Ransomware Decryption Tool User Manual

- Magniber -

2019. 9

Cryptography & Electronic Signature Team

KOREA INTERNET & SECURITY AGENCY

Warning : Make sure you remove the malware from your system first, otherwise it will repeatedly lock your system or encrypt files.

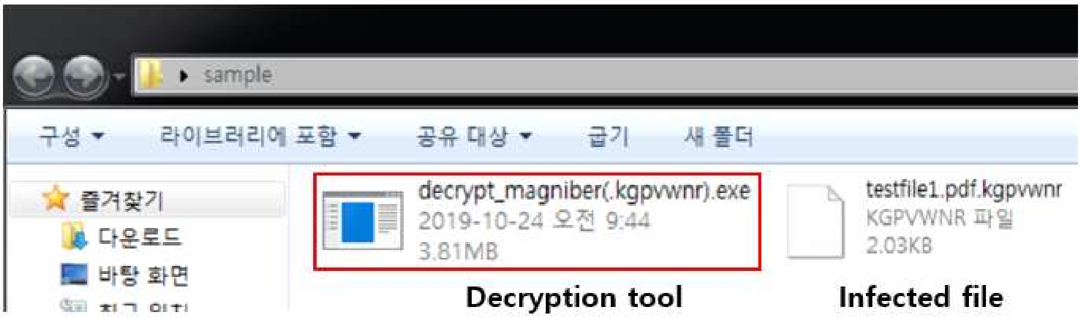
We are not responsible for any problems caused by misuse.

- This decryption tool decrypt the infected files of the Magniber Ransomware variant(file extension : .kgpvwnr)

Decryption tool Usage

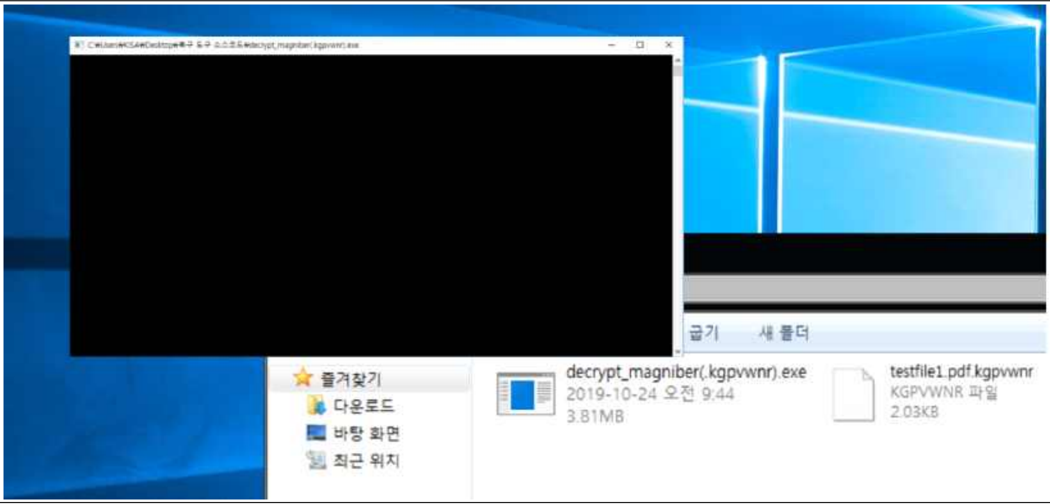
1. Double-click the decryption tool(decrypt_magniber(.kgpvwnr).exe) to execute.

Magniber decryption tool and infected file



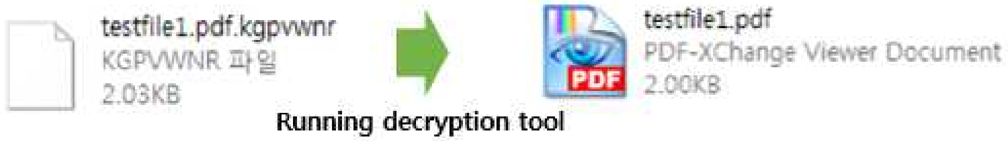
2. Automatically detect and decrypt infected files within the syste m when the decrypt tool is run.

Running decryption tool screen



3. Once the execution is complete, you can check that the file has been recovered normally.

fully decrypted infected files



testfile1.pdf.kgpvwnr
KGPVWNR 파일
2.03KB

testfile1.pdf
PDF-XChange Viewer Document
2.00KB

3. Not all variants of Magniber Ransomware infection files are resotred. It is only decryptable if infected with the .kgpvwnr extension of Magniber Ransomware, and you need to be very careful about using the decryption tools. (Decryption tools do not infect normal files.)

What is Magniber Ransomware?

From around October 5, 2017, it attacked the Korean-speaking Windows operating system. Magniber ransomware is distributed through the Magnitude Exploit Kit. Encrypts the file and adds an '.kgpvwnr' extension.

For more information, please refer to the analysis report below:
※ Magniber ransomware analysis report download URL :
https://seed.kisa.or.kr/kisa/Board/48/detalView.do

Attached manual is intended solely for the Korea Internet & Security Agency and may contain information that is privileged, confidential or otherwise protected under applicable law. Any unauthorized dissemination, distribution, copying or use of the information contained in this communication is strictly prohibited.

Ransomware decryption tool user manual

2019. 9

Publisher KISA KOREA INTERNET & SECURITY AGENCY