Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

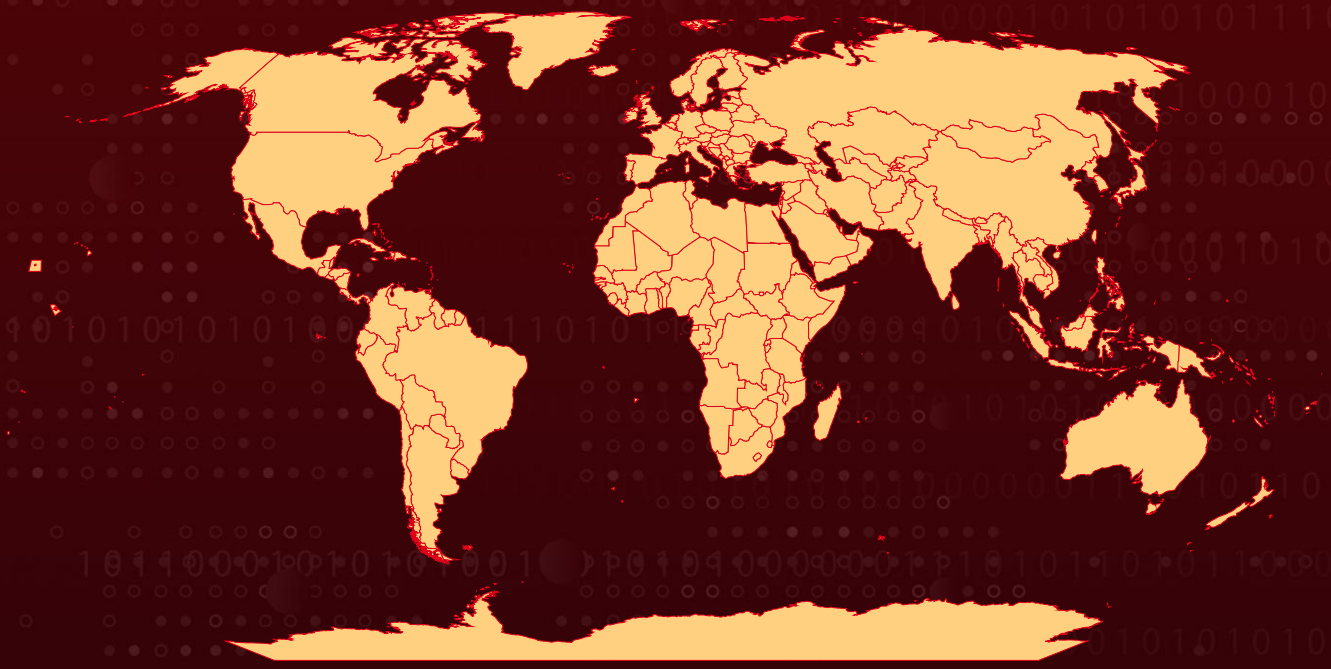
Shai-Hulud 2.0 Fuels Global NPM Supply-Chain Compromise

Date of Publication	Admiralty Code	TA Number
November 27, 2025	A1	TA2025362

Summary

Attack Commenced: November 21, 2025
Targeted Countries: Worldwide
Targeted Platforms: npm ecosystem, GitHub repositories, CI/CD environments, cloud providers (AWS, Azure, GCP)
Malware: Sha1-Hulud 2.0
Campaign Name: Sha1-Hulud: The Second Coming
Attack: The Shai-Hulud 2.0 attack is a critical supply-chain compromise targeting the npm ecosystem, infecting hundreds of packages and exposing credentials from over 25,000 GitHub repositories. It achieves early execution through malicious preinstall scripts and a Bun-based payload, enabling propagation via automated re-publishing using stolen tokens. The most severe escalation is a destructive failsafe that attempts to wipe user directories if propagation fails, requiring immediate secret rotation, dependency auditing, and enhanced supply-chain defenses.

Attack Regions



Attack Details

#1

The Shai-Hulud 2.0 supply-chain attack, also known as “The Second Coming,” represents a major escalation of the original 2025 npm compromise. Emerging in late November 2025, the campaign targeted hundreds of npm packages, including those maintained by prominent organizations such as Zapier, ENS Domains, AsyncAPI, PostHog, and Postman. By exploiting preinstall lifecycle scripts, the malware executes early in developer machines and CI/CD pipelines, allowing rapid infiltration and widespread propagation across the open-source ecosystem.

