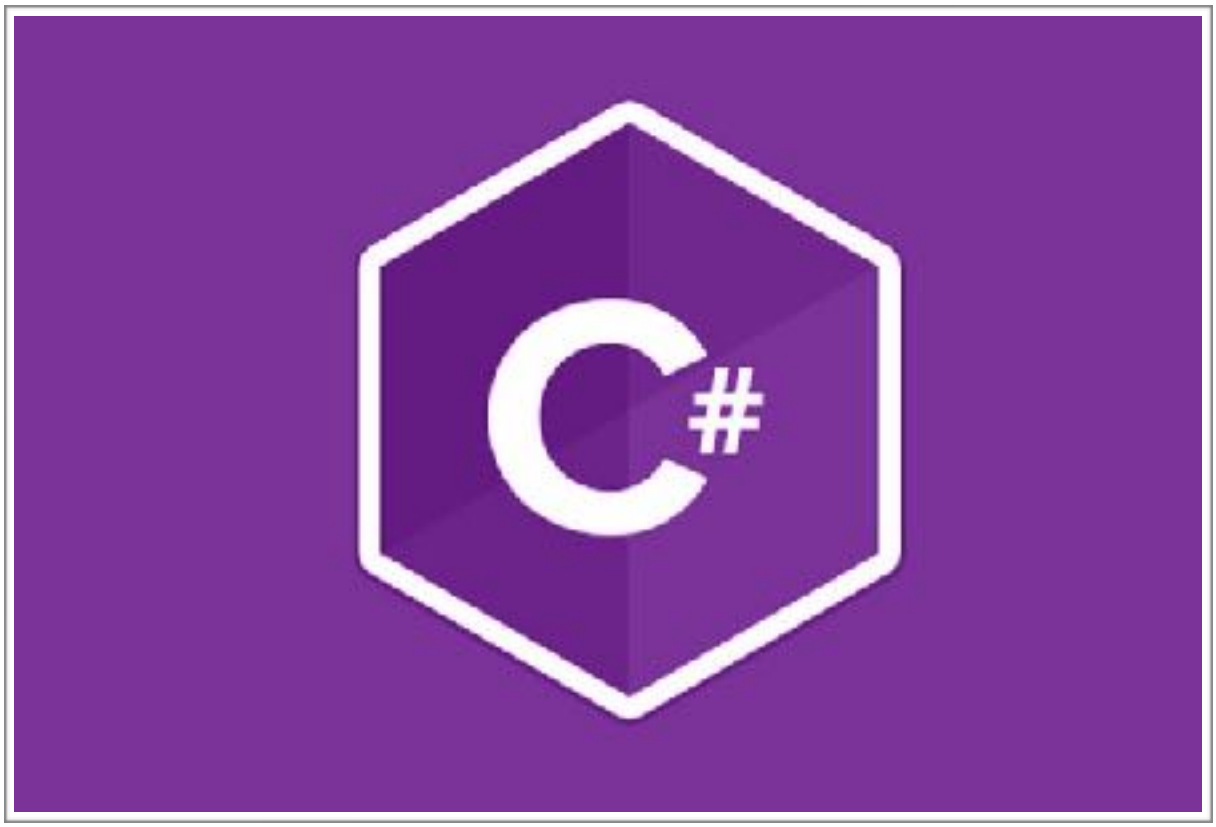
C# 프로젝트

C# Project



10220 정민우

C# 프로젝트

C# Project

1. 제작 동기

2017년에 가장 뜨거웠던 malware는 ransomware였습니다. 그래서 C#으로 제작할만한 프로그램을 찾는 중 우연히 ransomware를 분석하게 되었고 분석한 결과를 토대로 제작하게 되었습니다.

제가 분석한 ransomware는 WannaCRY이고 암호화 알고리즘이나 동작 방식을 모방한 C#프로그램을 제작하였습니다.

