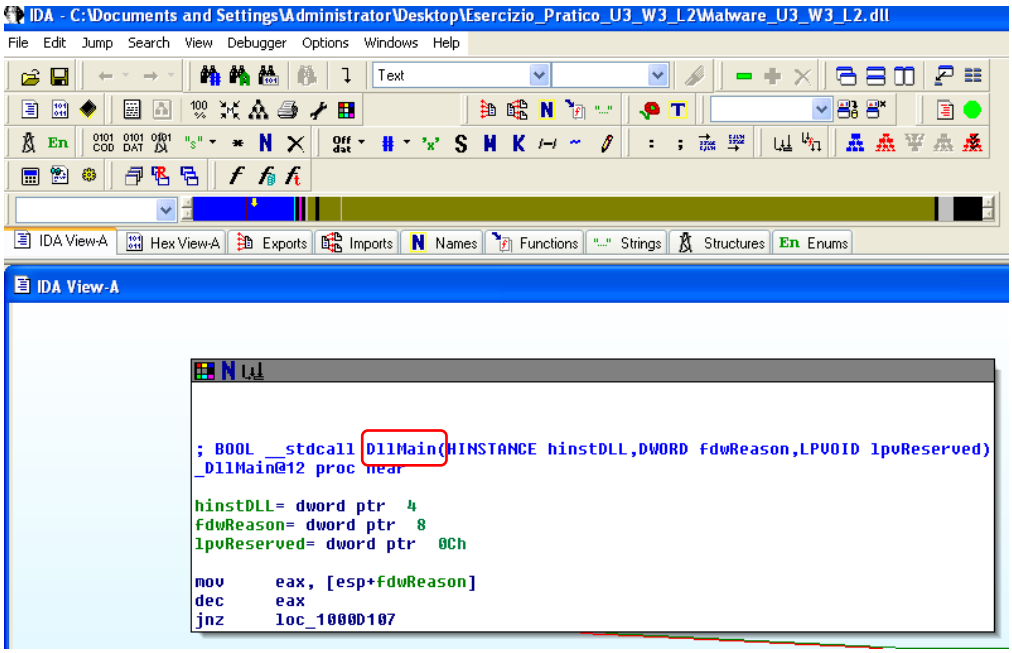
Analisi statica avanzata con IDA

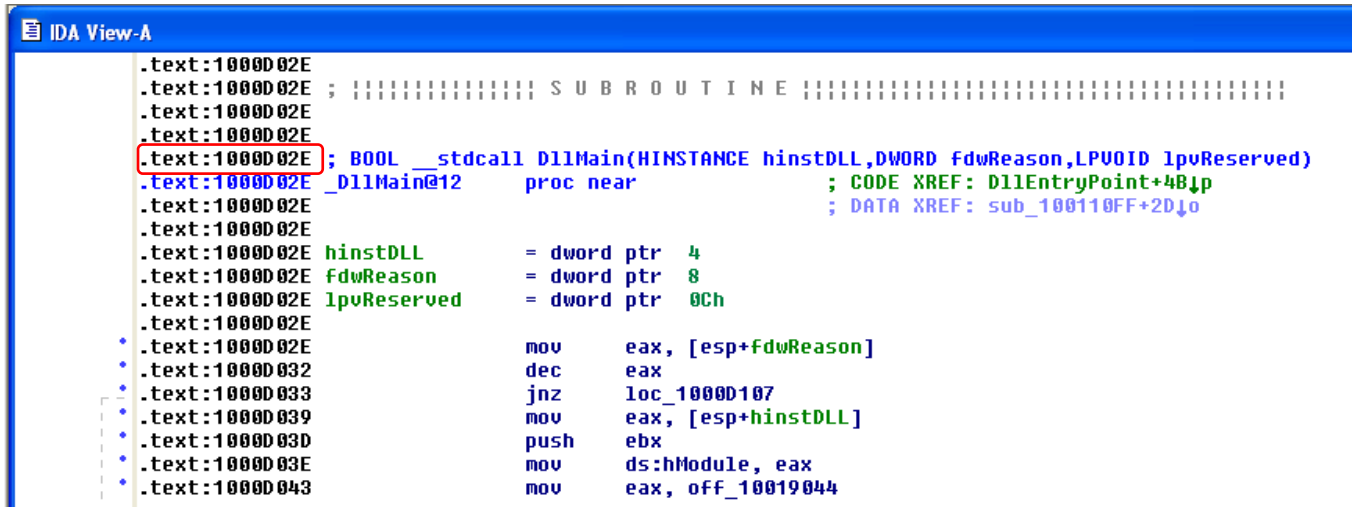
Malware_U3_W3_L2

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

Nel pannello centrale di IDA vengono mostrate le traduzioni in Assembly del codice macchina dell'eseguibile (in questo caso **Malware_U3_W3_L2.dll**). Nel rettangolo rosso vediamo la funzione DllMain.

