

Ransomware-Samples

github.com/kh4sh3i/Ransomware-Samples

Scanned 18 September 2026 at 19:50 · Report generated 29 October 2026 · 294 stars

OVERALL ASSESSMENT

Critical

Combined score 352 · 49 findings after filtering

Summary

This repository has been flagged as extremely dangerous because it contains files that have been identified by security tools as ransomware agents, exploit kits, and malware designed to steal data or encrypt files. The scan found over 49 specific instances of these malicious patterns, with the highest priority alerts coming from ClamAV which detected numerous different types of ransomware like Cerber, Locky, and various droppers. While the vulnerability risk score is low because there are no obvious coding errors that an attacker could easily exploit, the malicious-pattern risk score is critically high, indicating that the code itself likely contains intentional malware rather than just bad security practices. Because these files have been confirmed to be active ransomware agents with 98% confidence, using this repository would expose your system to severe data theft or encryption attacks immediately upon execution.

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

Critical

 (352)

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
clamav	Known malware signatures	32	0	0	32
yara	Signatures of malicious behaviour in source files	17	0	0	17

32 of 49 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.Ransomware.Thanos-9755595-0	4	/Thanos/ Ransomware. Thanos_extr acted/ c460fc0d4fd af5c68623e18 de106f1c3601 d7bd6ba80dd ad86c10fd6e a123850
HIGH	clamav	ClamAV detected: Win.Ransomware.Cryakl-9816021-0	3	/Vipasana/ Ransomware. Vipasana_ex tracted/ c0cf40b8830 d666a24bdd4 febd162e95 aa30ed968fa3 675e26ad97b2 e88e03a
HIGH	clamav	ClamAV detected: Win.Downloader.MSWord-6331390-3	2	/Petrwrap/ Ransomware. Petrwrap_ex tracted/ myguy.hta

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	clamav	ClamAV detected: Win.Exploit.CVE_2017_0147-6331310-0	2	/Petrwrap/ Ransomware. Petrwrap_ex tracted/ 027cc450ef5 f8c5f6533296 41ec1fed91f6 94e0d2299289 63b30f6b0d7 d3a745_98ST Jd8lju.bin. gz
HIGH	clamav	ClamAV detected: Rtf.Exploit.CVE_2017_0199-6331394-6	1	/Petrwrap/ Ransomware. Petrwrap_ex tracted/ fe2e5d0543b4 c8769e401ec2 16d78a5a3547 dfd426fd47e0 97df04a5f7d6 d206_OFkNP1 kKL9.bin.gz
HIGH	clamav	ClamAV detected: Win.Trojan.TeslaCrypt-3	1	/TeslaCrypt/ Ransomware. TeslaCrypt_ extracted/ 3372c1edab46 837f1e973164 fa2d726c5c5 e17bcb888828 ccd7c4dfcc23 4a370
HIGH	clamav	ClamAV detected: Win.Trojan.Satana-3	1	/Satana/ Ransomware. Satana_extr acted/ 683a09da2199 18258c58a7f6 1f7dc4161a3 a7a377cf82a3 1b840baabfb9 a4a96.bin

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	clamav	ClamAV detected: Win.Trojan.Petya-6312160-0	1	/Petya/ Ransomware. Petya_extra cted/ 4c1dc737915 d76b7ce579a bddaba74ead6 fdb5b519a1e a45308b8c49 b950655c.bin
HIGH	clamav	ClamAV detected: Win.Trojan.Petya-5637914-0	1	/Petya/ Ransomware. Petya_extra cted/ 26b4699a7b9 eeb16e76305 d843d4ab05e9 4d43f3201436 927e13b3eba fa90739.bin
HIGH	clamav	ClamAV detected: Win.Trojan.CryptoWall-1	1	/Cryptowall/ Ransomware. Cryptowall_ extracted/ cryptowall. bin
HIGH	clamav	ClamAV detected: Win.Ransomware.Wannacryptor-9940180-0	1	/WannaCry/ Ransomware. WannaCry_ex tracted/ ed01ebfbc9e b5bbea545af4 d01bf5f10716 61840480439 c6e5babe8e08 0e41aa.exe
HIGH	clamav	ClamAV detected: Win.Ransomware.Wanna-9769986-0	1	/ WannaCry_Pl us/ Ransomware. WannaCry_Pl us_extracted / Win32.Wanna cry.exe

