

Target popnow-media

No malicious behavior observed

We ran it 8 times, with a normal setup, the environment variables it says it needs, POPNOW_API_KEY set and LC_MESSAGES 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	popnow-media
Source	clawhub 1.0.0
SHA-256	c5a8096c33be9cae88f79a0bfb923b7bff9533ca3feae3396c9222d596b14266
Files	6
Scanned	27 Oct 2026, 12:05 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, declared-env, guided:POPNOW_API_KEY, guided:LC_MESSAGES.
Note	batch:clawhub:2026-10-27

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/client.py; python3 <skill>/scripts/popnow.py; python3 scripts/popnow.py models --search image; python3 scripts/popnow.py balance
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log

scripts:baseline ok 2.9s
no new behavior



scripts:declared-env ok 3.6s

no new behavior

scripts:guided:POPNOW_API_KEY ok 2.4s

no new behavior

scripts:baseline ok 4.0s

no new behavior

scripts:guided:LC_MESSAGES ok 3.5s

no new behavior

scripts:declared-env ok 4.3s

no new behavior

obedient:baseline ok 8.8s

no new behavior

obedient:declared-env ok 5.4s

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.