랜섬웨어 복구도구 사용 매뉴얼

- Ragnar -

2022. 05

차세대암호융합팀

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

복구도구 사용 방법

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

1. 복구 준비

Ragnar 랜섬웨어 복구도구를 사용하려면 **감염된 파일과 감염된 파일의 원본 파일 1쌍이 필요**하다. 감염된 PC에 설치된 프로그램과 동일한 버전을 다른 PC에 설치하여 원본 파일을 획득할 수 있다. 보통 '.exe' 형태로 배포되는 프로그램을 설치하면 'Program Files', 'Program Files(x86)' 등의 설치 경로에 '.zip', '.jar' 형태의 압축파일, '.jpeg', '.png' 형태의 사진 파일 등 다양한 형태의 파일이 생성된다. 해당 파일을 감염된 파일과 비교하는 과정을 반복하면 원본 파일을 획득할 수 있다.

또한, 이메일을 통해 송·수신한 파일, USB 저장장치에 있는 파일, 클라우드 스토리지에 저장된 파일을 감염된 파일과 비교하여 원본 파일을 획득하는 방법도 있다.

원활한 복구를 위해 필요한 파일 1쌍의 크기는 각각 **10MB 이상**이어야 한다. 그리고 서로의 파일 이름과 파일 버전이 같아야 한다.

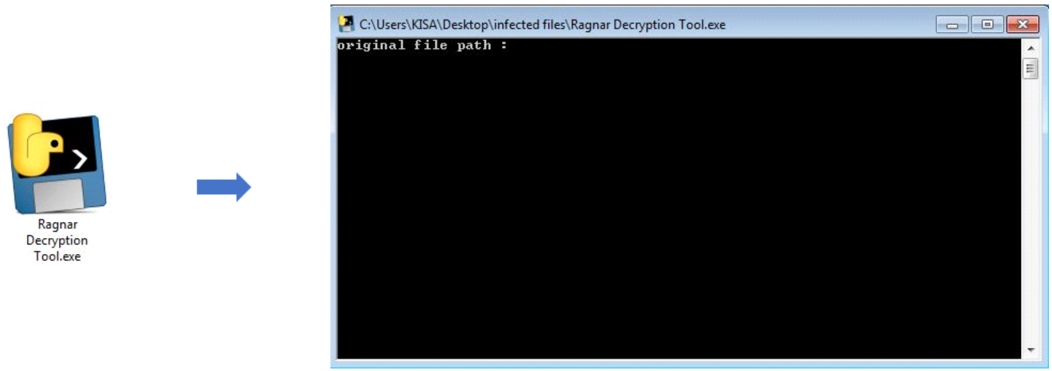
Ragnar 랜섬웨어는 특정 폴더, 파일, 확장자를 제외하고 암호화를 수행한다. [표 1]에 해당되는 경우 감염된 파일이 존재하지 않으므로, 복구에 필요한 파일 1쌍을 준비할 때 주의해야 한다.

제외 폴더	Windows Google Mozilla	Windows.old Opera Mozilla Firefox	Tor browser Opera Software ProgramData	Internet Explorer $Recycle.Bin All Users
제외 파일	autorun.inf desktop.ini ntuser.ini	boot.ini ntldr thumbs.db	bootfont.bin ntuser.dat 랜섬노트	bootsect.bak ntuser.dat.log
제외 확장자	.db .dll	.msi .exe	.sys .lnk	.drv

