POC OF TOOLS

Tool Name: MacRansom Decryption Tool / Magniber Decryptor

HISTORY :-

MacRansom and Magniber are ransomware families known for targeting macOS and Windows systems respectively. Both emerged in different timeframes—MacRansom around 2017, distributed via RaaS (Ransomware-as-a-Service), and Magniber targeting mostly Asian regions via browser-based exploits. Security researchers and antivirus firms developed specialized decryption tools once vulnerabilities were found in the encryption methods used, especially in earlier versions of these ransomware variants. These tools were released to assist victims in data recovery without paying ransom.

DESCRIPTION :-

This tool is a cybersecurity utility designed to decrypt files encrypted by MacRansom or Magniber ransomware. It attempts to reverse the encryption process using known flaws or leaked keys in the ransomware's encryption logic.

WHAT IS THIS TOOL ABOUT ?

The tool is used to restore access to files that were encrypted by MacRansom or Magniber ransomware attacks. It analyzes encrypted file structures, identifies the ransomware variant, and attempts decryption based on available signatures or cryptographic weaknesses.

KEY CHARACTERISTICS / FEATURES :-

- Detects specific MacRansom and Magniber variants.
- Uses static keys or decryption algorithms based on reverse engineering.
- Supports batch decryption of encrypted files.
- Compatible with multiple file formats (e.g., .doc, .pdf, .jpg).
- Cross-platform support (macOS and Windows).
- Generates log files for investigation documentation.
- Simple GUI and CLI version available.
- Free and open-source (in most versions).
- Signature-based identification of ransomware version.
- Does not require internet access.
- Lightweight and fast execution.

 Includes file integrity verification post-decryption.

 Automatic backup before decryption.

 Frequently updated by cybersecurity community.
Supports integration into forensic toolkits.

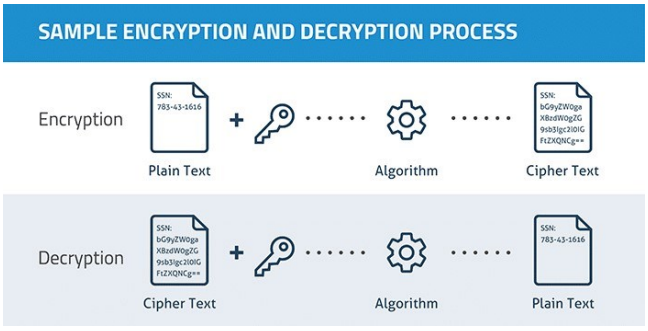
TYPES / MODULES AVAILABLE :-

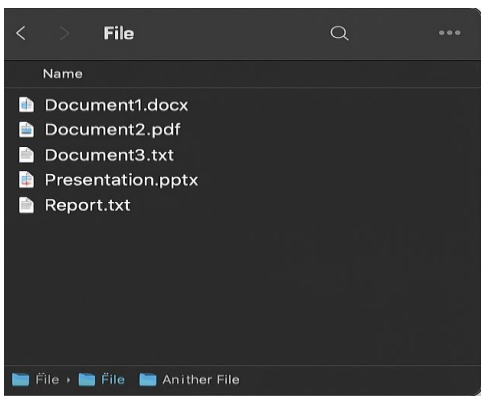
- Variant Detector.
- Static Key-Based Decryptor.
- File Type Handler.
- Log Generator.
- Decryption Verification Module. - GUI/CLI Interface Modules.

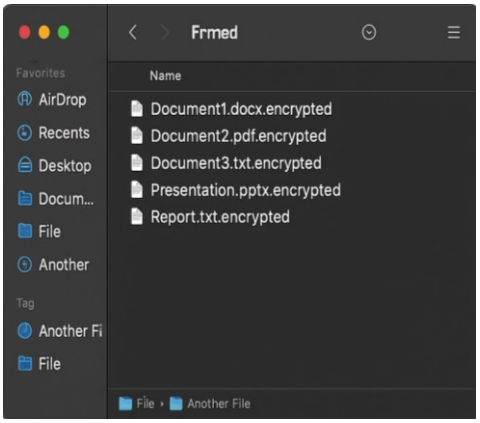
HOW WILL THIS TOOL HELP ?

