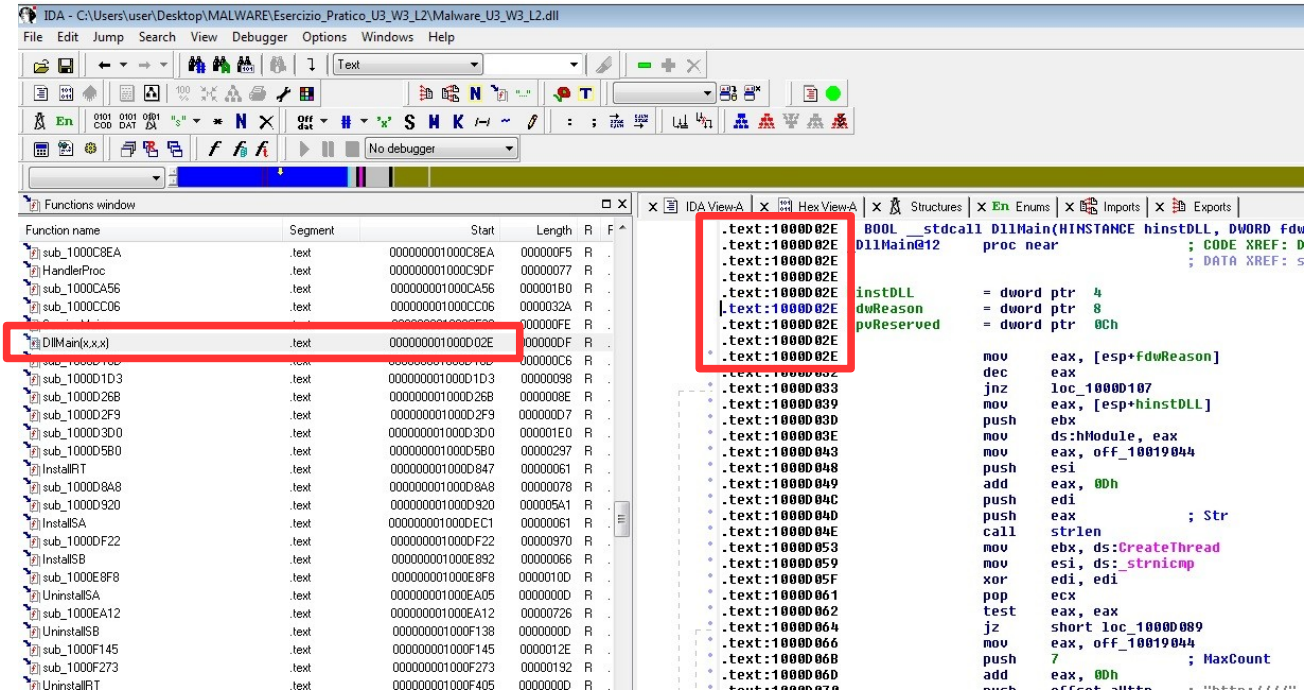
Esercizio settimana 11 lezione 2 Daniele D'Esposito

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.

