

CodeEngn

Solving problems

basic level7

Nick : C y __ h

Email : h61cker@gmail.com

Challenges : Basic 07

Author : abex

Korean :

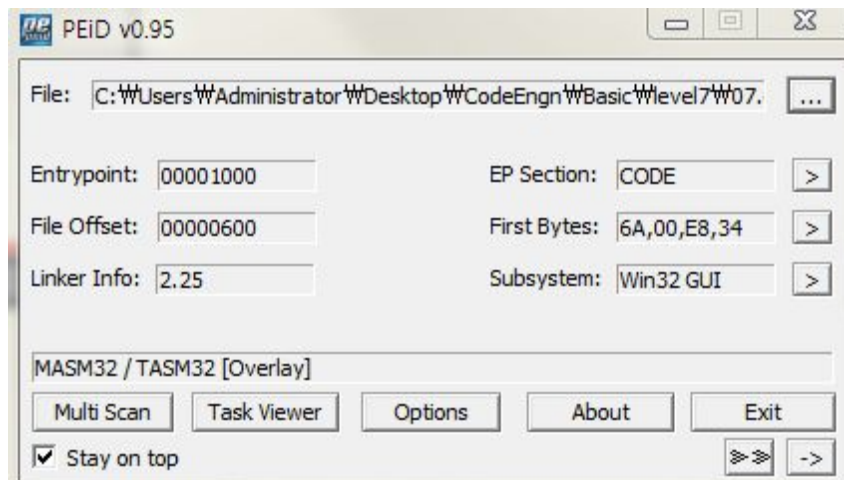
컴퓨터 C 드라이브의 이름이 CodeEngn 일경우 시리얼이 생성될때 CodeEngn은 "어떤것"으로 변경되는가

English :

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

C 드라이브의 이름이 CodeEngn 이라고 하네요

즉 , C 드라이브 함수를 호출하는 API 를 찾으면 가능할거 같습니다.



어셈블리어 로 프로그래밍 되어있습니다.

0040108B	. 68 94214000	push 07.00402194	pVolumeSerialNumber = 07.00402194
00401090	. 6A 32	push 32	MaxVolumeNameSize = 32 (50.)
00401092	. 68 5C224000	push 07.0040225C	VolumeNameBuffer = 07.0040225C
00401097	. 6A 00	push 0	RootPathName = NULL
00401099	E8 B5000000	call <jmp.&KERNEL32.GetVolumeInformation>	하드디스크 볼륨값 조회
0040109E	. 68 F3234000	push 07.004023F3	StringToAdd = "4562-ABEX"
004010A3	. 68 5C224000	push 07.0040225C	ConcatString = ""
004010A8	. E8 94000000	call <jmp.&KERNEL32.lstrcatA>	lstrcatA
004010AD	. B2 02	mov dl, 2	
004010AF	> 8305 5C224000	add dword ptr ds:[40225C], 1	
004010B6	. 8305 5D224000	add dword ptr ds:[40225D], 1	
004010BD	. 8305 5E224000	add dword ptr ds:[40225E], 1	

하드디스크 볼륨값 조회하는 함수를 찾았습니다.

GetVolumeInformation A < 하드디스크 볼륨값 조회 >

ConcatString 에서 디버깅을 하다보면 자기 컴퓨터 드라이브 이름이 나옵니다.

그 주소를 타고 덤브를 분석하면 문자열이 나오는데 그걸 CodeEngn 으로 바꿔주면 됩니다.

Address	Hex dump	ASCII
0040225C	43 79 5F 68 00 00 00 00 00 00 00 00 00 00 00 00	Cy_h.....
0040226C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040227C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040228C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040229C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004022AC	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004022BC	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004022CC	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004022DC	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004022EC	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
004022FC	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040230C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040231C	00 00 00 00 00 00 00 00 68 36 31 63 68 65 72 00h61cker.
0040232C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040233C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040234C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040235C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040236C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040237C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Edit data at 0040225C

ASCII

CodeEngn

UNICODE

U+0000

HEX +08

43 6F 64 65 45 6E 67 6E 00 00 00 00 00 00 00 00

00 00 00 00

Keep size

OK

Cancel

Address	Hex	Disassembly	Comment
00401099	E8 B5000000	call <jmp.&KERNEL32.GetVolumeInformation>	하드디스크 볼륨 정보
0040109E	68 F3234000	push 07.004023F3	StringToAdd = "4562-ABEX"
004010A3	68 5C224000	push 07.0040225C	ConcatString = "CodeEngn"
004010A8	E8 94000000	call <jmp.&KERNEL32.lstrcatA>	lstrcatA
004010AD	B2 02	mov dl, 2	
004010AF	8305 5C224000	add dword ptr ds:[40225C], 1	
004010B6	8305 5D224000	add dword ptr ds:[40225D], 1	
004010BD	8305 5E224000	add dword ptr ds:[40225E], 1	

바꿔주고 디버깅합시다.

Address	Hex	Disassembly
004010AD	B2 02	mov dl, 2
004010AF	8305 5C224000	add dword ptr ds:[40225C], 1
004010B6	8305 5D224000	add dword ptr ds:[40225D], 1
004010BD	8305 5E224000	add dword ptr ds:[40225E], 1
004010C4	8305 5F224000	add dword ptr ds:[40225F], 1
004010CB	FECA	dec dl
004010CD	75 E0	jnz short 07.004010AF

저기 위치한 반복문은 CodeEngn 을 다른 문자열로 치환해주는 루프입니다.

```
Registers (FPU) < < <
EAX 0040225C ASCII "EqfgEngn4562-ABEX"
ECX 76BB2BAD kernel32.76BB2BAD
EDX 00000000
EBX 00000001
ESP 0018FA44
EBP 0018FA48
ESI 00401029 07.00401029
EDI 00000000
EIP 004010CF 07.004010CF

C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
7 1 DS 002B 32bit 0(FFFFFFFF)
```

그리고 레지스터에서 함수 리턴값 즉, eax 를 보면

문자열이 나타납니다.

key flag : EqfgEngn