

프로그램의 등록키를 찾아라!

올리디버거로 열자마자 보이는 pushad..

00455BAF	FF	DB FF	
00455BB0	\$ 60	PUSHAD	
00455BB1	. BE 00704300	MOV ESI,05.00437000	
00455BB6	. 8DBE 00A0FCF	LEA EDI,DWORD PTR DS:[ESI+FFFC0000]	
00455BBC	. C787 D024040	MOV DWORD PTR DS:[EDI+42400],689C0471	
00455BC6	. 57	PUSH EDI	
00455BC7	. 83CD FF	OR EBP,FFFFFFFF	
00455BCA	~ EB 0E	JMP SHORT 05.00455BDA	
00455BCC	90	NOP	
00455BCD	90	NOP	
00455BCE	90	NOP	
00455BCF	90	NOP	
00455BD0	> 8A06	MOV AL,BYTE PTR DS:[ESI]	
00455BD2	. 46	INC ESI	
00455BD3	. 8807	MOV BYTE PTR DS:[EDI],AL	
00455BD5	. 47	INC EDI	
00455BD6	> 01DB	ADD EBX,EBX	
00455BD8	~ 75 07	JNZ SHORT 05.00455BE1	
00455BDA	> 8B1E	MOV EBX,DWORD PTR DS:[ESI]	
00455BDC	. 83EE FC	SUB ESI,-4	
00455BDF	. 11DB	ADC EBX,EBX	
00455BE1	>^ 72 ED	JB SHORT 05.00455BD0	
00455BE3	. B8 01000000	MOV EAX,1	

아니 자네 실행압축아닌가!

POPAD부분을 찾아가야겠다. (사실 upx압축해제 하려다 fail했다.)

PUSHAD만 실행하면 그 때의 레지스터값들이 스택에 저장된다.

0012FF6C	00000000	
0012FF70	00000000	
0012FF74	0012FF94	
0012FF78	0012FF8C	
0012FF7C	7FFDF000	
0012FF80	00455BB0	05.<ModuleEntryPoint>
0012FF84	00000000	
0012FF88	76353C33	kernel32.BaseThreadInitThunk
0012FF8C	76353C45	RETURN to kernel32.76353C45
0012FF90	7FFDF000	
0012FF94	0012FFD4	
0012FF98	776337F5	RETURN to ntdll.776337F5
0012FF9C	7FFDF000	
0012FFA0	77D0E55E	
0012FFA4	00000000	

맨 위에 있는 값은 EDI 의 값으로 이 때의 주소를 dump창에서 찾은다음 berakpoint->hardware,on access->byte 하고 F9로 실행하면

00455CEA	- 57	PUSH EDI	Registers (FPU)
00455CEB	- 48	DEC EAX	EAX 76353C33 kernel3
00455CEC	- F2:AE	REPNE SCAS BYTE PTR ES:[EDI]	ECX 00000000
00455CEE	- 55	PUSH EBP	EDX 00455BB0 05.<Mod
00455CEF	- FF96 0061050	CALL DWORD PTR DS:[ESI+56100]	EBX 7FFDF000
00455CF5	- 09C0	OR EAX,EAX	ESP 0012FF8C
00455CF7	- 74 07	JE SHORT 05.00455D00	EBP 0012FF94
00455CF9	- 8903	MOV DWORD PTR DS:[EBX],EAX	ESI 00000000
00455CFB	- 83C3 04	ADD EBX,4	EDI 00000000
00455CFE	- EB E1	JMP SHORT 05.00455CE1	EIP 00455D07 05.0045
00455D00	> FF96 0061050	CALL DWORD PTR DS:[ESI+56104]	C 0 ES 0023 32bit 0
00455D06	> 61	POPAD	P 1 CS 001B 32bit 0
00455D07	- E9 64B5FEFF	JMP 05.00441270	A 0 SS 0023 32bit 0
00455D0C	- 245D4500	DD 05.00455D24	Z 1 DS 0023 32bit 0
00455D10	- 345D4500	DD 05.00455D34	S 0 FS 003B 32bit 7
00455D14	- D0344400	DD 05.004434D0	T 0 GS 0000 NULL
00455D18	- 00	DB 00	D 0
00455D19	- 00	DB 00	O 0 LastErr ERROR_E
00455D1A	- 00	DB 00	FFI 00000246 /NO NR
00455D1B	- 00	DB 00	

POPAD를 실행한 후(복구끝난후)의 레지스터 상태가 된다.

