

Code Engn Basic 10

4.Z320

elttzero@gmail.com

Challenges : Basic 10

Author : ArturDents

Korea :

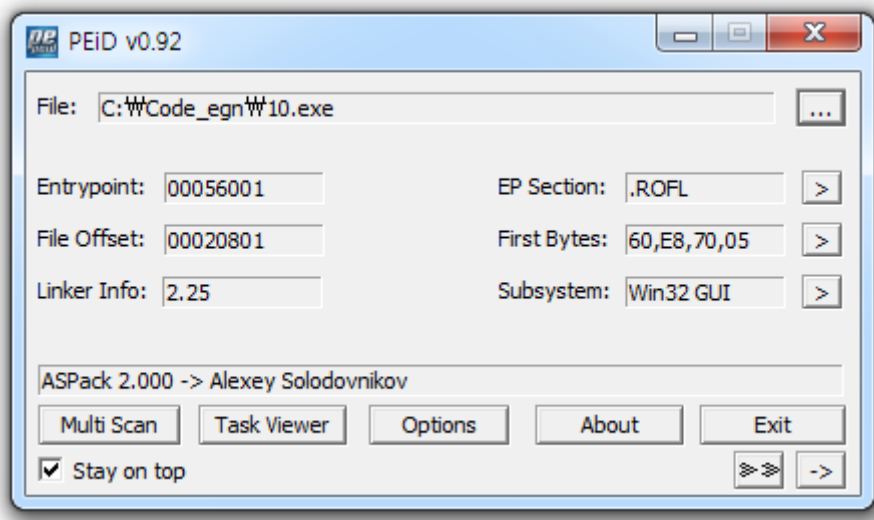
OEP를 구한 후 "등록성공"으로 가는 분기점의 OPCODE를 구하시오. 정답인종은 OEP + OPCODE
EX) 00400000EB03

English :

After finding the OEP, find the OPCODE of the branch instruction going to the "goodboy routine"
The solution should be in this format : OEP + Serial
EX) 00400000EB03

[Download](#)

OEP 및 등록성공 으로 가는 분기점을 구하는 문제입니다.



PEiD 로 확인해 보니 ASPack 이 되어 있음을 확인할 수 있습니다.

004564E2	0385 04484400	ADD EAX, DWORD PTR SS:[EBP+444804]	
004564E8	59	POP ECX	
004564E9	0BC9	OR ECX, ECX	
004564EB	8985 A13E4400	MOV DWORD PTR SS:[EBP+443EA1], EAX	
004564F1	61	POPAD	
004564F2	75 08	JNZ SHORT 10.004564FC	
004564F4	B8 01000000	MOV EAX, 1	
004564F9	C2 0C00	SETB EC	
004564FC	68 00000000	PUSH 0	
00456501	C3	RETN	
00456502	8B85 08484400	MOV EAX, DWORD PTR SS:[EBP+444808]	
00456508	8D8D 41484400	LEA ECX, DWORD PTR SS:[EBP+444841]	
0045650E	51	PUSH ECX	
0045650F	50	PUSH EAX	
00456510	FF95 14494400	CALL DWORD PTR SS:[EBP+444914]	
00456516	8985 08484400	MOV EAX, DWORD PTR SS:[EBP+444808]	

프로그램의 언패킹이 끝나고 돌아가는 부분을 찾아서 안으로 들어가면 OEP 를 찾을 수 있습니다.

00445834	55	DB 55	CHAR 'U'
00445835	8B	DB 8B	
00445836	EC	DB EC	
00445837	83	DB 83	
00445838	C4	DB C4	
00445839	F4	DB F4	
0044583A	B8	DB B8	
0044583B	F4564400	DD 10.004456F4	
0044583F	E8	DB E8	
00445840	. 04 08	ADD AL,8	
00445842	. FC	CLD	
00445843	. FFA1 6C6C4400	JMP DWORD PTR DS:[ECX+446C6C]	
00445849	8B	DB 8B	
0044584A	00	DB 00	
0044584B	E8	DB E8	

찾아낸 OEP 에서 OllyDbg 의 플러그인을 이용하여 수동 Dump 하여 Unpack 합니다.

