INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-28 13:43 UTC

DPRK Lazarus Group Positioned to Exploit AI Productivity Gains for Crypto Theft Scale

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0232
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Anthropic Claude Mythos (preview), LiteLLM, Trivy, Safe{Wallet}, Bybit
Published	2026-04-28T00:00:00+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

DPRK-linked Lazarus Group and TraderTraitor are using AI tooling, including compromised third-party contractor access, to accelerate cryptocurrency theft at scale. The February 2026 Safe{Wallet}/Bybit incident and March 2026 LiteLLM supply chain compromise demonstrate that attacker productivity gains, not novel AI capabilities, are widening the operational gap between threat actor velocity and defensive detection speed. Organizations running AI development infrastructure, crypto custody platforms, or third-party-integrated financial services face elevated and immediate risk.

Technical Analysis

This campaign combines supply chain compromise, stolen cloud credentials, and AI-assisted malware development across a multi-stage attack surface. The Safe{Wallet}/Bybit incident (February 2026) exploited third-party contractor access chains to execute a cryptocurrency theft operation. The LiteLLM supply chain compromise (March 2026) involved malicious code inserted into the LiteLLM proxy framework, affecting downstream AI-integrated applications. Trivy, the open-source container scanner, was separately abused as a delivery vector. Anthropic's Claude Mythos preview model was accessed by threat actors via third-party contractor breach, raising dual-use concerns regarding the model's zero-day discovery capability. **Source Quality Note: This assessment is based on T3 sources (vendor blogs and news outlets). Specific technical claims regarding Lazarus attribution, the Bybit incident details, and the scope of Claude Mythos access should be treated as working intelligence pending confirmation from primary sources (CISA, Recorded Future, or law enforcement advisories).** Relevant CWEs: CWE-284 (Improper Access Control), CWE-306 (Missing Authentication for Critical Function), CWE-494 (Download of Code Without Integrity Check), CWE-522 (Insufficiently Protected Credentials). MITRE ATT&CK techniques include T1195.002 (Compromise Software

Supply Chain), T1078.004 (Valid Accounts: Cloud Accounts), T1136.003 (Create Account: Cloud Account), T1566.002 (Spearphishing Link), T1552.001 (Credentials In Files), and T1486 (Data Encrypted for Impact). No CVE IDs have been assigned to this campaign; it does not rely on novel vulnerabilities but on supply chain access control failures and compromised third-party credentials. No vendor patch exists for the underlying access control failures; remediation is architectural. Severity is assessed as critical based on scope, actor capability, and impact breadth.

Action Checklist

1. Step 1: Containment, Audit all third-party and contractor access to AI development environments, crypto custody systems, and cloud infrastructure immediately. Revoke any access tokens or credentials issued to contractors touching Safe{Wallet}, LiteLLM, Trivy, or Anthropic preview environments. Suspend non-essential third-party integrations pending review.
2. Step 2: Detection, Review cloud authentication logs for anomalous account creation (T1136.003) and credential use from unexpected geolocations or service principals (T1078.004). Search for LiteLLM dependency versions pulled between February and March 2026 in CI/CD pipeline logs. Audit Trivy scanner invocations for unexpected network egress or payload downloads. Look for unsigned or integrity-unverified package downloads in build logs (CWE-494).
3. Step 3: Eradication, Pin LiteLLM to a verified, integrity-checked version released after the March 2026 security update (consult https://docs.litellm.ai for the current security advisory, verify this URL is live before following). Re-validate all Trivy scanner binaries against official checksums. Rotate all credentials stored in files or environment variables accessible to compromised build pipelines (CWE-522). Enforce MFA and least-privilege on all cloud accounts with access to AI tooling or financial infrastructure.
4. Step 4: Recovery, After credential rotation, validate that no new cloud accounts were created by unauthorized principals during the exposure window (T1136.003). Monitor crypto wallet and custody system transaction logs for anomalous outbound transfers. Confirm that all third-party contractor access follows documented, approved access control policies with audit trails. Run dependency integrity checks across all AI-integrated services before restoring normal operations.
5. Step 5: Post-Incident, Conduct a third-party access review against the principle of least privilege; contractor access to preview AI models and financial infrastructure in the same access chain is a structural control gap. Implement software supply chain integrity controls (SLSA framework, SBOM generation, signed artifacts) across all AI tooling dependencies. Map contractor access chains to NIST SP 800-53 SA-12 (Supply Chain Protection) and SR-6 (Supplier Assessments and Reviews) controls and document gaps for remediation planning.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership, legal counsel, and relevant financial regulators (FinCEN, applicable state MSB regulators) immediately if any unauthorized outbound crypto transaction is confirmed from Safe{Wallet} or Bybit-integrated custody systems, if PII or private key material is confirmed exfiltrated via compromised LiteLLM pipeline, or if forensic evidence cannot rule out active persistent access by the threat actor within the past 72 hours.

