

Target aimegeo-campaign-plan

No malicious behavior observed

We ran it 8 times, with a normal setup, LC_MESSAGES set, docs:examples/qinghe/campaign.json and date>2026-10-29 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	aimegeo-campaign-plan
Source	clawhub 1.0.1
SHA-256	e80aa0c351332d9390aff59bb3e2cbf81d2bca512bbb87551adc692ec121ac56
Files	24
Scanned	27 Oct 2026, 11:34 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:examples/qinghe/campaign.json, guided:date>2026-10-29.
Note	batch:clawhub:2026-10-27

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/check_campaign.py; python3 <skill>/scripts/check_campaign.py examples/qinghe/campaign.json; python3 <skill>/scripts/self_test.py; /usr/bin/python3 <skill>/scripts/check_campaign.py /tmp/campaign-input-w0l9mgzj/bad.json; /usr/bin/python3 <skill>/scripts/check_campaign.py /tmp/campaign-input-w0l9mgzj/absent.js; /usr/bin/python3 <skill>/scripts/check_campaign.py <skill>/examples/qinghe/campaign.json
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder



Run log

scripts:baseline ok 2.5s

no new behavior

scripts:guided:LC_MESSAGES ok 2.4s

no new behavior

scripts:docs:examples/qinghe/campaign.json ok 1.6s

no new behavior

scripts:baseline ok 9.4s

new behavior: write:./bad.json, write:./campaign.json, write:./check_campaign.py, write:./examples, write:./scripts

scripts:guided:LC_MESSAGES ok 5.2s

no new behavior

scripts:guided:date>2026-10-29 ok 6.1s

no new behavior

obedient:baseline ok 8.3s

no new behavior

obedient:guided:LC_MESSAGES ok 6.5s

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.