

Target video-overloaded-shot-split-cn

No malicious behavior observed

We ran it 4 times, with a normal setup, BASH_SOURCE set and a GitHub Actions environment. 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	video-overloaded-shot-split-cn
Source	clawhub 1.0.1
SHA-256	0b63c305ef06b3a4b79f69e43af38b640c50cc213510e2da6dbad58543e65c0d
Files	17
Scanned	27 Oct 2026, 11:18 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. 4 runs: baseline, guided:BASH_SOURCE, ci-github.
Note	batch:clawhub:2026-10-27

Observed behavior

Install step	none
Runs as	bash <skill>/scripts/self-test.sh; dirname <skill>/scripts/self-test.sh; grep -q ^name: video-overloaded-shot-split-cn\$ SKILL.md; grep -q ^name: video-overloaded-shot-split-cn\$ manifest.yaml; grep -q ^slug: video-overloaded-shot-split-cn\$ manifest.yaml; grep -q ^icon: icon-512.png\$ manifest.yaml
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log

**scripts:baseline ok 2.0s**

no new behavior

scripts:guided:BASH_SOURCE ok 0.5s

no new behavior

scripts:ci-github ok 2.0s

no new behavior

llm:baseline ok 11.7s

no new behavior | 5 model steps, 4 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.