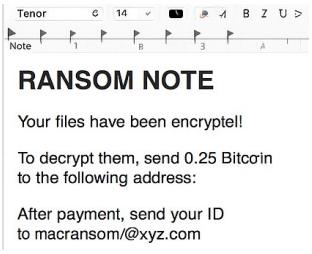
- Assists in data recovery after ransomware attacks.
- Reduces downtime and financial loss.
- Avoids ransom payment.
- Supports forensic investigations by identifying ransomware behavior.
- Can be integrated into forensic or incident response workflows.
- Enables analysts to test and train using ransomware samples in labs.

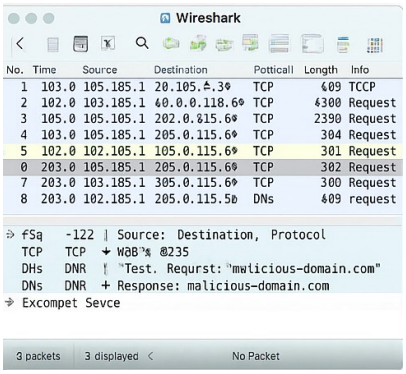
PROOF OF CONCEPT(POC) IMAGES :-

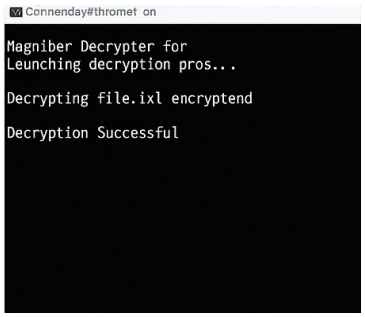


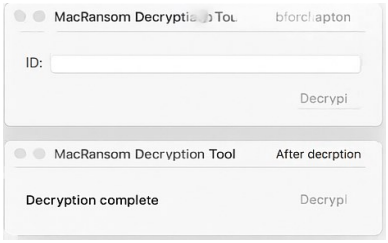


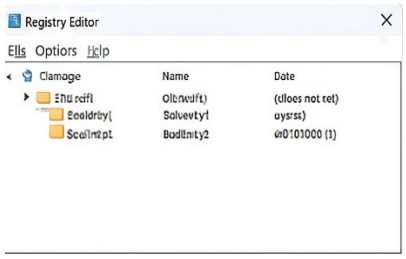


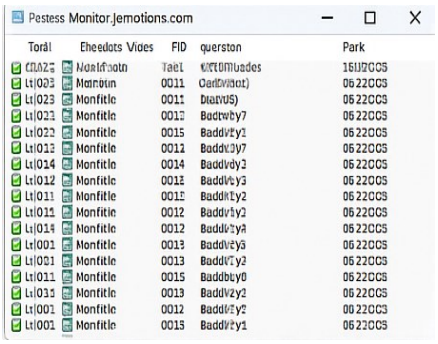

Tenor
14
Note
RANSOM NOTE
Your files have been encrypte!!
To decrypt them, send 0.25 Bitcoin to the following address:
After payment, send your ID to macransom/@xyz.com


Wireshark
No. Time Source Destination Potticall Length Info
1 103.0 105.185.1 20.105.4.3 TCP 609 TCCP
2 102.0 103.185.1 60.0.0.118.6 TCP 6300 Request
3 105.0 105.105.1 202.0.&15.6 TCP 2390 Request
4 103.0 105.185.1 205.0.115.6 TCP 304 Request
5 102.0 102.105.1 105.0.115.6 TCP 301 Request
0 203.0 105.185.1 205.0.115.6 TCP 302 Request
7 203.0 103.185.1 305.0.115.6 TCP 300 Request
8 203.0 102.185.1 205.0.115.5 DNs 609 request
fSq -122 | Source: Destination, Protocol
TCP TCP W0B %235
DHs DNR "Test. Requrst: "malicious-domain.com"
DNs DNR Response: malicious-domain.com
Excompet Sevce
3 packets 3 displayed No Packet

