Ransomware 뿌시기

개념부터 보안, 개발까지

INDEX

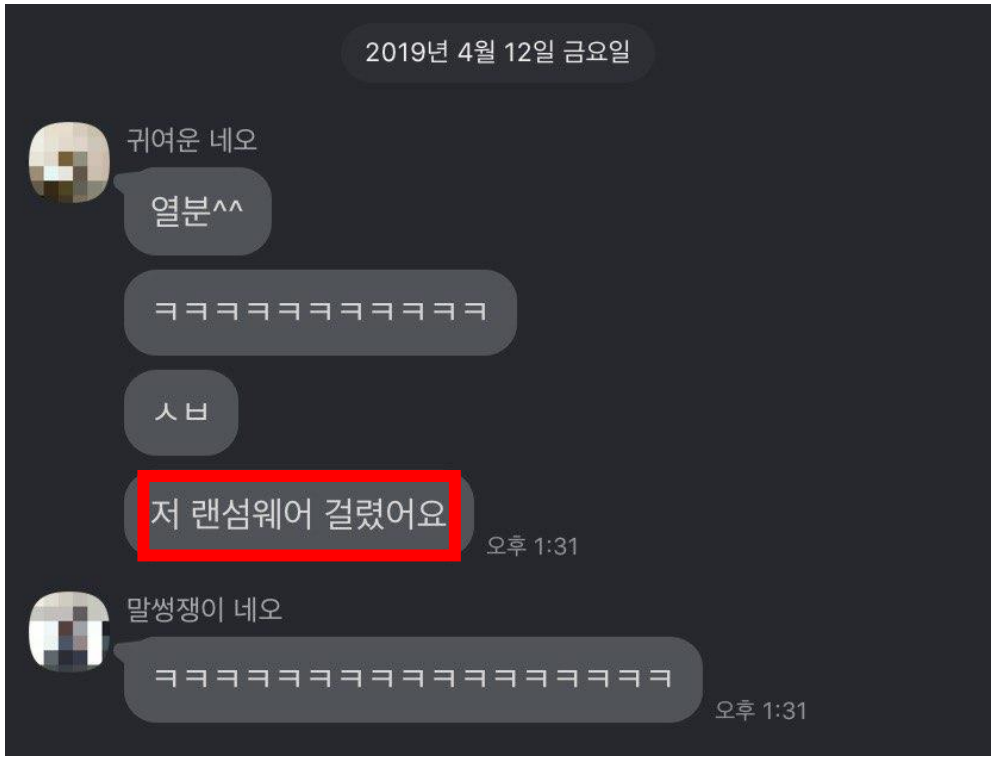
1

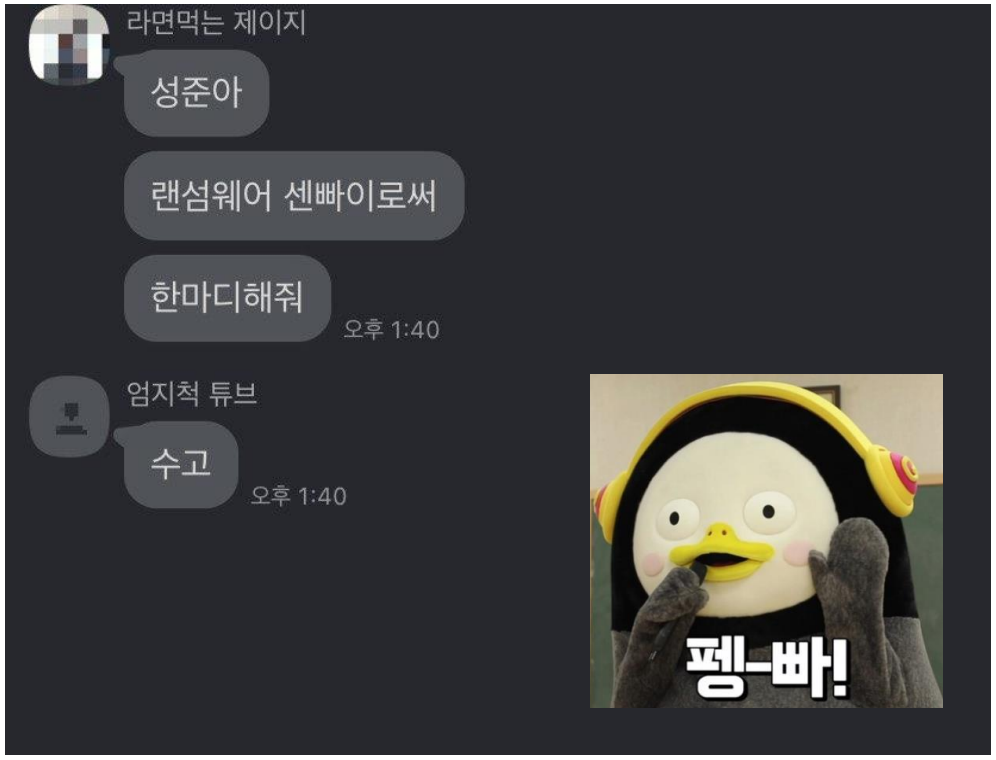
랜섬웨어는 알지?

