10 December 2025

TLP: WHITE

INTEL471

EMERGING THREATS

Shai-Hulud Worm 2.0

UPDATE 12/08/2025: Shai-Hulud 2.0 represents an escalation of capability of the original npm-based supply-chain attack, adding earlier and broader execution paths, significantly expanded propagation, and deeper compromise capabilities across developer, CI/CD, and cloud environments. This new version has added preinstall execution for example, allowing the malware to run earlier in the installation process and reach more systems. It also introduces new payload components, including Bun-runtime-based scripts, which broaden where and how the malware can execute. Researchers have observed the campaign has grown dramatically in scale, compromising hundreds of npm packages and tens of thousands of GitHub repositories, aided by aggressive automated replication. It is also worthy to note that Shai-Hulud 2.0 also adds advanced exfiltration and persistence mechanisms, such as malicious GitHub Actions workflows that steal secrets or register backdoored runners, and it extends beyond the developer ecosystem to actively target cloud credentials across AWS, GCP, and Azure. Overall, Shai-Hulud 2.0 transforms the original worm into a far more automated, multi-platform, cloud-aware, and large-scale supply-chain threat.

THREAT SUMMARY

UPDATE 12/08/2025: Shai-Hulud 2.0 represents an escalation of capability of the original npm-based supply-chain attack, adding earlier and broader execution paths, significantly expanded propagation, and deeper compromise capabilities across developer, CI/CD, and cloud environments. This new version has added preinstall execution for example, allowing the malware to run earlier in the installation process and reach more systems. It also introduces new payload components, including Bun-runtime-based scripts, which broaden where and how the malware can execute. Researchers have observed the campaign has grown dramatically in scale, compromising hundreds of npm packages and tens of thousands of GitHub repositories, aided by aggressive automated replication. It is also worthy to note that Shai-Hulud 2.0 also adds advanced exfiltration and persistence mechanisms, such as malicious GitHub Actions workflows that steal secrets or register backdoored runners, and it extends beyond the developer ecosystem to actively target cloud credentials across AWS, GCP, and Azure. Overall, Shai-Hulud 2.0 transforms the original worm into a far more automated, multi-platform, cloud-aware, and large-scale supply-chain threat.

The "Shai-Hulud" worm represents a significant escalation in software supply chain attacks, particularly within the Node.js ecosystem. Discovered in mid-September 2025, this self-replicating malware has compromised over 500 npm packages, including widely used libraries such as @ctrl/tinycolor and several maintained by CrowdStrike. This worm's primary objective is to harvest developer credentials, such as GitHub Personal Access Tokens (PATs), npm tokens, and cloud service API keys, and exfiltrate them to attacker-controlled endpoints. Additionally, stolen credentials have been observed to be uploaded to public GitHub repositories named "Shai-Hulud," making them accessible to the public. The impact of this attack is significant, as it not only compromises individual developer environments but also exposes private repositories and organizational secrets, potentially leading to further exploitation.

TITAN References:

- Underground Perspective: Node package manager supply chain attack dubbed Shai-Hulud compromises hundreds of packages
- Malware Campaign: Node package manager packages compromised in Shai-Hulud 2.0 campaign

SYNOPSIS

The Shai-Hulud worm operates by injecting malicious scripts into npm packages, which execute immediately upon installation. Once active, it scans the victim's environment for sensitive credentials, including npm tokens, GitHub Personal Access Tokens (PATs), and cloud service keys for AWS, GCP, and Azure. These credentials are then encoded and exfiltrated to attacker-controlled endpoints, as well as uploaded to a public GitHub repository named Shai-Hulud. The malware also deploys a malicious GitHub Actions workflow (shai-hulud-workflow.yml) that executes during CI/CD pipeline runs, enabling further exfiltration of secrets from compromised repositories and maintaining persistent access even after the initial infection.

