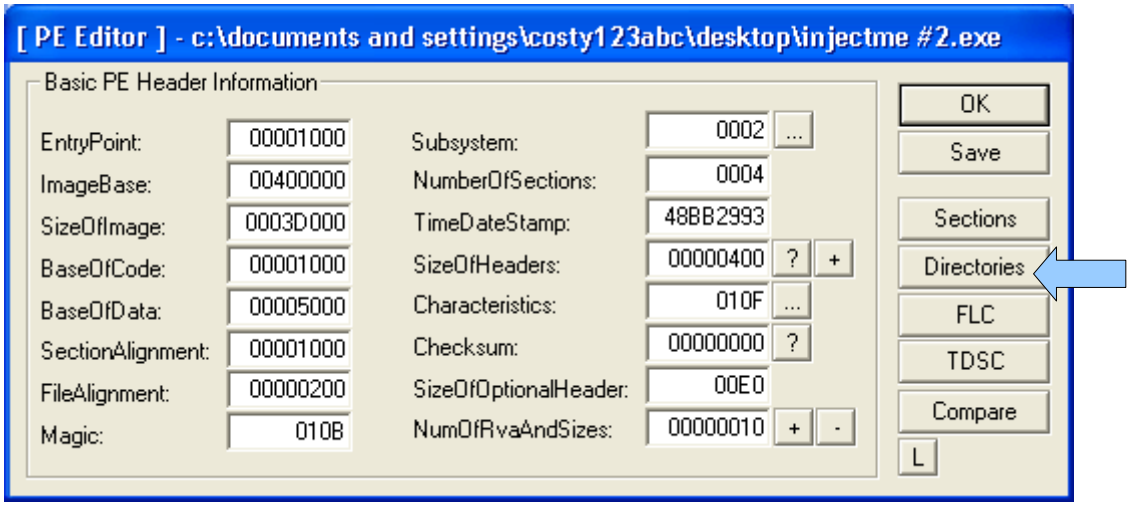
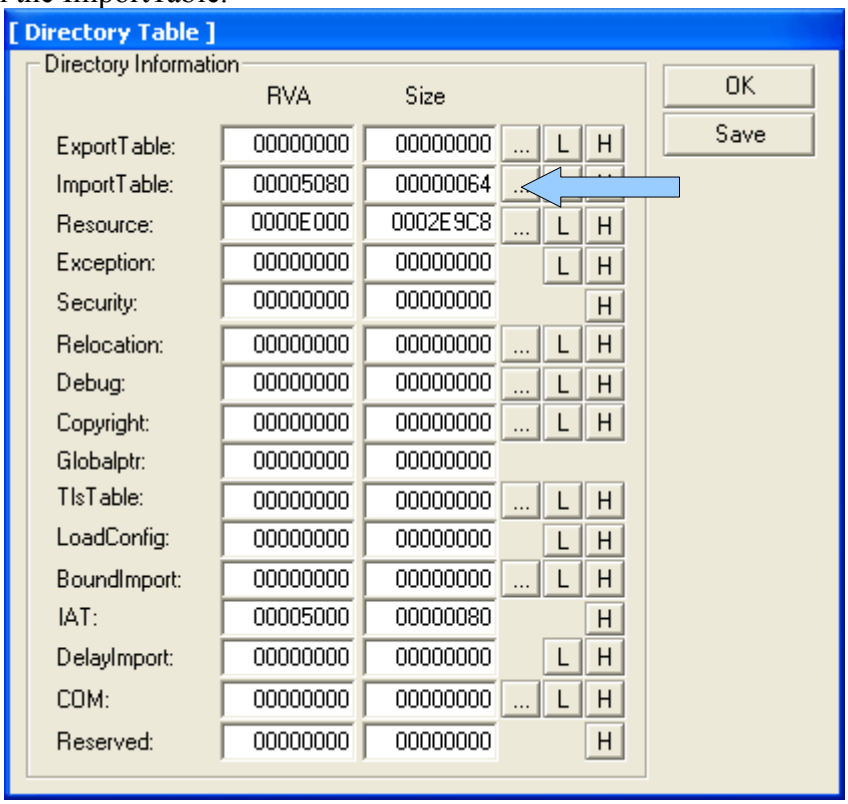
InjectME #2
Solution by Costy

We need to add a message box at start up.
MessageBox api isn't present in the exe so I added it with LordPE.

