S1ngularity/nx attackers strike again

By Charlie Eriksen

Published: 2025-09-16 · Archived: 2026-04-29 02:11:47 UTC

Published on:

Sep 16, 2025

This morning, we were alerted to a large-scale attack against npm. This appears to the be work of the same threat actors behind the Nx attack on August 27th 2025. This was originally published by Socket and StepSecurity who noted 40 packages had been comrpomised, since then an additional 147 packages have been infected with malware including packages from CrowdStrike.

The scale, scope and impact of this attack is significant. The attackers are using the same playbook in large parts as the original attack, but have stepped up their game. They have turned it into a full worm, which does these things automatically:

- Steal secrets and publish them to GitHub publicly
- Run trufflehog and query Cloud metadata endpoints to gather secrets
- Attempt to create a new GitHub action with a data exiltration mechanism through webhook[.]site
- Iterate the repositories on GitHub a user has access to, and make them public

Since our initial alert this morning we've confirmed the following additional behaviours and important details. For those that don't know, Shai Hulud is the name for the worm in the Dune franchise. A clear indication of the intent of the attackers.

Shai Hulud, from Dune

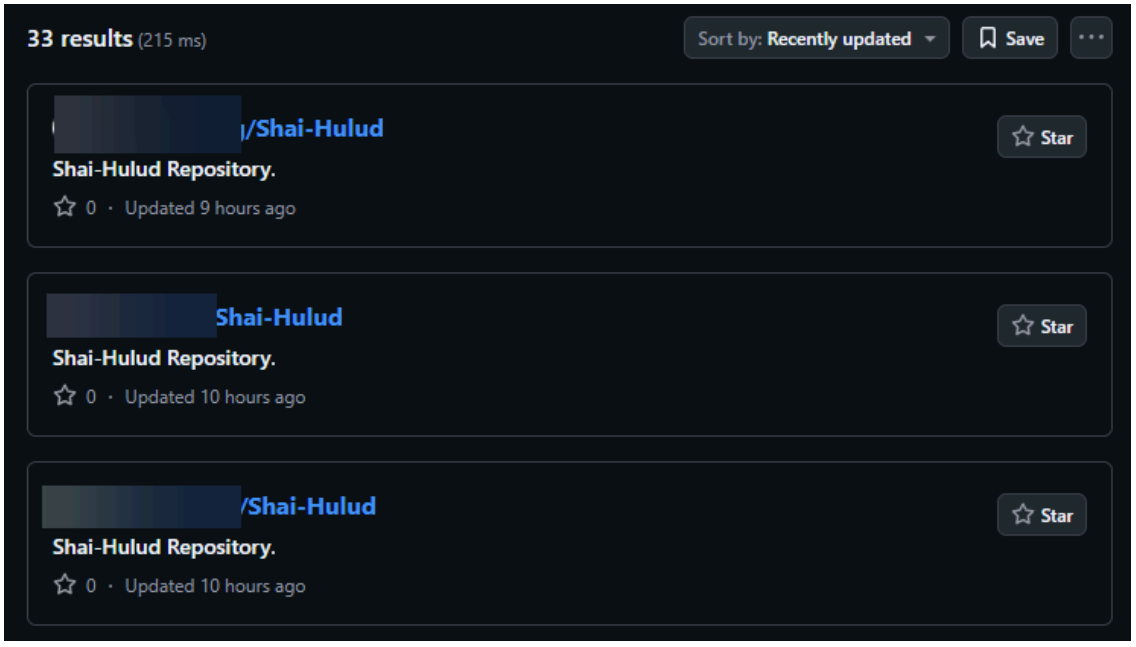
To avoid being compromised by packages like this, check out Aikido safe-chain!

