

코드엔진 Basic RCE L04

문제

CodeEngn.com [코드엔진]

코드엔진은 국내 리버스엔지니어링 정보공유를 위해 2007년 부터 리버스엔지니어링 컨퍼런스 및 세미나, 워크숍을
현업 실무자들과 함께 운영하고 있는 비영리 커뮤니티입니다.

 <https://ch.codeengn.com/>

의 Basic RCE L04

해결 과정

- startUp 코드의 형식을 이용하여 main 함수를 찾음

PUSH EDX	04.<ModuleEntryPoint>
MOV EAX, DWORD PTR DS:[438940]	
PUSH EAX	kernel32.BaseThreadInitThunk
MOV ECX, DWORD PTR DS:[43893C]	
PUSH ECX	
CALL 0040100F	
ADD ESP, 0C	
MOV [LOCAL.7], EAX	kernel32.BaseThreadInitThunk
MOV EDX, [LOCAL.7]	
PUSH EDX	04.<ModuleEntryPoint>

빨간 선 박스안에 있는 코드가 main 함수를 CALL 하는 코드

- main함수에서 IsDebuggerPresent라는 이름의 정답으로 추측되는 함수를 발견

00401055	. 3BF4	CMP ESI, ESP	
00401057	. E8 B4710000	CALL 00408210	
0040105C	. 8BF4	MOV ESI, ESP	
0040105E	. FF15 64B1430	CALL DWORD PTR DS:[&KERNEL32.IsDebuggerPresent]	IsDebuggerPresent
00401064	. 3BF4	CMP ESI, ESP	
00401066	. E8 A5710000	CALL 00408210	
0040106B	. 85C0	TEST EAX, EAX	

빨간 선 박스안에 있는 코드가 IsDebuggerPresent를 CALL 하는 코드

- IsDebuggerPresent 함수를 CALL한 이후에 문자열이 나타나고 다시
IsDebuggerPresent 함수의 위로 JUMP 하는 것을 보아 IsDebuggerPresent 함수가
실제 찾는 함수임을 파악하여 해결

실행 흐름

- IsDebuggerPresent 함수를 사용하여 현재 실행파일의 프로세스가 디버깅 되고 있는지 확인
- 디버깅 되고 있을 경우 '디버깅 당함' 문자열을 띄우고 디버깅 되고 있지 않을 경우 '정상' 문자열을 띄움
- 이를 계속 반복