INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-15 15:23 UTC

China-Nexus and DPRK Actors Drive Multi-Vector Campaign Against Technology Sector; eCrime Extortion Surges to 572 Named Organizations

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0471
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Technology sector broadly; GitHub repositories; axios npm package (100M+ weekly downloads); macOS platforms; tech organizations across North America, Europe, and Asia
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike's 2026 Technology Threat Landscape Report documents a coordinated multi-vector campaign against the technology sector, with China-nexus actors accounting for more than 58% of observed state-sponsored intrusions and DPRK operatives compromising the axios npm package, used by approximately 100 million projects weekly, to deliver a remote access trojan. DPRK-affiliated personnel also embedded themselves inside technology firms across North America, Europe, and Asia to steal intellectual property and maintain persistent access. Simultaneously, ransomware and extortion groups named 572 technology organizations on leak sites during the reporting period, the highest volume of any sector, compounding nation-state pressure with criminal financial risk.

Technical Analysis

The axios npm supply chain compromise involved DPRK-affiliated actors publishing malicious package versions to npm, deploying a remote access trojan (RAT) against downstream consumers of one of the most widely installed JavaScript HTTP client libraries (~100M weekly downloads). The attack maps to CWE-494 (Download of Code Without Integrity Check), CWE-1357 (Reliance on Insufficiently Trustworthy Component), and CWE-693 (Protection Mechanism Failure). No single CVE ID has been assigned to this campaign item per the provided source data. DPRK fraudulent IT worker operations involve credential and identity abuse (CWE-522), using legitimate-appearing insider access to exfiltrate IP and maintain persistence via valid accounts (T1078) and command scripting (T1059). China-nexus actors drove more than 58% of state-sponsored intrusions, leveraging techniques including supply chain compromise (T1195.001, T1195.002), spearphishing (T1566),

trusted relationship abuse (T1199), and exfiltration to cloud storage (T1567.001). eCrime actors used ransomware deployment (T1486), email collection (T1114), and data from information repositories (T1213) against 572 named technology organizations. Relevant MITRE ATT&CK techniques across all three vectors: T1486, T1213, T1114, T1608.001, T1657, T1199, T1190, T1110.003, T1566, T1195.001, T1195.002, T1059, T1543, T1078, T1567.001.

Action Checklist

1. Step 1: Containment, Immediately audit your npm dependency tree for axios and identify all versions in use across development, CI/CD, and production environments. Pin axios to the latest verified clean release confirmed in the official axios GitHub post-mortem (https://github.com/axios/axios/issues/10636). Freeze npm installs from unvetted package versions until verification is complete. Suspend any contractor or remote worker accounts onboarded without in-person identity verification pending review, per DPRK IT worker TTPs.
2. Step 2: Detection, Query package manager logs, CI/CD pipeline artifacts, and software bill of materials (SBOM) records for axios versions flagged in the StepSecurity and Trend Micro advisories. Search endpoint and server logs for anomalous outbound connections from Node.js processes, unexpected child process spawning from npm-installed packages, and RAT-associated beacon patterns. For insider threat vector: review access logs for unusual bulk data access or exfiltration to cloud storage (T1567.001) by recently onboarded remote contractors. Apply CIS 8.2 (Collect Audit Logs) and NIST AU-6 (Audit Record Review, Analysis, and Reporting) to ensure log coverage across build and runtime environments. Use file integrity monitoring to detect modifications to package lock files and build artifacts.
3. Step 3: Eradication, Upgrade axios to the clean version identified in the official post-mortem. Regenerate any secrets, tokens, or credentials accessible to systems that ran compromised axios versions. Remove unauthorized or unverified contractor accounts; revoke associated SSH keys, API tokens, and VPN certificates. Re-scan all build artifacts produced during the compromise window using file integrity and cryptographic hash verification. Enforce build artifact integrity scanning via CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) post-remediation.
4. Step 4: Recovery, Validate clean axios versions are deployed across all environments by re-running dependency audits post-upgrade. Monitor outbound network traffic from application servers for 30 days post-remediation for residual RAT beacon activity. Re-verify contractor and remote worker identities using out-of-band methods before restoring elevated access. Confirm audit logging is intact per NIST AU-9 (Protection of Audit Information) and CIS 8.2. Restore from known-good build artifacts for any pipeline stages that processed compromised package versions.
5. Step 5: Post-Incident, Implement mandatory SBOM generation for all software releases and enforce cryptographic package integrity checks in CI/CD pipelines, addressing CWE-494 and CWE-1357 gaps. Formalize a vendor and dependency vetting process aligned with NIST AC-20 (Use of External Systems) and CIS 2.1 (Establish and Maintain a Software Inventory). Establish or strengthen insider threat detection controls covering remote contractor onboarding, referencing NIST AC-2 (Account Management), AC-6 (Least Privilege), and file integrity monitoring. Require MFA for all remote access per CIS 6.4 (Require MFA for Remote Network Access) and CIS 6.5 (Require MFA for Administrative Access).

