MALDET · STATIC SECURITY REPORT

malware-samples

github.com/InQuest/malware-samples

Scanned 30 October 2026 at 04:34 · Report generated 30 October 2026 · ActionScript · 945 stars

OVERALL ASSESSMENT

Medium

Combined score 80 · 45 findings after filtering

Summary

All 45 findings look like noise (low confidence) — nothing here likely needs attention.

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

Low (18)

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

MALICIOUS PATTERN

High (62)

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	32	0	0	**32**
semgrep	Insecure coding patterns across many languages	0	12	0	**12**
bandit	Insecure coding patterns in Python source	0	0	1	**1**

0 of 45 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	yara	YARA rule matched: detect_process_injection — Windows process-injection API sequence	6	/2018-04-Common-Malware-Carrier/payload
HIGH	yara	YARA rule matched: detect_anti_analysis — Checks for a debugger, VM, or sandbox before continuing - a common malware evasion technique, essentially never present in ordinary application code	23	/CVE-2018-4878-Adobe-Flash-DRM-UAF-0day/pe-e1546323dc746ed2f7a5c973dcecc79b014b68bdd8a6230239283b4f775f4bbd.report
HIGH	yara	YARA rule matched: detect_persistence_mechanism — Modifies a startup/scheduling location - legitimate application code essentially never does this	3	/2019-07-Base64-Encoded-Powershell-Directives/0d64cc01fca51dc44a50f877631dbb3b94aa1c5902da6d71aaa7879646b90b17
MEDIUM	semgrep	Detected the use of eval(). eval() can be dangerous if used to evaluate dynamic content. If this content can be input from outside the program, this may be a code injection vulnerability. Ensure evaluated content is not definable by external sources.	12	/2018-04-GandCrab-Swarm/dropper-javascript/0638e4dfe95bdae94a751404e4c91adbb72a57967d4443cde3e4abb16bc293b0.js:1
LOW	bandit	Try, Except, Continue detected.	1	/2020-07-GlobalSign/extract_ps_from_png.py:19

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 30 October 2026.