Gabriele Di giampietro **Esercitazione 17/01/2023**

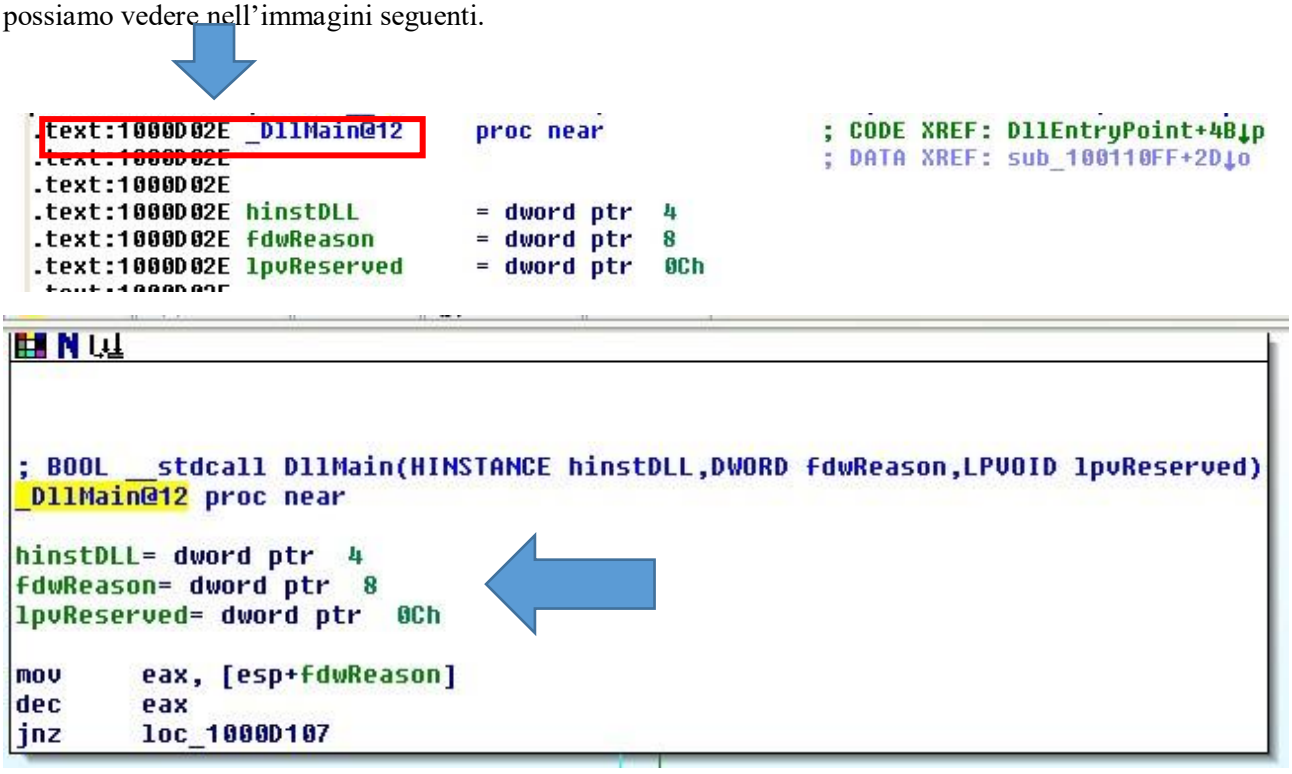
Obbiettivo: Con riferimento al Malware_U3_W3_L2 sulla Virtual Machine dedicata all'analisi dei Malware, rispondere ai seguenti quesiti.

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 0×10001656?
4. Quanti sono, invece, i parametri della funzione sopra?

Prima Parte

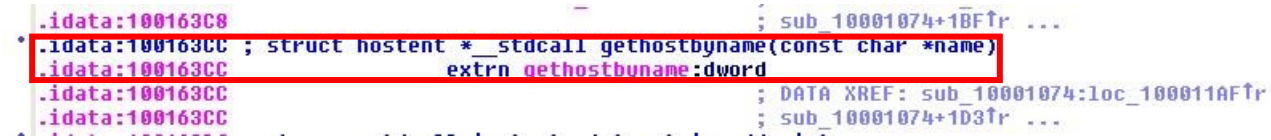
Per lo svolgimento di questa esercitazione useremo il tool **disassembler IDA pro free,** che ci tradurrà in **Assembly** il linguaggio macchina del nostro Malware in analisi.

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 **1000D02E** come possiamo vedere nell'immagini seguenti.



Seconda Parte

Nella seconda parte di analisi consultiamo la **scheda degli imports**, abbiamo cosi 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 paramento** che al contrario viene associato ad un offset positivo.