Analisi statica avanzata con IDA

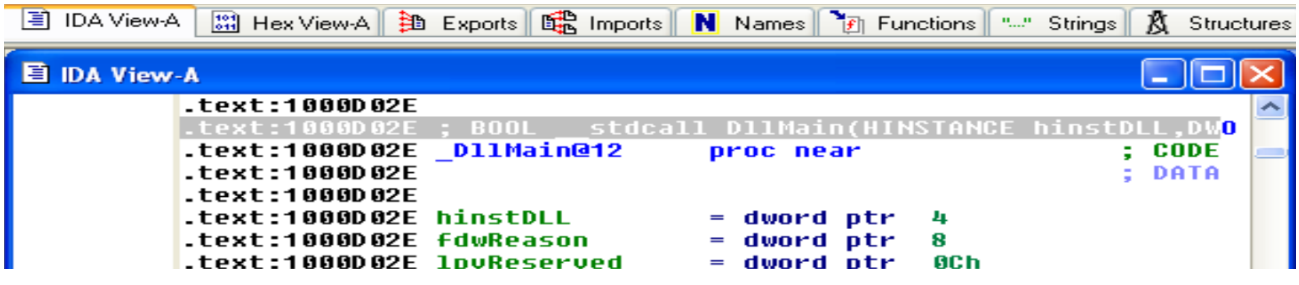
Con riferimento ad un malware chiamato «Malware_U3_W3_L2» presente all'interno della cartella «Esercizio_Pratico_U3_W3_L2» sul Desktop della macchina virtuale Windows XP dedicata all'esercitazione dell'analisi dei malware, rispondere ai seguenti quesiti utilizzando IDA Pro:

- **1)** Individuare l'indirizzo della funzione DLLMain;
- **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).

SOLUZIONI:

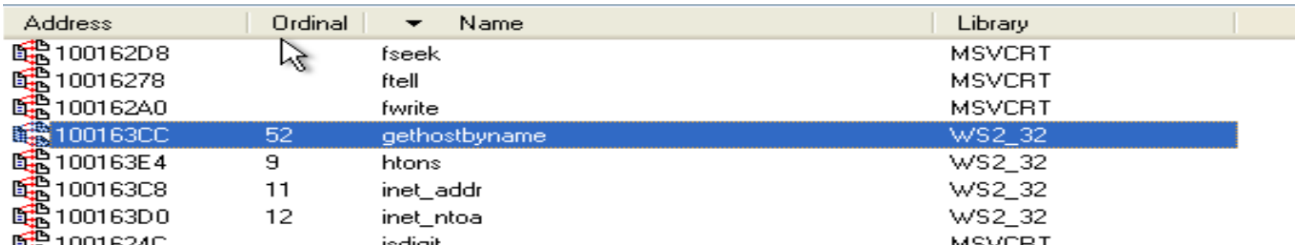
Dopo aver impostato la macchina virtuale per l'analisi malware, ossia in rete interna per non avere accesso ad internet, ed aver scollegato ogni possibile contatto con la macchina host ed i dispositivi di archiviazione esterna, procedo con le soluzioni:

1)



L'indirizzo della funzione "DLLMain" è "1000D02E";

