

Target horse-racing-research

No malicious behavior observed

We ran it 4 times, with a normal setup, docs:or the named and docs:/fanduel/racing/races. 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 0 info

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

Scope

Package	horse-racing-research
Source	clawhub 1.0.0
SHA-256	8655f190b1279bfd7cd64aad1b6ebbd66521e528bff53670425dea906a4dc28d
Files	5
Scanned	26 Oct 2026, 17:51 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:/fanduel/racing/races.
Note	batch:clawhub:2026-10-26

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 /fanduel/racing/races; ls -la; ls -la skill; ls -la skill/scripts
Network	no connections
Credentials	no planted credential touched
Files written	nothing outside its own folder

Run log

scripts:baseline ok 0.6s
no new behavior



scripts:docs:or the named ok 0.6s

no new behavior

scripts:docs:/fanduel/racing/races ok 0.8s

no new behavior

llm:baseline ok 16.2s

no new behavior | 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.