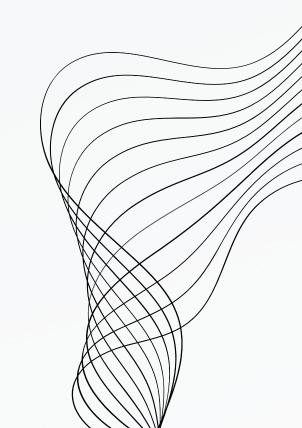
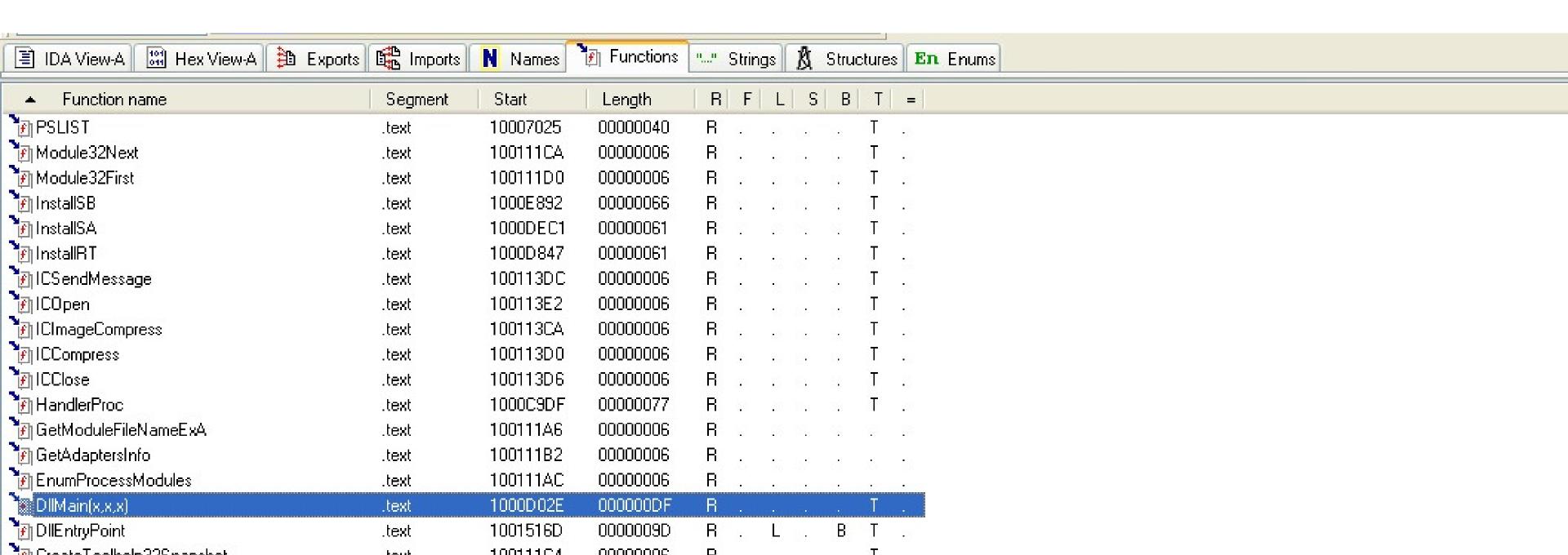