2. 제작 기간

총 제작 기간 : 2017년 7월 30일 ~ 2017년 8월 30일

2017년 7월 30일 ~ 2017년 8월 5일 : WannaCRY분석

2017년 8월 6일 ~ 2017년 8월 9일 : C# 프로젝트 생성 및 기초 UI작업

2017년 8월 10일 ~ 2017 년 8월 15일 : 암호화 알고리즘 작성

2017년 8월 16일 ~ 2017년 8월 20일 : 웹서버 세팅 및 원격지 서버 프로그램과 연동

2017년 8월 21일 ~ 2017년 8월 25일 : 복호화 알고리즘 작성

2017년 8월 26일 ~ 2017년 8월 30 : 나머지 작업 및 디버깅

3. 코드 분석

우선 전체 코드를 첨부하겠습니다.

4. 프로그램 실행 과정

먼저 제 서버인 https://phantom-cat.me/killswitch.html 에 접속을 시도하여 접속이 불가할 시에만 프로그램을 계속 실행합니다.

그 후 랜덤한 AES 256 Key를 생성하고 서버에 업로드 합니다.

(https://phantom-cat.me/encrypt.php 에 pc_name과 Key를 GET방식으로 넘겨서 DB에서 처리합니다)

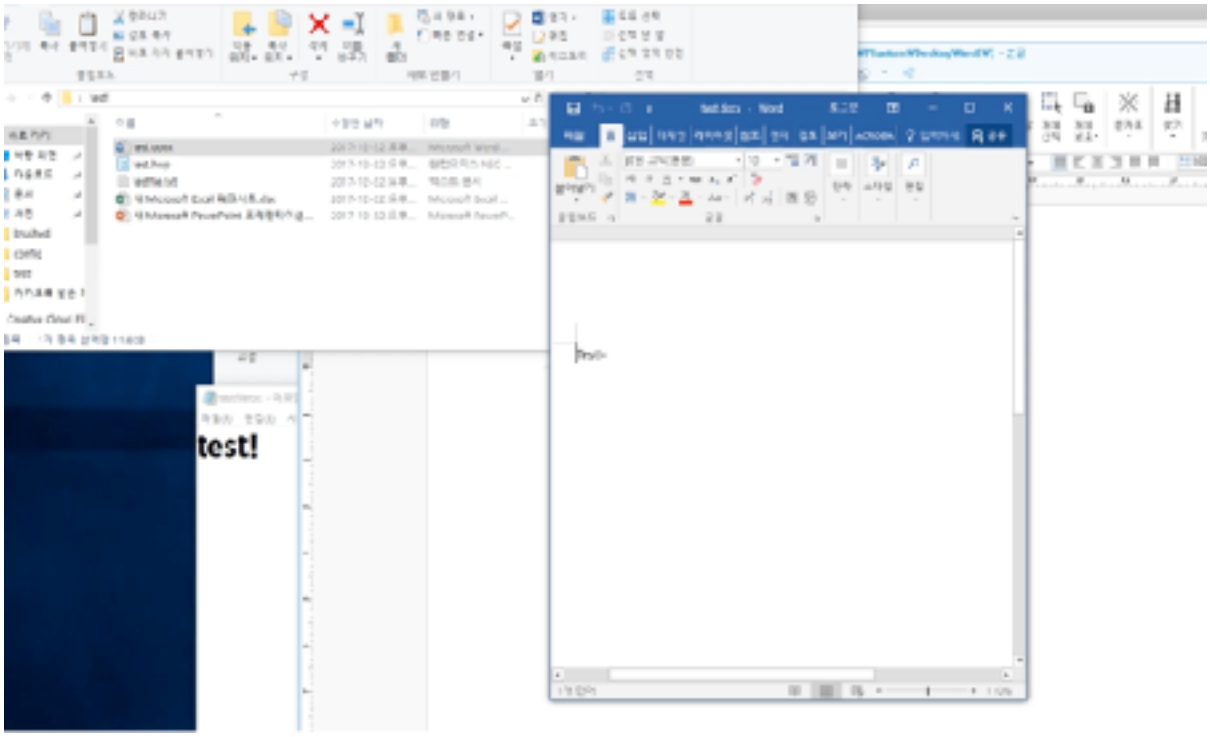
프로그램에 지정된 특정 경로 아래에 있는 파일과 폴더들을 스캔하여 배열에 넣고 위에서 생성된 암호화 Key로 파일들을 암호화합니다. 확장자를 프로그램의 시그니쳐로 바꾸어 버립니다.

