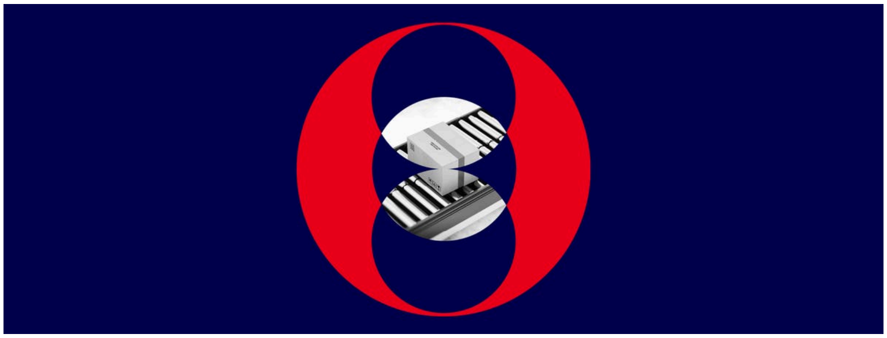
Massive Malicious NPM Package Attack Threatens Software Supply Chains



In mid-September, cybersecurity researchers uncovered a self-propagating malware called “Shai-Hulud”, which is involved in a large-scale supply chain attack targeting a tool that helps manage JavaScript packages and dependencies. This attack leverages malicious Node Package Manager (NPM) packages planted in the NPM ecosystem used by millions of software developers worldwide. As of this writing, the ongoing attack has affected more than 700 packages, including high-profile CrowdStrike packages.

The campaign aims to compromise developers' machines, then extract credentials, tokens, and other secrets. Organizations with significant software development operations, especially those that rely heavily on NPM packages and CI/CD pipelines in their development processes, should be particularly vigilant. Shai-Hulud is capable of targeting both Windows and Linux systems.

Below, we summarize what is currently known about this attack, link to additional information, and highlight tools and resources from Recorded Future that can help organizations defend themselves. This is an evolving threat and we will be providing new information as it becomes available.

Key Shai-Hulud characteristics

The malicious Shai-Hulud payload (it’s named after the sandworms in the sci-fi epic, *Dune*) is contained in trojanized NPM packages, including some important CrowdStrike packages and others with millions of weekly downloads. The attack centers on a “bundle.js” script that downloads and executes TruffleHog, a legitimate credential scanner, to collect developer and CI/CD tokens, cloud service credentials, and environment variables. The script validates tokens and exfiltrates the collected data via hard-coded webhooks and GitHub Actions workflows.

Rather than simply deploying malware on individual machines, Shai-Hulud propagates through NPM packages in a worm-like fashion while simultaneously creating unauthorized GitHub Actions workflows (“shai-hulud.yaml” or “shai-hulud-workflow.yml” files) in compromised repositories. These workflows serve as persistent backdoors that automatically exfiltrate repository secrets and sensitive data whenever CI pipelines execute, creating a self-sustaining attack mechanism that can survive even after the initial compromise is detected and remediated. This technique effectively weaponizes the victim's own development infrastructure for ongoing espionage and data theft.

High-priority next steps for this particularly dangerous attack

Add up the factors detailed above and it’s clear why this is a serious attack with potentially damaging consequences:

- Automatically spreads to new packages (worm-like behavior)
- Steals developer credentials and CI/CD pipeline tokens
- Creates persistent backdoors in GitHub repositories
- Affects some high-profile, widely used packages

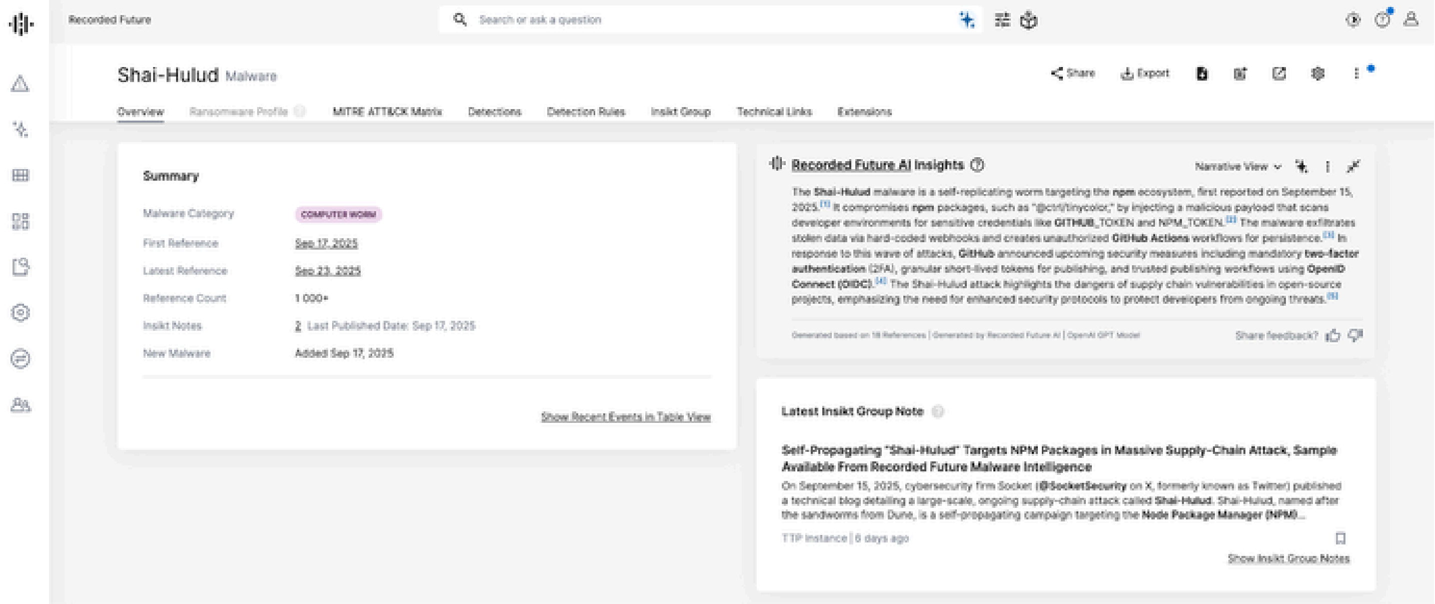
Although known affected packages have been removed from the NPM registry, Insikt Group strongly advises organizations to take these steps:

- Search for and remove compromised NPM versions
- Rotate tokens
- Audit CI/CD environments
- Review repositories for unauthorized workflows or anomalous branches

What Recorded Future is doing to help clients defend against the Shai-Hulud attack

Threat Intelligence Coverage

Recorded Future is providing real-time reporting via the Insikt Group to track the evolution of this campaign, as well as highlighting background insights from previous similar attacks to offer additional context.



Shai-Hulud Malware

Summary

Malware Category	COMPUTER WORM
First Reference	Sep 17, 2025
Latest Reference	Sep 23, 2025
Reference Count	1 000+
Insikt Notes	2 Last Published Date: Sep 17, 2025
New Malware	Added Sep 17, 2025

Recorded Future AI Insights

The **Shai-Hulud** malware is a self-replicating worm targeting the **npm** ecosystem, first reported on September 15, 2025.[1] It compromises **npm** packages, such as "@ctrl/tinycolor," by injecting a malicious payload that scans developer environments for sensitive credentials like **GITHUB**_TOKEN and NPM_TOKEN.[2] The malware exfiltrates stolen data via hard-coded webhooks and creates unauthorized **GitHub Actions** workflows for persistence.[3] In response to this wave of attacks, **GitHub** announced upcoming security measures including mandatory **two-factor authentication** (2FA), granular short-lived tokens for publishing, and trusted publishing workflows using **OpenID Connect (OIDC)**.[4] The Shai-Hulud attack highlights the dangers of supply chain vulnerabilities in open-source projects, emphasizing the need for enhanced security protocols to protect developers from ongoing threats.[5]

