Basic

RCE_04 문제풀이

name : 조 성환
nickname : Lum4n
@Lum4n, namul10@mail.com
문제 : http://codeengn.com/

Reverse L04 Start

Author : CodeEngn / Lee Kang-Seok

Korea :

이 프로그램은 디버거 프로그램을 탐지하는 기능을 갖고 있다. 디버거를 탐지하는 함수의 이름은 무엇인가

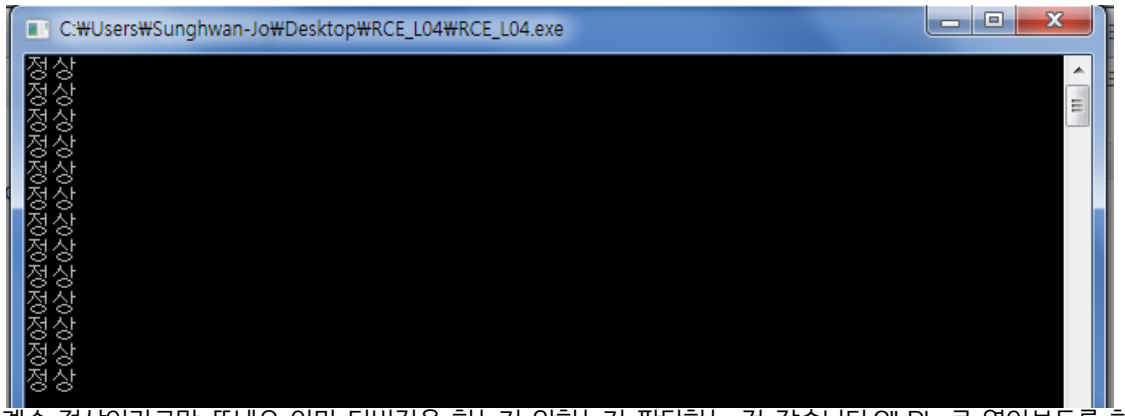
English :

This program can detect debuggers. Find out the name of the debugger detecting function the program uses.

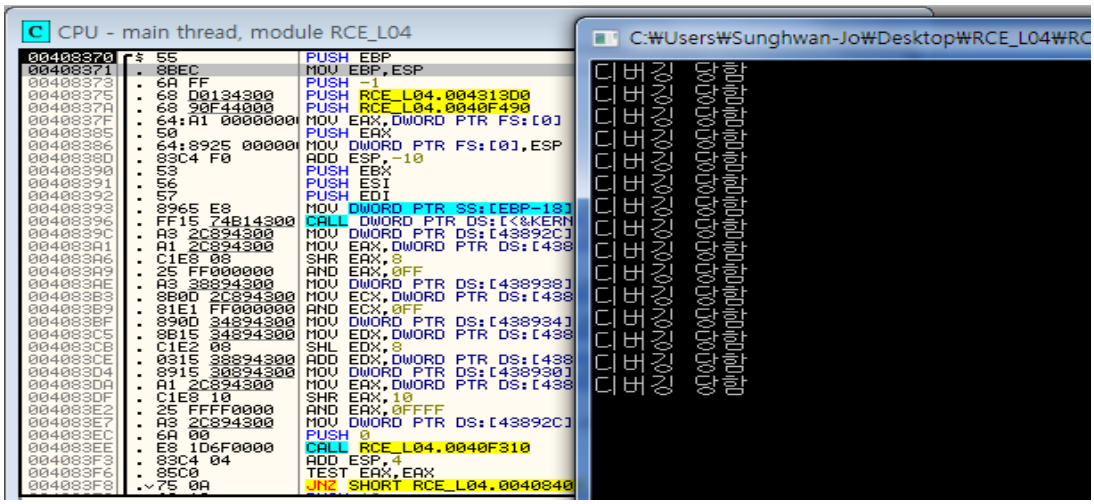
Down

총 96 분이 이 문제를 푸셨습니다. / 96 people solved this problem.

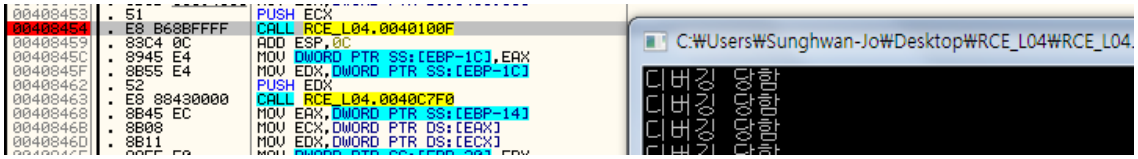
4번입니다! 우선 프로그램을 실행시켜 보겠습니다.



