Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

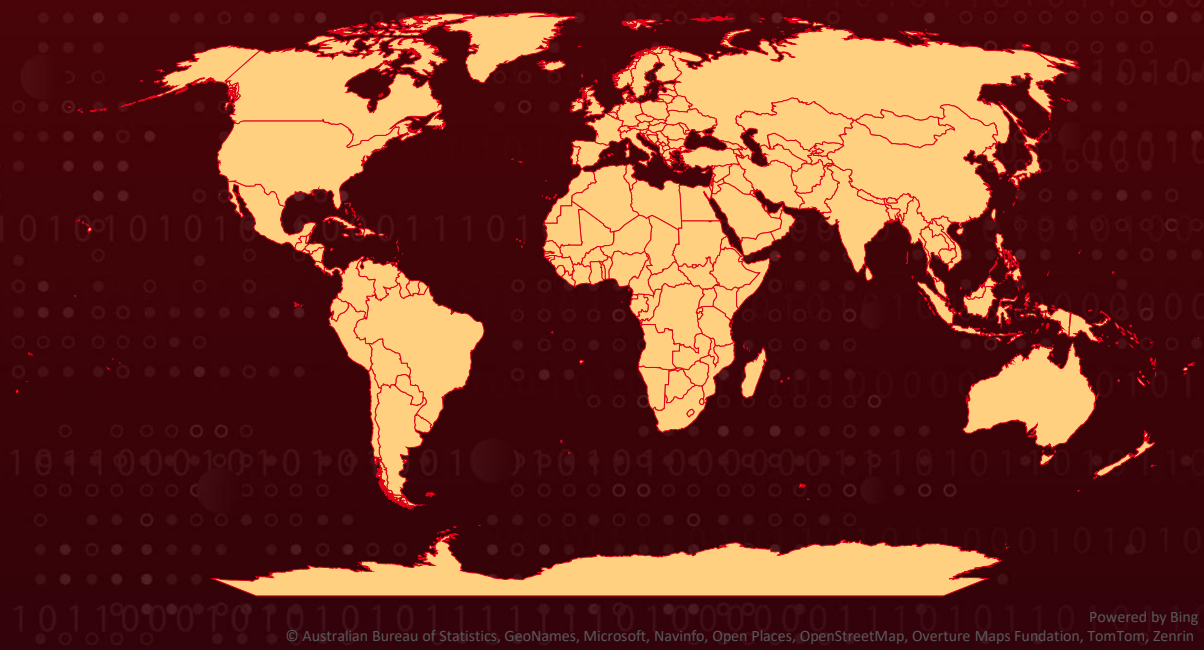
SANDWORM_MODE: npm Supply Chain Attack Targeting AI Development Tools

Date of Publication	Admiralty Code	TA Number
February 25, 2026	A1	TA2026056

Summary

First Seen: February 17, 2026
Targeted Regions: Global
Targeted Platforms: macOS, Linux, Windows
Malware: SANDWORM_MODE
Attack: SANDWORM_MODE, a sophisticated self-propagating npm supply chain worm distributed through 19 typosquatted packages on npm. The malware deploys multi-stage, obfuscated payloads that immediately harvest developer and CI/CD secrets, then bypasses time delays in CI environments to accelerate lateral spread. It hijacks repositories on GitHub by injecting malicious workflows, modifying lockfiles, and abusing repository tokens for propagation. Uniquely, it also poisons AI development toolchains by installing a rogue MCP server to manipulate coding assistants into exposing additional credentials. The campaign highlights an evolution toward hybrid wormable supply chain attacks targeting developer workstations, CI pipelines, and AI-assisted workflows.

Attack Regions



Attack Details

#1 The SANDWORM_MODE campaign, first disclosed by Socket's Threat Research Team on February 20, 2026, is a sophisticated npm supply chain attack involving a self-propagating worm designed to infect developer environments and CI/CD pipelines. Distributed through at least 19 typosquatted packages on npm published under the aliases official334 and javaorg, the malware mimics legitimate libraries to trick developers into installing it. Once executed, it deploys multi-stage, heavily obfuscated payloads that immediately begin harvesting sensitive credentials from infected systems.