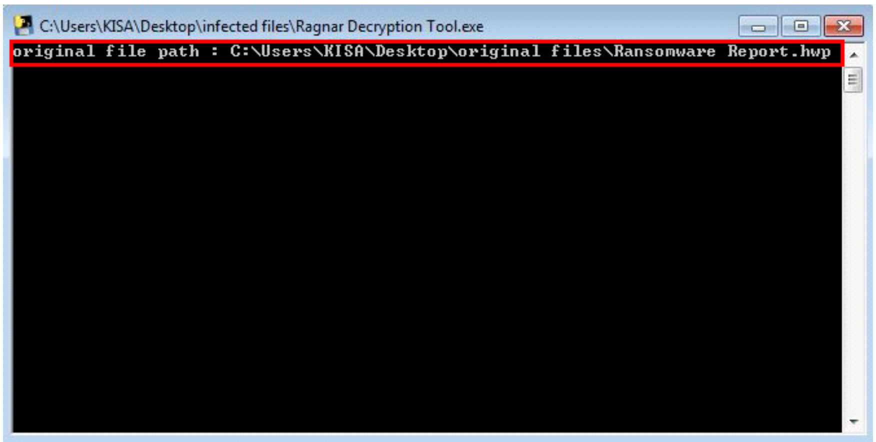
< 표 1 > 암호화 제외 대상 목록

2. 복구 수행

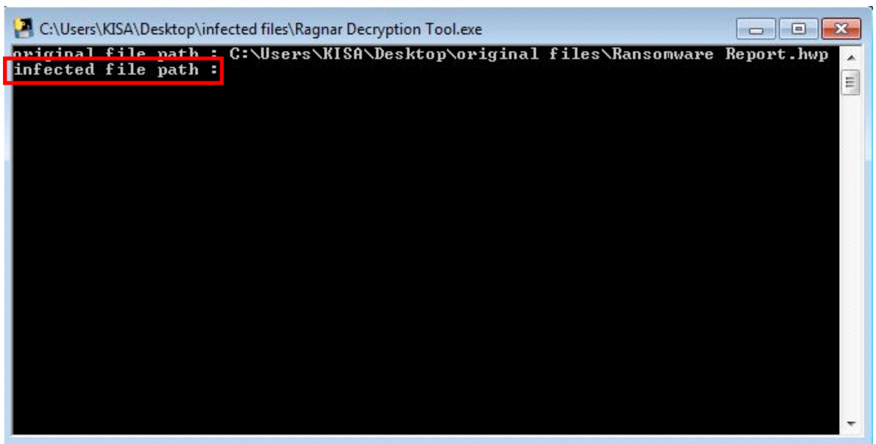
 Ragnar 랜섬웨어 복구도구(Ragnar Decryption Tool.exe)를 관리자 권한으로 실행하면 감염된 파일의 원본 파일이 위치한 경로를 입력하는 창이 나타난다.



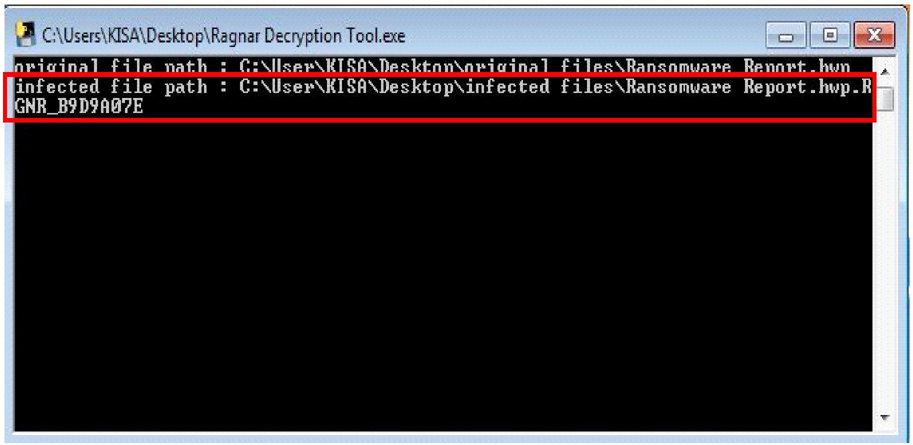
 원본 파일의 이름과 확장자를 포함한 경로를 입력한 후 Enter 키를 입력한다.



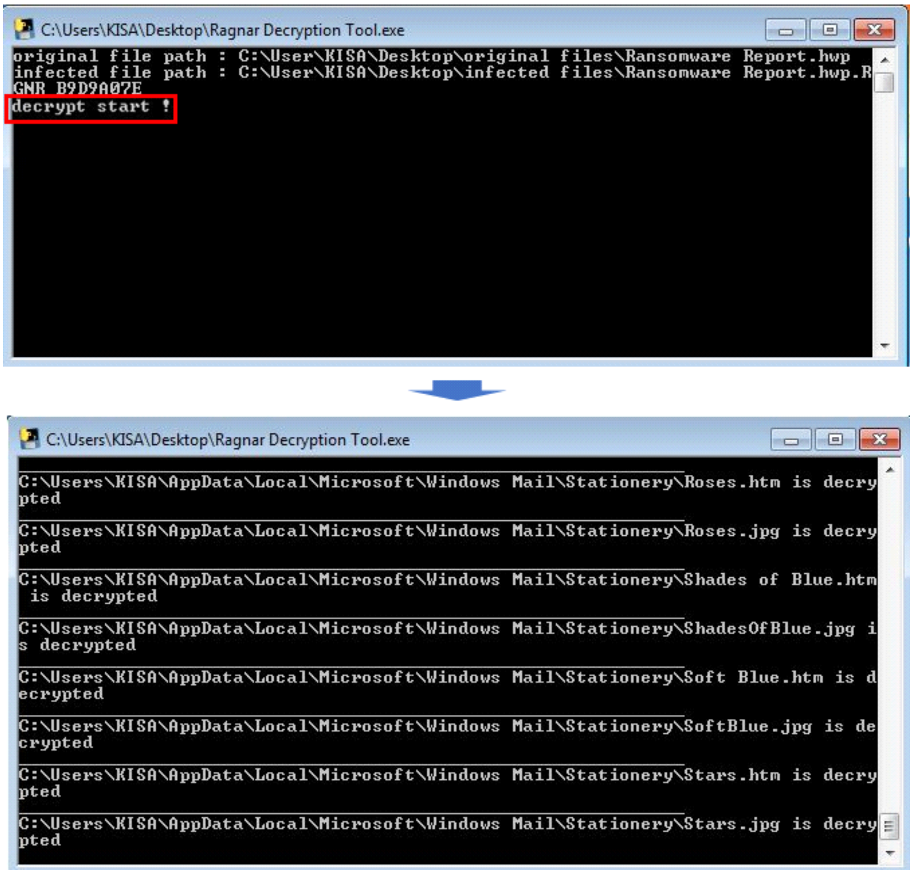
 감염된 파일이 위치한 경로를 입력하는 창이 나타난다.



