

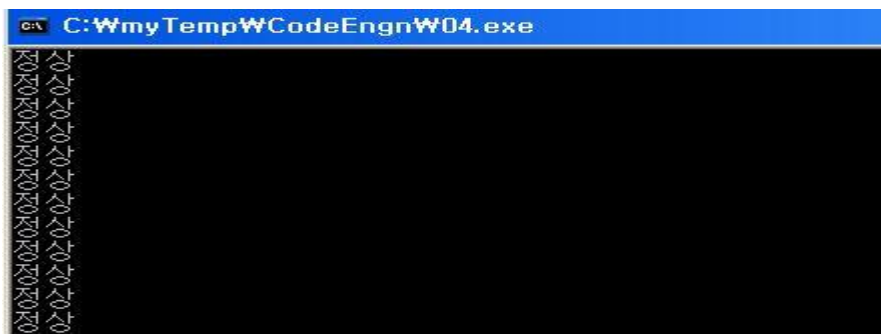
Basic 04 풀이

[문제]

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

1. 프로그램 실행하여 기능 확인

04.exe를 실행시키면 아래와 같이 나온다.



하지만 OllyDbg를 통해서 실행시키면 아래와 같이 '디버깅 당함'이라고 나온다. 프로그램이 디버깅을 당하고 있는지 탐지하는 기능을 가지고 있다.



2. Step by Step

프로그램을 순차적으로 진행해 나가면서 특정 함수를 호출후 '정상' 또는 '디버깅 당함' 문자열을 출력하는 분기점을 발견하였다.

아래 그림에서 IsDebuggerPresent 함수 호출후 출력문의 분기가 이루어 지는 것을 확인할 수 있다.

00401057	E8 B4710000	CALL 04.00408210	
0040105C	8BF4	MOV ESI,ESP	
0040105E	FF15 64B14300	CALL DWORD PTR DS:[<&KERNEL32.IsDebuggerPresent>]	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	
0040107E	68 1C104300	PUSH 04.0043101C	Arg1 = 0043101C
00401083	E8 08710000	CALL 04.00408190	04.00408190
00401088	83C4 04	ADD ESP,4	
0040108D	EB 0D	JMP SHORT 04.00401094	
00431024=04.00431024			

Address	Hex dump	ASCII		
00431024	B5 F0 B9 F6 B1 EB 20 B4 E7 C7 D4 20 0A 00 00 00	디버깅 당함		0012FF34 7C940
00431034	C8 28 43 00 D0 2D 40 00 00 00 00 00 04 00 00 00	?C.?@.....		0012FF38 FFFFFFF
00431044	30 29 43 00 10 2E 40 00 80 29 43 00 40 2E 40 00	0)C.!.@.)C.@.		0012FF3C 7FFDD
00431054	00 00 00 00 08 00 00 00 E8 29 43 00 B0 2E 40 00?C.?@.		0012FF40 CCCCC
				0012FF44 CCCCC

따라서 이번 문제의 답은 IsDebuggerPresent 이다.

- End -