Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

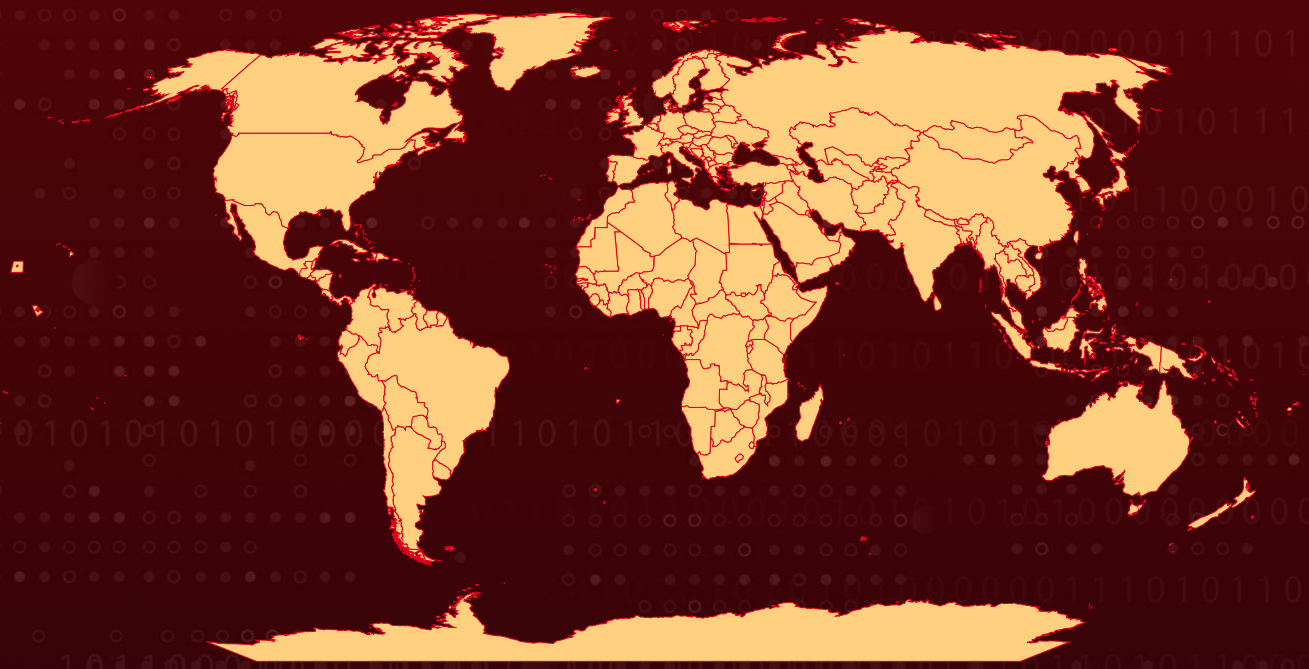
Shai-Hulud: Massive npm Supply Chain Attack Infects Hundreds of Packages

Date of Publication	Admiralty Code	TA Number
September 18, 2025	A1	TA2025288

Summary

First Seen: September 5, 2025
Targeted Region: Worldwide
Targeted Platforms: npm ecosystem, GitHub repositories
Malware: Shai-Hulud
Attack: A major supply chain attack, dubbed “Shai-Hulud,” is targeting the npm ecosystem through phishing campaigns against maintainers, allowing attackers to compromise accounts and inject self-propagating malware into popular packages. The malicious code, often hidden in bundle.js, scans for and exfiltrates secrets while some variants attempt to expose private repositories and deploy malicious GitHub Actions. With at least 180 and possibly over 500 packages affected, including widely used utilities and vendor libraries, the incident represents one of the most severe threats to the JavaScript ecosystem.

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

A large-scale supply chain attack is currently unfolding in the npm ecosystem, tracked under the codename “Shai-Hulud.” The campaign began with targeted phishing campaigns against npm maintainers, which allowed attackers to gain initial access to trusted accounts. Once inside, they injected malicious code into legitimate open-source packages, enabling the malware to spread in a worm-like manner by automatically modifying other projects maintained by the same author. This self-propagating behavior makes the incident especially dangerous, as the compromise rapidly escalates beyond a single package.

