POC of Tools

Tool Name:

DarkSide Ransomware Decryption Tool

Description:

A digital forensics tool designed to assist in decrypting files encrypted by the DarkSide ransomware variant. It allows cybersecurity professionals to identify encryption patterns and attempt recovery of affected data.

What Is This Tool About?

The tool attempts to decrypt files encrypted by the DarkSide ransomware by exploiting known weaknesses or using stored private keys. It supports various file types and assists in reducing ransom payment necessity.

Key Characteristics / Features:

- Decrypts files locked by DarkSide ransomware variants
- Supports bulk file decryption
- Identifies encryption keys or patterns
- Runs on Windows and Linux
- Portable and requires no installation
- CLI and GUI support
- Logging and reporting capability
- Supports encrypted file backup
- Error-handling and rollback features
- Regularly updated key database

Types / Modules Available:

- Encrypted File Scanner
- Key Analyzer
- Decryption Engine
- Log Generator
- Rollback Utility

- Hash Verifier

How Will This Tool Help?

- Attempts decryption of files without paying ransom
- Analyzes ransomware encryption behavior
- Supports incident response and data recovery
- Assists in understanding ransomware artifacts
- Enables audit reporting and chain-of-custody

15-Liner Summary:

- Decrypts files encrypted by DarkSide ransomware
- No need for ransom payments in some cases
- Supports various file types and extensions
- Automated decryption with backup handling
- Runs in CLI or GUI mode
- Supports key injection and pattern-based guessing
- Generates detailed forensic logs
- Cross-platform: Linux and Windows support
- Performs hash verification post decryption
- Modular and scriptable design
- Lightweight and portable
- Actively maintained and updated
- Error handling and rollback supported
- Ideal for IR and LEA teams
- Supports multiple ransomware samples

Time to Use / Best Case Scenarios:

- Immediately after a DarkSide ransomware infection

- During data recovery planning
- When ransom demands are made
- For educational simulation environments
- During forensic analysis of affected machines

When to Use During Investigation:

- Post-incident ransomware analysis
- File recovery in infected systems
- Forensic chain-of-custody preservation
- Behavioral analysis of ransomware samples
- Key identification and reuse scenarios

Best Person to Use This Tool & Required Skills:

Best User: Ransomware Analyst / Incident Responder

- Understanding of ransomware structure
- Basic cryptographic knowledge
- CLI tool handling experience
- Incident response methodology
- Experience in digital forensics suites

Flaws / Suggestions to Improve:

- Limited to known encryption patterns
- Fails if encryption keys aren't available
- Lacks real-time monitoring capabilities
- May need admin rights to decrypt certain files

Good About the Tool:

- Lightweight and effective
- Free alternative to ransom payments

POC of Tools

- CLI and GUI support

- Detailed decryption reports

- Helps recover encrypted data safely