

Target web-video-to-md

No malicious behavior observed

We ran it 8 times, with a normal setup, MARKITDOWN_SKILL_DIR and VTMD_FFMPEG and VTMD_MARKITDOWN_SKILL_DIR and VTMD_PYTHON... set, a GitHub Actions environment, LC_MESSAGES set and docs:--probe. 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	web-video-to-md
Source	clawhub 1.0.0
SHA-256	2ce37eccf71e5872fec788537b1ae48b0524c36b0bd2526f7a14b714cd678f7
Files	9
Scanned	27 Oct 2026, 13:07 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:MARKITDOWN_SKILL_DIR,VTMD_FFMPEG,VTMD_MARKITDOWN_SKILL_DIR,VTMD_PYTHON..., ci-github, guided:LC_MESSAGES, docs:--probe.
Note	batch:clawhub:2026-10-27

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/_vtmd_common.py; python3 <skill>/scripts/fetch_videos.py; python3 <skill>/scripts/fetch_videos.py --probe; python3 <skill>/scripts/video_to_md.py
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder



Run log

scripts:baseline ok 1.6s

no new behavior

scripts:guided:MARKITDOWN_SKILL_DIR,VTMD_FFMPEG,VTMD_MARKITDOWN_SKILL_DIR,VTMD_PYTHON... ok 1.7s

no new behavior

scripts:ci-github ok 2.4s

no new behavior

scripts:baseline ok 1.6s

no new behavior

scripts:guided:LC_MESSAGES ok 1.8s

no new behavior

scripts:docs:--probe ok 1.4s

no new behavior

scripts:baseline ok 1.8s

no new behavior

scripts:guided:LC_MESSAGES ok 2.1s

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.