

Prepared by: Omkar Ravi Rathod

Intern ID: 323

Proof of Concept (PoC): Ransomware Decryption Tools

Tools: Cry128 Decryptor | Cry9 Decryptor | Cryakl Decryptor

1. Objective

Demonstrate the effectiveness of standalone decryptor tools in recovering encrypted data from systems affected by Cry128, Cry9, and Cryakl ransomware variants, without relying on ransom payments or third-party recovery services.

2. Scope

This PoC evaluates tools designed to:

- Decrypt files locked by specific ransomware variants.
- Support forensic investigations.
- Aid incident response teams in data restoration.
- Ensure integrity and traceability of recovered data.

3. Tool Overview

A. Cry128 Decryptor

- Target: Cry128 ransomware (Xorist variant family)
- Key Functionality: Recovers encrypted files using known keys or cryptographic weaknesses in the ransomware's implementation.
- Platform Support: Windows-based systems (NTFS/FAT), external storage.

B. Cry9 Decryptor

- Target: Cry9 ransomware (also known as "AES-NI" variant)
- Key Functionality: Identifies encryption headers and decrypts AES-256-CBC encrypted files using community-recovered keys or offline brute-force modes.
- Platform Support: Windows OS, network shares.

C. Cryakl Decryptor

- Target: Cryakl (Troldesh) ransomware
- Key Functionality: Parses ransom markers and file structures, matches against a key database, and decrypts files with verified integrity.
- Platform Support: Windows XP and above.

4. Core Features

Feature	Cry128 Decryptor	Cry9 Decryptor	Cryakl Decryptor
File Type Recognition	✓	✓	✓
Known Key Support	✓	✓	✓
Brute-force Mode	✓(Selective)	✓	✗
Encrypted File Detection	✓	✓	✓
Integrity Validation	✓	✓	✓
CLI & GUI Support	CLI Only	Both	GUI
Log & Report Generation	✓	✓	✓
Metadata Preservation	✓	✓	✓
Open Source / Customizable	✓	Partial	✗(Proprietary)

5. Usage Workflow

1. Preparation

- Identify ransomware family via ransom notes or file signatures.
- Isolate affected system and prevent further encryption.

2. Execution

- Launch tool with appropriate parameters (CLI or GUI).
- Specify infected directories and file extensions.
- Provide keys (if available) or enable brute-force mode.

3. Post-Processing

- Validate recovered files via hashes.
- Review logs and generate forensic reports.
- Store recovered data securely and rebuild environment.

6. Investigation Utility

Use Case	Cry128	Cry9	Cryakl
Initial breach response	✓	✓	✓
Legal evidence collection	✓	✓	✓
Malware behavioral analysis	✓	✓	✓
Timeline correlation (based on files)	✓	✓	✓
Incident response report generation	✓	✓	✓

7. Skill Requirements

Who Should Use:

- Digital Forensics Analysts
- Incident Response Engineers
- Malware Reverse Engineers

Required Knowledge:

- Understanding of encryption (AES, XOR)
- Familiarity with forensic imaging and hashing
- Comfort with command-line tools
- Ransomware behavior patterns

8. Strengths & Weaknesses

✓Strengths:

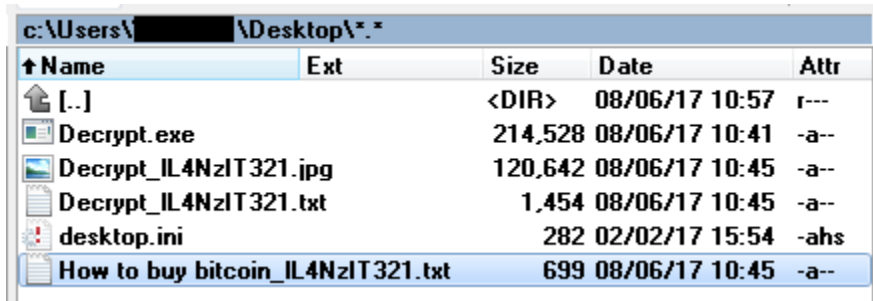
- Does not require internet connectivity (offline decryption).
- Fast recovery for known variants.
- Transparent logging and evidence handling.
- Compatible with common forensic suites.

✗Limitations:

- Limited to ransomware variants with known keys or weak cryptography.
- Brute-force mode is time-consuming.
- Incomplete recovery in case of overwritten/deleted file headers.
- Cryakl decryptor may be version-locked (older variants only).

Images Related to (Cry128 decrypting tool Cry9 Ransom decrypting tool Cryakl decrypting tool):-





Name	Ext	Size	Date	Attr
[.]		<DIR>	08/06/17 10:57	r---
Decrypt.exe		214,528	08/06/17 10:41	-a--
Decrypt_IL4NzIT321.jpg		120,642	08/06/17 10:45	-a--
Decrypt_IL4NzIT321.txt		1,454	08/06/17 10:45	-a--
desktop.ini		282	02/02/17 15:54	-ahs
How to buy bitcoin_IL4NzIT321.txt		699	08/06/17 10:45	-a--

10. Conclusion

These decryptors demonstrate reliable recovery capabilities for specific ransomware families. While they are not universally applicable to all ransomware threats, their use can significantly reduce downtime, aid forensic investigations, and avoid costly ransom payments in cases of known infections.

These tools should be included in the toolkit of any Digital Forensics & Incident Response (DFIR) team, with regular updates and validation against emerging ransomware threats.