What the worm does

- **Harvest**: scans the host and CI environment for secrets — process.env, scanning with TruffleHog, and cloud metadata endpoints (AWS/GCP) that return instance/service credentials.
- **Exfiltrate (1) — GitHub repo**: creates a repo named **Shai-Hulud** under the compromised account and commits a JSON dump containing system info, environment variables, and collected secrets.
- **Exfiltrate (2) — GitHub Actions → webhook**: drops a workflow `.github/workflows/shai-hulud-workflow.yml` that serializes `${{ toJSON(secrets) }}`, POSTs them to an attacker `webhook[.]site` URL and writes a double-base64 copy into the Actions logs.
- **Propagate**: uses any valid npm tokens it finds to enumerate and attempt to update packages the compromised maintainer controls (supply-chain propagation).
- **Amplify**: iterates the victim's accessible repositories, making them public or adding the workflow/branch that will trigger further runs and leaks.

Leaking of secrets

As with the original Nx attack, we're seeing the attackers doing a smash-and-grab style attack. The malicous payload both publishes a "Shai-Hulud" repository with stolen credentials/tokens, and it will go through a GitHub account and turn private repository to public:



Stolen credentials being published

Private repositories being turned public

Self-propogation through npm

One of the most striking features of this attack is that it behaves like a **true worm**. Rather than relying on a single infected package to spread, the code is designed to **re-publish itself into other npm packages** owned by the compromised maintainer.

Here's how the worm logic works:

- **Download a target tarball** – it fetches an existing package version from the npm registry.
- **Modify** `package.json` – the worm bumps the patch version (e.g. `1.2.3 → 1.2.4`) and inserts a new lifecycle hook (`postinstall`)
- **Copy its own payload** – the running script (`process.argv[1]`) is written into the tarball as `bundle.js`. This ensures that whatever code infected one package now lives inside the next.
- **Re-publish the trojanized package** – the modified tarball is gzipped and pushed back to npm using the maintainer's credentials.

This cycle allows the malware to **continuously infect every package** a maintainer has access to. Each published package becomes a new distribution vector: as soon as someone installs it, the worm executes, replicates, and pushes itself further into the ecosystem.

In short: the attacker doesn't need to manually target packages. Once a single environment is compromised, the worm automates the spread by **piggybacking on the maintainer's own publishing rights**.

For a complete malware breakdown we recommend reviewing the getsafety post

Impacted packages

Package	Versions
@ahmedhfarag/ngx-perfect-scrollbar	20.0.20
@ahmedhfarag/ngx-virtual-scroller	4.0.4
@art-ws/common	2.0.28
@art-ws/config-eslint	2.0.4, 2.0.5
@art-ws/config-ts	2.0.7, 2.0.8
@art-ws/db-context	2.0.24
@art-ws/di	2.0.28, 2.0.32
@art-ws/di-node	2.0.13
@art-ws/eslint	1.0.5, 1.0.6
@art-ws/fastify-http-server	2.0.24, 2.0.27
@art-ws/http-server	2.0.21, 2.0.25
@art-ws/openapi	0.1.9, 0.1.12
@art-ws/package-base	1.0.5, 1.0.6
@art-ws/prettier	1.0.5, 1.0.6
@art-ws/slf	2.0.15, 2.0.22
@art-ws/ssl-info	1.0.9, 1.0.10
@art-ws/web-app	1.0.3, 1.0.4
@crowdstrike/commitlint	8.1.1, 8.1.2
@crowdstrike/falcon-shoelace	0.4.1, 0.4.2
@crowdstrike/foundry-js	0.19.1, 0.19.2
@crowdstrike/glide-core	0.34.2, 0.34.3
@crowdstrike/logscale-dashboard	1.205.1, 1.205.2