Generated based on 18 References | Generated by Recorded Future AI | OpenAI GPT Model

Latest Insikt Group Note

Self-Propagating "Shai-Hulud" Targets NPM Packages in Massive Supply-Chain Attack, Sample Available From Recorded Future Malware Intelligence

On September 15, 2025, cybersecurity firm Socket (**@SocketSecurity** on X, formerly known as Twitter) published a technical blog detailing a large-scale, ongoing supply-chain attack called **Shai-Hulud**. Shai-Hulud, named after the sandworms from Dune, is a self-propagating campaign targeting the **Node Package Manager (NPM)**...

TTP Instance | 6 days ago

Intelligence Card® for Shai-Hulud

Malware Intelligence

The Insikt Group obtained and analyzed compromised package samples and provided IOCs, including command and control infrastructure, webhook endpoints, and file hashes. We have also conducted a detailed technical breakdown of “bundle.js” payload and attack mechanisms.

Based on static code analysis, bundle.js performs the following actions on a victim's machine:

AWS Integration Capabilities:

- Detects if an HTTP status code is a redirect
- Validates and resolves Web Identity AWS credential profiles
- Provides a fully configured AWS Security Token Service (STS) client with retry, signing, user-agent, region, and middleware setup
- Implements an IP address resolver for ipv4:// and ipv6:// URIs in Google Remote Procedure Call (gRPC)-style resolution
- Exposes AWS Secrets Manager command serializers/deserializers, such as create, get, update, delete, rotate, and replicate secrets

GitHub Repository Compromise:

- Verifies the supplied GitHub Personal Access Token (PAT) and checks if it contains repository and workflow scopes
- Fetches the default branch SHA for each repository
- Defines a new branch named "shai-hulud" and creates it across targeted repositories