#2

Once installed, the malware deploys two JavaScript files that leverage a Bun-compatible runtime to execute its payload. The payload actively scans for sensitive credentials, including GitHub tokens, npm tokens, and cloud provider secrets. Stolen credentials are exfiltrated through automatically created public GitHub repositories, often referencing “Sha1-Hulud: The Second Coming.” Using these tokens, the worm republishes compromised npm packages, enabling self-replication across trusted maintainer accounts.

#3

A new feature in this variant is its destructive fallback behavior. If authentication or propagation fails, some variants attempt to erase user home directories, marking a departure from the prior stealth-focused Shai Hulud campaign. This destructive capability increases the overall risk, turning a supply-chain compromise into a potential data-loss incident.

#4

The scale of Shai-Hulud 2.0 is significant: researchers report over 25,000 affected GitHub repositories and 600–800 compromised npm packages, exposing large numbers of secrets and developer environments. The attack demonstrates advanced automation, rapid replication, and early-execution tactics, underscoring the growing sophistication of supply-chain threats in modern software development.

#5

Organizations relying on npm are urged to act immediately, audit dependencies, revoke exposed tokens, remove unauthorized repositories, and rebuild affected environments from trusted sources. The campaign highlights the importance of stricter supply-chain security, including restricting lifecycle scripts, enforcing trusted publishing, and continuous monitoring for anomalous activity.

Recommendations

Revoke and Rotate All Credentials Immediately: Assume all tokens accessible in developer machines or CI/CD pipelines may be compromised. Revoke and regenerate GitHub PATs, npm tokens, cloud keys (AWS/GCP/Azure), CI/CD secrets, and SSH keys. Enforce least-privilege scopes for newly created tokens.

Audit npm Dependencies and Build Pipelines: Review all npm packages, particularly recently updated or low-activity packages, for malicious preinstall or postinstall scripts. Reinstall dependencies from a clean state, validate package integrity (shasums), and use pinned versions or lockfiles.

Inspect GitHub for Unauthorized Activity: Check for suspicious public repositories, unexpected commits, or malicious package publications. Remove unauthorized repos and investigate any signs of credential abuse or automated publishing.

Rebuild Affected Environments: For any machine or CI agent that installed compromised packages, rebuild from a trusted baseline. Avoid cleaning in place, variants of Shai-Hulud may persist or destroy directories on failure.

Strengthen Supply-Chain Defenses: Disable npm lifecycle scripts where possible, enforce trusted publishing workflows, implement SBOM validation, require 2FA for maintainers, and adopt short-lived, scoped access tokens. Integrate real-time secret scanning and dependency monitoring into CI/CD pipelines.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0006 Credential Access	TA0001 Initial Access	TA0040 Impact
TA0007 Discovery	TA0002 Execution	TA0011 Command and Control	TA0010 Exfiltration
T1078 Valid Accounts	T1195 Supply Chain Compromise	T1059.004 Unix Shell	T1059 Command and Scripting Interpreter
T1552 Unsecured Credentials	T1082 System Information Discovery	T1083 File and Directory Discovery	T1567 Exfiltration Over Web Service
T1071 Application Layer Protocol	T1059.007 JavaScript	T1486 Data Encrypted for Impact	T1567.002 Exfiltration to Cloud Storage
T1195.001 Compromise Software Dependencies and Development Tools	T1485 Data Destruction	T1070.004 File Deletion	T1070 Indicator Removal

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	62ee164b9b306250c1172583f138c9614139264f889fa99614903c12755468d0, e0250076c1d2ac38777ea8f542431daf61fcbaab0ca9c196614b28065ef5b918, cbb9bc5a8496243e02f3cc080efbe3e4a1430ba0671f2e43a202bf45b05479cd, f1df4896244500671eb4aa63ebb48ea11cee196fafaa0e9874e17b24ac053c02, f099c5d9ec417d4445a0328ac0ada9cde79fc37410914103ae9c609cbc0ee068,

