REPORT

Basic RCE Level 2

이름 : 신 민 구
제 출 일 : 2018.06.06

1. 문제 분석 및 실행

Challenges : Basic 02

Author : ArturDents

Korean :
패스워드로 인증하는 실행파일이 손상되어 실행이 안되는 문제가 생겼다. 패스워드가 무엇인지 분석하시오

English :
The program that verifies the password got messed up and ceases to execute. Find out what the password is.

Download

그림 1.1 Problem

Basic 02의 문제는 패스워드가 무엇인지 찾으라는 것이다. 한번 실행을 시켜보자.

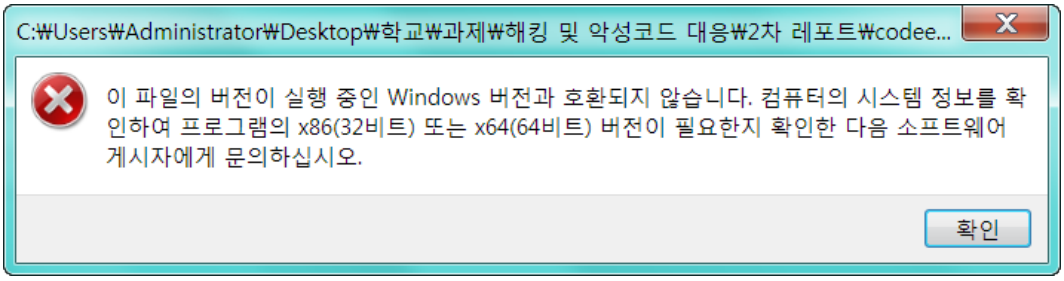

그림 1.2 실행 모습

파일이 손상이 되어서 위와 같은 메시지 박스가 나타났다. PEView를 통하여 파일이 어떻게 손상이 되었는지 살펴보자.

2. PEView

PEView라는 툴이 있는데 이는 파일의 구조를 볼 수 있다. PEView툴을 이용하여 열어보자.

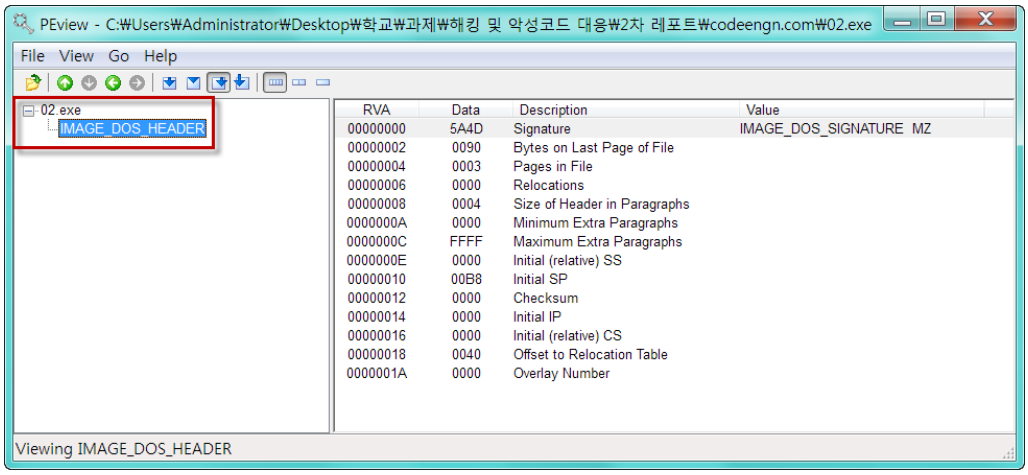

그림 2.1 PEView

구조를 보면 IMAGE_DOS_HEADER만 있다. 필수적으로 있어야 할 IMAGE_NT_HEADER, IMAGE_SECTION_HEADER 등 많은 것들이 없다. IMAGE_DOS_HEADER의 형태를 보면 많은 부분들이 잘못되어 있는 것을 알 수 있다. 이것을 Hex Editor라는 프로그램으로 열어보자. Hex Editor은 binary 형식의 파일을 hex형식으로 보여주는 도구이다.

그림 2.12 Hex Editor

아무리 봐도 뭔가 상당히 잘못되어있는 것 같다. 그러나 이 HxD(Hex Editor) 에서도 함수나 여러 가지 정보를 보여준다. 그러니 밑으로 내려가서 살펴보도록 하자.

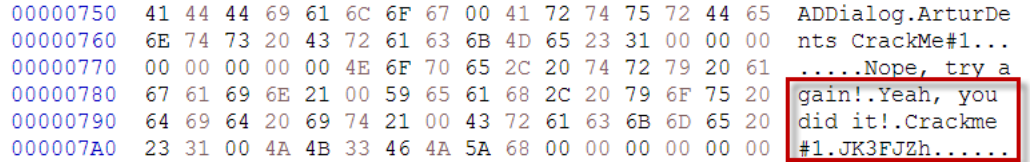

그림 2.13 Password

'Yeah, you did it!' 이라는 문자열이 있고 뒤에 Crack me#1과 'JK3FJZh' 라는 문자열이 보인다. JK3FJZh가 뭔가를 나타내는 것 같은데 패스워드 인 것 같아 보인다. 이 값을 가지고 인증을 하면 인증이 되는 것을 보아 패스워드임을 알 수 있다.