Codeengn Challenges Advance RCE LEVEL6 풀이

Reverse2 L06 Start

Author : CodeEngn / Lee Kang-Seok

Korea :

남은 군생활은 몇일 인가

정답인증은 MD5 해쉬값(대문자) 변환 후 인증하시오

English :

How many more days to serve for the military

The solution is the MD5 hash of the answer

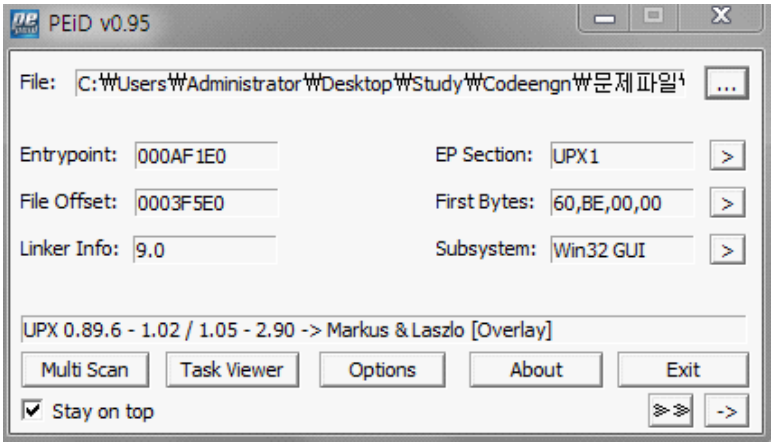
Down

실행해본 결과 메시지 창이 계속 뜨면서 표시되는 숫자가 증가한다 ,

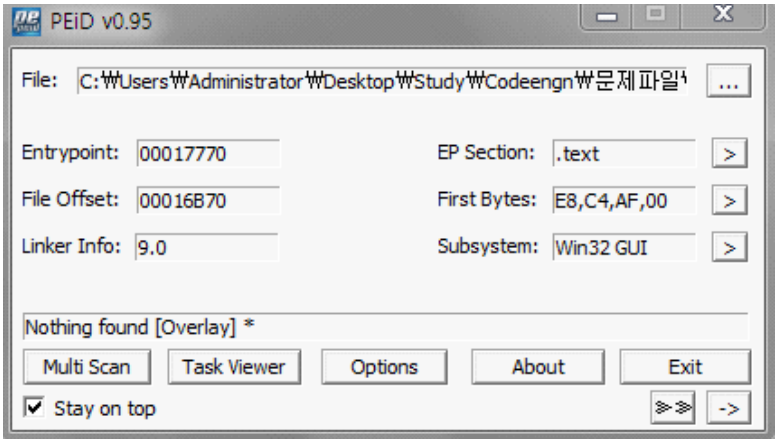
창이 귀찮게 계속 뜨길래 니가 이기나 내가 이기나 해보자는 식으로 확인란에 마우스 커서를 놓고 계속 엔터를 쭉 눌렀는데 790에서 메세지창이 끝났다.

분석 시작 전에 답을 알아버렸다……ㅠ_ㅠ

아무튼 PEID로 PE를 확인해보았다.

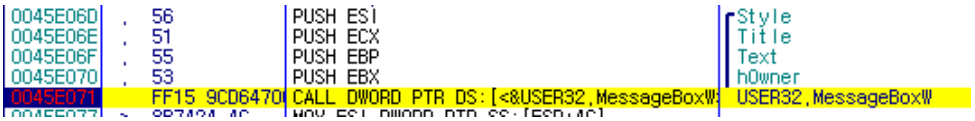


UPX 패킹되어있어서 패킹을 풀어줬다.



OLLY로 열어 분석을 해보았다 .