1. 개념
2. 원리
3. 트렌드

1. 개념

항상 우리들 주변에 ㅎㅎ





1. 개념

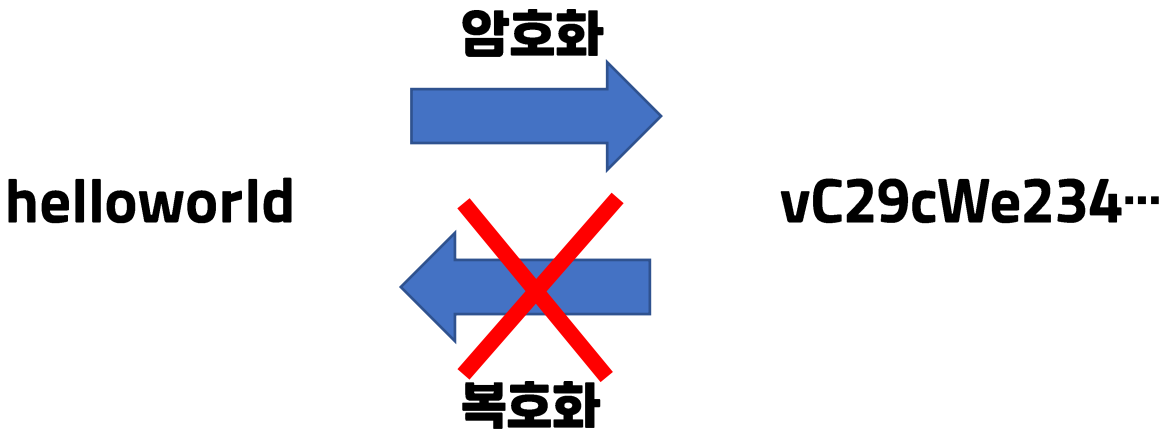
랜섬웨어 들어보셨죠?

컴퓨터 시스템 감염 후
파일 접근 제한

몸값 요구

자세히 알아보기 전에!
단방향 암호화 vs 양방향 암호화

자세히 알아보기 전에!
단방향 암호화 vs 양방향 암호화



Ransomware가 이용!