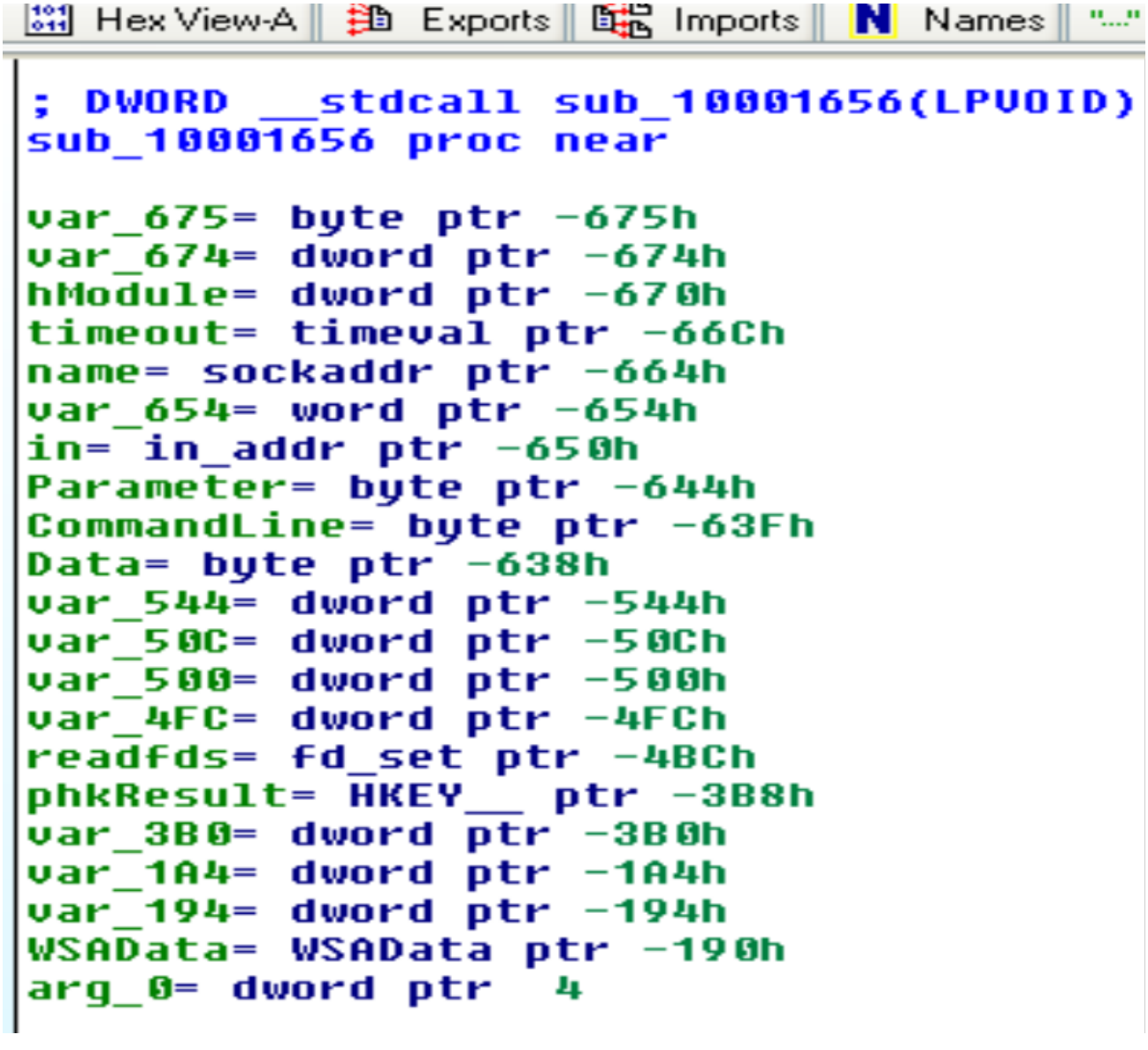
2)



Address	Ordinal	Name	Library
100162D8		fseek	MSVCRT
10016278		ftell	MSVCRT
100162A0		fwrite	MSVCRT
100163CC	52	gethostbyname	WS2_32
100163E4	9	htons	WS2_32
100163C8	11	inet_addr	WS2_32
100163D0	12	inet_ntoa	WS2_32

L'indirizzo della funzione "gethostbyname" nella scheda "imports" è "100163CC", questa funzione ridà l'indirizzo IP di un host richiesto, come una specie di DNS.

3 + 4)



Nella locazione di memoria "10001656" si trovano 20 variabili (tutte quelle con offset negativo) mentre l'unico parametro (con offset positivo) è "arg0" in fondo.

5) Le macro considerazioni sul comportamento del malware mi portano a pensare che, avendo molte chiamate di funzioni di rete come socket, chiamate di funzioni

per librerie Windows e comparazioni di stringhe, si tratta probabilmente di uno spyware.