مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Supply Chain Compromise of LiteLLM via TeamPCP Campaign

Tracking #:432318655
Date:25-03-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a sophisticated supply chain attack attributed to the threat actor TeamPCP has compromised the Python package LiteLLM, specifically versions 1.82.7 and 1.82.8.

TECHNICAL DETAILS:

A sophisticated supply chain attack attributed to the threat actor TeamPCP has compromised the Python package LiteLLM, specifically versions 1.82.7 and 1.82.8. The malicious packages were distributed via PyPI on March 24, 2026, likely following a prior compromise of Trivy within CI/CD pipelines.

The attack introduces a multi-stage payload enabling credential harvesting, Kubernetes cluster compromise, lateral movement, and persistent backdoor installation. Given the automated execution mechanisms embedded in these versions, any environment that installed or executed them should be treated as fully compromised.

This campaign represents a broader escalation in software supply chain attacks, targeting high-trust developer tooling and infrastructure across multiple ecosystems.

Technical Details

Affected Components

- LiteLLM versions: 1.82.7, 1.82.8 (malicious – removed from PyPI)
- Likely infection vector: Compromised Trivy usage in CI/CD pipelines

Attack Chain Overview

The payload operates in three distinct stages:

1. Credential Harvester
    - Targets sensitive data including:
        - SSH keys
        - Cloud provider credentials
        - Kubernetes secrets
        - .env files
        - Cryptocurrency wallets
    - Data is exfiltrated as an encrypted archive (tpcp.tar.gz) via HTTPS to:
        - models.litellm[.]cloud
2. Kubernetes Lateral Movement
    - Uses Kubernetes service account tokens (if available)
    - Enumerates cluster nodes
    - Deploys privileged pods across all nodes
    - Pods:
        - Chroot into host filesystem
        - Install persistence mechanisms on each node
3. Persistence Mechanism
    - Installs a systemd user service:
        - sysmon.service
    - Executes:
        - ~/.config/sysmon/sysmon.py
    - Beaconing:

        - Contacts checkmarx[.]zone/raw every 50 minutes
    - Includes kill-switch logic (e.g., aborts on youtube[.]com response)

Execution Mechanisms

- Version 1.82.7
    - Malicious code embedded in:
        - litellm/proxy/proxy_server.py
    - Triggered at module import time (no user interaction required)
- Version 1.82.8 (Enhanced Threat)
    - Introduces malicious .pth file:
        - litellm_init.pth
    - Automatically executes on every Python interpreter startup
    - Uses subprocess.Popen to:
        - Spawn a background process
        - Decode and execute Base64 payload

Indicators of Compromise (IOCs):

IoC	**Type**	**Status**
litellm==1.82.7	PyPI Package	Removed from PyPI
litellm==1.82.8	PyPI Package	Removed from PyPI
8395c3268d5c5dbae1c7c6d4bb3c318c752ba4608cfcd90eb97ffb94a910eac2	SHA-256 (1.82.7 wheel)	Active IoC
d2a0d5f564628773b6af7b9c11f6b86531a875bd2d186d7081ab62748a800ebb	SHA-256 (1.82.8 wheel)	Active IoC
a0d229be8efcb2f9135e2ad55ba275b76ddcfeb55fa4370e0a522a5bdee0120b	SHA-256 (compromised proxy_server.py)	Active IoC
71e35aef03099cd1f2d6446734273025a163597de93912df321ef118bf135238	SHA-256 (litellm_init.pth, 1.82.8 only)	Active IoC
models.litellm.cloud	C2 Domain (exfiltration)	Active
checkmarx.zone	C2 Domain (persistence)	Active
checkmarx.zone/raw	C2 Endpoint (payload delivery)	Active
~/.config/sysmon/sysmon.py	Filesystem (persistence script)	Active IoC
~/.config/systemd/user/sysmon.service	Filesystem (systemd unit)	Active IoC
/tmp/pglog	Filesystem (downloaded binary)	Active IoC
/tmp/.pg_state	Filesystem (state tracking)	Active IoC
node-setup-* pods in kube-system	Kubernetes (attacker pods)	Active IoC
tpcp.tar.gz	Exfiltration archive name	Active IoC
X-Filename: tpcp.tar.gz	HTTP header (exfiltration POST)	Active IoC

litellm_init.pth	Filesystem (.pth payload, 1.82.8 only)	Active IoC

RECOMMENDATIONS:

1. Immediate Containment Actions

- **Identify and Remove Malicious Versions**
    - Audit environments:

```
pip show litellm
```

-
    - Downgrade to a verified safe version
- **Isolate Affected Systems**
    - Quarantine all hosts that executed affected versions
    - Treat as fully compromised

2. Eradication Steps

- **Remove Persistence**

```
systemctl --user stop sysmon.service
systemctl --user disable sysmon.service
```

-
    - Delete:
        - ~/.config/sysmon/sysmon.py
        - ~/.config/systemd/user/sysmon.service
- **Terminate Malicious Processes**
    - Kill /tmp/pglog processes
    - Remove:
        - /tmp/pglog
        - /tmp/.pg_state

3. Kubernetes Remediation

- Inspect cluster for rogue pods:
    - node-setup-* in kube-system
- Remove all unauthorized pods
- Check all nodes for:
    - /root/.config/sysmon/ persistence artifacts

4. Network-Level Controls

- Block outbound communication to:
    - models.litellm[.]cloud
    - checkmarx[.]zone
- Review logs for historical connections to these domains

5. Credential Security

- **Revoke and rotate all credentials**, including:
    - Cloud IAM keys
    - SSH keys
    - API tokens
    - Kubernetes secrets

6. CI/CD Pipeline Security

- Audit pipelines for:

    - Use of Trivy or KICS during compromise window
- Rebuild pipelines from trusted sources
- Validate integrity of dependencies and artifacts

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://research.jfrog.com/post/litellm-compromised-teampcp/