Package	Versions
@crowdstrike/logscale-file-editor	1.205.1, 1.205.2
@crowdstrike/logscale-parser-edit	1.205.1, 1.205.2
@crowdstrike/logscale-search	1.205.1, 1.205.2
@crowdstrike/tailwind-toucan-base	5.0.1, 5.0.2
@ctrl/deluge	7.2.1, 7.2.2
@ctrl/golang-template	1.4.2, 1.4.3
@ctrl/magnet-link	4.0.3, 4.0.4
@ctrl/ngx-codemirror	7.0.1, 7.0.2
@ctrl/ngx-csv	6.0.1, 6.0.2
@ctrl/ngx-emoji-mart	9.2.1, 9.2.2
@ctrl/ngx-rightclick	4.0.1, 4.0.2
@ctrl/qbittorrent	9.7.1, 9.7.2
@ctrl/react-adsense	2.0.1, 2.0.2
@ctrl/shared-torrent	6.3.1, 6.3.2
@ctrl/tinycolor	4.1.1, 4.1.2
@ctrl/torrent-file	4.1.1, 4.1.2
@ctrl/transmission	7.3.1
@ctrl/ts-base32	4.0.1, 4.0.2
@hestjs/core	0.2.1
@hestjs/cqrs	0.1.6
@hestjs/demo	0.1.2
@hestjs/eslint-config	0.1.2
@hestjs/logger	0.1.6
@hestjs/scalar	0.1.7
@hestjs/validation	0.1.6
@nativescript-community/arraybuffers	1.1.6, 1.1.7, 1.1.8

Package	Versions
@nativescript-community/gesturehandler	2.0.35
@nativescript-community/perms	3.0.5, 3.0.6, 3.0.7, 3.0.8
@nativescript-community/sqlite	3.5.2, 3.5.3, 3.5.4, 3.5.5
@nativescript-community/text	1.6.9, 1.6.10, 1.6.11, 1.6.12
@nativescript-community/typeorm	0.2.30, 0.2.31, 0.2.32, 0.2.33
@nativescript-community/ui-collectionview	6.0.6
@nativescript-community/ui-document-picker	1.1.27, 1.1.28
@nativescript-community/ui-drawer	0.1.30
@nativescript-community/ui-image	4.5.6
@nativescript-community/ui-label	1.3.35, 1.3.36, 1.3.37
@nativescript-community/ui-material-bottom-navigation	7.2.72, 7.2.73, 7.2.74, 7.2.75
@nativescript-community/ui-material-bottomsheet	7.2.72
@nativescript-community/ui-material-core	7.2.72, 7.2.73, 7.2.74, 7.2.75
@nativescript-community/ui-material-core-tabs	7.2.72, 7.2.73, 7.2.74, 7.2.75
@nativescript-community/ui-material-ripple	7.2.72, 7.2.73, 7.2.74, 7.2.75
@nativescript-community/ui-material-tabs	7.2.72, 7.2.73, 7.2.74, 7.2.75
@nativescript-community/ui-pager	14.1.36, 14.1.37, 14.1.38
@nativescript-community/ui-pulltorefresh	2.5.4, 2.5.5, 2.5.6, 2.5.7
@nexe/config-manager	0.1.1
@nexe/eslint-config	0.1.1
@nexe/logger	0.1.3
@nstudio/angular	20.0.4, 20.0.5, 20.0.6
@nstudio/focus	20.0.4, 20.0.5, 20.0.6

