Tools POC

Pletor Decrypting Tool

Tool Name:

Pletor Decrypting Tool

Description:

A cybersecurity decryption utility aimed at decoding ransomware-encrypted files, specifically those affected by the Pletor ransomware strain.

What Is This Tool About?

Pletor Decrypting Tool is designed to analyze, identify, and decrypt files that have been encrypted by the Pletor ransomware family using known cryptographic weaknesses or key recovery mechanisms.

Key Characteristics / Features:

1. Decrypts files affected by Pletor ransomware
2. Automatic file type recognition and batch decryption
3. Supports both offline and network-based key retrieval
4. Generates forensic reports with decryption logs
5. No internet required for local decryption
6. Lightweight, portable tool (no installation)
7. Command-line and GUI versions
8. Integration-ready with existing IR pipelines
9. Works on encrypted files from external drives
10. Logging with timestamps and hash validation
11. Compatible with Windows XP 11
12. Custom rules engine for unknown variants
13. REST API for automation
14. Error handling and recovery
15. Open-source modules available for extension

Tools POC

Types / Modules Available:

- FileScanner Engine
- Key Identifier
- Decryption Engine
- Error Recovery Handler
- Forensic Log Generator
- Pletor Variant Detector

How Will This Tool Help?

- Recovers encrypted user data
- Assists in forensic investigation of ransomware attacks
- Speeds up incident response
- Provides reports for legal or audit trails
- Minimizes downtime post-infection

Proof of Concept (PoC) Images:

(Insert 10 screenshots showing file decryption interface, decrypted file list, and logs)

15-Liner Summary:

1. Specialized for Pletor ransomware
2. Offline and online key recovery
3. Cross-platform file system support
4. CLI and GUI options
5. Logging for chain of custody
6. Error correction module
7. Works on removable media
8. Supports batch operations
9. Minimal resource usage
10. Encrypted file pattern recognition
11. Open-source friendly architecture

12. REST API for scripting
13. Auto-mapping of original filenames
14. Integration with SIEMs
15. Frequent updates and support

Time to Use / Best Case Scenarios:

- Immediately after ransomware attack
- During recovery phase post-infection
- After disk/image acquisition
- For testing ransomware simulations
- In training cyber defense teams

When to Use During Investigation:

- Ransomware infection reports
- Data breach response
- Internal compromise analysis
- IR tabletop exercises
- National CERT advisories

Best Person to Use This Tool & Required Skills:

Best User: Incident Responder / Malware Analyst

Required Skills:

- Familiarity with ransomware behavior
- File system forensics
- Basic cryptography knowledge
- Hands-on with CLI tools and logs

Flaws / Suggestions to Improve:

- Limited to known variants
- No GUI log export

Tools POC

- Add support for live RAM analysis
- Include backup integration module
- Improve UX for non-technical users

Good About the Tool:

- Efficient and lightweight
- Portable and works offline
- Reliable key detection
- Simple interface with good logs

Polyglot Decrypting Tool

Tool Name:

Polyglot Decrypting Tool

Description:

A reverse engineering and decryption suite designed to analyze and extract payloads from polyglot filesmalicious files that masquerade as multiple formats.

What Is This Tool About?

Polyglot Decrypting Tool inspects files containing multiple embedded formats or obfuscations (e.g., PDF+EXE, JPG+ZIP), helping analysts uncover malicious payloads hidden via polyglot techniques.

Key Characteristics / Features:

1. Detects file format overlaps
2. Extracts embedded scripts/binaries
3. Disassembles hybrid formats
4. Cross-platform compatibility
5. Visualizes overlapping header regions
6. CLI and GUI support

Tools POC

7. Format-specific extractors (PDF, JPG, EXE, etc.)
8. Supports both static and dynamic modes
9. Hex viewer with entropy highlight
10. YARA rule integration
11. Timeline view of file execution paths
12. Custom signature builder
13. Metadata analysis
14. Sandbox integration optional
15. Supports encrypted embedded payloads

Types / Modules Available:

- Polyglot Detector
- Format Splitter
- Entropy Analyzer
- Binary Extractor
- Visualization Panel
- YARA Engine Connector

How Will This Tool Help?

- Reveals hidden or obfuscated threats
- Helps in APT and red-team investigations
- Supports detection of malware hidden in images/docs
- Useful for malware reverse engineering training

Proof of Concept (PoC) Images:

(Insert screenshots of overlapping file analysis, format separation, and disassembly outputs)

15-Liner Summary:

1. Decrypts and separates polyglot files
2. Identifies hidden malware

Tools POC

3. Supports static/dynamic analysis
4. Offers entropy-based anomaly detection
5. CLI & GUI support
6. Visual format overlay
7. Cross-format compatibility
8. Hex editor built-in
9. Forensically sound extraction
10. Format signature matching
11. Timeline view of execution paths
12. Embedded encryption handling
13. Detailed logging & metadata
14. Custom rule-based scan
15. Integration with malware sandboxes

Time to Use / Best Case Scenarios:

- Analyzing suspicious attachments
- Threat hunting for APTs
- Incident response triage
- Malware research labs
- Detecting file-based evasion tactics

When to Use During Investigation:

- Email-based attacks
- Steganographic payloads
- Polyglot malware campaigns
- Suspicious file format detections
- Red team simulations

Best Person to Use This Tool & Required Skills:

Best User: Malware Analyst / Threat Researcher

Tools POC

Required Skills:

- File format internals (PDF, EXE, JPG, etc.)
- Malware unpacking
- YARA rule writing
- Static/dynamic analysis familiarity

Flaws / Suggestions to Improve:

- No built-in sandbox (external required)
- Heavy memory usage on large files
- Improve automation scripting options
- Add cloud support
- Improve embedded file entropy graph UI

Good About the Tool:

- Highly specialized for complex payloads
- Powerful visualization
- Strong community rule support
- Deep binary extraction features