CS-019 · Malware

Cryptominers

Malicious software that hijacks a device's computing power to mine cryptocurrency for an attacker.

Executive Summary

A cryptominer is malware that secretly uses an infected device's processor or graphics hardware to mine cryptocurrency, sending the proceeds to an attacker. This theft of computing resources, often called cryptojacking, quietly runs in the background, driving up power costs, slowing systems, and wearing out hardware. Because it aims to stay hidden rather than destroy data, it can persist for a long time before anyone notices.

What It Is

Cryptomining is the legitimate process of validating cryptocurrency transactions and earning coins in return, and it consumes large amounts of computing power. A cryptominer, sometimes called a coin miner or cryptojacker, is unauthorized software that performs this work on someone else's hardware without permission so the attacker collects the reward while the victim pays the cost. It can arrive as a standalone program dropped onto a server or laptop, or as a browser-based script that runs while a victim visits a compromised or malicious web page. Unlike ransomware or a wiper, a cryptominer usually does not want to be seen. Its goal is simple, steady, long-term theft of processing capacity, so it often throttles itself to avoid drawing attention.

Why It Matters

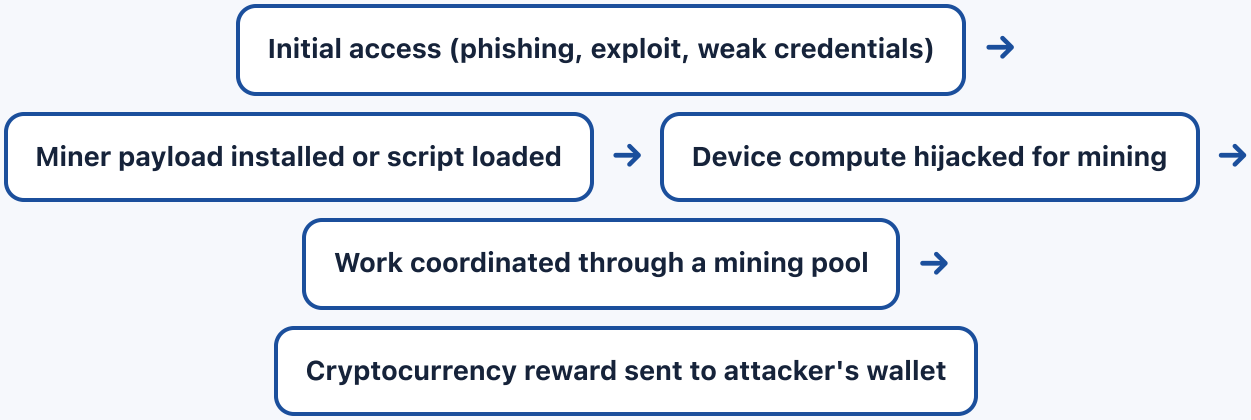
Cryptojacking turns your infrastructure into a profit engine for an attacker. On a laptop it may only mean a hot, sluggish machine and a shorter battery life, but at scale the damage compounds. In a cloud environment an attacker who compromises credentials or exposed services can spin up expensive compute and leave the organization with a large, unexpected bill.

On business servers and industrial systems, sustained maximum load causes overheating, premature hardware failure, and degraded performance for real workloads. Just as important, a cryptominer is a signal: if an attacker can plant one, they had enough access to plant something far worse. Treating a miner as merely a nuisance can mean ignoring a real breach.

How It Works

Attackers gain a foothold through familiar routes: phishing, exploiting an unpatched vulnerability, weak or stolen credentials, malicious software supply chains, or exposed cloud services and container platforms. Once inside, they install the mining payload and connect it to a mining pool, a shared service that coordinates the work and distributes rewards to the attacker's wallet. The miner then consumes processor and graphics resources to solve the computations that earn coins. To stay hidden, it may limit its resource use, pause when a user is active, disguise its process name, and establish persistence so it survives reboots. Browser-based cryptojacking is simpler and needs no installation: a script embedded in a page mines only while the tab is open, which is why closing the page usually stops it.

