

Target ofac-crypto-address-check

No malicious behavior observed

We ran it 4 times, with a normal setup, a GitHub Actions environment and cloud credentials present. It contacted 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
No action needed	n/a	0 high 0 med 2 info

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

Scope

Package	ofac-crypto-address-check
Source	clawhub 1.0.0
SHA-256	33a6e59cb4d48bd8879e426863802d59ff62bdd9ae27b40290b3e9bf9b2e613f
Files	3
Scanned	27 Oct 2026, 13:02 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
F02	Low	Info	Loaded the project's .env file

Observed behavior

Install step	none
Runs as	<pre>curl -s -X POST https://finch-agent-catalog.finch-catalog-mcp.workers.dev... -H; ls -la ./skill; head -50; cat ./skill/SKILL.md; cat ./skill/_meta.json; cat ./skill/skill-card.md</pre>
Network	finch-agent-catalog.finch-catalog-mcp.workers.dev (3 conn, 996 B sent; while running)

Credentials	./.env (read)
Files written	nothing outside its own folder

Finding details

F01 Network destinations contacted

Severity: Low Confidence: Info Observed in: obedient: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
```

Remediation

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

F02 Loaded the project's .env file

Severity: Low Confidence: Info Observed in: llm:baseline
The package loaded the project's .env file.

Description

The process loaded the project's .env file. Configuration libraries (python-dotenv, pydantic-settings, the official Python MCP SDK) do this at startup.

Impact

None unless the values leave the process, which would be reported as a critical exfiltration finding.

Evidence

```
./.env (by sed)
```

Remediation

No action needed. Keep long-lived secrets out of project .env files where possible.

Run log

obedient:baseline ok 0.6s

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

obedient:ci-github ok 0.9s

no new behavior

obedient:cloud-creds ok 1.1s

no new behavior



llm:baseline ok 10.3s

new behavior: ownread:./env | 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.