2024

EPICODE

CS0124

REPORT

Week 11 Lesson 2

PREPARED BY : Bruno Falconi

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.

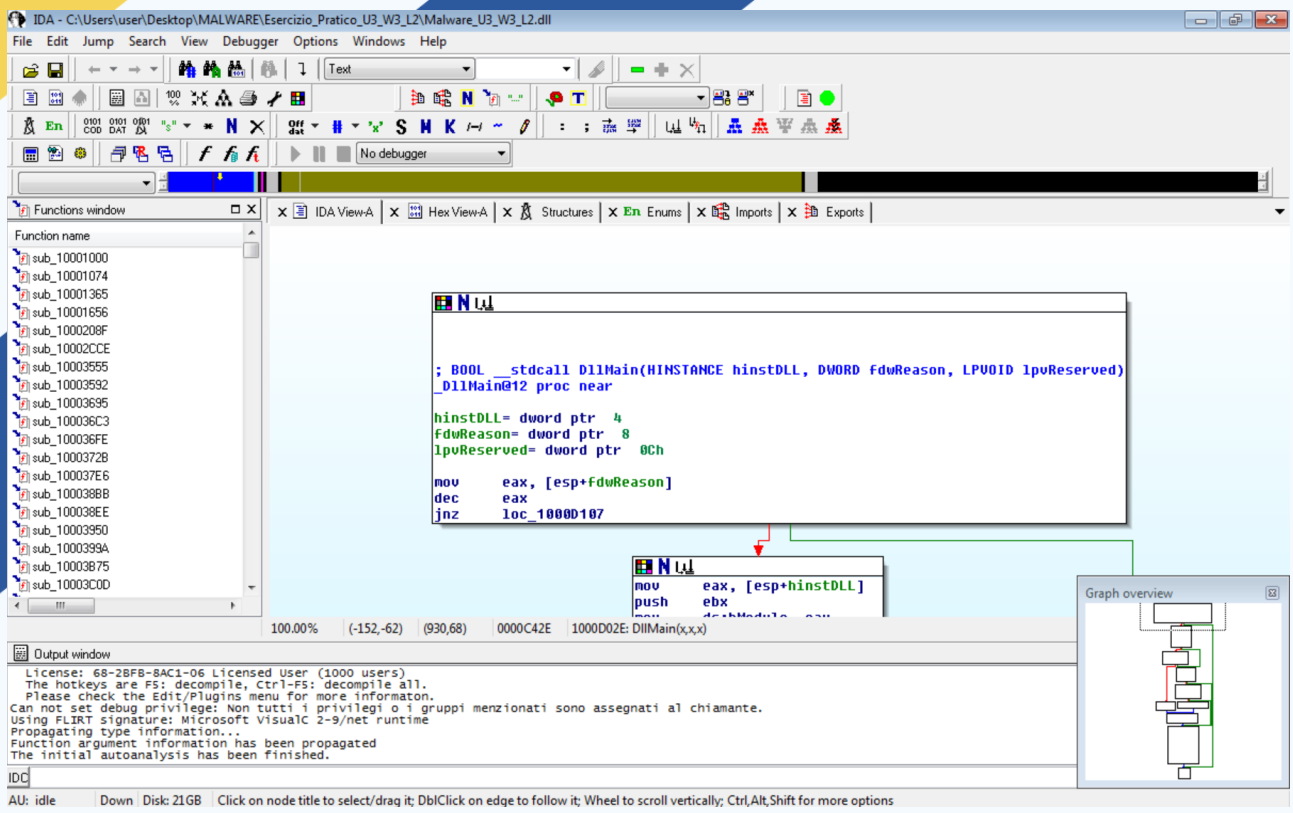
1. Individuare l'indirizzodella funzione DLLMain(così com'è, in esadecimale) 2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import? Cosa fa la funzione?

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

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

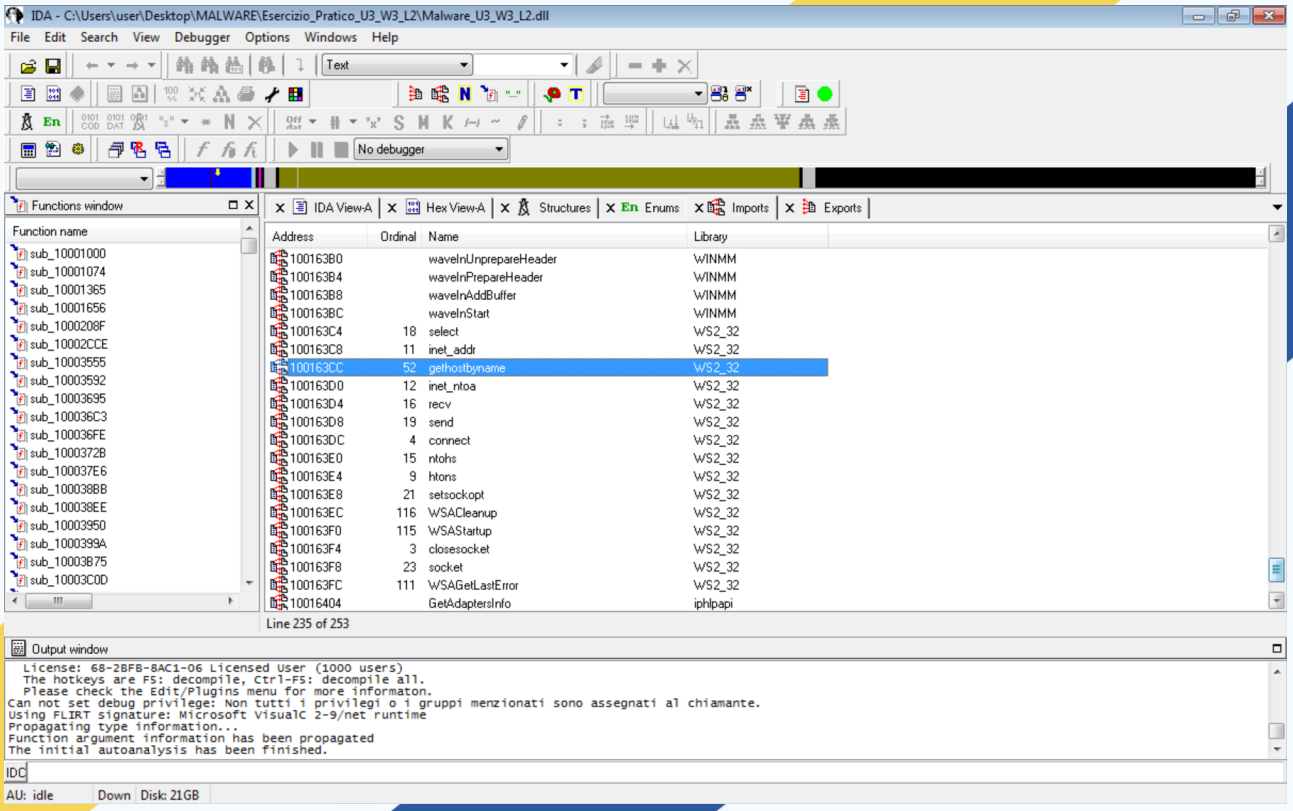
5. Inserire altre considerazioni macro livello sul malware (comportamento)

