SECURITY INCIDENT RESPONSE · 14 FEBRUARY – 2 MARCH 2026

Cryptomining via exposed unauthenticated cluster services

CRYPTOMINER | EXPOSED SERVICE | UNAUTHENTICATED API | GPU CLUSTER | SELF-HEALING PERSISTENCE | NETWORK HARDENING

01 Executive summary

Between February and March 2026 the UPNIX team investigated cryptomining malware on a client's GPU compute cluster. The root cause was management and data services exposed to the public internet without authentication: a job-submission dashboard and, on a related node, a database service. Attackers scanning the internet submitted malicious jobs that downloaded a cryptominer and installed self-healing persistence. The UPNIX team identified the entry vector, the full infection pattern and the command-and-control infrastructure, and recommended network isolation of all management ports plus a cluster-wide sweep.

02 Environment

A client's GPU compute cluster built on a distributed job-scheduling framework, with a management node and multiple GPU worker nodes, several of them reachable on public addresses.

03 Entry vector

Two exposed, unauthenticated services were the way in:

- A distributed-computing job dashboard and API reachable on a public address with no authentication — anyone could submit jobs, which the scheduler dispatched to worker nodes and ran as the worker-process account.
- On an earlier, related infection, a database service exposed on a public address that permitted command execution.

In both cases the attacker needed no credentials: internet-wide scanning found the open service, and a submitted job (or query) ran code on the node. SSH was not involved — confirmed by the absence of any corresponding login.

04 Timeline (UTC)

14 Feb 00:57	A malicious job downloads a cryptominer to a worker node and installs a scheduled task for persistence.
14 Feb–2 Mar	The miner runs continuously; the scheduled task re-fetches and re-installs it from command-and-control every few minutes.
2–3 Mar	The UPNIX team maps the infection across nodes, confirms the unauthenticated dashboard as the entry vector, and documents the C2.

05 Findings

- A cryptominer (XMRig) launched under a worker-process account and running for weeks.
- A scheduled task that re-fetched and re-installed the miner from C2 every few minutes, protected with immutable file attributes.
- A C2 payload that removed competing malware, blocked rival miners, and killed high-CPU processes other than its own — typical cryptojacking hygiene.

- The same pattern on a related node through a different exposed service, confirming opportunistic internet-wide scanning rather than a targeted breach.

06 Containment and recommendations

- Block the job dashboard and all cluster management and data ports on public addresses; allow them only from the internal network.
- On infected nodes: kill the miner, remove the downloaded binary and the malicious scheduled task (clearing immutable attributes first).
- Sweep every worker node, since the scheduler can distribute jobs cluster-wide.
- Audit all services on public addresses — no management or data port (job scheduler, database, in-memory store, notebook) should face the internet.

07 Lessons learned

- **Never expose a management or data service to the internet without authentication and network restriction.** Internet-wide scanners find open services within hours.
- **An unauthenticated job-scheduling control plane is remote code execution by design.** Treat it as privileged and keep it on the internal network.
- **Cryptomining persistence is self-healing** and uses immutable file attributes; remove the whole set — binary, scheduled task and attributes — at once.
- **In a cluster, one exposed control plane can seed every worker.** Contain at the network boundary, then sweep all nodes.

This report has been fully anonymized. All client identifiers — organization names, hostnames, domains, IP addresses, account names and storage locations — have been removed. Technical findings, methods and recommendations are retained unchanged so the case remains useful to other operators.

About UPNIX Technologies. The UPNIX team builds, monitors, protects and keeps running the infrastructure businesses depend on — security, 24/7 monitoring and operations for clients worldwide, alongside software and AI engineering.