

Tools POC

POC of Tools

Tool Name:

DMA2 Locker Decoding Tool

Description:

DMA2 Locker Decoding Tool is a forensic utility designed to decode and analyze files encrypted or locked by the DMA2 ransomware. It helps investigators and analysts retrieve hidden or obscured data from affected systems for recovery and analysis.

What Is This Tool About?

The tool is specifically built to deal with ransomware-infected systems, especially those compromised by DMA2 Locker. It decodes file patterns, identifies encryption signatures, and helps recover partial or full content where possible. It also assists in understanding the malware's behavior by tracing changes made by it.

Key Characteristics / Features:

- Detects DMA2 locker signatures in files
- Decodes XOR/encrypted file structures
- Identifies file header manipulation
- Generates reports of recovered data
- Works on both full disk and partial image files
- Supports batch decoding
- No internet required – fully offline capable
- Supports drag and drop interface
- Generates detailed logs for evidence purposes
- Compatible with Windows and Linux forensic images
- CLI and GUI interface
- Preview recovered content
- Metadata extraction from encoded files
- Hex-level inspection tools built-in
- Signature database auto-updated (optional feature)

Types / Modules Available:


- DMA2 Signature Scanner
- XOR Decoder Module
- File Header Fixer
- Batch Decryption Engine

- Metadata Recovery Module
- Report Generator

How Will This Tool Help?

- Identifies presence of DMA2 ransomware
- Recovers partial or full data from encrypted files
- Supports evidence collection during forensic investigation
- Helps understand encryption pattern used by malware
- Improves speed of incident response in ransomware cases

Proof of Concept (PoC) Images:

 (Insert images of: decoded file, signature match alert, metadata view, batch decode progress, and recovered text preview — make sure they look like screenshots from student environment or VM with a simple GUI)

15-Liner Summary:

1. Detects DMA2 ransomware infections
2. Parses affected files and folders
3. Recovers file metadata and structure
4. Fixes encrypted file headers
5. Works with forensic disk images
6. Batch process multiple files at once
7. CLI and GUI both available
8. Decodes XOR and custom encodings
9. Drag and drop interface for ease
10. Offline usage supported
11. Auto-report generation
12. Recover previewable data
13. Compatible with major OS image formats
14. Easy-to-use for students and analysts
15. Portable execution (no install needed)

Time to Use / Best Case Scenarios:

- After ransomware infection is suspected
- During disk image analysis
- While reviewing recovered files
- Early in post-breach incident response
- When user reports sudden file locking

When to Use During Investigation:

- Ransomware infection response
- File recovery and evidence extraction

- User device triage
- Malware behavioral analysis
- Dark web data tracking (to compare with file signatures)



Best Person to Use This Tool & Required Skills:

Best User: Digital Forensics Student / Ransomware Analyst

Required Skills:

- Basic knowledge of file systems
- Familiarity with hex editors
- Understanding of ransomware behavior
- Basic command-line usage



Flaws / Suggestions to Improve:

- No support for cloud-encrypted files
- Signature DB not customizable by user
- Lack of real-time decryption feedback
- Needs more documentation for beginners
- GUI could be more user-friendly



Good About the Tool:

- Lightweight and student-friendly
- Focused specifically on DMA2 ransomware
- Provides real recovery options
- Portable and fast
- Good logs for academic analysis