

Target hyperliquid-stock-perps-snapshot

# No malicious behavior observed

We ran it 4 times, with a normal setup, a GitHub Actions environment and cloud credentials present. It contacted api.hyperliquid.xyz, example.com and finch-agent-catalog.finch-catalog-mcp.workers.dev. It did not touch the fake credentials we planted, and nothing it sent carried them.

| Recommendation          | Confidence | Findings                   |
|-------------------------|------------|----------------------------|
| <b>No action needed</b> | <b>n/a</b> | <b>0 high 0 med 1 info</b> |

Nothing observed calls for action. This is evidence, not a guarantee.

## Scope

|         |                                                                                                                                                                           |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Package | hyperliquid-stock-perps-snapshot                                                                                                                                          |
| Source  | clawhub 1.0.0                                                                                                                                                             |
| SHA-256 | 28709455499879fc385b31d979acd1b0d67a936220ad2418b48ca018baaaf238                                                                                                          |
| Files   | 3                                                                                                                                                                         |
| Scanned | 27 Oct 2026, 13:01 UTC                                                                                                                                                    |
| Engine  | detonator 0.5.1                                                                                                                                                           |
| Method  | Executed in an isolated sandbox with decoy credentials and a captive network; every file access, process and connection traced. 4 runs: baseline, ci-github, cloud-creds. |
| Note    | batch:clawhub:2026-10-27                                                                                                                                                  |

## Findings summary

| ID  | Severity | Confidence | Finding                        |
|-----|----------|------------|--------------------------------|
| F01 | Low      | Info       | Network destinations contacted |

## Observed behavior

|              |                                                                                                                                                                                                                                                                       |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Install step | none                                                                                                                                                                                                                                                                  |
| Runs as      | <pre>curl -s -X POST https://finch-agent-catalog.finch-catalog-mcp.workers.dev... -H; curl -s -i -X POST https://finch-agent-catalog.finch-catalog-mcp.workers.dev...; head -60; head -c 3000; curl -s -X POST https://api.hyperliquid.xyz/info -H; head -c 500</pre> |



|               |                                                                                                                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network       | api.hyperliquid.xyz (1 conn, 154 B sent; while running)<br>example.com (1 conn, 144 B sent; while running)<br>finch-agent-catalog.finch-catalog-mcp.workers.dev (10 conn, 2781 B sent; while running) |
| Credentials   | no planted credential touched                                                                                                                                                                         |
| Files written | nothing outside its own folder                                                                                                                                                                        |

## Finding details

### F01 Network destinations contacted

Severity: Low Confidence: Info Observed in: obedient:baseline, llm:baseline  
The package connected to these hosts.

#### Description

Network destinations the package resolved or connected to during the runs. All traffic was captured by the sandbox; nothing reached the internet.

#### Impact

Context only. Unexpected destinations are worth checking against what the package claims to do.

#### Evidence

finch-agent-catalog.finch-catalog-mcp.workers.dev

api.hyperliquid.xyz

example.com

#### Remediation

Confirm each host is expected (the package's API, its registry). Allowlist expected egress in production.

## Run log

**obedient:baseline ok 1.0s**

new behavior: dns:finch-agent-catalog.finch-catalog-mcp.workers.dev, exec:curl

**obedient:ci-github ok 1.0s**

no new behavior

**obedient:cloud-creds ok 0.8s**

no new behavior

**llm:baseline ok 18.7s**

new behavior: dns:api.hyperliquid.xyz, dns:example.com | 5 model steps, 4 commands

Observed behavior only. A clean result does not prove a package is safe. Findings describe what Detonator observed during these runs, not a guarantee about code paths it did not reach.