그다음 search for strings로 뭔가 있나 보다가 영어로 no name entered를 보았다. 그 근처에 시리얼 성공/실패 글도 있을 것이라 생각해 이동했고 언패킹이 끝나 코드분석이 안되어있길래 analysis를 했다.

그러면 이런 화면이 나온다.

00440EB0	- 55	PUSH EBP	
00440EB1	- 8BEC	MOV EBP,ESP	
00440EB3	- 6A 00	PUSH 0	
00440EB5	- 53	PUSH EBX	
00440EB6	- 8BD8	MOV EBX,EAX	
00440EB8	- 33C0	XOR EAX,EAX	
00440EBA	- 55	PUSH EBP	
00440EBB	- 68 BA0F4400	PUSH 05.00440FBA	
00440EC0	- 64:FF30	PUSH DWORD PTR FS:[EAX]	
00440EC3	- 64:8920	MOV DWORD PTR FS:[EAX],ESP	
00440EC6	- 8D55 FC	LEA EDX,DWORD PTR SS:[EBP-4]	
00440EC9	- 8B83 C402000	MOV EAX,DWORD PTR DS:[EBX+2C4]	
00440ECF	- E8 4CFFDFF	CALL 05.00420E20	
00440ED4	- 837D FC 00	CMP DWORD PTR SS:[EBP-4],0	
00440ED8	- 75 18	JNZ SHORT 05.00440EF2	
00440EDA	- 6A 00	PUSH 0	
00440EDC	- B9 C80F4400	MOV ECX,05.00440FC8	ASCII "No Name entered"
00440EE1	- BA D80F4400	MOV EDX,05.00440FD8	ASCII "Enter a Name!"
00440EE6	- A1 442C4400	MOV EAX,DWORD PTR DS:[442C44]	
00440EEB	- 8B00	MOV EAX,DWORD PTR DS:[EAX]	
00440EED	- E8 76C1FFFF	CALL 05.0043D068	
00440EF2	> 8D55 FC	LEA EDX,DWORD PTR SS:[EBP-4]	
00440EF5	- 8B83 C802000	MOV EAX,DWORD PTR DS:[EBX+2C8]	
00440EFB	- E8 20FFDFF	CALL 05.00420E20	
00440F00	- 837D FC 00	CMP DWORD PTR SS:[EBP-4],0	
00440F04	- 75 18	JNZ SHORT 05.00440F1E	
00440F06	- 6A 00	PUSH 0	
00440F08	- B9 E80F4400	MOV ECX,05.00440FE8	ASCII "No Serial entered"
00440F0D	- BA FC0F4400	MOV EDX,05.00440FFC	ASCII "Enter a Serial!"
00440F12	- A1 442C4400	MOV EAX,DWORD PTR DS:[442C44]	
00440F17	- 8B00	MOV EAX,DWORD PTR DS:[EAX]	
00440F19	- E8 4AC1FFFF	CALL 05.0043D068	
00440F1E	> 8D55 FC	LEA EDX,DWORD PTR SS:[EBP-4]	

위쪽은 스택공간 만드는 역할이고 함수00420E20과 0043D068을 부르고 있다. 00420E20은 이름에도 serial에도 부르는 것을 보면 입력받는함수인듯하다.

