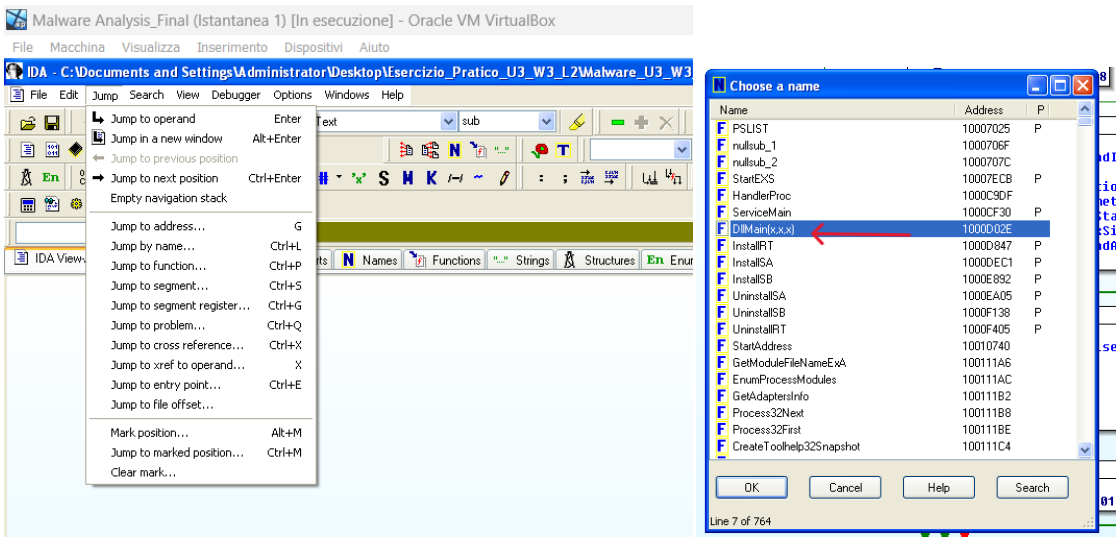
Epicode Unit 3, Week 3 Lesson 2

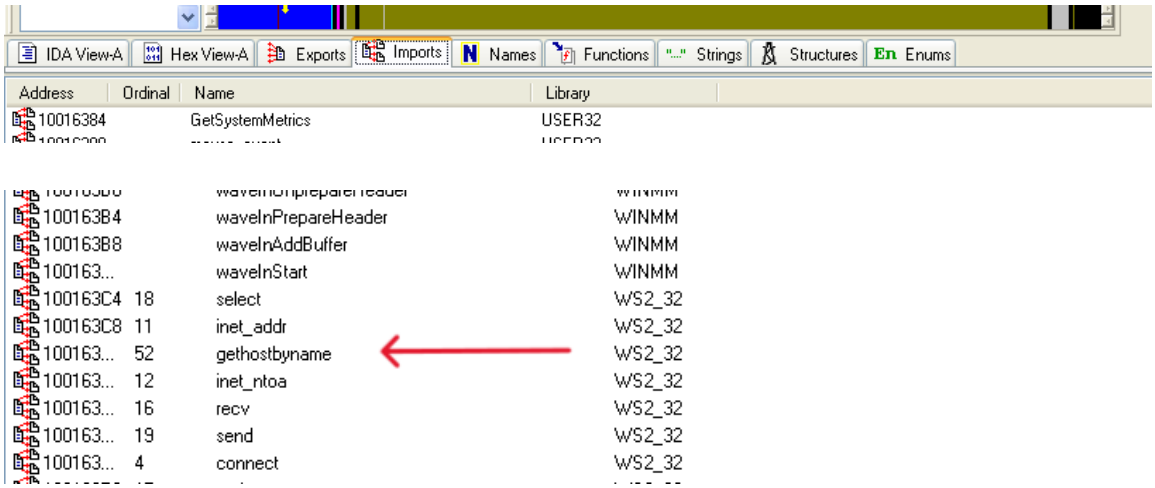
Ida Static Analysis

1) **Per la risoluzione del primo quesito, basterà utilizzare la funzione “Jump by name” del tool, e ricercare la funzione main.**



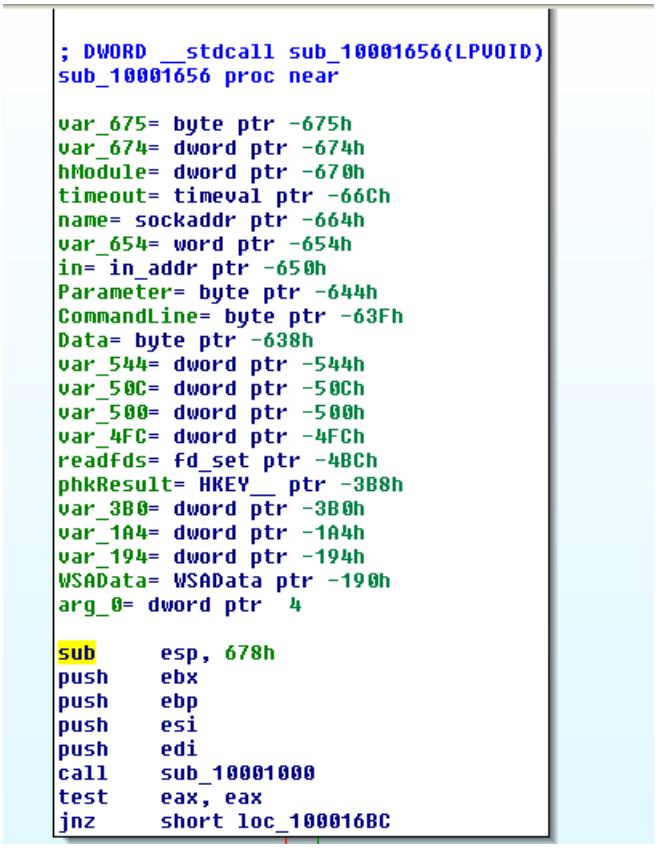
Si può dunque notare che la funzione specifica si trova all’indirizzo di memoria 1000D02E.

2) **Per completare la seconda richiesta, mi sposta dapprima nella sezione “Imports”, per poi andare a cercare la specifica funzione della libreria WS2_32.**



Facendo doppio click sulla funzione da analizzare, si può notare che essa si trova all'indirizzo 100163CC.

3) Utilizzando di nuovo la funzione "Jump" del tool, mi sposto all'indirizzo di memoria specificato, 0x10001656. Posso notare dall'intestazione della sezione di codice assembly, che la funzione in analisi è una funzione "Void"



4) In ultimo, vado a contare le variabili locali presenti all'interno della funzione, definite da "dword" in Assembly x86. Nello specifico, in questa funzione si individuano 10 variabili locali.

5) Alla luce di quanto analizzato, considerando l'utilizzo da parte del Malware di librerie e funzioni di rete, tra cui WS2_32 e "Sleep", notoriamente usate per Backdoor e Trojan, insieme a "RegisterServiceCtrlHandlerA", e alla

funzione “RegOpenKey”, che può essere un valido indizio del tentativo del Malware di ottenere Persistenza sulla macchina infetta.