AI-Assisted Investigation Report

Analyst

MalwareLab User

Analysis Time

2026-07-15 20:42:09 (EDT - America/New_York) | 2026-07-16 00:42:09 UTC

Model

gpt-4.1-mini

Version

beta-v2.0

Report Metrics

Input Size: 4.63 KB
IOCs Found: 4
ATT&CK Techniques: 0

Severity

Medium

Confidence

75% - Moderate Confidence

Confidence Factors

• VirusTotal URL reputation shows 13 malicious detections for http://rb3.ftnt.io/download00/eicar.com
• File contains references to EICAR test file URL and drop.com in strings
• PE file with typical Windows executable structure and low entropy consistent with non-packed benign or test file

Reducing Factors

• MalwareBazaar and VirusTotal hash lookups returned no matches for the file hashes
• Entropy values are low (3.44 overall), indicating no packing or obfuscation

Reducing Factors — continued

• No packers detected
• File metadata and embedded text indicate this is a Fortinet FortiSandbox Suspicious Test File used for demonstrations

Threat Type

Suspicious Test File / Potential False Positive

Executive Summary

The analyzed file is a Windows PE executable identified as a Fortinet FortiSandbox Suspicious Test File. It contains references to the EICAR test file URL and drop.com, and VirusTotal flags the URL as malicious by multiple vendors. However, the file hashes are not found in malware repositories, entropy is low, and no packers are detected. The file is likely benign and intended for sandbox testing or demonstration purposes rather than actual malicious activity.

Evidence Supporting Assessment

• File contains embedded URL http://rb3.ftnt.io/download00/eicar.com referenced in VirusTotal with 13 malicious detections
• File strings include 'Fortinet FortiSandbox Suspicious Test File' and 'This file is safe and is only to be used for demonstrations'
• PE sections show low entropy and no packers detected, consistent with non-obfuscated test file
• MalwareBazaar and VirusTotal hash lookups returned no matches indicating no known malware
• VirusTotal URL reputation indicates some vendors classify the URL as malicious or spyware

Ambiguity Notes

• No direct execution or behavioral telemetry is available to confirm if the file performs malicious actions
• URL reputation is mixed with some vendors flagging it as malicious and others as harmless
• File may be used in controlled testing environments which can resemble malware behavior
• Absence of hash matches in malware databases limits confidence in maliciousness

Alternative Hypotheses

• Fortinet FortiSandbox test or demonstration file used for security product validation
• Benign file containing references to EICAR test file for sandbox evasion or testing
• Potentially a benign downloader stub with no active malicious payload

Alternative Explanations

• File is a legitimate security testing artifact designed to trigger sandbox detections
• File is a harmless placeholder or decoy referencing known test malware files

Alternative Explanations — continued

• File is a sample used for educational or research purposes

Indicators of Compromise

Domains
- rb3.ftnt.io

URLs
- http://rb3.ftnt.io/download00/eicar.com

Hashes
- 83ac51c5a5149768c7e3edc669a89e691781e0d0
- 53a3fa5a92df144d980493942bc9282025f4b3de4253adba1e0102b43c3093c9

MITRE ATT&CK Mapping

None

Recommended Actions

• Verify the file origin and confirm it is intended for sandbox testing or demonstration
• Monitor any execution of this file in production environments for unexpected behavior
• Investigate network connections to rb3.ftnt.io for suspicious activity
• Avoid blocking this file in environments where Fortinet FortiSandbox testing is performed

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.

