랜섬웨어 복구도구 사용 매뉴얼

- LooCipher -

2021. 08

차세대암호융합팀

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

주의 : 먼저 시스템에서 악성코드를 삭제하시기 바랍니다. 그렇지 않으면 감염파일이 복구 되더라도 다시 감염될 수 있습니다.
오사용으로 인한 문제 발생시 책임지지 않습니다.

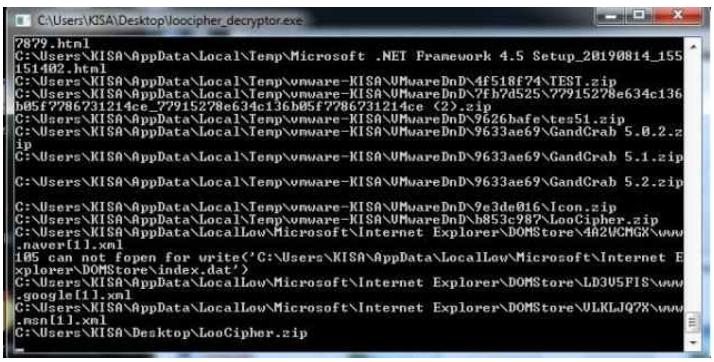
복구도구 사용 방법

1. 복구도구(LooCipher_decryptor.exe) 아이콘에 감염된 파일을 드래그 앤 드롭한다.
   ※ 감염된 파일의 원본 파일 확장자가 jpeg, jpg, pdf, docx, pptx, xlsx, png인 경우에만 드래그 앤 드롭 가능

LooCipher 복구도구 실행파일

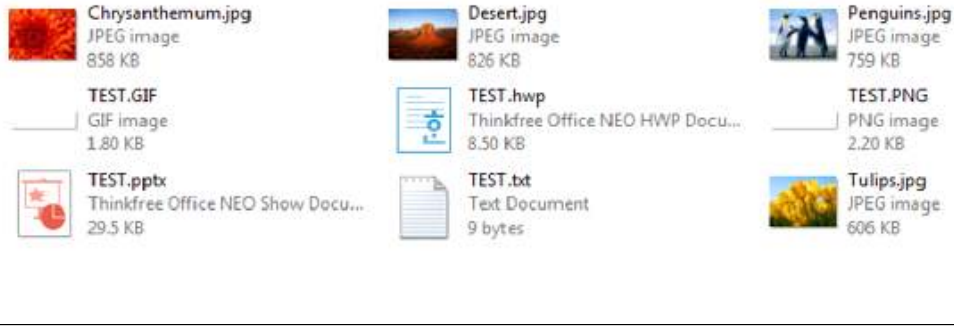
2. CMD창에서 복구도구 코드가 수행되어 자동으로 복호화가 진행된다.
   – 복구도구가 실행되면 암호화된 파일을 분석하여 키를 복구한다. 그리고, 'key.txt' 이름의 파일을 생성해 복구한 키를 저장하고 이 파일을 참조하여 사용한다.

실행 중인 복구도구



3. 실행이 완료되면 파일들이 정상적으로 복구된 것을 확인할 수 있다.

복구 완료된 파일



LooCipher 랜섬웨어란

2019년 하반기 등장한 랜섬웨어로 주로 스팸메일을 통해 유포되었다. 파일을 암호화하여 '.lcphr' 확장자를 추가시킨다.

LooCipher 랜섬웨어의 자세한 정보를 확인하고자 하는 경우 아래의 분석 보고서를 참고해주시기 바랍니다.

※ LooCipher 랜섬웨어 분석 보고서 다운로드 URL :

https://seed.kisa.or.kr/kisa/Board/64/detalView.do

랜섬웨어 복구도구 사용 매뉴얼

2021년 8월

발행처 KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY