Target keyword-radar

No malicious behavior observed

We ran it 8 times, with a normal setup, LC_MESSAGES set, docs:setup, ARI_BASE_URL and LC_MESSAGES and REQUEST_METHOD and SSLKEYLOGFILE set and docs:configure. It contacted ari.funewa.com. 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 1 info**

Nothing observed calls for action. This is evidence, not a guarantee.

Scope

Package	keyword-radar
Source	clawhub 1.5.3
SHA-256	8111647b84e887d42a07e21a53e29f7db3a192dfd8b69071973f6370188d4a84
Files	10
Scanned	26 Oct 2026, 17:36 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:setup, guided:ARI_BASE_URL,LC_MESSAGES,REQUEST_METHOD,SSLKEYLOGFILE, docs:configure, guided:ARI_API_KEY,ARI_BASE_URL,LC_MESSAGES,REQUEST_METHOD....
Note	batch:clawhub:2026-10-26

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Network destinations contacted

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/ari.py; python3 <skill>/scripts/ari.py setup; python3 <skill>/scripts/ari.py configure
Network	ari.funewa.com (1 conn, 243 B sent; while running)

Credentials	no planted credential touched
Files written	nothing outside its own folder

Finding details

F01 Network destinations contacted

Severity: Low Confidence: Info Observed in: scripts:docs:setup
The package connected to these hosts.

Description

Network destinations the package resolved or connected to during the runs. All traffic was captured by the sandbox; nothing reached the internet.

Impact

Context only. Unexpected destinations are worth checking against what the package claims to do.

Evidence

```
ari.funewa.com
```

Remediation

Confirm each host is expected (the package's API, its registry). Allowlist expected egress in production.

Run log

scripts:baseline ok 4.3s
no new behavior

scripts:guided:LC_MESSAGES ok 5.1s
no new behavior

scripts:docs:setup ok 7.9s
new behavior: dns:ari.funewa.com

scripts:guided:ARI_BASE_URL,LC_MESSAGES,REQUEST_METHOD,SSLKEYLOGFILE ok 4.8s
no new behavior

scripts:docs:configure ok 7.2s
no new behavior

obedient:baseline ok 1.3s
no new behavior

obedient:guided:ARI_BASE_URL,LC_MESSAGES,REQUEST_METHOD,SSLKEYLOGFILE ok 0.4s
no new behavior

obedient:guided:ARI_API_KEY,ARI_BASE_URL,LC_MESSAGES,REQUEST_METHOD... ok 1.2s
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.