

Target `srv-guard`

No malicious behavior observed

We ran it 8 times, with a normal setup, the clock moved a year ahead, a GitHub Actions environment, `LC_MESSAGES` set and `docs:--target`. 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	<code>srv-guard</code>
Source	<code>clawhub 1.0.0</code>
SHA-256	<code>cb960be77c4aea7017f44438f940b7b93523bcbdc16e69dbf7d29dd553ca682</code>
Files	<code>14</code>
Scanned	<code>26 Oct 2026, 17:31 UTC</code>
Engine	<code>detonator 0.5.1</code>
Method	<code>Executed in an isolated sandbox with decoy credentials and a captive network; every file access, process and connection traced. 8 runs: baseline, time-travel, ci-github, guided:LC_MESSAGES, docs:--target.</code>
Note	<code>batch:clawhub:2026-10-26</code>

Observed behavior

Install step	<code>none</code>
Runs as	<code>python3 <skill>/scripts/_common.py; python3 <skill>/scripts/attack_defend.py; python3 <skill>/scripts/attack_defend.py --target; python3 <skill>/scripts/attack_monitor.py</code>
Network	<code>no connections</code>
Credentials	<code>no planted credential touched</code>
Files written	<code>nothing outside its own folder</code>

Run log



scripts:baseline ok 1.9s

no new behavior

scripts:time-travel ok 3.2s

no new behavior

scripts:ci-github ok 2.0s

no new behavior

scripts:baseline ok 3.5s

no new behavior

scripts:guided:LC_MESSAGES ok 1.9s

no new behavior

scripts:docs:--target ok 1.7s

no new behavior

scripts:baseline ok 1.6s

no new behavior

scripts:guided:LC_MESSAGES ok 2.4s

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.