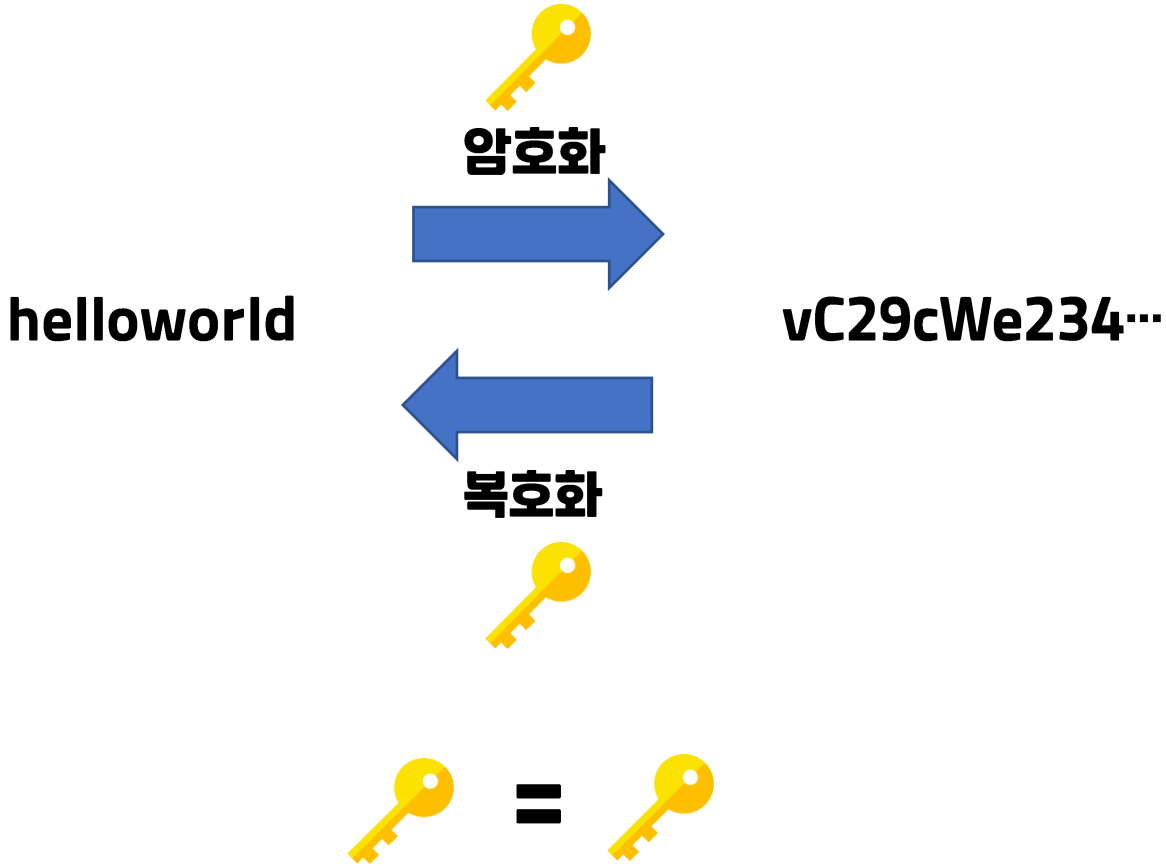
자세히 알아보기 전에!
단방향 암호화 vs 양방향 암호화

암호화 →

helloworld ⟷ vC29cWe234…