00445830	CC	INIT	
00445831	. 56 44 00	ASCII "UD",0	
00445834	\$ 55	PUSH EBP	
00445835	. 8BEC	MOV EBP,ESP	
00445837	. 83C4 F4	ADD ESP,-0C	
0044583A	. B8 F4564400	MOV EAX,10.004456F4	
0044583F	. E8 0408FCFF	CALL 10.00406048	
00445844	. A1 6C6C4400	MOV EAX,DWORD PTR DS:[446C6C]	
00445849	. 8B00	MOV EAX,DWORD PTR DS:[EAX]	
0044584B	. E8 F0CCFFFF	CALL 10.00442540	
00445850	. 8B0D 386D4400	MOV ECX,DWORD PTR DS:[446D38]	10.0044784C
00445856	. A1 6C6C4400	MOV EAX,DWORD PTR DS:[446C6C]	
0044585B	. 8B00	MOV EAX,DWORD PTR DS:[EAX]	
0044585D	. 8B15 104F4400	MOV EDX,DWORD PTR DS:[444F10]	10.004451D4
00445863	. E8 F0CCFFFF	CALL 10.00442558	
00445868	. 8B0D 586D4400	MOV ECX,DWORD PTR DS:[446D58]	10.00447844
0044586E	. A1 6C6C4400	MOV EAX,DWORD PTR DS:[446C6C]	
00445873	. 8B00	MOV EAX,DWORD PTR DS:[EAX]	
00445875	. 8B15 104F4400	MOV EDX,DWORD PTR DS:[444F10]	10.00444F5C
0044587B	. E8 D8CCFFFF	CALL 10.00442558	
00445880	. A1 6C6C4400	MOV EAX,DWORD PTR DS:[446C6C]	
00445885	. 8B00	MOV EAX,DWORD PTR DS:[EAX]	
00445887	. E8 4CCDFFFF	CALL 10.004425D8	
0044588C	. E8 17DFFBFF	CALL 10.004037A8	
00445891	. 8D40 00	LEA EAX,DWORD PTR DS:[EAX]	
00445894	. 0000	ADD BYTE PTR DS:[EAX],AL	
00445896			
00445898			
0044589A			
0044589C			
0044589E			
004458A0			
004458A2			
004458A4			
004458A6			
004458A8			
004458AA			
004458AC			
004458AE			
004458B0			
004458B2			
004458B4			
004458B6			
004458B8			
004458BA			
004458BC			
004458BE			
004458C0			
004458C2			
004458C4			
004458C6			
004458C8			
004458CA			
004458CC			
004458CE	. 0000	ADD BYTE PTR DS:[EAX],AL	
004458D0	. 0000	ADD BYTE PTR DS:[EAX],AL	
004458D2	. 0000	ADD BYTE PTR DS:[EAX],AL	
004458D4	. 0000	ADD BYTE PTR DS:[EAX],AL	
004458D6	. 0000	ADD BYTE PTR DS:[EAX],AL	

PEID v0.92

File: C:\Code_egn\10_.exe

Entrypoint: 00045834 EP Section: CODE

File Offset: 00045834 First Bytes: 55,8B,EC,83

Linker Info: 2.25 Subsystem: Win32 GUI

Borland Delphi 4.0 - 5.0

Multi Scan Task Viewer Options About Exit

☒ Stay on top

제대로 실행이 되는것으로 OEP 를 잘 찾아 Unpack 하였음을 알 수 있습니다.

004453C6	. 55	PUSH EBP	
004453C7	. 68 87554400	PUSH 10_00445587	
004453CC	. 64:FF30	PUSH DWORD PTR FS:[EAX]	
004453CF	. 64:8920	MOV DWORD PTR FS:[EAX],ESP	
004453D2	. 8D45 F8	LEA EAX,DWORD PTR SS:[EBP-8]	
004453D5	. BA A0554400	MOV EDX,10_004455A0	ASCII "15935785264587569231133566485"
004453DA	. E8 99E5FBFF	CALL 10_00403978	
004453DF	. 33D2	XOR EDX,EDX	
004453E1	. 55	PUSH EBP	
004453E2	. 68 3F554400	PUSH 10_0044553F	
004453E7	. 64:FF32	PUSH DWORD PTR FS:[EDX]	
004453EA	. 64:8922	MOV DWORD PTR FS:[EDX],ESP	
004453ED	. BA 1C564400	MOV EDX,10_0044561C	ASCII "cm5.dat"
004453F2	. 8D85 2CFEFFFF	LEA EAX,DWORD PTR SS:[EBP-104]	
004453F8	. E8 AD00FCFF	CALL 10_004054AA	
004453FD	. 8D85 2CFEFFFF	LEA EAX,DWORD PTR SS:[EBP-104]	
00445403	. E8 EF02FCFF	CALL 10_004056F7	
00445408	. E8 8FD3FBFF	CALL 10_0040279C	
0044540D	. 8D95 17FEFFFF	LEA EDX,DWORD PTR SS:[EBP-1E9]	
00445413	. B9 14000000	MOV ECX,14	
00445418	. 8D85 2CFEFFFF	LEA EAX,DWORD PTR SS:[EBP-104]	
0044541E	. E8 D901FCFF	CALL 10_004055FC	
00445423	. 8D85 2CFEFFFF	LEA EAX,DWORD PTR SS:[EBP-104]	
00445429	. E8 6602FCFF	CALL 10_00405694	
0044542E	. E8 69D3FBFF	CALL 10_0040279C	
00445433	. 8D95 02FEFFFF	LEA EDX,DWORD PTR SS:[EBP-1FE]	
00445439	. B9 14000000	MOV ECX,14	
0044543E	. 8D85 2CFEFFFF	LEA EAX,DWORD PTR SS:[EBP-104]	

