

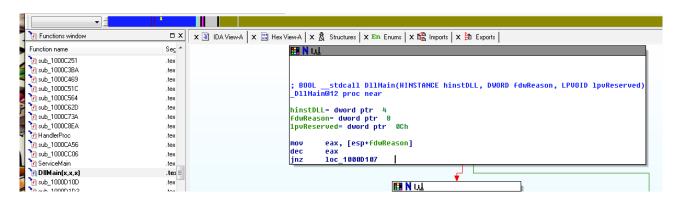


## Traccia:

Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica. A tal proposito, con riferimento al malware chiamato «Malware\_U3\_W3\_L2» presente all'interno della cartella «Esercizio\_Pratico\_U3\_W3\_L2» sul Desktop della macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti, utilizzando IDA Pro.

- 1. Individuare l'indirizzo della funzione DLLMain (così com'è, in esadecimale)
- 2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import?
- 3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?
- 4. Quanti sono, invece, i parametri della funzione sopra?
- 5. Inserire altre considerazioni macro livello sul malware

## Svolgimento:



```
.idata:100163CC ; struct hostent *__stdcall pethostbyname (const char *name)
.idata:100163CC extrn pethostbyname dword
.idata:100163CC ; struct hostent *__stdcall pethostbyname dword
.idata:100163CC extrn pethostbyname dword
.idata:100163CC ; sub_1000107
.idata:100163CC ; sub_10001074+1D3↑p ...
```

```
push
         edi
                          ; lpParameter
push
         offset sub 10001656; lpStartAddress
                     w
push
         edi
                          : dwStackSize
                     readfds= fd_set ptr -48Ch
push
         edi
         ebx ; CreatephkResult= byte ptr -388h
call
                     var_380= dword ptr -380h
         edi
pop
                      var_1A4= dword ptr -1A4h
pop
         esi
         ds:dword 10(var_194= dword ptr -194h
mov
                      WSAData= WSAData ptr -190h
pop
                     arg 0= dword ptr 4
                N Lsub
                              esp, 678h
                      push
                              ebx
0000C4F6
        1000D0F6: DIIMain(x,x,x)+C8
```