

REPORT:

코드엔진 Basic

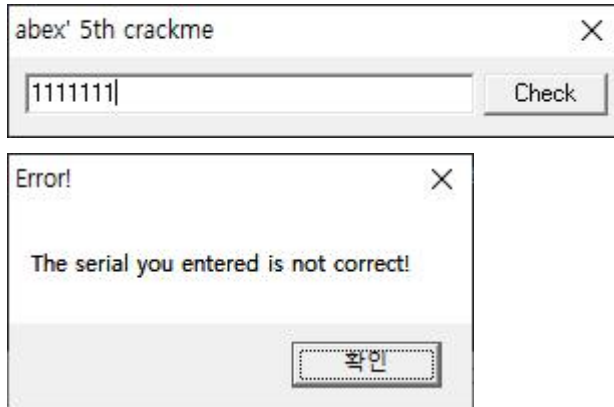
RCE 07 Writeup

COLONY
1824275 정상지

2021.05.30

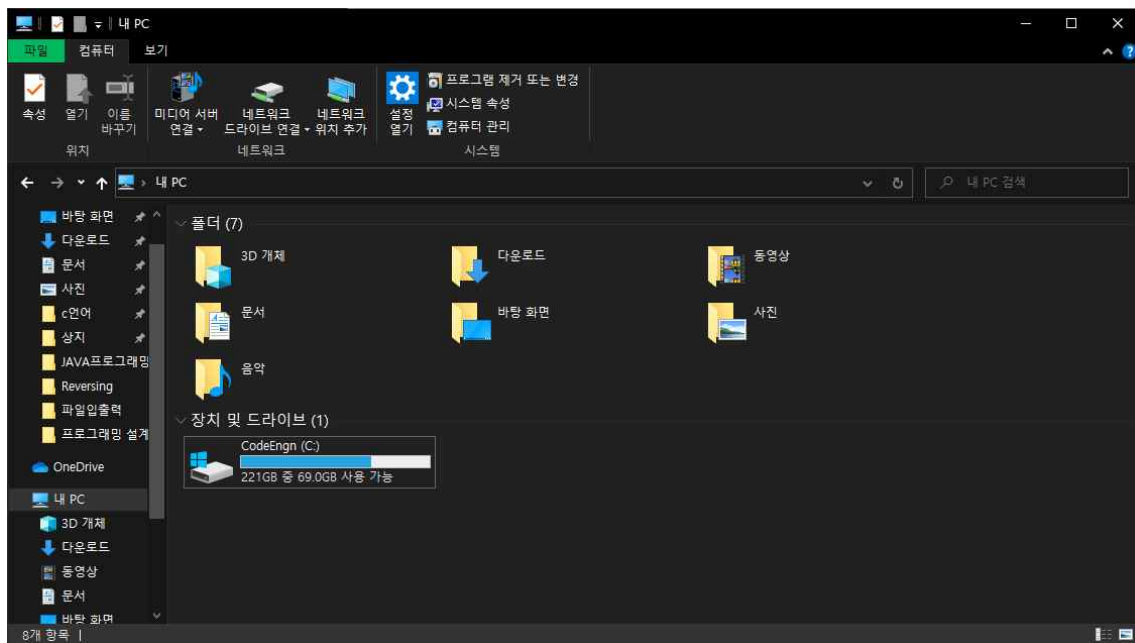
컴퓨터 C 드라이브의 이름이 CodeEngn 일경우 시리얼이 생성될때 CodeEngn은 '8어떤것'으로 변경되는가