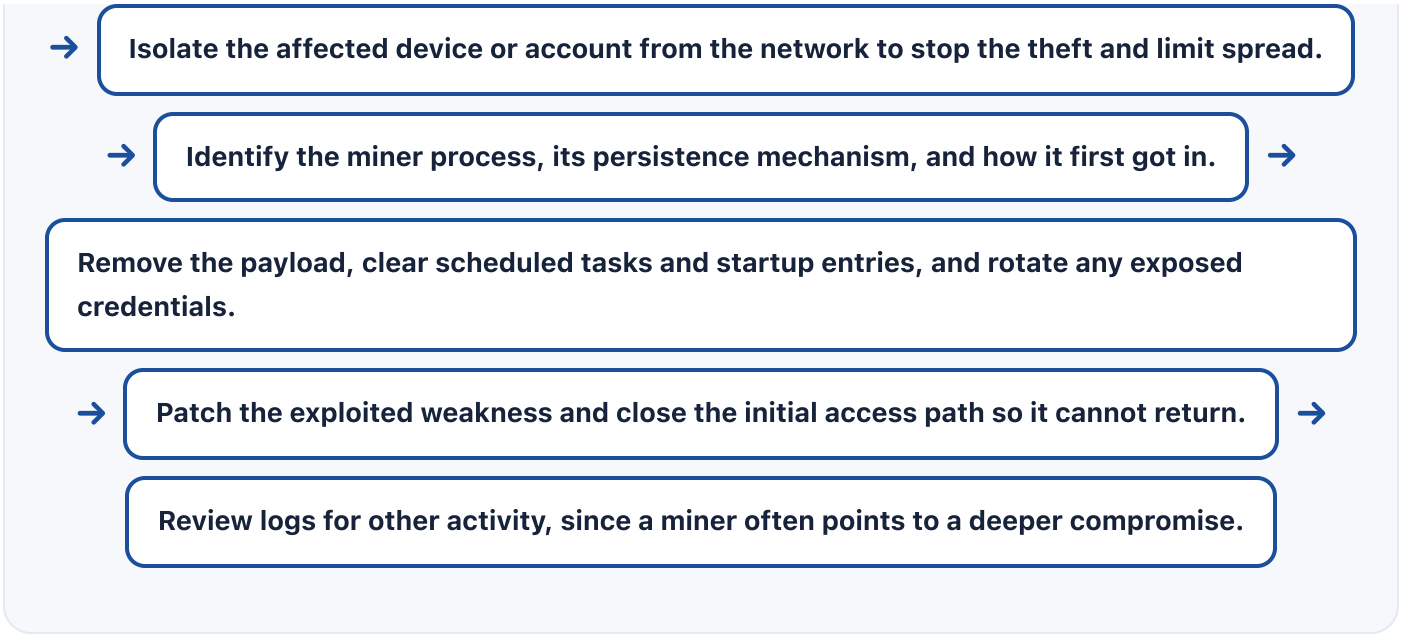
Architecture Diagram



A cryptominer infects a device, quietly consumes its computing power to mine coins, and routes the reward to the attacker.

Visual Workflow

Detect the signs: sustained high processor or graphics usage, overheating, slowdowns, or unexpected cloud spend.



Common Attacks

- Phishing emails that deliver a coin miner as an attachment or link
- Exploitation of unpatched servers and exposed cloud or container services
- Compromised credentials used to run mining on cloud infrastructure
- Malicious browser scripts that mine while a page is open (drive-by cryptojacking)
- Trojanized software, plugins, or supply-chain packages that bundle a miner

Common Mistakes

- Dismissing a miner as a harmless nuisance instead of investigating the breach behind it
- Leaving cloud services, dashboards, and container platforms exposed to the internet
- Ignoring billing anomalies and unexpected spikes in cloud compute costs
- Not monitoring processor and graphics usage or setting alerts for sustained load
- Removing the payload but never closing the vulnerability that let it in

Best Practices

- Patch promptly and reduce the attack surface of internet-facing systems
- Enforce multi-factor authentication and least-privilege access on cloud accounts
- Monitor resource usage and cloud spend, and alert on unusual sustained load

- Use endpoint detection and response to catch mining behavior and persistence
- Restrict which software can run with application allowlisting where practical
- Use browser protections or extensions that block known mining scripts

Quick Checklist

- [x] Baselines for normal processor, graphics, and cloud usage established
- [x] Alerts configured for sustained high load and cloud billing spikes
- [x] Internet-facing services patched and unnecessary ones removed
- [x] MFA and least privilege enforced on cloud and admin accounts
- [x] EDR deployed and tuned to flag mining behavior
- [x] Incident process treats a miner as a possible sign of deeper compromise

Recommended Tools

Endpoint Detection and Response (EDR)
Detects mining processes, persistence, and related malicious behavior

Cloud cost and usage monitoring
Flags unexpected compute spend that can indicate cryptojacking

Network monitoring
Spots traffic to known mining pools and unusual outbound connections

Vulnerability scanner
Finds the unpatched weaknesses attackers use to plant miners

Industry Standards

MITRE ATT&CK: Resource Hijacking (T1496)
Describes the technique cryptominers use to steal compute

NIST SP 800-61
Incident handling guidance for responding to a miner infection

CIS Critical Security Controls
Baseline safeguards that reduce exposure to cryptomining

Career Relevance

Cryptomining shows up daily for SOC analysts triaging resource and billing alerts, incident responders confirming whether a miner masks a larger breach, and security engineers hardening cloud and endpoint environments. Malware analysts study miner families to build detections, and cloud and GRC professionals weigh the cost and risk implications, all part of the audience AI-Governance-Jobs.com serves.

Interview Questions

- What is cryptojacking, and how does it differ from ransomware in intent?
- What signals would make you suspect a device or cloud account is mining cryptocurrency?
- Why should a discovered cryptominer be treated as a potential sign of a larger compromise?
- How does browser-based cryptojacking work, and how do you stop it?
- What controls best reduce the risk of cryptomining in a cloud environment?

Related Certifications

CompTIA Security+ | GIAC GREM | ISC2 Certified in Cybersecurity (CC)

Further Reading

- MITRE ATT&CK: Resource Hijacking
- CISA: Cybersecurity Best Practices
- NIST Cybersecurity Framework

Key Takeaways

- A cryptominer steals a device's computing power to mine cryptocurrency for an attacker.

- Cryptojacking favors stealth and persistence over visible damage, so it often runs unnoticed.
- The clearest signs are sustained high resource use, overheating, and unexpected cloud spend.
- A miner is frequently evidence of a deeper breach, not just a standalone nuisance.
- Patching, MFA, least privilege, and resource monitoring are the strongest defenses.

FAQ

Is cryptomining always malicious?

How can I tell if my computer is cryptojacked?

Does closing my browser stop cryptojacking?

Related Careers

RELATED ROLES

Soc Analyst | Incident Responder | Security Engineer

RELATED CERTIFICATIONS

CompTIA Security+ | GIAC GREM | ISC2 Certified in Cybersecurity (CC)

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Cryptominers**

3. Go deeper: Cybersecurity
4. Go deeper: Ransomware
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

CS-001 Cybersecurity | CS-014 Ransomware | CS-018 Botnets | CS-021 Fileless Malware | CS-081 Patch Management