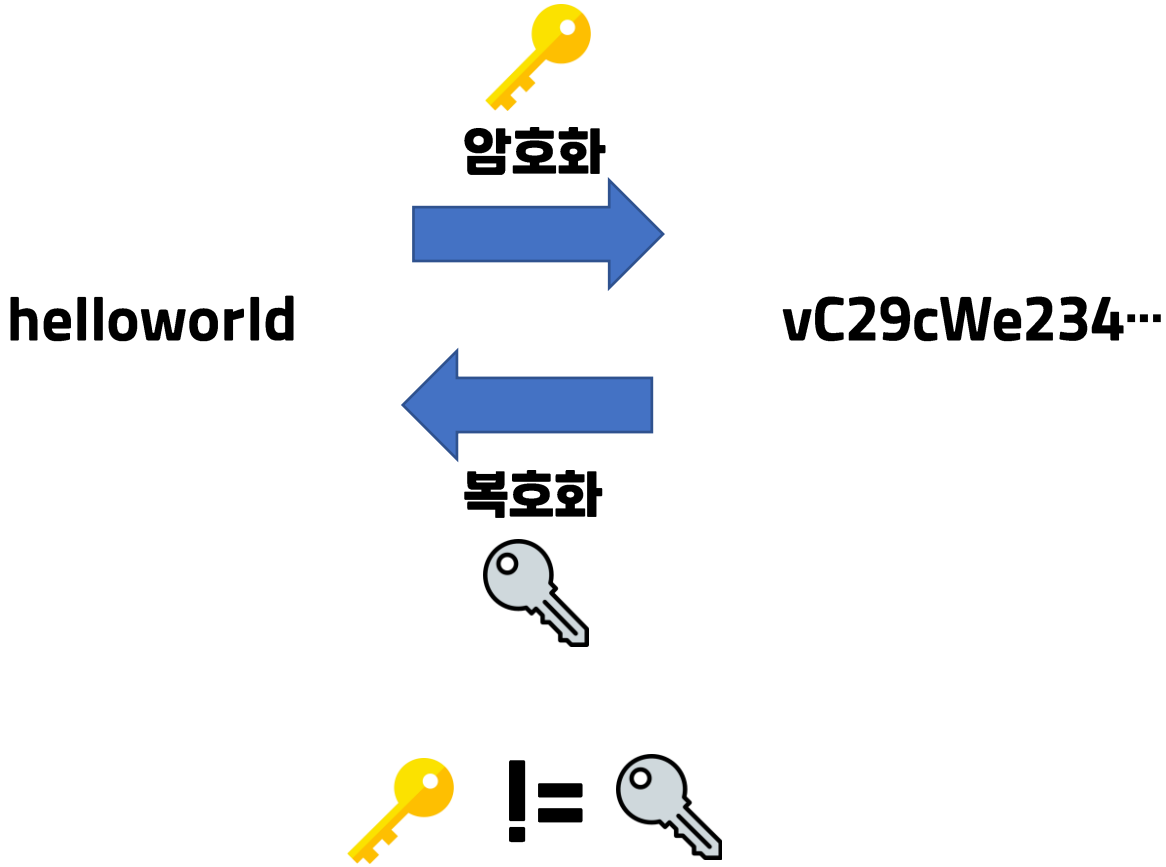
← 복호화

양방향 암호화에서 또 나뉨!
비공개키 암호화 vs 공개키 암호화

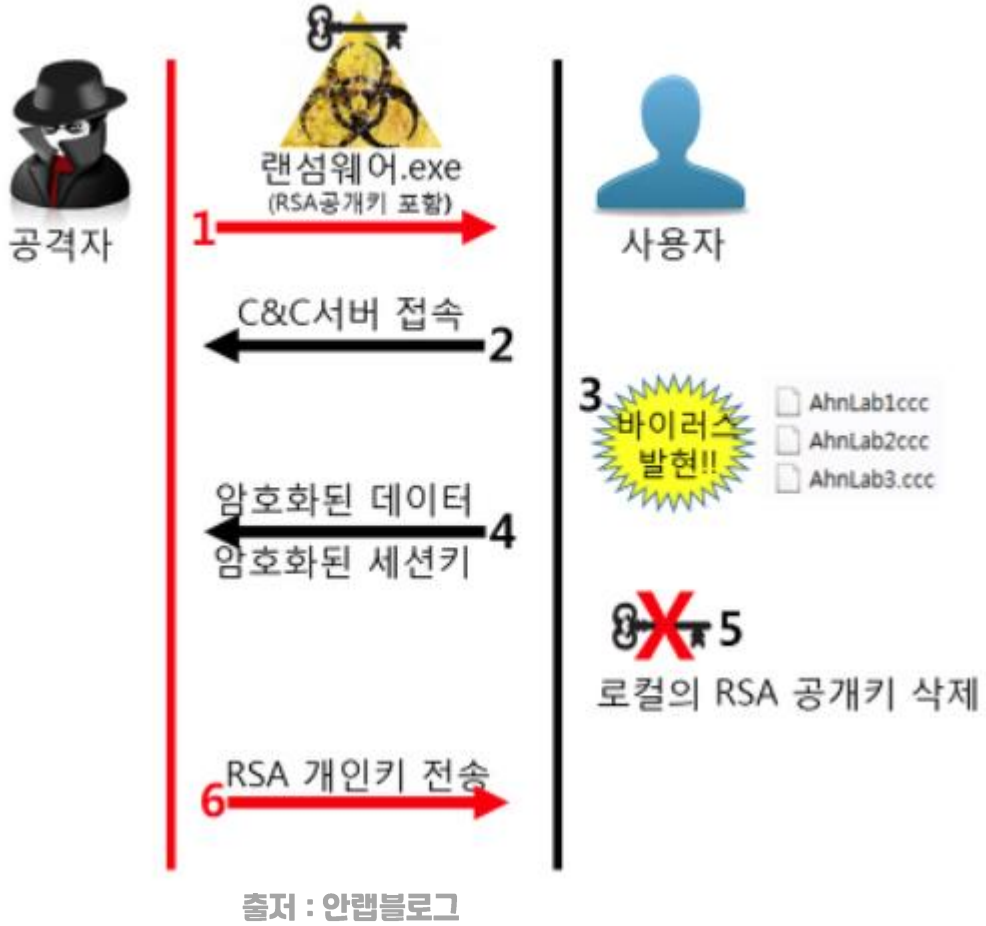


Ransomware가 이용!

양방향 암호화에서 또 나뉨!
비공개키 암호화 vs 공개키 암호화



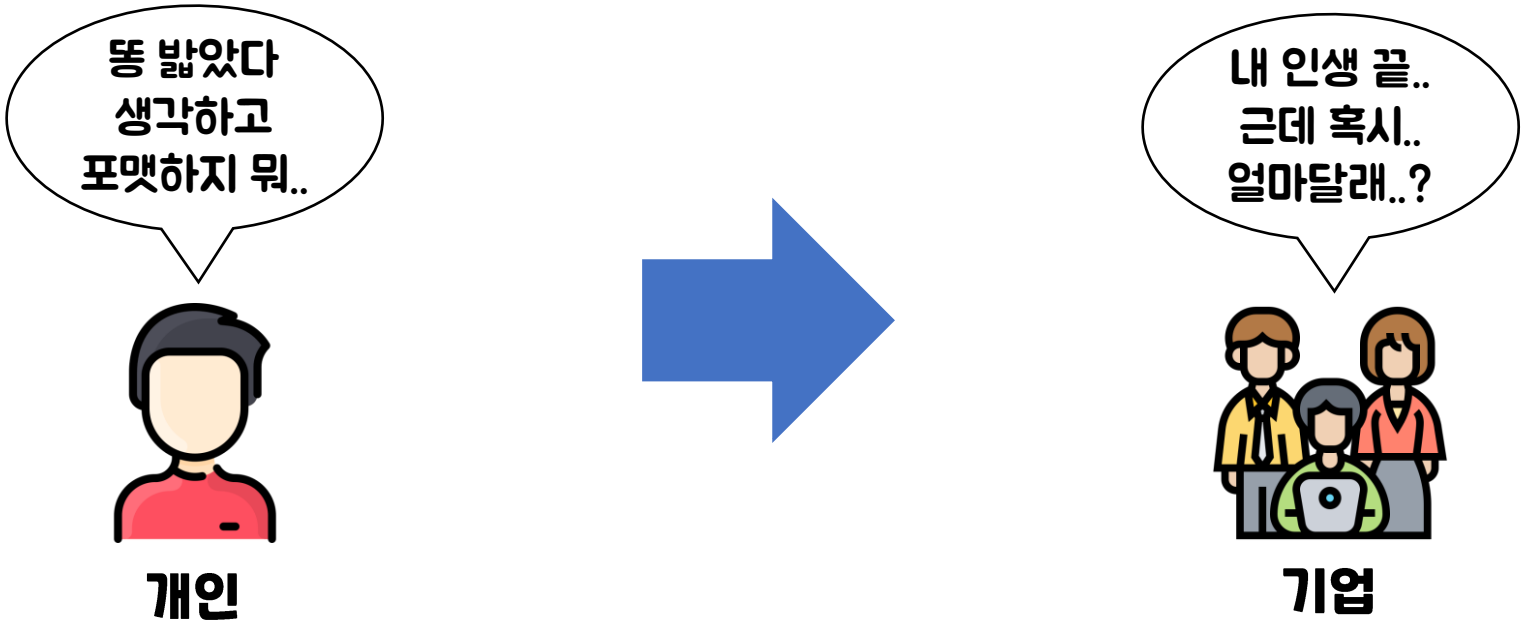
랜섬웨어는 어떻게 동작할까?



출저 : 안랩블로그

1. 실행
2. 폴더 하나씩 순환하며 파일 hex 값 뽑기
3. 공개키로 암호화
4. Readme 생성 > 돈벌려고 만든거니까
5. 해커 PC로 개인키 전송
6. 흔적 삭제(악성코드, 공개키 등)
7. 개인키로 협박

최근 랜섬웨어 트렌드는?



2

보안

1. 사후 대책
2. 사전 예방
3. 탐지 및 차단

2 보안

1. 사후 대책

사실 예방 말고 답이 없다.

백신

최신 업데이트

알수없는 출저

뻔하긴 한데 진짜 이게 대표 대응 메뉴얼

어떻게 랜섬웨어를 탐지? 차단?

Talking about 특징

어떻게 랜섬웨어를 탐지? 차단?

