

Target pdf

No malicious behavior observed

We ran it 8 times, with a normal setup, a GitHub Actions environment, cloud credentials present and PYTHON_COLORS set. 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	pdf
Source	github
SHA-256	69e2ac9eb2bbe2881df26acc53b46b39a15cfda206f5357e5f9c83feb0fadcc7
Files	12
Scanned	25 Oct 2026, 12:14 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, ci-github, cloud-creds, guided:PYTHON_COLORS.

Run log

```
scripts:baseline    ok    0.4s
no new behavior

scripts:ci-github   ok    0.4s
no new behavior

scripts:cloud-creds ok    0.4s
no new behavior

scripts:baseline    ok    0.4s
no new behavior

scripts:guided:PYTHON_COLORS ok    0.4s
no new behavior

scripts:ci-github   ok    0.4s
no new behavior

scripts:baseline    ok    0.4s
no new behavior

scripts:guided:PYTHON_COLORS ok    0.4s
no new behavior
```



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.