

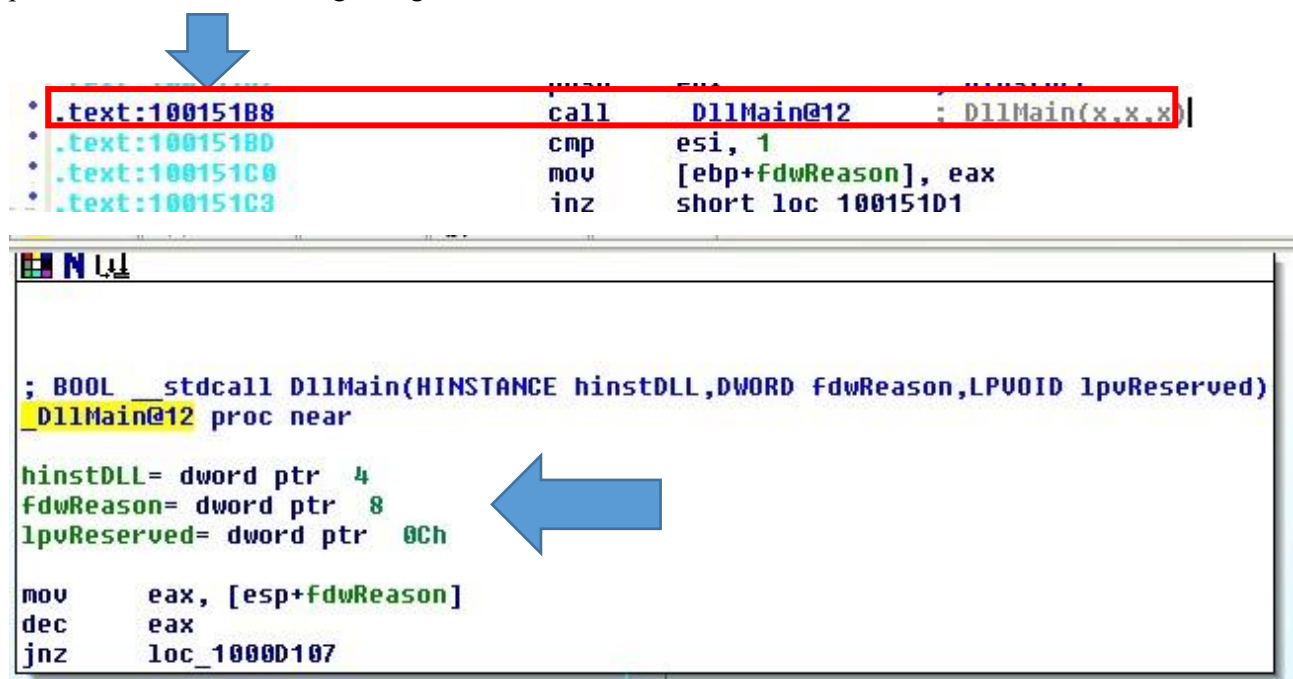
Obbiettivo: Con riferimento al Malware_U3_W3_L2 sulla Virtual Machine dedicata all'analisi dei Malware, rispondere ai seguenti quesiti.

1. Individuare l'indirizzo della funzione DLLMain
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?

Prima Parte

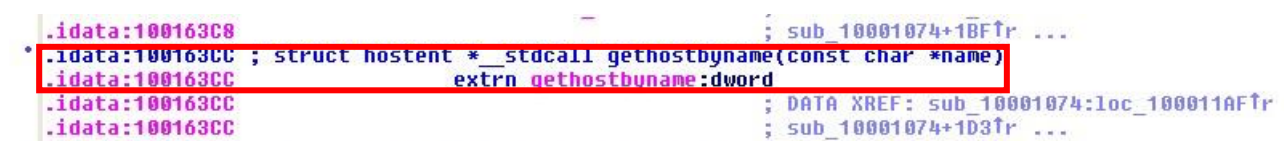
Per lo svolgimento di questa esercitazione useremo il tool **disassembler IDA pro free**, che ci tradurrà in **Assembly** il linguaggio macchina del nostro Malware in analisi.

Andiamo quindi a caricare il nostro Malware e analizziamo il codice tradotto, abbiamo subito ricavato la porzione di codice e l'indirizzo della funzione **DLLMain**, che risulta essere nella locazione **100151B8** come possiamo vedere nell'immagini seguenti.



Seconda Parte

Nella seconda parte di analisi consultiamo la **scheda degli imports**, abbiamo così individuato anche l'indirizzo di memoria della funzione richiesta, **gethostbyname**, che risulta essere **100163CC**.



Terza Parte

Nella terza e ultima parte andiamo ad analizzare la locazione di memoria 0x10001656, dove abbiamo individuato **20 variabili locali importate** dalla funzione, le possiamo riconoscere dal simbolo negativo che l'interfaccia di IDA pro associa ad esse. Mentre troviamo **un solo parametro** che al contrario viene associato ad un offset positivo.

The screenshot shows the IDA Pro interface with the disassembly window open. The function being analyzed is `sub_10001656`, which is a `proc near` function. The list of local variables is displayed, with their offsets relative to the stack frame. The variable `arg_0` is highlighted in red, indicating it is the only parameter of the function. A red arrow points from `arg_0` to a box labeled "Parametro della funzione". Blue arrows point to the negative offsets of the local variables, indicating they are imported from the stack.

Offset	Variable Name	Offset	Variable Name
var_675	= byte ptr -675h	var_4FC	= dword ptr -4FCh
var_674	= dword ptr -674h	readfds	= fd_set ptr -4BCh
hModule	= dword ptr -670h	phkResult	= HKEY__ ptr -3B8h
timeout	= timeval ptr -66Ch	var_3B0	= dword ptr -3B0h
name	= sockaddr ptr -664h	var_1A4	= dword ptr -1A4h
var_654	= word ptr -654h	var_194	= dword ptr -194h
in	= in_addr ptr -650h	WSAData	= WSAData ptr -190h
Parameter	= byte ptr -644h	arg_0	= dword ptr 4
CommandLine	= byte ptr -63Fh		
Data	= byte ptr -638h		
var_544	= dword ptr -544h		
var_50C	= dword ptr -50Ch		
var_500	= dword ptr -500h		

sub esp, 678h