

Target realtime-price-compare

No malicious behavior observed

We ran it 7 times, with a normal setup, docs:--file, SHOP_SEARCH_API_URL set and a GitHub Actions environment. It contacted 47.100.160.98:443. 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	realtime-price-compare
Source	clawhub 1.0.0
SHA-256	2286c6ab1b83ad0266003ee0e8ac84baadfa0ecd97017f6391329f82a82d1392
Files	7
Scanned	27 Oct 2026, 13:03 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. 7 runs: baseline, docs:--file, guided:SHOP_SEARCH_API_URL, ci-github.
Note	batch:clawhub:2026-10-27

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Agent connected to an IP address directly

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/shop_search.py; python3 <skill>/scripts/shop_search.py --file; ls -la ./skill; ls -la ./skill/scripts; cat scripts/shop_search.py; cat _meta.json
Network	47.100.160.98 (5 conn, 1629 B sent; while running) 47.100.160.98:443 (0 conn, 0 B sent; while running)
Credentials	no planted credential touched



Files written nothing outside its own folder

Finding details

F01 Agent connected to an IP address directly

Severity: Low Confidence: Info Observed in: llm:baseline
A connection went to a raw IP address instead of a hostname.

Description

A connection was made to a hard-coded IP address rather than a hostname.

Impact

Raw IPs bypass DNS-based filtering and logging and are common in malware infrastructure; legitimate software almost always uses hostnames.

Evidence

47.100.160.98:443

Remediation

Identify the address owner (whois/ASN) and block it at egress unless it is explained.

References

ATT&CK T1071 Application Layer Protocol

Run log

scripts:baseline ok 1.5s

no new behavior

scripts:docs:--file ok 1.2s

no new behavior

scripts:guided:SHOP_SEARCH_API_URL ok 1.0s

no new behavior

obedient:baseline ok 0.6s

no new behavior

obedient:guided:SHOP_SEARCH_API_URL ok 0.6s

no new behavior

obedient:ci-github ok 0.6s

no new behavior

llm:baseline ok 20.7s

new behavior: exec:curl, ip:47.100.160.98:443 | 8 model steps, 7 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.