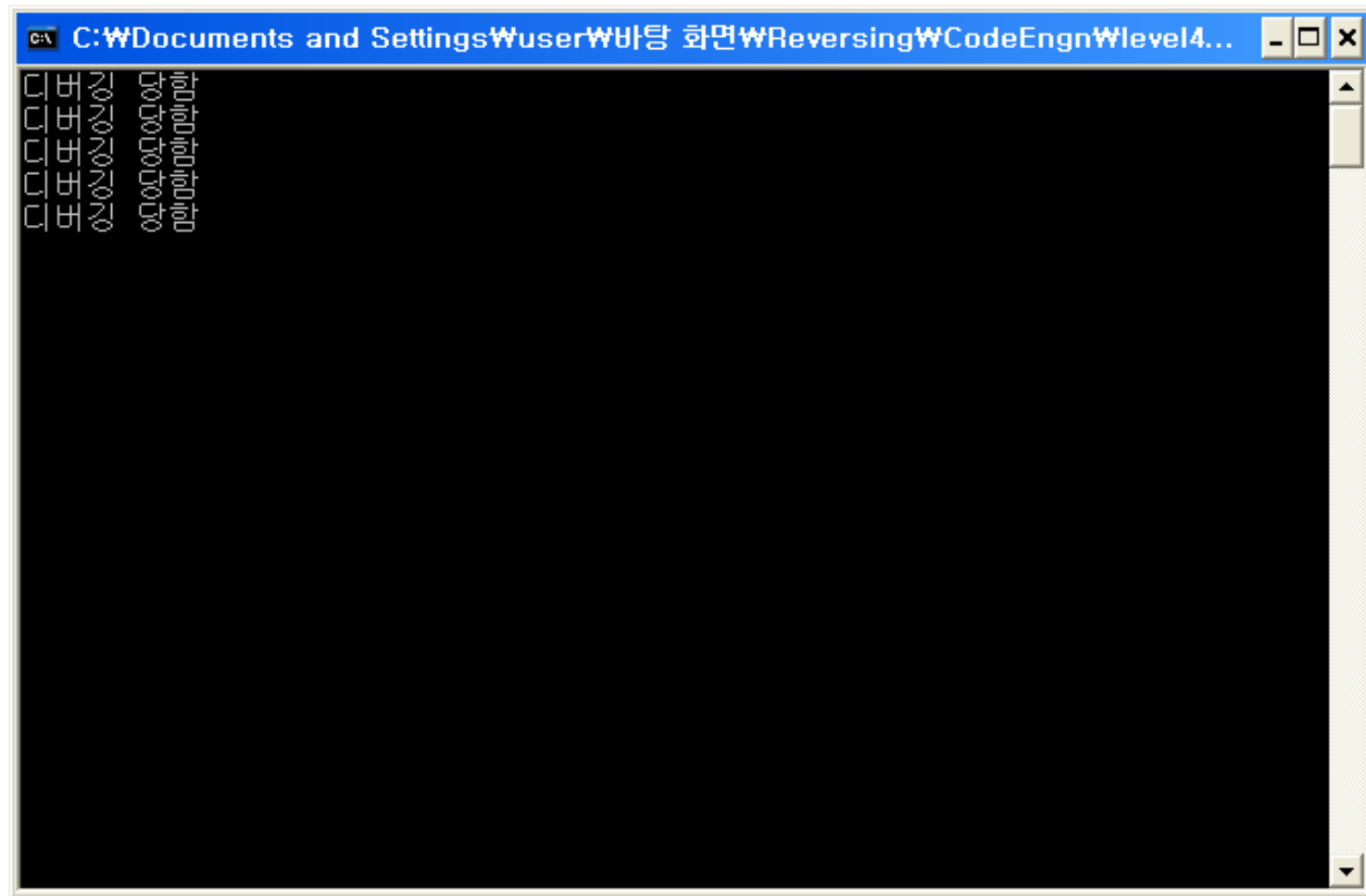


CODE ENGN level4

문제 풀이

STEP 1. 프로그램 동작



디버깅해고 뒤편 말후에그살행했했을경우

STEP2. 문제 파악

문제의 프로그램의 동작 중 에 스스로 디버기가 됐는지 그렇지 않은지 확인하는 기능을 가지고 있다.