I opened the exe with lord PE
I clicked on the Directories.

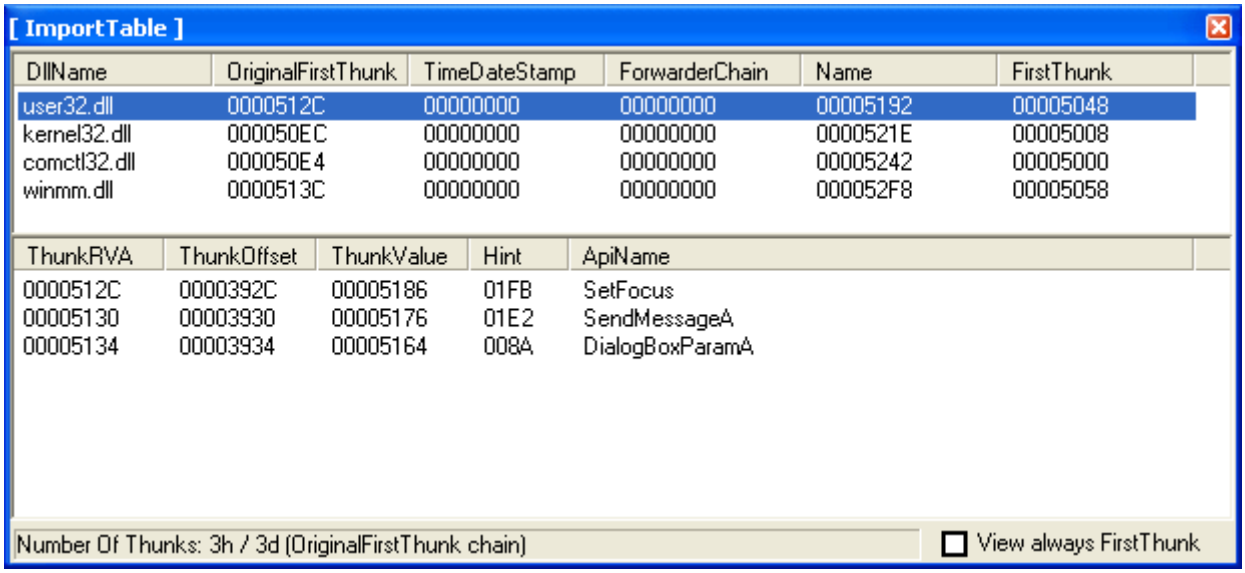


Then I clicked on the ImportTable.

