



랜섬웨어 복구도구 사용 매뉴얼

- 심플락커 -

2019. 08



차세대암호인증팀

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

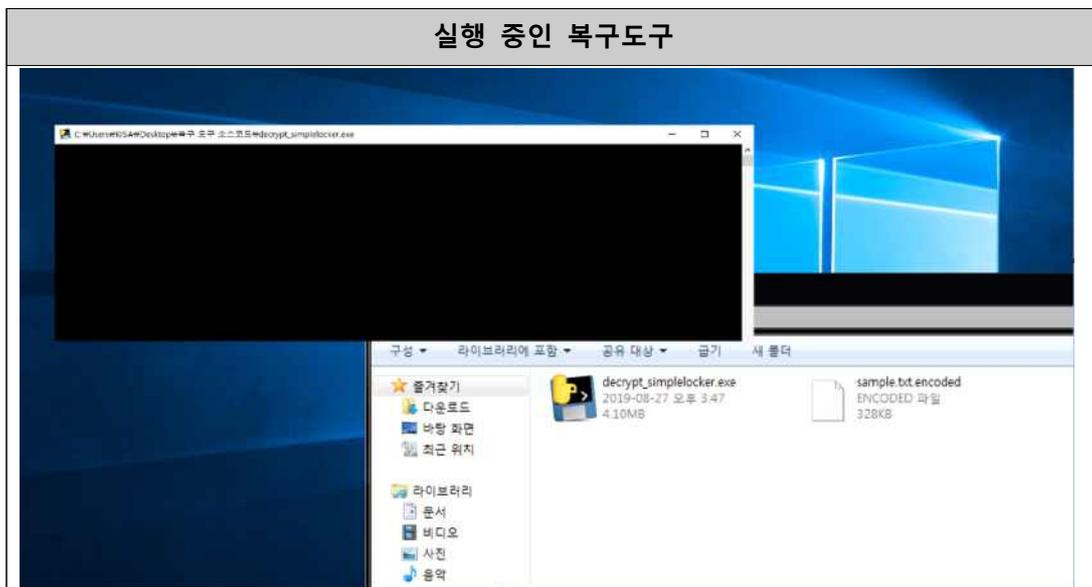
- 본 복구 도구는 심플락커(Simplelocker) 랜섬웨어 변종의(감염 후 확장자 : .encoded) 감염 파일을 복구합니다.

복구 도구 사용 방법

1. 모바일에서 PC로 감염 파일들을 복사한다. 복구도구(decrypt_simplelocker.exe)를 더블클릭하여 실행한다.



2. 복구도구를 실행하면 자동으로 시스템 내의 감염파일을 검색하고 복구한다.



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



심플라커란?

SimpleLocker 랜섬웨어는 2015~2016년에 사이에 유포된 최초의 안드로이드 모바일 대상 랜섬웨어이다. 동유럽, 미주 지역을 기반으로 활동하였고, 2016년 후반까지 약 15만 회 정도 다운로드된 것으로 파악된다.¹⁾ SimpleLocker 랜섬웨어는 스마트폰의 파일을 암호화하고, 암호화된 파일을 복구하기 위한 비용을 피해자에게 요구한다.

심플라커의 자세한 정보를 원하시면 아래의 분석보고서를 참고해주시기 바랍니다.

※ SimpleLocker 랜섬웨어 분석 보고서 다운로드 URL :

<https://seed.kisa.or.kr/kisa/Board/49/detailView.do>

본 매뉴얼의 내용에 대해 한국인터넷진흥원의 허가 없이 무단전재 및 복사를 금하며, 위반시 저작권법에 저촉될 수 있습니다.

랜섬웨어 복구도구 사용 매뉴얼

2019년 8월

발행처

 **한국인터넷진흥원**
KOREA INTERNET & SECURITY AGENCY