

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.

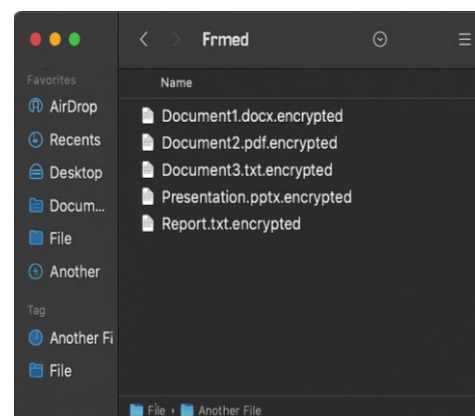
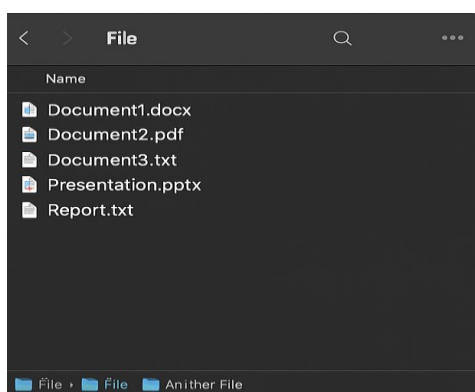
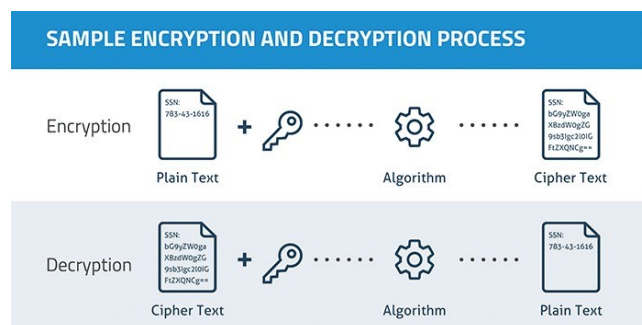
TYPES / MODULES AVAILABLE :-

- 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 :-





Your files have been encrypted!

To decrypt them, send 0.25 Bitcoin to the following address:

After payment, send your ID
to macransom/@xyz.com

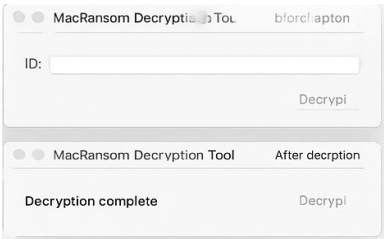
The image shows a Wireshark packet capture interface. The top toolbar includes icons for file operations, network analysis, and search. The main display area shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 5 is selected, showing a DNS request from 10.102.102.185 to 10.105.115.69. Packet 6 is the corresponding DNS response from 10.105.115.69 to 10.102.102.185. The packet details pane for packet 6 shows the DNS structure, including the question section with the query 'Test. Request: "imwlicious-domain.com"' and the answer section with the response 'malicious-domain.com'. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	103.0	105.185.1	20.105.4.30	TCP	409	TCP
2	102.0	103.185.1	40.0.0.118.69	TCP	4308	Request
3	105.0	105.185.1	202.8.115.69	TCP	2390	Request
3	103.0	105.185.1	205.0.115.69	TCP	304	Request
5	102.0	102.102.185	105.0.115.69	TCP	301	Request
6	103.0	105.185.1	205.0.115.69	TCP	302	Request
7	103.0	103.185.1	305.0.115.69	TCP	300	Request
8	203.0	102.185.1	205.0.115.50	DNS	409	request