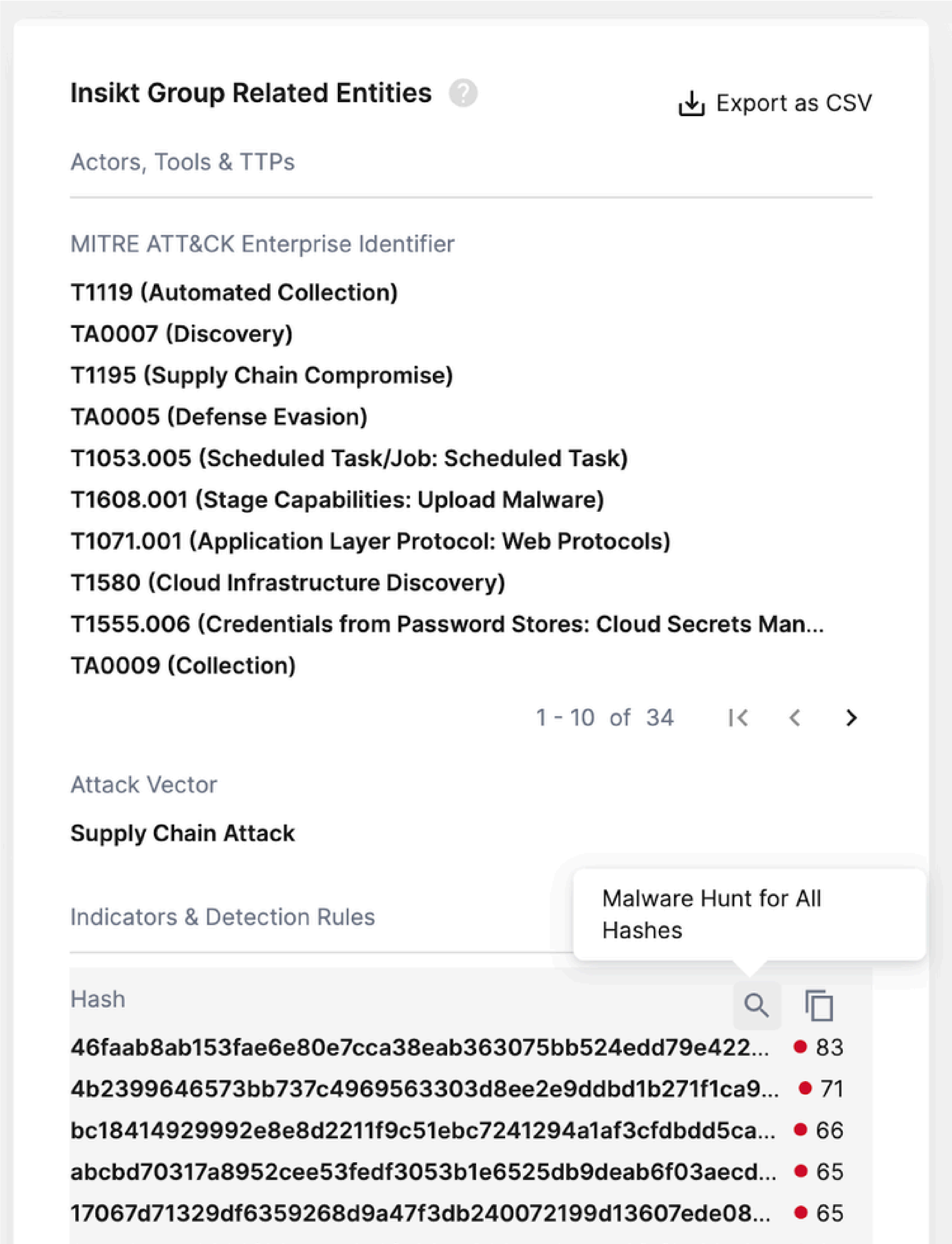
Malicious Workflow Deployment:

- Creates a workflow file at path ".github/workflows/shai-hulud-workflow.yml"
- Encodes the workflow file using Base64 and uploads it to the shai-hulud branch via the Contents API
- Embeds a workflow that triggers on every push with a single step that sets "CONTENTS=${{ toJSON(secrets) }}"

Data Exfiltration:

- Uses curl to exfiltrate all available repository secrets to its command-and-control (C2) server hosted on hxxps://webhook[.]site/bb8ca5f6-4175-45d2-b042-fc9ebb8170b7
- Encodes the secrets using Base64 and prints them to the logs
- Immediately runs the workflow on the shai-hulud branch, exfiltrating secrets off-site and leaking them in job logs once a push is made

Customers can easily investigate these samples further from the Shai-Hulud Intelligence Card®.



Insikt Group Related Entities

Actors, Tools & TTPs

MITRE ATT&CK Enterprise Identifier

T1119 (Automated Collection)

TA0007 (Discovery)

T1195 (Supply Chain Compromise)

TA0005 (Defense Evasion)

T1053.005 (Scheduled Task/Job: Scheduled Task)

T1608.001 (Stage Capabilities: Upload Malware)

T1071.001 (Application Layer Protocol: Web Protocols)

T1580 (Cloud Infrastructure Discovery)

T1555.006 (Credentials from Password Stores: Cloud Secrets Man...

