Tool Name:

Dragon Cyber Ransomware Decryption Tool

Description:

A specialized decryption utility designed to recover files encrypted by the Dragon Cyber ransomware strain, helping victims regain access to their data without paying a ransom.

What Is This Tool About?

This tool targets a specific ransomware family—Dragon Cyber—and decrypts the affected files using reverse-engineered keys or known weaknesses in the ransomware's encryption method.

⭑Key Characteristics / Features:

- Supports decryption of files encrypted by Dragon Cyber variants
- Detects encrypted files automatically
- Lightweight and easy to use
- No internet connection required
- Command-line and GUI interfaces
- Batch decryption supported
- Verifies file integrity post-decryption
- Compatible with Windows systems
- Safe to run on infected machines
- Decryption log generation
- Ability to restore original filenames
- Checks for ransomware presence before operation
- Fast decryption with minimal system resource use
- Does not require original encrypted files for key identification
- Offline operation enhances security

Types / Modules Available:

- File Scanner & Identifier
- Key Generator (if keys are recoverable)
- Decryption Engine
- Logging Module
- Backup Creator (optional)
- File Integrity Validator

How Will This Tool Help?

- Enables recovery of encrypted files without ransom payment
- Aids in ransomware variant identification
- Helps IT admins restore critical business operations quickly
- Assists forensic teams in analyzing encryption mechanisms

- Offers log files for further reporting and legal evidence

15-Liner Summary:

- Detects Dragon Cyber ransomware encrypted files
- Recovers data without paying ransom
- CLI and GUI options available
- Lightweight and standalone
- Works with major Windows file systems
- Logs every decrypted file
- Restores original filenames where possible
- Compatible with backups
- Useful for both IT and forensic teams
- No network required (offline mode)
- Generates detailed report logs
- Supports bulk decryption
- Automatically detects encryption signatures
- Verifies decrypted file integrity
- Updated regularly to include new variants

Time to Use / Best Case Scenarios:

- Immediately after ransomware attack detection
- Before restoring from backups
- During post-incident response
- While collecting forensic evidence
- When verifying extent of ransomware impact

When to Use During Investigation:

- During triage of ransomware infection
- While identifying encryption footprint
- During system recovery planning
- Before malware eradication
- While validating data recovery integrity

Best Person to Use This Tool & Required Skills:

- Best User:
  Incident Responder / Digital Forensics Analyst / IT Administrator
- Required Skills:
  - Familiarity with ransomware behavior
  - Basic forensic investigation experience
  - Knowledge of Windows file systems
  - Comfort with command-line or GUI forensic tools
  - Understanding of safe malware handling procedures

⍰ Flaws / Suggestions to Improve:

- Currently Windows-only; lacks Linux/Mac support
- Limited to known ransomware keys—cannot brute-force unknown variants
- GUI could be made more intuitive for non-technical users
- No live ransomware neutralization (decryption only)
- Add automatic secure file backup before decryption

✓Good About the Tool:

- Free and frequently updated
- Safe to use even on infected systems
- Portable and does not require installation
- Recovers files effectively from known ransomware strains
- Provides logs for accountability and auditing