INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-17 08:02 UTC

Technology Sector Under Sustained State and Criminal Siege: China Dominates Nation-State Targeting While DPRK and eCrime Actors Compound Risk

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0497
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	npm ecosystem (Axios package, specific malicious versions unconfirmed from available sources), GitHub repositories, macOS platforms, North American and East/Southeast Asian technology organizations
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike's 2026 Technology Threat Landscape Report documents a sustained, multi-actor campaign targeting technology sector organizations across North America and East/Southeast Asia. China-nexus adversaries drove more than 58% of state-sponsored intrusions, focusing on intellectual property and AI capabilities; eCrime actors named 572 technology firms on data leak sites, with initial access broker listings rising approximately 30% year-over-year. Concurrently, the widely used Axios npm package was compromised in a supply chain attack that delivered a remote access trojan to downstream software consumers, compounding third-party risk across organizations that depend on JavaScript ecosystems.

Technical Analysis

CrowdStrike's report (coverage April 2025-March 2026) identifies China-nexus actors as the dominant state-sponsored threat to the technology sector, with collection objectives centered on AI assets, semiconductor IP, and strategic technology. DPRK-nexus actors operated under revenue-generation and technology-acquisition mandates consistent with prior campaigns. MITRE techniques active across the campaign set include T1566 (Phishing), T1195.002 (Compromise Software Supply Chain), T1195.001 (Compromise Software Dependencies and Development Tools), T1078 (Valid Accounts), T1133 (External Remote Services), T1213 (Data from Information Repositories), T1041 (Exfiltration Over C2 Channel), T1083 (File and Directory Discovery), T1486 (Data Encrypted for Impact), T1587.001 (Develop Capabilities: Malware),

T1059 (Command and Scripting Interpreter), T1110.003 (Password Spraying), and T1588.006 (Obtain Capabilities: Vulnerabilities). The Axios npm supply chain compromise, documented by Orca Security, StepSecurity, Trend Micro, and the axios GitHub issue tracker, involved malicious package versions delivering a RAT to downstream consumers. Specific malicious version numbers are unconfirmed from available sources; attribution for the Axios event is not established. Relevant CWE mappings: CWE-494 (Download of Code Without Integrity Check), CWE-1104 (Use of Unmaintained Third-Party Components), CWE-287 (Improper Authentication). No CVE ID is associated with this item. Confidence: HIGH for CrowdStrike report statistics; MEDIUM for Axios version-specific technical details.

Action Checklist

1. Step 1: Containment, Audit all production and CI/CD environments for Axios npm package installations; cross-reference installed versions against the axios GitHub issue tracker (https://github.com/axios/axios/issues/10636) to identify any malicious versions. Isolate build pipelines that consumed affected versions until verified clean versions are confirmed. For state-sponsored intrusion exposure, review VPN and external remote access logs (NIST AC-17) for anomalous authentication from unexpected geographies, consistent with T1133 and T1078 activity patterns.
2. Step 2: Detection, Query npm audit logs, package-lock.json, and SBOM records for Axios version entries. Review endpoint and network telemetry for RAT-associated C2 beaconing from systems that executed builds using affected Axios versions. For the broader campaign, monitor SIEM for password-spraying patterns (T1110.003) against externally exposed services; review identity provider logs for impossible-travel or off-hours administrative access consistent with T1078. Enable and review audit records per NIST AU-2 and AU-6, and ensure logs are retained per AU-11. Reference CIS 8.2 for audit log collection completeness across enterprise assets.
3. Step 3: Eradication, Upgrade Axios to a verified clean version confirmed via the official axios GitHub issue tracker post-mortem. Validate package integrity using cryptographic checksums or signed package metadata (addresses CWE-494). Remove any Axios versions identified as malicious from all package caches, artifact registries, and container images. Rotate credentials and API keys on systems where malicious Axios versions executed, per NIST IA controls and D3-CRO (Credential Rotation). For broader campaign exposure, enforce MFA on all externally exposed applications and remote access per CIS 6.3 and CIS 6.4.
4. Step 4: Recovery, Rebuild affected CI/CD pipeline artifacts from clean, verified source. Validate that no malicious Axios version persists in container registries, artifact repositories, or deployed application images. Reconfirm software inventory accuracy per CIS 2.1. Monitor post-remediation network traffic from previously affected build systems for residual C2 activity for a minimum of 30 days. Re-validate access control lists and least-privilege posture on accounts accessed during the incident window per NIST AC-6 and AC-3.
5. Step 5: Post-Incident, Implement or mature software bill of materials (SBOM) generation and continuous third-party dependency monitoring to address CWE-1104 and CWE-494 gaps (aligns with NIST CM controls and CIS 2.1, CIS 2.2). Establish or review supply chain risk management policy to require integrity verification for all third-party packages before build consumption (NIST AC-20). Assess IAB exposure by reviewing dark web monitoring coverage for technology-sector leak site activity. Evaluate whether current threat intelligence subscriptions provide sufficient coverage for China-nexus and DPRK-nexus TTPs mapped above.