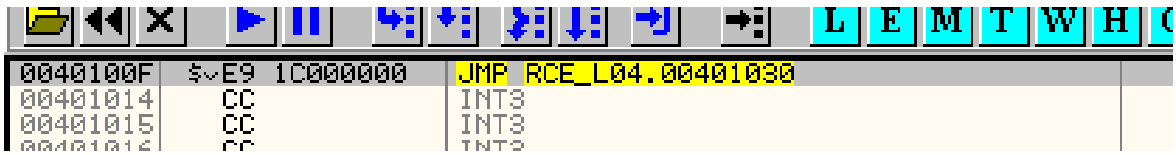
계속 정상이라고만 뜨네요 아마 디버깅을 하는지 안하는지 판단하는 것 같습니다.OllyDbg로 열어보도록 하겠습니다



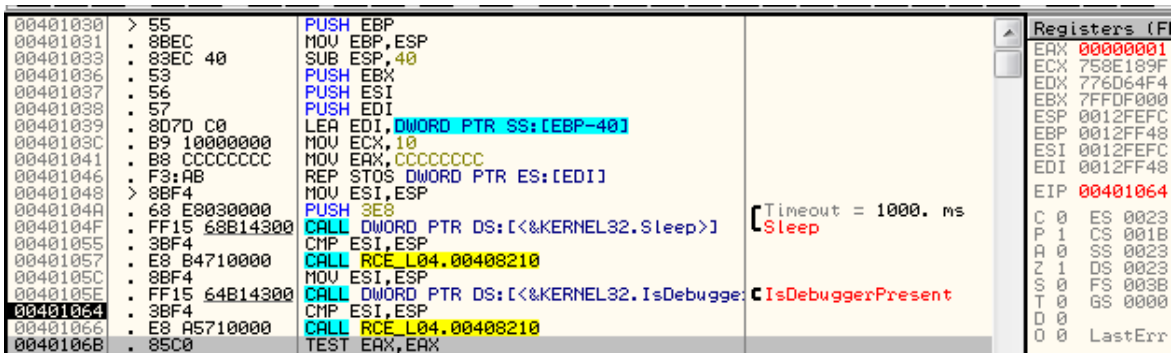
OllyDbg로 연후 실행을 시켜보니 '디버깅을 당함'이라고 출력을 하네요.그래서 프로그램을 차근차근히 실행시켜 보니



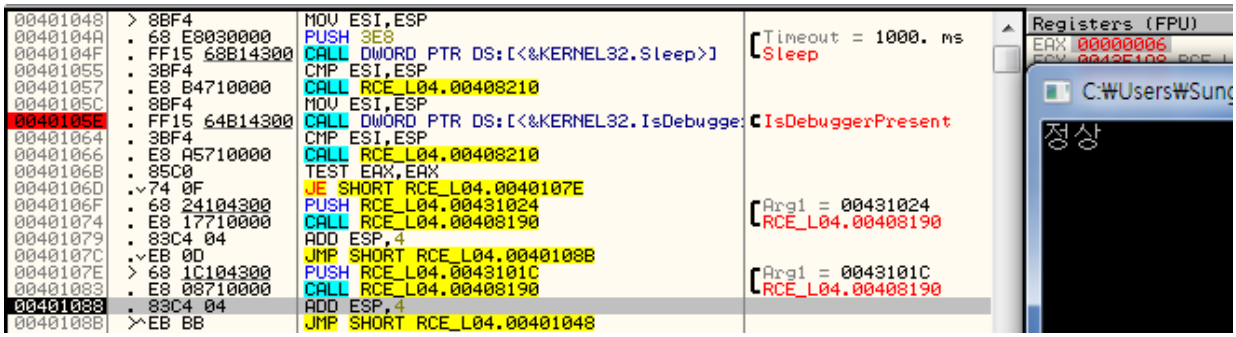
00408454 부분의 함수가 호출되고 난후에 '디버깅 당함'이라는 문자열을 출력하는 것을 보니 저 함수 내부에는 디버깅을 체크하는 함수가 잇는것 같습니다.



0040100F로 가보니 또다시 JMP하는 부분이 있네요 다시 들어가 보니



이런 모양의 함수가 나옵니다. 보아하니 'IsDebuggerPresent' 가 의심스러운데 IsDebuggerPresent 함수가 실행된후에 1이 리턴이 되었습니다. 리턴값을 0으로 변조시킨후에 실행을 시켜보니



멍청한 프로그램을 감쪽같이 속였네요 :)
IsDebuggerPresent는 디버깅중이면 1을 리턴 한다고 합니다!

그래서 정답은 IsDebuggerPresent !!