

Target cgartlab-down

No malicious behavior observed

We ran it 8 times, with a normal setup, LOCALAPPDATA and NO_PROXY set, a GitHub Actions environment and LC_MESSAGES and LOCALAPPDATA set. 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	cgartlab-down
Source	clawhub 0.2.0
SHA-256	6c8c301fafa06a871d734184e173f0afa8126b9dfea1c9050a703854e9cba6bc
Files	22
Scanned	26 Oct 2026, 19:27 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:LOCALAPPDATA,NO_PROXY, ci-github, guided:LC_MESSAGES,LOCALAPPDATA.
Note	batch:clawhub:2026-10-26

Observed behavior

Install step	none
Runs as	python3 <skill>/evals/__init__.py; python3 <skill>/evals/test_check_tools.py; python3 <skill>/evals/test_detect.py
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log

scripts:baseline ok 0.5s
no new behavior



scripts:guided:LOCALAPPDATA,NO_PROXY ok 0.8s
no new behavior

scripts:ci-github ok 0.9s
no new behavior

scripts:baseline ok 2.5s
no new behavior

scripts:guided:LC_MESSAGES,LOCALAPPDATA ok 3.2s
no new behavior

scripts:guided:LOCALAPPDATA,NO_PROXY ok 2.6s
no new behavior

scripts:baseline ok 2.8s
no new behavior

scripts:guided:LC_MESSAGES,LOCALAPPDATA ok 1.3s
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.