모든 파일이 암호화 되면 메모리 내에 저장된 Key를 삭제하고 프로그램의 UI가 표시되면서 특정 행동을 지시합니다.

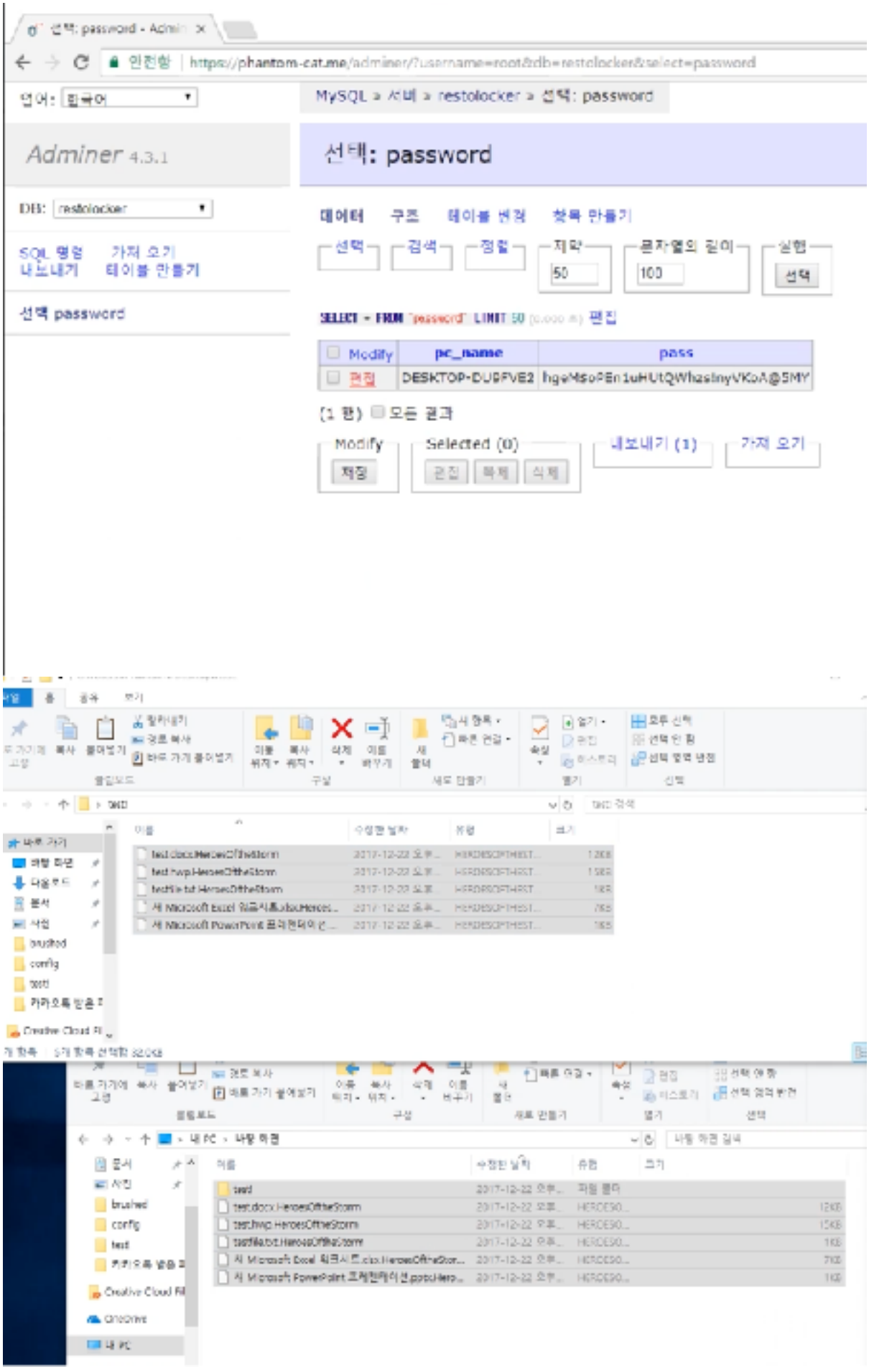
프로그램에서 요구한 특정 행동이 충족되면 서버에서 Key를 받아와 복호화를 진행합니다.

