

Target `taplio-linkedin-smart-comment-writer`

No malicious behavior observed

We ran it 4 times, with a normal setup, the clock moved a year ahead 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	<code>taplio-linkedin-smart-comment-writer</code>
Source	<code>clawhub 1.0.0</code>
SHA-256	<code>79e197e52651f5987891ab78fdeccaae63cdc835461f5e5133f1dca8cca4deac</code>
Files	<code>3</code>
Scanned	<code>26 Oct 2026, 18:54 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. 4 runs: baseline, time-travel, ci-github.</code>
Note	<code>batch:clawhub:2026-10-26</code>

Observed behavior

Install step	<code>none</code>
Network	<code>no connections</code>
Credentials	<code>no planted credential touched</code>
Files written	<code>nothing outside its own folder</code>

Run log

obedient:baseline **ok** **0.4s**

no new behavior

obedient:time-travel **ok** **0.7s**

no new behavior

**obedient:ci-github ok 0.5s**

no new behavior

llm:baseline ok 3.0s

no new behavior | 1 model steps, 0 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.