

MALWARE ANALYSIS CERTIFICATE

CASE AND COMPUTER IDENTIFICATION

Case: Ransomware sample analysis (ID: CASE-MAL)
FIR number: FIR-2026-77
Analyst: Pallavi Pawar
Organisation: Innovativa SoftTech
Computer: LAPTOP-PL914FQ9
Operating system: Windows 11 10.0
Software: e-Dex v1.4.0
Algorithms used: SHA-256
Period covered: 2026-06-01 IST to 2026-06-18 IST
Chain of custody: Recorded in the application's tamper-evident, hash-chained audit log (append-only; altering any one entry breaks every following record).

MALWARE ANALYSIS

Sample name / family: LockBit variant
Sample SHA-256: 7d6b24a3c139a44fdcd0ddf53d833ee73b04c1d30bffdde63...ed2281f3424a01
Analysis type: Static + dynamic (sandbox)
Tools / sandbox: Cuckoo Sandbox, IDA, e-Dex

FINDINGS

The sample encrypts user files with AES-256 and appends a lockbit extension, contacts a command-and-control host over HTTPS, and drops a ransom note. No anti-VM evasion was observed in this run. The sample hash and dropped artifacts are listed in the annexure.

ANNEXURE - EVIDENCE RECORDS AND HASH VALUES (hashes per algorithm, as labelled)

#	FILE	SIZE	STATUS
1.	evidence-1.dd SHA-256: 874e9c3ea2b3c4dda2b3...4f3a2b3c4eda2b3c4f5a2b3c4fda2b3c505a2b3c50d Integrity: MATCH - computed hash equals the recorded expected hash.	51.0 MB	Verified
2.	evidence-2.dd SHA-256: 913213d9...13b4c...dea3b4c5e6a3b4c5eea3b4c5f6a3b4c5fea3b4c606a3b4c60e Integrity: MATCH - computed hash equals the recorded expected hash.	52.0 MB	Verified

VERIFICATION RESULT

Files checked: 2
Integrity verified: 2
Integrity failed: 0

RESULT: INTEGRITY VERIFIED - all recorded files match their expected hash values.

DECLARATION

I certify that I analysed the malware sample identified above using the analysis type and tools recorded, that the cryptographic hash values of the sample and any artifacts are reproduced in the annexure, and that the findings stated above are a true and accurate record of the results of that analysis to the best of my knowledge, information and belief.

Malware Analysis Certificate

Certificate No. 0019

Generated 2026-06-27 10:17:57 UTC (2026-06-27 15:47:57 IST)

CERTIFICATION

I, the undersigned, do hereby affirm that the analysis particulars and the findings set out in this certificate are true and correct to the best of my knowledge, information and belief, and were recorded without alteration.

Signature: _____
Name (printed): _____
Designation: Senior Forensic Analyst
Place: Pune
Date: _____

e-Dex generates this certificate as a workflow aid from the recorded analysis particulars and hash values; it does not itself analyse the sample. The analyst is solely responsible for the correctness of the methodology, findings and every fact stated, and for the sufficiency of this certificate for its intended purpose. The vendor makes no warranty of fitness for any particular use.

All times are stamped in UTC and shown in IST (Asia/Kolkata, UTC+5:30). Times displayed by third-party archive or extraction tools may differ due to local timezone conversion.

SAMPLE - NOT REAL EVIDENCE