Package	Versions
@nstudio/nativescript-checkbox	2.0.6, 2.0.7, 2.0.8, 2.0.9
@nstudio/nativescript-loading-indicator	5.0.1, 5.0.2, 5.0.3, 5.0.4
@nstudio/ui-collectionview	5.1.11, 5.1.12, 5.1.13, 5.1.14
@nstudio/web	20.0.4
@nstudio/web-angular	20.0.4
@nstudio/xplat	20.0.5, 20.0.6, 20.0.7
@nstudio/xplat-utils	20.0.5, 20.0.6, 20.0.7
@operato/board	9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42, 9.0.43, 9.0.44, 9.0.45, 9.0.46
@operato/data-grist	9.0.29, 9.0.35, 9.0.36, 9.0.37
@operato/graphql	9.0.22, 9.0.35, 9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42, 9.0.43, 9.0.44, 9.0.45, 9.0.46
@operato/headroom	9.0.2, 9.0.35, 9.0.36, 9.0.37
@operato/help	9.0.35, 9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42, 9.0.43, 9.0.44, 9.0.45, 9.0.46
@operato/i18n	9.0.35, 9.0.36, 9.0.37
@operato/input	9.0.27, 9.0.35, 9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42, 9.0.43, 9.0.44, 9.0.45, 9.0.46
@operato/layout	9.0.35, 9.0.36, 9.0.37
@operato/popup	9.0.22, 9.0.35, 9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42, 9.0.43, 9.0.44, 9.0.45, 9.0.46
@operato/pull-to-refresh	9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42
@operato/shell	9.0.22, 9.0.35, 9.0.36, 9.0.37, 9.0.38, 9.0.39
@operato/styles	9.0.2, 9.0.35, 9.0.36, 9.0.37
@operato/utils	9.0.22, 9.0.35, 9.0.36, 9.0.37, 9.0.38, 9.0.39, 9.0.40, 9.0.41, 9.0.42, 9.0.43, 9.0.44, 9.0.45, 9.0.46
@teselagen/bounce-loader	0.3.16, 0.3.17
@teselagen/liquibase-tools	0.4.1

Package	Versions
@teselagen/range-utils	0.3.14, 0.3.15
@teselagen/react-list	0.8.19, 0.8.20
@teselagen/react-table	6.10.19
@thangved/callback-window	1.1.4
@things-factory/attachment-base	9.0.43, 9.0.44, 9.0.45, 9.0.46, 9.0.47, 9.0.48, 9.0.49, 9.0.50
@things-factory/auth-base	9.0.43, 9.0.44, 9.0.45
@things-factory/email-base	9.0.42, 9.0.43, 9.0.44, 9.0.45, 9.0.46, 9.0.47, 9.0.48, 9.0.49, 9.0.50, 9.0.51, 9.0.52, 9.0.53, 9.0.54
@things-factory/env	9.0.42, 9.0.43, 9.0.44, 9.0.45
@things-factory/integration-base	9.0.43, 9.0.44, 9.0.45
@things-factory/integration-marketplace	9.0.43, 9.0.44, 9.0.45
@things-factory/shell	9.0.43, 9.0.44, 9.0.45
@tnf-dev/api	1.0.8
@tnf-dev/core	1.0.8
@tnf-dev/js	1.0.8
@tnf-dev/mui	1.0.8
@tnf-dev/react	1.0.8
@ui-ux-gang/devextreme-angular-rpk	24.1.7
@yoobic/design-system	6.5.17
@yoobic/jpeg-camera-es6	1.0.13
@yoobic/yobi	8.7.53
airchief	0.3.1
airpilot	0.8.8
angulartics2	14.1.1, 14.1.2
browser-webdriver-downloader	3.0.8
capacitor-notificationhandler	0.0.2, 0.0.3

Package	Versions
capacitor-plugin-healthapp	0.0.2, 0.0.3
capacitor-plugin-ihealth	1.1.8, 1.1.9
capacitor-plugin-vonage	1.0.2, 1.0.3
capacitorandroidpermissions	0.0.4, 0.0.5
config-cordova	0.8.5
cordova-plugin-voxeet2	1.0.24
cordova-voxeet	1.0.32
create-hest-app	0.1.9
db-evo	1.1.4, 1.1.5
devextreme-angular-rpk	21.2.8
ember-browser-services	5.0.2, 5.0.3
ember-headless-form	1.1.2, 1.1.3
ember-headless-form-yup	1.0.1
ember-headless-table	2.1.5, 2.1.6
ember-url-hash-polyfill	1.0.12, 1.0.13
ember-velcro	2.2.1, 2.2.2
encounter-playground	0.0.2, 0.0.3, 0.0.4, 0.0.5
eslint-config-crowdstrike	11.0.2, 11.0.3
eslint-config-crowdstrike-node	4.0.3, 4.0.4
eslint-config-teselagen	6.1.7
globalize-rpk	1.7.4
graphql-sequelize-teselagen	5.3.8
html-to-base64-image	1.0.2
json-rules-engine-simplified	0.2.1
jumpgate	0.0.2
koa2-swagger-ui	5.11.1, 5.11.2

