

Target `taplio-linkedin-post-writer`

No malicious behavior observed

We ran it 4 times, with a normal setup, a GitHub Actions environment and a production 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 1 info

Nothing observed calls for action. This is evidence, not a guarantee.

Scope

Package	<code>taplio-linkedin-post-writer</code>
Source	<code>clawhub 1.0.0</code>
SHA-256	<code>8a981fe46118b0926dd79aa24493f0d05defde36f9e45ce321a0af1dcaabf399</code>
Files	3
Scanned	26 Oct 2026, 18:55 UTC
Engine	<code>detonator 0.5.1</code>
Method	Executed in an isolated sandbox with decoy credentials and a captive network; every file access, process and connection traced. 4 runs: <code>baseline</code> , <code>ci-github</code> , <code>production</code> .
Note	<code>batch:clawhub:2026-10-26</code>

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Loaded the project's <code>.env</code> file

Observed behavior

Install step	<code>none</code>
Runs as	<code>ls -la; ls -la skill; cat .env; cat skill/_meta.json; cat skill/skill-card.md; cat README.md</code>
Network	<code>no connections</code>
Credentials	<code>./.env (read)</code>
Files written	<code>nothing outside its own folder</code>



Finding details

F01 Loaded the project's .env file

Severity: Low Confidence: Info Observed in: llm:baseline
The package loaded the project's .env file.

Description

The process loaded the project's .env file. Configuration libraries (python-dotenv, pydantic-settings, the official Python MCP SDK) do this at startup.

Impact

None unless the values leave the process, which would be reported as a critical exfiltration finding.

Evidence

```
./.env (by cat)
```

Remediation

No action needed. Keep long-lived secrets out of project .env files where possible.

Run log

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

no new behavior

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

no new behavior

obedient:production **ok** **0.5s**

no new behavior

llm:baseline **ok** **6.1s**

new behavior: ownread:./.env | 3 model steps, 2 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.