

INTELLIGENCE BRIEFING
Security Command Center

TLP: CLEAR
2026-06-15 14:28 UTC

Multi-Front Threat Wave Targets Technology Sector: China-Nexus Espionage, DPRK Supply Chain Attacks, and eCrime Converge in 2025-2026

THREAT CAMPAIGN | HIGH | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0467
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Axios npm package (v1.14.1, v0.30.4; ~100M weekly downloads), GitHub repositories (350+ compromised), OpenClaw AI platform (used as lure), unnamed software development company code repositories (570GB, 28,000 projects)
Discovery Source	Rss:T1 Threatintel

Executive Summary

CrowdStrike's 2026 Technology Threat Landscape Report identifies the technology sector as the most persistently targeted industry, with converging threats from Chinese state-sponsored espionage, North Korean supply chain attacks, and organized eCrime. A reported compromise of the Axios npm package (versions v1.14.1 and v0.30.4), widely used in JavaScript development, injected a remote access trojan into downstream development environments. A parallel campaign is reported to have breached software development repositories, exfiltrating source code and intellectual property. Organizations that build, distribute, or depend on open-source JavaScript libraries face immediate risk of intellectual property theft, ransomware deployment, and unauthorized persistent access across their development pipelines.

Technical Analysis

The Axios npm package, one of the most widely downloaded JavaScript HTTP client libraries, is reported to have been compromised in versions v1.14.1 and v0.30.4 via dependency poisoning (CWE-829) and inclusion of a remote access trojan (CWE-494). The RAT enables persistent command-and-control communication (T1041), arbitrary command execution (T1059), and server-side implant establishment (T1505) within developer workstations and CI/CD environments that installed the malicious versions. A parallel campaign attributed to DPRK-linked actors is reported to have breached software development repositories, consistent with T1213 (Data from Information Repositories) and T1195.001 (Compromise Software Dependencies and Development

Tools). China-nexus actors are significant contributors to state-sponsored intrusions in the sector [per CrowdStrike 2026 Technology Threat Landscape Report], employing valid accounts (T1078), phishing (T1566), and external remote services (T1133) for initial access and long-term persistence (T1543). eCrime initial access brokers are reported to advertise access to technology companies, with social engineering tactics documented across campaigns. CWE-798 (hardcoded credentials) surfaces in compromised developer credential chains. No CVE ID is assigned to this campaign; CVSS base score 9.5 represents the highest-severity component vulnerability in the affected scope. Affected artifacts: Axios npm v1.14.1 and v0.30.4. Safe versions: any release outside these two versions per vendor and Trend Micro guidance.

Action Checklist

- 1. Step 1: Containment.** Audit all package.json, package-lock.json, and yarn.lock files across development, CI/CD, and production environments for Axios versions v1.14.1 or v0.30.4. Immediately block outbound connections from affected build systems pending remediation. Isolate any developer workstation or build agent that installed either compromised version. Apply NIST SP 800-53 AU-6 (Audit Record Review) to ensure audit log coverage spans build agents and developer endpoints.
- 2. Step 2: Detection.** Search SIEM and EDR logs for npm install events referencing axios@1.14.1 or axios@0.30.4. Query endpoint logs for unusual outbound connections or process spawning from Node.js processes. Review CI/CD pipeline execution logs for dependency resolution timestamps coinciding with the compromise window. Apply CIS Controls v8 8.2 (Collect Audit Logs) to ensure log coverage spans build agents and developer endpoints. Inspect node_modules directories for unexpected binaries or modified Axios source files using NIST SI-7 (Software Integrity Verification).
- 3. Step 3: Eradication.** Upgrade Axios to a verified clean version as directed by Trend Micro and Orca Security advisories (see Sources section). Run npm audit or equivalent in all affected repositories. Rotate all credentials, tokens, API keys, and secrets accessible from any environment where the compromised package was installed, per NIST AC-2 (Account Management). Apply CIS Controls v8 7.4 (Perform Automated Application Patch Management) to enforce dependency updates across the enterprise.
- 4. Step 4: Recovery.** After upgrading, re-run full build and test pipelines to confirm clean dependency trees. Verify no new outbound C2 connections originate from previously affected hosts. Monitor for persistence mechanisms: scheduled tasks, service registrations, and modified startup configurations consistent with T1543 and T1505. Apply NIST SI-7 (Software Integrity Verification) to confirm no implants survived remediation. Validate repository integrity for any of the identified GitHub repositories flagged in the campaign scope.
- 5. Step 5: Post-Incident.** Implement software composition analysis (SCA) tooling in CI/CD pipelines to block installation of dependency versions that fail integrity checks, addressing CWE-829 (Inclusion of Functionality from Untrusted Control Sphere) and CWE-494 (Download of Code Without Integrity Check). Enforce CIS Controls v8 2.1 (Establish Software Inventory) and CIS 7.1 (Establish Vulnerability Management Process) for third-party package governance. Apply NIST AC-6 (Least Privilege) to restrict which pipeline roles can install or publish packages. Evaluate insider threat controls given DPRK-linked infiltration tactics documented in the campaign.

