# THE FORENSICS WAY

ISSUE 10 | FORENSICS AWARENESS THIS WEEK | TUESDAY, APRIL 7, 2026

## FRONT PAGE

NATION-STATE SUPPLY CHAIN

### Axios Poisoned: North Korea's UNC1069 Targeted 183 Million Weekly Downloads in a Three-Hour Window

On March 31, North Korea-linked **UNC1069** compromised the npm credentials of Axios maintainer Jason Saayman via targeted social engineering and published two backdoored versions of the most popular JavaScript HTTP client — 1.14.1 and 0.30.4 — with a combined reach of an estimated 183 million weekly downloads across the entire ecosystem.

The malicious packages installed **SILKBELL**, an obfuscated dropper that self-deletes after execution and replaces itself with a clean decoy that passes npm audit. Investigators must check *package-lock.json* files for *plain-crypto-js* as a dependency and hunt CI/CD build logs for unexpected outbound connections during install phases.

CLOUD FORENSICS

### Trust the Scanner, Lose 92 GB: The Trivy Breach That Hit 29 European Union Entities

When the European Commission's automated security pipeline pulled a compromised Trivy update on March 19, it unknowingly harvested an embedded AWS API key — giving attackers five days of undetected access before CERT-EU detected abnormal activity. By March 28, 92 GB of data from 29 EU entities appeared on the ShinyHunters dark web site.

CERT-EU's April 3 attribution report traced a complete forensic chain: poisoned Trivy update → stolen AWS API key → five-day undetected exfiltration. Any organization running Trivy in CI/CD pipelines during March 19–27 should treat cloud credentials as compromised and conduct a full retrospective review of API activity during that window.

## Threat Bulletin

ACTIVE EXPLOIT

**CVE-2026-35616**

Fortinet FortiClient EMS v7.4.5–7.4.6 — Unauthenticated API bypass allows arbitrary code execution on the EMS host; CVSS 9.1. Added to CISA KEV April 6; federal deadline April 9. *Forensic Note:* EMS controls enterprise endpoint policy — review API call patterns and scheduled tasks on the EMS host for unauthorized lateral movement.

HIGH

**CVE-2026-3502**

TrueConf Client — Update mechanism lacks integrity verification, allowing server-side arbitrary executable delivery to all connected endpoints; CVSS 7.8. Exploited against Southeast Asian government networks; CISA KEV April 2. *Forensic Note:* Compare binary hashes to known-good versions; hunt processes spawned from the TrueConf update service.

MALWARE SPOTLIGHT

**WAVESHAPER.V2 (UNC1069)**

North Korea's cross-platform backdoor — PowerShell on Windows, Mach-O on macOS, Python on Linux — delivered via the poisoned Axios npm package, beaconing every 60 seconds. Its dropper SILKBELL self-destructs post-execution, defeating npm audit. *Forensic Note:* Hunt via package-lock.json diffs for plain-crypto-js and outbound C2 connections in CI/CD build logs.

# THE FORENSICS WAY

HISTORICAL ARCHIVES | HISTORY OF DIGITAL INVESTIGATION | TUESDAY, APRIL 7, 2026


## CASE STUDIES: HISTORICAL GRID

XCODEGHOST (2015)

### 4,000 Infected iOS Apps: When China Poisoned the Developer Toolchain Itself

In 2015, Chinese attackers distributed a counterfeit version of Apple's Xcode through domestic file-sharing sites, causing thousands of iOS developers to unknowingly compile malware into their own apps. Over 4,000 infected apps — including WeChat — passed Apple's code-signing process and reached end users worldwide. The case proved developer toolchain compromise is more dangerous than direct payload delivery — the developer becomes an unwitting distributor at scale.

EVENT-STREAM NPM POISONING (2018)

### Ownership Transfer as an Attack Vector: The npm Compromise That Foreshadowed This Week

In November 2018, a malicious contributor convinced the maintainer of event-stream — 2 million weekly downloads — to transfer package ownership, then quietly added a dependency containing a cryptocurrency stealer targeting Copay Bitcoin wallet users. The package sat undetected for two months. The case first demonstrated that npm ownership transfer itself was an attack vector, directly foreshadowing UNC1069's social engineering of the Axios maintainer this week.