MSDN에서 정의하고 있는 디버깅을 당하고 있는지 확인할수 있는 함수는 다음이 있다.

1. IsDebuggerPresent()
2. CheckRemoteDebuggerPresent()

00401030	>	55	PUSH EBP	
00401031	.	8BEC	MOV EBP,ESP	
00401033	.	83EC 40	SUB ESP,40	
00401036	.	53	PUSH EBX	
00401037	.	56	PUSH ESI	
00401038	.	57	PUSH EDI	
00401039	.	8D7D C0	LEA EDI,DWORD PTR SS:[EBP-40]	
0040103C	.	B9 10000000	MOV ECX,10	
00401041	.	B8 CCCCCCCC	MOV EAX,CCCCCCCC	
00401046	.	F3:AB	REP STOS DWORD PTR ES:[EDI]	
00401048	>	8BF4	MOV ESI,ESP	
0040104A	.	68 E8030000	PUSH 3E8	
0040104F	.	FF15 68B14300	CALL DWORD PTR DS:[<&KERNEL32.Sleep>]	[Timeout = 1000. ms Sleep
00401055	.	3BF4	CMP ESI,ESP	
00401057	.	E8 B4710000	CALL AFA7AD21.00408210	
0040105C	.	8BF4	MOV ESI,ESP	
0040105E	.	FF15 64B14300	CALL DWORD PTR DS:[<&KERNEL32.IsDebuggerPresent>]	IsDebuggerPresent
00401064	.	3BF4	CMP ESI,ESP	
00401066	.	E8 A5710000	CALL AFA7AD21.00408210	
0040106B	.	85C0	TEST EAX,EAX	
0040106D	✓	74 0F	JE SHORT AFA7AD21.0040107E	
0040106F	.	68 24104300	PUSH AFA7AD21.00431024	[Arg1 = 00431024
00401074	.	E8 17710000	CALL AFA7AD21.00408190	AFA7AD21.00408190
00401079	.	83C4 04	ADD ESP,4	
0040107C	✓	EB 0D	JMP SHORT AFA7AD21.0040108B	
0040107E	>	68 1C104300	PUSH AFA7AD21.0043101C	[Arg1 = 0043101C
00401083	.	E8 08710000	CALL AFA7AD21.00408190	AFA7AD21.00408190
00401088	.	83C4 04	ADD ESP,4	
0040108B	✓	EB BB	JMP SHORT AFA7AD21.00401048	

