

Target `taplio-linkedin-niche-definer`

No malicious behavior observed

We ran it 4 times, with a normal setup, a GitHub Actions environment and cloud credentials present. 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-niche-definer</code>
Source	<code>clawhub 1.0.0</code>
SHA-256	<code>b1f4e190eb4b42476545f5c0184a487beea7c2ebad6991be242393414e649a77</code>
Files	3
Scanned	26 Oct 2026, 18:56 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>cloud-creds</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; head -50; cat skill/SKILL.md; cat .env; cat skill/_meta.json</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 0.8s

no new behavior

obedient:ci-github ok 0.7s

no new behavior

obedient:cloud-creds ok 0.7s

no new behavior

llm:baseline ok 8.6s

new behavior: ownread:./.env | 4 model steps, 3 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.