Proof of concept report

Crypt888 Decrypting Tool

History

Crypt888 (also known as Mircop ransomware) was active around mid-2016. It encrypted user files and demanded ransom notes in aggressive, threatening language. Researchers later released a decryption tool after reverse-engineering the ransomware's weak encryption mechanism.

Description

A free decryption utility developed by cybersecurity experts to recover files encrypted by the Crypt888 ransomware without paying the ransom.

What Is This Tool About?

The Crypt888 Decrypting Tool is designed to analyze and reverse the encryption scheme used by Crypt888 and restore access to locked files.

Key Characteristics / Features

- Recovers files encrypted with ".locked", ".mircop" extensions
- No internet connection required
- Scans entire directories for infected files
- Detects encryption keys from known patterns
- Supports batch file decryption
- Compatible with FAT32, NTFS systems
- Logs decrypted files
- Developed by trusted vendors (e.g., Emsisoft, Avast)
- Lightweight and portable
- Built-in verification of decrypted content
- GUI and CLI versions available
- No user credentials needed
- Works on Windows 7 and above
- Updates for new variants (if any)
- Easy-to-use wizard interface

Types / Modules Available

- Full Directory Scanner
- Custom File Selector
- Decryption Engine

- Logs Generator
- Verification Module

How Will This Tool Help?

It provides victims with a free way to recover their files and avoid ransom payments, supporting digital forensics, incident response, and user data recovery.

15-Liner Summary

- Recovers .mircop/.locked ransomware files
- Works offline
- GUI + CLI available
- Developed by reputable cybersecurity teams
- Full directory scan or individual file selection
- Verification and logging support
- Minimal setup required
- Actively maintained
- Restores original filenames
- No registry modifications
- Uses heuristic detection
- Open-source version available
- Can be used in corporate environments
- User-friendly design
- Supports command-line automation

Time to Use / Best Case Scenarios

After initial ransomware detection After isolating infected machine Before reformatting disk

When to Use During Investigation

As part of containment & recovery After malware sample analysis To compare pre/post-encryption files When collecting encrypted file evidence

Best Person to Use This Tool & Required Skills

Best User: Forensic Analyst / Incident Responder Required Skills: Basic understanding of ransomware Familiarity with Windows directory structure Log and signature analysis

Flaws / Suggestions to Improve

Doesn’t work if ransomware has corrupted files Limited to older variants needs better compatibility with deep-nested directories Add option to auto-detect variant

Advantages of the Tools

- 100% free
- Saves valuable data
- Community-trusted
- Offline usage
- Efficient and fast decryption

CryptInfinite Decrypting Tool

History

CryptInfinite (also known as DecryptorMax) emerged in 2016, encrypting files and appending ".crinf" extensions. Security researchers exploited flaws in the encryption process to release a free decryptor.

Description

A utility that reverses CryptInfinite encryption using pre-identified static keys or heuristics to restore access to victim files.

What Is This Tool About?

The tool scans systems infected by the CryptInfinite ransomware and decrypts files using hard-coded or recovered keys.

Key Characteristics / Features

- Decrypts ".crinf" extension files
- Recovers original filenames
- No ransom payment required
- In-built key recovery logic
- Fully portable
- Detects multiple encryption formats
- User log generation
- Minimal memory usage
- Compatible with Windows 7+
- Command-line and GUI available
- Real-time progress updates
- Generates backup before decryption
- Includes file integrity verification
- Developed in collaboration with law enforcement
- Updated with variant signature detection

Types / Modules Available

- Encrypted File Scanner
- Static Key Library
- Variant Identifier
- Decryption Routine
- User Logs Viewer

How Will This Tool Help?

This tool enables quick, effective recovery from CryptInfinite attacks, minimizing downtime and loss of data.

15-Liner Summary

- Decrypts .crinf files
- Static + dynamic key detection
- Compatible across OS versions
- Can run on compromised systems
- Open-source components
- No installation needed
- Backup before decryption
- Minimal system resources
- CLI for advanced usage
- Detailed logs generated
- Safe and legal tool
- Developed by anti-malware labs
- Real-time decryption view
- Can work with removable media
- Recognizes multiple ransomware strains

Time to Use / Best Case Scenarios

After malware is quarantined Before reimaging system In post-incident response

When to Use During Investigation

During file recovery efforts After sample analysis of the malware When correlating encrypted with decrypted artifacts

Best Person to Use This Tool & Required Skills

Best User: Malware Analyst / Digital Recovery Specialist Required Skills: Experience with ransomware behavior File structure familiarity Optional: Scripting knowledge for CLI version

Flaws / Suggestions to Improve

Ineffective against newer or modified variants UI could be more intuitive Needs cloud backup detection module Add checksum verification

Advantages of the Tools

- Quick data restoration
- 100% safe and trusted
- Low resource footprint
- Active community support
- Widely used in forensic investigations