00440F3E	- 8B83 C8020000	MOV EAX,DWORD PTR DS:[EBX+2C8]	
00440F44	- E8 D7FEFDFF	CALL 05.00420E20	
00440F49	- 8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
00440F4C	- BA 2C104400	MOV EDX,05.0044102C	ASCII "GFX-754-IER-954"
00440F51	- E8 D62BFCFF	CALL 05.00403B2C	
00440F56	~ 75 1A	JNZ SHORT 05.00440F72	
00440F58	- 6A 00	PUSH 0	
00440F5A	- B9 3C104400	MOV ECX,05.0044103C	ASCII "CrackMe cracked successfully"
00440F5F	- BA 5C104400	MOV EDX,05.0044105C	ASCII "Congrats! You cracked this CrackMe!"
00440F64	- A1 442C4400	MOV EAX,DWORD PTR DS:[442C44]	
00440F69	- 8B00	MOV EAX,DWORD PTR DS:[EAX]	
00440F6B	- E8 F8C0FFFF	CALL 05.0043D068	
00440F70	~ EB 32	JMP SHORT 05.00440FA4	
00440F72	> 6A 00	PUSH 0	
00440F74	- B9 80104400	MOV ECX,05.00441080	ASCII "Beggar off!"
00440F79	- BA 8C104400	MOV EDX,05.0044108C	ASCII "Wrong Serial,try again!"
00440F7E	- A1 442C4400	MOV EAX,DWORD PTR DS:[442C44]	
00440F83	- 8B00	MOV EAX,DWORD PTR DS:[EAX]	
00440F85	- E8 DEC0FFFF	CALL 05.0043D068	
00440F8A	~ EB 18	JMP SHORT 05.00440FA4	
00440F8C	> 6A 00	PUSH 0	
00440F8E	- B9 80104400	MOV ECX,05.00441080	ASCII "Beggar off!"
00440F93	- BA 8C104400	MOV EDX,05.0044108C	ASCII "Wrong Serial,try again!"
00440F98	- A1 442C4400	MOV EAX,DWORD PTR DS:[442C44]	
00440F9D	- 8B00	MOV EAX,DWORD PTR DS:[EAX]	

내려가면 좀 수상한 키를 함수인자로 받는 00403B2C가 있다.

00403B2C	53	PUSH EBX
00403B2D	56	PUSH ESI
00403B2E	57	PUSH EDI
00403B2F	89C6	MOV ESI,EAX
00403B31	89D7	MOV EDI,EDX
00403B33	39D0	CMP EAX,EDX
00403B35	~ 0F84 8F000000	JE 05.00403BCA
00403B3B	85F6	TEST ESI,ESI
00403B3D	~ 74 68	JE SHORT 05.00403BA7
00403B3F	85FF	TEST EDI,EDI
00403B41	~ 74 6B	JE SHORT 05.00403BAE
00403B43	8B46 FC	MOV EAX,DWORD PTR DS:[ESI-4]
00403B46	8B57 FC	MOV EDX,DWORD PTR DS:[EDI-4]
00403B49	29D0	SUB EAX,EDX
00403B4B	~ 77 02	JA SHORT 05.00403B4F
00403B4D	01C2	ADD EDX,EAX
00403B4F	52	PUSH EDX
00403B50	C1EA 02	SHR EDX,2
00403B53	~ 74 26	JE SHORT 05.00403B7B
00403B55	8B0E	MOV ECX,DWORD PTR DS:[ESI]
00403B57	8B1F	MOV EBX,DWORD PTR DS:[EDI]
00403B59	39D9	CMP ECX,EBX
00403B5B	~ 75 58	JNZ SHORT 05.00403BB5
00403B5D	4A	DEC EDX
00403B5E	~ 74 15	JE SHORT 05.00403B75
00403B60	8B4E 04	MOV ECX,DWORD PTR DS:[ESI+4]
00403B63	8B5F 04	MOV EBX,DWORD PTR DS:[EDI+4]
00403B66	39D9	CMP ECX,EBX
00403B68	~ 75 4B	JNZ SHORT 05.00403BB5
00403B6A	83C6 08	ADD ESI,8
00403B6D	83C7 08	ADD EDI,8
00403B70	4A	DEC EDX
00403B71	^ 75 E2	JNZ SHORT 05.00403B55
00403B73	~ EB 06	JMP SHORT 05.00403B7B

들어가보면 이렇게 뭔가 비교하고 점프하는데, 시리얼을 비교하는 구문같아 보인다.

따라가보니 역시 00403B2C에서 문자열을 비교하는데 먼저 입력된 name과 Registered User를 비교하는 것 발견했다. 그래서 다음 시도에 name=Registered User를 넣었다.