Detection Guidance

For the axios supply chain compromise: compare installed axios package hashes in all environments against hashes published in the official axios post-mortem (https://github.com/axios/axios/issues/10636) and the StepSecurity and Trend Micro advisories. Query npm audit logs and package-lock.json history for version changes during the compromise window. Monitor runtime environments for Node.js processes spawning unexpected child processes, unusual outbound TCP connections from application servers, and file writes to temp directories by npm-installed packages. For DPRK insider threat: flag bulk data access from contractor accounts to source code repositories (T1213), anomalous email forwarding rules (T1114), and large outbound transfers to cloud storage services (T1567.001), cross-reference with NIST AU-6 review cadence. For China-nexus intrusions: hunt for credential stuffing patterns (T1110.003), unexpected trusted relationship access (T1199), and staged data in cloud storage prior to exfiltration (T1567.001). Apply file integrity monitoring to detect modifications to build configuration files and package manifests. Monitor for lateral movement or privilege escalation from contractor or insider accounts. Behavioral indicator: any npm package installation that triggers outbound connections to non-registry infrastructure during install or require() execution.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://github.com/axios/axios/issues/10636`	Official axios post-mortem issue thread documenting compromised npm package versions and clean release confirmations — primary reference for version verification	HIGH

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1213** — Data from Information Repositories
- **T1114** — Email Collection
- **T1608.001** — Upload Malware
- **T1657** — Financial Theft
- **T1199** — Trusted Relationship
- **T1190** — Exploit Public-Facing Application
- **T1110.003** — Password Spraying
- **T1566** — Phishing
- **T1195.001** — Compromise Software Dependencies and Development Tools
- **T1195.002** — Compromise Software Supply Chain
- **T1059** — Command and Scripting Interpreter
- **T1543** — Create or Modify System Process
- **T1078** — Valid Accounts
- **T1567.001** — Exfiltration to Code Repository

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **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
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-3** — Configuration Change Control
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

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

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **15.1** — Establish and Maintain an Inventory of Service Providers

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication

NIST-CSF-2

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

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1213	Data from Information Repositories	Collection
T1114	Email Collection	Collection
T1608.001	Upload Malware	Resource-Development
T1657	Financial Theft	Impact
T1199	Trusted Relationship	Initial-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1110.003	Password Spraying	Credential-Access
T1566	Phishing	Initial-Access
T1195.001	Compromise Software Dependencies and Development Tools	Initial-Access
T1195.002	Compromise Software Supply Chain	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1543	Create or Modify System Process	Persistence
T1078	Valid Accounts	Defense-Evasion
T1567.001	Exfiltration to Code Repository	Exfiltration

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-technology-...	T3
axios Compromised on npm - Malicious Versions Drop Remote ...	https://www.stepsecurity.io/blog/axios-compromised-on-npm-malicious...	T3
Axios NPM Package Compromised: Supply Chain Attack Hits ...	https://www.trendmicro.com/en_us/research/26/c/axios-npm-package-co...	T3
Axios Supply Chain Attack: Analysis & Fix - Orca Security	https://orca.security/resources/blog/axios-npm-supply-chain-attack-...	T3
Post Mortem: axios npm supply chain compromise #10636 - GitHub	https://github.com/axios/axios/issues/10636	T3

Generated 2026-06-15 15:23 UTC by TJS Security Command Center