Smarttech
YOUR 24/7 SECURITY PARTNER

Axios Supply Chain Attack

Contents

Introduction

This document was prepared as a part of the latest threat intelligence research conducted by the Smarttech247 team.

Methodology

This report presents proprietary rising cyber threat data and research from the Smarttech247 threat intelligence team. All the facts and statements about to be presented are gathered based on the information that the Smarttech247 team collects as part of its threat intelligence department.

Overview

On March 31, 2026, the axios npm package (~100M weekly downloads) was compromised. Attackers bypassed GitHub-based CI/CD security by using a stolen long-lived npm token to manually publish two malicious versions: 1.14.1 and 0.30.4.

The attack used a "ghost dependency," plain-crypto-js, which executed a cross-platform Remote Access Trojan (RAT). **Key Finding:** The malware includes a "self-healing" anti-forensic mechanism that swaps its own metadata to evade standard npm list detection.

Attack Timeline

Date/Time	Event
2026-03-30 05:57	Clean decoy plain-crypto-js@4.2.0 published.
2026-03-30 23:59	Malicious plain-crypto-js@4.2.1 published containing obfuscated RAT dropper.
2026-03-31 00:21	axios@1.14.1 published using compromised maintainer credentials.
2026-03-31 01:00	axios@0.30.4 published, also injecting malicious dependency.
2026-03-31 03:15	npm unpublishes both malicious Axios versions.
2026-03-31 03:25	npm security hold placed on plain-crypto-js.

Technical Details

A. The "OIDC" Forensic Signal
Legitimate Axios releases use npm OIDC Trusted Publisher (published via GitHub Actions). The malicious versions lacked the trustedPublisher and gitHead fields in the npm metadata. This confirms the attacker used a classic manual access token, likely stolen from a developer's local machine.

B. Anti-Forensic "Version Spoofing"
The malicious package plain-crypto-js@4.2.1 contains a file named package.md. After the RAT executes, it deletes the malicious package.json and renames package.md to package.json.

- The Trap: The new package.json reports the version as 4.2.0.
- The Result: If you run npm list, it will report the "clean" version 4.2.0, leading you to believe your environment is safe.
- The Fix: Do not trust the version number. If the directory node_modules/plain-crypto-js exists at all, you are compromised.

C. OS-Specific Payload Details

Platform	Malware Vector	Specific Behavior
macOS	Mach-O Universal	Downloads AppleScript (.scpt) to /tmp/, executes via osascript, then unlinks (deletes) the script immediately.
Windows	PowerShell	Installs **persistence** via a hidden batch file in the Run registry key. Targets OneDrive and AppData for data exfiltration.
Linux	Python	Uses DMI (Desktop Management Interface) to detect if it's in a VM/Sandbox before beaconing. Inventories all running processes.

Indicators of Compromise

Malicious Packages

Package	Versions	Notes
axios	1.14.1, 0.30.4	Compromised versions; assume compromise.
plain-crypt-js	4.2.1	Malicious RAT dropper.

C2 Indicators

Type	Indicator
Domain	sfrclak[.]com
IP	142[.]11[.]206[.]73
URL	hxxp[://]sfrclak[.]com:8000/6202033
POST body (macOS)	packages[.]npm[.]org/product0
POST body (Windows)	packages[.]npm[.]org/product1
POST body (Linux)	packages[.]npm[.]org/product2

Disk Artifacts (post-infection)

