

Target novel-foreshadow-map-cn

No malicious behavior observed

We ran it 7 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	novel-foreshadow-map-cn
Source	clawhub 1.0.0
SHA-256	b82a6a9c837f5b27fef9a2ab3bd0673aed132a243055a273c53ca124e9652231
Files	19
Scanned	27 Oct 2026, 11:20 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, guided:BASH_SOURCE, ci-github.
Note	batch:clawhub:2026-10-27

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/render-promo.py; bash <skill>/scripts/self-test.sh; dirname <skill>/scripts/self-test.sh; python3 -; dirname true; ls -la
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log

scripts:baseline ok 1.1s
no new behavior



scripts:guided:BASH_SOURCE ok 1.3s

no new behavior

scripts:ci-github ok 0.9s

no new behavior

scripts:baseline ok 1.4s

no new behavior

scripts:guided:BASH_SOURCE ok 0.6s

no new behavior

scripts:ci-github ok 1.4s

no new behavior

llm:baseline ok 11.8s

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.