FLASH REPORT

FORTUNE FAVORS THE PREPARED | fortunefavorsthepreprepared.com/dtr/

ISSUED: 01 APRIL 2026 | ~1430 ET | POST-CYCLE | UNCLASSIFIED // OSINT

FLASH | BOTTOM LINE UP FRONT

01 APR 2026 | PREP-CON 3 (ELEVATED)

CYB-F01 | North Korean state actor UNC1069 executed a precision supply chain attack against the axios npm JavaScript library (100M+ weekly downloads), deploying the WAVESHAPER.V2 backdoor (Windows/macOS/Linux) via a compromised maintainer account. Exposure window: ~3 hours (00:21-03:15 UTC 31 MAR). Blast radius estimated at ~600,000 downloads. Formal Google GTIG attribution confirmed 01 APR 2026. **Risk Score: 20/25 (FLASH threshold met).**

RECOMMENDED POSTURE: Immediately audit environments using axios. Check for plain-crypto-js in node_modules. Block C2 IOCs. Rotate credentials from exposure window. See PREP-CON guidance.

CYB-F01 | UNC1069 / AXIOS NPM SUPPLY CHAIN COMPROMISE -- WAVESHAPER.V2

FLASH
RISK: 20/25
L:4 x I:5

SECTOR: CYBER (SEC 4A) | STATUS: NEW | ACTOR: UNC1069 (DPRK/BlueNoroff nexus) | VECTOR: npm Supply Chain | 01 APR 2026 ~1430 ET

SIZE	Package: axios npm -- JavaScript HTTP client library, ~183M combined weekly downloads. Affected versions: 1.14.1 and 0.30.4 (both removed from registry ~03:15 UTC 31 MAR). Estimated exposure: ~600,000 downloads during 3-hour window. Wiz reports malicious versions present in ~3% of scanned enterprise cloud environments. Transitive dependency risk: thousands of packages depend on axios; organizations may be exposed without having directly installed it.
ACTIVITY	Attacker compromised npm maintainer account via long-lived access token (GitHub account also breached). Maintainer email changed to attacker-controlled ProtonMail. Malicious dependency "plain-crypto-js" v4.2.1 pre-staged 18 hours before deployment. Both axios release branches poisoned within 39 minutes of each other. postinstall hook silently executed obfuscated dropper SILKBELL on npm install. Dropper detected host OS, delivered platform-specific WAVESHAPER.V2 payload, then self-destructed and replaced infected files with clean axios -- masking the intrusion. WAVESHAPER.V2 RAT capabilities: system reconnaissance, file system enumeration, command execution, in-memory PE injection, Windows registry persistence. Beacons C2 every 60 seconds via Base64-encoded JSON.
LOCATION	npm registry (global). Any developer workstation, CI/CD pipeline, serverless function, or enterprise backend running npm install during 00:21-03:15 UTC 31 MAR 2026. **C2:** `sfrclak[.]com	142.11.206[.]73	port 8000` **Network IOC:** `User-Agent: mozilla/4.0 (compatible; msie 8.0; windows nt 5.1; trident/4.0)` **Persistence (Win):** `%PROGRAMDATA%\system.bat	MicrosoftUpdate registry run key` **Staging path (macOS):** `/Library/Caches/com.apple.act.mond`
UNIT / ACTOR	**UNC1069** (Google GTIG). North Korea-nexus, financially motivated, active since 2018. Associated with BlueNoroff / Lazarus Group / RGB. Known for 3CX supply chain attack (2023); estimated $200M+ crypto theft 2018-2020.

	Attribution: WAVESHAPER.V2 malware lineage (direct evolution of WAVESHAPER, previously exclusive to UNC1069) + C2 infrastructure overlap via AstrillVPN node historically linked to UNC1069 + macOS build path artifact matching BlueNoroff RustBucket/Hidden Risk tooling (2023). **NOTE:** This attack is confirmed UNRELATED to concurrent UNC6780/TeamPCP campaign (Trivy, LiteLLM poisoning). Two separate nation-state supply chain operations active simultaneously.
TIME	Maintainer account breach: est. ~1800-2000 UTC 30 MAR (18 hrs pre-deployment). Malicious axios 1.14.1 published: 00:21 UTC 31 MAR 2026. Malicious axios 0.30.4 published: ~01:00 UTC 31 MAR 2026. Discovery and removal: ~03:15 UTC 31 MAR 2026 (~3-hr window). GTIG formal attribution: 31 MAR - 01 APR 2026.
EQUIP / METHOD	**Malware:** WAVESHAPER.V2 -- C++ (macOS), PowerShell (Windows), Python (Linux). Full RAT. **Dropper:** `SILKBELL (setup.js) -- self-destructing, OS-aware. SHA256: e10b1fa84f1d6481625f741b69892780140d4e0e7769e7491e5f4d894c2e0e09` **Vector:** Compromised maintainer npm account (long-lived token). No zero-day. Bypasses all package-name verification. Any lockfile pointing to axios@^1.14.0 auto-received the compromised version.

ANALYST ASSESSMENT

Risk Score 20/25 (L:4 x I:5) -- FLASH threshold met. Active, ongoing threat. The self-destructing dropper was engineered to survive post-removal -- environments that ran npm install during the 00:21-03:15 UTC window retain active WAVESHAPER.V2 implants regardless of whether the malicious package version has since been removed from the registry. The threat is not historical; it is present in any unaudited environment.

This attack is architecturally significant. The attacker targeted a legitimate maintainer account -- not a typosquatting package -- bypassing all defenses that rely on package-name verification. The payload was pre-staged 18 hours in advance and built for three operating systems. Execution began before npm finished resolving dependencies. This level of pre-positioning is inconsistent with opportunistic cybercrime and consistent with a nation-state directed operation.

ALTERNATIVE HYPOTHESES

ALT-1 (LOW): False flag by a non-DPRK actor mimicking UNC1069 TTPs. Assessment: LOW. Multiple independent forensic indicators converge (malware lineage, VPN node, ASN history, build path artifacts). If true, the threat level does not materially change.

ALT-2 (LOW-MEDIUM): Primary motive is espionage, not cryptocurrency theft. Given the breadth of developer environments exposed -- including government contractors and critical infrastructure operators -- intelligence collection cannot be ruled out. Financial motivation remains lead hypothesis consistent with UNC1069 history.

ALT-3 -- REJECT: Threat has passed given rapid removal. Rejected. The self-destructing dropper was specifically engineered to persist after package removal. Active implants remain on any unaudited host from the exposure window.

SOURCES

[T1] Google GTIG -- Primary attribution, YARA rules, full IOC set
[T1] SecurityWeek -- Hultquist direct attribution quote
[T1] The Record (Recorded Future) -- Independent corroboration
[T1] Help Net Security -- Blast radius, CI/CD pipeline exposure analysis
[T1] Mondoo -- Network fingerprint and C2 beacon analysis
[T2] The Hacker News -- UNC1069 profile and attribution detail
[T2/DATA] Wiz -- 3% environment exposure figure (enterprise cloud sample; not representative of full npm universe).

END OF FLASH -- CYB-F01

Full DTR | DTR Lite | Daily Preparedness Brief -- fortunefavorstheprepared.com/dtr/