Esercizio S11 L2

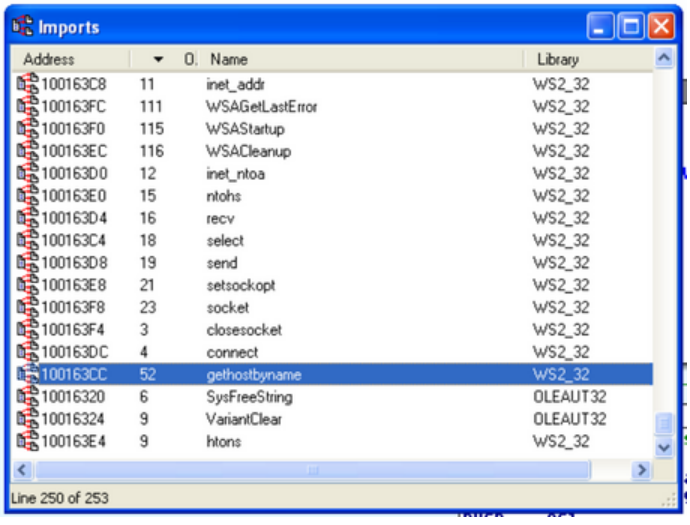
Traccia:
Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica. A tal proposito, con riferimento al malware chiamato «Malware_U3_W3_L2» presente all'interno della cartella «Esercizio_Pratico_U3_W3_L2» sul desktop della macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti, utilizzando IDA Pro.

Individuare l'indirizzo della funzione DLLMain.

```
.text:1000D02E
.text:1000D02E ; ||||||||||||||| S U B R O U T I N E |||||||||||||||||||||||||||||||||||||||
.text:1000D02E
.text:1000D02E
.text:1000D02E ; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DWORD fdwReason,LPVOID lpvReserved)
.text:1000D02E _DllMain@12     proc near               ; CODE XREF: DllEntryPoint+4B↓p
.text:1000D02E                                         ; DATA XREF: sub_100110FF+2D↓o
.text:1000D02E
.text:1000D02E hinstDLL        = dword ptr  4
.text:1000D02E fdwReason       = dword ptr  8
.text:1000D02E lpvReserved     = dword ptr  0Ch
.text:1000D02E
.text:1000D02E                 mov     eax, [esp+fdwReason]
```

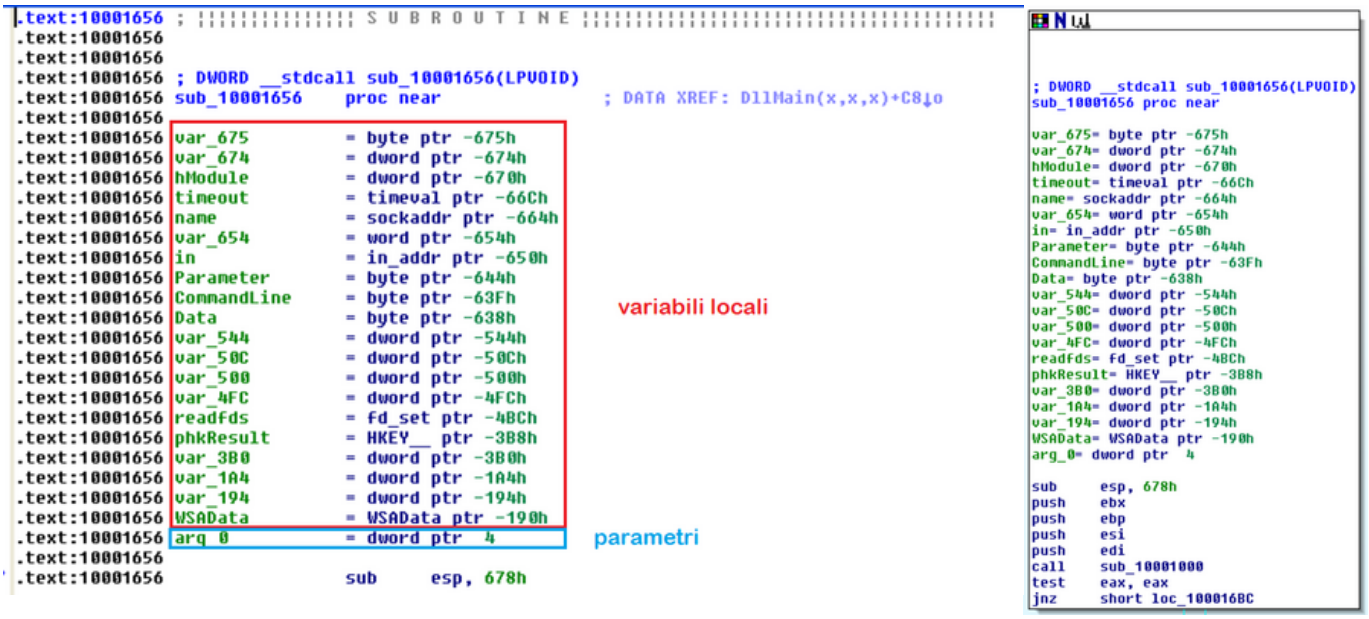
L'indirizzo della funzione DLLMain è **1000D02E**.

Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import?



L'indirizzo dell'import è **100163CC** .

Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?



Possiamo notare **venti variabili** con offset negativo.

Quanti sono, invece, i parametri della funzione sopra?

Sempre dall'immagine sopra possiamo notare **solo un parametro** con offset positivo,

Inserire considerazioni macro livello sul malware.

Esplorando il codice assmbly è facile notare che il malware esegue diverse operazioni , esegue e modifica file e cartelle, verifica versioni di hardware e software e moltro altro. Inoltre si collega ad un server esterno. Si tratta di una backdoor con funzioni di C&C. La cosa è confermata da alcune righe come questa: