

Target amazon-review-intelligence

No malicious behavior observed

We ran it 8 times, with a normal setup, LC_MESSAGES set, docs:check, ARI_API_KEY and ARI_BASE_URL and LC_MESSAGES and REQUEST_METHOD... set and docs:setup. 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	amazon-review-intelligence
Source	clawhub 1.5.3
SHA-256	16228754dcea3fb47b2df3a29a9bb6a9b12e6e3332be8429faac56d4bafd77c3
Files	8
Scanned	27 Oct 2026, 13:17 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:check, guided:ARI_API_KEY,ARI_BASE_URL,LC_MESSAGES,REQUEST_METHOD..., docs:setup, guided:ARI_API_KEY,ARI_BASE_URL,ARI_EXPORT_DIR,LC_MESSAGES....
Note	batch:clawhub:2026-10-27

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 check; python3 <skill>/scripts/ari.py setup
Network	ari.funewa.com (2 conn, 394 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:check
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 2.8s

no new behavior

scripts:guided:LC_MESSAGES ok 3.7s

no new behavior

scripts:docs:check ok 10.1s

new behavior: dns:ari.funewa.com

scripts:guided:ARI_API_KEY,ARI_BASE_URL,LC_MESSAGES,REQUEST_METHOD... ok 3.9s

no new behavior

scripts:docs:setup ok 4.2s

no new behavior

obedient:baseline ok 0.7s

no new behavior

obedient:guided:ARI_API_KEY,ARI_BASE_URL,LC_MESSAGES,REQUEST_METHOD... ok 0.6s

no new behavior

obedient:guided:ARI_API_KEY,ARI_BASE_URL,ARI_EXPORT_DIR,LC_MESSAGES... ok 0.4s

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.