

Mini Shai-Hulud Strikes Again: TanStack + more npm Packages Compromised

By Rami McCarthy, Amitai Cohen, Benjamin Read

Published: 2026-05-12 · Archived: 2026-08-06 02:00:59 UTC

On 11 May 2026, TeamPCP launched a coordinated supply chain attack against the npm and PyPi ecosystems, compromising packages across multiple namespaces simultaneously.

May 13, 2026 2:30 UTC update: Further analysis of the `@uiopath/*` and `@mistralai/*` npm packages has identified a bug in the payload that renders the malware non-functional in those cases.

Impacted packages include:

- Packages in the `@tanstack` namespace, which includes `@tanstack/react-router`, one of the most widely-used routing libraries in the React ecosystem with approximately 12 million weekly downloads. [Postmortem](#)
- Packages in the `@uiopath` namespace, which provides tooling for UiPath's enterprise automation platform, including `@uiopath/apollo-core`, CLI tools, and agent SDKs. [Postmortem](#)
- The `@mistralai/mistralai` package, which is the official TypeScript client for the Mistral AI platform. The `mistralai` PyPi packages was also impacted. [Postmortem](#)
- The `guardrails-ai` LLM guardrails Python package.

See [Affected Packages](#) for detailed versions.

The **npm team is aware of the campaign and has been acting quickly** to remove the malicious package versions from the registry.

May 12, 2026, 11AM UTC update: Added additional IOCs and updated the affected packages table.

The TanStack vulnerability

The TanStack compromise exploited a chain of three vulnerabilities in GitHub Actions. The attacker created a fork of the `TanStack/router` repository (renamed to `zblgg/configuration` to evade fork-list searches), then opened a pull request that triggered a `pull_request_target` workflow. This workflow checked out and executed the attacker's fork code, which poisoned the GitHub Actions cache with a malicious pnpm store.

When legitimate maintainer PRs were later merged to `main`, the release workflow restored the poisoned cache. Attacker-controlled binaries then **extracted OIDC tokens directly from the GitHub Actions runner's process memory** (`/proc/<pid>/mem`). The attacker was able to use these tokens to publish the malicious package versions without ever stealing npm credentials.

The published packages contain two infection vectors: an `optionalDependencies` entry pointing to an orphan commit (`github:tanstack/router#79ac49eedf774dd4b0cfa308722bc463cfe5885c`) that executes a payload via a `prepare` script, and an embedded ~2.3MB obfuscated file `router_init.js` placed directly in the package tarball.

Shortly after the `@tanstack` attack, packages in the `@uiopath` namespace were compromised. These packages use a preinstall script (`node setup.mjs`) that downloads the Bun runtime and executes the payload. This is the same delivery mechanism that was seen in the earlier SAP compromise. The UiPath variant uses a re-obfuscated version of the same payload with **a different campaign key but identical C2 infrastructure**.

When executed, the payload is a credential stealer and self-propagating worm. It targets CI/CD tokens (GitHub Actions OIDC, GitLab, CircleCI), cloud credentials (AWS IMDSv2, GCP, Azure), Kubernetes service accounts, HashiCorp Vault, and package registry tokens. It uses stolen npm tokens and GitHub Actions OIDC tokens to publish poisoned versions of additional packages the victim has write access to, functioning as a worm that spreads through the npm ecosystem.

The payload exfiltrates stolen credentials via three redundant channels: a typosquat domain (`git-tanstack[.]com`), the decentralized Session messenger network, and GitHub API dead drops using stolen tokens.

On developer machines, the malware installs a persistent `gh-token-monitor` daemon (via macOS LaunchAgent or Linux systemd) that polls GitHub every 60 seconds. On receiving a `40X` error due to token revocation, **the monitor attempts to run** `rm -rf ~/` . The daemon automatically exits after 24 hours without triggering the destructive handler.

As with previous Mini Shai-Hulud variants, the malware checks if the system is configured for the Russian language and terminates without exfiltrating data if so.

Notable updates

This operation delivers a payload that uses the same methods used in previous TeamPCP operations but contains several notable evolutions.

Triple C2 architecture

The payload exfiltrates stolen credentials via three redundant channels:

1. **Typosquat domain:** `https://git-tanstack[.]com`
2. **Session messenger network:** Decentralized, encrypted exfiltration via `*.getsession.org` to recipient ID `05f9e609d79eed391015e11380dee4b5c9ead0b6e2e7f0134e6e51767a87323026`
3. **GitHub API dead drops:** Creates Dune-themed repositories using stolen tokens with `Shai-Hulud: Here We Go Again` as the repo description.