Package	Versions
mcfly-semantic-release	1.3.1
mcp-knowledge-base	0.0.2
mcp-knowledge-graph	1.2.1
mobioffice-cli	1.0.3
monorepo-next	13.0.1, 13.0.2
mstate-angular	0.4.4
mstate-cli	0.4.7
mstate-dev-react	1.1.1
mstate-react	1.6.5
ng2-file-upload	7.0.2, 7.0.3, 8.0.1, 8.0.2, 8.0.3, 9.0.1
ngx-bootstrap	18.1.4, 19.0.3, 19.0.4, 20.0.3, 20.0.4, 20.0.5
ngx-color	10.0.1, 10.0.2
ngx-toastr	19.0.1, 19.0.2
ngx-trend	8.0.1
ngx-ws	1.1.5, 1.1.6
oradm-to-gql	35.0.14, 35.0.15
oradm-to-sqlz	1.1.2
ove-auto-annotate	0.0.9
pm2-gelf-json	1.0.4, 1.0.5
printjs-rpk	1.6.1
react-complaint-image	0.0.32
react-jsonschema-form-conditionals	0.3.18
remark-preset-lint-crowdstrike	4.0.1, 4.0.2
rxnt-authentication	0.0.3, 0.0.4, 0.0.5, 0.0.6
rxnt-healthchecks-nestjs	1.0.2, 1.0.3, 1.0.4, 1.0.5
rxnt-kue	1.0.4, 1.0.5, 1.0.6, 1.0.7

Package	Versions
swc-plugin-component-annotate	1.9.1, 1.9.2
tbssnch	1.0.2
teselagen-interval-tree	1.1.2
tg-client-query-builder	2.14.4, 2.14.5
tg-redbird	1.3.1
tg-seq-gen	1.0.9, 1.0.10
thangved-react-grid	1.0.3
ts-gaussian	3.0.5, 3.0.6
ts-imports	1.0.1, 1.0.2
tvi-cli	0.1.5
ve-bamreader	0.2.6
ve-editor	1.0.1
verror-extra	6.0.1
voip-callkit	1.0.2, 1.0.3
wdio-web-reporter	0.1.3
yargs-help-output	5.0.3
yoo-styles	6.0.326

Story developing…

Last updated on:

Sep 19, 2025

4.7/**5**

April 23, 2026

•

Vulnerabilities & Threats

Is Shai-Hulud Back? Compromised Bitwarden CLI Contains a Self-Propagating npm Worm

Malware found in @bitwarden/cli v2026.4.0 steals SSH keys, cloud secrets, and AI coding tool credentials, then spreads through victims' own npm packages. Inside: a worm calling itself "Shai-Hulud: The Third Coming."

#

Malware

April 22, 2026

•

Vulnerabilities & Threats

GPT-Proxy Backdoor in npm and PyPI turns Servers into Chinese LLM Relays

A newly discovered npm and PyPI malware campaign installs hidden LLM proxies on compromised servers, turning them into relay nodes for LLM traffic.

#

Malware

April 17, 2026

•

Vulnerabilities & Threats

Multiple Cross-Site Scripting (XSS) Vulnerabilities in Mailcow

Aikido's AI pentest agent found three XSS vulnerabilities in Mailcow, one of which let unauthenticated attackers take over administrator accounts. All issues have been patched as of version 2026-03b.

