INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-14 05:01 UTC

Multi-Vector State and Criminal Campaign Targets Technology Sector: China, DPRK, and eCrime Groups Drive 2025-2026 Intrusion Surge

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0454
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Axios npm package (100M+ weekly downloads), GitHub repositories, macOS systems, North American technology organizations, mail infrastructure
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike's 2026 Technology Threat Landscape Report documents a sustained, coordinated campaign against the technology sector from April 2025 through March 2026, driven by China-nexus state actors, North Korean operatives embedded as fraudulent employees, and organized criminal extortion groups. The Axios npm package, downloaded over 100 million times weekly, was compromised to deliver a remote access trojan, threatening any organization whose software build pipeline consumed affected versions. Technology companies face simultaneous pressure from espionage, insider threat, supply chain sabotage, and ransomware extortion, with 572 organizations named on leak sites during the reporting period.

Technical Analysis

The campaign spans three distinct threat clusters. China-nexus actors account for more than 58% of state-sponsored targeted intrusions against the technology sector, prioritizing persistent access and intelligence collection. DPRK IT worker operatives secured employment inside technology companies under fraudulent identities (T1586.002, T1078) while concurrently executing supply chain attacks, most notably the Axios npm compromise. Malicious versions of the Axios HTTP client were published to the npm registry and dropped a remote access trojan on affected macOS systems (T1195.002, T1195.001). Associated CWEs: CWE-494 (Download of Code Without Integrity Check), CWE-506 (Embedded Malicious Code), CWE-1104 (Use of Unmaintained Third-Party Components). Post-mortem documentation is available via the axios GitHub issue tracker (issue #10636). eCrime groups leveraged phishing (T1566), valid accounts (T1078), external remote services (T1133), and ransomware (T1486) to extort technology organizations at a volume exceeding all other

sectors combined. Additional observed techniques include command execution (T1059), file and directory discovery (T1083), trusted relationship abuse (T1199), and exfiltration to cloud storage (T1567.001). No single CVE ID is associated with the Axios compromise; the attack exploited weak supply chain integrity controls rather than a patchable software vulnerability. Corroborating analysis is available from Trend Micro, Huntress, and StepSecurity.

Action Checklist

1. Step 1: Containment. Audit all active npm dependencies for Axios; identify any version published outside the official axios maintainer release history per the axios GitHub issue #10636 post-mortem. Isolate CI/CD pipelines and build systems that consumed affected versions from production networks until integrity is confirmed. Block outbound connections from build infrastructure to unknown or unexpected remote endpoints.
2. Step 2: Detection. Query npm audit logs and package-lock.json or yarn.lock files across all repositories for anomalous Axios version strings. Search endpoint detection logs on macOS build and developer systems for unexpected process creation events, new persistence mechanisms (T1543), or outbound RAT callback traffic. Review identity and access logs for accounts exhibiting behavior consistent with DPRK insider-threat TTPs: access outside normal hours, bulk data enumeration (T1083), or credential stuffing patterns (T1110.003). Cross-reference employee onboarding records against known DPRK IT worker indicators published by CISA.
3. Step 3: Eradication. Upgrade Axios to a verified clean version confirmed in the axios GitHub issue #10636 post-mortem. Rebuild affected artifacts from clean source in an isolated pipeline environment. Rotate all secrets, tokens, and credentials accessible from compromised build systems (D3-CRO). Remove any unauthorized accounts or persistence mechanisms identified during detection. Apply NIST SI-4 continuous monitoring controls to all build and CI/CD infrastructure.
4. Step 4: Recovery. Re-validate software bill of materials (SBOM) for all products built during the affected window. Deploy subresource integrity checks and configure npm to enforce package signature verification before restoring full pipeline operations (aligned with CWE-494 remediation). Monitor production systems for residual RAT activity for a minimum of 30 days post-remediation. Re-enable CIS 7.3 and CIS 7.4 automated patch management controls with verified-source enforcement.
5. Step 5: Post-Incident. Conduct a formal gap assessment against NIST SP 800-53 Rev. 5 controls SA-12 (Supply Chain Protection) and SR-4 (Provenance) to identify weaknesses in third-party component vetting. Implement D3-MFA on all CI/CD and repository access. Establish a documented process under CIS 6.1 and CIS 6.2 for access granting and revocation that includes identity verification requirements sufficient to detect fraudulent employment. Brief hiring and HR teams on DPRK IT worker indicators. Review extortion exposure by confirming sensitive data inventories align with CIS 3.2 and that data access controls meet CIS 3.3.