그리고 프로그램을 시작시키게 되면

무한 루프

00401030	> 55	PUSH EBP	
00401031	. 8BEC	MOV EBP,ESP	
00401033	. 83EC 40	SUB ESP,40	
00401036	. 53	PUSH EBX	
00401037	. 56	PUSH ESI	
00401038	. 57	PUSH EDI	
00401039	. 8D7D C0	LEA EDI,DWORD PTR SS:[EBP-40]	
0040103C	. B9 10000000	MOV ECX,10	
00401041	. B8 CCCCCCCC	MOV EAX,CCCCCCCC	
00401046	. F3:AB	REP STOS DWORD PTR ES:[EDI]	
00401048	> 8BF4	MOV ESI,ESP	
0040104A	. 68 E8030000	PUSH 3E8	
0040104F	. FF15 68B14300	CALL DWORD PTR DS:[<&KERNEL32.Sleep>]	[Timeout = 1000. ms Sleep
00401055	. 3BF4	CMP ESI,ESP	
00401057	. E8 B4710000	CALL AFA7AD21.00408210	
0040105C	. 8BF4	MOV ESI,ESP	
0040105E	. FF15 64B14300	CALL DWORD PTR DS:[<&KERNEL32.IsDebuggerPresent>]	[IsDebuggerPresent
00401064	. 3BF4	CMP ESI,ESP	
00401066	. E8 A5710000	CALL AFA7AD21.00408210	
0040106B	. 85C0	TEST EAX,EAX	
0040106D	. 74 0F	JE SHORT AFA7AD21.0040107E	
0040106F	. 68 24104300	PUSH AFA7AD21.00431024	[Arg1 = 00431024 AFA7AD21.00408190
00401074	. E8 17710000	CALL AFA7AD21.00408190	
00401079	. 83C4 04	ADD ESP,4	
0040107C	. EB 0D	JMP SHORT AFA7AD21.0040108B	
0040107E	. 68 1C104300	PUSH AFA7AD21.0043101C	[Arg1 = 0043101C AFA7AD21.00408190
00401083	. E8 08710000	CALL AFA7AD21.00408190	
00401088	. 83C4 04	ADD ESP,4	
0040108B	. EB BB	JMP SHORT AFA7AD21.00401048	

위 내용을 분석해보면 무한 루프를 돌면서

1초에 한번씩

디버깅을 당하는지 확인을 하면서

조건부 분기문에 의해서

디버깅을 당하고 있다면 “디버깅당함”을 출력

그렇지 않다면 “정상”을 출력

무한 루프에 의해서 계속적으로 반복

STEP3. 문제 해결

<pre>> 8BF4 MOV ESI,ESP . 68 E8030000 PUSH 3E8 . FF15 68B14300 CALL DWORD PTR DS:[<&KERNEL32.Sleep>] . 3BF4 CMP ESI,ESP . E8 B4710000 CALL AFA7AD21.00408210 . 8BF4 MOV ESI,ESP . FF15 64B14300 CALL DWORD PTR DS:[<&KERNEL32.IsDebuggerPresent>] . 3BF4 CMP ESI,ESP . E8 A5710000 CALL AFA7AD21.00408210 . 85C0 TEST EAX,EAX . EB 0F JMP SHORT AFA7AD21.0040107E . 68 24104300 PUSH AFA7AD21.00431024 . E8 17710000 CALL AFA7AD21.00408190 . 83C4 04 ADD ESP,4 . EB 0D JMP SHORT AFA7AD21.0040108B > 68 1C104300 PUSH AFA7AD21.0043101C . E8 08710000 CALL AFA7AD21.00408190 . 83C4 04 ADD ESP,4 > EB BB JMP SHORT AFA7AD21.00401048</pre>	<pre>MOV ESI,ESP PUSH 3E8 CALL DWORD PTR DS:[<&KERNEL32.Sleep>] CMP ESI,ESP CALL AFA7AD21.00408210 MOV ESI,ESP CALL DWORD PTR DS:[<&KERNEL32.IsDebuggerPresent>] CMP ESI,ESP CALL AFA7AD21.00408210 TEST EAX,EAX JMP SHORT AFA7AD21.0040107E PUSH AFA7AD21.00431024 CALL AFA7AD21.00408190 ADD ESP,4 JMP SHORT AFA7AD21.0040108B PUSH AFA7AD21.0043101C CALL AFA7AD21.00408190 ADD ESP,4 JMP SHORT AFA7AD21.00401048</pre>	<pre>[Timeout = 1000. ms Sleep IsDebuggerPresent Arg1 = 00431024 AFA7AD21.00408190 Arg1 = 0043101C AFA7AD21.00408190</pre>
---	--	---

그리고 해결방법으로는 조건 분기가 아닌 무조건 분기로 바꿔주면된다.

이것으로 문제의 정답인 디버거를 탐지하는 함수의 이름은
IsDebuggerPresent();