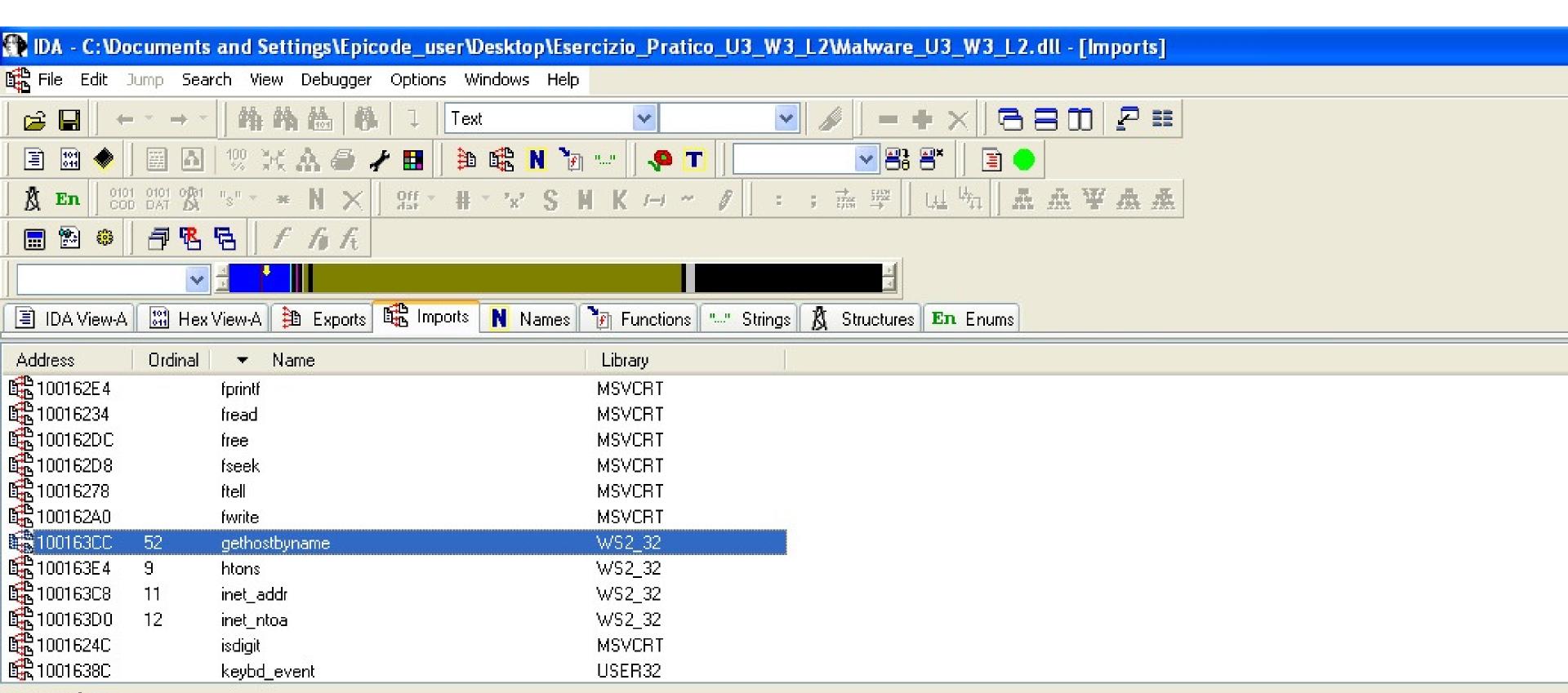
S11L2



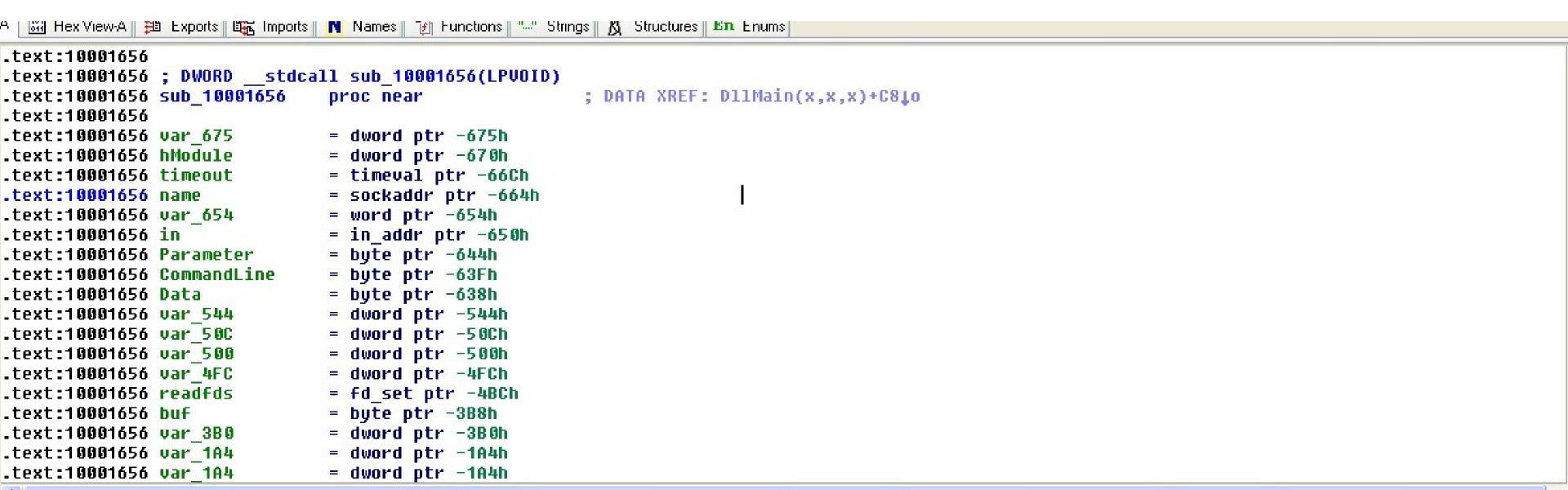
Individuare indirizzo di funzione DLLMain



L'indirizzo della funzione gethostbyname è: 100163CC



Indivduate le variabili locali (19 in totale) e i parametri (1 in totale ovvero arg0) all'indirizzo 0x10001656



La tipologia del Malware è una Backdoor

```
🚻 Hex View-A || 趙 Exports || 📺 Imports || 🙌 Names || 🗿 Functions || "--" Strings || 🐧 Structures || 🗷 Enums |
                                                        ; lpBuffer
.text:1000437C
                               push
                                       eax
                                                        ; nBufferLength
                               push
                                       edi
.text:1000437D
                                       ds:GetCurrentDirectoryA
.text:1000437E
                               call
                                       esi, ds:sprintf
.text:10004384
                               MOV
.text:1000438A
                                       eax, [ebp+buf]
                               lea
                                       .text:10004390
                               push
.text:10004395
                               push
                                                        : char *
                                       eax
                                                        ; char aBackdoorServer[]
                                       esi : sprintf
.text:10004396
                               call
                                                                                                ; DATA XREF: sub_100042DB+B510
                                                        aBackdoorServer db ODh,OAh
.text:10004398
                                       ebx, [ebp+5]
                               MOV
                                                                        db ODh, OAh
                                       eax, [ebp+buf]
.text:1000439B
                               lea
                                                                        .text:100043A1
                               push
                                       eax
                                                                          '[BackDoor Server Update Setup]', ODh, OAh
.text:100043A2
                               push
                                       ebx
                                                                        db '*********************************** , 0Dh , 0Ah
                               call
                                       sub 100038BB
.text:100043A3
                                                                        db ODh, OAh, O
                                       esp, 10h
.text:100043A8
                               add
                                       eax, [ebp+PathName]
.text:100043AB
                               lea
                                                       ; 1pPathName
.text:100043B1
                               push
                                       eax
                               call
                                       ds:SetCurrentDirectoryA
.text:100043B2
.text:100043B8
                               test
                                       eax, eax
.text:100043BA
                               jz
                                       loc 100046E1
                               lea
                                       eax, [ebp+PathName]
.text:100043C0
.text:100043C6
                               push
                                       eax
.text:100043C7
                               lea
                                       eax, [ebp+buf]
00003790
         10004390: sub 100042DB+B5
                          Down Dick: 7CB
rmation from the database ALL idle
```