이 프로그램은 cm5.dat 파일을 불러와서 시리얼을 비교함을 알 수 있습니다만

0044545F	. E8 E800FCFF	CALL 10_0040554C	
00445464	. E8 33D3FBFF	CALL 10_0040279C	
00445469	. 80BD 17FEFFFF	CMP BYTE PTR SS:[EBP-1E9],5	
00445470	. 73 0A	JNB SHORT 10_0044547C	
00445472	. B8 2C564400	MOV EAX,10_0044562C	ASCII "Name must be at least 5 characters long!"
00445477	. E8 A4F8FBFF	CALL 10_00444D20	
0044547C	. 0FB6B5 17FEFF	MOVZX ESI,BYTE PTR SS:[EBP-1E9]	
00445483	. 85F6	TEST ESI,ESI	
00445485	. 7E 2E	JLE SHORT 10_004454B5	
00445487	. 8D9D 18FEFFFF	LEA EBX,DWORD PTR SS:[EBP-1E8]	
0044548D	. 8D85 FCFDFFFF	LEA EAX,DWORD PTR SS:[EBP-204]	
00445493	. 33D2	XOR EDX,EDX	
00445495	. 8A13	MOV DL,BYTE PTR DS:[EBX]	
00445497	. 8B4D F8	MOV ECX,DWORD PTR SS:[EBP-8]	
0044549A	. 8A5411 F5	MOV DL,BYTE PTR DS:[ECX+EDX-B]	
0044549E	. E8 E5E5FBFF	CALL 10_00403A88	
004454A3	. 8B95 FCFDFFFF	MOV EDX,DWORD PTR SS:[EBP-204]	
004454A9	. 8D45 FC	LEA EAX,DWORD PTR SS:[EBP-4]	
004454AC	. E8 B7E6FBFF	CALL 10_00403B68	
004454B1	. 43	INC EBX	
004454B2	. 4E	DEC ESI	
004454B3	. 75 D8	JNZ SHORT 10_0044548D	

안의 파일의 첫번째 문장의 글자수가 5 글자 이하이면 에러메세지를 띄우게 되어 있습니다.

0044547C	. 0FB6B5 17FEFF	MOVZX ESI,BYTE PTR SS:[EBP-1E9]	
00445483	. 85F6	TEST ESI,ESI	
00445485	. 7E 2E	JLE SHORT 10_004454B5	
00445487	. 8D9D 18FEFFFF	LEA EBX,DWORD PTR SS:[EBP-1E8]	
0044548D	. 8D85 FCFDFFFF	LEA EAX,DWORD PTR SS:[EBP-204]	
00445493	. 33D2	XOR EDX,EDX	
00445495	. 8A13	MOV DL,BYTE PTR DS:[EBX]	
00445497	. 8B4D F8	MOV ECX,DWORD PTR SS:[EBP-8]	
0044549A	. 8A5411 F5	MOV DL,BYTE PTR DS:[ECX+EDX-B]	
0044549E	. E8 E5E5FBFF	CALL 10_00403A88	
004454A3	. 8B95 FCFDFFFF	MOV EDX,DWORD PTR SS:[EBP-204]	
004454A9	. 8D45 FC	LEA EAX,DWORD PTR SS:[EBP-4]	
004454AC	. E8 B7E6FBFF	CALL 10_00403B68	
004454B1	. 43	INC EBX	
004454B2	. 4E	DEC ESI	
004454B3	. 75 D8	JNZ SHORT 10_0044548D	

이후 글자의 길이를 ESI 에 넣은 뒤 루프의 카운터로 쓰게 되고 ECX 에 기본적으로 들어있던 숫자열의 주소를, EDX 에는 읽어들인 NAME 의 첫번째 글자를 읽어오게 됩니다.