00440F17	8B00	MOV EAX,DWORD PTR DS:[EAX]	
00440F19	E8 4AC1FFFF	CALL 05.0043D068	
00440F1E	> 8D55 FC	LEA EDX,DWORD PTR SS:[EBP-4]	
00440F21	8B83 C4020000	MOV EAX,DWORD PTR DS:[EBX+2C4]	
00440F27	E8 F4FEFDFE	CALL 05.00420E20	
00440F2C	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
00440F2F	BA 14104400	MOV EDX,05.00441014	ASCII "Registered User"
00440F34	E8 F32BFCFF	CALL 05.00403B2C	
00440F39	75 51	JNZ SHORT 05.00440F8C	
00440F3B	8D55 FC	LEA EDX,DWORD PTR SS:[EBP-4]	
00440F3E	8B83 C8020000	MOV EAX,DWORD PTR DS:[EBX+2C8]	
00440F44	E8 D7FEFDFE	CALL 05.00420E20	
00440F49	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
00440F4C	BA 2C104400	MOV EDX,05.0044102C	ASCII "GFX-754-IER-954"
00440F51	E8 D62BFCFF	CALL 05.00403B2C	
00440F56	75 1A	JNZ SHORT 05.00440F72	
00440F58	6A 00	PUSH 0	
00440F5A	B9 3C104400	MOV ECX,05.0044103C	ASCII "CrackMe cracked successfully"
00440F5F	BA 5C104400	MOV EDX,05.0044105C	ASCII "Congrats! You cracked this CrackMe!"
00440F64	A1 442C4400	MOV EAX,DWORD PTR DS:[442C44]	
00440F69	8B00	MOV EAX,DWORD PTR DS:[EAX]	
00440F6B	E8 F8C0FFFF	CALL 05.0043D068	
00440F70	EB 32	JMP SHORT 05.00440FA4	

그랬더니 아까까지 JUMP하던 440F39자리를 점프하지 않는 것을 볼 수 있다.

그리고 다음은 GFX-754-IER-954를 인자로받아 또 403B2C에게 주는 것이 보인다.

따라서 403B2C에는 문자열 비교 함수가 있는 것을 알 수 있으며 name=Registered User, PW=GFX-754-IER-954임을 알 수 있다.

그래서 name과 PW에 각각 추론한 내용을 넣어보면

00440F2C	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
00440F2F	BA 14104400	MOV EDX,05.00441014	ASCII "Registered User"
00440F34	E8 F32BFCFF	CALL 05.00403B2C	
00440F39	75 51	JNZ SHORT 05.00440F8C	
00440F3B	8D55 FC	LEA EDX,DWORD PTR SS:[EBP-4]	
00440F3E	8B83 C8020000	MOV EAX,DWORD PTR DS:[EBX+2C8]	
00440F44	E8 D7FEFDFE	CALL 05.00420E20	
00440F49	8B45 FC	MOV EAX,DWORD PTR SS:[EBP-4]	
00440F4C	BA 2C104400	MOV EDX,05.0044102C	ASCII "GFX-754-IER-954"
00440F51	E8 D62BFCFF	CALL 05.00403B2C	
00440F56	75 1A	JNZ SHORT 05.00440F72	
00440F58	6A 00	PUSH 0	
00440F5A	B9 3C104400	MOV ECX,05.0044103C	ASCII "CrackMe cracked successfully"
00440F5F	BA 5C104400	MOV EDX,05.0044105C	ASCII "Congrats! You cracked this CrackMe!"
00440F64	A1 442C4400	MOV EAX,DWORD PTR DS:[442C44]	
00440F69	8B00	MOV EAX,DWORD PTR DS:[EAX]	
00440F6B	E8 F8C0FFFF	CALL 05.0043D068	
00440F70	EB 32	JMP SHORT 05.00440FA4	
00440F72	> 6A 00	PUSH 0	
00440F74	B9 80104400	MOV ECX,05.00441080	ASCII "Beggan off!"
00440F79	BA 8C104400	MOV EDX,05.0044108C	ASCII "Wrong Serial,try again!"

이렇게 무사히 아래로 내려가게 되고