MOONLIGHT MAZE (1996–1999)

### The First State Cyber Espionage Campaign — Russia's Multi-Year Infiltration of US Military Networks

From 1996 to 1999, Russian state actors systematically exfiltrated terabytes from US military, NASA, and DoE networks in what became the first publicly attributed state-sponsored cyber espionage campaign — Moonlight Maze. Investigators traced the attack through telephone records and sustained international cooperation, establishing the

OPERATION APT1 / COMMENT CREW (2006–2013)

### The Mandiant Report That Named Names: China's PLA Stole Terabytes From 141 US Organizations

In February 2013, Mandiant publicly attributed years of systematic IP theft to China's PLA Unit 61398 — designating them APT1. The Comment Crew maintained persistent access to 141 US organizations across 20 industries for an average of 356 days per victim, stealing terabytes of intellectual property. The report pioneered the

attribution framework still applied in state-nexus cases today.

modern threat-actor attribution methodology that every state-nexus investigation now follows.

# TOOLS OF THE TRADE

OPEN SOURCE

### Velociraptor

V0.76.1 — MARCH 25, 2026

Endpoint DFIR platform using VQL for fleet-wide hunting and artifact collection. Version 0.76.1 ships with community artifacts specifically targeting the Axios npm supply chain compromise — hunting for plain-crypto-js dependencies and WAVESHAPER C2 URLs across running processes at scale. The fastest path to enterprise-wide WAVESHAPER exposure assessment this week.

OPEN SOURCE

### DFIR-IRIS

V2.4.27 — APRIL 2026

Free collaborative incident response platform for multi-analyst IR teams. Version 2.4.27 introduces live dashboard support — shared views of case status, task completion, and IOC tracking across active incidents. Provides structured case management with timeline building, evidence tracking, and full API integration for SOAR workflows.

UTILITY / SCRIPT

### Axios-SCA-2026 Scripts

COMMUNITY RELEASE — APRIL 2026

Community scripts scanning for the Axios npm supply chain compromise — checking package-lock.json for plain-crypto-js, flagging malicious Axios versions 1.14.1 and 0.30.4, and hunting build logs for unexpected outbound connections. Critical because SILKBELL self-destructs post-execution, making npm audit useless; lockfile diffs are the only reliable forensic indicator.

UTILITY / SCRIPT

### StepSecurity Harden-Runner

GITHUB ACTIONS — ACTIVE 2026

GitHub Actions runtime security tool that monitors and blocks unexpected outbound network calls from CI/CD workflows. Provides step-level network audit trails for every workflow run — capturing outbound connections made during npm install phases that expose WAVESHAPER.V2 C2 beaconing. Would have flagged both the Trivy and Axios supply chain attacks at the install step.

## PRIORITY CVE ADVISORIES

ARCHIVE ALERT

**CVE-2025-53521 (F5 BIG-IP APM)**

Unauthenticated RCE triggered by malicious traffic when an APM policy is active; CVSS 9.3. Added to CISA KEV March 27. *Forensic Note:* BIG-IP APM compromise gives attackers auth-perimeter access — audit all systems that authenticated through it.

ARCHIVE ALERT

**CVE-2026-21643 (FORTICLIENT EMS)**

Pre-auth SQL injection extracts full admin credentials via unsanitized tenant header; CVSS 9.8. 2,000+ exposed instances tracked. *Forensic Note:* Audit EMS policy deployment chains for unauthorized endpoint policy changes.

## RECENT MALWARE WATCH

ARCHIVE: MAR 31, 2026

**INFINITI STEALER (CLICKFIX)**

Python-based macOS infostealer delivered via fake Cloudflare browser verification prompts using Bash one-liners that bypass Gatekeeper. No traditional binary footprint — detection requires script-execution monitoring.

ARCHIVE: MAR 24, 2026

**CANISTERWORM (TEAMPCP)**

Self-propagating npm worm using ICP blockchain C2. Seeded via Trivy supply chain compromise; spread autonomously via stolen npm auth tokens; pivoted to Vect ransomware-as-a-service within eight days.