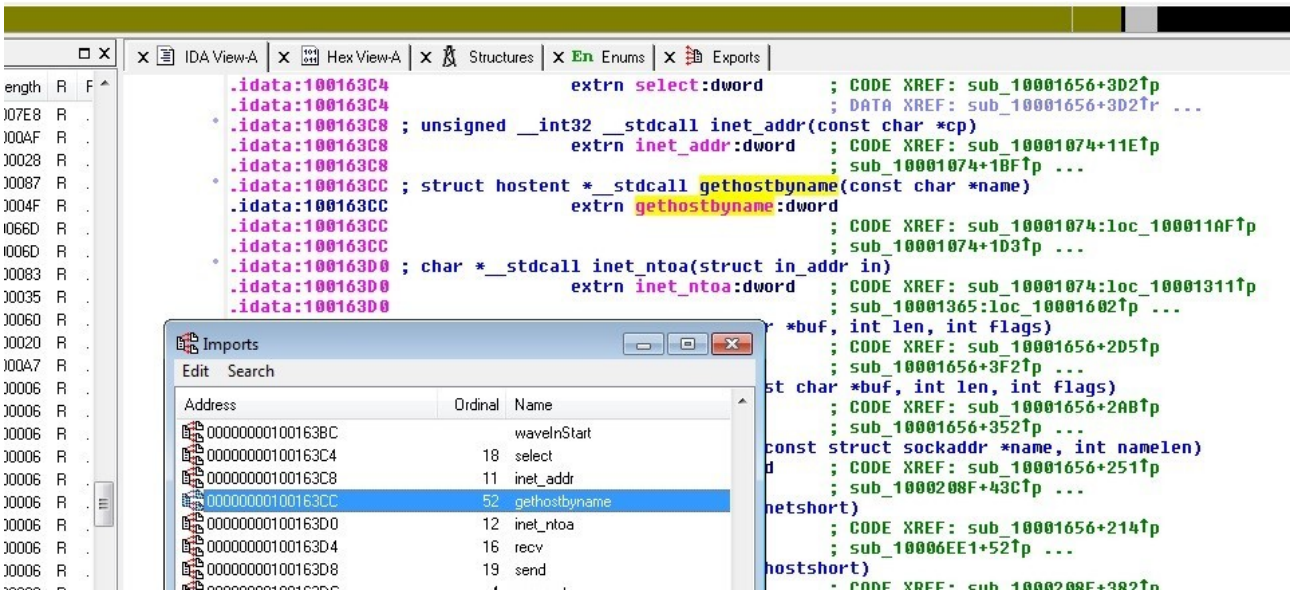
1. Individuare l'indirizzo della funzione DLLMain(così com'è, in esadecimale)
2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import? Cosa fa la funzione?
3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?
4. Quanti sono,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

Individuare l'indirizzo della funzione DLLMain(così com'è, in esadecimale)



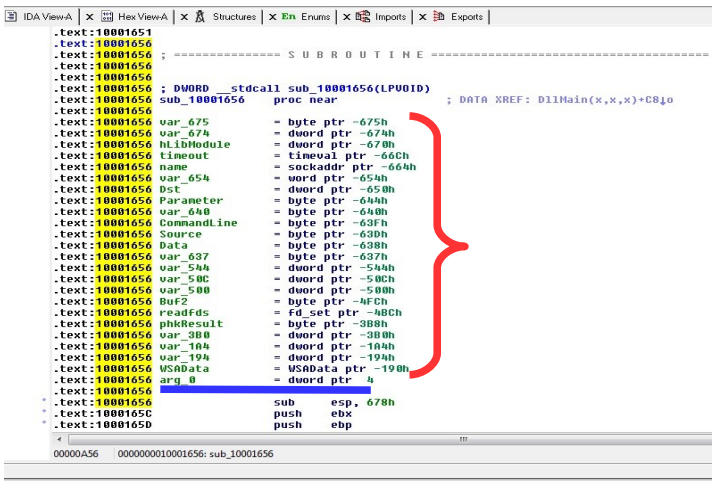
L'indirizzo della funzione DllMain e' **1000D02E**

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



La funzione **gethostbyname** della libreria **winsock.h** recupera le informazioni host corrispondenti ad un nome host da un database host; e' stata rimpiazzata dalla funzione **getaddrinfo**.
L'indirizzo in questo malware e' **100163CC**.

Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656? Quanti sono, invece, i parametri della funzione sopra?



La funzione **stdcall** nella locazione di memoria **10001656** ha **23** variabili; sono segnate con un valore negativo rispetto al registro EBP(graffa rossa dell'immagine).
I parametri invece sono solo **1**; sono segnati con un valore positivo rispetto al registro EBP(riga blu dell'immagine).

Inserire altre considerazioni macro livello sul malware (comportamento)

Non sono in grado di comprendere il comportamento generale del malware; mi ci vorrebbe troppo tempo per analizzarlo