#2 The attack operates in phases. An initial loader decodes and executes encrypted payloads directly in memory, followed by rapid credential theft targeting npm tokens, cloud credentials, SSH keys, and environment secrets. A delayed second stage, protected behind a 48-hour time gate with encrypted payloads, activates deeper persistence and propagation mechanisms, including modifications to project files and CI workflows. In CI environments, the delay is bypassed entirely to accelerate spread and maximize token theft. Stolen data is exfiltrated through multiple channels, including HTTPS endpoints, GitHub repository uploads, and DNS tunneling, ensuring redundancy if any single path is blocked.

#3 A core feature of the campaign is CI/CD hijacking, particularly targeting repositories hosted on GitHub. The malware injects malicious GitHub Actions workflows such as quality.yml, modifies lockfiles, and abuses repository tokens to move laterally across projects. It leverages attacker-controlled infrastructure, including a GitHub organization named ci-quality, to host and distribute its payloads. The worm also establishes persistence via global Git configuration changes, ensuring newly initialized repositories inherit malicious hooks even after the original package is removed.

#4 What distinguishes this campaign from earlier npm worms is its focus on AI toolchain poisoning. The malware installs a rogue local MCP (Model Context Protocol) server into a hidden directory and registers it with developer AI assistants and coding tools using innocuous-sounding tool names. Through prompt injection and configuration tampering, it manipulates AI systems into silently exposing additional secrets, including API keys for large language model providers. This represents a significant evolution in supply chain attacks, expanding the threat surface beyond traditional build systems into AI-assisted development environments.

#5 The campaign demonstrates a shift from traditional package-level compromise toward a hybrid model combining wormable supply chain infection, CI/CD pipeline hijacking, and AI toolchain manipulation.

Recommendations

Audit npm Dependencies for Typosquatted Packages: Immediately review all project dependencies against the list of 19 known malicious packages associated with SANDWORM_MODE (e.g., `claud-code`, `cloude-code`, `suport-color`, `rimarf`, `yarsg`). Remove any matches and rotate all credentials that may have been exposed.

Rotate and Revoke All Exposed Credentials: Immediately revoke and rotate npm tokens, GitHub personal access tokens, CI/CD secrets, cloud provider keys, SSH keys, and LLM API keys. Assume any credential present on an affected system may have been harvested. Replace long-lived tokens with scoped, least-privilege, short-lived credentials to reduce blast radius.

Inspect and Secure CI/CD Workflows: Review all CI/CD workflows for unauthorized YAML files, unexpected steps, or external repository references. Pay close attention to modifications within .github/workflows/ and changes to lockfiles without corresponding dependency updates. Enforce branch protections and require approval for workflow changes.

Check for Git-Based Persistence Mechanisms: Inspect global Git configuration for tampering, particularly changes to init.templateDir that could propagate malicious hooks. Remove unknown Git hook templates and validate repository-level hooks. Persistence at the Git level can survive package removal if not explicitly addressed.

Implement Least-Privilege: Reduce permissions of CI tokens and GitHub automation credentials to the minimum required. Scope secrets per environment and disable unnecessary write access. Monitor developer endpoints and CI runners for anomalous outbound HTTPS traffic or DNS patterns indicative of data exfiltration.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1195: Supply Chain Compromise	T1195.002: Compromise Software Supply Chain
		T1195.001: Compromise Software Dependencies and Development Tools
Execution	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
Persistence	T1546: Event Triggered Execution	
Credential Access	T1555: Credentials from Password Stores	T1555.005: Password Managers
	T1552: Unsecured Credentials	T1552.001: Credentials In Files
Collection	T1119: Automated Collection	
Exfiltration	T1048: Exfiltration Over Alternative Protocol	T1048.001: Exfiltration Over Symmetric Encrypted Non-C2 Protocol
	T1567: Exfiltration Over Web Service	T1567.001: Exfiltration to Code Repository
Lateral Movement	T1072: Software Deployment Tools	
Defense Evasion	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
Impact	T1485: Data Destruction	
Resource Development	T1583: Acquire Infrastructure	T1583.006: Web Services

