

2019.02.14. CodeEngn basic RCE L06

Tree to Tree

Basic RCE L07

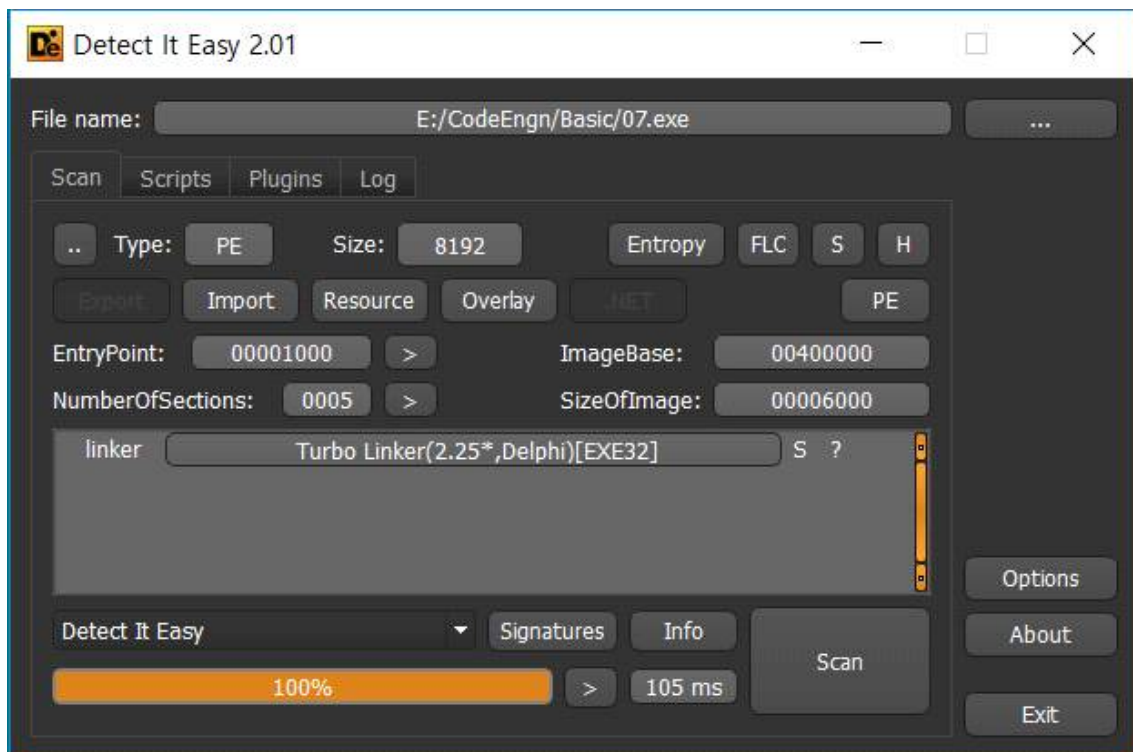
컴퓨터 C 드라이브의 이름이 CodeEngn 일경우 시리얼이 생성
될때 CodeEngn은 'ß어떤것'으로 변경되는가

— Author: abex

— File Password: codeengn



이번에도 시리얼 번호 찾기
패킹이 따로 되어있지 않다.



열심히 트레이싱을 하다보니

소프트웨어	주소	내용	비고	값	비고
00401099	<07.exe.EntryPoint>	One-time 활성화됨	push 0	0	진입점 중단점
00401097	07.exe	활성화됨	call <JMP.&GetVolumeInformationA>	0	
			call <JMP.&IstrcmpA>	0	

이렇게 3가지의 breakpoint가 필요했다.

