CONSEGNA

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? Cosa fa la funzione?

3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?

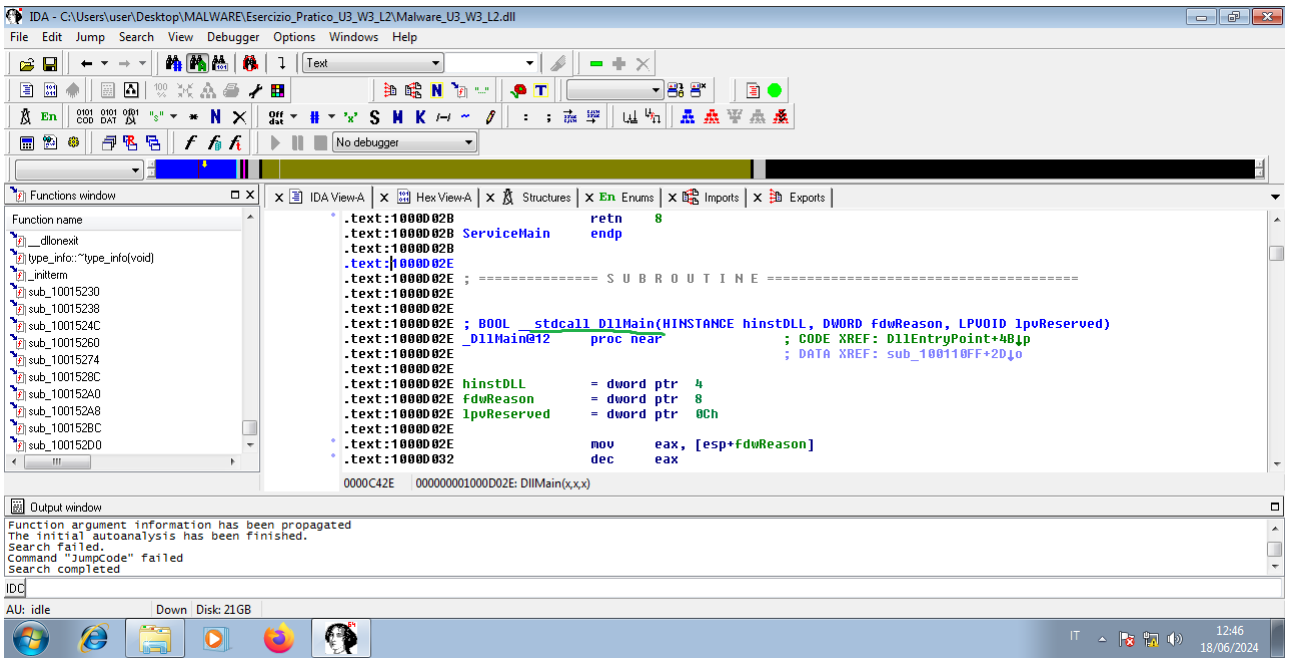
4. Quanti sono, invece, i parametri della funzione sopra?

5. Inserire altre considerazioni macro livello sul malware (comportamento)

SVOLGIMENTO

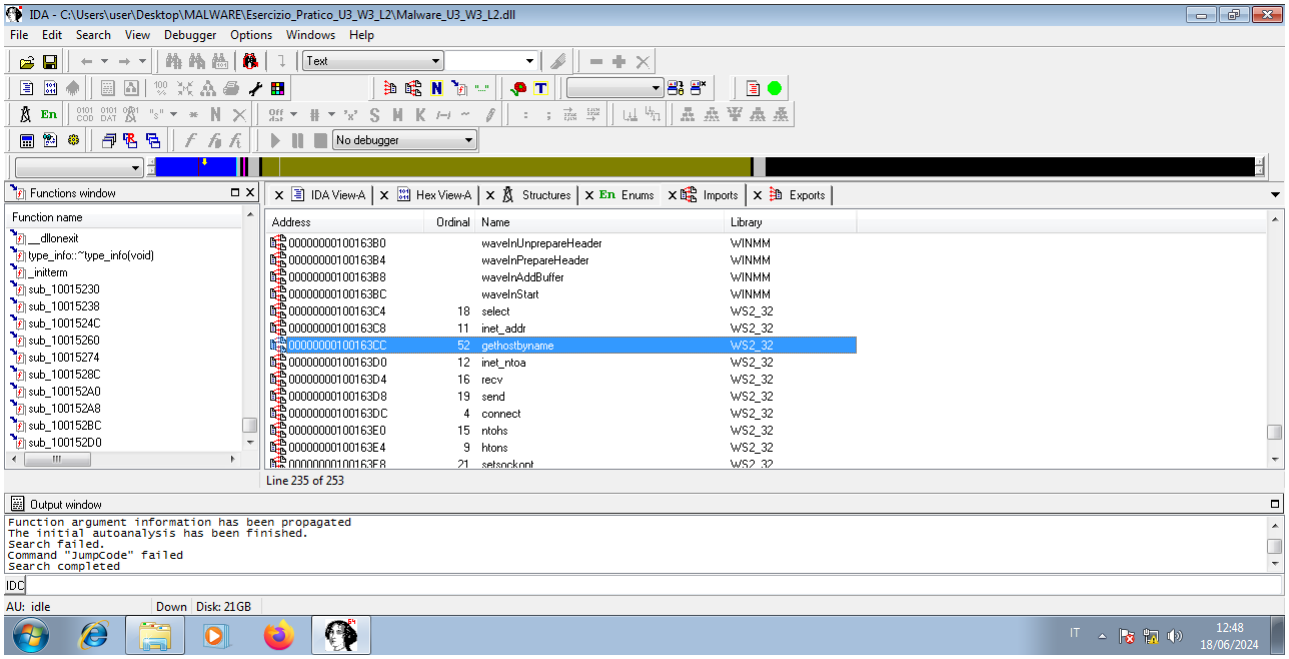
Dopo Aver aperto il malware con IDA, ci comparirà la "mappa" della struttura del codice assembly (versione grafica).

