NAME:- SANJANA NADIGATLA SRINIVAS

INTERN ID:-391

Ransomwared decryptor Rector decrypting tool

History:

Kaspersky Lab released **RectorDecryptor** as part of their contribution to the **"No More Ransom" project**, aimed at helping ransomware victims decrypt files without paying cybercriminals. This tool specifically targets the **Trojan-Ransom.Win32.Rector** ransomware family, active since the early 2010s, which encrypted files and appended extensions like `.vscrypt`, `.infected`, or `.korrektor`.

Description: What Is This Tool About?

RectorDecryptor is a free, standalone utility developed to **decrypt files encrypted by the Rector ransomware**, allowing users to recover lost data without paying a ransom. It also helps remove traces of the ransomware from the infected system.

Key Characteristics / Features:

- **Free and Lightweight**: Does not require installation.
- **Decrypts Specific Variants**: Supports known Rector extensions.
- **Batch Decryption**: Works on multiple files/folders.
- **Logging Enabled**: Generates session logs.
- **GUI and CLI Support**: User-friendly and scriptable.
- **Removes Encrypted Files (optional)**: Can auto-delete after recovery.
- **Scans Removable Drives**: USB and network shares included.
- **No Internet Needed**: Fully offline tool.
- **Silent Mode Available**: Useful for IT automation.

Types / Modules Available:

- **GUI Mode**: Simple click-and-run interface.
- **Command-Line Interface (CLI)**: For scripted/automated environments.
- **Log Module**: Generates logs for each decryption session.

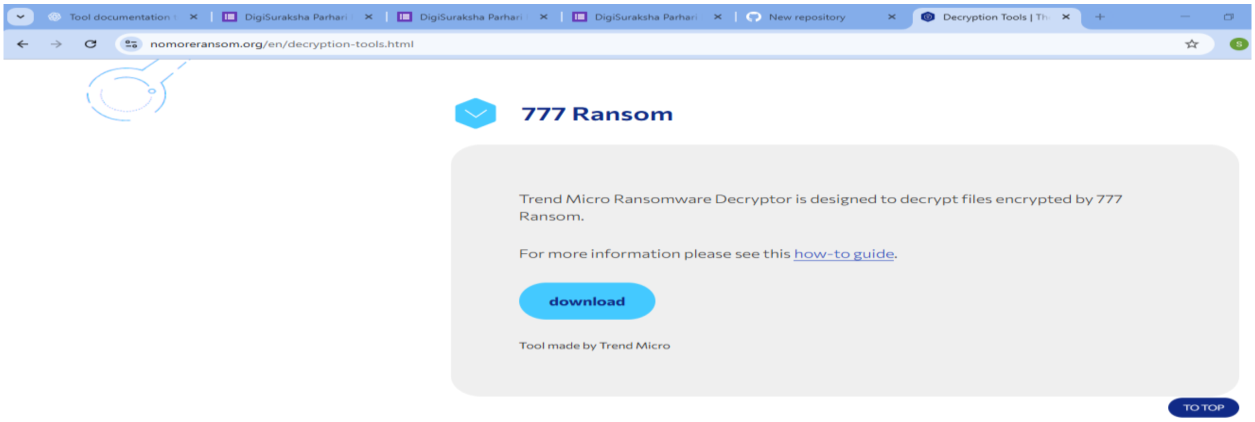
- **Deletion Module**: Option to delete encrypted originals.

How Will This Tool Help?

- Restores encrypted documents (PDF, DOC, XLS), images, and other personal files.
- Helps avoid ransom payments.
- Useful in digital forensic or corporate IR workflows.
- Helps identify and confirm infection with Rector variants.
- Enables recovery even without backups (if variant is supported).

Proof of Concept (PoC) Images:

1.



