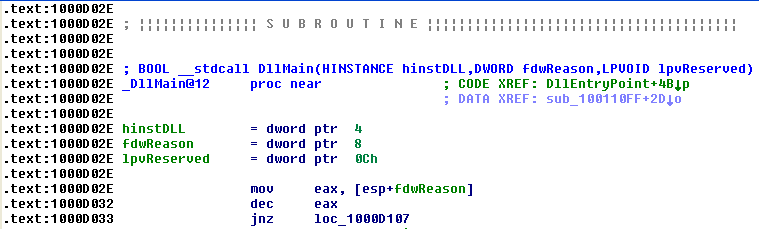
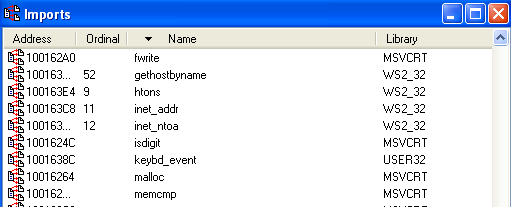
**ANALISI STATICA AVANZATA CON IDA**

**TRACCIA**

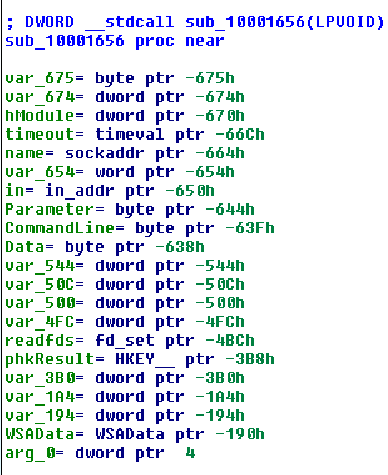
Lo scopo dell’esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l’analisi statica. A tal proposito, con riferimento al malware chiamato «Malware\_U3\_W3\_L2» presente all’interno della cartella «Esercizio\_Pratico\_U3\_W3\_L2» sul Desktop della macchina virtuale dedicata all’analisi 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).

**ESERCIZIO**

1) L’indirizzo è 1000D02E.

2)

La chiamata GETHOSTBYNAME restituisce il nome e l’IP di un host specificato nella chiamata.   
Un dato host TCP/IP può avere più nomi alias e più indirizzi Internet host.

  
  
3-4) Variabili e Parametri  
  
  
Possiamo trovare 20 variabili (offset   
negativi rispetto ad EBP)  
e 1 parametro (offset positivi rispetto  
ad EBP).

5) Tramite l’utilizzo di CFF Explorer, ci procuriamo l’hash del malware e tramite VirusTotal abbiamo potuto vedere che si tratta di una backdoor.