Shai-Hulud: Ongoing Package Supply Chain Worm Delivering Data-Stealing Malware

By Merav Bar, Rami McCarthy, Barak Sharoni

Published: 2025-09-16 · Archived: 2026-04-05 15:18:34 UTC

On September 15, 2025, malicious versions of multiple popular packages were published to npm. They contained a post-install script that harvested sensitive data and exfiltrated it to attacker-created public GitHub repos named Shai-Hulud. Beyond data theft, the malware exhibits worm-like behaviour: when a compromised package encounters additional npm tokens in its environment, it will automatically publish malicious versions of any packages it can access - spreading across the npm ecosystem. Wiz Research assesses this campaign is directly downstream of the late-August 2025 s1ngularity/Nx compromise (initial GitHub token theft to npm token theft to mass package poisoning). As the first successful self-propagating attack in the npm ecosystem, this appears to be one of the most severe JavaScript supply-chain attacks observed to date.

September 17, 2025 10AM UTC: payload analysis section was added.

September 17, 2025 1PM UTC: additional packages and versions have been added to the appendix.

Once a version of one of the malicious packages is installed, the included payload uses the TruffleHog secret scanning tool to identify secrets, in addition to harvesting environment variables and IMDS-exposed cloud keys when available.

Additionally, the script validates collected credentials and, if it finds GitHub tokens, it abuses them in multiple ways:

This attack is a self-propagating worm. When a compromised package encounters additional npm tokens in a victim environment, it will automatically publish malicious versions of any packages it can access. See further discussion of the malicious code in Socket's initial analysis.

Based on victimology, Wiz Research assesses this activity is tied to the recent s1ngularity / Nx supply chain attack, where initial GitHub token theft enabled the broader chain of compromise and leaking of formerly private repositories. The initial npm packages that started this chain reaction included multiple known-compromised victims of the s1ngularity attack.

The worm deploys a "workflow script" to `/tmp/processor.sh`, executing it to trigger automated branch creation, triggering GitHub workflows to exfiltrate its secrets. Similarly, it drops a "migration script" at `/tmp/migrate-repos.sh`, which, once executed, forces private repositories to be cloned and republished as public repositories with the `-migration` suffix.

During this process, the malware appears to use `/tmp/github-migration` as a temporary working directory for cloning and related operations - though this is not fully confirmed due to some obfuscation and irregularities in the code. Importantly, the migration routine first creates the repository as private and then immediately flips its

visibility to public. This results in two observable GitHub events in quick succession: a `CreateEvent` followed by a `PublicEvent`.

Another observation, one of the payloads appears to be AI-generated, another variant lacks that same stylistic pattern, suggesting it may have been copied from an external source that we have not yet identified.

The attacker exfiltrated data using `webhook[.]site` within a malicious GitHub Action. However, under the free plan used, the webhook can only receive a total of 100 callbacks. We observed that the webhook had been deactivated by the platform for excessive activity. This renders the webhook based exfiltration non-functional. However, secrets will still be exposed in the workflow log on GitHub.

Wiz Research initially observed 36 GitHub users with secrets exposed in the “Shai-Hulud” repo (`data.json`, double–base64 encoded) and 8 users whose private repositories were force-migrated to public with the label “Shai-Hulud Migration.”

Tracking down repositories with the malicious workflow proved challenging, since GitHub doesn't index deleted branches, commits, or file contents. Still, we were able to uncover 64 additional repositories where a `shai-hulud` branch had been created, and in most of them, we found a commit containing the malicious workflow. In many cases, the workflow logs exposed sensitive secrets like GitHub tokens, NPM credentials, Atlassian keys, and Datadog API keys. These are still accessible as of writing this blog.

Despite the clear propagation of the worm to additional npm packages, we have not currently observed the creation of further repositories.

Revoke and regenerate all GitHub tokens, npm tokens, SSH keys, API keys, and environment variable secrets that may have been leaked in these repositories.

Mika AI, Wiz's AI assistant, can investigate new threat center items, analyze your environment for impact, and create recommendation plan to minimize impact, turning hours of manual analysis into minutes of AI-powered insights.

Simply ask Mika AI, *"How do I know if I'm affected by the latest Shai-Hulud NPM Supply Chain Attack?"*, and get comprehensive analysis, based on all Wiz capabilities of affected resources, exposure level, real-time threats and risk, and receive step-by-step remediation recommendations.

- @ctrl/deluge (7.2.2, 7.2.1)
- @ctrl/golang-template (1.4.3, 1.4.2)
- @ctrl/magnet-link (4.0.4, 4.0.3)
- @ctrl/ngx-codemirror (7.0.2, 7.0.1)
- @ctrl/ngx-csv (6.0.2, 6.0.1)
- @ctrl/ngx-emoji-mart (9.2.2, 9.2.1)
- @ctrl/ngx-rightclick (4.0.2, 4.0.1)