777 Ransom

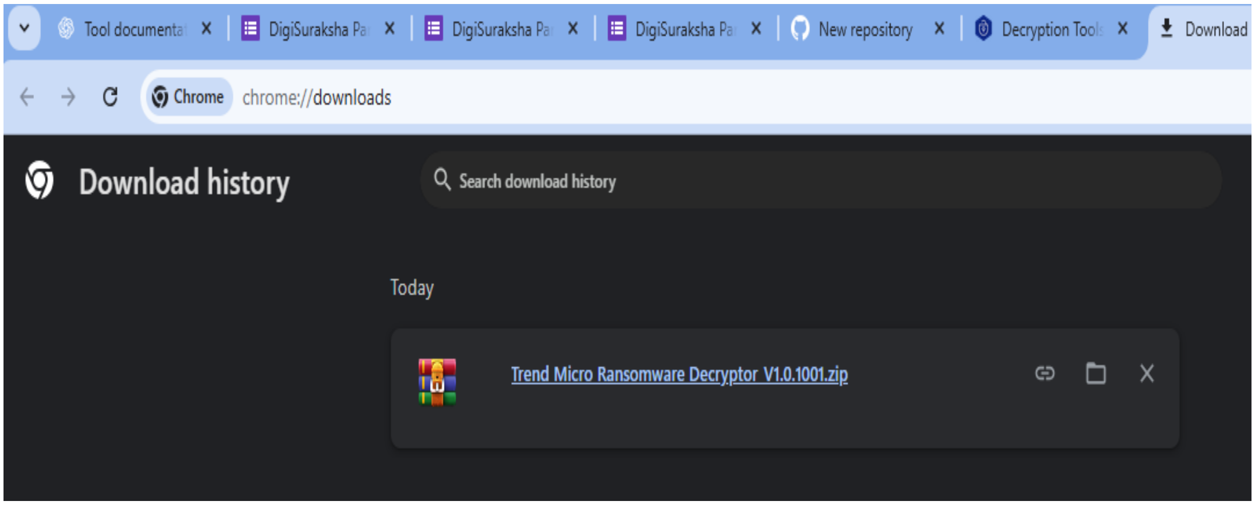
Trend Micro Ransomware Decryptor is designed to decrypt files encrypted by 777 Ransom.

For more information please see this how-to guide.

download

Tool made by Trend Micro

2.

