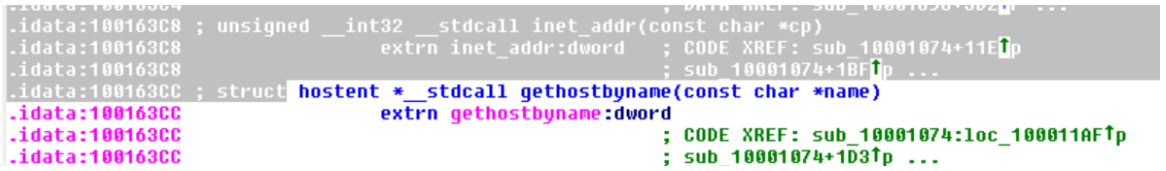
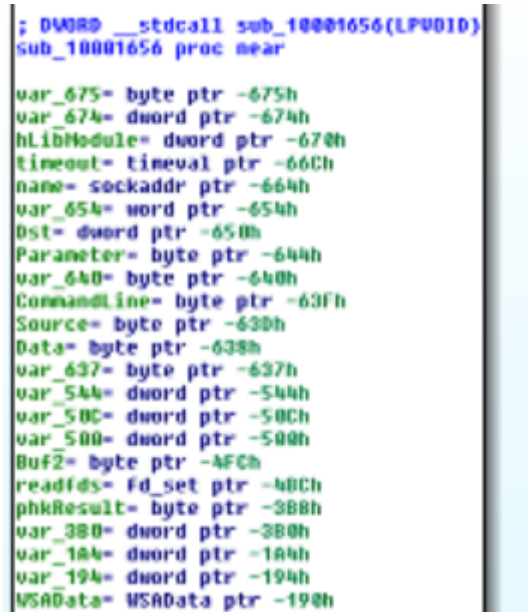
Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica. A tal proposito, con riferimento al malware chiamato «Malware_U3_W3_L2» presente all'interno della cartella «Esercizio_Pratico_U3_W3_L2» sul Desktop della macchina virtuale dedicata all'analisi 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?

1. 

2. 

La funzione gethostbyname è una funzione utilizzata per ottenere informazioni associate a un nome host. È una funzione di sistema che restituisce una struttura di tipo 'hostent' contenente informazioni come l'indirizzo IP associato al nome host, l'elenco degli alias del nome host e altri dettagli.

3. 

Capiamo che sono variabili perchè hanno un risultato negativo mentre con risultato positivo sono i parametri.

4. 
```
WSAData= WSAData ptr -190h
arg_0= dword ptr  4
```
   Il parametro è solo uno ed è quello con il risultato positivo.

5. Il malware in teoria è un trojan che tramite backdoor può instaurare connessioni o eseguire comandi in background