해당 프로그램 실행시 시리얼 입력 창이 나타나고 무작위 시리얼을 입력했을 경우의 모습



PE구조 확인 결과 따로 패킹되어있지않았다

컴퓨터 C드라이브 이름을 codeengn으로 변경 후 디버깅



문자열 참조를 통해 메시지 박스에서 출력되는 문자열을 따라감

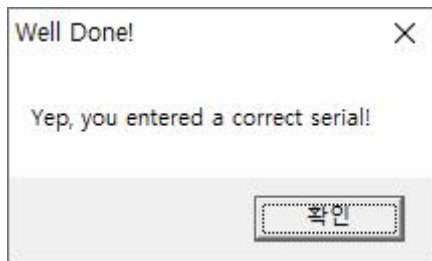
00401069	C2 1000	ret 10	
0040106C	6A 25	push 25	
0040106E	68 24234000	push 07.402324	
00401073	6A 68	push 68	
00401075	FF75 08	push dword ptr ss:[ebp+8]	
00401078	E8 F4000000	call <JMP.&GetDigitItemTextA>	
0040107D	6A 00	push 0	
0040107F	6A 00	push 0	
00401081	68 C8204000	push 07.4020C8	
00401086	68 90214000	push 07.402190	
00401088	68 94214000	push 07.402194	
00401090	6A 32	push 32	
00401092	68 5C224000	push 07.40225C	
00401097	6A 00	push 0	
00401099	E8 85000000	call <JMP.&GetVolumeInformationA>	
0040109E	68 F3234000	push 07.4023F3	4023F3:"4562-ABEX"
004010A3	68 5C224000	push 07.40225C	
004010A8	E8 94000000	call <JMP.&strcatA>	
004010AD	B2 02	mov dl,2	
004010AF	8305 5C224000 01	add dword ptr ds:[40225C],1	
004010B6	8305 5D224000 01	add dword ptr ds:[40225D],1	
004010BD	8305 5E224000 01	add dword ptr ds:[40225E],1	
004010C4	8305 5F224000 01	add dword ptr ds:[40225F],1	
004010C8	FECA	dec dl	
004010CD	75 E0	jne 07.4010AF	
004010CF	68 FD234000	push 07.4023FD	4023FD:"L2C-5781"
004010D4	68 00204000	push 07.402000	
004010D9	E8 63000000	call <JMP.&strcatA>	
004010DE	68 5C224000	push 07.40225C	
004010E3	68 00204000	push 07.402000	
004010E8	E8 54000000	call <JMP.&strcatA>	
004010ED	68 24234000	push 07.402324	
004010F2	68 00204000	push 07.402000	
004010F7	E8 51000000	call <JMP.&strcmpA>	
004010FF	83F8 00	cmp eax,0	
00401101	74 16	je 07.401117	
00401103	6A 00	push 0	
00401108	68 34244000	push 07.402434	402434:"Error!"
0040110D	FF75 08	push dword ptr ss:[ebp+8]	402438:"The serial you entered is not correct!"
00401110	E8 56000000	call <JMP.&MessageBoxA>	
00401115	E8 16	jmp 07.40112D	
00401117	6A 00	push 0	
00401119	68 06244000	push 07.402406	402406:"Well done!"
0040111E	68 11244000	push 07.402411	402411:"Yep, you entered a correct serial!"
00401123	FF75 08	push dword ptr ss:[ebp+8]	
00401126	E8 40000000	call <JMP.&MessageBoxA>	
0040112B	E8 00	jmp 07.40112D	
0040112D	6A 00	push 0	

cmp에 breakpoint 설정 후 디버깅

00401053	C2 1000	ret 10	
00401056	837D 10 65	cmp dword ptr ss:[ebp+10],65	65:'e'
0040105A	74 10	je 07.40106C	
0040105C	837D 10 02	cmp dword ptr ss:[ebp+10],2	
00401060	0F84 C7000000	je 07.40112D	
00401066	33C0	xor eax,eax	
00401068	C9	leave	
00401069	C2 1000	ret 10	
0040106C	6A 25	push 25	
0040106E	68 24234000	push 07.402324	402324:"Enter your serial"
00401073	6A 68	push 68	
00401075	FF75 08	push dword ptr ss:[ebp+8]	
00401078	E8 F4000000	call <JMP.&GetDigitItemTextA>	
0040107D	6A 00	push 0	
0040107F	6A 00	push 0	
00401081	68 C8204000	push 07.4020C8	
00401086	68 90214000	push 07.402190	
00401088	68 94214000	push 07.402194	
00401090	6A 32	push 32	
00401092	68 5C224000	push 07.40225C	40225C:"EqfgEngn4562-ABEX"
00401097	6A 00	push 0	
00401099	E8 85000000	call <JMP.&GetVolumeInformationA>	
0040109E	68 F3234000	push 07.4023F3	4023F3:"4562-ABEX"
004010A3	68 5C224000	push 07.40225C	40225C:"EqfgEngn4562-ABEX"
004010A8	E8 94000000	call <JMP.&strcatA>	
004010AD	B2 02	mov dl,2	
004010AF	8305 5C224000 01	add dword ptr ds:[40225C],1	0040225C:"EqfgEngn4562-ABEX"
004010B6	8305 5D224000 01	add dword ptr ds:[40225D],1	0040225D:"gfgEngn4562-ABEX"
004010BD	8305 5E224000 01	add dword ptr ds:[40225E],1	0040225E:"fgEngn4562-ABEX"
004010C4	8305 5F224000 01	add dword ptr ds:[40225F],1	0040225F:"gEngn4562-ABEX"
004010C8	FECA	dec dl	
004010CD	75 E0	jne 07.4010AF	
004010CF	68 FD234000	push 07.4023FD	4023FD:"L2C-5781"
004010D4	68 00204000	push 07.402000	402000:"L2C-5781EqfgEngn4562-ABEX"
004010D9	E8 63000000	call <JMP.&strcatA>	
004010DE	68 5C224000	push 07.40225C	40225C:"EqfgEngn4562-ABEX"
004010E3	68 00204000	push 07.402000	402000:"L2C-5781EqfgEngn4562-ABEX"
004010E8	E8 54000000	call <JMP.&strcatA>	
004010ED	68 24234000	push 07.402324	
004010F2	68 00204000	push 07.402000	
004010F7	E8 51000000	call <JMP.&strcmpA>	
004010FF	83F8 00	cmp eax,0	
00401101	74 16	je 07.401117	
00401103	6A 00	push 0	
00401108	68 34244000	push 07.402434	402434:"Error!"
0040110D	FF75 08	push dword ptr ss:[ebp+8]	402438:"The serial you entered is not correct!"
00401110	E8 56000000	call <JMP.&MessageBoxA>	
00401115	E8 16	jmp 07.40112D	
00401117	6A 00	push 0	

cmp 이전의 L2C-5781EqfgEngn4562-ABEX를 프로그램 키에 입력

abex' 5th crackme



성공!

CodeEngn으로 C드라이브 이름을 변경할 시 L2C-5781EqfgEngn4562-ABEX로 해결할 수 있다