POC of Tools

Tool Name:

CryptoKuchlen Decryption Tool

Description:

CryptoKuchlen Decryption Tool is designed to reverse and analyze files encrypted by CryptoKuchlen ransomware. It supports multi-layer decryption involving XOR and substitution techniques.

What Is This Tool About?:

Focuses on decoding multi-layered ransomware encryptions and reconstructing partially lost data for forensic analysis.

⋆Key Characteristics / Features:

Hybrid XOR/Substitution decryption
Encrypted file classifier
Nested ransomware marker detection
Timeline correlation from metadata
Graph-based decryption path visualization

Types / Modules Available:

CryptoKuchlen Signature Scanner
Layer Decoder Module
Hybrid Decryption Engine
File Carver & Reconstructor
Report Generator

How Will This Tool Help?:

Decrypts files partially or fully, helps analysts understand multi-layer ransomware behaviors and assists recovery teams.

15-Liner Summary:

1. Identifies CryptoKuchlen ransomware
2. Scans and decrypts layers
3. Recovers metadata and timestamps
4. Batch file decryption supported
5. Forensic disk image compatible
6. GUI and CLI interface
7. Multi-layer report generation
8. Works offline

9. Graphical decryption map
10. Evidence-ready reporting
11. Recovers deleted file headers
12. Partial plaintext reconstruction
13. Supports dark web signature matching
14. Good for advanced analysts
15. Plugin compatible

⍰ Time to Use / Best Case Scenarios:

After ransomware detection
Advanced malware labs
Field recovery operations

⍰ When to Use During Investigation:

Layered encryption analysis
Disk carving and recovery
Behavioral malware inspection

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

Best User: Malware Analyst / Forensics Expert
Required Skills:
- Understanding of XOR and substitution ciphers
- Malware analysis techniques
- Familiarity with forensic toolkits

⍰ Flaws / Suggestions to Improve:

Complex for beginners
No Mac version
Key detection not automated

✓Good About the Tool:

Advanced decryption visualization
Effective on multi-layer infections
Integrated forensics features