POC of Tools

Tool Name:

CryptoHost Decryption Tool

Description:

CryptoHost Decryption Tool is a forensic utility developed to identify, decrypt, and analyze files encrypted by the CryptoHost ransomware. It assists in partial or full data recovery and helps digital forensic investigators trace the malwares encryption behavior.

What Is This Tool About?:

Specializes in reversing file encryption caused by CryptoHost ransomware in offline or isolated environments, detecting markers and decoding algorithms.

⋆Key Characteristics / Features:

Detects CryptoHost encryption signatures
Decrypts AES-based file encryption
Reconstructs original filenames and metadata
Works on physical and logical disk images
Batch decryption support
CLI & GUI support
Does not require internet access
Advanced log reporting
Forensic-grade evidence preservation
Supports known-plaintext attack module

Types / Modules Available:

CryptoHost Signature Detector
AES Key Brute Module
Metadata Recovery Engine
Batch File Processor
Encrypted Extension Mapper

How Will This Tool Help?:

Enables decryption, assists in investigations, and supports forensic analysis of CryptoHost ransomware cases.

15-Liner Summary:

1. Detects CryptoHost ransomware
2. Parses affected files and folders
3. Recovers metadata and file names

4. Fixes encrypted headers
5. Works with forensic images
6. Batch decryption enabled
7. CLI/GUI supported
8. Decrypts AES encodings
9. Drag-and-drop friendly
10. Fully offline
11. Auto reporting
12. Partial preview supported
13. Compatible with OS image formats
14. Student and analyst friendly
15. Portable, no install needed

⏱ Time to Use / Best Case Scenarios:

After ransomware infection
During disk image review
In ransomware analysis training

⏱ When to Use During Investigation:

Ransomware response
File recovery and forensics
Malware behavior analysis

⏱⏱ Best Person to Use This Tool & Required Skills:

Best User: Digital Forensics Student / Ransomware Analyst
Required Skills:
- File system knowledge
- Hex editing familiarity
- Understanding of ransomware behavior

⏱ Flaws / Suggestions to Improve:

No cloud-encrypted file support
Signature DB not user-editable
No real-time decryption feedback
GUI needs refinement

✓Good About the Tool:

Lightweight and portable
CryptoHost specific
Real recovery capabilities
Detailed logs for analysis