AI-Assisted Investigation Report

Analyst

MalwareLab User

Analysis Time

2026-07-15 20:18:30 (EDT - America/New_York) | 2026-07-16 00:18:30 UTC

Model

gpt-4.1-mini

Version

beta-v2.0

Report Metrics

Input Size: 667 bytes
IOCs Found: 2
ATT&CK Techniques: 2

Severity

Critical

Confidence

95% - High Confidence

Confidence Factors

• High entropy (8) indicating possible obfuscation or packing
• VirusTotal reports 65 malicious detections and 0 harmless detections for the file hash
• Filename 'WannaCrypt0r.exe' strongly suggests ransomware malware
• Tags from VirusTotal include 'exploit', 'malware', 'cve-2017-0147', 'self-delete', and 'detect-debug-environment' indicating malicious behavior
• Digital signature present but verification status unknown, increasing suspicion given malicious detections

Reducing Factors

• No packer detected which might indicate less obfuscation
• Digital signature claims Microsoft® Windows® Operating System as publisher, but signature verification is unknown

Threat Type

Ransomware

Executive Summary

The file 'WannaCrypt0r.exe' is a Windows PE executable with high entropy and is strongly associated with ransomware activity. VirusTotal reports 65 malicious detections with tags indicating exploitation of CVE-2017-0147 and ransomware behaviors. Despite a digital signature claiming Microsoft as publisher, the verification status is unknown, and the filename and behavior tags strongly indicate malicious ransomware activity.

Evidence Supporting Assessment

• File entropy is 8, indicating high entropy consistent with obfuscation or encryption
• VirusTotal reports 65 malicious detections for SHA1 and SHA256 hashes matching the file
• Filename 'WannaCrypt0r.exe' matches known ransomware naming conventions
• VirusTotal tags include 'exploit', 'cve-2017-0147', 'self-delete', and 'malware'
• Digital signature present but verification unknown, reducing trust in signature

Ambiguity Notes

• Digital signature is present but verification status is unknown, which prevents full trust in the signature
• MalwareBazaar did not find the file hash, limiting additional threat intelligence context
• No behavioral telemetry or runtime analysis available to confirm execution behavior

Alternative Hypotheses

• Controlled lab sample or research sample of WannaCry ransomware
• Modified malware variant or test sample
• False positive due to filename and signature mismatch, though unlikely given detections

Alternative Explanations

None

Indicators of Compromise

Hashes
- 5ff465afaabcbf0150d1a3ab2c2e74f3a4426467
- ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

MITRE ATT&CK Mapping

• T1486 - Data Encrypted for Impact
• T1210 - Exploitation of Remote Services

Recommended Actions

• Immediately isolate any systems where 'WannaCrypt0r.exe' is detected
• Conduct a full malware scan using updated AV/EDR tools referencing the file hashes
• Investigate network logs for exploitation attempts related to CVE-2017-0147
• Review and apply patches for SMB vulnerabilities to prevent exploitation
• Monitor for indicators of ransomware activity such as file encryption and ransom notes

Analyst Notes

None

AI-Assisted Analysis Disclaimer

This report was generated using AI-assisted analysis and is intended to support security investigations. Findings, conclusions, and recommendations should be reviewed and validated by a qualified analyst before operational, legal, or business decisions are made.

