Target localization-push

No malicious behavior observed

We ran it 1 time, with a normal setup. It contacted api.appgoat.ai. 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	localization-push
Source	clawhub 1.0.0
SHA-256	0dd5294196d1aa2ab0242f2cff6bca67642ccafcafa49f93f5f0f9f995a3c5d3
Files	4
Scanned	27 Oct 2026, 12:26 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. 1 runs: baseline.
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	ls -la; ls -R ./skill; head -50; cat ./skill/reference/api.md; head -200; cat .env
Network	api.appgoat.ai (3 conn, 307 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: 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

```
api.appgoat.ai
```

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 cat)
```

Remediation

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

Run log

llm:baseline ok 15.9s

new behavior: dns:api.appgoat.ai, exec:curl, ownread:./.env | 6 model steps, 6 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.