TA0009 (Collection)

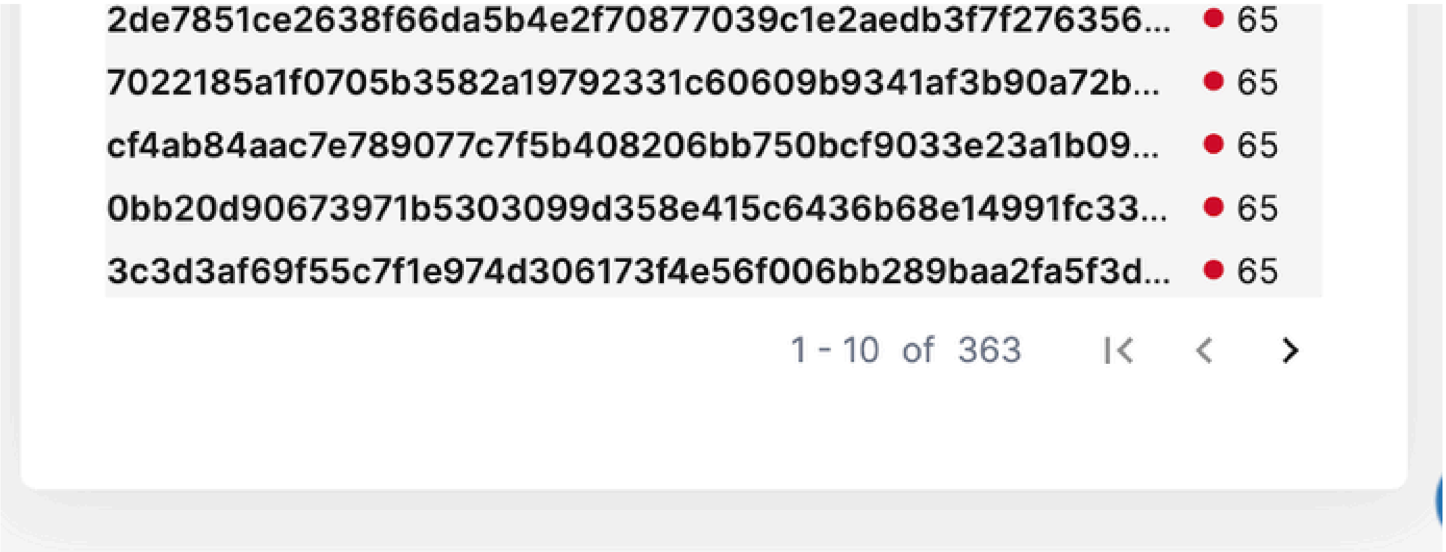
1 - 10 of 34

Attack Vector

Supply Chain Attack

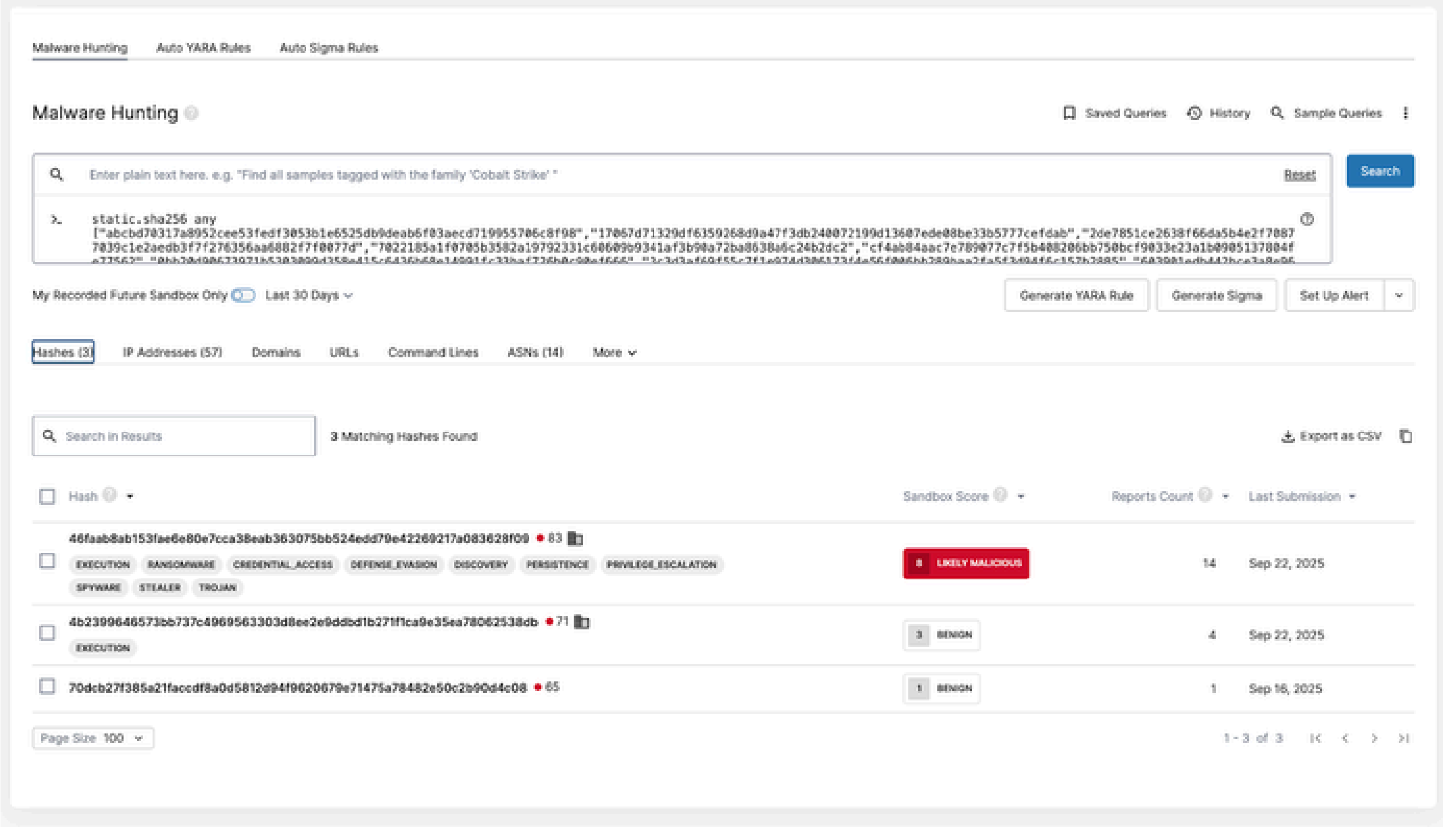
Indicators & Detection Rules

Hash	
46faab8ab153fae6e80e7cca38eab363075bb524edd79e422...	● 83
4b2399646573bb737c4969563303d8ee2e9ddbd1b271f1ca9...	● 71
bc18414929992e8e8d2211f9c51ebc7241294a1af3cfdbdd5ca...	● 66
abcbd70317a8952cee53fedf3053b1e6525db9deab6f03aecd...	● 65
17067d71329df6359268d9a47f3db240072199d13607ede08...	● 65



2de7851ce2638f66da5b4e2f70877039c1e2aedb3f7f276356...	● 65
7022185a1f0705b3582a19792331c60609b9341af3b90a72b...	● 65
cf4ab84aac7e789077c7f5b408206bb750bcf9033e23a1b09...	● 65
0bb20d90673971b5303099d358e415c6436b68e14991fc33...	● 65
3c3d3af69f55c7f1e974d306173f4e56f006bb289baa2fa5f3d...	● 65

Quickly Search for Associated Hashes from the Insikt Group



Malware Hunting

Enter plain text here. e.g. "Find all samples tagged with the family 'Cobalt Strike' "

```
static.sha256 any
["abcbd70317a8952cee53fedf3053b1e6525db9deab6f03aecd719955706c8f98","17067d71329df6359268d9a47f3db240072199d13607ede08be33b5777cefdab","2de7851ce2638f66da5b4e2f7087
7039c1e2aedb3f7f276356aa6882f7f0077d","7022185a1f0705b3582a19792331c60609b9341af3b90a72ba8638a6c24b2dc2","cf4ab84aac7e789077c7f5b408206bb750bcf9033e23a1b0905137804f
```