Per passare alla versione testuale, premiamo barra spaziatrice e ci spostiamo fino a trovare la funzione "stdcall_DllMain", che è proprio quella che ci viene richiesta dall'esercizio e serve a richiamare delle librerie.



L'indirizzo della funzione è **1000D02E.** Vediamo come la funzione richiede dei parametri che gli vengono passati (funzioni "dword").

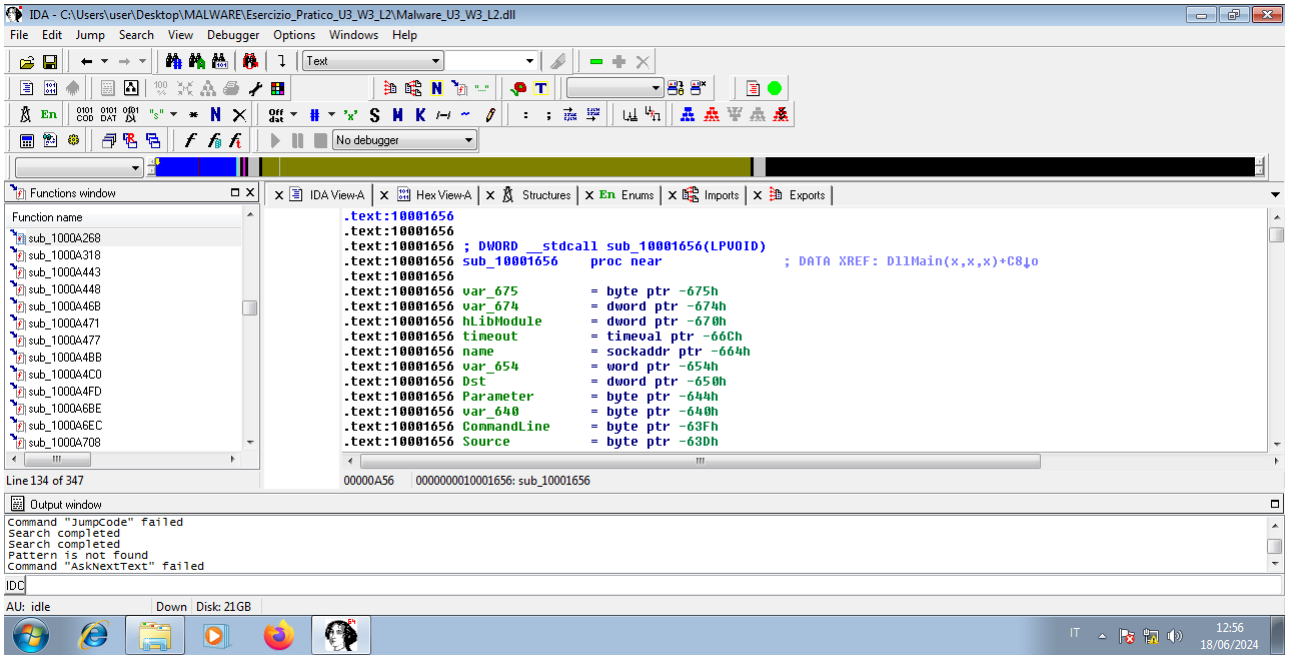
Ci spostiamo poi in “import” e scorriamo finché non troviamo la funzione cercata (gethostbyname)

