S11/L2

Analisi Statica con IDA Pro

Stefano Di Prospero

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)

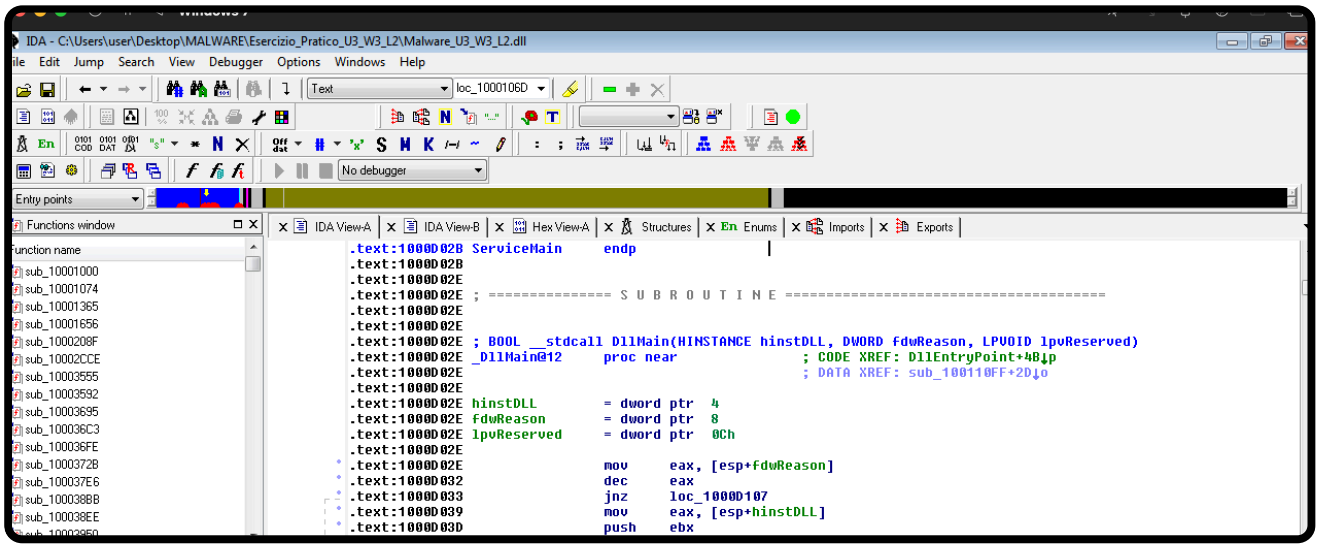
2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import? Cosa fa la funzione?

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

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

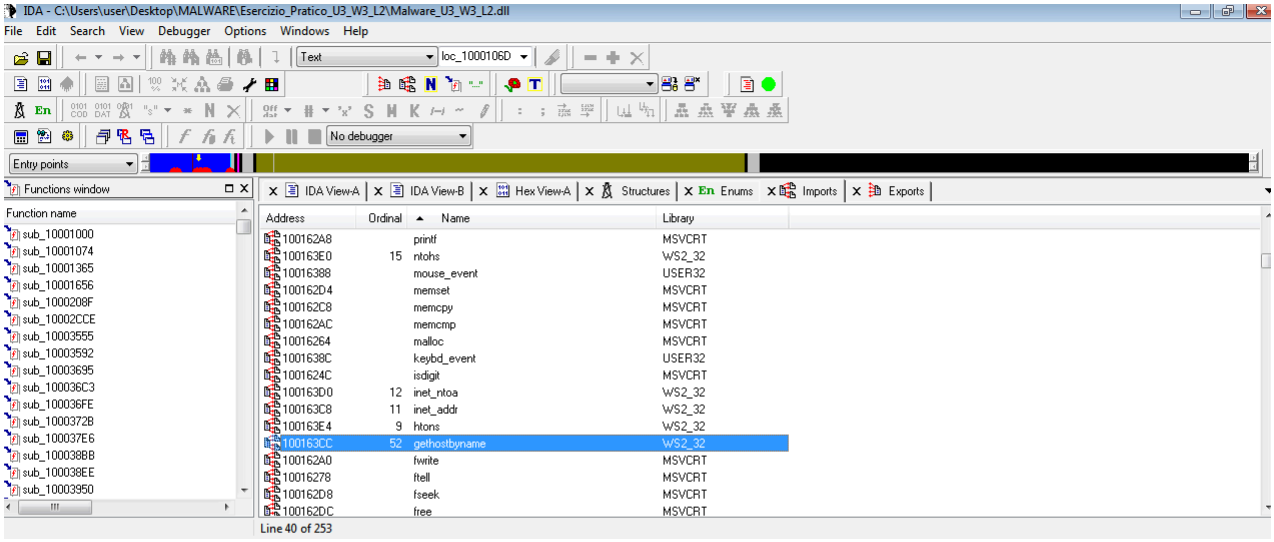
5. Inserire altre considerazioni macro livello sul malware (comportamento)

1)



