

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

 aikido.dev/blog/shai-hulud-npm-bitwarden-cli-compromise

Ilyas Makari

April 23, 2026



Version **2026.4.0** of the widely-used **@bitwarden/cli** npm package (78,000 weekly downloads) has been identified as malicious. The package contains a sophisticated multi-stage credential theft worm that explicitly names itself **"Shai-Hulud: The Third Coming"**, a direct callback to [previous](#)

[Shai-Hulud supply chain campaigns](#), and targets developer credentials including SSH keys, cloud secrets, and even MCP configuration files.

This comes shortly after the recent compromise of Checkmarx, which included a Docker Hub project and a VS Code extension. It is believed that access gained during that campaign may have been leveraged to compromise Bitwarden's publishing pipeline. Notably, the attacker appears to have bypassed Bitwarden's trusted publishing controls by infecting the CI/CD pipeline itself (`publish-ci.yml` in github.com/bitwarden/clients), allowing a malicious package to be published under the legitimate `@bitwarden` name.

What Happened

`@bitwarden/cli@2026.4.0` introduced a malicious `preinstall` hook pointing to a new file `bw_setup.js`. This fires automatically on `npm install` with no user interaction required.

Stage 1: `bw_setup.js`

A cross-platform bootstrapper. It detects the victim's OS and architecture, downloads the legitimate Bun JavaScript runtime directly from github.com/oven-sh/bun, and uses it to execute the Stage 2 payload.

Stage 2: `bw1.js`

A 10 MB heavily obfuscated payload. Once deobfuscated, it is a fully featured credential harvester and supply chain worm. The behavior closely mirrors previous Shai-Hulud waves, and it even contains the string "Shai-Hulud: The Third Coming" hardcoded as the description for the public GitHub repository it creates to exfiltrate stolen data.

This version comes with heavy Dune universe theming throughout: the exfil repo is named from randomised Dune vocabulary (`fremen-sandworm-441`, `harkonnen-melange-7`, etc.), and the payload contains an embedded anti-AI manifesto that it attempts to write to victims' shell config files.

What It Steals

The malware scans a hardcoded list of high-value credential files on the victim's machine:

```
~/.ssh/id* / ~/.ssh/id_ (SSH private keys)
~/.ssh/known_hosts (SSH host fingerprints)
~/.ssh/keys (additional SSH key storage)
~/.aws/credentials (AWS access keys)
~/.config/gcloud/credentials.db (GCP credentials)
~/.npmrc / .npmrc (npm auth tokens)
~/.claude.json / .claude.json (Claude Code auth token)
~/.claude/mcp.json (Claude Code MCP server configs, may contain API keys and DB
credentials)
~/.kiro/settings/mcp.json (Kiro MCP server configs)
.git/config (Git remote URLs and credentials)
.git-credentials (stored Git passwords)
.env (project environment variables and API keys)
~/.bash_history / ~/.zsh_history
```

Beyond local files, the malware also runs collectors for AWS SSM Parameter Store, AWS Secrets Manager, Azure Key Vault, and GCP Secret Manager using ambient cloud credentials. Anyone running this on a cloud-connected developer machine or CI runner loses their entire secrets infrastructure.

The malware contacts two C2 URLs:

- [hxxps://audit.checkmarx\[.\]cx/v1/telemetry](https://hxxps://audit.checkmarx[.]cx/v1/telemetry) — primary C2, hit directly on every infection. Not a legitimate Checkmarx domain; [.cx](https://hxxps://audit.checkmarx[.]cx/v1/telemetry) is the Christmas Island TLD. Block this immediately.
- [hxxps://api.github\[.\]com/search/commits?q=beautifulcastle%20](https://hxxps://api.github[.]com/search/commits?q=beautifulcastle%20) — fallback. If the primary C2 is down, the malware searches these GitHub commits for a signed replacement hostname.

The Shai-Hulud Propagation

We found evidence of Shai-Hulud-like propagation. Stolen data is exfiltrated to a public GitHub repository created under the victim's own account. For victims without org membership, their GitHub token is also published into a public GitHub commit dead-drop where other infected machines can find and reuse it to fund their own exfiltration. Victims with org membership have their token kept private inside the encrypted exfil data only.

How Aikido Detects This

If you are an Aikido user, check your central feed and filter on malware issues. This will surface as a 100/100 critical issue. Aikido rescans nightly, but we recommend triggering a manual rescan now.

If you are not yet an Aikido user, you can [create an account](#) and connect your repos. Our malware coverage is included in the free plan, no credit card required.

For broader coverage across your whole team, Aikido's [Endpoint Protection](#) gives you visibility and control over the software packages installed on your team's devices. It covers browser extensions, code libraries, IDE plugins, and build dependencies, all in one place. Stop malware before it gets installed.

For future protection, consider [Aikido Safe Chain](#) (open source). Safe Chain sits in your existing workflow, intercepting npm, npx, yarn, pnpm, and pnpm commands and checking packages against [Aikido Intel](#) before install.

IOCs

- Package: `@bitwarden/cli` (version 2026.4.0)
- Preinstall file: `bw_setup.js`
SHA256: `37f34aa3b86db6898065f3ca886031978580a15251f2576f6d24c3b778907336`
- Payload file: `bw1.js`
SHA256: `18f784b3bc9a0bcdcb1a8d7f51bc5f54323fc40cbd874119354ab609bef6e4cb`
- GitHub repo description: `Shai-Hulud: The Third Coming`
- Exfiltration endpoint: `audit.checkmarx[.]cx:443/v1/telemetry`
- Public commit messages starting with `LongLiveTheResistanceAgainstMachines`