AI-Assisted Investigation Report

Analyst

MalwareLab User

Analysis Time

2026-07-15 20:14:26 (EDT - America/New_York) | 2026-07-16 00:14:26 UTC

Model

gpt-4.1-mini

Version

beta-v2.0

Report Metrics

Input Size: 480.32 KB
IOCs Found: 8
ATT&CK Techniques: 6

Severity

Critical

Confidence

95% - High Confidence

Confidence Factors

• High detection count (64) on VirusTotal for both SHA1 and SHA256 hashes indicating malicious classification
• File named system.exe with no digital signature and unknown publisher
• Presence of ransomware ransom note text indicating file encryption and ransom demand
• Registry modifications to disable recovery and persistence mechanisms
• Scheduled task creation for persistence (uac task)
• Evidence of system reboot command to enforce ransomware activity

© 2026 MalwareLab.ai

Reducing Factors

None

Threat Type

Ransomware

Executive Summary

The analyzed PE executable (system.exe) is a ransomware sample that encrypts user files, drops ransom notes demanding Bitcoin payment, disables recovery options, persists via scheduled tasks and registry modifications, and forces system reboot. VirusTotal detections strongly support malicious classification.

Evidence Supporting Assessment

• File hashes (SHA1 and SHA256) detected as malicious by 64 vendors on VirusTotal
• Ransom note text instructing payment of 13 bitcoins to an email address for decryption
• Registry key 'crypted' added under CurrentVersion indicating ransomware state
• Scheduled task 'uac' created to execute persistence batch files
• Commands to disable recovery and advanced boot options via bcdedit
• Shutdown command issued to reboot system after infection

MalwareLab.ai
AI-Assisted Investigation Platform

Ambiguity Notes

• MalwareBazaar did not find this sample in its database, limiting attribution details
• No digital signature present, so no trust can be inferred from signing
• Lack of dynamic behavioral logs limits full attack chain reconstruction

Alternative Hypotheses

• Controlled malware research sample
• Red team simulation artifact
• Variant of known ransomware family

Alternative Explanations

None

Indicators of Compromise

URLs
- http://jaster.in/news/
- https://blockchain.info/api/receive?method=create&address=

 © 2026 MalwareLab.ai

Indicators of Compromise — continued

- http://c.e

Hashes
- 61ed25a706afa2f6684bb4d64f69c5fb29d20953
- 7d373ccb96d1dbb1856ef31afa87c2112a0c1795a796ab01cb154700288afec5

Processes
- system.exe
- schtasks.exe
- cmd.exe

MITRE ATT&CK Mapping

• T1486 - Data Encrypted for Impact
• T1059.003 - Windows Command Shell
• T1547.001 - Registry Run Keys / Startup Folder
• T1053.003 - Scheduled Task/Job
• T1562.001 - Disable or Modify Tools
• T1490 - Inhibit System Recovery

MalwareLab.ai
AI-Assisted Investigation Platform

Recommended Actions

• Investigate presence and execution of system.exe on endpoints
• Search for scheduled task 'uac' and related batch files in AppData\Local
• Review registry keys under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion for 'crypted' and 'rgd_bcd_condition'
• Monitor network connections to blockchain.info and related URLs
• Isolate infected hosts and perform forensic imaging
• Restore affected systems from clean backups
• Apply endpoint detection and response rules for ransomware behaviors including file encryption and persistence mechanisms

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.

 © 2026 MalwareLab.ai