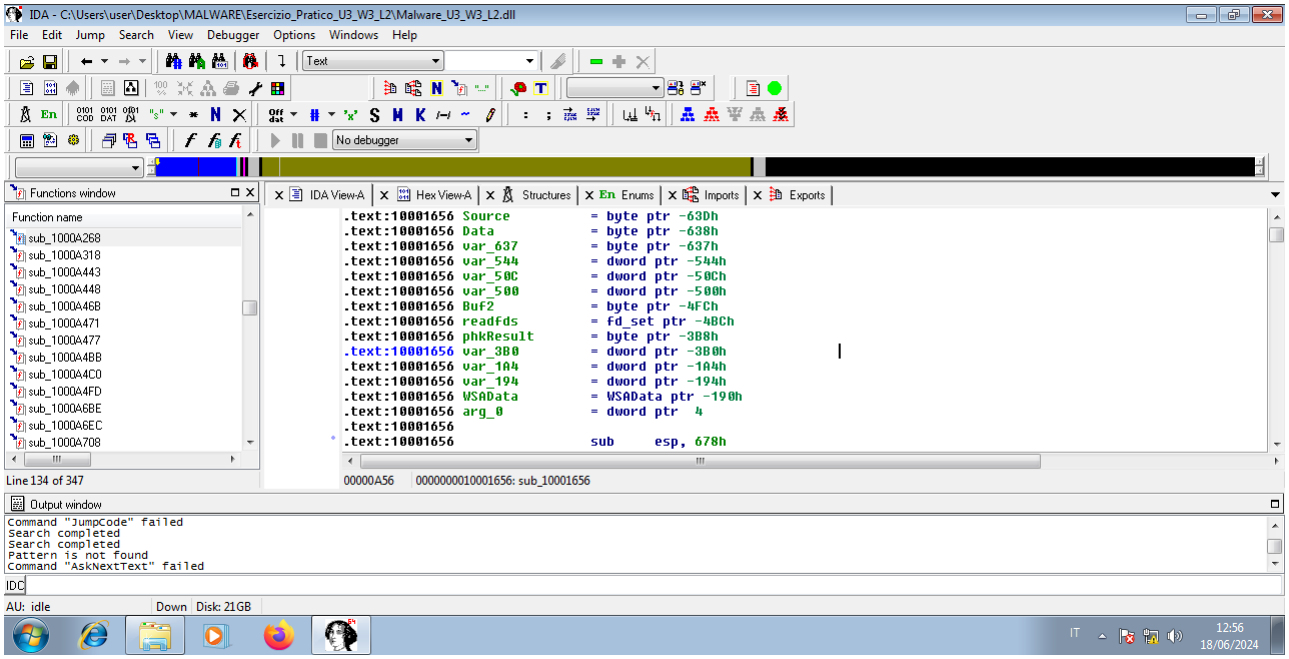


La funzione si trova all’indirizzo **100163CC**.

Si tratta di una funzione particolarmente pericolosa, poiché **estrapola l’IP ed altre informazioni** sensibili dalla macchina Host.

Le variabili della prima funzione esposta, all’indirizzo 1000D02E sono **20**; possiamo affermare che si tratta di variabili e non di parametri, poiché queste hanno valore negativo e il modulo di questo numero rappresenta la distanza rispetto ad EBP.




IDA - C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W3_L2\Malware_U3_W3_L2.dll
File Edit Jump Search View Debugger Options Windows Help
Text
No debugger
Functions window
Function name
sub_1000A268
sub_1000A318
sub_1000A443
sub_1000A448
sub_1000A46B
sub_1000A471
sub_1000A477
sub_1000A4BB
sub_1000A4C0
sub_1000A4FD
sub_1000A6BE
sub_1000A6EC
sub_1000A708
Line 134 of 347
IDA View-A
Hex View-A
Structures
Enums
Imports
Exports
.text:10001656 Source = byte ptr -63Dh
.text:10001656 Data = byte ptr -638h
.text:10001656 var_637 = byte ptr -637h
.text:10001656 var_544 = dword ptr -544h
.text:10001656 var_50C = dword ptr -50Ch
.text:10001656 var_500 = dword ptr -500h
.text:10001656 Buf2 = byte ptr -4FCh
.text:10001656 readfds = fd_set ptr -4BCh
.text:10001656 phkResult = byte ptr -3B8h
.text:10001656 var_3B0 = dword ptr -3B0h
.text:10001656 var_1A4 = dword ptr -1A4h
.text:10001656 var_194 = dword ptr -194h
.text:10001656 WSAData = WSAData ptr -190h
.text:10001656 arg_0 = dword ptr 4
.text:10001656
.text:10001656 sub esp, 678h
00000A56 0000000010001656: sub_10001656
Output window
Command "JumpCode" failed
Search completed
Search completed
Pattern is not found
Command "AskNextText" failed
IDC
AU: idle Down Disk: 21GB
IT
12:56
18/06/2024