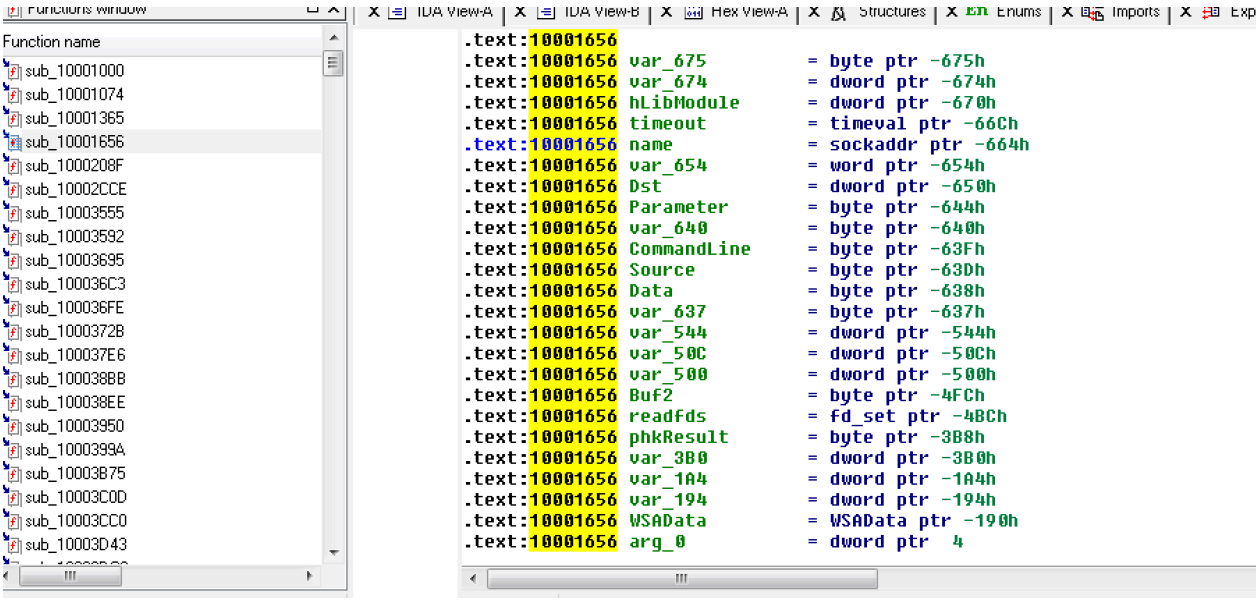
L’Indirizzo del DLLMain è 1000D02E

2)



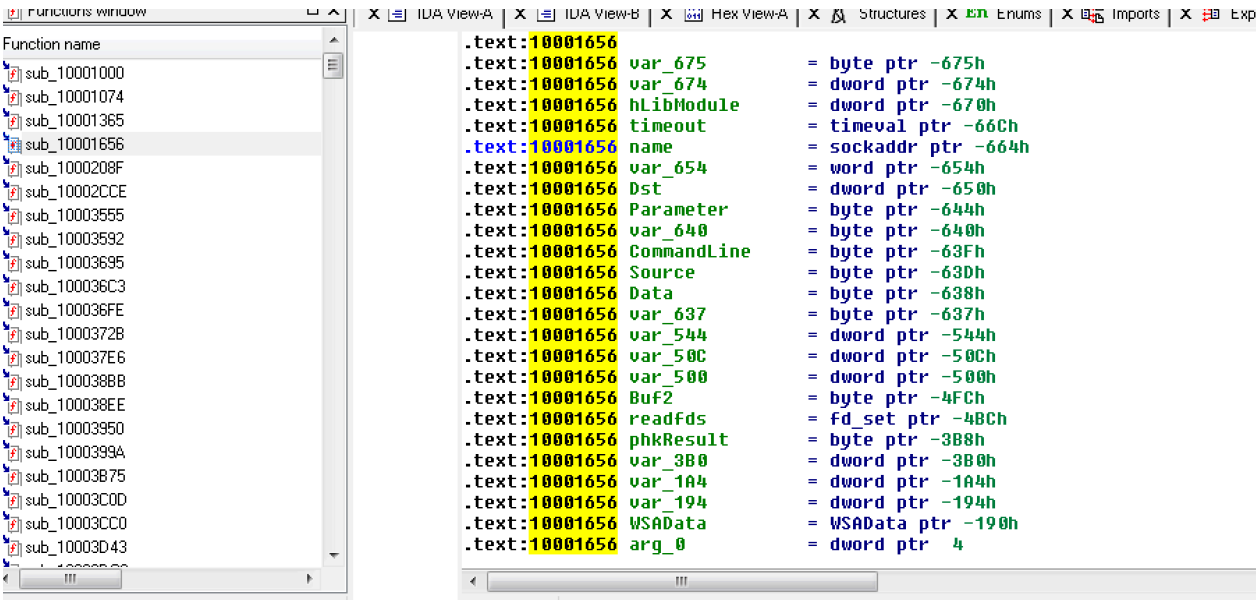
L’Indirizzo della funzione “*gethostbyname*” è 100163CC. Questa funzione si occupa di recuperare l’indirizzo IP associato ad un nome host.

3)



Nell’indirizzo 10001656 si contano, come da figura, 23 variabili. Queste variabili hanno un offset negativo.

4)



L’unico parametro constante risulta l’unico con offset positivo, ovvero “*arg_0*”.

5) Dalle funzioni richiamate e dall’analisi dell’hash il malware sembra essere una backdoor.