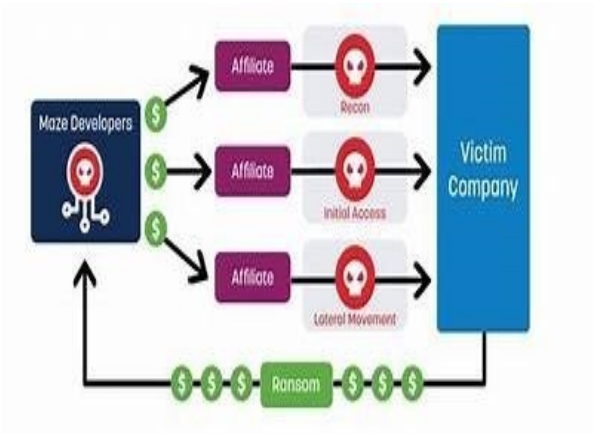

Connenday#thromet on
Magniber Decrypter for
Leunching decryption pros...
Decrypting file.ixl encryptend
Decryption Successful


MacRansom Decryption Tool
ID:
Decrypi
MacRansom Decryption Tool
After decrption
Decryption complete
Decrypi


Registry Editor
Ells Optiors Help
Clamage
Name
Date


Pestess Monitor.Jemotions.com
Torál
Eheedats Vides
FID
querston
Park


Phishing emails
Backup encryption
Increased network traffic and activity
Suspicious file extensions
RANSOMWARE
Increased disk activity
Audit policy changes
High CPU usage
Changes to system settings


Maze Developers
Affiliate
Affiliate
Affiliate
Recon
Initial Access
Lateral Movement
Victim Company
Ransom

15-LINERS SUMMARY :-

1. Decrypts MacRansom and Magniber encrypted files.
2. Identifies variant from encrypted file structure.
3. Compatible with macOS and Windows.
4. Uses reverse-engineered keys and logic.
5. 5. Offers CLI and GUI interfaces.
6. Helps recover common file formats.
7. Supports batch processing.
8. Secure and offline usage.
9. Free to use and community-supported.
10. Backup before decryption.
11. Logs every activity for documentation.
12. Lightweight and fast.
13. Reliable for earlier versions of ransomware.
14. Maintained by cybersecurity experts.
15. Useful in education, testing, and forensic recovery.

TIME TO USE / BEST CASE SCENARIOS :-

- Immediately after ransomware attack.
- When encrypted files are identified.
- During forensic file system analysis.
- When ransomware note suggests MacRansom/Magniber. - During controlled ransomware research/testing in labs.

WHEN TO USE DURING INVESTIGATION :-

- After detecting encryption patterns in file names.
- During malware/ransomware forensics.
- When log evidence suggests specific variants.
- Before considering system wipe or ransom payment. - As part of early incident response phase.

BEST PERSON TO USE THIS TOOL AND REQUIRED SKILLS :-

Best User: Malware Analyst / Cybersecurity Forensic Investigator.

Required Skills:

- Basic understanding of ransomware mechanics.
- Experience with encrypted file analysis.

- Familiarity with CLI or GUI decryption tools.
- Ability to analyze logs and validate results

FLAWS / SUGGESTIONS TO IMPROVE :-

- May not support newer, more complex variants.
- Not effective if strong encryption was used.
- Limited documentation in some releases.
- Suggest improvement in UX for non-technical users.
- Add support for encrypted archives and system files.

GOOD ABOUT THE TOOL :-

- Freely available and open-source.
- Reliable for many older ransomware variants.
- Easy to integrate into security workflows.
- Saves time and resources in post-attack recovery. - Valuable educational and forensic resource.