GetVolumeInformation함수에서
내 USB이름인 ESD-USB를 발견

ESP	0040109E	68 F3234000	push 07.4023F3	4023F3: "4562-ABEX"
	004010A3	68 5C224000	push 07.40225C	40225C: "ESD-USB"
	004010A8	E8 94000000	call <JMP.&Istrcat>	
	004010AD	82 02	mov d1,2	
	004010AF	8305 5C224000 01	add dword ptr ds:[40225C],1	0040225C: "ESD-USB"
	004010B6	8305 5D224000 01	add dword ptr ds:[40225D],1	0040225D: "SD-USB"
	004010BD	8305 5E224000 01	add dword ptr ds:[40225E],1	0040225E: "D-USB"
	004010C4	8305 5F224000 01	add dword ptr ds:[40225F],1	0040225F: "-USB"
	004010CB	FEC4	dec d1	
	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.&Istrcat>	
	004010DE	68 5C224000	push 07.40225C	40225C: "ESD-USB"
	004010E3	68 00204000	push 07.402000	
	004010E8	E8 54000000	call <JMP.&Istrcat>	
	004010ED	68 24234000	push 07.402324	402324: "hello"
	004010F2	68 00204000	push 07.402000	
	004010F7	E8 51000000	call <JMP.&IstrcmpA>	
	004010FC	83F8 00	cmp eax,0	
	004010FF	74 16	je 07.401117	
	00401101	6A 00	push 0	
	00401103	68 24244000	push 07.402434	402434: "Error!"
	00401108	68 3B244000	push 07.40243B	40243B: "The serial you entered is not corr
	0040110D	FF75 08	push dword ptr ss:[ebp+8]	
	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>	

ESD-USB -> FTE.USB

	0040109E	68 F3234000	push 07.4023F3	4023F3: "4562-ABEX"
	004010A3	68 5C224000	push 07.40225C	40225C: "FTE.USB4562-ABEX"
	004010A8	E8 94000000	call <JMP.&Istrcat>	
	004010AD	82 02	mov d1,2	
	004010AF	8305 5C224000 01	add dword ptr ds:[40225C],1	0040225C: "FTE.USB4562-ABEX"
	004010B6	8305 5D224000 01	add dword ptr ds:[40225D],1	0040225D: "TE.USB4562-ABEX"
	004010BD	8305 5E224000 01	add dword ptr ds:[40225E],1	0040225E: "E.USB4562-ABEX"
	004010C4	8305 5F224000 01	add dword ptr ds:[40225F],1	0040225F: ".USB4562-ABEX"
	004010CB	FEC4	dec d1	
	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.&Istrcat>	
	004010DE	68 5C224000	push 07.40225C	40225C: "FTE.USB4562-ABEX"
	004010E3	68 00204000	push 07.402000	
	004010E8	E8 54000000	call <JMP.&Istrcat>	
	004010ED	68 24234000	push 07.402324	402324: "hello"
	004010F2	68 00204000	push 07.402000	
	004010F7	E8 51000000	call <JMP.&IstrcmpA>	
	004010FC	83F8 00	cmp eax,0	
	004010FF	74 16	je 07.401117	
	00401101	6A 00	push 0	
	00401103	68 24244000	push 07.402434	402434: "Error!"
	00401108	68 3B244000	push 07.40243B	40243B: "The serial you entered is not corr
	0040110D	FF75 08	push dword ptr ss:[ebp+8]	
	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>	

FTE.USB -> GUF/USB 로 변환되는 모습을 보였고

중간중간 Istrcat으로 인해 4562-ABEX와 L2C-5781이라는 문자열이 추가되는 모습을 보임.

	0040109E	68 F3234000	push 07.4023F3	4023F3: "4562-ABEX"
	004010A3	68 5C224000	push 07.40225C	40225C: "GUF/USB4562-ABEX"
	004010A8	E8 94000000	call <JMP.&Istrcat>	
	004010AD	82 02	mov d1,2	
	004010AF	8305 5C224000 01	add dword ptr ds:[40225C],1	0040225C: "GUF/USB4562-ABEX"
	004010B6	8305 5D224000 01	add dword ptr ds:[40225D],1	0040225D: "UF/USB4562-ABEX"
	004010BD	8305 5E224000 01	add dword ptr ds:[40225E],1	0040225E: "F/USB4562-ABEX"
	004010C4	8305 5F224000 01	add dword ptr ds:[40225F],1	0040225F: "/USB4562-ABEX"
	004010CB	FEC4	dec d1	
	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.&Istrcat>	
	004010DE	68 5C224000	push 07.40225C	40225C: "GUF/USB4562-ABEX"
	004010E3	68 00204000	push 07.402000	
	004010E8	E8 54000000	call <JMP.&Istrcat>	
	004010ED	68 24234000	push 07.402324	402324: "hello"
	004010F2	68 00204000	push 07.402000	
	004010F7	E8 51000000	call <JMP.&IstrcmpA>	
	004010FC	83F8 00	cmp eax,0	
	004010FF	74 16	je 07.401117	
	00401101	6A 00	push 0	
	00401103	68 24244000	push 07.402434	402434: "Error!"
	00401108	68 3B244000	push 07.40243B	40243B: "The serial you entered is not corr
	0040110D	FF75 08	push dword ptr ss:[ebp+8]	
	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]	

