

Target dataify-ai-web-search

No malicious behavior observed

We ran it 8 times, with a normal setup, a GitHub Actions environment, a production environment, LC_MESSAGES set and docs:web --query. 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	dataify-ai-web-search
Source	clawhub 1.1.0
SHA-256	4e8c68e52d3083f20a0f4b9308b9245bfeecfabf070ce69194aed2264ed88717
Files	8
Scanned	26 Oct 2026, 19:07 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, ci-github, production, guided:LC_MESSAGES, docs:web --query, guided:AI_WEB_API_BASE_URL,DATAIFY_API_TOKEN,LC_MESSAGES.
Note	batch:clawhub:2026-10-26

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/ai_web_client.py; python3 <skill>/scripts/search.py; python3 <skill>/scripts/search.py web --query; python3 scripts/search.py web --query AI news --time-range; python3 scripts/search.py shopping --query wireless mouse --dry-run; python3 scripts/search.py news --query latest technology news --time-range
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder



Run log

scripts:baseline **ok** **1.7s**

no new behavior

scripts:ci-github **ok** **2.1s**

no new behavior

scripts:production **ok** **2.0s**

no new behavior

scripts:baseline **ok** **2.0s**

no new behavior

scripts:guided:LC_MESSAGES **ok** **2.8s**

no new behavior

scripts:docs:web --query **ok** **1.6s**

no new behavior

obedient:baseline **ok** **9.9s**

no new behavior

obedient:guided:AI_WEB_API_BASE_URL,DATAIFY_API_TOKEN,LC_MESSAGES **ok** **7.4s**

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.