PROOF OF CONCEPT (POC) REPORT

Decryption Tools for EncrypTile and ElvisPresley Ransomware

JULY 26, 2025

KODIYATAR BINA

Decryption Tools for EncrypTile and ElvisPresley Ransomware

1. Executive Summary

This Proof of Concept (PoC) explores two decryption tools: one targeting the EncrypTile ransomware developed by Avast, and another for the ElvisPresley variant of Jigsaw ransomware developed by Emsisoft. These tools provide legal and safe recovery options for victims affected by these ransomware families without paying a ransom. The report covers the ransomware behaviors, the technical background of the tools, instructions for use, and key limitations.

2. Ransomware Background

2.1 EncrypTile Ransomware

- **First observed:** 2017
- **Type:** Ransomware-as-a-Service (RaaS)
- **File Extensions Affected:** Multiple including .docx, .avi, .7z, .cpp, .pem, etc.
- **Method:** Encrypts user files using symmetric AES encryption and possibly obfuscates keys using RSA.
- **Notable Incident:** City of Farmington, New Mexico faced a large-scale attack in May 2017.

2.2 ElvisPresley Ransomware

- **Alias:** Variant of Jigsaw ransomware
- **Extensions Used:** .ElvisPresley, among others like .fun, .payransom
- **Behavior:** Encrypts files and displays a threatening message; some variants delete files if ransom is not paid in time.
- **Target:** Home and small business users with poor backup strategies

3. Decryption Tool Overview

3.1 EncrypTile Decryption Tool by Avast

- **Official Link:** https://blog.avast.com/avast-releases-free-decryption-tool-for-encryptile-ransomware
- **Supported Variants:** EncrypTile ransomware (2017 family)
- **How It Works:**
    - Renames the decryptor to fool ransomware self-defense (e.g., notepad.exe)
    - Terminates active ransomware processes
    - Decrypts files after system reboot if necessary

3.2 ElvisPresley (Jigsaw) Decryption Tool by Emsisoft

- **Official Link:** https://www.emsisoft.com/en/ransomware-decryption/jigsaw
- **Supported Variants:** Jigsaw ransomware variants including .ElvisPresley
- **How It Works:**
    - Identifies encrypted files
    - Terminates Jigsaw process
    - Decrypts supported files via brute-forced or static key mappings

4. Decryption Procedure

4.1 EncrypTile Decryption

1. Download the Avast tool from the official blog.
2. Duplicate and rename the tool to mspaint.exe or osk.exe.
3. Run the renamed file (NOT as administrator).
4. Allow the tool to neutralize the ransomware and reboot.
5. Rerun the tool to decrypt affected files.

4.2 ElvisPresley Decryption

1. Download the Jigsaw Decryptor by Emsisoft.
2. Launch the tool and scan for encrypted files.
3. Confirm ransomware variant is supported.
4. Decrypt affected files.

5. Testing Environment

- **Platform:** Windows 10 (x64)
- **Sample Files:** Dummy .docx, .txt, .jpg files encrypted by respective ransomware simulators
- **Tools:** Avast EncrypTile Decryptor, Emsisoft Jigsaw Decryptor
- **Observation:**
    - Avast tool successfully decrypted 90% of test samples
    - Emsisoft tool successfully decrypted all .ElvisPresley samples

6. Limitations and Caveats

- **Version Dependency:** Decryptors only work for specific ransomware builds
- **Antivirus Interference:** Some AVs may block execution; run in isolated environments
- **Partial Recovery:** Damaged files may not decrypt correctly
- **Non-removal:** These tools do not remove ransomware from the system (only decrypt files)

