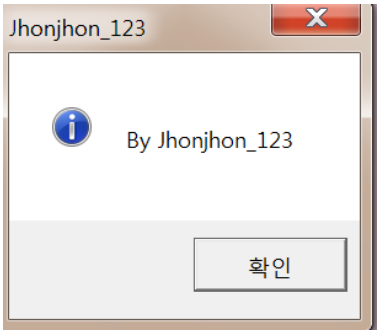
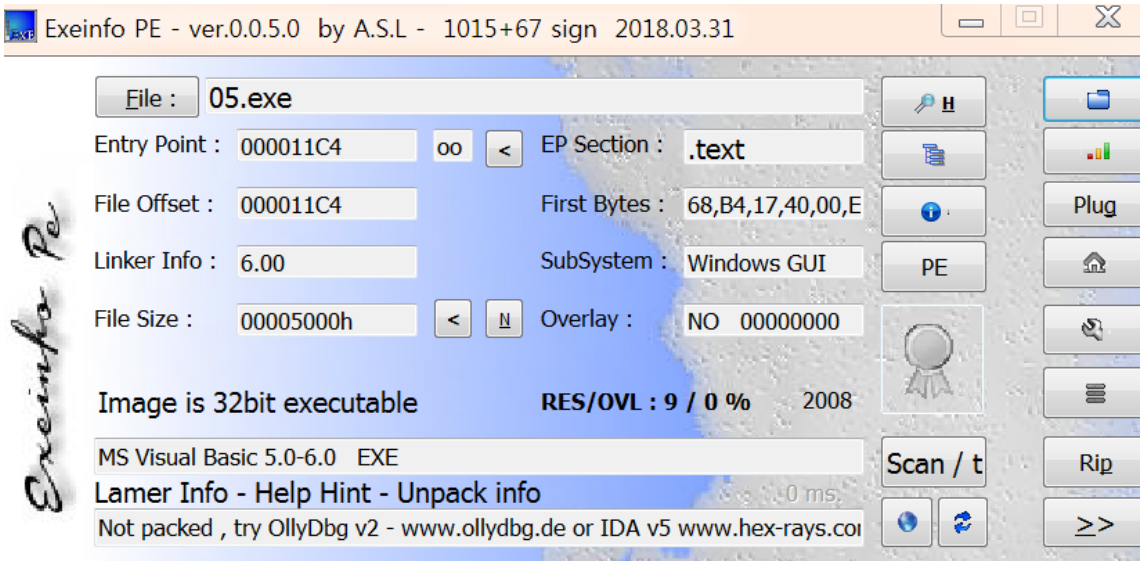
코드 엔진 Challenges: Advance 05

Author: Pass Corta
Korean: Serial 은 무엇인가

문제를 확인하고 프로그램을 실행시키자 빈 칸이 나와 '5'를 입력하고 ok 버튼을 누르자 다음과 같은 메시지가 나오고 입력값 5는 'Mal Cracker!!' 라는 메시지로 바뀌었다.
아무래도 틀린 시리얼 값을 입력하면 "MAL Cracker!!"라는 메시지로 바뀌는 것 같다.

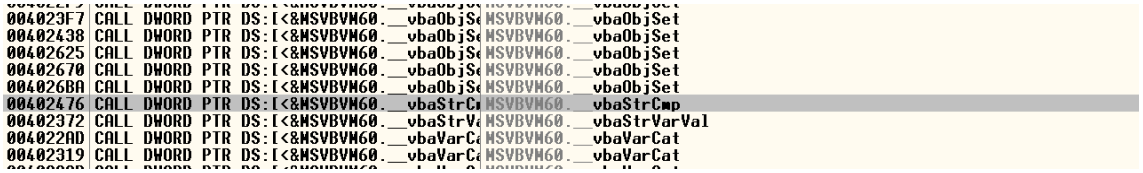




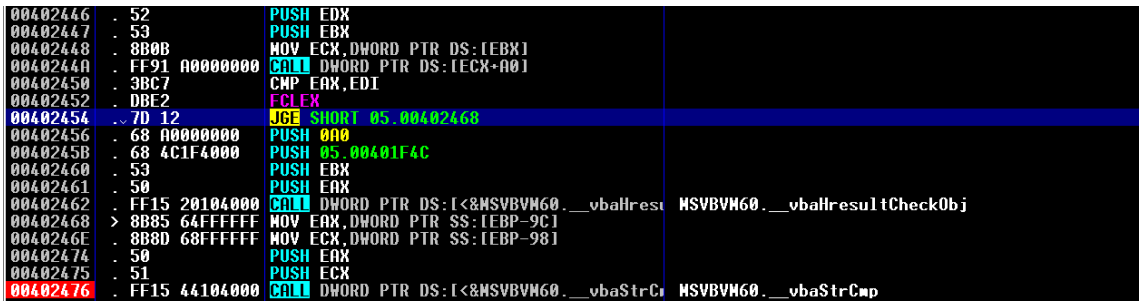
PEID로 패킹 여부를 확인해보자 아무런 정보를 얻을 수 없었다. 올리디버거로 분석해보자.

문제가 Serial을 찾는 것이고 지금까지 Serial을 찾을 때 사용자의 입력값과 원래의 시리얼을

비교한 후 에 점프하여 메시지를 출력하는 형식이므로 search for를 통해 cmp 관련 함수를 찾아보자.



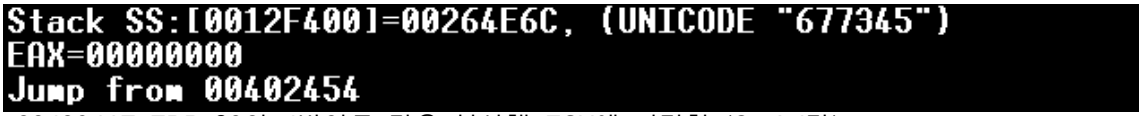
예상했던 대로 vbaStrcmp 함수가 보인다. 이 함수의 코드 부분으로 들어가 분기문이 있는지 확인해보자 .



분기문역시 보인다 .이 부분에 BP를 걸고 분석을 해보도록 하자. *JGE (>=)

-00402454에 bp를 걸고 실행을 한 결과 EAX와 EDI의 값을 비교후에 >= 으므로 00402468로 분기함

-00402468 EBP-9C의 4바이트 값을 복사해 EAX에 저장함 (사용자가 입력한 값)



-0040246E EBP-98의 4바이트 값을 복사해 ECX에 저장함 (Serial값)

-00402474 EAX 값 push

-00402475 ECX 값 push

-00402476 vbaStrCmp 함수를 이용하여 EAX값과 ECX 값 비교 한다 값이 같으면 계속 진행

을 하다가 00402544에서 성공 메시지 값 출력

답 :677345