

Target ats-keyword-extractor

No malicious behavior observed

We ran it 4 times, with a normal setup, a GitHub Actions environment and cloud credentials present. 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	ats-keyword-extractor
Source	clawhub 1.0.0
SHA-256	36b8bde9336795e5e025d1c6fcc002130879bc20ffb6cb87e42274cc8c5a3968
Files	3
Scanned	27 Oct 2026, 13:02 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. 4 runs: baseline, ci-github, cloud-creds.
Note	batch:clawhub:2026-10-27

Observed behavior

Install step	none
Runs as	python3 -c import json,urllib.request a={"job_description":open("jd...; ls -la; ls -la skill; cat README.md; cat package.json; ls -la src
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log



obedient:baseline ok 2.0s

no new behavior

obedient:ci-github ok 2.3s

no new behavior

obedient:cloud-creds ok 1.4s

no new behavior

llm:baseline ok 24.5s

no new behavior | 4 model steps, 3 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.