TYPE	VALUE
SHA256	46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09, b74caeaa75e077c99f7d44f46daaf9796a3be43ecf24f2a1fd381844669da777, dc67467a39b70d1cd4c1f7f7a459b35058163592f4a9e8fb4dffcbba98ef210c, 4b2399646573bb737c4969563303d8ee2e9ddbd1b271f1ca9e35ea78062538db, a3894003ad1d293ba96d77881ccd2071446dc3f65f434669b49b3da92421901a
URL	hxxps[:]//webhook[.]site/bb8ca5f6-4175-45d2-b042-fc9ebb8170b7
Domains	shai-hulud[.]xyz, hulud-sec[.]xyz, npm-sync-secure[.]net, env-dump-upload[.]net
File Names	postinstall.js, env-dump.js, token-grab.js, npmrc-mod.js, update.js
SHA1	D60ec97eea19fffb4809bc35b91033b52490ca11, 3d7570d14d34b0ba137d502f042b27b0f37a59fa, d1829b4708126dcc7bea7437c04d1f10eacd4a16

References

https://www.stepsecurity.io/blog/sha1-hulud-the-second-coming-zapier-ens-domains-and-other-prominent-npm-packages-compromised

https://www.wiz.io/blog/shai-hulud-2-0-ongoing-supply-chain-attack

https://blog.checkpoint.com/research/shai-hulud-2-0-inside-the-second-coming-the-most-aggressive-npm-supply-chain-attack-of-2025/

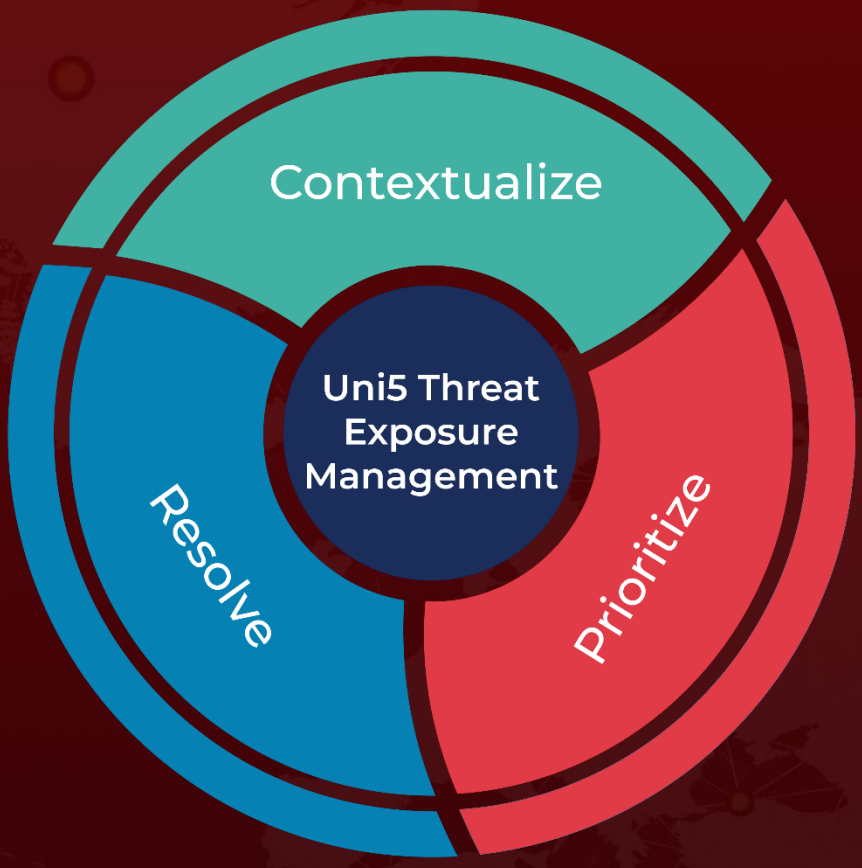
https://hivepro.com/threat-advisory/shai-hulud-massive-npm-supply-chain-attack-infects-hundreds-of-packages/

https://github.blog/security/supply-chain-security/our-plan-for-a-more-secure-npm-supply-chain/

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

November 27, 2025 . 8:30 AM

More at www.hivepro.com