CodeEngn Reverse Challange
Basic RCE #2

Reverse L02 Start

Author : ArturDents

Korea :

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.

Down

그림1

실행파일이 손상이되어 실행이 되지 않는다고 한다.
먼저 올리디버거나 IDA 로 이 exe 실행파일을 까보기로 하겠다.

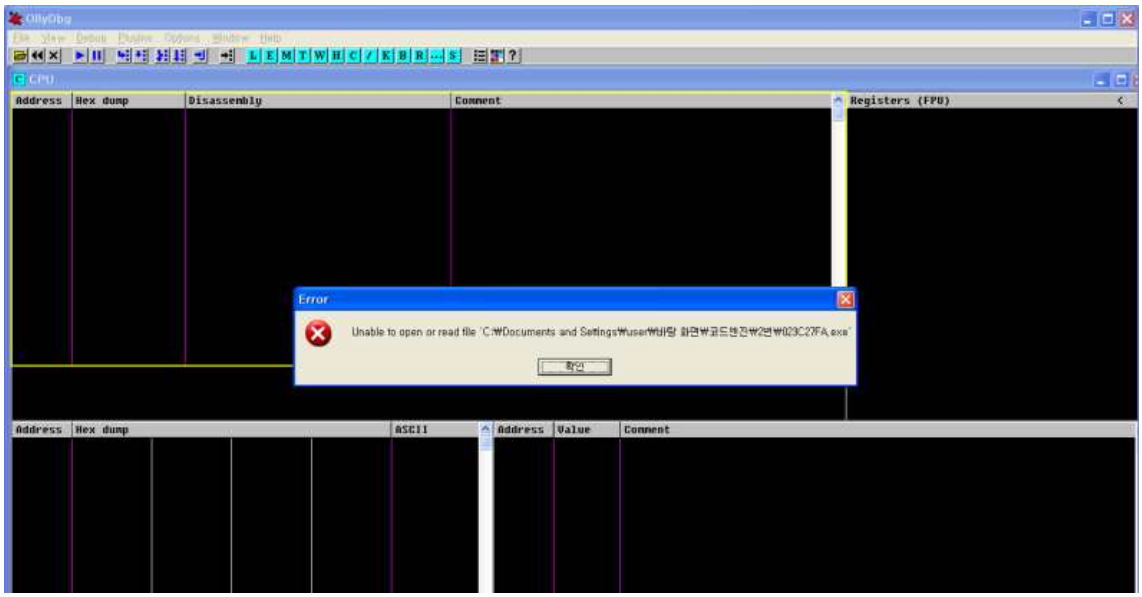

그림2

그림2와 같은 메시지가 나오면서 파일 불러오기에 실패한다.
Ida 로 비슷한 문제로 제대로 이 exe 파일을 분석하지 못한다.

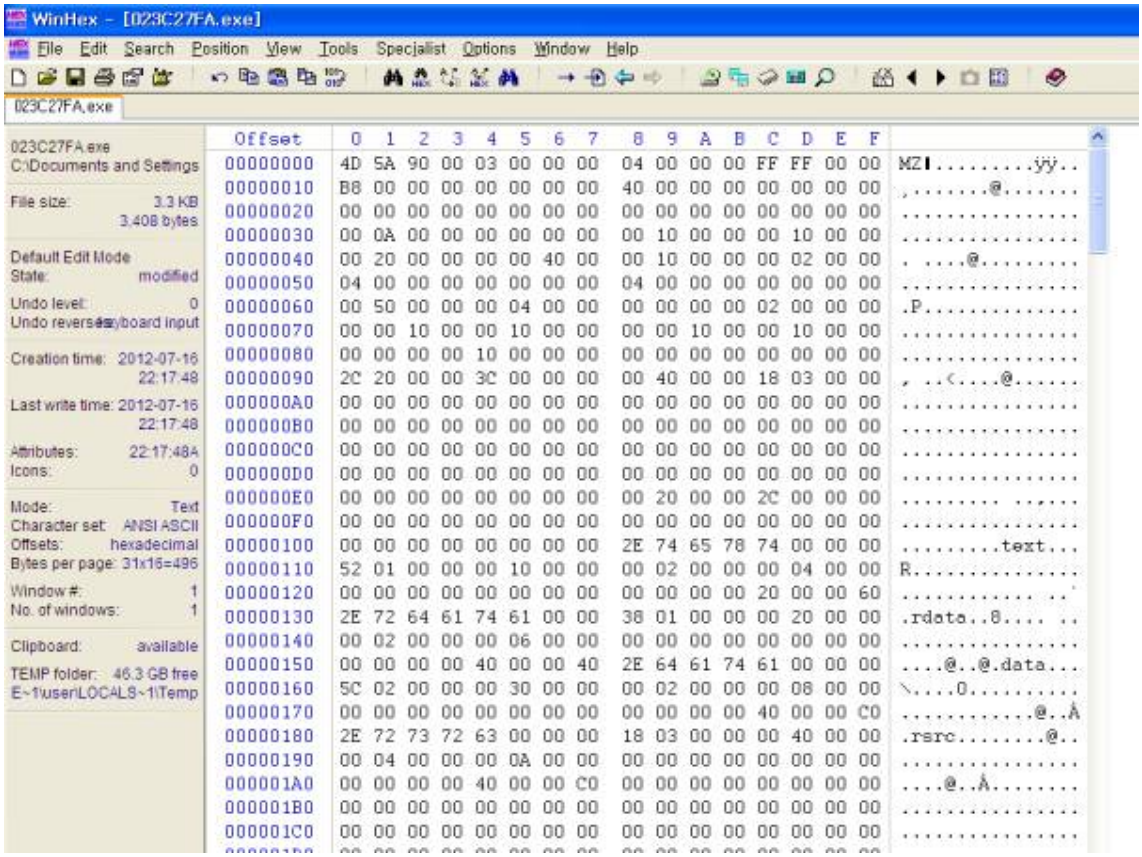

그림3

그렇다면 WinHex 로 exe 파일을 열어보면 MZ라는 시그니처는 보이는데 그 아래로 파일의 구성요소가 일부 없는 것이 보인다.

```
41 44 44 69 61 6C 6F 67  00 41 72 74 75 72 44 65 ADDialog.ArturDe
6E 74 73 20 43 72 61 63  6B 4D 65 23 31 00 00 00 nts CrackMe#1...
00 00 00 00 00 4E 6F 70  65 2C 20 74 72 79 20 61 .....Nope, try a
67 61 69 6E 21 00 59 65  61 68 2C 20 79 6F 75 20 gain!.Yeah, you
64 69 64 20 69 74 21 00  43 72 61 63 6B 6D 65 20 did it!.Crackme
23 31 00 4A 4B 33 46 4A  5A 68 00 00 00 00 00 00 #1.JK3FJZh......
```

그림4

아래로 스크롤 바를 조금 내려보면 수상한 문자가 보인다. JK3FJZh <== 이녀석이 바로 인증 키 값이다.

※ Ida 나 olly 디버거로 바이너리분석이 되지 않는 이유는, 원래 모든 파일은 바이트 코드로 이루어져 있고 이 파일들은 파일포맷 형태에 맞도록 바이트코드가 적재적소에 위치해 있어야 한다. 분석 툴들은 바이트 코드를 보고 파일을 분석해주기 때문이다. 예를들면, 헤더자리에 FF FF 같은 바이트 코드가 들어 있다던지 컴퓨터가 인지하고 있는 바이트 코드가 들어가있지 않으면 분석 툴은 이 바이너리가 무엇인지 파악을 하지 못한다.