MALDET · STATIC SECURITY REPORT

PSInject

github.com/EmpireProject/PSInject

Scanned 18 September 2026 at 19:49 · Report generated 29 October 2026 · PowerShell · 265 stars

OVERALL ASSESSMENT

Low

Combined score 13 · 2 findings after filtering

Summary

1 finding likely need attention. Most notable: ClamAV detected: Win.Trojan.PSempireInj-7013548-0 (98% confidence).

Generated from finding counts. A plain-English summary was not available for this scan.

Risk, by type

MalDet scores two different questions separately, because they call for different responses: code can be badly written without being hostile, and hostile code is not always badly written.

VULNERABILITY

Safe (0)

Insecure coding an attacker could exploit. Usually mistakes, and usually fixable in place.

MALICIOUS PATTERN

Low (13)

Signs the code may be trying to do harm: hidden payloads, credential access, persistence, exfiltration.

What each detector found

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
yara	Signatures of malicious behaviour in source files	1	0	0	**1**
clamav	Known malware signatures	1	0	0	**1**

1 of 2 findings were rated more likely genuine than noise by the classifier.

Evidence

Identical findings are grouped, so a single rule firing many times takes one row. Ordered worst first. “Seen” is how many times that finding occurred.

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	clamav	ClamAV detected: Win.Trojan.PSempireInj-7013548-0	1	`/Invoke-PSInject.ps1`
HIGH	yara	YARA rule matched: detect_process_injection — Windows process-injection API sequence	1	`/Invoke-PSInject.ps1`

How to read this report

- **This is a static scan.** The code was read, never executed. Behaviour that only appears at runtime is outside what any of these detectors can see.
- **Findings are not all equally real.** A classifier rates each finding on how likely it is to be genuine rather than noise, and that rating weights the scores. Measured against a hand-reviewed sample it reached precision 0.52 and recall 0.62 — useful for ranking, not a verdict on any single finding.
- **A high score is not proof of malice.** Security tools, penetration-testing frameworks and malware research repositories contain the same patterns as real malware by design. The two risk types above exist to keep that distinction visible.
- **Absence of findings is not proof of safety.** A detector that is not installed, or a language none of them parse, produces silence rather than a warning.
- **This scan is a snapshot.** The repository may have changed since 18 September 2026.