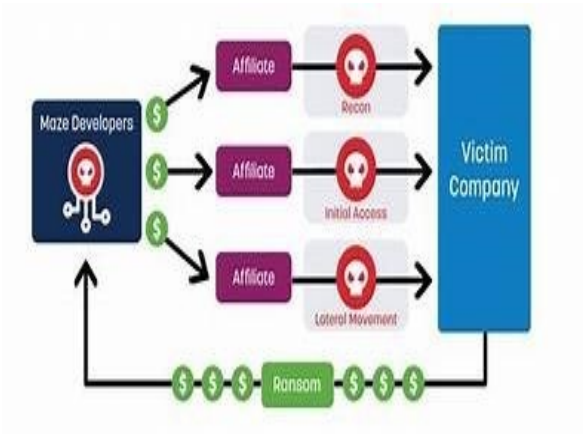
Packet 6 details:

```

Ethernet II, Src: Intel(R) Ethernet Controller (3:9:30:97:00:00:00:00), Dst: Intel(R) Ethernet Controller (3:9:30:97:00:00:00:00), Length: 1440
Internet Protocol Version 4, Src: 10.105.115.69, Dst: 10.102.102.185
Transmission Control Protocol, Src Port: 53, Dst Port: 53, Seq: 302, Len: 100
Domain Name System (query response)
  Standard query response
    Question
      Test. Request: "imwlicious-domain.com"
    Answer
      DNR #1: Test. Request: "imwlicious-domain.com"
      DNR #2: Test. Request: "imwlicious-domain.com"
      DNR #3: Test. Request: "imwlicious-domain.com"
      DNR #4: Test. Request: "imwlicious-domain.com"
      DNR #5: Test. Request: "imwlicious-domain.com"
      DNR #6: Test. Request: "imwlicious-domain.com"
      DNR #7: Test. Request: "imwlicious-domain.com"
      DNR #8: Test. Request: "imwlicious-domain.com"
      DNR #9: Test. Request: "imwlicious-domain.com"
      DNR #10: Test. Request: "imwlicious-domain.com"
      DNR #11: Test. Request: "imwlicious-domain.com"
      DNR #12: Test. Request: "imwlicious-domain.com"
      DNR #13: Test. Request: "imwlicious-domain.com"
      DNR #14: Test. Request: "imwlicious-domain.com"
      DNR #15: Test. Request: "imwlicious-domain.com"
      DNR #16: Test. Request: "imwlicious-domain.com"
      DNR #17: Test. Request: "imwlicious-domain.com"
      DNR #18: Test. Request: "imwlicious-domain.com"
      DNR #19: Test. Request: "imwlicious-domain.com"
      DNR #20: Test. Request: "imwlicious-domain.com"
      DNR #21: Test. Request: "imwlicious-domain.com"
      DNR #22: Test. Request: "imwlicious-domain.com"
      DNR #23: Test. Request: "imwlicious-domain.com"
      DNR #24: Test. Request: "imwlicious-domain.com"
      DNR #25: Test. Request: "imwlicious-domain.com"
      DNR #26: Test. Request: "imwlicious-domain.com"
      DNR #27: Test. Request: "imwlicious-domain.com"
      DNR #28: Test. Request: "imwlicious-domain.com"
      DNR #29: Test. Request: "imwlicious-domain.com"
      DNR #30: Test. Request: "imwlicious-domain.com"
      DNR #31: Test. Request: "imwlicious-domain.com"
      DNR #32: Test. Request: "imwlicious-domain.com"
      DNR #33: Test. Request: "imwlicious-domain.com"
      DNR #34: Test. Request: "imwlicious-domain.com"
      DNR #35: Test. Request: "imwlicious-domain.com"
      DNR #36: Test. Request: "imwlicious-domain.com"
      DNR #37: Test. Request: "imwlicious-domain.com"
      DNR #38: Test. Request: "imwlicious-domain.com"
      DNR #39: Test. Request: "imwlicious-domain.com"
      DNR #40: Test. Request: "imwlicious-domain.com"
      DNR #41: Test. Request: "imwlicious-domain.com"
      DNR #42: Test. Request: "imwlicious-domain.com"
      DNR #43: Test. Request: "imwlicious-domain.com"
      DNR #44: Test. Request: "imwlicious-domain.com"
      DNR #45: Test. Request: "imwlicious-domain.com"
      DNR #46: Test. Request: "imwlicious-domain.com"
      DNR #47: Test. Request: "imwlicious-domain.com"
      DNR #48: Test. Request: "imwlicious-domain.com"