1. 실행 파일을 실행
2. 여러개 파일을 순식간에 감염
3. 폴더를 순환
4. 파일이 수정됨
5. 네트워크를 사용
6. 키를 전송함
7. 흔적 삭제
8. 볼륨 쉐도우 삭제
9. MBR 파괴 등등

어떻게 랜섬웨어를 탐지? 차단?

Talking about 탐지, 차단

어떻게 랜섬웨어를 탐지? 차단?

1. 시그니쳐 기반 탐지
2. 커널(미니필터)에서 I/O(수정시간 등) 봐서 의심될 경우 차단
3. 미끼파일 생성, 해당 파일 수정되면 차단
4. EXE 실행 시 가상 환경 속에서 먼저 실행 후 문제없으면 실제 환경 실행
5. URL 필터링, 네트워크 로그 분석
6. AI 학습 등등

3. 탐지 및 차단

추가 정보 필요한분 나중에 드림

- 랜섬웨어 종류, 원리
  - 로키
    - 사용자가 인지하지 못하는 네트워크 경로를 찾아 데이터를 암호화
  - 테슬라크립트
    - 200MB이상의 파일은 손상시
  - 케르베르
    - 음성을 통해 암호화 사실을 전
  - 비너스락커
    - 감염사실을 알리기 위해 바탕
  - 워너크라이
    - 특정 도메인 접속 성공 시 미동
  - 에레버스
    - 감염사실을 알리기 위해 모든
  - 크립토락커
    - 시스템 자체 백업본 삭제 후 동
  - 크립토월
    - 감염 확장자 변조 없음, 파일의 고유 서명 값 위변조
  - 올크라이
    - 네트워크 연결 시 악성행위 동작, 감염 정보를 알리
  - 크립트XXX
    - 브라우저, 메일, 쿠키, FTP 계정 등 사용자 정보 탈취
  - 배드래빗
    - Windows SMB 취약점에 네트워크를 통해 전파, MB
  - 매그니버
    - 모든 폴더에 한국어로 작성된 랜섬노트 생성
  - 메이즈
    - 모든 폴더에 한국어로 작성된 랜섬노트 생성
  - 페트야
    - MBR 변조로 인한 운영체제 부팅 불가
- 랜섬웨어 솔루션 종류, 원리
  - 누리 안티랜섬(누리랩)
    - 행위기반 + AI
  - 데이터 세이프 + 안티 랜섬웨어
    - 백업 + 복원 + 가상화영역실
  - 랜섬쉴드(이스트시큐리티)
    - 행위기반 + 백업
  - 랜섬아이(베일리테크)
    - 행위기반 + 센서
  - 리자드 랜섬크런처(이노티움)
    - 소프트웨어인증 + 행위분석
  - 세이퍼존 안티 랜섬웨어(세이퍼존
    - 행위기반 + 백업
  - 앱체크(체크멀)
    - 행위기반 + 백업
  - 좀비제로 EDR for Ransomware
    - 행위기반 + 백업
- 보안적합성검사
- 파일변형
- 확장자변경
- 볼륨쉐도우삭제
- 미끼파일 우회방지
- 권한변경
- 블랙리스트, 화이트리스트
- 패킹이 자체적으로 진행해서 상용툴론 언패킹 힘듬
- 동적분석으로 진행해야됨

솔루션에 대부분들어감

- 시그니처기반 (hash나, 54번째에 특별한 값이런거)
- 가상환경
- URL 필터링
- Siem을 이용한 로그분석 (윈도우에 위협분석)
- DB분석을 통한 AI학습(AI학습을 통한 미래랜섬웨어 예측)
- 커널을 이용한 I/O 체크
- 네트워크 차단

2

개발

1. 실습
2. 랜섬웨어 개발

랜섬웨어 실습

C:₩ > python scpransomware.py

*pip install pycryptodomex

랜섬웨어 코딩

같이 소스 보면서 공부하는 시간

*배포 금지!

*AES 암호화 사용 > 비공개키 암호화(일반적으론 공개키 암호화)
*랜섬노트 미생성 > 실제 랜섬웨어 아니므로
*등등 실제 랜섬웨어와 차이 존재

만약 이 파일이?

1. 대상 경로가 C:₩라면?

2. 키를 제공하지 않는다면?

3. 기존 랜섬웨어처럼 공개키 방식이라면?

4. decrypt_file() 함수를 제공 안한다면?

5. 랜섬노트(readme)를 만든다면?

감사합니다 :)