

Stardrop Supply Chain Attack Targets Venture Capital Firms, Luxury Brands, and AI Companies

 opensourcemalware.com/blog/stardrop-attack

OpenSourceMalware.com

April 14, 2026



OpenSourceMalware has identified an ongoing threat campaign that has published more than 200 packages to NPM so far. These packages have names like "huggingface-cli", "webflow", "bessemer-vc", "omaha", "codeium", "givenchy" and "khosla-vc". The malicious packages pretend to deliver a new AI coding agent named "Stardrop", hence the name of this threat campaign.

Our malware analysis started identifying these packages on the 9th of April, and we have seen an average of 40+ packages per day since then. In a really unique circumstance NPM has been yanking these from the registry very quickly so there are no OSV or GHSA advisories for these packages. This might seem like the attack has been nullified but unfortunately, most of the global CDNs have picked up these packages and we've confirmed that these packages can be installed via Chinese and european NPM mirrors.

Unique Characteristics

These packages all use non-standard version numbers like:

0.0.0-dev-202603281859 0.0.0-dev-202603281254 0.0.0-dev-202603280649 0.0.0-dev-202603280649 0.0.0-dev-202603281254

In addition, each of the 200+ packages have a package.json that installs additional packages:

```

{
  "name": "minneapolis",
  "bin": {
    "minneapolis": "./bin/stardrop"
  },
  "scripts": {
    "postinstall": "bun ./postinstall.mjs || node ./postinstall.mjs"
  },
  "version": "0.0.0-dev-202603280649",
  "optionalDependencies": {
    "stardrop-linux-arm64": "0.0.0-dev-202603280649",
    "stardrop-linux-x64": "0.0.0-dev-202603280649",
    "stardrop-linux-x64-baseline": "0.0.0-dev-202603280649",
    "stardrop-linux-arm64-musl": "0.0.0-dev-202603280649",
    "stardrop-linux-x64-musl": "0.0.0-dev-202603280649",
    "stardrop-linux-x64-baseline-musl": "0.0.0-dev-202603280649",
    "stardrop-darwin-arm64": "0.0.0-dev-202603280649",
    "stardrop-darwin-x64": "0.0.0-dev-202603280649",
    "stardrop-darwin-x64-baseline": "0.0.0-dev-202603280649",
    "stardrop-windows-x64": "0.0.0-dev-202603280649",
    "stardrop-windows-x64-baseline": "0.0.0-dev-202603280649"
  }
}

```

These optional dependencies are where the real malicious payloads are. If you dig into these dependency packages you'll see that the package.json files are placeholders and the real intent by the authors is to make the binary payloads available

Technical Analysis

Stage 1: NPM Package Structure

The initial dropper consists of three main components:

- **package.json** - Declares optional dependencies for 11 platform-specific binaries
- **postinstall.mjs** - Automatic deployment script executed via npm's postinstall hook
- **bin/stardrop** - JavaScript wrapper for binary execution

The package leverages npm's optional dependencies feature to distribute platform-specific payloads:

```

{
  "optionalDependencies": {
    "stardrop-linux-arm64": "0.0.0-dev-202603281859",
    "stardrop-linux-x64": "0.0.0-dev-202603281859",
    "stardrop-linux-x64-baseline": "0.0.0-dev-202603281859",
    // ... 8 more platform variants
  }
}

```

Stage 2: Automated Deployment

The **postinstall.mjs** script performs sophisticated environment detection and binary deployment:

1. **OS/Architecture Detection:** Uses Node.js **os** module to identify the victim's platform
2. **Binary Resolution:** Locates appropriate platform-specific package in `node_modules`
3. **Symlink Creation:** Establishes binary accessibility through command-line PATH
4. **Stealth Operation:** Provides legitimate-sounding output to avoid suspicion

The deployment process is designed to fail gracefully, avoiding detection through installation errors.

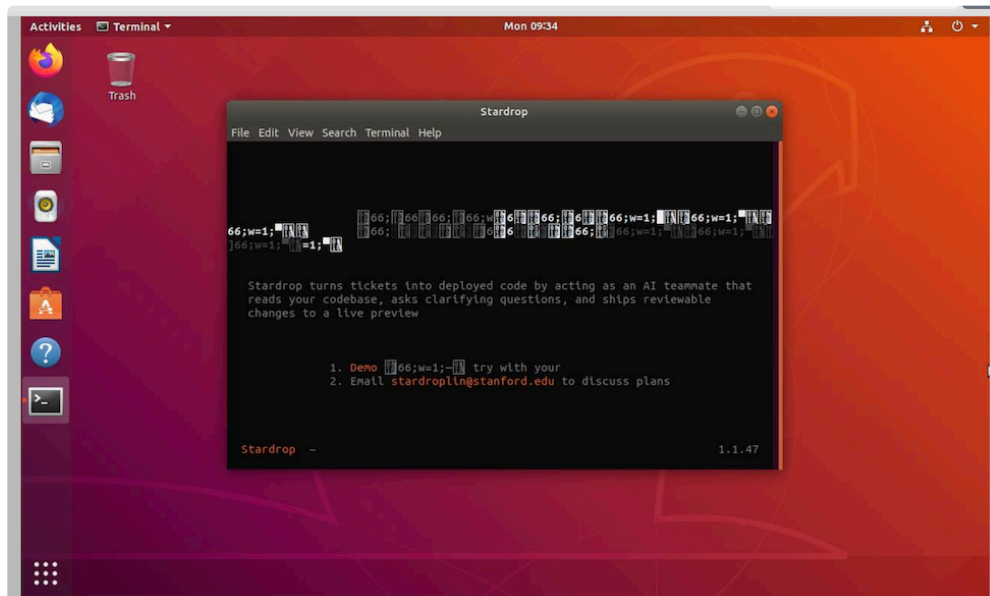
Stage 3: Binary Payloads

We successfully obtained and analyzed three platform-specific binary packages:

- **stardrop-linux-x64-1.1.47.tgz** (50MB compressed, 144MB executable)
- **stardrop-darwin-arm64-1.1.49.tgz** (33MB compressed, 99MB executable)

- [stardrop-windows-x64-1.1.47.tgz](#) (52MB compressed, 153MB executable)

When the binary payloads are run, a terminal window pops up and prompts the user for user information and OpenAI or Anthropic API keys. Meanwhile, in the background the malware is already harvesting [~/.local/share/stardrop/auth.json](#) and other files for credentials.



