



Target plainlykit-temporary-email

No malicious behavior observed

We ran it 7 times, with a normal setup, LC_MESSAGES set, docs:--state /private/path/inbox.json create and a GitHub Actions environment. It contacted plainlykit.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	plainlykit-temporary-email
Source	clawhub 1.0.0
SHA-256	1ddb826a9eeffd210be8d9d57ff6ce898b18576ec60ccd82261176997dccaeea
Files	4
Scanned	26 Oct 2026, 18:17 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. 7 runs: baseline, guided:LC_MESSAGES, docs:--state /private/path/inbox.json create, ci-github.
Note	batch:clawhub:2026-10-26

Findings summary

ID	Severity	Confidence	Finding
F01	Low	Info	Network destinations contacted

Observed behavior

Install step	none
Runs as	python3 <skill>/scripts/tempmail.py; python3 <skill>/scripts/tempmail.py --state /private/path/inbox.json create; python3 scripts/tempmail.py --state /private/path/inbox.json create; python3 scripts/tempmail.py --state /private/path/inbox.json list; python3 scripts/tempmail.py --state /private/path/inbox.json read MESSAGE_ID; python3 scripts/tempmail.py --state /private/path/inbox.json delete



Network	plainlykit.com (11 conn, 3352 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: 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

plainlykit.com

Remediation

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

Run log

scripts:baseline ok 3.6s

no new behavior

scripts:guided:LC_MESSAGES ok 2.9s

no new behavior

scripts:docs:--state /private/path/inbox.json create ok 3.1s

no new behavior

obedient:baseline ok 8.7s

no new behavior

obedient:guided:LC_MESSAGES ok 10.8s

no new behavior

obedient:ci-github ok 9.6s

no new behavior

llm:baseline ok 26.5s

new behavior: dns:plainlykit.com | 8 model steps, 7 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.