Recovery Notes	Post-containment, maintain elevated monitoring of all Safe{Wallet} signing events and cloud IAM activity for a minimum of 90 days, as Lazarus/TraderTraitor campaigns have demonstrated patience in re-exploiting access chains after initial detection and partial remediation. Before restoring any LiteLLM-integrated service to production, require a passing SLSA provenance verification and SBOM diff against the pre-incident dependency baseline to confirm no residual malicious packages remain. Coordinate with Safe{Wallet} and any Bybit-connected custody platform vendors directly to obtain their own incident timeline and IOC set, as the February 2026 incident demonstrated that the attacker's initial access was through a third-party vendor's compromised developer environment rather than direct organizational infrastructure.
Forensic Artifacts	CI/CD pipeline build logs (GitHub Actions workflow run logs, Jenkins build history) showing 'pip install litellm' invocations between 2026-02-01 and 2026-03-31, including the exact version strings and package hashes pulled — the malicious LiteLLM package would show a hash mismatch against PyPI's verified release checksums for the same version number | AWS CloudTrail or GCP Cloud Audit Log entries for 'CreateUser', 'CreateRole', 'AssumeRole', and 'AttachUserPolicy' events during the exposure window initiated by contractor service principals — Lazarus T1136.003 persistence artifacts would appear as new IAM identities with policy attachments to crypto custody or AI tooling namespaces not matching approved provisioning workflows | Safe{Wallet} Transaction Service API logs and on-chain Gnosis Safe guardian signing events for the February 2026 window, specifically any 'execTransaction' calls where the initiating signer address does not match the organization's documented co-signer roster — the Bybit incident involved manipulation of the signing flow itself, so log entries showing unexpected signer substitution or threshold bypass attempts are primary evidence | DNS resolution logs and outbound network connection records from Trivy scanner execution contexts (CI/CD runner /var/log/syslog or netflow captures) for any domains resolved outside the expected allowlist (aquasecurity.github.io, ghcr.io) during scanner invocations — a backdoored Trivy binary would produce anomalous C2 or exfiltration DNS queries immediately following scan completion | Git repository history and GitHub audit log entries ('GET /orgs/{org}/audit-log') for any workflow file modifications (.github/workflows/*.yml) made by contractor accounts during the exposure window, specifically changes that alter dependency pinning, add new environment variable references, or introduce new external action references — Lazarus supply chain compromises have used workflow poisoning to achieve persistent code execution in victim CI/CD pipelines

Per-Action IR Details

Step 1: Containment — Audit all third-party and contractor access to AI development environments, crypto custody systems, and cloud infrastructure immediately. Revoke any access tokens or credentials issued to contractors touching Safe{Wallet}, LiteLLM, Trivy, or Anthropic preview environments. Suspend non-essential third-party integrations pending review.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), NIST SA-9 (External System Services), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For a 2-person team without a PAM platform: export all IAM users, roles, and active sessions from AWS (aws iam list-users && aws iam list-roles) or GCP (gcloud iam service-accounts list) and cross-reference against a known-good contractor roster. Use 'aws iam list-access-keys --user-name ' to enumerate active keys and 'aws iam update-access-key --status Inactive' to revoke immediately. For GitHub Actions or CI/CD secrets, run 'gh secret list' per repo and revoke all secrets associated with contractor-controlled service accounts. Document each revocation with

timestamp and actor for the post-incident record.

