

Basic RCE L18

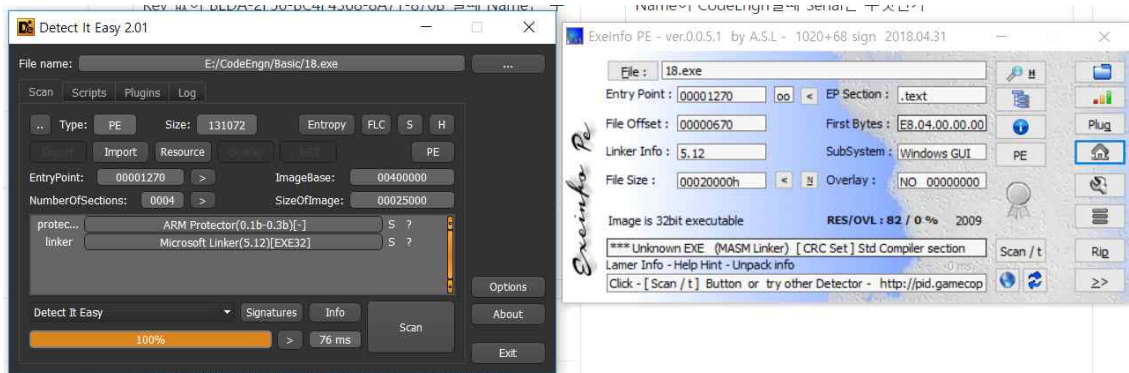
Name이 CodeEngn일때 Serial은 무엇인가

— Author: Xsp!d3r

— File Password: codeengn

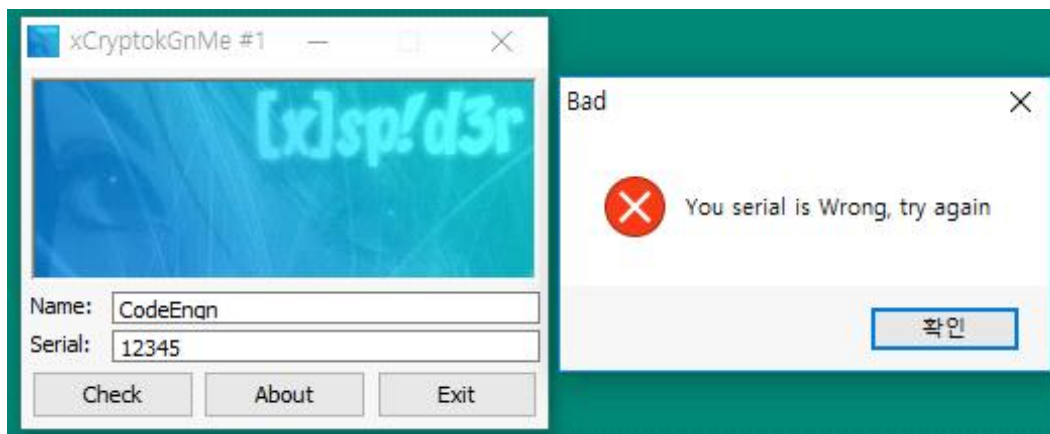


Serial문제!



Exeinfo PE로는 Unknown EXE라고 나오고 Detect It easy에서는 ARM Prtotector라는 프로텍터로 팩되어있다. 구글에 ARM Protector라고 검색하니 팔보호대만 나온다.

우선 CodeEngn과 12345를 입력



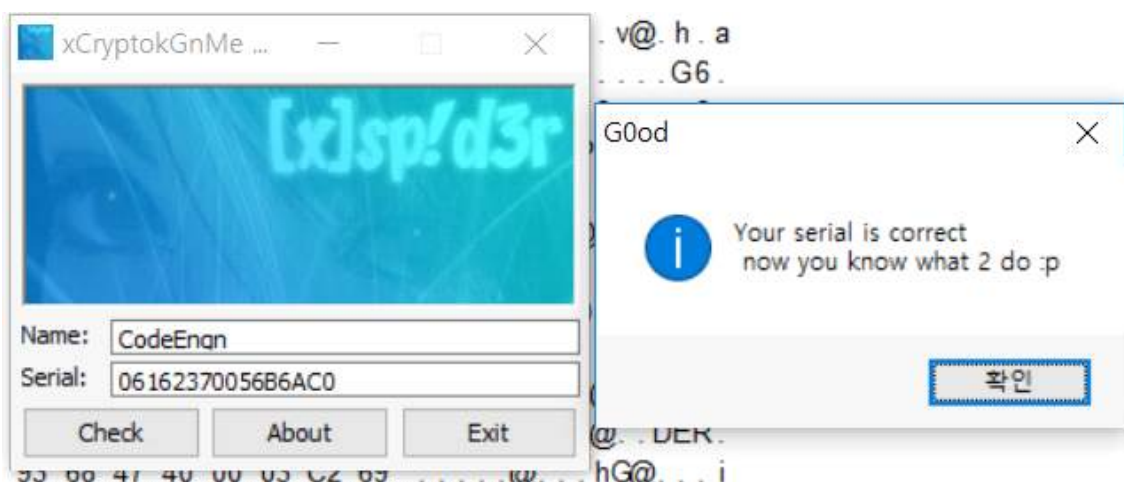
문자열을 따라가본다.

