorized mining

1. Compare current resource use with the system’s normal baseline and identify the responsible process or workload.
2. Check the executable path, signer, parent process, command line, user, start time, and file hash.
3. Review startup items, scheduled tasks, services, cron jobs, containers, and orchestration changes.
4. Inspect DNS and network telemetry for unexpected, repetitive connections to mining infrastructure.
5. Review identity and cloud audit logs for new keys, tokens, roles, instances, functions, images, and regions.
6. Scan with updated endpoint security tools, but do not rely on one detection result.

05 How to remove cryptojacking malware

Disconnect or isolate the affected system when business impact allows. Preserve process, network, identity, and cloud audit evidence before terminating workloads. Stopping the miner may reduce cost and heat, but it does not remove the entry point or persistence.

Quarantine malicious files, remove unauthorized tasks and services, patch the exploited component, and revoke affected sessions, tokens, API keys, and passwords. If privileged access or system integrity is uncertain, rebuild from a known-good image. Restore only necessary data and verify that it does not reintroduce the malware.

06 Cloud cryptojacking response

Contact the cloud provider promptly, especially when charges are rising. Disable compromised identities, preserve audit logs, stop unauthorized resources in every region, and check for hidden persistence such as new federation, roles, access keys, images, functions, pipelines, or billing contacts. Do not delete all evidence before the provider and incident team can review it.

07 How to prevent cryptojacking

- Patch public services and remove unnecessary exposure.
- Use phishing-resistant MFA and short-lived cloud credentials.
- Apply least privilege to users, service accounts, CI/CD, and orchestration systems.
- Allow only trusted software and container images.
- Set cloud budgets, quota alerts, and anomaly detection, while remembering that alerts do not block spending automatically.
- Monitor resource baselines, new workloads, and unusual outbound traffic.
- Use browser and endpoint protections to block known malicious scripts and downloads.

08 Why killing the miner is not enough

A miner proves that an unauthorized party could execute code or control an account. The same access may have been used to steal secrets, change backups, or install another payload. Complete the investigation, determine the initial access method, rotate exposed credentials, search other systems for the same indicators, and verify remediation before returning the resource to service.

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