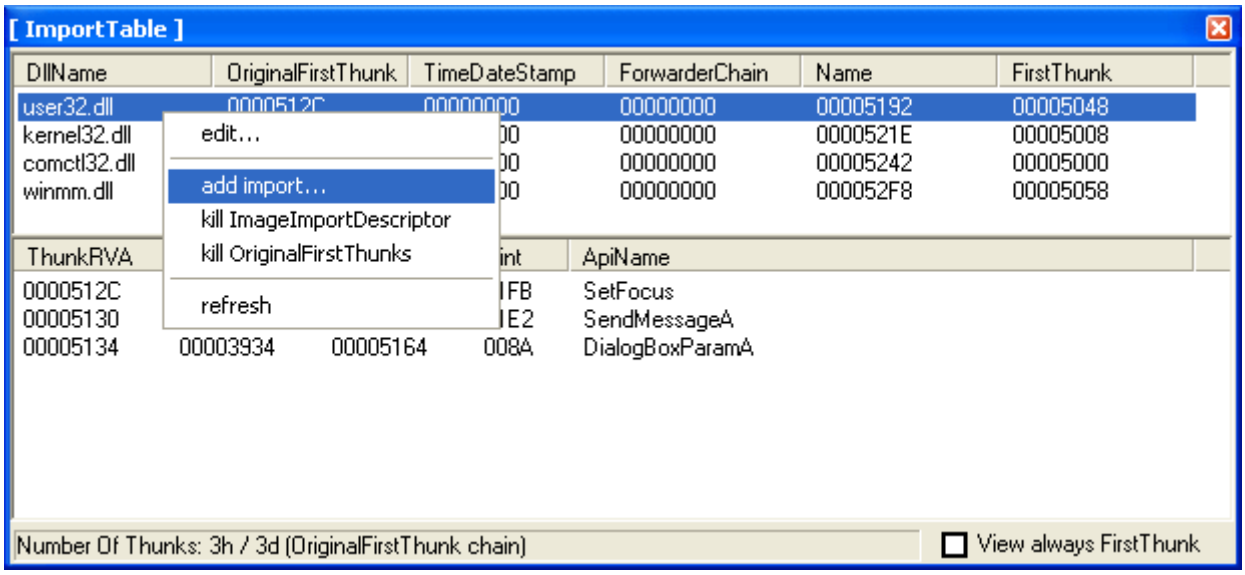


This is the original Import Table. It's the list of api used by the exe.
We need to add MessageBoxA.
MessageBoxA is in the User32 dll so i add it to the list.

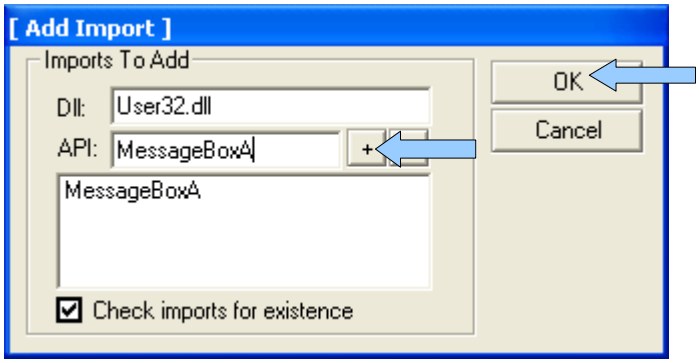
Original Import Table.



Rigth click on user32 and chose add import.



Type User32.dll
Type MessageBoxA press the “+” and ok.
Now just save the changes.



[ImportTable]

DllName	OriginalFirstThunk	TimeDateStamp	ForwarderChain	Name	FirstThunk
user32.dll	0000512C	00000000	00000000	00005192	00005048
kernel32.dll	000050EC	00000000	00000000	0000521E	00005008
comctl32.dll	000050E4	00000000	00000000	00005242	00005000
winmm.dll	0000513C	00000000	00000000	000052F8	00005058
User32.dll	0003D019	00000000	00000000	0003D000	0003D019

ThunkRVA	ThunkOffset	ThunkValue	Hint	ApiName
0003D019	00032819	0003D00B	0000	MessageBoxA

Number Of Thunks: 1h / 1d (OriginalFirstThunk chain) View always FirstThunk

The MessageBox function is added.
To call it inside the exe i need call dword ptr [ImageBase + ThunkRVA].
(call dword ptr [43d019])