Detection Guidance

Supply chain vector: Search SBOM records, package-lock.json files, and artifact registry logs for Axios npm package versions flagged in the axios GitHub issue tracker post-mortem (https://github.com/axios/axios/issues/10636). Query EDR and network monitoring tools for outbound connections from build servers or application hosts running suspect Axios versions; RAT C2 traffic patterns typically include periodic beaconing to non-standard ports or low-reputation domains. Use D3-SFA (System File Analysis) to check for unauthorized modifications to build configuration files or dependency manifests. For state-sponsored intrusion indicators: monitor identity logs for T1110.003 password-spraying patterns (high-volume failed authentications from single or rotating IPs against externally exposed services); alert on T1078 valid account abuse using D3-LAM (Local Account Monitoring) for off-hours or geographically anomalous logins. Apply D3-UAP (User Account Permissions) reviews to identify accounts with privileges inconsistent with current role assignments. NIST AU-6 audit record review and AU-12 audit record generation should be confirmed active across identity providers, VPN concentrators, and cloud access logs. Note: specific IOC hashes, IP addresses, and domains for the Axios RAT are not confirmed in available sources; consult Orca Security, StepSecurity, and Trend Micro reports directly for any published indicators.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://github.com/axios/axios/issues/10636`	Official axios GitHub post-mortem issue tracking the supply chain compromise; consult for malicious version identifiers and remediation guidance	HIGH

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1213** — Data from Information Repositories
- **T1078** — Valid Accounts
- **T1083** — File and Directory Discovery
- **T1041** — Exfiltration Over C2 Channel
- **T1195.002** — Compromise Software Supply Chain
- **T1133** — External Remote Services
- **T1486** — Data Encrypted for Impact
- **T1587.001** — Malware
- **T1059** — Command and Scripting Interpreter
- **T1110.003** — Password Spraying
- **T1195.001** — Compromise Software Dependencies and Development Tools
- **T1588.006** — Vulnerabilities

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
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **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
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CM-3** — Configuration Change Control
- **SA-4** — Acquisition Process
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A06:2021** — Vulnerable and Outdated Components
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **16.4** — Establish and Manage an Inventory of Third-Party Software Components
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **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
T1566	Phishing	Initial-Access
T1213	Data from Information Repositories	Collection
T1078	Valid Accounts	Defense-Evasion
T1083	File and Directory Discovery	Discovery
T1041	Exfiltration Over C2 Channel	Exfiltration
T1195.002	Compromise Software Supply Chain	Initial-Access
T1133	External Remote Services	Persistence
T1486	Data Encrypted for Impact	Impact
T1587.001	Malware	Resource-Development
T1059	Command and Scripting Interpreter	Execution
T1110.003	Password Spraying	Credential-Access
T1195.001	Compromise Software Dependencies and Development Tools	Initial-Access
T1588.006	Vulnerabilities	Resource-Development

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/crowdstrike-2026-technology-...	T3

Source	URL	Tier
Axios Supply Chain Attack: Analysis & Fix - Orca Security	https://orca.security/resources/blog/axios-npm-supply-chain-attack-...	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
Post Mortem: axios npm supply chain compromise #10636 - GitHub	https://github.com/axios/axios/issues/10636	T3

Generated 2026-06-17 08:02 UTC by TJS Security Command Center