A message left on the C2 domain

The Session network channel is new. Decentralized and takedown-resistant, it is **significantly harder to disrupt** than dedicated domains or GitHub-based exfiltration.

GitHub token persistence wiper daemon

If the malware identifies any `ghp_` (GitHub Personal Access Tokens) or `gho_` (Oauth Tokens) it runs them through a series of checks:

- It must be a valid token that contains a login field
- It must include repo or public_repo in its scope
- It must have a public profile
- It must have the ability to write to a repo
- It must be a member of an org

If these all pass the malware installs a persistent `gh-token-monitor` daemon that polls GitHub every 60 seconds and triggers if the token checked is revoked.

- **macOS:** LaunchAgent at `~/Library/LaunchAgents/com.user.gh-token-monitor.plist`
- **Linux:** systemd user service at `~/.config/systemd/user/gh-token-monitor.service`

The handler command passed to the daemon is `rm -rf ~/`, wiping the home directory. The daemon automatically exits 24 hours after being started.

Python Variant

In addition to the npm compromises above, a malicious version of the PyPI package `guardrails-ai@0.10.1` was published, as was `mistralai@2.4.6`.

These trojanized packages operates notably differently from the JavaScript versions distributed via npm. The malicious package itself only contains 13 lines of new code. This code downloads and executes `git-tanstack[.]com/tmp/transformers.pyz`. Unlike other TeamPCP payloads this one is not obfuscated, but instead contains a modular credential stealer.

The stealer will only execute on linux machines and will exit if it is in an environment with Russian language settings or less than four CPUs. It gathers a variety of information, of note for the first time this includes password vaults (1Password, Bitwarden) and exfiltrates it to `83.142.209[.]194`, with GitHub as a fallback, in which case `PUSH UR T3MPRR` is used as the repository description.

If the package is executed on a system with location settings in Israel or Iran (via timezone and language) it invokes `random.randint(1,6)` and if that equals 2, it plays an mp3 file at full volume and runs `rm -rf`, attempting deleting the files in the system.

Note that in modern Linux variants running that command without the flag `--no-preserve-root` will fail.

May 13, 2026 2:30 UTC update

: An updated payload has been observed staged, resolving the bug with `rm -rf`.

Attribution

Wiz assesses with high confidence that this is the work of TeamPCP, the same operators behind the [SAP](#), [Checkmarx](#), Bitwarden, Lightning, Intercom, and [Trivy](#) compromises.

Indicators of compromise

File	Hash
router_init.js (2,341,681 bytes)	SHA256: ab4fcadaec49c03278063dd269ea5eef82d24f2124a8e15d7b90f2fa8601266c
router_init.js (2,339,346 bytes)	SHA256: 2ec78d556d696e208927cc503d48e4b5eb56b31abc2870c2ed2e98d6be27fc96 SHA1: e7d582b98ca80690883175470e96f703ef6dc497
setup.mjs (5,047 bytes)	SHA256: 2258284d65f63829bd67eaba01ef6f1ada2f593f9bbe41678b2df360bd90d3df SHA1: 12f35b1081b17d21815b35feb57ab03d02482116
Trojanized tarball	SHA256: 1e8538c6e0563d50da0f2e097e979ebd5294ce1defe01d0b9fe361ba3bed1898
opensearch_init.js	SHA1: 820fa07a7328b6cf2b417078e103721d4d8f2e79

Network indicators

Type	Indicator
C2 Domain	git-tanstack.com
Session Seed Nodes	seed1.getsession.org, seed2.getsession.org, seed3.getsession.org
Session File Server	filev2.getsession.org
Session Recipient ID	05f9e609d79eed391015e11380dee4b5c9ead0b6e2e7f0134e6e51767a87323026
C2 IP Address	83.142.209.194
PyPI Payload URL	git-tanstack.com/tmp/transformers.pyz

Additional Indicators

Type	Indicator
Service Name	gh-token-monitor
macOS Persistence	~/Library/LaunchAgents/com.user.gh-token-monitor.plist
Linux Persistence	~/.config/systemd/user/gh-token-monitor.service
Runtime Artifact	router_runtime.js
Runtime Artifact	tanstack_runner.js
Hook	preinstall: node setup.mjs
Git Dependency	github:tanstack/router#79ac49eedf774dd4b0cfa308722bc463cfe5885c
Bun Version	1.3.13
Repository Description	Shai-Hulud: Here We Go Again
Commit Message	IfYouRevokeThisTokenItWillWipeTheComputerOfTheOwner
Destructive Command	rm -rf ~/

What steps should security teams take?

