랜섬웨어 복구도구 사용 매뉴얼

- 매그니베르 -

2019. 08

차세대암호인증팀

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

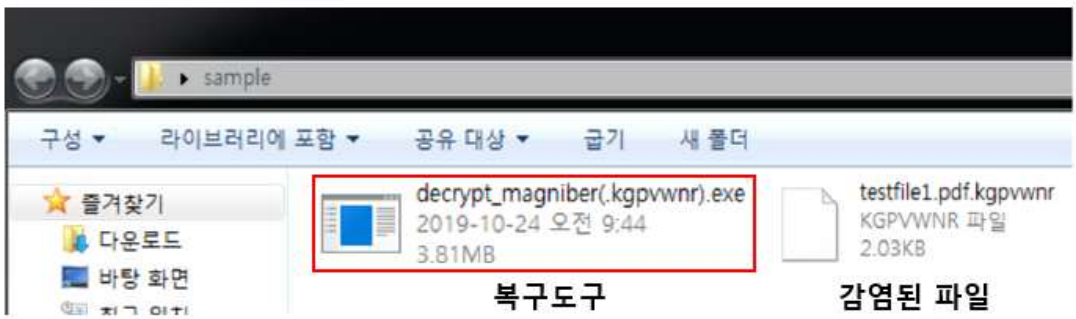
주의 : 먼저 시스템에서 악성코드를 삭제하시기 바랍니다. 그렇지 않으면 감염파일이 복구 되더라도 다시 감염될 수 있습니다.
오사용으로 인한 문제 발생시 책임지지 않습니다.

- 본 복구 도구는 매그니베르 랜섬웨어 변종의(감염 후 파일 확장자 : .kgpvwnr) 감염 파일을 복구합니다.

복구 도구 사용 방법

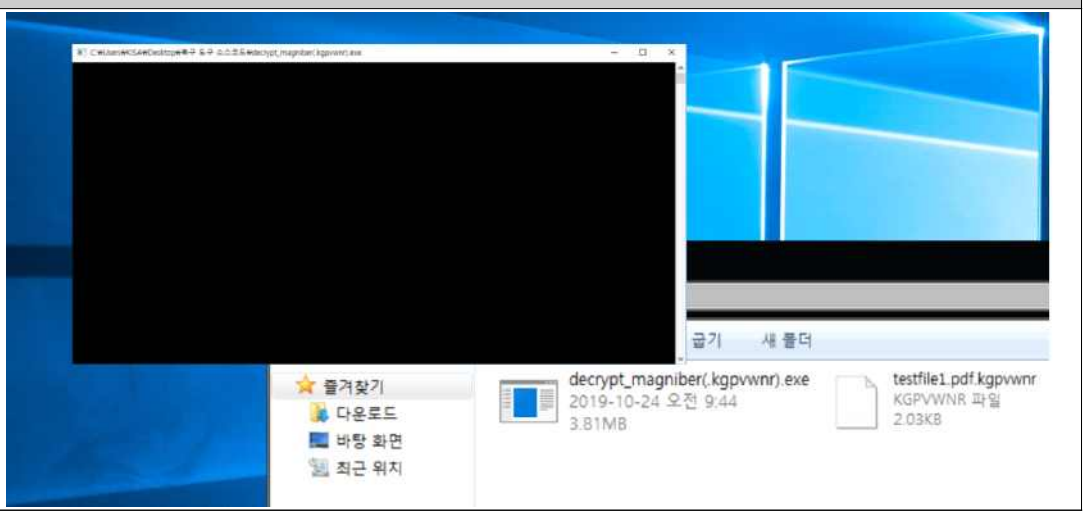
1. 복구도구(decrypt_magniber(.kgpvwnr).exe)를 더블클릭하여 실행한다.

매그니베르 복구도구와 감염된 파일



2. 복구도구를 실행하면 자동으로 시스템 내의 감염파일을 검색하고 복구한다.

실행 중인 복구도구



3. 실행이 완료 되면 파일들이 정상적으로 복구된 것을 확인할 수 있다.

복호화 완료된 감염 파일 모습

복구 도구 실행 후

4. 모든 변종의 매그니베르 랜섬웨어 감염파일을 복구하는 것이 아닙니다. 매그니베르 랜섬웨어 중 .kgpvwnr 확장자로 감염된 경우에만 복구 가능하니 복구도구를 사용하는데 매우 주의가 필요합니다. (일반 정상파일을 암호화 하지 않습니다.)

매그니베르 랜섬웨어란

2017년 10월 15일경부터 한국어를 사용하는 윈도우 운영체제를 공격한 하였다. Magnitude 익스플로잇 킷을 통해 유포되었으며, 파일 암호화 후 '.kgpvwnr' 확장명이 추가되고 주요 정보를 암호화시킨다.

매그니베르의 자세한 정보를 원하시면 아래의 분석보고서를 참고해주시기 바랍니다.

※ Magniber 랜섬웨어 분석 보고서 다운로드 URL :
https://seed.kisa.or.kr/kisa/Board/48/detalView.do

랜섬웨어 복구도구 사용 매뉴얼

2019년 8월

발행처 KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY