

Target aimegeo-llms-txt

No malicious behavior observed

We ran it 8 times, with a normal setup, LC_MESSAGES set, docs:build --input examples/four-pages.json, the clock moved a year ahead and a GitHub Actions environment. It contacted example.com. 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

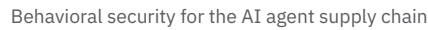
Package	aimegeo-llms-txt
Source	clawhub 1.0.0
SHA-256	c4b5e88be126d98e7c9279b7f6bc7fb251f2490db3e3a66b4336a07cab1e06a7
Files	19
Scanned	27 Oct 2026, 11:27 UTC
Engine	detonator 0.5.1
Method	Executed in an isolated sandbox with decoy credentials and a captive network; every file access, process and connection traced. 8 runs: baseline, guided:LC_MESSAGES, docs:build --input examples/four-pages.json, time-travel, ci-github.
Note	batch:clawhub:2026-10-27

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Network destinations contacted

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/llms_index.py; python3 <skill>/scripts/llms_index.py build --input examples/four-pages.json; python3 <skill>/scripts/self_test.py; /usr/bin/python3 -S -B <skill>/scripts/llms_index.py build --input; /usr/bin/python3 -S -B /tmp/llms-portable-z375i9s4/llms_index.py build --input; /usr/bin/python3 -S -B /tmp/llms-portable-cujxyrra/llms_index.py build --input



Network	example.com (1 conn, 184 B sent; while running)
Credentials	no planted credential touched
Files written	nothing outside its own folder

Finding details

F01 Network destinations contacted

Severity: Low Confidence: Info Observed in: obedient: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

example.com

Remediation

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

Run log

```
scripts:baseline    ok    2.9s
```

no new behavior

```
scripts:guided:LC_MESSAGES    ok    2.1s
```

no new behavior

```
scripts:docs:build --input examples/four-pages.json    ok    1.5s
```

no new behavior

```
scripts:baseline    timeout    20.3s
```

new behavior: write:./input.json, write:./llms.txt, write:./report.json

```
scripts:time-travel    ok    5.1s
```

new behavior: write:./llms_index.py, write:./pages.json

```
scripts:guided:LC_MESSAGES    ok    20.0s
```

no new behavior

```
scripts:ci-github    timeout    20.3s
```

no new behavior

obedient:baseline ok 27.1s

```
new behavior: dns:example.com, write:./output/llms.txt, write:./output/pages.json, write:./output/â€œæ¥¥â€œ.json,
write:./output/æ-â€œâ€œæ .json
```

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.