Registers (FPU)		
EAX	0012EBCC	
ECX	004455A0	ASCII "159357852645875692311335664857"
EDX	00000039	
EBX	0012EBE8	ASCII "ffffffc"
ESP	0012EBA0	
EBP	0012EDD0	
ESI	00000006	
EDI	011E17D4	ASCII "?D"

이후 ECX 의 문자열 중에서 첫번째 글자의 ASCII Code 값 - B 만큼 이동한 곳의 숫자를 읽어온 뒤 EDX 레지스터에 저장하게 됩니다. 그리고 이것이 시리얼 값이 됩니다.

0044549E	. E8 E5E5FBFF	CALL 10, .00403A88	
004454A3	. 8B95 FCFDFF	MOV EDX, DWORD PTR SS:[EBP-204]	
004454A9	. 8D45 FC	LEA EAX, DWORD PTR SS:[EBP-4]	
004454AC	. E8 B7E6FBFF	CALL 10, .00403B68	
004454B1	. 43	INC EBX	
004454B2	. 4E	DEC ESI	
004454B3	. 75 D8	JNZ SHORT 10, .0044548D	
004454B5	> 8D85 F8FDFF	LEA EAX, DWORD PTR SS:[EBP-208]	
004454BB	. 8D95 02FEFF	LEA EDX, DWORD PTR SS:[EBP-1FE]	
004454C1	. E8 3EE6FBFF	CALL 10, .00403B04	
004454C6	. 8B85 F8FDFF	MOV EAX, DWORD PTR SS:[EBP-208]	
004454CC	. 8B55 FC	MOV EDX, DWORD PTR SS:[EBP-4]	
004454CF	. E8 9CE7FBFF	CALL 10, .00403C70	
004454D4	. 75 55	JNZ SHORT 10, .0044552B	

그후 만들어진 시리얼 값을 스택 [EBP - 4]에 저장하게 되고 cm5.dat 에서 다음 문장을 저장해 둔 곳인 [EBP - 208]의 값을 읽어온 뒤 만들어진 시리얼 값과 한글자씩 비교하게 됩니다. 이때 [EBP - 208]에 있는 문장의 길이는 NAME 값과 같아야 합니다.

004454CF	. E8 9CE7FBFF	CALL 10, .00403C70	
004454D4	. 75 55	JNZ SHORT 10, .0044552B	
004454D6	. 8D85 F4FDFF	LEA EAX, DWORD PTR SS:[EBP-20C]	
004454DC	. 8D95 17FEFF	LEA EDX, DWORD PTR SS:[EBP-1E9]	
004454E2	. E8 1DE6FBFF	CALL 10, .00403B04	
004454E7	. 8B95 F4FDFF	MOV EDX, DWORD PTR SS:[EBP-20C]	
004454ED	. 8B87 D4020000	MOV EAX, DWORD PTR DS:[EDI+2D4]	
004454F3	. E8 B4F5DFFF	CALL 10, .00424AAC	
004454F8	. 8B87 D8020000	MOV EAX, DWORD PTR DS:[EDI+2D8]	
004454FE	. 8B55 FC	MOV EDX, DWORD PTR SS:[EBP-4]	
00445501	. E8 A6F5DFFF	CALL 10, .00424AAC	
00445506	. 8B87 E8020000	MOV EAX, DWORD PTR DS:[EDI+2E8]	
0044550C	. BA 60564400	MOV EDX, 10, .00445660	
00445511	. E8 96F5DFFF	CALL 10, .00424AAC	
00445516	. 8B87 E8020000	MOV EAX, DWORD PTR DS:[EDI+2E8]	
0044551C	. 8B40 58	MOV EAX, DWORD PTR DS:[EAX+58]	
0044551F	. BA 00800000	MOV EDX, 8000	
00445524	. E8 BFF2FCFF	CALL 10, .004147E8	

ASCII "Registered ... well done!"

만약 비교하여 서로의 문자열 값이 같다면 아래의 분기점인 JNZ 에 걸리지 않게 되고 Registered 구문을 만날 수 있게 됩니다. 즉 정답으로 가는 분기점의 OPCODE 는 JNZ 인 7555 가 되게 됩니다. 이번 문제의 OEP 는 00445834 이며 OPCODE 는 7555 이므로 정답은 004458347555 가 되게 됩니다.