- @ctrl/qbittorrent (9.7.2, 9.7.1)
- @ctrl/react-adsense (2.0.2, 2.0.1)
- @ctrl/shared-torrent (6.3.2, 6.3.1)
- @ctrl/tinycolor@4.1.1, (4.1.2)
- @ctrl/torrent-file (4.1.2, 4.1.1)
- @ctrl/transmission (7.3.1)
- @ctrl/ts-base32 (4.0.2, 4.0.1)
- @nativescript-community/gesturehandler (2.0.35)
- @nativescript-community/sentry (4.6.43)
- @nativescript-community/text (1.6.13, 1.6.10, 1.6.11, 1.6.12, 1.6.9)
- @nativescript-community/ui-collectionview (6.0.6)
- @nativescript-community/ui-drawer (0.1.30)
- @nativescript-community/ui-image (4.5.6)
- @nativescript-community/ui-material-bottomsheet (7.2.72)
- @nativescript-community/ui-material-core (7.2.76, 7.2.72, 7.2.73, 7.2.74, 7.2.75)
- @nativescript-community/ui-material-core-tabs (7.2.76, 7.2.72, 7.2.73, 7.2.74, 7.2.75)
- @teselagen/bio-parsers (0.4.29, 0.4.30)
- @teselagen/bounce-loader (0.3.16, 0.3.17)
- @teselagen/file-utils (0.3.21, 0.3.22)
- @teselagen/liquibase-tools (0.4.1)
- @teselagen/ove (0.7.39, 0.7.40)
- @teselagen/range-utils (0.3.14, 0.3.15)
- @teselagen/react-list (0.8.19, 0.8.20)
- @teselagen/react-table (6.10.21, 6.10.19, 6.10.20, 6.10.22)
- @teselagen/sequence-utils (0.3.33, 0.3.34)
- @teselagen/ui (0.9.9, 0.9.10)

- angulartics2 (14.1.2, 14.1.1)
- encounter-playground (0.0.4, 0.0.5, 0.0.2, 0.0.3)
- eslint-config-teselagen (6.1.7, 6.1.8)
- graphql-sequelize-teselagen (5.3.8, 5.3.9)
- json-rules-engine-simplified (0.2.3, 0.2.4, 0.2.1)
- koa2-swagger-ui (5.11.2, 5.11.1)
- ng2-file-upload (8.0.3, 7.0.2, 7.0.3, 8.0.1, 8.0.2, 9.0.1)
- ngx-bootstrap (18.1.4, 19.0.3, 20.0.4, 20.0.5, 20.0.6, 19.0.4, 20.0.3)
- ngx-color (10.0.2, 10.0.1)
- ngx-toastr (19.0.2, 19.0.1)
- ngx-trend (8.0.1)
- oradm-to-gql (35.0.14, 35.0.15)
- oradm-to-sqlz (1.1.4, 1.1.2)
- ove-auto-annotate (0.0.9, 0.0.10)
- react-complaint-image (0.0.34, 0.0.35, 0.0.32)
- react-jsonschema-form-conditionals (0.3.20, 0.3.21, 0.3.18)
- react-jsonschema-form-extras (1.0.3, 1.0.4)
- react-jsonschema-rxnt-extras (0.4.8, 0.4.9)
- rxnt-authentication (0.0.5, 0.0.6, 0.0.3, 0.0.4)
- rxnt-healthchecks-nestjs (1.0.4, 1.0.5, 1.0.2, 1.0.3)
- rxnt-kue (1.0.6, 1.0.7, 1.0.4, 1.0.5)
- swc-plugin-component-annotate (1.9.2, 1.9.1)
- tg-client-query-builder (2.14.4, 2.14.5)
- tg-redbird (1.3.1, 1.3.2)
- tg-seq-gen (1.0.9, 1.0.10)
- ts-gaussian (3.0.6, 3.0.5)

- ve-bamreader (0.2.6, 0.2.7)
- ve-editor (1.0.1, 1.0.2)
- @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-node (2.0.13)
- @art-ws/di (2.0.28, 2.0.32)
- @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 (0.1.12, 0.1.9)
- @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 (1.0.10, 1.0.9)
- @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)
- @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/tinycolor (4.1.1, 4.1.2)
- @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)
- @nativescript-community/perms (3.0.5, 3.0.6, 3.0.7, 3.0.8, 3.0.9)
- @nativescript-community/sqlite (3.5.2, 3.5.3, 3.5.4, 3.5.5)
- @nativescript-community/typeorm (0.2.30, 0.2.31, 0.2.32, 0.2.33)
- @nativescript-community/ui-document-picker (1.1.27, 1.1.28, 13.0.32)
- @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-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)

- @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-angular (20.0.4)
- @nstudio/web (20.0.4)
- @nstudio/xplat-utils (20.0.5, 20.0.6, 20.0.7)
- @nstudio/xplat (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, 9.0.47, 9.0.48)
- @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, 9.0.49)
- @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, 9.0.49)
- @thangved/callback-window (1.1.4)
- @things-factory/attachment-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, 9.0.55)
- @things-factory/auth-base (9.0.42, 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, 9.0.55, 9.0.56, 9.0.57, 9.0.58, 9.0.59)
- @things-factory/env (9.0.42, 9.0.43, 9.0.44, 9.0.45)
- @things-factory/integration-base (9.0.42, 9.0.43, 9.0.44, 9.0.45)
- @things-factory/integration-marketplace (9.0.42, 9.0.43, 9.0.44, 9.0.45)
- @things-factory/shell (9.0.42, 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)
- browser-webdriver-downloader (3.0.8)
- capacitor-notificationhandler (0.0.2, 0.0.3)
- 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-yup (1.0.1)
- ember-headless-form (1.1.2, 1.1.3)
- 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)
- eslint-config-crowdstrike-node (4.0.3, 4.0.4)
- eslint-config-crowdstrike (11.0.2, 11.0.3)
- globalize-rpk (1.7.4)
- html-to-base64-image (1.0.2)
- jumpgate (0.0.2)
- 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)
- ngx-ws (1.1.5, 1.1.6)
- pm2-gelf-json (1.0.4, 1.0.5)
- printjs-rpk (1.6.1)
- remark-preset-lint-crowdstrike (4.0.1, 4.0.2)

- tbssnch (1.0.2)
- teselagen-interval-tree (1.1.2)
- thangved-react-grid (1.0.3)
- ts-imports (1.0.1, 1.0.2)
- tvi-cli (0.1.5)
- 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)
- devextreme-rpk (21.2.8)
- @basic-ui-components-stc/basic-ui-components (1.0.5)
