



Target `pressmark`

No malicious behavior observed

We ran it 1 time, with a normal setup. It contacted `pressmark.dev`. 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 2 info

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

Scope

Package	<code>pressmark</code>
Source	<code>clawhub 1.2.1</code>
SHA-256	<code>ec962245aa0e3a29d6063e50096ad3f3682ec6d825653af010da6d1524853a26</code>
Files	3
Scanned	26 Oct 2026, 17:33 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. 1 runs: <code>baseline</code> .
Note	<code>batch:clawhub:2026-10-26</code>

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Network destinations contacted
F02	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 skill/SKILL.md; cat .env; cat skill/_meta.json; cat skill/skill-card.md</code>
Network	<code>pressmark.dev</code> (16 conn, 2192 B sent; while running)
Credentials	<code>./.env</code> (read)
Files written	<code>nothing outside its own folder</code>



Finding details

F01 Network destinations contacted

Severity: Low Confidence: Info Observed in: llm:baseline
The package connected to these hosts.

Description

Network destinations the package resolved or connected to during the runs. All traffic was captured by the sandbox; nothing reached the internet.

Impact

Context only. Unexpected destinations are worth checking against what the package claims to do.

Evidence

```
pressmark.dev
```

Remediation

Confirm each host is expected (the package's API, its registry). Allowlist expected egress in production.

F02 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

llm:baseline **ok** **64.4s**

new behavior: dns:pressmark.dev, exec:curl, ownread:./.env | 8 model steps, 8 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.