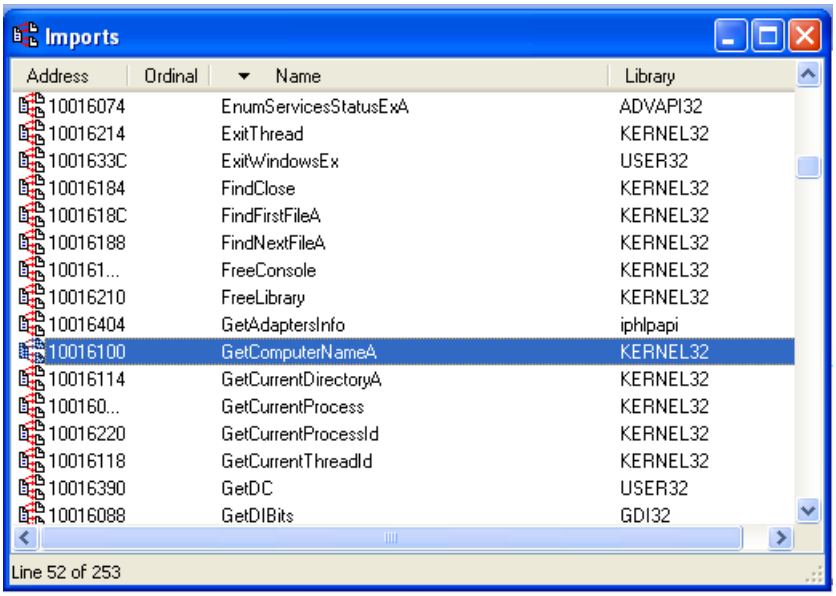


Premendo la barra spaziatrice si attiva la versione testuale dell'interfaccia grafica vista prima. Da qua possiamo vedere che la funzione **DllMain si trova all'indirizzo 1000D02E.**



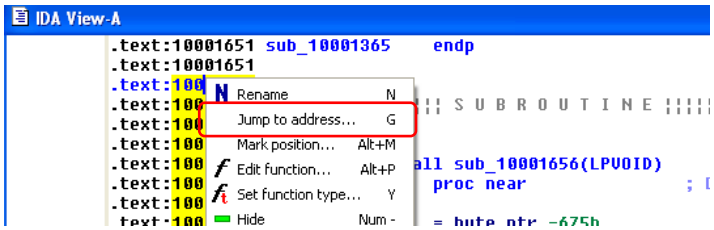
2. **Dalla scheda “Imports” individuare la funzione “GetComputerName”. Qual è l’indirizzo dell’import?**

La scheda Imports mostra le funzioni importate dall’eseguibile. La prima colonna, Address, specifica l’indirizzo della funzione, che come evidenziato nell’immagine è **10016100.**



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

Dall’interfaccia testuale col tasto destro selezionamo l’opzione “Jump to address..” per saltare all’indirizzo di memoria richiesto.

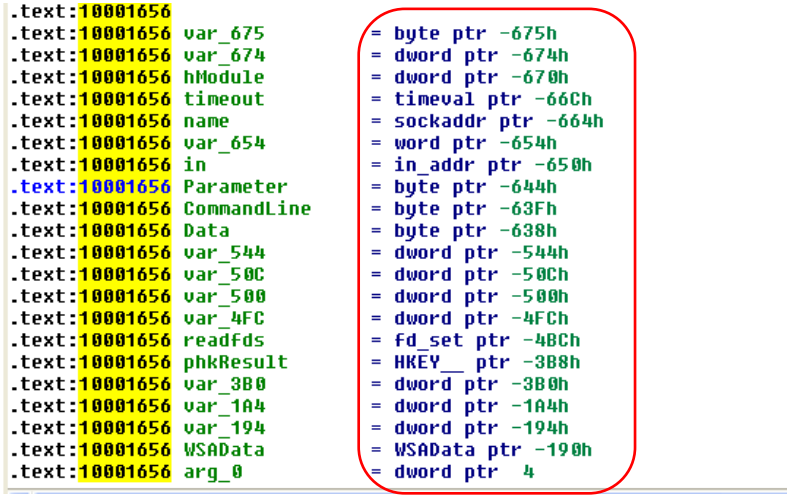


A questo indirizzo dall’interfaccia testuale di IDA possiamo vedere che viene chiamata la funzione DllMain.

```
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID)
.text:10001656 sub_10001656    proc near               ; DATA XREF: DllMain(x,x,x)+C8↓o
```

Nelle sezioni sottostanti vediamo in verde i parametri e le variabili della funzione. Con IDA sappiamo che la variabili hanno un offset negativo rispetto al registro ebp, mentre i parametri hanno un offset positivo.

L’offset, evidenziato nella figura sotto, è riportato in verde in coda al parametro / variabile.



Abbiamo un totale di 21 voci, di cui 20 hanno offset negativo rispetto a ebp, e sono quindi variabili della funzione, mentre 1, **arg_0**, ha un offset positivo. **arg_0** è quindi l'unico parametro della funzione.