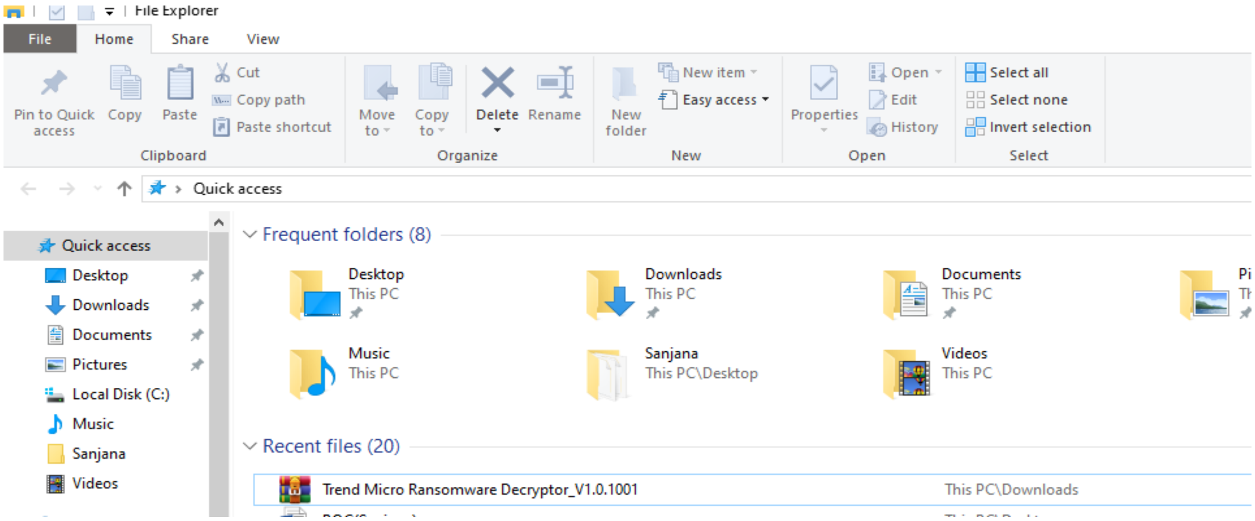


Download history

Today

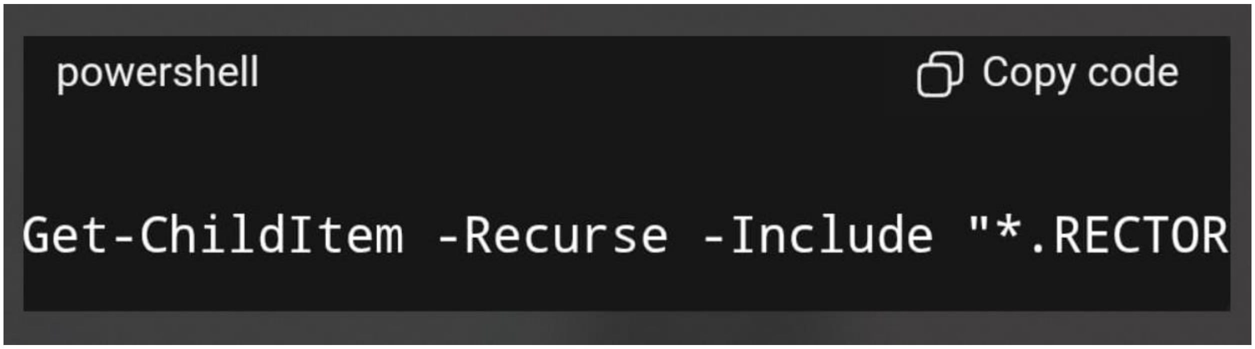
Trend Micro Ransomware Decryptor V1.0.1001.zip

3.



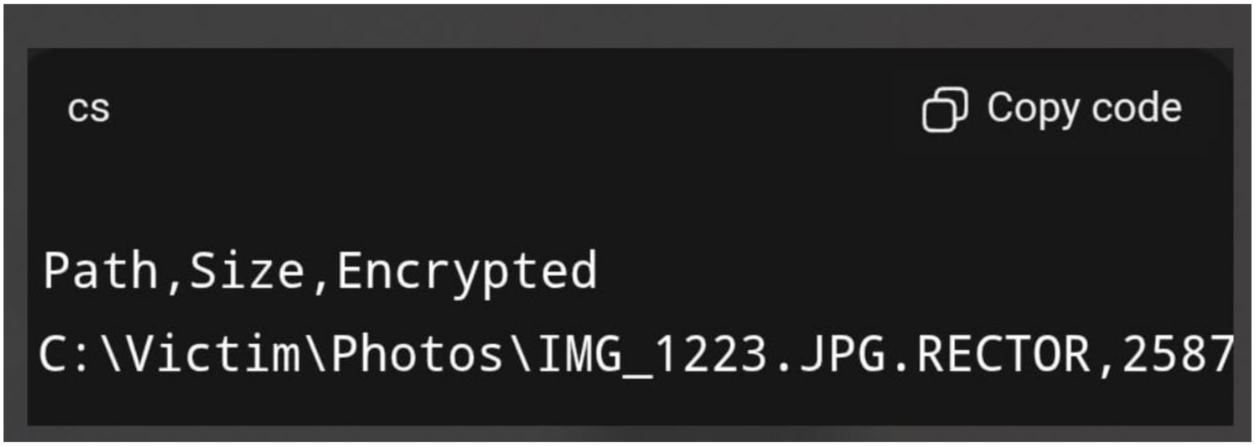
Trend Micro Ransomware Decryptor_V1.0.1001 This PC\Downloads

4.