#2

The malicious payload is typically embedded in a bundle.js file or similar script that executes during installation. It scans the host environment for secrets such as API keys, tokens, and cloud credentials, validating them and exfiltrating the results to attacker-controlled endpoints. Some variants go further, attempting to make private repositories public or insert malicious GitHub Actions workflows, thereby heightening the risk of persistent access and additional data leakage across developer environments and CI/CD pipelines.

#3

The scale of impact is significant, with estimates ranging from at least 180 confirmed packages to possibly over 500 affected so far. These include not only widely used utilities like chalk, ansi-styles, and strip-ansi, but also packages published by major vendors. Together, these compromised projects account for billions of weekly downloads, meaning a large number of developers and enterprises may have unknowingly integrated malicious code through both direct and transitive dependencies.

#4

This incident follows earlier compromises in the ecosystem, such as the s1ngularity/Nx breach, which involved credential theft and the exposure of private repositories. By combining phishing, worm-like propagation, and credential exfiltration, this campaign represents one of the most aggressive and far-reaching supply chain attacks the JavaScript ecosystem has faced to date. It highlights the fragility of open-source trust models and the risks posed when attacker-controlled code is distributed under the guise of legitimate projects.

Recommendations

Audit and Pin Dependencies: Organizations should immediately review their lockfiles (package-lock.json, yarn.lock, pnpm-lock.yaml) to identify if any compromised versions are present. Dependencies should be pinned to known safe versions rather than relying on floating ups like latest.

Rotate and Secure Credentials: Since the attack harvests API keys, tokens, and secrets, perform a comprehensive rotation of all accessible credentials, including npm tokens, GitHub personal access tokens, CI/CD secrets, and cloud provider keys. Ensure all authentication tokens adhere to the principle of least privilege, minimizing the scope of potential misuse.

Harden Maintainer and Developer Accounts: Enforce strict authentication controls on all package maintainer and developer accounts. Require hardware-based or app-based two-factor authentication, limit account access to essential personnel, and provide ongoing phishing awareness training to mitigate social engineering risks.

Strengthen CI/CD Pipelines: Harden build pipelines by enforcing immutable infrastructure principles and isolating build environments to prevent persistent access to secrets. Monitor and restrict modifications to GitHub Actions workflows, and implement automated malware and security scanning integrated into CI/CD processes to detect malicious dependencies early.

Monitor and Respond to Suspicious Activity: Continuously monitor logs, network connections, and telemetry for unusual behaviors such as outbound connections to attacker endpoints (e.g., webhook.site), unexpected publication or visibility changes in repositories, and abnormal runtime activity consistent with injected malware.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	**TA0001** Initial Access	**TA0002** Execution	**TA0011** Command and Control
TA0003 Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0040** Impact
TA0008 Lateral Movement	**TA0009** Collection	**TA0010** Exfiltration	**TA0006** Credential Access
T1204 User Execution	**T1027** Obfuscated Files or Information	**T1059** Command and Scripting Interpreter	**T1068** Exploitation for Privilege Escalation
T1204.002 Malicious File	**T1567** Exfiltration Over Web Service	**T1195.002** Compromise Software Supply Chain	**T1195** Supply Chain Compromise
T1119 Automated Collection	**T1528** Steal Application Access Token	**T1072** Software Deployment Tools	**T1098** Account Manipulation
T1566 Phishing	**T1566.002** Spearphishing Link	**T1059.007** JavaScript	**T1586** Compromise Accounts
T1059.004 Unix Shell	**T1550.001** Application Access Token	**T1550** Use Alternate Authentication Material	**T1078** Valid Accounts
T1555 Credentials from Password Stores	**T1195.001** Compromise Software Dependencies and Development Tools		

Indicators of Compromise (IOCs)

