

Target media-download

No malicious behavior observed

We ran it 8 times, with a normal setup, opt=a set and opt=c set. 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	media-download
Source	clawhub 1.0.0
SHA-256	f18aa3b4180e02ea82cfa22198041b173d6ffa4786db9ebee6916e73e6d390cd
Files	6
Scanned	27 Oct 2026, 12:14 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:opt=a, guided:opt=c.
Note	batch:clawhub:2026-10-27

Observed behavior

Install step	none
Runs as	bash <skill>/scripts/pinterest.sh; bash <skill>/scripts/video.sh; bash <url>; bash -q 720 <url>; bash -a <url>; bash -p <playlist or carousel>
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log

scripts:baseline ok 0.3s

no new behavior

scripts:guided:opt=a ok 0.4s

no new behavior



scripts:guided:opt=c ok 0.4s

no new behavior

scripts:baseline ok 0.5s

no new behavior

scripts:guided:opt=a ok 0.5s

no new behavior

scripts:guided:opt=c ok 0.6s

no new behavior

obedient:baseline ok 1.5s

no new behavior

obedient:guided:opt=a ok 3.3s

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.