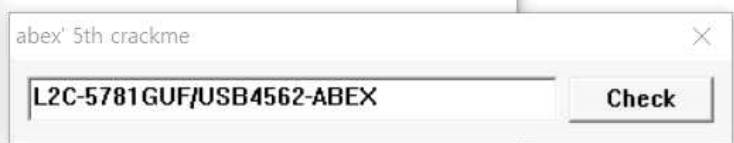
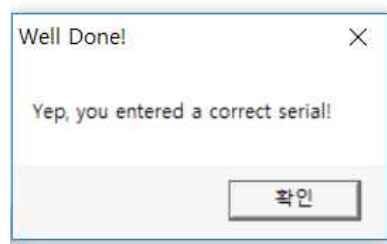
004010D9	E8 63000000	call <JMP.&Istrcat>	
004010DE	68 5C224000	push 07.40225C	40225C: "GUF/USB4562-ABEX"
004010E3	68 00204000	push 07.402000	402000: "L2C-5781"
004010E8	E8 54000000	call <JMP.&Istrcat>	
004010ED	68 24234000	push 07.402324	402324: "hello"
004010F2	68 00204000	push 07.402000	402000: "L2C-5781"
004010F8	E8 51000000	call <JMP.&Istrcmp1A>	
004010FC	83 F8 00	cmp eax, 0	eax: "L2C-5781"
004010FF	74 16	je 07.401117	
00401101	6A 00	push 0	
00401103	68 34244000	push 07.402434	402434: "Error!"
00401108	68 3B244000	push 07.40243B	40243B: "The serial you entered is not corr
0040110D	FF 75 08	push dword ptr ss:[ebp+8]	
00401110	E8 56000000	call <JMP.&MessageBoxA>	
00401115	EB 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	FF 75 08	push dword ptr ss:[ebp+8]	

마지막으로 내가 입력한 시리얼코드와 비교하는 부분이 실행되는 함수 Istrcmp1A 가 실행되면서

004010CF	68 FD234000	push 07.4023FD	4023FD: "L2C-5781"
004010D4	68 00204000	push 07.402000	402000: "L2C-5781GUF/USB4562-ABEX"
004010D9	E8 63000000	call <JMP.&Istrcat>	
004010DE	68 5C224000	push 07.40225C	40225C: "GUF/USB4562-ABEX"
004010E3	68 00204000	push 07.402000	402000: "L2C-5781GUF/USB4562-ABEX"
004010E8	E8 54000000	call <JMP.&Istrcat>	
004010ED	68 24234000	push 07.402324	402324: "hello"
004010F2	68 00204000	push 07.402000	402000: "L2C-5781GUF/USB4562-ABEX"
004010F8	E8 51000000	call <JMP.&Istrcmp1A>	
004010FC	83 F8 00	cmp eax, 0	eax: "L2C-5781GUF/USB4562-ABEX"
004010FF	74 16	je 07.401117	
00401101	6A 00	push 0	
00401103	68 34244000	push 07.402434	402434: "Error!"
00401108	68 3B244000	push 07.40243B	40243B: "The serial you entered is not corr
0040110D	FF 75 08	push dword ptr ss:[ebp+8]	
00401110	E8 56000000	call <JMP.&MessageBoxA>	
00401115	EB 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!"

내가 입력한 값 hello와 만들어진 시리얼값을 비교하게 된다.

74F66908	8B 55 0C	mov ebx, dword ptr ss:[ebp+C]	[ebp+C]: "gogo"
74F6690B	8B 5D 08	mov ecx, dword ptr ss:[ebp+8]	[ebp+8]: "L2C-5781GUF/USB4562-ABEX"
74F6690E	E8 461B0400	call kernel32.74FA8456	
74F66910	5D	pop ebp	
74F66911	C2 0800	ret 8	
74F66912		int3	
74F66913		int3	
74F66914		int3	
74F66915		int3	
74F66916		int3	
74F66917		int3	
74F66918		int3	
74F66919		int3	
74F6691A		int3	
74F6691B		int3	
74F6691C		int3	
74F6691D		int3	



종합한 결과로 시리얼 값을 입력하면 성공!