모든 파일이 복호화 되면 프로그램에서 복호화를 알린 후 프로그램을 종료할 수 있는 버튼이 나오게 됩니다.

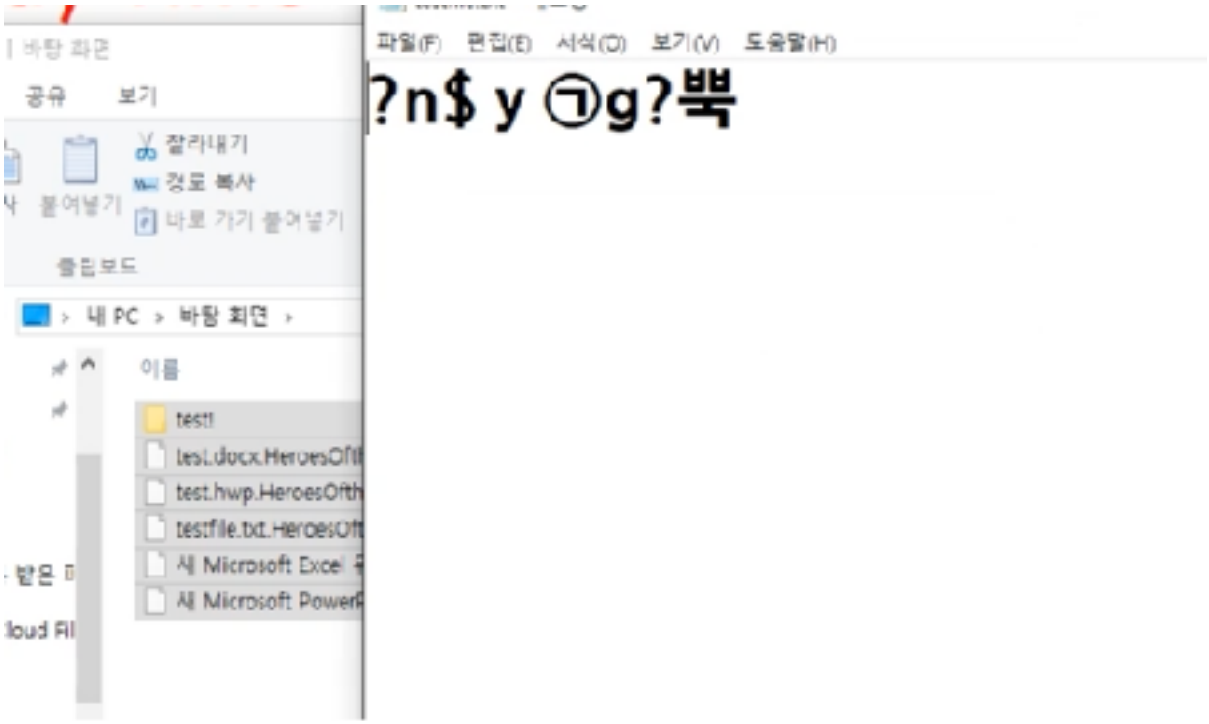
다음은 동작 스크린샷 입니다.