      DNR #49: Test. Request: "imwlicious-domain.com"
      DNR #50: Test. Request: "imwlicious-domain.com"
      DNR #51: Test. Request: "imwlicious-domain.com"
      DNR #52: Test. Request: "imwlicious-domain.com"
      DNR #53: Test. Request: "imwlicious-domain.com"
      DNR #54: Test. Request: "imwlicious-domain.com"
      DNR #55: Test. Request: "imwlicious-domain.com"
      DNR #56: Test. Request: "imwlicious-domain.com"
      DNR #57: Test. Request: "imwlicious-domain.com"
      DNR #58: Test. Request: "imwlicious-domain.com"
      DNR #59: Test. Request: "imwlicious-domain.com"
      DNR #60: Test. Request: "imwlicious-domain.com"
      DNR #61: Test. Request: "imwlicious-domain.com"
      DNR #62: Test. Request: "imwlicious-domain.com"
      DNR #63: Test. Request: "imwlicious-domain.com"
      DNR #64: Test. Request: "imwlicious-domain.com"
      DNR #65: Test. Request: "imwlicious-domain.com"
      DNR #66: Test. Request: "imwlicious-domain.com"
      DNR #67: Test. Request: "imwlicious-domain.com"
      DNR #68: Test. Request: "imwlicious-domain.com"
      DNR #69: Test. Request: "imwlicious-domain.com"
      DNR #70: Test. Request: "imwlicious-domain.com"
      DNR #71: Test. Request: "imwlicious-domain.com"
      DNR #72: Test. Request: "imwlicious-domain.com"
      DNR #73: Test. Request: "imwlicious-domain.com"
      DNR #74: Test. Request: "imwlicious-domain.com"
      DNR #75: Test. Request: "imwlicious-domain.com"
      DNR #76: Test. Request: "imwlicious-domain.com"
      DNR #77: Test. Request: "imwlicious-domain.com"
      DNR #78: Test. Request: "imwlicious-domain.com"
      DNR #79: Test. Request: "imwlicious-domain.com"
      DNR #80: Test. Request: "imwlicious-domain.com"
      DNR #81: Test. Request: "imwlicious-domain.com"
      DNR #82: Test. Request: "imwlicious-domain.com"
      DNR #83: Test. Request: "imwlicious-domain.com"
      DNR #84: Test. Request: "imwlicious-domain.com"
      DNR #85: Test. Request: "imwlicious-domain.com"
      DNR #86: Test. Request: "imwlicious-domain.com"
      DNR #87: Test. Request: "imwlicious-domain.com"
      DNR #88: Test. Request: "imwlicious-domain.com"
      DNR #89: Test. Request: "imwlicious-domain.com"
      DNR #90: Test. Request: "imwlicious-domain.com"
      DNR #91: Test. Request: "imwlicious-domain.com"
      DNR #92: Test. Request: "imwlicious-domain.com"
      DNR #93: Test. Request: "imwlicious-domain.com"
      DNR #94: Test. Request: "imwlicious-domain.com"
      DNR #95: Test. Request: "imwlicious-domain.com"
      DNR #96: Test. Request: "imwlicious-domain.com"
      DNR #97: Test. Request: "imwlicious-domain.com"
      DNR #98: Test. Request: "imwlicious-domain.com"
      DNR #99: Test. Request: "imwlicious-domain.com"
      DNR #100: Test. Request: "imwlicious-domain.com"
      DNR #101: Test. Request: "imwlicious-domain.com"
      DNR #102: Test. Request: "imwlicious-domain.com"
      DNR #103: Test. Request: "imwlicious-domain.com"
      DNR #104: Test. Request: "imwlicious-domain.com"
      DNR #105: Test. Request: "imwlicious-domain.com"