Evidence: BEFORE revoking any access, snapshot the full IAM access key last-used data ('aws iam get-access-key-last-used') for all contractor accounts touching Safe{Wallet} build pipelines and LiteLLM CI/CD environments — this establishes whether keys were used during the February–March 2026 exposure window. Capture cloud provider authentication logs (AWS CloudTrail 'AssumeRole' events, GCP Cloud Audit Logs 'google.iam.admin.v1.CreateServiceAccountKey') showing which principals accessed AI tooling namespaces or crypto custody APIs. Preserve GitHub Actions workflow run logs from repos pulling LiteLLM or Trivy between 2026-02-01 and 2026-03-31 before any branch cleanup or log rotation occurs.

Step 2: Detection — Review cloud authentication logs for anomalous account creation (T1136.003) and credential use from unexpected geolocations or service principals (T1078.004). Search for LiteLLM dependency versions pulled between February and March 2026 in CI/CD pipeline logs. Audit Trivy scanner invocations for unexpected network egress or payload downloads. Look for unsigned or integrity-unverified package downloads in build logs (CWE-494).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a SIEM: query AWS CloudTrail directly using 'aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=CreateUser' filtered to the February–March 2026 window to surface MITRE T1136.003 (Cloud Account Creation) activity. For LiteLLM version tracking, grep CI/CD pipeline logs for 'pip install litellm' or lockfile entries (requirements.txt, poetry.lock) and compare version hashes against PyPI release checksums using 'pip hash'. For Trivy binary integrity, recompute SHA-256 ('sha256sum trivy') against the official release checksums published at github.com/aquasecurity/trivy/releases. Use Sigma rule 'aws_cloudtrail_root_account_usage' and 'proc_creation_win_susp_network_connection' (adapted for Linux CI runners) to detect unexpected egress from scanner processes without a SIEM by running them against exported JSON CloudTrail logs with 'sigma-cli'.

Evidence: Collect PyPI package download receipts and pip audit logs from CI/CD runners for any LiteLLM version installed between 2026-02-01 and 2026-03-31, paying specific attention to versions that deviate from the organization's pinned lockfile. Extract AWS CloudTrail 'ConsoleLogin' and 'AssumeRole' events filtered on source IP geolocation inconsistent with contractor base countries — Lazarus/TraderTraitor operations have historically originated from DPRK-adjacent infrastructure (China, Russia exit nodes). Capture DNS query logs from CI/CD build agents (systemd-resolved logs at /var/log/syslog or /var/log/dns.log) for any resolution of domains not in the expected package registry allowlist (i.e., anything outside pypi.org, files.pythonhosted.org) triggered during Trivy scanner execution.

Step 3: Eradication — Pin LiteLLM to a verified, integrity-checked version released after the March 2026 security update (see https://docs.litellm.ai/blog/security-update-march-2026). Re-validate all Trivy scanner binaries against official checksums. Rotate all credentials stored in files or environment variables accessible to compromised build pipelines (CWE-522). Enforce MFA and least-privilege on all cloud accounts with access to AI tooling or financial infrastructure.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IA-5 (Authenticator Management), NIST CM-2 (Baseline Configuration), NIST SA-12 (Supply Chain Protection), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.2 (Use Unique Passwords), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams without a secrets management platform: use 'grep -rn "LITELLM\|ANTHROPIC_API\|AWS_SECRET" /path/to/repo' and 'git log --all --full-history -S "" ' to identify any credentials committed to git history — use BFG Repo Cleaner to purge before rotating. Pin LiteLLM in requirements.txt with hash enforcement: 'pip install litellm== --require-hashes' using hashes from PyPI's verified release page. Re-download Trivy from github.com/aquasecurity/trivy/releases, verify 'sha256sum -c trivy__checksums.txt', and

replace all CI/CD runner instances of the binary. For MFA enforcement on AWS accounts with no SSO: use 'aws iam list-virtual-mfa-devices' to find accounts without MFA and enforce via SCP or IAM policy 'DenyWithoutMFA' on all roles accessing AI tooling or financial infrastructure.