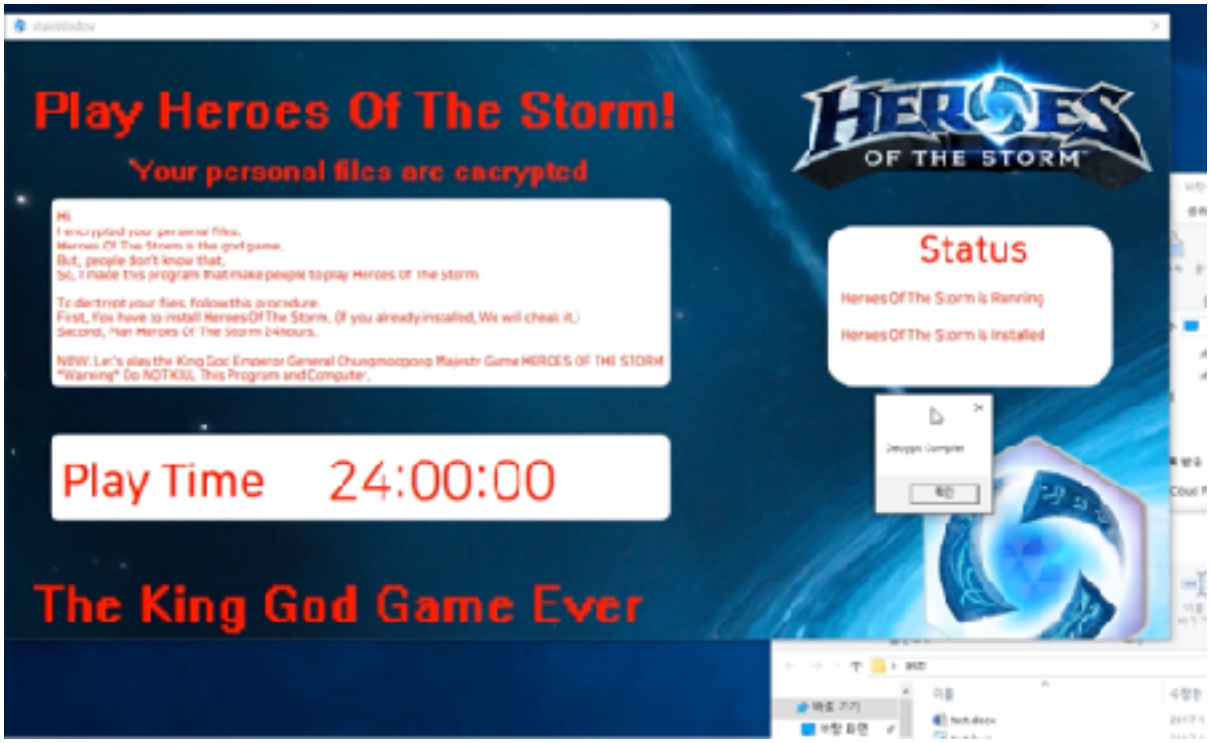
모든 파일이 정상임



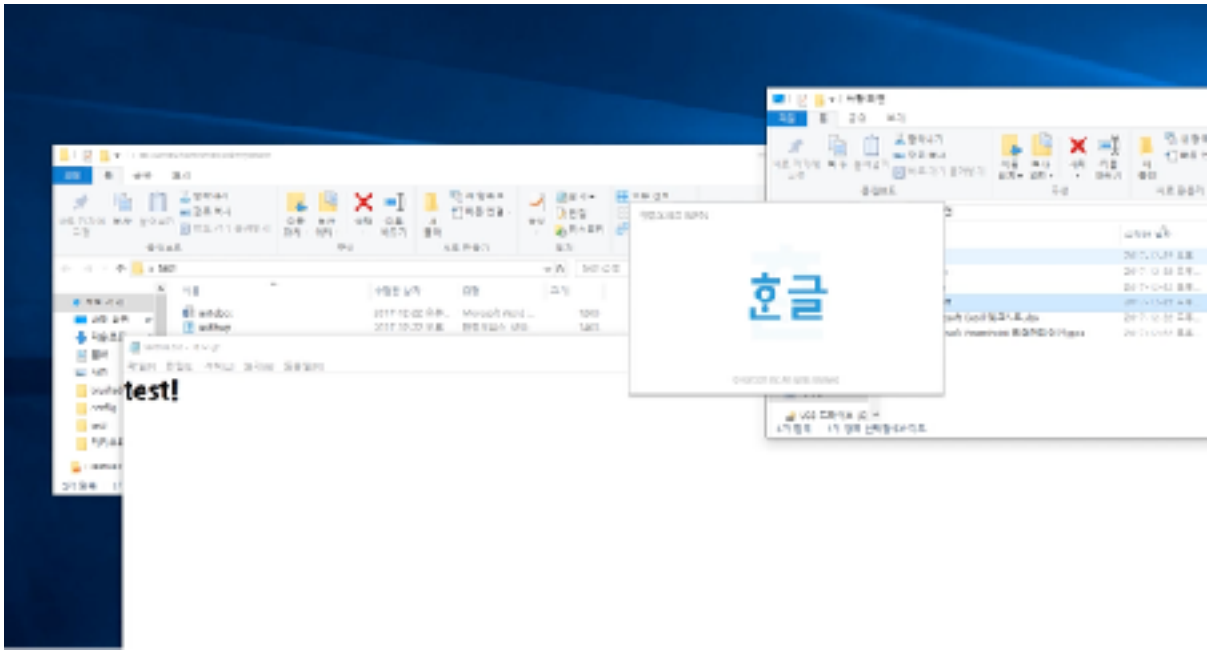
프로그램 실행 이후 파일이 암호화 되고 암호화 키가 서버에 업로드 됨



파일 자체를 암호화 했으므로 확장자를 바꾸어도 파일은 돌아오지 않음



지시한 행동을 완료 하였을 때 복호화 완료 창

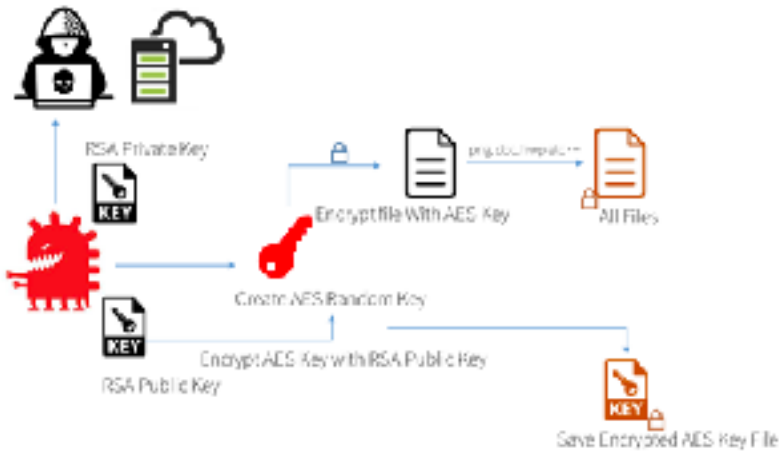


모든 파일이 정상적으로 돌아옴

5. 느낀점

원래 계획한 rsa 알고리즘으로 한번 더 묶는 과정이 생략되어 너무 아쉬웠다.

분석한 WannaCRY에서는 rsa알고리즘으로 추가적인 암호화가 진행되는데 그 과정이 너무 복잡하다 보니 계획한 기간 내에 개발할 수 없었다. 하지만 내 손으로 이러한 프로그램을 만들고 분석하면서 악성 프로그램들이 어떤 방식으로 활동하는지 분석하는데에 수월해졌고 앞으로 이러한 방식의 악성코드의 소스가 없어도 분석하는데에 훨씬 수월할것같다.



(분석했던 WannaCRY의 암호화 과정)