1. Individuare l'indirizzodella funzione DLLMain(così com'è, in esadecimale)



Come si può vedere l'indirizzo della funzione Main è 100D02E

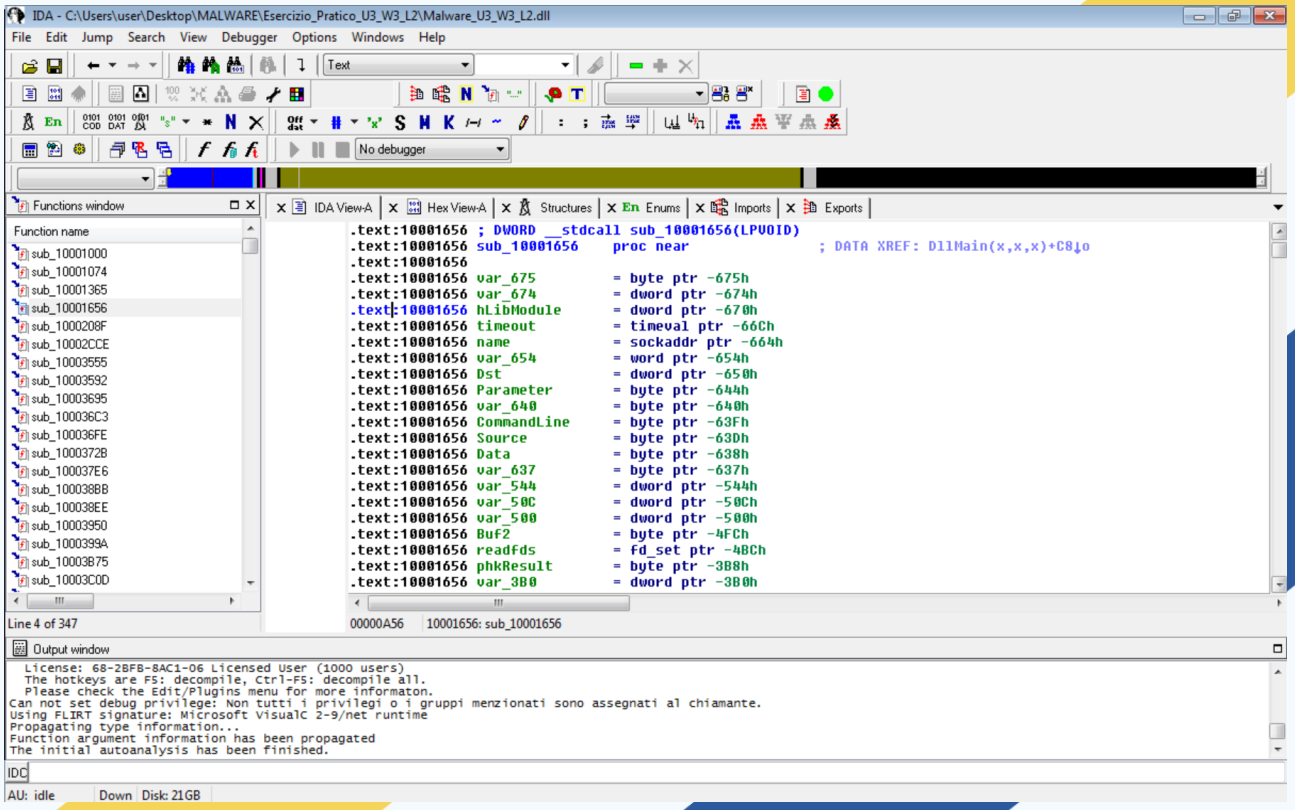
2. **Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import? Cosa fa la funzione?**



L'indirizzo dell'import è il 100163CC per quello che riguarda la funzione richiesta. La funzione gethostbyname() è una funzione di libreria standard in diversi linguaggi di programmazione, come C e C++, utilizzata per ottenere informazioni sulle informazioni di un host tramite il suo nome host.

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

Ci sono ventitrè variabili locali della funzione ala locazione di memoria 0x10001656



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

I parametri della funzione sono uno soltanto