INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-15 15:21 UTC

Technology Sector Under Coordinated State and Criminal Pressure: China-Nexus Actors Lead, DPRK Infiltrates From Within

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0470
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	GitHub repositories, npm ecosystem (Axios package v1.14.1 and v0.30.4), macOS platforms, North American and European technology organizations, mail infrastructure
Discovery Source	Rss:T1 Threatintel

Executive Summary

China-nexus and North Korea-linked state actors are conducting a sustained, coordinated campaign against the technology sector, accounting for more than 58% of state-sponsored intrusions between April 2025 and March 2026. North Korea-linked actors compromised the Axios npm library, downloaded approximately 100 million times per week, embedding a remote access trojan in versions v1.14.1 and v0.30.4, while simultaneously placing fraudulent employees inside technology firms to establish persistent insider access. Organizations that build or ship software using the Axios library face direct supply chain exposure, and those that have hired contractors without rigorous identity vetting face undetected insider threats.

Technical Analysis

This campaign encompasses two distinct DPRK-nexus attack tracks and a broader China-nexus intrusion pattern targeting the technology vertical.

Track 1, Axios npm Supply Chain Compromise: Versions v1.14.1 and v0.30.4 of the Axios npm package were trojanized with a remote access trojan payload delivered via a malicious dependency. The attack aligns with CWE-494 (Download of Code Without Integrity Check) and MITRE T1195.002 (Supply Chain Compromise: Compromise Software Supply Chain). Any build pipeline or production application that installed these versions, whether directly or via transitive dependency, is potentially affected. Axios reaches approximately 100 million weekly downloads across the npm ecosystem, including heavy usage in Node.js backends, frontend toolchains, and CI/CD pipelines. Attribution is linked to DPRK-nexus actors (suspected Lazarus Group affiliation) per reporting from Orca Security, Phoenix Security, Trend Micro, and HivePro.

Track 2, DPRK Insider Placement: DPRK-linked actors placed fraudulent IT workers inside North American and European technology organizations, exploiting authentication weaknesses (CWE-287) and missing authentication controls (CWE-306) during hiring and onboarding. Relevant MITRE techniques include T1078 (Valid Accounts), T1591 (Gather Victim Org Information), and T1650 (Acquire Access). Once embedded, insiders establish persistent footholds aligned with T1534 (Internal Spearphishing) and T1213 (Data from Information Repositories).

Track 3, China-Nexus Intrusions: China-nexus actors conducted the majority of state-sponsored intrusions against the technology sector during the reporting period, focusing on AI capability theft and intellectual property exfiltration. eCrime groups compounded sector pressure with a 30% rise in initial access broker listings and 572 named extortion victims in the technology vertical (CrowdStrike 2026 Technology Threat Landscape Report).

Relevant CWEs: CWE-287, CWE-306, CWE-494. No CVE identifiers are assigned to this campaign in the provided source data.

Action Checklist

1. Step 1: Containment. Immediately audit all package.json, package-lock.json, and yarn.lock files across every build environment and production deployment for Axios versions v1.14.1 and v0.30.4. Block installation of these versions at the artifact repository level (npm registry proxy, Nexus, Artifactory). Isolate any system confirmed to have run these versions until analysis is complete. Source: Orca Security, Phoenix Security, Trend Micro, HivePro advisories on the Axios compromise.
2. Step 2: Detection. Query SIEM and EDR for anomalous outbound network connections from Node.js processes and CI/CD runners, particularly to unfamiliar IPs or domains. Review npm audit logs and build pipeline logs for installation of Axios v1.14.1 or v0.30.4. For insider threat detection, correlate access logs against HR records: flag accounts with unusual access patterns to source code repositories, AI model training data, or IP stores. Relevant log sources: npm install logs, GitHub Actions/CI logs, endpoint network telemetry, identity provider access logs. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) processes. CIS 8.2 (Collect Audit Logs) should already have these sources enabled.
3. Step 3: Eradication. Upgrade Axios to a verified clean version above v0.30.4 and v1.14.1 (consult the official Axios GitHub release history and npm advisory for the designated safe version). Run a full dependency tree audit using 'npm audit' and 'npm ls axios' to identify transitive pulls of the compromised versions. For insider threat cases: revoke access for any contractor or employee flagged during investigation, rotate all credentials and API keys they had access to, and re-image any endpoints they used. Apply NIST AC-6 (Least Privilege) and credential rotation protocols.
4. Step 4: Recovery. After upgrading Axios, rebuild all affected artifacts from source in a clean environment rather than promoting potentially tainted builds. Validate artifact integrity using checksum verification before deployment (aligns with CWE-494 remediation). Re-enable production pipelines only after confirming clean dependency trees. Monitor endpoint and network telemetry for 30 days post-remediation for indicators of residual RAT activity. Apply NIST AU-6 review cadence and confirm CIS 7.3 and CIS 7.4 (automated patch management) are enforcing version controls going forward.
5. Step 5: Post-Incident. Conduct a dependency integrity review: implement subresource integrity checks, npm package lockfile enforcement, and private registry mirroring to prevent future unapproved package versions from entering pipelines. Align with NIST CM controls and CIS 2.1 (Software Inventory) and CIS 2.2 (Ensure Authorized Software is Currently Supported). For insider threat exposure: strengthen contractor identity verification against government-issued documentation, implement NIST AC-2 (Account

Management) with time-limited access grants, and apply multi-factor authentication for all remote and administrative access per CIS 6.3, 6.4, and 6.5. Brief leadership on the sector targeting pattern documented in the CrowdStrike 2026 Technology Threat Landscape Report.