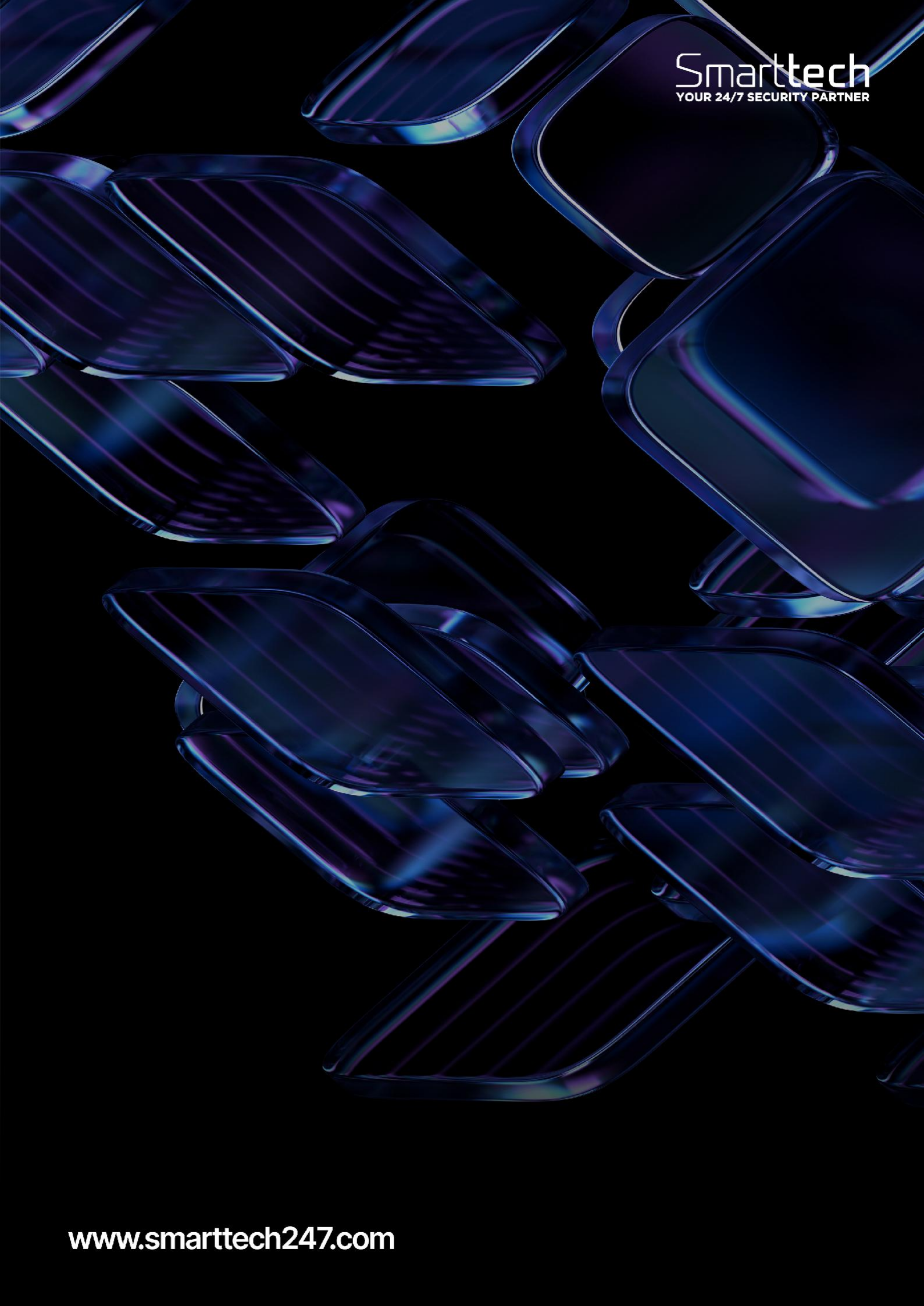
OS	Indicator
macOS	/Library/Caches/com.apple.act.mond
Windows	%PROGRAMDATA%\wt.exe
Linux	/tmd/ld.py

Recommendations

1. Check for malicious axios versions, the hidden dropper package and RAT artifacts on disk.
2. Downgrade to safe Axios versions
    a. `axios@1.14.0` for 1.x
    b. `axios@0.30.0` for 0.x
3. Use an `overrides` block to stop transitive dependencies from resolving to the malicious versions.
4. Remove the malicious dependency `plain-crypto-js`.
5. If any RAT artifacts are found rebuild from a known-good state.
6. Rotate all secrets & credentials
    a. API keys
    b. CI/CD tokens
    c. Authentication credentials
7. Block command-and-control traffic at the network/DNS layer as a precaution on any potentially exposed system.

References

1. https://thehackernews.com/2026/03/axios-supply-chain-attack-pushes-cross.html
2. https://www.aikido.dev/blog/axios-npm-compromised-maintainer-hijacked-rat
3. https://www.stepsecurity.io/blog/axios-compromised-on-npm-malicious-versions-drop-remote-access-trojan
4. https://www.ox.security/blog/axios-compromised-with-a-malicious-dependency



Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com