

# BASIC RCE Level 7

**CodeEngn**  
ReverseEngineering Conference

2013 07/27

[Malcook90@naver.com](mailto:Malcook90@naver.com)

## Challenges : Basic 07

Author : abex

Korea :

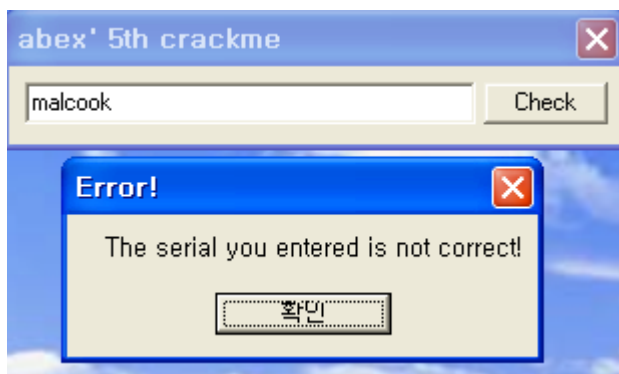
컴퓨터 C 드라이브의 이름이 CodeEngn 일경우 시리얼이 생성될때 CodeEngn은 "어떤것"으로 변경되는가

English :

Assuming the drive name of C is CodeEngn, what does CodeEngn transform into in the process of the serial construction

C드라이브의 이름에 따라 Serial Key을 생성하는 프로그램

이라는 것을 유추 해 볼 수 있다.



임의의 값을 넣어준 결과

Error! 라는 MessageBox 을 값을 띄어준다.

String 값으로 접근하면 쉽게 찾을 수 있을 거 같다.

Address	Disassembly	Text string
00401000	PUSH 0	(Initial CPU selection)
0040109E	PUSH 07.004023F3	ASCII "4562-ABEX"
004010CF	PUSH 07.004023FD	ASCII "L2C-5781"
00401103	PUSH 07.00402434	ASCII "Error!"
00401108	PUSH 07.0040243B	ASCII "The serial you entered is not correct!"
00401119	PUSH 07.00402406	ASCII "Well Done!"
0040111E	PUSH 07.00402411	ASCII "Yep, you entered a correct serial!"

String 값을 추출한 결과

우리가 띄어줘야 할 값이 한눈에 들어 온다.

더블클릭 하고 이동해 보자.

00401099	E8 B5000000	CALL <JMP.&KERNEL32.GetVolumeInformationA>	GetVolumeInformationA
0040109E	68 F3234000	PUSH 07.004023F3	StringToAdd = "4562-ABEX"
004010A3	68 5C224000	PUSH 07.0040225C	ConcatString = "EqfgEngn4562-ABEX"
004010A8	E8 94000000	CALL <JMP.&KERNEL32.lstrcatA>	lstrcatA
004010AD	B2 02	MOV DL,2	
004010B6	8305 5C224000	ADD DWORD PTR DS:[40225C],1	
004010BB	8305 5D224000	ADD DWORD PTR DS:[40225D],1	
004010B0	8305 5E224000	ADD DWORD PTR DS:[40225E],1	
004010C4	8305 5F224000	ADD DWORD PTR DS:[40225F],1	
004010C8	FECA	DEC DL	
004010CD	75 E0	JNZ SHORT 07.004010AF	
004010CF	68 FD234000	PUSH 07.004023FD	StringToAdd = "L2C-5781"
004010D4	68 00204000	PUSH 07.00402000	ConcatString = "L2C-5781EqfgEngn4562-ABEX"
004010D9	E8 63000000	CALL <JMP.&KERNEL32.lstrcatA>	lstrcatA
004010DE	68 5C224000	PUSH 07.0040225C	StringToAdd = "EqfgEngn4562-ABEX"
004010E3	68 00204000	PUSH 07.00402000	ConcatString = "L2C-5781EqfgEngn4562-ABEX"
004010E8	E8 54000000	CALL <JMP.&KERNEL32.lstrcatA>	lstrcatA
004010ED	68 24234000	PUSH 07.00402324	String2 = "1234"
004010F2	68 00204000	PUSH 07.00402000	String1 = "L2C-5781EqfgEngn4562-ABEX"
004010F7	E8 51000000	CALL <JMP.&KERNEL32.lstrcmpA>	lstrcmpA
004010FC	83F8 00	CMP EAX,0	
004010FF	74 16	JE SHORT 07.00401117	
00401101	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
00401103	68 34244000	PUSH 07.00402434	Title = "Error!"
00401108	68 3B244000	PUSH 07.0040243B	Text = "The serial you entered is not correct!"
0040110D	FF75 08	PUSH DWORD PTR SS:[EBP+8]	hOwner
00401110	E8 56000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
00401115	EB 16	JMP SHORT 07.0040112D	
00401117	6A 00	PUSH 0	Style = MB_OK!MB_APPLMODAL
00401119	68 06244000	PUSH 07.00402406	Title = "Well Done!"
0040111E	68 11244000	PUSH 07.00402411	Text = "Yep, you entered a correct serial!"
00401123	FF75 08	PUSH DWORD PTR SS:[EBP+8]	hOwner
00401126	E8 40000000	CALL <JMP.&USER32.MessageBoxA>	MessageBoxA
0040112B	EB 00	JMP SHORT 07.0040112D	
0040112D	6A 00	PUSH 0	Result = 0
0040112F	FF75 08	PUSH DWORD PTR SS:[EBP+8]	hWnd
00401132	E8 22000000	CALL <JMP.&USER32.EndDialog>	EndDialog
00401137	C9	LEAVE	
00401138	C2 1000	RETN 10	

CodeEngn(C:W) 앞 4자리 +2씩 증가

먼저 프로그램의 구조를 알아보자

GetVolumeInformationA 함수에 BP을 걸고 실행시켜 보면

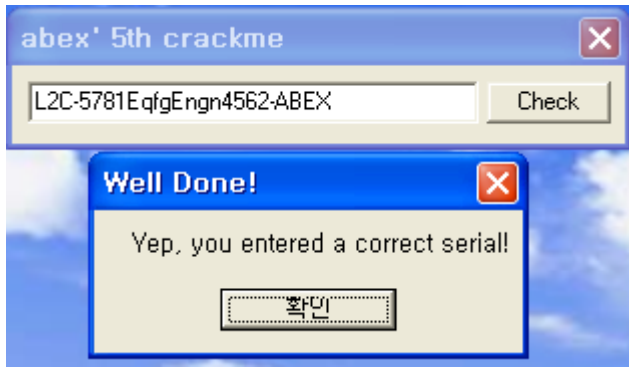
StringToAdd 에 있는 값과 C드라이브에 있는 값이 합쳐지는 것을 볼 수 있다  
(현재 C Drive Name -> CodeEngn)

그리고 2회 Loop 문으로 앞에 4글자(Code) 값을 +2 씩 증가 시키고

다음 StringToAdd(L2C-5781) 하고자 합쳐지는 것을 볼 수 있다.

그 후 임의로 입력한 값 String2 = "1234" 와 String1 값을

CMP 하여 JE로 점프 하는 것을 볼 수 있다.



Serial Key을 알았으니

이제 맞는지 확인!!!

Well Done! MessageBox 을 띄어주면서 잘 됩니다.