#

Vulnerabilities

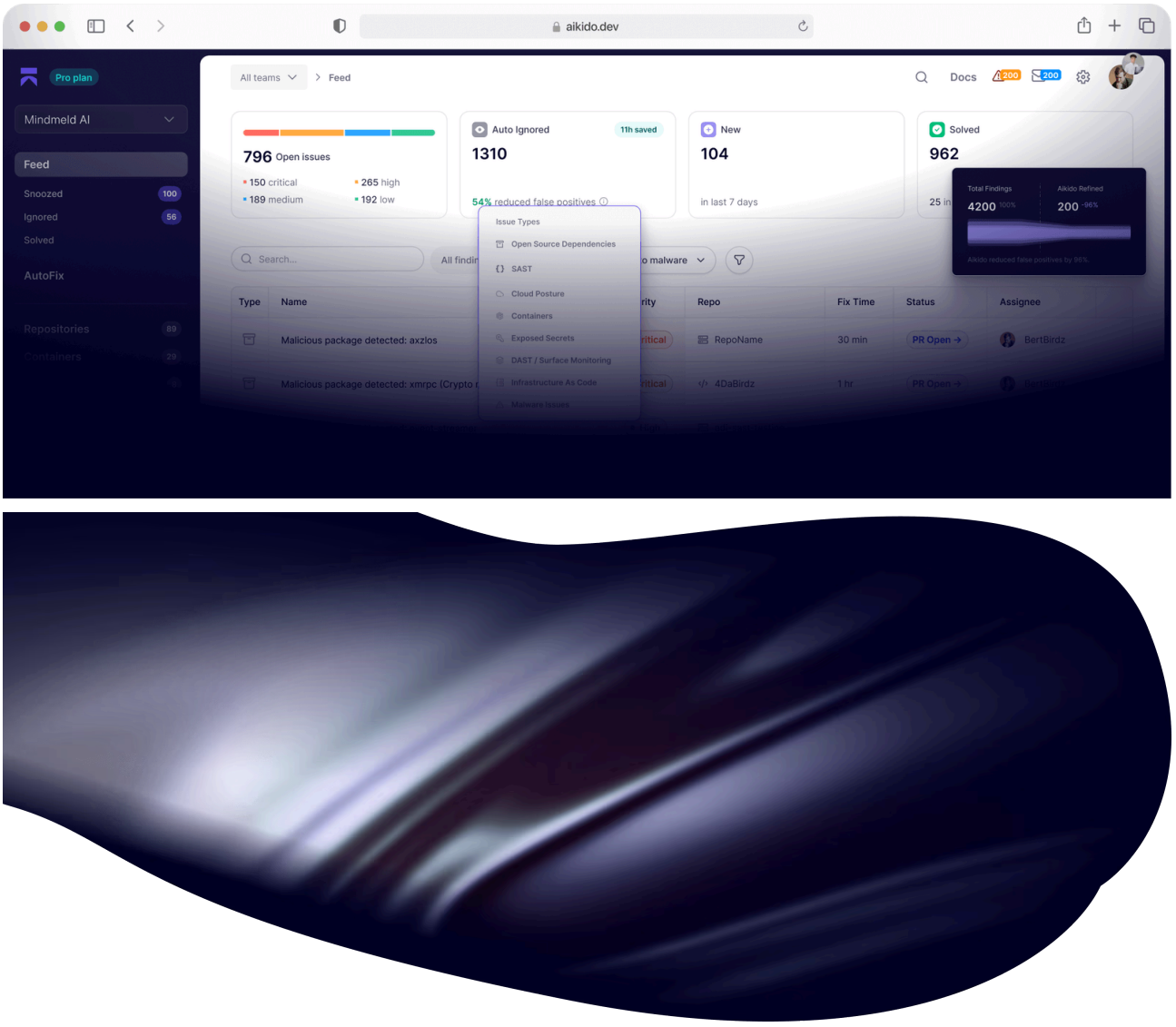
#

open-source

Get secure now

Secure your code, cloud, and runtime in one central system.
Find and fix vulnerabilities fast automatically.

No credit card required | Scan results in 32secs.



Source: https://www.aikido.dev/blog/s1ngularity-nx-attackers-strike-again