In addition to credential theft, Shai-Hulud autonomously propagates by modifying the package.json files of all npm packages maintained by the victim, injecting its malicious script and republishing the packages to the npm registry. This self-replication mechanism allows the worm to spread to other developers and organizations using the infected packages. By combining automated propagation, persistent access through CI/CD workflows, and large-scale credential exfiltration, Shai-Hulud d

SHAI-HULUD WORM 2.0 COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:relevance,term:!(c5d0f271-73cf-44a1-98ff-e6ed809d30e6),touched:!t)

RELATED HUNT PACKAGES

Base64 Encoding with Potential Exfiltration

https://hunter.cyborgsecurity.io/research/hunt-package/d65c7ebb-08e9-4a23-b964-1041d3384d4a

JavaScript Runtime Initiated DNS and Firewall Manipulation

https://hunter.cyborgsecurity.io/research/hunt-package/5c085831-88db-45b1-b28b-b61f362f97eb

CURL/WGET Download and Execute - Potential Payload Download Followed by Execution

https://hunter.cyborgsecurity.io/research/hunt-package/b585a013-e56d-4c3f-ac29-f2a610ac0ce8

Linux Generic Disk or File Wipe Activity

https://hunter.cyborgsecurity.io/research/hunt-package/435a6265-ae9b-4500-a027-5abfb31e80bd

Suspicious Use of Cipher.exe

https://hunter.cyborgsecurity.io/research/hunt-package/554ec3d7-da28-4513-9519-6a88f33ddba2

Usage of chmod to Enable Execution - Potential Payload Staging

https://hunter.cyborgsecurity.io/research/hunt-package/dfbdc565-a37c-472b-a4c7-6c0e5325b255

Methods for Downloading Files with PowerShell

https://hunter.cyborgsecurity.io/research/hunt-package/c7b320fb-ac67-45b0-92c4-b0f1e10b4e46

Unusual Secret Scanning Processes - Trufflehog Activity

https://hunter.cyborgsecurity.io/research/hunt-package/b6fba6ae-ffab-421b-9832-44b4c62e6fc7

Suspicious DNS Request - GitHub API

https://hunter.cyborgsecurity.io/research/hunt-package/8295dc2e-4cd4-425c-aecc-480617bc2c51

Node Spawning Bun Runtime (Suspicious NPM Lifecycle Execution)

https://hunter.cyborgsecurity.io/research/hunt-package/8e4c1bab-3695-4e5c-a900-934512d05205

Double Base64 Encoding

https://hunter.cyborgsecurity.io/research/hunt-package/f5aec910-25b6-462c-982a-a4eb20fa7c91

Docker Privileged Container With Host Filesystem Mount (Privilege Escalation)

https://hunter.cyborgsecurity.io/research/hunt-package/3e94cb90-1398-401b-8068-27357454a28c

MITRE CONTEXT

- MITRE Tactic Names:
  - Execution
  - Collection
  - Command and Control
  - Impact
  - Credential Access
  - Privilege Escalation
  - Defense Evasion
  - Discovery
  - Exfiltration
- MITRE Technique Names:
  - Sudo and Sudo Caching
  - Disable or Modify System Firewall
  - PowerShell
  - Automated Collection
  - Account Discovery
  - Indicator Removal
  - Credentials In Files
  - Exfiltration Over C2 Channel
  - Ingress Tool Transfer
  - Obfuscated Files or Information
  - Deploy Container
  - Credentials in Files
  - Impair Defenses
  - Escape to Host
  - Command and Scripting Interpreter
  - Stored Data Manipulation
  - Data Destruction
  - File Deletion
  - JavaScript
  - Linux and Mac File and Directory Permissions Modification
- MITRE Technique IDs:
  - T1059
  - T1027

    - T1562.004
    - T1059.001
    - T1119
    - T1087
    - T1552.001
    - T1059.007
    - T1070
    - T1485
    - T1041
    - T1611
    - T1548.003
    - T1610
    - T1070.004
    - T1105
    - T1222.002
    - T1562
    - T1081
    - T1565.001
- Exploitation Vulnerabilities:
    - CVE-2023-46747
    - CVE-2024-3400
    - CVE-2025-59287
    - CVE-2024-1709
    - CVE-2021-4436
    - CVE-2025-0282

REFERENCES

1. https://www.trendmicro.com/en_us/research/25/i/npm-supply-chain-attack.html
2. https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem
3. https://unit42.paloaltonetworks.com/npm-supply-chain-attack/
4. https://www.blackduck.com/blog/npm-malware-attack-shai-hulud-threat.html
5. https://www.wiz.io/blog/shai-hulud-2-0-ongoing-supply-chain-attack
6. https://securitylabs.datadoghq.com/articles/shai-hulud-2.0-npm-worm/
7. https://www.trendmicro.com/en_us/research/25/k/shai-hulud-2-0-targets-cloud-and-developer-systems.html