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	5ce544f624fd2aee173f4199da62818ff78deca4ba70d9cf33460974d460395c, 5440e1a424631192dff1162eebc8af5dc2389e3d3b23bd26e9c012279ae116e4
Domains	freefan[.]net, fanfree[.]net
URLs	hxxps[:]//pkg-metrics[.]official334[.]workers[.]dev/exfil, hxxps[:]//pkg-metrics[.]official334[.]workers[.]dev/drain, hxxp[:]//localhost[:]11434/api/tags, hxxp[:]//localhost[:]11434/api/generate, hxxp[:]//localhost[:]1234/v1/models, hxxp[:]//localhost[:]5000/v1/models, hxxp[:]//localhost[:]8000/v1/models, hxxp[:]//localhost[:]8080/v1/models, hxxp[:]//localhost[:]4873
Malicious npm Packages	claud-code@0.2.1, cloude-code@0.2.1, cloude@0.3.0, crypto-locale@1.0.0, crypto-reader-info@1.0.0, detect-cache@1.0.0, format-defaults@1.0.0, hardhta@1.0.0, locale-loader-pro@1.0.0, naniod@1.0.0, node-native-bridge@1.0.0, opencraw@2026.2.17, parse-compat@1.0.0, rimarf@1.0.0, scan-store@1.0.0, secp256@1.0.0, suport-color@1.0.1, veim@2.46.2, yarsg@18.0.1
npm Publisher Alias	official334, javaorg
Email Address	Official334[@]proton[.]me, JAVAorg[@]proton[.]me

TYPE	VALUE
GitHub User	official334
GitHub Organization	ci-quality
GitHub Repository	ci-quality/code-quality-check (tags: v1, v1.0.0)
Malicious Workflow File	.github/workflows/quality.yml
DGA Seed	sw2025
Persistence Mechanism	git config --global init.templateDir (malicious template directory)
Hidden Directory	~/.dev-utils/ (rogue MCP server location)

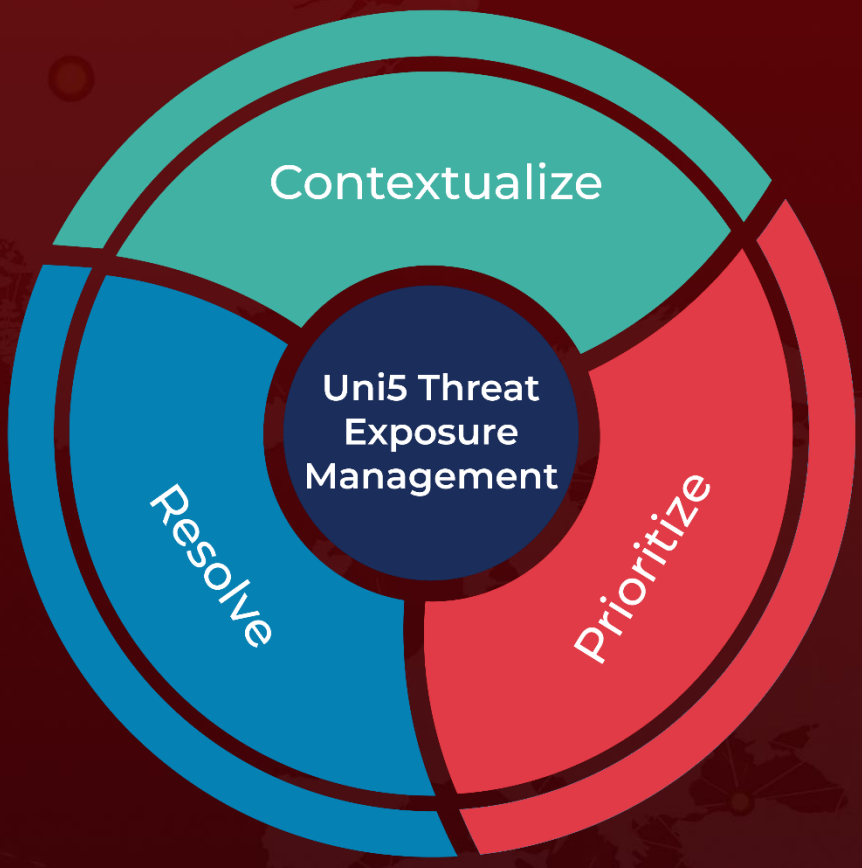
References

https://socket.dev/blog/sandworm-mode-npm-worm-ai-toolchain-poisoning

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 25, 2026 • 05:30 AM

More at www.hivepro.com