Wiz customers should refer to the [Wiz Threat Intelligence Center Advisory](#) on this incident.

1. **Immediately identify exposure:** Search lockfiles and CI logs for affected package versions. Look for `router_init.js` or `setup.mjs` at package roots.
2. **Check for persistence:** Search for the `gh-token-monitor` daemon on developer machines and remove it. Do this before revoking GitHub tokens, to avoid the wiper.
3. **Rotate all credentials:** If exposure is suspected, rotate GitHub tokens, npm tokens, AWS credentials, Vault tokens, Kubernetes service accounts, and CI/CD secrets.
4. **Audit IDE directories:** Check `.claude/` and `.vscode/` directories for `router_runtime.js` or `setup.mjs`. These persist after npm uninstall.
5. **Block C2 infrastructure:** Block `git-tanstack.com` and `*.getsession.org` at DNS/proxy level.

For longer term hardening guidance, Wiz has developed:

- [How to Harden GitHub Actions: An Updated Guide](#)
- [Practical Package Security: The Unofficial Guide](#)

Affected packages

PyPi Packages

1. `guardrails-ai@0.10.1`
2. `mistralai@2.4.6`

npm Packages

Package	Affected Versions
@beproduct/nestjs-auth	0.1.2, 0.1.3, 0.1.4, 0.1.5, 0.1.6, 0.1.7, 0.1.8, 0.1.9, 0.1.10, 0.1.11, 0.1.12, 0.1.13, 0.1.14, 0.1.15, 0.1.16, 0.1.17, 0.1.18, 0.1.19
@cap-js/db-service	2.10.1
@cap-js/postgres	2.2.2
@cap-js/sqlite	2.2.2
@dirigible-ai/sdk	0.6.2, 0.6.3
@draftauth/client	0.2.1, 0.2.2
@draftauth/core	0.13.1, 0.13.2
@draftlab/auth	0.24.1, 0.24.2
@draftlab/auth-router	0.5.1, 0.5.2
@draftlab/db	0.16.1, 0.16.2
@mesadev/rest	0.28.3
@mesadev/saguaro	0.4.22
@mesadev/sdk	0.28.3
@mistralai/mistralai	2.2.2, 2.2.3, 2.2.4
@mistralai/mistralai-azure	1.7.1, 1.7.2, 1.7.3
@mistralai/mistralai-gcp	1.7.1, 1.7.2, 1.7.3
@ml-toolkit-ts/preprocessing	1.0.2, 1.0.3
@ml-toolkit-ts/xgboost	1.0.3, 1.0.4
@opensearch-project/opensearch	3.5.3, 3.6.2, 3.7.0, 3.8.0
@squawk/airport-data	0.7.4, 0.7.5, 0.7.6, 0.7.7, 0.7.8
@squawk/airports	0.6.2, 0.6.3, 0.6.4, 0.6.5, 0.6.6

Package	Affected Versions
@squawk/airspace	0.8.1, 0.8.2, 0.8.3, 0.8.4, 0.8.5
@squawk/airspace-data	0.5.3, 0.5.4, 0.5.5, 0.5.6, 0.5.7
@squawk/airway-data	0.5.4, 0.5.5, 0.5.6, 0.5.7, 0.5.8
@squawk/airways	0.4.2, 0.4.3, 0.4.4, 0.4.5, 0.4.6
@squawk/fix-data	0.6.4, 0.6.5, 0.6.6, 0.6.7, 0.6.8
@squawk/fixes	0.3.2, 0.3.3, 0.3.4, 0.3.5, 0.3.6
@squawk/flight-math	0.5.4, 0.5.5, 0.5.6, 0.5.7, 0.5.8
@squawk/flightplan	0.5.2, 0.5.3, 0.5.4, 0.5.5, 0.5.6
@squawk/geo	0.4.4, 0.4.5, 0.4.6, 0.4.7, 0.4.8
@squawk/icao-registry	0.5.2, 0.5.3, 0.5.4, 0.5.5, 0.5.6
@squawk/icao-registry-data	0.8.4, 0.8.5, 0.8.6, 0.8.7, 0.8.8
@squawk/mcp	0.9.1, 0.9.2, 0.9.3, 0.9.4, 0.9.5
@squawk/navaid-data	0.6.4, 0.6.5, 0.6.6, 0.6.7, 0.6.8
@squawk/navaids	0.4.2, 0.4.3, 0.4.4, 0.4.5, 0.4.6
@squawk/notams	0.3.6, 0.3.7, 0.3.8, 0.3.9, 0.3.10
@squawk/procedure-data	0.7.3, 0.7.4, 0.7.5, 0.7.6, 0.7.7
@squawk/procedures	0.5.2, 0.5.3, 0.5.4, 0.5.5, 0.5.6
@squawk/types	0.8.1, 0.8.2, 0.8.3, 0.8.4, 0.8.5
@squawk/units	0.4.3, 0.4.4, 0.4.5, 0.4.6, 0.4.7
@squawk/weather	0.5.6, 0.5.7, 0.5.8, 0.5.9, 0.5.10
@supersurkhet/cli	0.0.2, 0.0.3, 0.0.4, 0.0.5, 0.0.6, 0.0.7
@supersurkhet/sdk	0.0.2, 0.0.3, 0.0.4, 0.0.5, 0.0.6, 0.0.7
@tallyui/components	1.0.1, 1.0.2, 1.0.3
@tallyui/connector-medusa	1.0.1, 1.0.2, 1.0.3
@tallyui/connector-shopify	1.0.1, 1.0.2, 1.0.3
@tallyui/connector-vendure	1.0.1, 1.0.2, 1.0.3