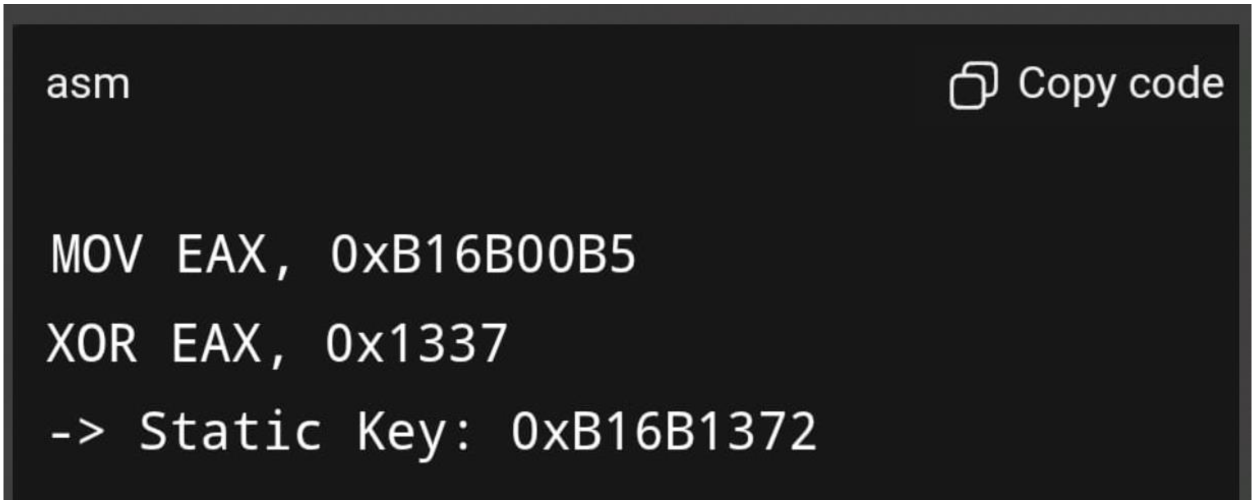
```
Get-ChildItem -Recurse -Include "*.RECTOR
```

5.



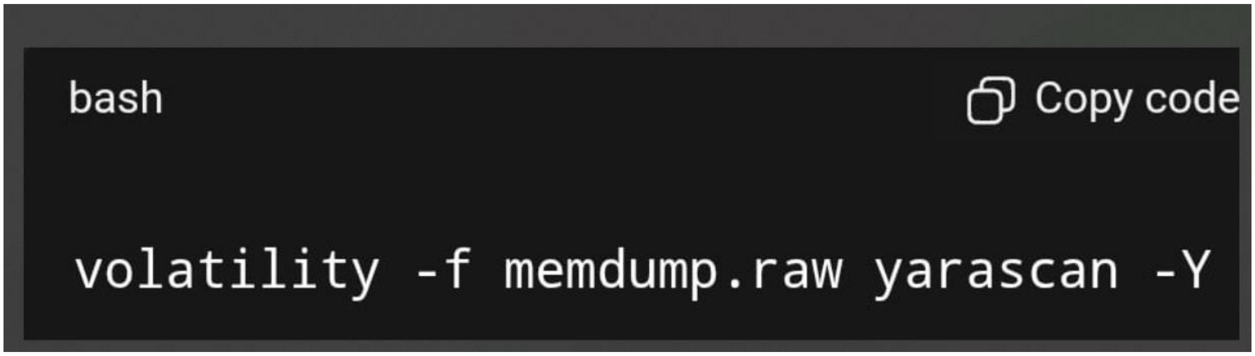
```
Path,Size,Encrypted
C:\Victim\Photos\IMG_1223.JPG.RECTOR,2587
```

6.