Detection Guidance

Axios Compromise Detection:

- Run 'npm ls axios' in all project directories to identify installed versions. Flag any result returning v1.14.1 or v0.30.4.

- Search package-lock.json and yarn.lock files across repositories for 'axios' entries matching the compromised version strings.

- In EDR/endpoint telemetry, query for Node.js processes (node, npm, npx) initiating outbound TCP connections to external IPs not in your known allowlist, particularly on non-standard ports.

- Review CI/CD pipeline logs (GitHub Actions, Jenkins, GitLab CI) for npm install steps that resolved Axios to the compromised versions during the affected window.

- Check npm audit output: 'npm audit --json' will surface known advisories if the npm registry has published an advisory for these versions.

Insider Threat Detection:

- Cross-reference identity provider (Okta, Azure AD, Google Workspace) access logs against HR records for contractors hired within the past 12 months. Flag accounts with access to source code, AI training datasets, or model weights that do not align with stated job function.

- Alert on bulk data access or download events from code repositories (GitHub, GitLab, Bitbucket), internal wikis, or data stores by contractor accounts, particularly during off-hours.

- Apply NIST AU-6 and local account monitoring to flag anomalous account behavior patterns.

- Review VPN and remote access logs for contractor accounts connecting from geographic locations inconsistent with stated employment location (aligns with NIST AC-17).

Behavioral IOC Patterns:

- Unexpected cron jobs, scheduled tasks, or persistence mechanisms created shortly after Axios-dependent application startup.

- Outbound DNS queries to domains registered within the past 90 days from build servers or application hosts.

- New administrative accounts or SSH keys added to systems that previously ran Axios v1.14.1 or v0.30.4.

Note: No specific IOC hashes, IPs, or domains were provided in the source material. The iocs field reflects this accurately.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`not available in source material`	No specific IOC domains were provided in the referenced advisories for the Axios RAT payload. Consult Orca Security, Trend Micro, Phoenix Security, and HivePro advisories directly for network IOCs as they are published.	LOW
HASH	`not available in source material`	No file hashes for the malicious Axios package versions were included in the provided source data. Check npm advisory records and the referenced vendor reports for package integrity hashes.	LOW

Framework Mappings

MITRE-ATTACK

- **T1608.001** — Upload Malware
- **T1534** — Internal Spearphishing
- **T1204.002** — Malicious File
- **T1133** — External Remote Services
- **T1110.003** — Password Spraying
- **T1195.002** — Compromise Software Supply Chain
- **T1591** — Gather Victim Org Information
- **T1105** — Ingress Tool Transfer
- **T1650** — Acquire Access
- **T1059** — Command and Scripting Interpreter
- **T1566** — Phishing
- **T1567** — Exfiltration Over Web Service
- **T1204** — User Execution
- **T1213** — Data from Information Repositories
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CM-7** — Least Functionality
- **SA-9** — External System Services

- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **CM-3** — Configuration Change Control
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **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(d)** — Person or Entity Authentication

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1608.001	Upload Malware	Resource-Development
T1534	Internal Spearphishing	Lateral-Movement
T1204.002	Malicious File	Execution
T1133	External Remote Services	Persistence
T1110.003	Password Spraying	Credential-Access
T1195.002	Compromise Software Supply Chain	Initial-Access
T1591	Gather Victim Org Information	Reconnaissance
T1105	Ingress Tool Transfer	Command-And-Control
T1650	Acquire Access	Resource-Development
T1059	Command and Scripting Interpreter	Execution
T1566	Phishing	Initial-Access
T1567	Exfiltration Over Web Service	Exfiltration
T1204	User Execution	Execution
T1213	Data from Information Repositories	Collection
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-technology-...	T3
Axios Supply Chain Attack: Analysis & Fix - Orca Security	https://orca.security/resources/blog/axios-npm-supply-chain-attack-...	T3
axios npm Compromised: RAT in v1.14.1 & v0.30.4 (2026)	https://phoenix.security/axios-supply-chain-compromise-npm-rat-2026/	T3
Axios NPM Package Compromised: Supply Chain Attack Hits ...	https://www.trendmicro.com/en_us/research/26/c/axios-npm-package-co...	T3
Axios npm Supply Chain Attack: What You Need to Know - Hive Pro	https://hivepro.com/threat-advisory/axios-npm-supply-chain-attack-w...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-15 15:21 UTC by TJS Security Command Center