Package	Affected Versions
@tallyui/connector-woocommerce	1.0.1, 1.0.2, 1.0.3
@tallyui/core	0.2.1, 0.2.2, 0.2.3
@tallyui/database	1.0.1, 1.0.2, 1.0.3
@tallyui/pos	0.1.1, 0.1.2, 0.1.3
@tallyui/storage-sqlite	0.2.1, 0.2.2, 0.2.3
@tallyui/theme	0.2.1, 0.2.2, 0.2.3
@tanstack/arktype-adapter	1.166.12, 1.166.15
@tanstack/eslint-plugin-router	1.161.9, 1.161.12
@tanstack/eslint-plugin-start	0.0.4, 0.0.7
@tanstack/history	1.161.9, 1.161.12
@tanstack/nitro-v2-vite-plugin	1.154.12, 1.154.15
@tanstack/react-router	1.169.5, 1.169.8
@tanstack/react-router-devtools	1.166.16, 1.166.19
@tanstack/react-router-ssr-query	1.166.15, 1.166.18
@tanstack/react-start	1.167.68, 1.167.71
@tanstack/react-start-client	1.166.51, 1.166.54
@tanstack/react-start-rsc	0.0.47, 0.0.50
@tanstack/react-start-server	1.166.55, 1.166.58
@tanstack/router-cli	1.166.46, 1.166.49
@tanstack/router-core	1.169.5, 1.169.8
@tanstack/router-devtools	1.166.16, 1.166.19
@tanstack/router-devtools-core	1.167.6, 1.167.9
@tanstack/router-generator	1.166.45, 1.166.48
@tanstack/router-plugin	1.167.38, 1.167.41
@tanstack/router-ssr-query-core	1.168.3, 1.168.6
@tanstack/router-utils	1.161.11, 1.161.14

Package	Affected Versions
@tanstack/router-vite-plugin	1.166.53, 1.166.56
@tanstack/solid-router	1.169.5, 1.169.8
@tanstack/solid-router-devtools	1.166.16, 1.166.19
@tanstack/solid-router-ssr-query	1.166.15, 1.166.18
@tanstack/solid-start	1.167.65, 1.167.68
@tanstack/solid-start-client	1.166.50, 1.166.53
@tanstack/solid-start-server	1.166.54, 1.166.57
@tanstack/start-client-core	1.168.5, 1.168.8
@tanstack/start-fn-stubs	1.161.9, 1.161.12
@tanstack/start-plugin-core	1.169.23, 1.169.26
@tanstack/start-server-core	1.167.33, 1.167.36
@tanstack/start-static-server-functions	1.166.44, 1.166.47
@tanstack/start-storage-context	1.166.38, 1.166.41
@tanstack/valibot-adapter	1.166.12, 1.166.15
@tanstack/virtual-file-routes	1.161.10, 1.161.13
@tanstack/vue-router	1.169.5, 1.169.8
@tanstack/vue-router-devtools	1.166.16, 1.166.19
@tanstack/vue-router-ssr-query	1.166.15, 1.166.18
@tanstack/vue-start	1.167.61, 1.167.64
@tanstack/vue-start-client	1.166.46, 1.166.49
@tanstack/vue-start-server	1.166.50, 1.166.53
@tanstack/zod-adapter	1.166.12, 1.166.15
@taskflow-corp/cli	0.1.24, 0.1.25, 0.1.26, 0.1.27, 0.1.28, 0.1.29
@tolka/cli	1.0.2, 1.0.3, 1.0.4, 1.0.5, 1.0.6
@uipath/access-policy-sdk	0.3.1
@uipath/access-policy-tool	0.3.1

