

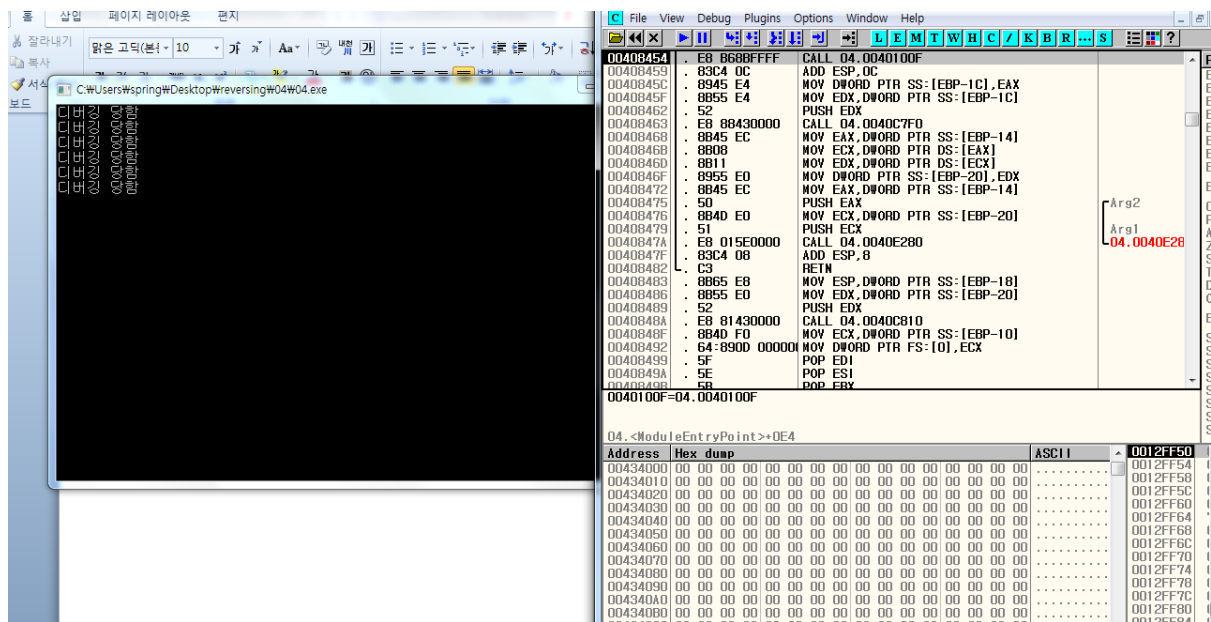
Challenges : Basic 04

Author : CodeEngn

Korea :

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

처음에 F9 로 실행을 시켜보면



디버깅 당함 이 계속 나온다

그러면 저 어셈코드를 하나하나 F8로 내려보다가

어디서 저 문구가 나오는지 보고 거기에 breakpoint 를 걸어놓고 F7 로 들어가보자

0040844D	. 8B0D 3C894300	MOV ECX,DWORD PTR DS:[43893C]
00408453	. 51	PUSH ECX
00408454	. E8 B68BFFFF	CALL 04.0040100F
00408459	. 83C4 0C	ADD ESP,0C
0040845C	. 8945 E4	MOV DWORD PTR SS:[EBP-1C],EAX
0040845F	. 8B55 E4	MOV EDX,DWORD PTR SS:[EBP-1C]

Breakpoint 걸고 f7 로 들어가보면

0040100F	\$ E9 1C000000	JMP 04.00401030
00401014	CC	INT3
00401015	CC	INT3
00401016	CC	INT3
00401017	CC	INT3
00401018	CC	INT3
00401019	CC	INT3
0040101A	CC	INT3
0040101B	CC	INT3
0040101C	CC	INT3
0040101D	CC	INT3
0040101E	CC	INT3
0040101F	CC	INT3
00401020	CC	INT3
00401021	CC	INT3
00401022	CC	INT3
00401023	CC	INT3
00401024	CC	INT3
00401025	CC	INT3
00401026	CC	INT3
00401027	CC	INT3
00401028	CC	INT3

이런게 나온다

그럼 f8로 한 단계씩 실행 해보자

0040104F	. FF15 68B14300	CALL DWORD PTR DS:[<&KERNEL32.Sleep>]	L Sleep
00401055	. 3BF4	CMP ESI,ESP	
00401057	. E8 B4710000	CALL 04.00408210	
0040105C	. 8BF4	MOV ESI,ESP	
0040105E	. FF15 64B14300	CALL DWORD PTR DS:[<&KERNEL32.IsDebuggerPresent>]	L IsDebuggerPresent
00401064	. 3BF4	CMP ESI,ESP	
00401066	. E8 A5710000	CALL 04.00408210	
0040106B	. 85C0	TEST EAX,EAX	
0040106D	. 74 0F	JE SHORT 04.0040107E	
0040106F	. 68 24104300	PUSH 04.00431024	[Arg1 = 00431024
00401074	. E8 17710000	CALL 04.00408190	04.00408190
00401079	. 83C4 04	ADD ESP,4	
0040107C	. EB 0D	JMP SHORT 04.0040108B	

그러면 여기서 isDebuggerPresent 라는 함수가 실행되고

밑에서 비교하여서 디버깅당함 을 출력해준다

따라서 디버거를 탐지하는 함수의 이름은 isDebuggerPresent 이다!