

Traccia:

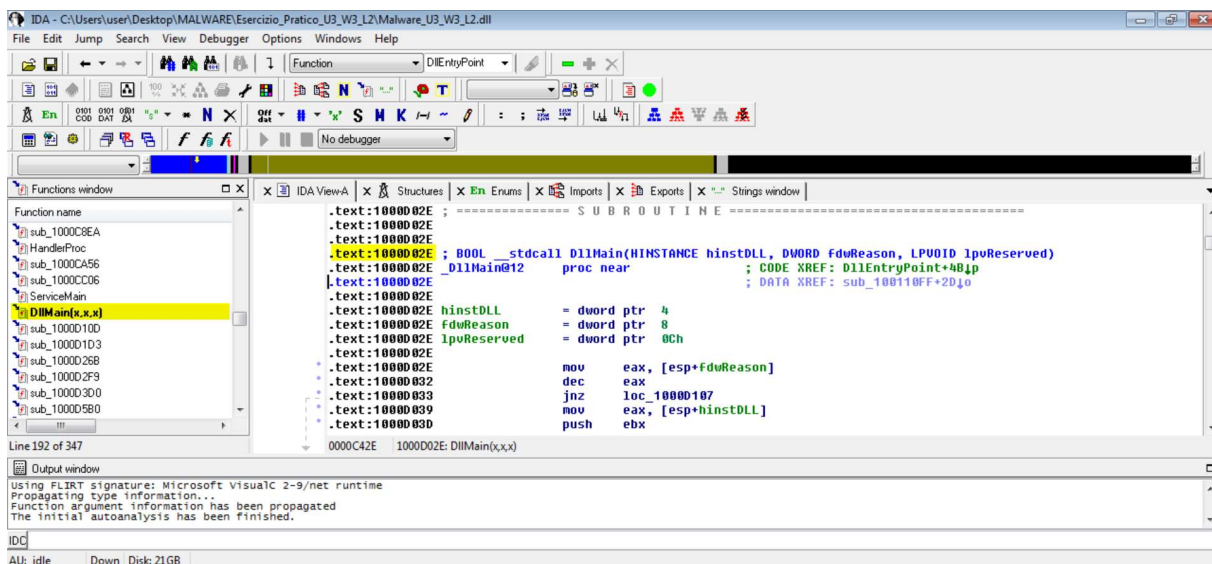
Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica.

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

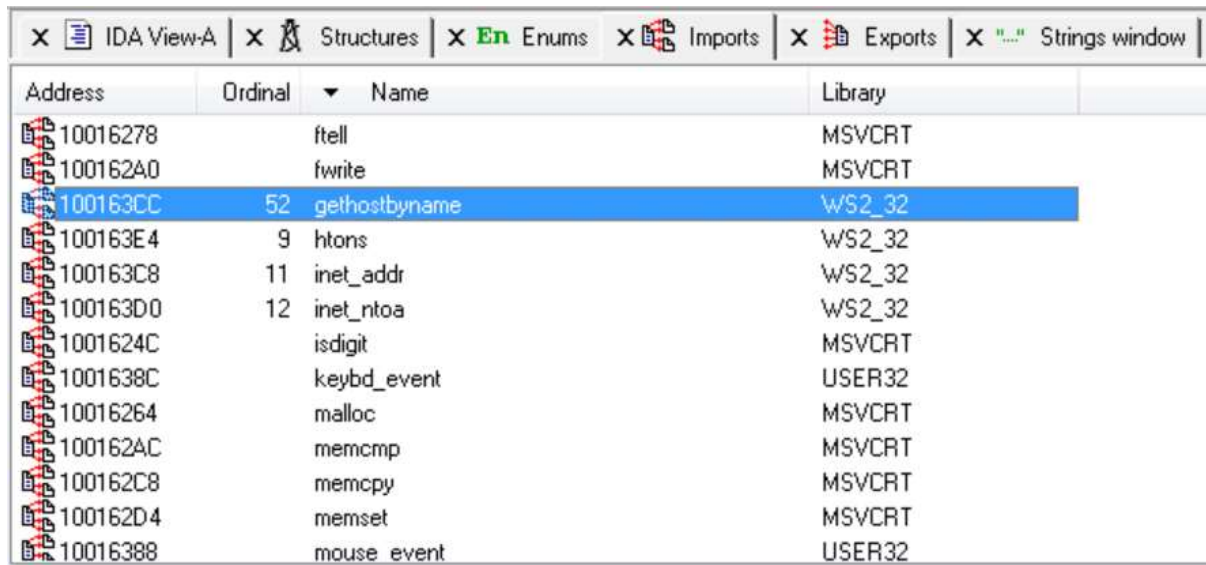
Soluzione

1.



Tramite il tab di sinistra Function name riusciamo a rintracciare tutte le funzioni presenti e tramite una semplice ricerca troviamo la DllMain e tramite un semplice click viene intercettata la dichiarazione a codice.

2.



Address	Ordinal	Name	Library
10016278		ftell	MSVCRT
100162A0		fwrite	MSVCRT
100163CC	52	gethostname	WS2_32
100163E4	9	htons	WS2_32
100163C8	11	inet_addr	WS2_32
100163D0	12	inet_ntoa	WS2_32
1001624C		isdigit	MSVCRT
1001638C		keybd_event	USER32
10016264		malloc	MSVCRT
100162AC		memcmp	MSVCRT
100162C8		memcpy	MSVCRT
100162D4		memset	MSVCRT
10016388		mouse_event	USER32

3. 23 locali variabili locali

4. 1 parametro