Package	Affected Versions
@uipath/admin-tool	0.1.1
@uipath/agent-sdk	1.0.2
@uipath/agent-tool	1.0.1
@uipath/agent.sdk	0.0.18
@uipath/aops-policy-tool	0.3.1
@uipath/ap-chat	1.5.7
@uipath/api-workflow-tool	1.0.1
@uipath/apollo-core	5.9.2
@uipath/apollo-react	4.24.5
@uipath/apollo-wind	2.16.2
@uipath/auth	1.0.1
@uipath/case-tool	1.0.1
@uipath/cli	1.0.1
@uipath/codedagent-tool	1.0.1
@uipath/codedagents-tool	0.1.12
@uipath/codedapp-tool	1.0.1
@uipath/common	1.0.1
@uipath/context-grounding-tool	0.1.1
@uipath/data-fabric-tool	1.0.2
@uipath/docsai-tool	1.0.1
@uipath/filesystem	1.0.1
@uipath/flow-tool	1.0.2
@uipath/functions-tool	1.0.1
@uipath/gov-tool	0.3.1
@uipath/identity-tool	0.1.1
@uipath/insights-sdk	1.0.1

Package	Affected Versions
@uipath/insights-tool	1.0.1
@uipath/integrationservice-sdk	1.0.2
@uipath/integrationservice-tool	1.0.2
@uipath/llmgw-tool	1.0.1
@uipath/maestro-sdk	1.0.1
@uipath/maestro-tool	1.0.1
@uipath/orchestrator-tool	1.0.1
@uipath/packager-tool-apiworkflow	0.0.19
@uipath/packager-tool-bpmn	0.0.9
@uipath/packager-tool-case	0.0.9
@uipath/packager-tool-connector	0.0.19
@uipath/packager-tool-flow	0.0.19
@uipath/packager-tool-functions	0.1.1
@uipath/packager-tool-webapp	1.0.6
@uipath/packager-tool-workflowcompiler	0.0.16
@uipath/packager-tool-workflowcompiler-browser	0.0.34
@uipath/platform-tool	1.0.1
@uipath/project-packager	1.1.16
@uipath/resource-tool	1.0.1
@uipath/resourcecatalog-tool	0.1.1
@uipath/resources-tool	0.1.11
@uipath/robot	1.3.4
@uipath/rpa-legacy-tool	1.0.1
@uipath/rpa-tool	0.9.5

Package	Affected Versions
@uipath/solution-packager	0.0.35
@uipath/solution-tool	1.0.1
@uipath/solutionpackager-sdk	1.0.11
@uipath/solutionpackager-tool-core	0.0.34
@uipath/tasks-tool	1.0.1
@uipath/telemetry	0.0.7
@uipath/test-manager-tool	1.0.2
@uipath/tool-workflowcompiler	0.0.12
@uipath/traces-tool	1.0.1
@uipath/ui-widgets-multi-file-upload	1.0.1
@uipath/uipath-python-bridge	1.0.1
@uipath/vertical-solutions-tool	1.0.1
@uipath/vss	0.1.6
@uipath/widget.sdk	1.2.3
agentwork-cli	0.1.4, 0.1.5
cmux-agent-mcp	0.1.3, 0.1.4, 0.1.5, 0.1.6, 0.1.7, 0.1.8
cross-stitch	1.1.3, 1.1.4, 1.1.5, 1.1.6, 1.1.7
git-branch-selector	1.3.3, 1.3.4, 1.3.5, 1.3.6, 1.3.7
git-git-git	1.0.8, 1.0.9, 1.0.10, 1.0.11, 1.0.12
guardrails-ai	0.10.1
intercom-client	7.0.4
lightning	2.6.2, 2.6.3
mbt	1.2.48
mistralai	2.4.6
ml-toolkit-ts	1.0.4, 1.0.5
nextmove-mcp	0.1.3, 0.1.4, 0.1.5, 0.1.6, 0.1.7

Package	Affected Versions
safe-action	0.8.3, 0.8.4
ts-dna	3.0.1, 3.0.2, 3.0.3, 3.0.4, 3.0.5
wot-api	0.8.1, 0.8.2, 0.8.3, 0.8.4

References

- [TanStack acknowledgment](#)
- [Socket.dev: TanStack npm Packages Compromised](#)
- [StepSecurity: Mini Shai-Hulud is Back](#)

Source: <https://www.wiz.io/blog/mini-shai-hulud-strikes-again-tanstack-more-npm-packages-compromised>