Detection Guidance

Supply chain detection: Scan all package-lock.json, yarn.lock, and requirements-equivalent files for Axios versions flagged in the axios GitHub issue #10636 post-mortem. Run 'npm audit' across all active repositories. Compare installed package hashes against hashes published by the official axios maintainer. Flag any Axios version not present in the verified release history on the official npm registry. Endpoint detection (macOS): Hunt

for unexpected child processes spawned by Node.js or npm install scripts, particularly those establishing outbound network connections. Search for new LaunchAgent or LaunchDaemon plist entries created during or after dependency installation, consistent with T1543 persistence. Look for file enumeration activity (T1083) following package installation. Identity and insider threat detection: Audit access logs for accounts that perform bulk data access, connect from atypical geolocations, or exhibit access patterns inconsistent with their stated role. Cross-reference new hire identities against CISA advisories on DPRK IT worker indicators. Review contractor and remote employee identity verification records. eCrime detection: Monitor for credential stuffing patterns against externally exposed applications (T1110.003). Review external remote access logs (VPN, RDP) for unusual session timing or volume (T1133). Alert on large outbound data transfers to cloud storage providers (T1567.001). NIST AU-6 mandates regular audit record review for exactly these behavioral indicators; ensure SIEM rules are tuned to surface them.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://github.com/axios/axios/issues/10636`	Official axios post-mortem documenting malicious npm versions and compromise timeline — primary IOC reference for affected version identification	HIGH

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1195.002** — Compromise Software Supply Chain
- **T1526** — Cloud Service Discovery
- **T1587.001** — Malware
- **T1133** — External Remote Services
- **T1586.002** — Email Accounts
- **T1195.001** — Compromise Software Dependencies and Development Tools
- **T1543** — Create or Modify System Process
- **T1083** — File and Directory Discovery
- **T1078** — Valid Accounts
- **T1059** — Command and Scripting Interpreter
- **T1199** — Trusted Relationship
- **T1608.001** — Upload Malware
- **T1110.003** — Password Spraying
- **T1486** — Data Encrypted for Impact
- **T1567.001** — Exfiltration to Code Repository

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CM-7** — Least Functionality
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **SA-4** — Acquisition Process
- **CM-3** — Configuration Change Control
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A06:2021** — Vulnerable and Outdated Components
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **16.4** — Establish and Manage an Inventory of Third-Party Software Components
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **15.1** — Establish and Maintain an Inventory of Service Providers

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

ISO-27001-2022

- **A.5.29** — Information security during disruption

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

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1195.002	Compromise Software Supply Chain	Initial-Access
T1526	Cloud Service Discovery	Discovery
T1587.001	Malware	Resource-Development
T1133	External Remote Services	Persistence
T1586.002	Email Accounts	Resource-Development
T1195.001	Compromise Software Dependencies and Development Tools	Initial-Access
T1543	Create or Modify System Process	Persistence
T1083	File and Directory Discovery	Discovery
T1078	Valid Accounts	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution
T1199	Trusted Relationship	Initial-Access
T1608.001	Upload Malware	Resource-Development
T1110.003	Password Spraying	Credential-Access
T1486	Data Encrypted for Impact	Impact
T1567.001	Exfiltration to Code Repository	Exfiltration

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-technology-...	T3
Axios NPM Package Compromised: Supply Chain Attack Hits ...	https://www.trendmicro.com/en_us/research/26/c/axios-npm-package-co...	T3

Source	URL	Tier
Tradecraft Tuesday Recap: axios npm Supply Chain Compromise	https://www.huntress.com/blog/axios-npm-compromise	T3
axios Compromised on npm - Malicious Versions Drop Remote ...	https://www.stepsecurity.io/blog/axios-compromised-on-npm-malicious...	T3
Post Mortem: axios npm supply chain compromise #10636 - GitHub	https://github.com/axios/axios/issues/10636	T3

Generated 2026-06-14 05:01 UTC by TJS Security Command Center