



Target casino-game-research

No malicious behavior observed

We ran it 4 times, with a normal setup, docs:or the named and docs:/draftkings/casino/slots/categories. It contacted api.crawlora.net. 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	casino-game-research
Source	clawhub 1.0.0
SHA-256	58cc64208049cc9bb2a7aef58ec33f4b8d31a0d04d9fc050fd9bb00c2db4e284
Files	5
Scanned	26 Oct 2026, 17:54 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. 4 runs: baseline, docs:or the named, docs:/draftkings/casino/slots/categories.
Note	batch:clawhub:2026-10-26

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Network destinations contacted
F02	Low	Info	Loaded the project's .env file

Observed behavior

Install step	none
Runs as	bash <skill>/scripts/crawlora.sh; bash <skill>/scripts/crawlora.sh or the named; bash <skill>/scripts/crawlora.sh /draftkings/casino/slots/categories; ls -la; ls -la skill; cat skill/SKILL.md
Network	api.crawlora.net (3 conn, 416 B sent; while running)



Credentials	./.env (read)
Files written	nothing outside its own folder

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

```
api.crawlora.net
```

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, grep)
```

Remediation

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

Run log

scripts:baseline ok 0.4s

no new behavior

scripts:docs:or the named ok 0.3s

no new behavior

scripts:docs:/draftkings/casino/slots/categories ok 0.6s

no new behavior

**llm:baseline ok 17.3s**

new behavior: dns:api.crawlora.net, 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.