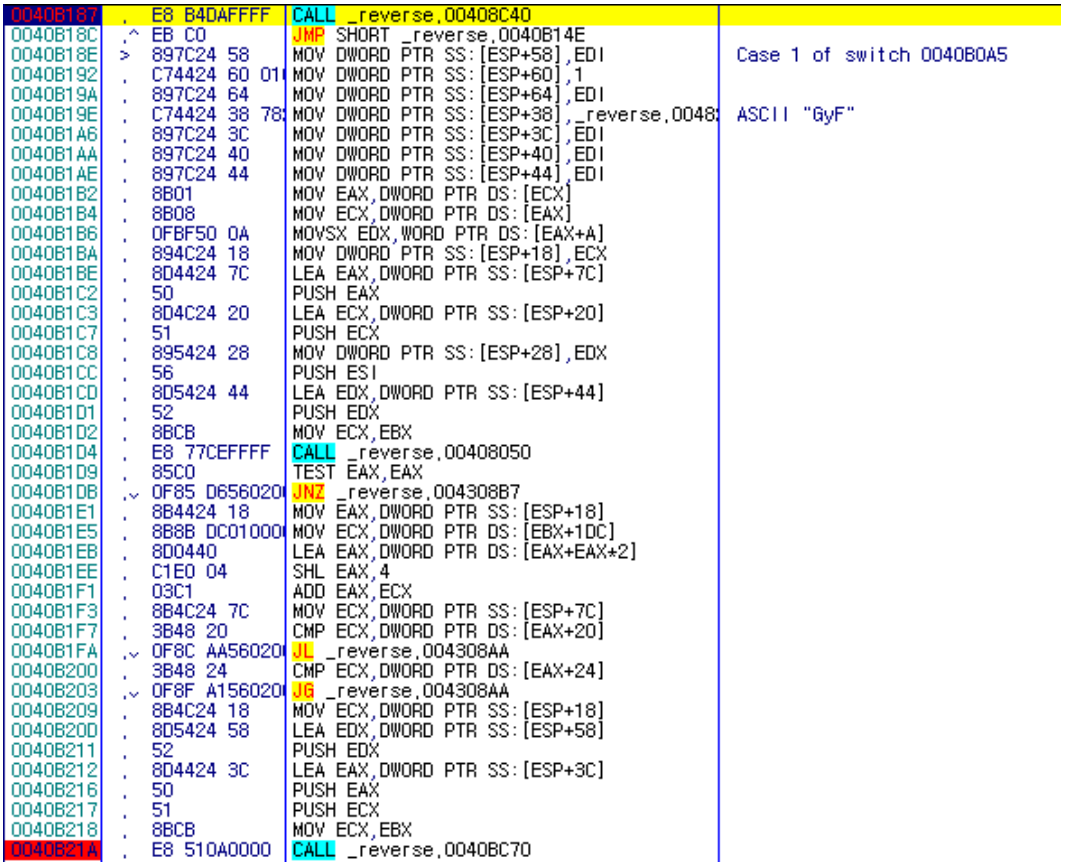
Back to user 모드를 이용해 messageBox함수를 call하는 부분을 찾았고 ,



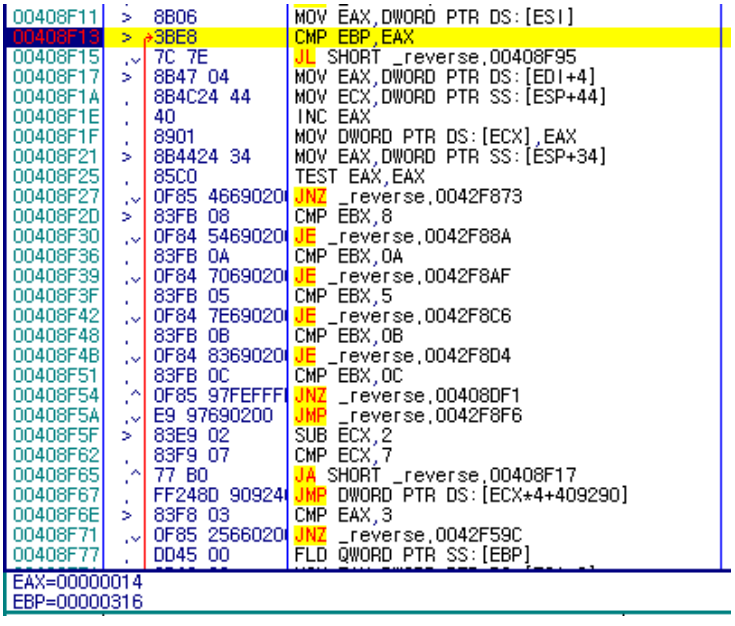
그리고 그 안으로 파고들어 MessageBoxTimeoutW라는 함수를 호출해 주는 부분을 찾았다.

MessageBoxTimeout 함수는 맨 마지막 인자로 종료될 시간을 밀리세컨트 단위로 받는데 -1로 되어있는걸 1로 바꿔주었다. 즉 1밀리 세컨드 후 자동적으로 메세지창이 소멸되게 만들어주었다.

그리고 계속 분석을해서 메세지창을 출력 하게 해주는 함수를 call하는 부분과 비교하는 함수를 call 하는 부분을 찾았다.



주소 부분이 빨간 저 두부분이 위에서 부터 비교 , 출력 하는 함수인데 비교하는 함수를 파헤치다보면 다음과 같은 비교문을 볼 수가있다.



14와 316을 비교해주는데 316을 10진수로 바꿔주면 790이 된다.
이전에 내가 우연히 노가다로 알아낸 답과 같다! :D