코드엔진 Basic RCE L05

문제

CodeEngn.com [코드엔진]

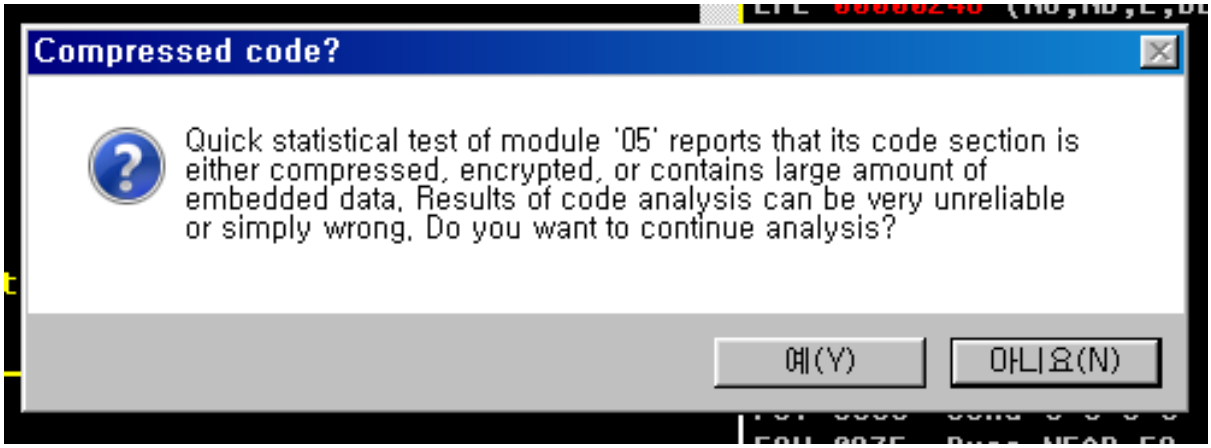
코드엔진은 국내 리버스엔지니어링 정보공유를 위해 2007년 부터 리버스엔지니어링 컨퍼런스 및 세미나, 워크숍을 현업 실무자들과 함께 운영하고 있는 비영리 커뮤니티입니다.

https://ch.codeengn.com/

의 Basic RCE L05

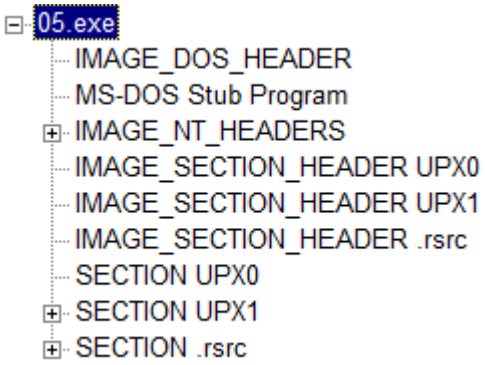
해결 과정

- ollyDbg로 실행파일을 분석하려고 하니 압축이 되어있는 실행파일이라는 경고문 출력



압축이 되어있는 실행파일 이라는 경고문

- PEview를 통해 실행파일을 열어본 결과 upx라는 단어를 자신의 섹션이름에 포함하고 있는 섹션들을 발견하여 검색해본 결과 실행파일이 upx로 압축이 되었다는 사실을 파악



upx라는 단어을 이름에 포함하는 섹션들

- upx로 압축이 되어있는 실행파일이라 upx 프로그램을 설치한 후 사용하여 압축을 풀음

```
                                                    >upx -d 05.exe
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    315392 <-    131584   41.72%    win32/pe     05.exe

Unpacked 1 file.
```

upx 프로그램을 실행할 때 '-d' 라는 인자를 주는 것을 통해 압축 풀기

- ollyDbg에서 All referenced text strings를 이용하여 알맞은 시리얼을 입력하였거나 그렇지 않았을 경우에 나오는 문자열을 검색

```
00440F5A|MOV     ECX, 0044103C                |ASCII "CrackMe cracked successfully"
00440F5F|MOV     EDX, 0044105C                |ASCII "Congrats! You cracked this CrackMe!"
00440F74|MOV     ECX, 00441080                |ASCII "Beggar off!"
00440F79|MOV     EDX, 0044108C                |ASCII "Wrong Serial,try again!"
00440F8E|MOV     ECX, 00441080                |ASCII "Beggar off!"
00440F93|MOV     EDX, 0044108C                |ASCII "Wrong Serial,try again!"
```

사용자가 입력한 시리얼이 True/False인지에 따라 출력되는 문자열들을 검색하여 찾은 결과

- 문자열 주변에서 입력된 문자열을 비교하기 위해 존재하는 것으로 보이는 문자열을 찾아 실제 실행파일에 입력해 본 후 맞는 입력임을 확인하여 해결

비교하기 위해 존재하는 것으로 보이는 문자열을 실행파일에 입력하여 맞는 입력임을 확인

UPX

- 실행 파일 압축 프로그램
- UPX의 github에서 설치가능