Evidence: Before rotating credentials, forensically image or export all environment variable stores accessible to compromised CI/CD pipelines — on GitHub Actions, retrieve the audit log ('GET /orgs/{org}/audit-log?phrase=secrets') to determine if secrets were accessed by unauthorized workflows. Preserve copies of the original compromised LiteLLM package (do not delete) in an isolated evidence store with hash documentation, as the malicious package itself is primary forensic evidence of the supply chain compromise. Document the full dependency tree of every service that imported LiteLLM during the exposure window using 'pip show litellm' and 'pipdeptree' outputs — this maps the blast radius for downstream credential exposure under CWE-522.

Step 4: Recovery — After credential rotation, validate that no new cloud accounts were created by unauthorized principals during the exposure window (T1136.003). Monitor crypto wallet and custody system transaction logs for anomalous outbound transfers. Confirm that all third-party contractor access follows documented, approved access control policies with audit trails. Run dependency integrity checks across all AI-integrated services before restoring normal operations.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), NIST AC-2 (Account Management), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.1 (Establish an Access Granting Process)

Compensating: Run 'aws iam generate-credential-report && aws iam get-credential-report' and parse the CSV output to identify any IAM users created after the contractor access event with no corresponding HR onboarding record — flag all accounts created between 2026-02-01 and rotation date as potentially unauthorized (T1136.003). For crypto custody monitoring without a commercial platform, configure webhook alerts on Safe{Wallet} transaction signing events and cross-reference with a known-good signer address whitelist using the Safe Transaction Service API ('GET /api/v1/safes/{address}/transactions/'). Use osquery ('SELECT * FROM users WHERE created > ') on all CI/CD build agents to detect OS-level accounts created during the exposure window.

Evidence: Before restoring any service, capture a final state snapshot of all cloud IAM policies, role bindings, and group memberships as they exist post-rotation — this creates a clean baseline for comparison against the pre-incident state exported in Step 1, and documents the full scope of unauthorized changes attributable to the Lazarus/TraderTraitor intrusion. For Safe{Wallet}-integrated systems, preserve the on-chain transaction history and Safe guardian signing logs for the exposure window as immutable blockchain evidence; this data cannot be altered and provides authoritative proof of any unauthorized transfer attempts originating from compromised signing keys.

Step 5: Post-Incident — Conduct a third-party access review against the principle of least privilege; contractor access to preview AI models and financial infrastructure in the same access chain is a structural control gap. Implement software supply chain integrity controls (SLSA framework, SBOM generation, signed artifacts) across all AI tooling dependencies. Map contractor access chains to NIST SP 800-53 SA-12 (Supply Chain Protection) and SR-6 (Supplier Assessments and Reviews) controls and document gaps for remediation planning.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SA-9 (External System Services), NIST SA-12 (Supply Chain Protection), NIST SR-6 (Supplier Assessments and Reviews), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For SBOM generation without enterprise tooling: use Syft ('syft packages dir:/path/to/project -o syclonedx-json > sbom.json') to generate a CycloneDX SBOM for all AI tooling dependencies including LiteLLM and

Trivy, then scan with Grype ('grype sbom:sbom.json') for known vulnerabilities. Implement SLSA Level 1 minimally by adding 'actions/attest-build-provenance' to GitHub Actions workflows for all AI tooling build pipelines — this generates signed provenance attestations at no cost. Document the Lazarus/TraderTraitor contractor access chain as a threat model entry mapping to MITRE ATT&CK T1195.001 (Compromise Software Dependencies and Development Tools) and T1078.004 (Valid Accounts: Cloud Accounts) to drive detection rule development for future campaigns.