My Recorded Future Sandbox Only ○ Last 30 Days

3 Matching Hashes Found

□	Hash	Sandbox Score	Reports Count	Last Submission
□	46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09 ● 83 EXECUTION RANSOMWARE CREDENTIAL_ACCESS DEFENSE_EVASION DISCOVERY PERSISTENCE PRIVILEGE_ESCALATION SPYWARE STEALER TROJAN	8 LIKELY MALICIOUS	14	Sep 22, 2025
□	4b2399646573bb737c49695633O3d8ee2e9ddbd1b271f1ca9e35ea78062538db ● 71 EXECUTION	3 BENIGN	4	Sep 22, 2025
□	70dcb27f385a21faccdf8a0d5812d94f9620679e71475a78482e50c2b90d4c08 ● 65	1 BENIGN	1	Sep 16, 2025

Page Size 100

1 - 3 of 3

Investigate Commonalities Across Shai-Hulud Related Malware Samples

Third-Party Intelligence

Public reporting on companies impacted by Shai-Hulud will trigger Risk Rules and Playbook Alerts, providing immediate visibility into supply chain exposure across an organization’s vendor ecosystem.

Brand Intelligence

Add "Shai-Hulud" as a keyword to your Code Repo Playbook Alerts to detect any references to this campaign in your code repositories or development environments.

Fallout and what’s next

As of this writing, it's too early to say how this attack will evolve or to assess the scale of its effects.

Additional Sources

- https://socket.dev/blog/ongoing-supply-chain-attack-targets-crowdstrike-NPM-packages?utm_medium=feed
  - https://cybernews.com/crypto/NPM-users-advanced-supply-chain-attack-infiltrates-40-packages/
  - https://x.com/feross/status/1967732902256579014
  - https://app.recordedfuture.com/portal/research/insikt/doc:-B9Srl
- https://www.aikido.dev/blog/NPM-debug-and-chalk-packages-compromised
  - https://app.recordedfuture.com/live/sc/3DMkqz2mkLyR
  - https://x.com/AikidoSecurity/status/1965073757262827796
  - https://app.recordedfuture.com/live/sc/21MCvGQ4Qusi
  - https://x.com/CharlieEriksen/status/1965134623224242208
  - https://app.recordedfuture.com/live/sc/7DUqR0yiqxs4
  - https://x.com/sifex/status/1965082909519630624
  - https://socket.dev/blog/NPM-author-qix-compromised-in-major-supply-chain-attack
  - https://app.recordedfuture.com/live/sc/6kNzRN3jdsnU
  - https://socket.dev/blog/duckdb-NPM-account-compromised-in-continuing-supply-chain-attack
  - https://app.recordedfuture.com/live/sc/1hi7Un0QRCU4
  - https://x.com/SocketSecurity/status/1965363025264914918
  - https://app.recordedfuture.com/live/sc/2qEjfYLWHQKA
  - https://www.linkedin.com/posts/advocatemack_malware-NPM-supplychain-activity-7370829639537291264-jxZD/
  - https://app.recordedfuture.com/live/sc/6efJTQoCRAqG
  - https://jdstaerk.substack.com/p/we-just-found-malicious-code-in-the
  - https://github.com/advisories/GHSA8mgj-vmr8-frr6
  - https://app.recordedfuture.com/live/sc/40fEFSw5I0RG
  - https://x.com/Cyb3rMonk/status/1965149631836463252
  - https://app.recordedfuture.com/live/sc/6KqmRMDuxybB
  - https://github.com/Cyb3r-Monk/Threat-Hunting-and-Detection/blob/main/Uncategorized/NPM%20debug%20and%20chalk%20compromise%20092025.md
  - https://tria.ge/250908-wl45pazyc1/behavioral2