

Target `cgartlab-search`

No malicious behavior observed

We ran it 8 times, with a normal setup, BRAVE_SEARCH_API_KEY and EXA_API_KEY and PYTHON and TENCENT_NEWS_CLI_PATH... set, a GitHub Actions environment and BRAVE_SEARCH_API_KEY and CONTEXT7_API_KEY and EXA_API_KEY and TENCENT_NEWS_KEY... 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	<code>cgartlab-search</code>
Source	<code>clawhub 0.1.1</code>
SHA-256	<code>fff177e4ec8e28ae560f404c944d80d1f28cfd4096c8a94659ead99767b5ce6d</code>
Files	<code>17</code>
Scanned	<code>26 Oct 2026, 19:28 UTC</code>
Engine	<code>detonator 0.5.1</code>
Method	<code>Executed in an isolated sandbox with decoy credentials and a captive network; every file access, process and connection traced. 8 runs: baseline, guided:BRAVE_SEARCH_API_KEY,EXA_API_KEY,PYTHON,TENCENT_NEWS_CLI_PATH..., ci-github, guided:BRAVE_SEARCH_API_KEY,CONTEXT7_API_KEY,EXA_API_KEY,TENCENT_NEWS_KEY</code>
Note	<code>batch:clawhub:2026-10-26</code>

Observed behavior

Install step	<code>none</code>
Runs as	<code>bash <skill>/scripts/gate.sh; dirname <skill>/scripts/gate.sh; python3 -c print(1); node --check scripts/search.mjs; bash -n scripts/search.sh; python3 -c import json,sys,json.load(sys.stdin)</code>
Network	<code>no connections</code>
Credentials	<code>no planted credential touched</code>



Files written nothing outside its own folder

Run log

scripts:baseline ok 6.5s

no new behavior

scripts:guided:BRAVE_SEARCH_API_KEY, EXA_API_KEY, PYTHON, TENCENT_NEWS_CLI_PATH... ok 5.5s

no new behavior

scripts:ci-github ok 5.5s

no new behavior

scripts:baseline ok 0.8s

no new behavior

scripts:guided:BRAVE_SEARCH_API_KEY, CONTEXT7_API_KEY, EXA_API_KEY, TENCENT_NEWS_KEY... ok 0.7s

no new behavior

scripts:guided:BRAVE_SEARCH_API_KEY, EXA_API_KEY, PYTHON, TENCENT_NEWS_CLI_PATH... ok 1.1s

no new behavior

scripts:baseline ok 0.4s

no new behavior

scripts:guided:BRAVE_SEARCH_API_KEY, CONTEXT7_API_KEY, EXA_API_KEY, TENCENT_NEWS_KEY... ok 0.6s

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.