

Forum:[Hack Forums](#)

Thread: [TeamPCPs Multi-Stage Supply Chain Attack on Security Infrastructure](#)

MadScientist - April 6, 2026, 12:34 pm

Between late February and March 2026, threat group TeamPCP conducted a highly calculated, escalating sequence of supply chain threats. It systematically compromised widely trusted open-source security tools, including the vulnerability scanners Trivy and KICS and the popular AI gateway LiteLLM. The affected software also includes the official Python SDK of Telnyx.

These ongoing supply chain attacks injected malicious infostealer payloads directly into GitHub Actions and Python Package Index (PyPI) registries. Once executed during routine automated workflows, the malware silently extracts highly sensitive data, such as:

- Cloud access tokens
- SSH keys
- Kubernetes secrets

These attacks also establish persistent backdoors for lateral movement across clusters.

The affected software includes:

- BerriAI LiteLLM, an open-source library used to route requests across LLM providers (its documentation states it has over 95 million monthly downloads)

- Aqua Security Trivy and Checkmarx KICS (Keeping Infrastructure as Code Secure), which are embedded in millions of enterprise CI/CD pipelines

- The widely used official Python SDK of Telnyx, a global communications platform providing programmable APIs for voice and messaging

Attackers are believed by sources such as vx-underground to have already exfiltrated data from 500,000 infected machines over 300 GB of data and secrets from 500,000 machines, exposing major organizations across all business verticals to severe follow-on attacks.

Source - <https://unit42.paloaltonetworks.com/teampcp-supply-chain-attacks/>