

Target aimegeo-knowledge-distill

No malicious behavior observed

We ran it 8 times, with a normal setup, LC_MESSAGES set, docs:index --sources examples/input, CURL_CA_BUNDLE and DENO_CERT and GIT_SSL_CAINFO and LC_MESSAGES... set and a GitHub Actions environment. It made no network connections. 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 0 info

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

Scope

Package	aimegeo-knowledge-distill
Source	clawhub 1.0.1
SHA-256	ebefe5eb14b8800956daf6b41e8651124df4151b53744051d8ecf06c3372da14
Files	29
Scanned	27 Oct 2026, 11:25 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. 8 runs: baseline, guided:LC_MESSAGES, docs:index --sources examples/input, guided:CURL_CA_BUNDLE,DENO_CERT,GIT_SSL_CAINFO,LC_MESSAGES..., ci-github, guided:CI,CURL_CA_BUNDLE,DENO_CERT,GITHUB_ACTIONS....
Note	batch:clawhub:2026-10-27

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/knowledge.py; python3 <skill>/scripts/knowledge.py index --sources examples/input; python3 <skill>/scripts/self_test.py; /usr/bin/python3 /tmp/knowledge-distill-test-g8326q6t/standalone/scripts/k... check --sour; /usr/bin/python3 /tmp/knowledge-distill-test-1uhb2zf_/standalone/scripts/k... check --sour; /usr/bin/python3 /tmp/knowledge-distill-test-cj00pusn/standalone/scripts/k... check --sour
Network	no connections



Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log

scripts:baseline ok 1.6s

no new behavior

scripts:guided:LC_MESSAGES ok 1.1s

no new behavior

scripts:docs:index --sources examples/input ok 2.7s

no new behavior

scripts:baseline ok 12.5s

new behavior: write:./="èj",ä,".txt, write:./bad.json, write:./bundle.json, write:./deadlines.txt, write:./decimal-result

scripts:guided:CURL_CA_BUNDLE,DENO_CERT,GIT_SSL_CAINFO,LC_MESSAGES... ok 8.4s

no new behavior

scripts:ci-github ok 9.4s

no new behavior

scripts:guided:CI,CURL_CA_BUNDLE,DENO_CERT,GITHUB_ACTIONS... ok 10.3s

no new behavior

scripts:cloud-creds ok 9.5s

no new behavior

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.