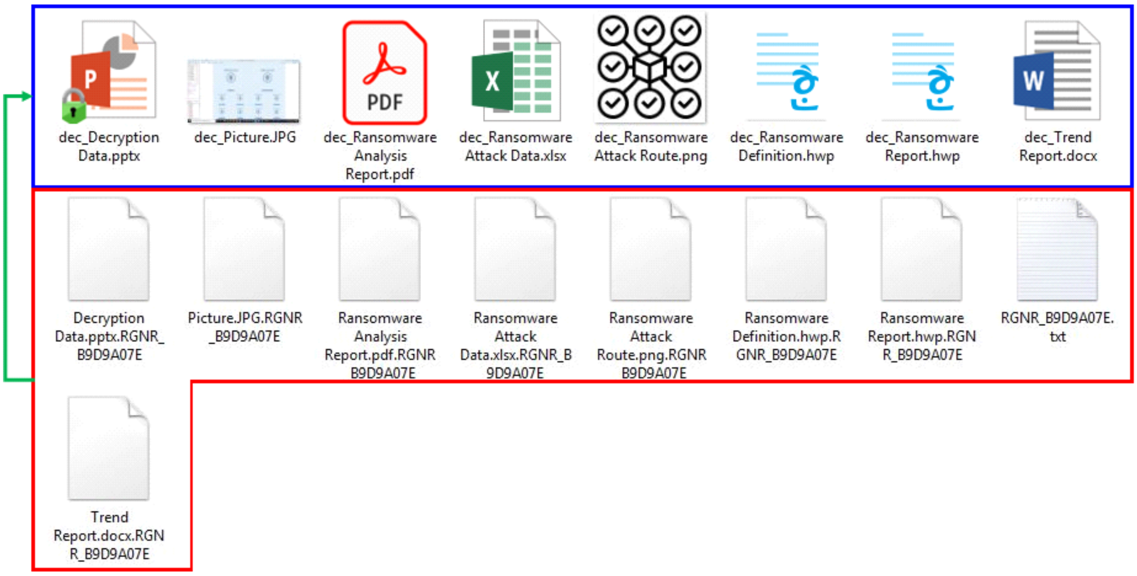
감염된 파일의 이름과 확장자를 포함한 경로를 입력한 후 Enter 키를 입력한다. 참고로 Ragnar 랜섬웨어는 감염된 파일의 확장자 뒤에 'RGNR_(랜덤한 8자리 문자열)' 확장자를 추가하므로, 경로 입력 시 추가된 확장자까지 정확히 입력해야 한다.



원본 파일과 감염된 파일의 이름과 확장자를 포함한 경로를 모두 입력하면 복구도구는 해당 파일을 이용하여 암호키 복구에 필요한 값을 추출한다. 암호키 복구가 완료되면 감염된 파일의 복구가 자동으로 수행된다.



복구된 파일은 감염된 파일이 위치한 경로마다 생성된다. 복구된 파일의 이름 앞에 ‘dec_’라는 문자열이 추가되며, 해당 파일을 열어보면 정상적으로 실행되는 것을 확인할 수 있다.



Ragnar 랜섬웨어란?

Ragnar 랜섬웨어는 주로 기업들을 대상으로 공격하는 랜섬웨어이다. 해당 랜섬웨어는 스트림 암호를 사용하여 데이터를 암호화하며, 데이터 복구를 위한 조건으로 감염자에게 많은 금액을 요구한다. 자세한 내용은 분석 보고서에서 확인할 수 있다.

※ Ragnar 랜섬웨어 분석 보고서 다운로드 URL
→ https://seed.kisa.or.kr/kisa/Board/101/detailView.do

Ragnar 랜섬웨어 복구도구 사용 매뉴얼

2022년 5월

발행처 KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY