

malware-samples

github.com/fabrimagic72/malware-samples

Scanned 22 August 2026 at 09:17 · Report generated 29 October 2026 · 1,819 stars

OVERALL ASSESSMENT

Medium

Combined score 29 · 11 findings after filtering

Summary

This repository has been flagged as having a medium risk score of 29.0, which indicates that while the code itself is safe from known vulnerabilities, it contains several suspicious patterns that suggest the project may be intentionally malicious. The most concerning finding is a high-confidence match on VirusTotal for malware samples, meaning many security engines have identified this code as harmful. Additionally, two YARA rules were triggered, one of which detects cryptocurrency mining pools and another checks for common malware evasion techniques like debuggers or sandboxes. These specific patterns are not typical of normal software development and strongly point to the repository being used for malicious purposes rather than legitimate applications.

Written by a language model running locally on the scanning machine, from the findings in this report. The risk levels above and below were decided by the scoring model, not by this summary.

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

Medium (29)

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	10	0	0	10

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
virustotal	Known malware signatures (legacy scans)	1	0	0	1

1 of 11 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	virustotal	VirusTotal: 2/93 engines flagged as malicious	1	https://github.com/fabrimagic72/malware-samples
HIGH	yara	YARA rule matched: detect_crypto_miner — Cryptocurrency mining pool connection patterns	1	/Bitcoin miners/ 02ca4397da55b3175aaa1ad2c99981e792f66151_extracted/ 02ca4397da55b3175aaa1ad2c99981e792f66151.bin
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	9	/Ransomware/Wannacry/mssecsvc_41b5ba4bf74e65845fa8c9861ca34508_extracted/mssecsvc.bin

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 22 August 2026.