Binary Analysis Findings

The binary payloads are info stealers that focus on cloud and AI credential harvesting. It saves the harvested creds at [~/.local/share/stardrop/registration.json](#)

- References to cloud metadata services (AWS EC2 metadata at 169.254.169.254)
- Cloudflare R2 storage infrastructure references
- Cryptographic key handling capabilities

Windows Payload

When the windows payload is run, the exe initially scans for credentials and then downloads a file and saves it as [C:\Users\Admin\AppData\Local\Temp\.79f7f37b7f7bffff1-00000000.dll](#)

MacOS Payload

We saw a more complete info stealer set of behaviours with the MacOS payload. We suspect this is the primary target for the Stardrop campaign

Indicators of Compromise (IOCs)

NPM Packages

Here's a complete list of the packages we know about so far. Each of these has been tagged and can be found in OSM via the [#stardrop](#) tag.

a16z, abudhabi, acr-agent, addisababa, agentcoder, ai-pair, allahabad, anaheim, andreessen, anyscale, arbitrum, arlington, asuncion, baltimore, bamako, bareilly, barnaul, baserow, belfast, belgrade, berachain, vc, bhopal, bhubaneswar, bilbao, bito-ai, bolt-new, brussels, cardiff, cerebras-ai, chennai, cline-ai, cnvrg, coatue, cocopilot, codeassistant, codebooga, codecompanion, codeium, codemate, codepartner, codeqwen, coderabbit, coderabbit-ai, codiga-ai, cody-ai, coimbatore, continue-dev, coreweave, cortana, coveragent, cursor-ai, dafny, dehradun, determined-ai, devika, dfgrowth, dongguan, dragonfly-vc, eindhoven, faridabad, felicity-vc, fireworks-ai, foshan, founders-fund, foundersf, frankfurt, fukuoka, gangtok, ggvcapital, ghaziabad, ghostty-cli, givenchy, gothenburg, groq-ai, gurgaon, guwahati, hamburg, hanover, helix-editor, howrah, huggingface-cli, imphal, inflection-ai, instacart, irkutsk, isabelle, islamabad, jacksonville, jodhpur, johannesburg, kamatera, kampala, kanpur, khartoum, khosla-vc, kinshasa, kolkata, lamborghini, lapaz, lapce-editor, lille, lmstudio-cli, louisville, louisvuitton, lovable-ai, luanda, lucknow, lux-capital, madrid, madurai, mangalore, marseille, matrixpartners, midjourney-ai, milwaukee, mogadishu, mosaic-ml, multicoincv, munich, nashik, northface, nusmv, ohmyzsh, omaha, paperspace, paradigm-vc, patagonia, philadelphia, polychain, pondicherry, qingdao, rajkot, redpoint-vc, reebok, rewind-ai, ribbit-capital, riyadh, runpod, sacramento, saintpetersburg, sanjose, santaana, seville, shenyang, smol-developer, socialcapital, sourcepilot, sourcery-ai, squarespace, srinagar, starcoder, stardrop-darwin-x64-baseline, stardrop-linux-arm64, stardrop-linux-

arm64-musl,stardrop-linux-x64,stardrop-linux-x64-musl,stardrop-windows-x64,stardrop-windows-x64-baseline,strasbourg,stuttgart,supermaven,supermaven-ai,tabby-ai,tabnine-ai,taskweaver,tianjin,tirupati,tiruppur,tolyatti,tooljet,trivandrum,ujjain,upstartportal,utrecht,v0-dev,vadodara,valentino,varanasi,versace,vijayawada,visakhapatnam,warp-terminal,warsaw,webflow,wichita,windsurf-ai,wizardcoder,ycombinator,zaragoza,zed-editor

File Hashes

Main Package:

- SHA-256: d780fe3b635ff099682677f3c93e42d789e572926fd0db076c27e775bb109b06
- MD5: d70e7e37dfa4cf501cbd0ef6a236c84b

Linux Binary (stardrop-linux-x64-1.1.47.tgz):

- SHA-256: 18e8742fb6fb5e70c0c91823d72f5d9074be1d1cba1cbfc0eca75b5427e544da
- MD5: 43f446a86f1fbee74a486185c6dc1d51

macOS Binary (stardrop-darwin-arm64-1.1.49.tgz):

- SHA-256: 646f3904ff03e64229f938ac23fa8bb79ed1658ee5aa0bee4aa8909f38f763cd
- MD5: 823f13d45fe0dd05d2f1ac4344d8ae75

Windows Binary (stardrop-windows-x64-1.1.47.tgz):

- SHA-256: f2248973be75ce70b96424edb405d5a9af3c1fbca378566bfff3c0a0994d6f48
- MD5: 29b31bb2a2c4fbe0c3cec2022562927c

Network Indicators

- stardrop.dev
- p9ia72yajp.us-east-1.awsapprunner.com

Behavioral Indicators

- Environment variable STARDROP_BIN_PATH for binary override
- Injects into the .github/workflows/stardrop.yml workflow

File Hashes and IOCs: Reach out to the OSM team if you want more detailed information about this malware campaign and its TTPs