      DNR #106: Test. Request: "imwlicious-domain.com"
      DNR #107: Test. Request: "imwlicious-domain.com"
      DNR #108: Test. Request: "imwlicious-domain.com"
      DNR #109: Test. Request: "imwlicious-domain.com"
      DNR #110: Test. Request: "imwlicious-domain.com"
      DNR #111: Test. Request: "imwlicious-domain.com"
      DNR #112: Test. Request: "imwlicious-domain.com"
      DNR #113: Test. Request: "imwlicious-domain.com"
      DNR #114: Test. Request: "imwlicious-domain.com"
      DNR #115: Test. Request: "imwlicious-domain.com"
      DNR #116: Test. Request: "imwlicious-domain.com"
      DNR #117: Test. Request: "imwlicious-domain.com"
      DNR #118: Test. Request: "imwlicious-domain.com"
      DNR #119: Test. Request: "imwlicious-domain.com"
      DNR #120: Test. Request: "imwlicious-domain.com"
      DNR #121: Test. Request: "imwlicious-domain.com"
      DNR #122: Test. Request: "imwlicious-domain.com"
      DNR #123: Test. Request: "imwlicious-domain.com"
      DNR #124: Test. Request: "imwlicious-domain.com"
      DNR #125: Test. Request: "imwlicious-domain.com"
      DNR #126: Test. Request: "imwlicious-domain.com"
      DNR #127: Test. Request: "imwlicious-domain.com"
      DNR #128: Test. Request: "imwlicious-domain.com"
      DNR #129: Test. Request: "imwlicious-domain.com"
      DNR #130: Test. Request: "imwlicious-domain.com"
      DNR #131: Test. Request: "imwlicious-domain.com"
      DNR #132: Test. Request: "imwlicious-domain.com"
      DNR #133: Test. Request: "imwlicious-domain.com"
      DNR #134: Test. Request: "imwlicious-domain.com"
      DNR #135: Test. Request: "imwlicious-domain.com"
      DNR #136: Test. Request: "imwlicious-domain.com"
      DNR #137: Test. Request: "imwlicious-domain.com"
      DNR #138: Test. Request: "imwlicious-domain.com"
      DNR #139: Test. Request: "imwlicious-domain.com"
      DNR #140: Test. Request: "imwlicious-domain.com"
      DNR #141: Test. Request: "imwlicious-domain.com"
      DNR #142: Test. Request: "imwlicious-domain.com"
      DNR #143: Test. Request: "imwlicious-domain.com"
      DNR #144: Test. Request: "imwlicious-domain.com"
      DNR #145: Test. Request: "imwlicious-domain.com"
      DNR #146: Test. Request: "imwlicious-domain.com
```

[illegible]

Pestess Monitor:jemotions.com							X
Total	Etheaded	Vides	FID	question	Parik		
Li002	Monifile	0011	Badwby1	06/22/03			
Li003	Monifile	0011	Badwby1	06/22/03			
Li002	Monifile	0011	Badwby1	06/22/03			
Li022	Monifile	0015	Badwby1	06/22/03			
Li012	Monifile	0012	Badwby1	06/22/03			
Li014	Monifile	0014	Badwby1	06/22/03			
Li012	Monifile	0012	Badwby1	06/22/03			
Li011	Monifile	0012	Badwby1	06/22/03			
Li012	Monifile	0012	Badwby1	06/22/03			
Li014	Monifile	0012	Badwby1	06/22/03			
Li001	Monifile	0013	Badwby1	06/22/03			
Li001	Monifile	0013	Badwby1	06/22/03			
Li011	Monifile	0015	Badwby1	06/22/03			
Li013	Monifile	0013	Badwby1	06/22/03			
Li001	Monifile	0012	Badwby1	06/22/03			
Li001	Monifile	0013	Badwby1	06/22/03			



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.