

The-MALWARE-Repo

github.com/Da2dalus/The-MALWARE-Repo

Scanned 15 September 2026 at 05:19 · Report generated 29 October 2026 · VBScript · 1,702 stars

OVERALL ASSESSMENT

High

Combined score 81 · 38 findings after filtering

Summary

This repository has been flagged as having a high risk of malicious intent, which means it likely contains code designed to harm users rather than just being poorly written. The most concerning issue is that the code appears to be connected to cryptocurrency mining pools and uses Windows process-injection techniques, which are strong indicators of malware rather than standard buggy software. While some findings point to insecure coding patterns like plaintext URLs, these are common mistakes in any application and do not necessarily mean the code is dangerous on its own. The developer should treat this as a high-risk asset that requires immediate review or removal before use, as the presence of mining connections and injection attempts suggests it could be used for illegal activities.

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

Low (1)

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

MALICIOUS PATTERN

High (80)

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	37	0	0	37

DETECTOR	LOOKS FOR	HIGH	MEDIUM	LOW	TOTAL
semgrep	Insecure coding patterns across many languages	0	1	0	1

0 of 38 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_crypto_miner — Cryptocurrency mining pool connection patterns	1	/Botnets/ FritzFrog/ 103b8404dc64c9a44 511675981a09fd013 95ee837452d114f13 50c295357c046
HIGH	yara	YARA rule matched: detect_process_injection — Windows process-injection API sequence	7	/Joke/ DesktopBoom.exe
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	29	/Joke/ DesktopBoom.exe
MEDIUM	semgrep	This link points to a plaintext HTTP URL. Prefer an encrypted HTTPS URL if possible.	1	/Email-Worm/ BubbleBoy.html:14

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 15 September 2026.