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	clamav	ClamAV detected: Win.Ransomware.Trustezeb-9966715-0	1	/Matsnu/ Ransomware. Matsnu_extr acted/ Matsnu- MBRwipingRa nsomware_1B2 D2A4B97C7C27 27D571BBF937 6F54F_Inkas so Rechnung vom 27.05.2013 . com_
HIGH	clamav	ClamAV detected: Win.Ransomware.TeslaCrypt-9849895-0	1	/TeslaCrypt/ Ransomware. TeslaCrypt_ extracted/ E906FA3D51E8 6A61741B3499 145A114E9BF B7C56
HIGH	clamav	ClamAV detected: Win.Ransomware.TeslaCrypt-7090181-1	1	/TeslaCrypt/ Ransomware. TeslaCrypt_ extracted/ 51B4EF5DC9D2 6B7A26E214C EE90598631E2 EAA67
HIGH	clamav	ClamAV detected: Win.Ransomware.Radam-10038734-0	1	/Radamant/ Ransomware. Radamant_ex tracted/ DUMP_00A1000 0-00A1D000. exe.ViR
HIGH	clamav	ClamAV detected: Win.Ransomware.Locky-9659911-0	1	/Locky/ Ransomware. Locky_extra cted/Locky
HIGH	clamav	ClamAV detected: Win.Ransomware.Karo-6331638-1	1	/Petrwrap/ Ransomware. Petrwrap_ex tracted/ svchost.exe

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	clamav	ClamAV detected: Win.Ransomware.HDDCryptor-2	1	/Mamba/ Ransomware. Mamba_extracted/131.exe
HIGH	clamav	ClamAV detected: Win.Ransomware.Cerber-6922156-0	1	/Cerber/ Ransomware. Cerber_extracted/ cerber.exe
HIGH	clamav	ClamAV detected: Win.Malware.Jigsaw-1	1	/Jigsaw/ Ransomware. Jigsaw_extracted/jigsaw
HIGH	clamav	ClamAV detected: Win.Dropper.Autit-8177147-0	1	/RedBoot/ Ransomware. RedBoot_extracted/ 1001a8c7f331 85217e6e1bd bb8dba9780d4 75da944684f b4bf1fc04809 525887
HIGH	clamav	ClamAV detected: Win.Coinminer.MSILMiner-6554134-0	1	/Unnamed_0/ Ransomware. Unnamed_0_extracted/ Ransomware. Unnamed_0.exe
HIGH	clamav	ClamAV detected: Unix.Malware.Agent-1628853	1	/Rex/ Ransomware. Rex_extracted/ WTEpZSFwgb
HIGH	clamav	ClamAV detected: Doc.Dropper.Agent-7447536-0	1	/Petrwrap/ Ransomware. Petrwrap.zip

SEVERITY	DETECTOR	FINDING	SEEN	EXAMPLE LOCATION
HIGH	yara	YARA rule matched: detect_process_injection — Windows process-injection API sequence	5	/Thanos/Ransomware.Thanos_extracted/5d40615701c48a122e44f831e7c8643d07765629a83b15d090587f469c77693d
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	11	/Mamba/Ransomware.Mamba_extracted/131.exe
HIGH	yara	YARA rule matched: detect_obfuscated_string_execution — Reconstructs a string character-by-character or from hex escapes, then immediately executes it - fromCharCode/chr() alone are common in ordinary text-processing code, so this requires both the reconstruction and an execution call together	1	/Rex/Ransomware.Rex_extracted/WTEpZSFwgb

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.