Detection Guidance

Primary detection focus: identify installations of Axios v1.14.1 or v0.30.4 in any environment, then hunt for RAT activity originating from Node.js processes. Query package manager logs and lockfiles for exact version strings 'axios@1.14.1' and 'axios@0.30.4'. In EDR, alert on Node.js or npm processes spawning shells (cmd.exe, /bin/sh, /bin/bash) or establishing outbound TCP connections to non-standard ports. In SIEM, correlate npm install timestamps against network connection logs for beaconing patterns. For repository breach indicators (T1213), monitor for bulk git clone or archive operations, especially outside business hours or from unfamiliar source IPs. For credential-based initial access (T1078, T1110.003), alert on authentication events from new geolocations, service account logins to developer portals, and password spray patterns against GitHub, npm registry, or CI/CD platforms. Apply NIST SP 800-53 AU-6 (Audit Record Review) to developer workstations where the RAT may have established local persistence. Detailed IOCs (C2 IP addresses, domain names, file hashes) are provided in the Trend Micro and Orca Security advisories (see Sources). Before ingesting into threat intel platforms, validate IOCs against VirusTotal, WHOIS, and passive DNS records to confirm legitimacy.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	not confirmed in provided source data	Malicious Axios v1.14.1 and v0.30.4 package hashes — retrieve from Trend Micro and Orca Security advisories linked in sources; do not use values from memory	LOW
URL	https://www.trendmicro.com/en_us/research/26/c/axios-npm-package-compromised.html	Trend Micro analysis of Axios npm compromise — IOCs and package hashes expected in this report; human validation of URL resolution recommended	MEDIUM
URL	https://orca.security/resources/blog/axios-npm-supply-chain-attack-remediation/	Orca Security remediation guide for Axios supply chain attack — expected to contain C2 indicators and file integrity details; human validation of URL resolution recommended	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1195.002** — Compromise Software Supply Chain
- **T1133** — External Remote Services
- **T1059** — Command and Scripting Interpreter
- **T1505** — Server Software Component
- **T1486** — Data Encrypted for Impact
- **T1566** — Phishing
- **T1078** — Valid Accounts
- **T1195.001** — Compromise Software Dependencies and Development Tools

- **T1543** — Create or Modify System Process
- **T1041** — Exfiltration Over C2 Channel
- **T1587.001** — Malware
- **T1110.003** — Password Spraying
- **T1588.001** — Malware
- **T1213** — Data from Information Repositories
- **T1087** — Account Discovery

NIST-800-53R5

- **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
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **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

- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **6.3** — Require MFA for Externally-Exposed Applications
- **15.1** — Establish and Maintain an Inventory of Service Providers

- **8.2** — Collect Audit Logs

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.5.21** — Managing information security in the ICT supply chain

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

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

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1195.002	Compromise Software Supply Chain	Initial-Access
T1133	External Remote Services	Persistence
T1059	Command and Scripting Interpreter	Execution
T1505	Server Software Component	Persistence
T1486	Data Encrypted for Impact	Impact
T1566	Phishing	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1195.001	Compromise Software Dependencies and Development Tools	Initial-Access
T1543	Create or Modify System Process	Persistence
T1041	Exfiltration Over C2 Channel	Exfiltration
T1587.001	Malware	Resource-Development
T1110.003	Password Spraying	Credential-Access
T1588.001	Malware	Resource-Development
T1213	Data from Information Repositories	Collection
T1087	Account Discovery	Discovery

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
Axios Supply Chain Attack: Analysis & Fix Orca Security	https://orca.security/resources/blog/axios-npm-supply-chain-attack-...	T3
the WORST hack of 2026 - YouTube	https://www.youtube.com/watch?v=eGSsoSEppNU	T3
axios npm Compromised: RAT in v1.14.1 & v0.30.4 (2026)	https://phoenix.security/axios-supply-chain-compromise-npm-rat-2026/	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 14:28 UTC by TJS Security Command Center