

REPORT:

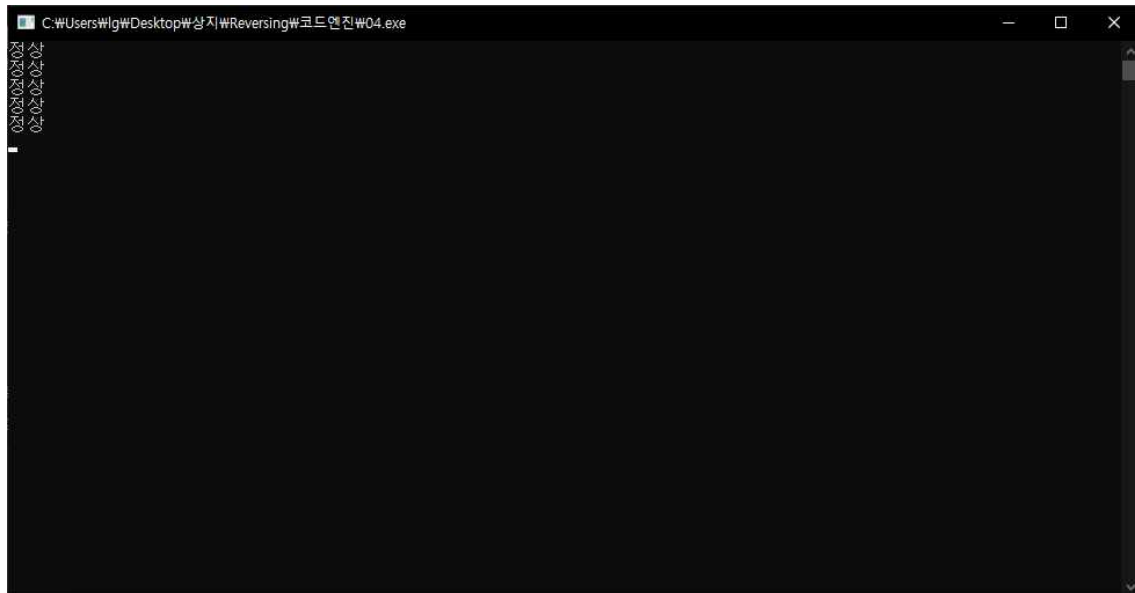
코드엔진 Basic

RCE 04 Writeup

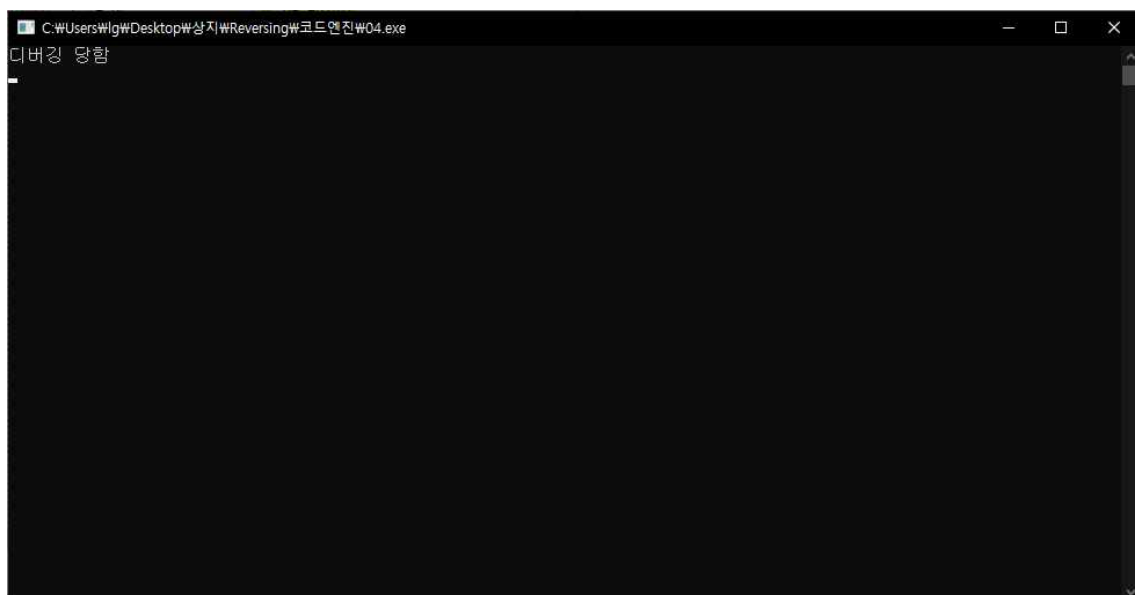
COLONY
1824275 정상지

2021.05.23

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



4번 프로그램 동작 시 출력



x32dbg를 이용하여 디버깅 시 출력

00401046	F3:AB	rep stosd	
00401047	8BF4	mov esi,esp	
0040104A	68 E8030000	push 3E8	
0040104F	FF15 68B14300	call dword ptr ds:[<&Sleep>]	
00401055	3BF4	cmp esi,esp	
00401057	E8 B4710000	call 04.408210	
0040105C	8BF4	mov esi,esp	
0040105E	FF15 64B14300	call dword ptr ds:[<&IsDebuggerPresent>]	현재 디버깅 프로그램으로 실행하는지 확인
00401064	3BF4	cmp esi,esp	
00401066	E8 A5710000	call 04.408210	
00401068	85C0	test eax,eax	
0040106D	74 0F	je 04.40107E	
0040106F	68 24104300	push 04.431024	431024: "디버깅 당함 \n"
00401074	E8 17710000	call 04.408190	
00401079	83C4 04	add esp,4	
0040107C	EB 0D	jmp 04.401088	
0040107E	68 1C104300	push 04.43101C	43101C: "정상 \n"
00401083	E8 08710000	call 04.408190	
00401088	83C4 04	add esp,4	
00401088	EB BB	jmp 04.401048	
0040108D	CC	int3	
0040108E	CC	int3	
0040108F	CC	int3	

“정상” / “디버깅 당함” --> <&IsDebuggerPresent>을 통해 현재 디버깅 프로그램을 실행하는지 확인하여 정상/디버깅당함 출력

이 프로그램에서 디버거 프로그램을 탐지하는 함수는 <&IsDebuggerPresent> 이다