TYPE	VALUE
Email	support[@]npmjs[.]help
URL	hxxps[://]webhook[.]site/bb8ca5f6-4175-45d2-b042-fc9ebb8170b7
Domain	npmjs[.]help
SHA256	46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09, b74caeaa75e077c99f7d44f46daaf9796a3be43ecf24f2a1fd381844669da777, dc67467a39b70d1cd4c1f7f7a459b35058163592f4a9e8fb4dffcbba98ef210c, 4b2399646573bb737c4969563303d8ee2e9ddbd1b271f1ca9e35ea78062538db, de0e25a3e6c1e1e5998b306b7141b3dc4c0088da9d7bb47c1c00c91e6e4f85d6, 81d2a004a1bca6ef87a1caf7d0e0b355ad1764238e40ff6d1b1cb77ad4f595c3, 83a650ce44b2a9854802a7fb4c202877815274c129af49e6c2d1d5d5d55c501e

References

https://www.csa.gov.sg/alerts-and-advisories/advisories/ad-2025-019

https://threatprotect.qualys.com/2025/09/17/multiple-npm-packages-affected-by-the-ongoing-supply-chain-attack-shai-hulud-malware/

https://www.trendmicro.com/en_us/research/25/i/npm-supply-chain-attack.html

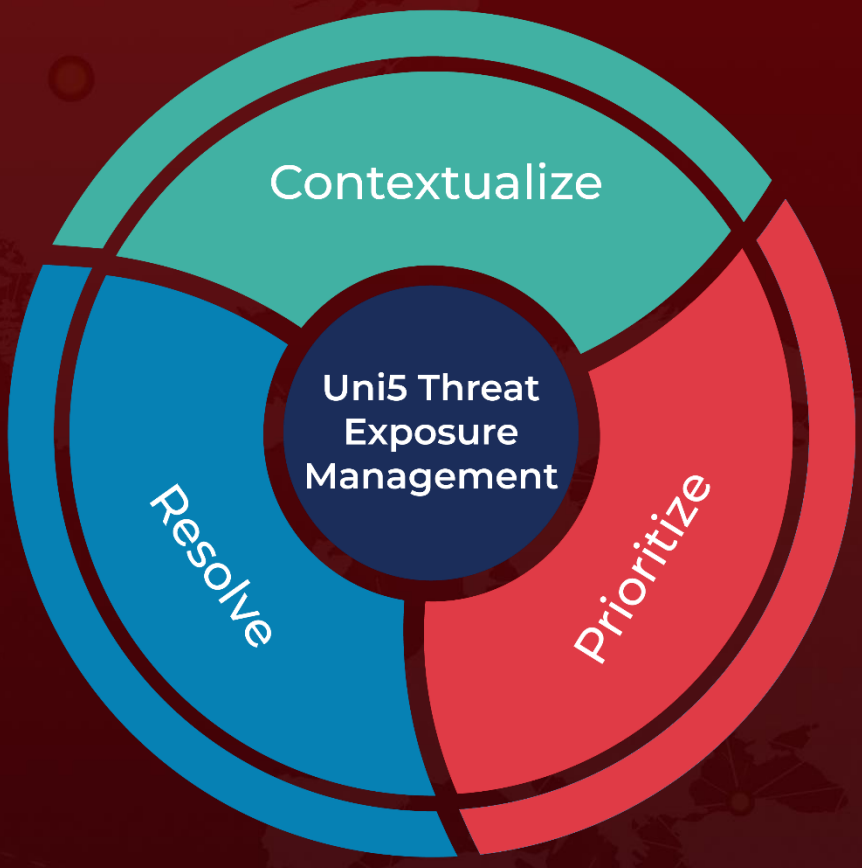
https://unit42.paloaltonetworks.com/npm-supply-chain-attack/

https://hivepro.com/threat-advisory/s1ngularity-nx-supply-chain-attack-ai-driven-credential-theft-mass-exposure/

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

September 18, 2025 . 11:30 PM

© 2025 All Rights are Reserved by Hive Pro

More at www.hivepro.com