이제 변환과정을 ASCII코드표로 봐봤더니

4개의 문자가 아스키코드값 2씩 밀려서 치환되는 규칙을 발견하여.

CodeEngn -> EqfgEngn 으로 치환되는 모습

제어 문자 공백 문자 구두점 숫자 알파벳

10진	16진	문자	10진	16진	문자	10진	16진	문자	10진	16진	문자
0	0x00	NUL	32	0x20	SP	64	0x40	@	96	0x60	`
1	0x01	SOH	33	0x21	!	65	0x41	A	97	0x61	a
2	0x02	STX	34	0x22	"	66	0x42	B	98	0x62	b
3	0x03	ETX	35	0x23	#	67	0x43	C	99	0x63	c
4	0x04	EOT	36	0x24	\$	68	0x44	D	100	0x64	d
5	0x05	ENQ	37	0x25	%	69	0x45	E	101	0x65	e
6	0x06	ACK	38	0x26	&	70	0x46	F	102	0x66	f
7	0x07	BEL	39	0x27	'	71	0x47	G	103	0x67	g
8	0x08	BS	40	0x28	(72	0x48	H	104	0x68	h
9	0x09	HT	41	0x29)	73	0x49	I	105	0x69	i
10	0x0A	LF	42	0x2A	*	74	0x4A	J	106	0x6A	j
11	0x0B	VT	43	0x2B	+	75	0x4B	K	107	0x6B	k
12	0x0C	FF	44	0x2C	,	76	0x4C	L	108	0x6C	l
13	0x0D	CR	45	0x2D	-	77	0x4D	M	109	0x6D	m
14	0x0E	SO	46	0x2E	.	78	0x4E	N	110	0x6E	n
15	0x0F	SI	47	0x2F	/	79	0x4F	O	111	0x6F	o
16	0x10	DLE	48	0x30	0	80	0x50	P	112	0x70	p
17	0x11	DC1	49	0x31	1	81	0x51	Q	113	0x71	q
18	0x12	DC2	50	0x32	2	82	0x52	R	114	0x72	r
19	0x13	DC3	51	0x33	3	83	0x53	S	115	0x73	s
20	0x14	DC4	52	0x34	4	84	0x54	T	116	0x74	t
21	0x15	NAK	53	0x35	5	85	0x55	U	117	0x75	u
22	0x16	SYN	54	0x36	6	86	0x56	V	118	0x76	v
23	0x17	ETB	55	0x37	7	87	0x57	W	119	0x77	w
24	0x18	CAN	56	0x38	8	88	0x58	X	120	0x78	x
25	0x19	EM	57	0x39	9	89	0x59	Y	121	0x79	y
26	0x1A	SUB	58	0x3A	:	90	0x5A	Z	122	0x7A	z
27	0x1B	ESC	59	0x3B	;	91	0x5B	[123	0x7B	{
28	0x1C	FS	60	0x3C	<	92	0x5C	\	124	0x7C	
29	0x1D	GS	61	0x3D	=	93	0x5D]	125	0x7D	}
30	0x1E	RS	62	0x3E	>	94	0x5E	^	126	0x7E	~
31	0x1F	US	63	0x3F	?	95	0x5F	_	127	0x7F	DEL

74F66900	8B FF	mov edi,edi	1strcmpA
74F66902	55	push ebp	
74F66903	8B EC	mov ebp,esp	
74F66905	8B 55 0C	mov edx,dword ptr [ebp+0C]	[ebp+0C]: "h1h1"
74F66908	8B 4D 08	mov ecx,dword ptr [ebp+08]	[ebp+8]: "L2C-B761YkpF0ws4562-ABEX"
74F6690B	E8 46 1B 04 00	call kernel32.74FA8456	
74F66910	5D	pop ebp	
74F66911	C2 08 00	ret 8	

혹시나 하고 다른 환경 Window라는 이름의C:// 경로에 넣고 디버깅해보니 똑같은 규칙으로 변하는 모습을 보임.