Ransomware Decryption Tool Instruction Manual

- LooCipher -

2022. 02

KISA Korea Internet & Security Agency

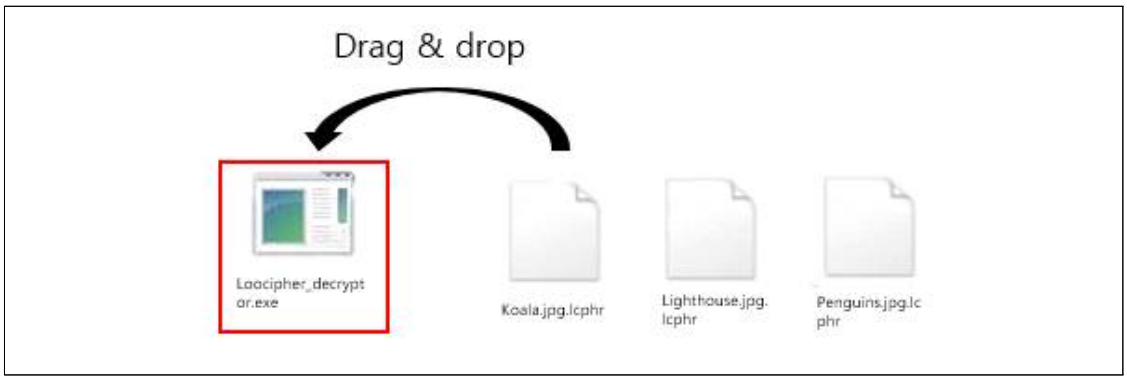
Caution : Delete any malicious code from the system first. Otherwise, the computer can be infected again after recovery.

KISA is not responsible for any issues caused by misuse.

How to Use the Decryption Tool

1. **Drag and drop the infected file on the decryption tool(LooCipher_decryptor.exe) icon.**

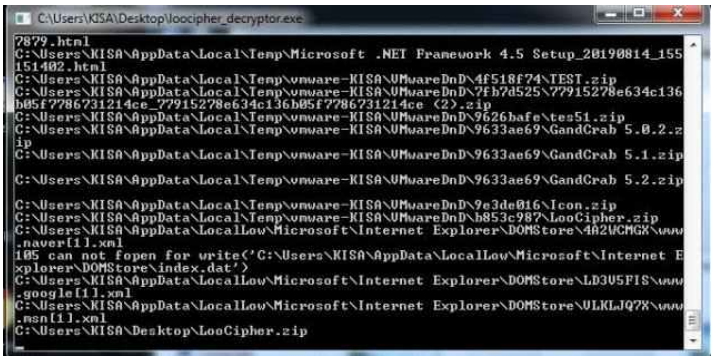
   ※ You can only drag and drop the infected files with file extension of jpeg, jpg, pdf, docx, pptx, xlsx or png.



2. **The decryption tool code is automatically executed in the CMD for decoding.**

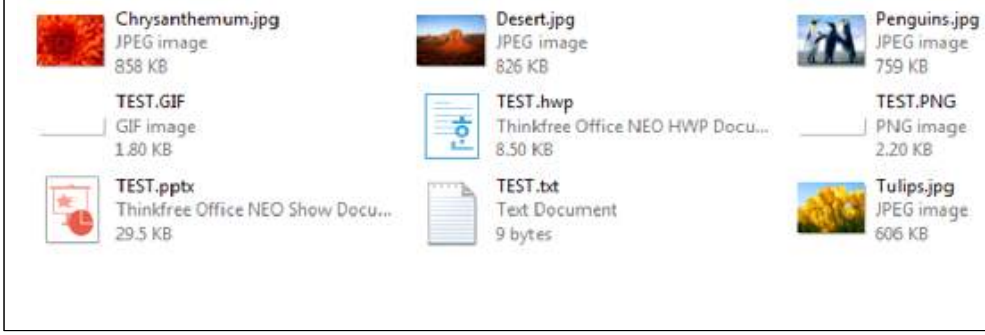
- When the decryption tool is executed, it analyzes the file to recover the key. Then it generates a file named 'key.txt' to save the recovered key and uses this file as a reference.

Decryption Tool Execution Status



3. When execution is complete, you can check the recovered files.

Recovered Files



What is the LooCipher Ransomware?

It is a ransomware that emerged in second-half of 2019, and it was mostly distributed through spam emails. It encrypts the file and adds the '.lcphr' extension.

If you wish to see more detailed information on LooCipher ransomware, refer to the cryptographic analysis report below.

※ LooCipher ransomware cryptographic analysis report download URL
→ https://seed.kisa.or.kr/kisa/Board/64/detalView.do

LooCipher Ransomware Decryption Tool Instruction Manual

February 2022

Publisher KISA Korea Internet & Security Agency