Evidence: Compile the complete lessons-learned artifact package: the timeline of contractor access grants cross-referenced against Safe{Wallet}/Bybit incident dates, all LiteLLM/Trivy dependency versions in use during the exposure window with their provenance (or lack thereof), IAM policy snapshots showing the structural gap where contractor accounts held simultaneous access to AI preview environments and financial infrastructure, and all IOCs (malicious package hashes, unauthorized cloud account identifiers, anomalous IP addresses) formatted for STIX 2.1 sharing with FS-ISAC and CISA's Known Exploited Vulnerabilities reporting channel.

Detection Guidance

Focus detection on four areas. First, cloud account anomalies: alert on new IAM or cloud service account creation (T1136.003) outside approved provisioning workflows, and on logins from unexpected IPs or regions for accounts with access to AI infrastructure or crypto custody systems. Second, supply chain integrity: compare hashes of LiteLLM packages in your environment against the verified post-March-2026 release checksums published in the LiteLLM security update. Flag any dependency pulled without integrity verification (CWE-494). Third, credential exposure: scan build pipeline logs, environment variable stores, and container images for hardcoded credentials or tokens (CWE-522, T1552.001). Fourth, network egress: alert on unexpected outbound connections from Trivy scanner processes or LiteLLM proxy services, particularly to non-standard endpoints or known proxy/anonymization infrastructure (T1090.003, T1041). Behavioral indicators include macOS developer toolchain processes spawning unexpected child processes, and AI API calls originating from build pipeline contexts rather than application runtime contexts.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://docs.litellm.ai/blog/security-update-march-2026`	LiteLLM official security update disclosing the March 2026 supply chain compromise; use to identify affected versions	HIGH
URL	`https://www.legitsecurity.com/blog/when-your-scanner-becomes-the-weapon-from-trivy-to-litellm`	Technical analysis of Trivy scanner abuse chained to LiteLLM compromise; review for indicators specific to your pipeline tooling	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1566.002** — Spearphishing Link
- **T1041** — Exfiltration Over C2 Channel
- **T1078.004** — Cloud Accounts

- **T1136.003** — Cloud Account
- **T1195.002** — Compromise Software Supply Chain
- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1496** — Resource Hijacking
- **T1090.003** — Multi-hop Proxy
- **T1552.001** — Credentials In Files
- **T1195** — Supply Chain Compromise
- **T1059** — Command and Scripting Interpreter
- **T1588.001** — Malware
- **T1583.001** — Domains
- **T1566** — Phishing

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-7** — Continuous Monitoring
- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **SR-2** — Supply Chain Risk Management Plan
- **AC-3** — Access Enforcement
- **CM-3** — Configuration Change Control
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A08:2021** — Software and Data Integrity Failures
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566.002	Spearphishing Link	Initial-Access
T1041	Exfiltration Over C2 Channel	Exfiltration
T1078.004	Cloud Accounts	Defense-Evasion
T1136.003	Cloud Account	Persistence
T1195.002	Compromise Software Supply Chain	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact

Technique ID	Technique Name	Tactic
T1496	Resource Hijacking	Impact
T1090.003	Multi-hop Proxy	Command-And-Control
T1552.001	Credentials In Files	Credential-Access
T1195	Supply Chain Compromise	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1588.001	Malware	Resource-Development
T1583.001	Domains	Resource-Development
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Recorded Future	https://www.recordedfuture.com/blog/lazarus-does-not-need-agi	T3
Anthropic's Claude Mythos Finds Thousands of Zero-Day Flaws ...	https://thehackernews.com/2026/04/anthropics-claude-mythos-finds.html	T3
Bybit Uncovers AI-Assisted macOS Malware Targeting Developers	https://letsdatascience.com/news/bybit-uncovers-ai-assisted-macos-m...	T3
When Your Scanner Becomes the Weapon: From Trivy to LiteLLM	https://www.legitsecurity.com/blog/when-your-scanner-becomes-the-we...	T3
Security Update: Suspected Supply Chain Incident - liteLLM	https://docs.litellm.ai/blog/security-update-march-2026	T3

Generated 2026-04-28 13:43 UTC by TJS Security Command Center