



Target huawei-cloud-daily-hot-topics

No malicious behavior observed

We ran it 8 times, with a normal setup, LC_MESSAGES and REQUEST_METHOD and SSLKEYLOGFILE set, docs:--format text --top, docs:--format json --top and a GitHub Actions environment. It contacted 60s.viki.moe. 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	huawei-cloud-daily-hot-topics
Source	clawhub 1.0.0
SHA-256	c99fe2604cfadbf0e42a2f49c32bbbbc3285da27f6abbb23d93f51d98c044e0f
Files	12
Scanned	27 Oct 2026, 13:00 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,REQUEST_METHOD,SSLKEYLOGFILE, docs:--format text --top, docs:--format json --top, ci-github.
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/fetch_hot_topics.py; python3 <skill>/scripts/fetch_hot_topics.py --format text --top; python3 <skill>/scripts/fetch_hot_topics.py --format json --top; python3 <skill>/tests/test_fetch_hot_topics.py; python3 scripts/fetch_hot_topics.py; python3 scripts/fetch_hot_topics.py --format text --top 5



Network	60s.viki.moe (63 conn, 11424 B sent; while running)
Credentials	no planted credential touched
Files written	./HTENVj0tgNGNPRfGPuWvzupGuRSaK (written) ./hot.md (written)

Finding details

F01 Network destinations contacted

Severity: Low Confidence: Info Observed in: scripts:baseline
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

60s.viki.moe

Remediation

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

Run log

scripts:baseline ok 1.8s

new behavior: dns:60s.viki.moe

scripts:guided:LC_MESSAGES,REQUEST_METHOD,SSLKEYLOGFILE ok 1.5s

new behavior: write:./HTENVj0tgNGNPRfGPuWvzupGuRSaK

scripts:docs:--format text --top ok 1.3s

no new behavior

scripts:docs:--format json --top ok 1.3s

no new behavior

scripts:baseline ok 1.9s

new behavior: write:./hot.json

scripts:guided:LC_MESSAGES,REQUEST_METHOD,SSLKEYLOGFILE ok 2.1s

no new behavior

scripts:ci-github ok 2.0s

no new behavior

obedient:baseline ok 14.2s

new behavior: write:./hot.md

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.