

Example on how to use oepfinder against execryptor:

Target : **execryptor.2.2.50.j.exe** from www.tuts4you.com



Click on **Trace**:



Click on **Cancel**



Write down values, click on ok and attach olly to our target:

004271C5	-EB FE	JMP SHORT 004271C5
004271C7	8925 00000000	MOV DWORD PTR DS:[0],ESP
004271CD	83C4 A8	ADD ESP,-58
004271D0	53	PUSH EBX
004271D1	56	PUSH ESI
004271D2	57	PUSH EDI
004271D3	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP
004271D6	FF15 DC0A4600	CALL DWORD PTR DS:[460ADC]
004271DC	33D2	XOR EDX,EDX
004271DE	8AD4	MOV DL,AH
004271E0	8915 34E64500	MOV DWORD PTR DS:[45E634],EDX
004271E6	8BC8	MOV ECX,EAX
004271E8	81E1 FF000000	AND ECX,0FF
004271EE	890D 30E64500	MOV DWORD PTR DS:[45E630],ECX
004271F4	C1E1 08	SHL ECX,8
004271F7	03CA	ADD ECX,EDX
004271F9	890D 2CE64500	MOV DWORD PTR DS:[45E62C],ECX
004271FF	C1E8 10	SHR EAX,10
00427202	A3 28E64500	MOV DWORD PTR DS:[45E628],EAX
00427207	E8 94210000	CALL 004293A0
0042720C	85C0	TEST EAX,EAX
0042720E	75 0A	JNZ SHORT 0042721A

Restore opcodes:

004271C5 -EB FE JMP SHORT 004271C5

004271C7 8925 00000000 MOV DWORD PTR DS:[0],ESP

Edit code at 004271C5

ASCII Pd

UNICODE

HEX +02 50 64

☒ Keep size

OK Cancel

And yup we are at the oep:

004271C5	50	PUSH EAX
004271C6	64:8925 00000000	MOV DWORD PTR FS:[0],ESP
004271CD	83C4 A8	ADD ESP,-58
004271D0	53	PUSH EBX
004271D1	56	PUSH ESI
004271D2	57	PUSH EDI
004271D3	8965 E8	MOV DWORD PTR SS:[EBP-18],ESP
004271D6	FF15 DC0A4600	CALL DWORD PTR DS:[460ADC]
004271DC	33D2	XOR EDX,EDX
004271DE	8AD4	MOV DL,AH
004271E0	8915 34E64500	MOV DWORD PTR DS:[45E634],EDX
004271E6	8BC8	MOV ECX,EAX
004271E8	81E1 FF000000	AND ECX,0FF
004271EE	890D 30E64500	MOV DWORD PTR DS:[45E630],ECX

And now run target from olly:



Well that's it... as you can see it works against our ExeCryptoreeeeeee with all protections =)

S verom u Boga, deroko/ARTeam

<http://cracking.accessroot.com>