문자열
"xCryptokGnMe #1"
"Name must be at least 5 chars or more..."
"Xsp!d3r // RED Crew"
"Xsp!d3r // RED Crew"
"%.8X%.8X"
"%.8X%.8X"
"Bad"
"You serial is wrong, try again"
"Good"
"Your serial is correct\r\n now you know what 2 do :p"
"About"

분기문쪽 함수를 보니 strcmpiA라는 문자열 비교함수를 찾았다.

그쪽에 breakpoint를 걸고 실행시키니 바로 Serial이 나온다.

004011D8	68 EC 03 00 00	push 3EC	
004011DD	FF 75 08	push dword ptr ss:[ebp+8]	
004011E0	E8 01 01 00 00	call <JMP.&GetDlgItemTextA>	
004011E5	68 F0 80 40 00	push 18.4080F0	
004011EA	68 F0 7E 40 00	push 18.407E40	
004011F5	E8 DA 00 00 00	call <JMP.&strcmpiA>	
004011F4	08 C0	or eax, eax	
004011F6	74 16	je 18.40120E	
004011F8	6A 10	push 10	
004011FA	68 04 66 40 00	push 18.406604	
004011FF	68 E4 65 40 00	push 18.4065E4	406604: "Bad"
00401204	FF 75 08	push dword ptr ss:[ebp+8]	4065E4: "You serial is wrong, try again"
00401207	E8 E6 00 00 00	call <JMP.&MessageBoxA>	
0040120C	EB 5C	jmp 18.40126A	
0040120E	6A 40	push 40	
00401210	68 3C 66 40 00	push 18.40663C	40663C: "Good"
00401215	68 08 66 40 00	push 18.406608	406608: "Your serial is correct\r\n now you
0040121A	FF 75 08	push dword ptr ss:[ebp+8]	
0040121D	E8 D0 00 00 00	call <JMP.&MessageBoxA>	
00401222	C9	leave	
00401223	C2 10 00	ret 10	
00401226	EB 42	jmp 18.40126A	
00401228	66 3D EA 03	cmp ax, 3EA	
0040122C	75 16	jne 18.401244	
0040122E	6A 00	push 0	
00401230	68 00 60 40 00	push 18.406000	406000: "About"
00401235	68 06 60 40 00	push 18.406006	
0040123A	FF 75 08	push dword ptr ss:[ebp+8]	
0040123D	E8 D0 00 00 00	call <JMP.&MessageBoxA>	
004011E0	E8 01 01 00 00	call <JMP.&GetDlgItemTextA>	
004011E5	68 F0 80 40 00	push 18.4080F0	4080F0: "06162370056B6AC0"
004011EA	68 F0 7E 40 00	push 18.407E40	407E40: "12345"
004011F5	E8 DA 00 00 00	call <JMP.&strcmpiA>	
004011F4	08 C0	or eax, eax	
004011F6	74 16	je 18.40120E	
004011F8	6A 10	push 10	
004011FA	68 04 66 40 00	push 18.406604	406604: "Bad"
004011FF	68 E4 65 40 00	push 18.4065E4	4065E4: "You serial is wrong, try again"
00401204	FF 75 08	push dword ptr ss:[ebp+8]	
00401207	E8 E6 00 00 00	call <JMP.&MessageBoxA>	
0040120C	EB 5C	jmp 18.40126A	
0040120E	6A 40	push 40	
00401210	68 3C 66 40 00	push 18.40663C	40663C: "Good"
00401215	68 08 66 40 00	push 18.406608	406608: "Your serial is correct\r\n now you
0040121A	FF 75 08	push dword ptr ss:[ebp+8]	



Clear ARM프로텍터 때문에 겁먹었는데 뭘 보호해주는건지....