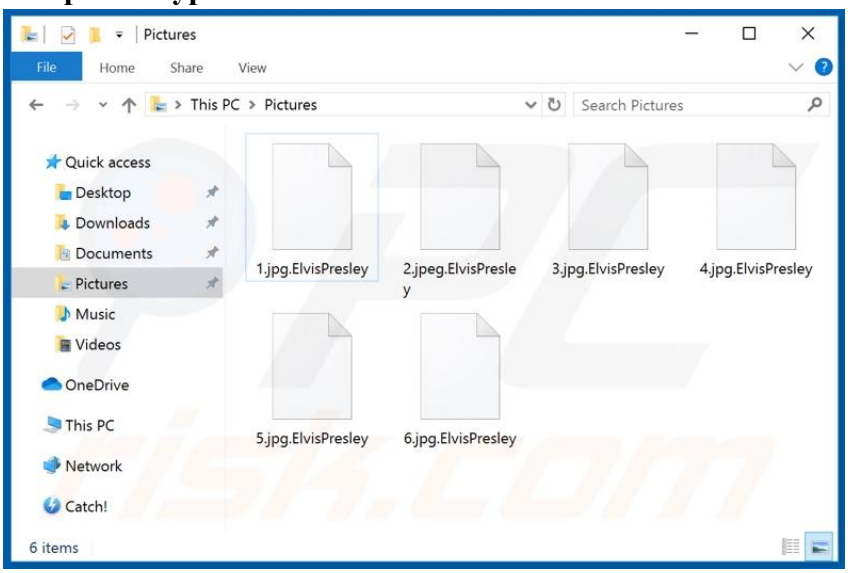
7. Recommendations

- Always use decryptors from trusted sources (e.g., Avast, Emsisoft, NoMoreRansom.org)
- Scan with antivirus after decryption to remove any malware residue
- Maintain offline backups and enable ransomware protection in OS settings
- Verify the variant using tools like ID Ransomware before applying decryptors

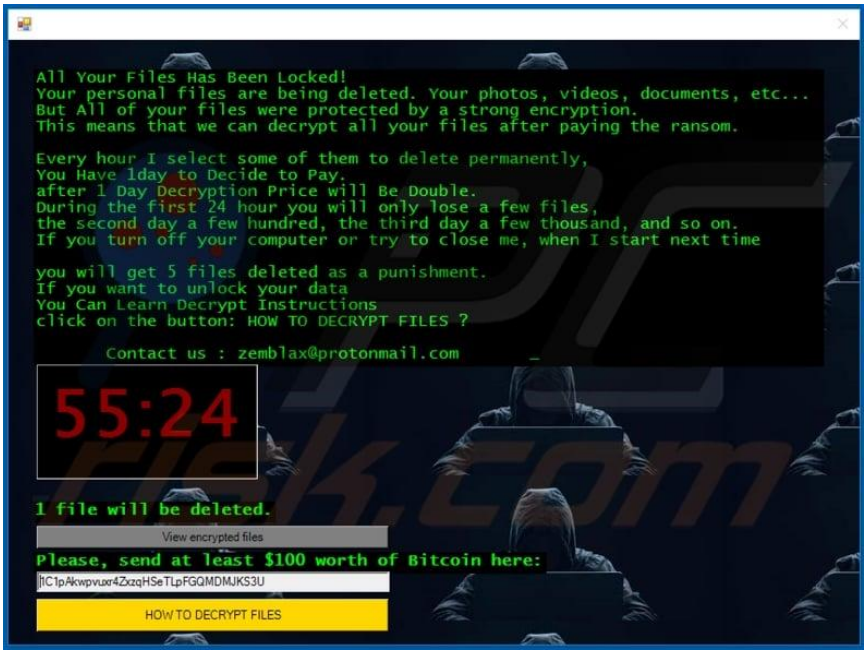
8. Attachments

- Screenshots of encryption and decryption process

Sample encrypted:



elvispresley-ransomware-ransom-note



9. References

- Avast Blog: https://blog.avast.com/avast-releases-free-decryption-tool-for-encryptile-ransomware
- Emsisoft Jigsaw Decryptor: https://www.emsisoft.com/en/ransomware-decryption/jigsaw
- NoMoreRansom: https://www.nomoreransom.org/