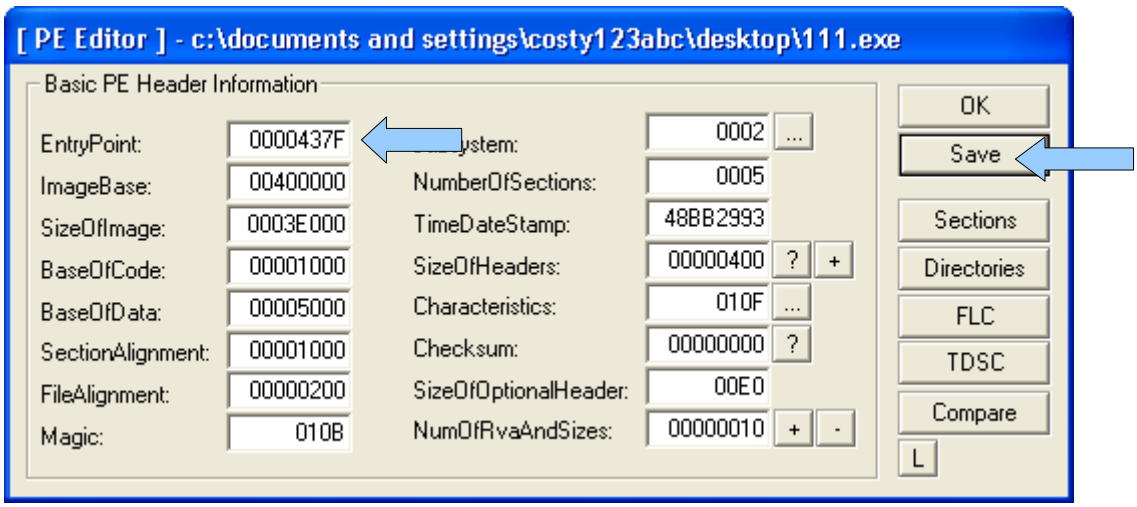
I need to put in the exe the sentence “Injected by COSTY!!!”
I used OllyDbg to make the job.

Address	Hex dump	ASCII
00404366	49 6E 6A 65 63 74 65 64	Injected
0040436E	20 62 79 20 43 4F 53 54	by COST
00404376	59 21 21 21 00 00 00 00	Y!!!....
0040437E	00 00 00 00 00 00 00 00	....
00404386	00 00 00 00 00 00 00 00	....
0040438E	00 00 00 00 00 00 00 00	....
00404396	00 00 00 00 00 00 00 00	....
0040439E	00 00 00 00 00 00 00 00	....
004043A6	00 00 00 00 00 00 00 00	....
004043AE	00 00 00 00 00 00 00 00	....
004043B6	00 00 00 00 00 00 00 00	....
004043BE	00 00 00 00 00 00 00 00	....
004043C6	00 00 00 00 00 00 00 00	....
004043CE	00 00 00 00 00 00 00 00	....
004043D6	00 00 00 00 00 00 00 00	....
004043DE	00 00 00 00 00 00 00 00	....
004043E6	00 00 00 00 00 00 00 00	....
004043EE	00 00 00 00 00 00 00 00	....
004043F6	00 00 00 00 00 00 00 00	....

Now the sentence is at 404366.
I added the following code to the exe.

```
0040437F    6A 00           PUSH 0
00404381    68 66434000     PUSH Copia_di.00404366                ASCII "Injected by COSTY!!!"
00404386    68 66434000     PUSH Copia_di.00404366                ASCII "Injected by COSTY!!!"
0040438B    6A 00           PUSH 0
0040438D    FF15 19D04300   CALL DWORD PTR DS:[<&User32.MessageBoxA  user32.MessageBoxA
00404393  ^E9 68CCFFFF     JMP Copia_di.<ModuleEntryPoint>
00404398    90              NOP
00404399    0000            ADD BYTE PTR DS:[EAX],AL
0040439B    0000            ADD BYTE PTR DS:[EAX],AL
```

This code executes a messagebox with the title and the text identical: “Injected By COSTY!!!”
using the text at 404366 and the MessageBox function I added to the import table.
Then it jumps to the entry point.
I need to change the initial entry point becouse the program must starts at 40437F.
I simply saved the file with OllyDbg.
Now I need to change the Entry Point in Order to make the program start from 40437f.
I made the last modification with LordPe. Look at the image.



The end
BYE BYE