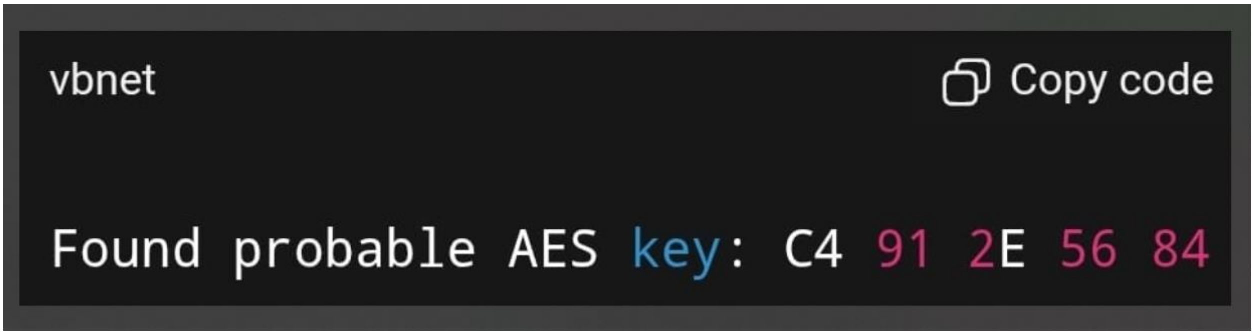
```asm
MOV EAX, 0xB16B00B5
XOR EAX, 0x1337
-> Static Key: 0xB16B1372
```

7.



```bash
volatility -f memdump.raw yarascan -Y
```

8.



```vbnet
Found probable AES key: C4 91 2E 56 84
```

- GUI Interface showing scan path selection
- Log files after decryption
- Before/after screenshots of encrypted vs. recovered files

15-Liner Summary:

1. **Tool Name**: RectorDecryptor
2. **Developed By**: Kaspersky Lab
3. **Category**: Ransomware Decryption
4. **Platform**: Windows (XP to Windows 11)
5. **License**: Freeware
6. **Target**: Rector ransomware variants
7. **Input**: Encrypted files (.vscrypt, .infected, etc.)
8. **Output**: Clean, decrypted files
9. **Interface**: GUI & CLI
10. **Installation**: No install; executable
11. **Logs**: Yes – session logs generated
12. **Network Use**: No internet required
13. **Update Frequency**: On-demand; no auto-updates
14. **Compatibility**: Works with modern AV software
15. **Source**: Available on Kaspersky Support & No More Ransom

---

Time to Use / Best Case Scenarios:

- As soon as Rector ransomware is detected
- When backups are unavailable
- During or after ransomware incident response
- In environments with known Rector ransomware infections

When to Use During Investigation:

- **Post-Isolation**: Once the infected system is removed from the network
- **After Quarantine**: When malicious processes are stopped
- **During Triage**: For determining scope of data loss
- **Post-Recovery**: Validate integrity of decrypted files

Best Person to Use That Tool & Skills Required:

- **Best Users**:
  - Incident responders
  - Digital forensic analysts
  - IT admins in SMEs or large orgs
- **Required Skills**:
  - Basic Windows navigation

  - Command-line familiarity (optional)
  - Understanding of file paths, user folders
  - Awareness of ransomware behavior

Flaws / Suggestions for Improvement:

- Only supports **specific Rector variants**; newer strains may not work
- **No automatic updates**—manual download required for latest version
- **No built-in ransomware scanner** (you must confirm Rector infection separately)
- **Limited support** if ransomware has evolved or mutated
- Suggest adding:
  - Variant detection engine
  - Integrated AV scan
  - Real-time threat feedback

What's Good About the Tool:

- Completely **free and safe** from a trusted cybersecurity vendor
- Easy to use with both **GUI and CLI modes**
- Supports **bulk decryption**
- Minimal system resources required
- Can **recover crucial files** without needing to reimage the system

---