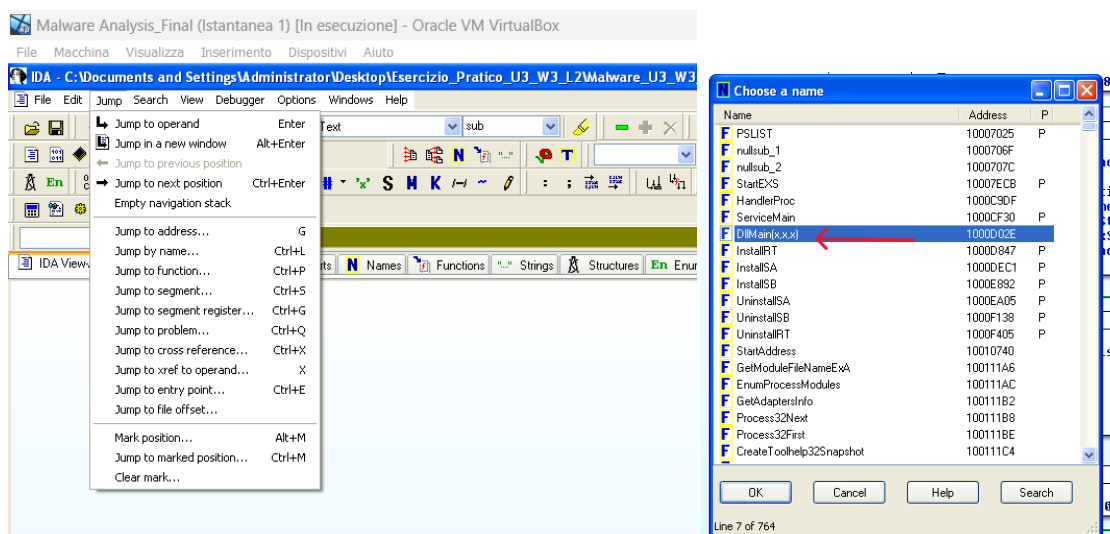


## Epicode Unit 3, Week 3 Lesson 2

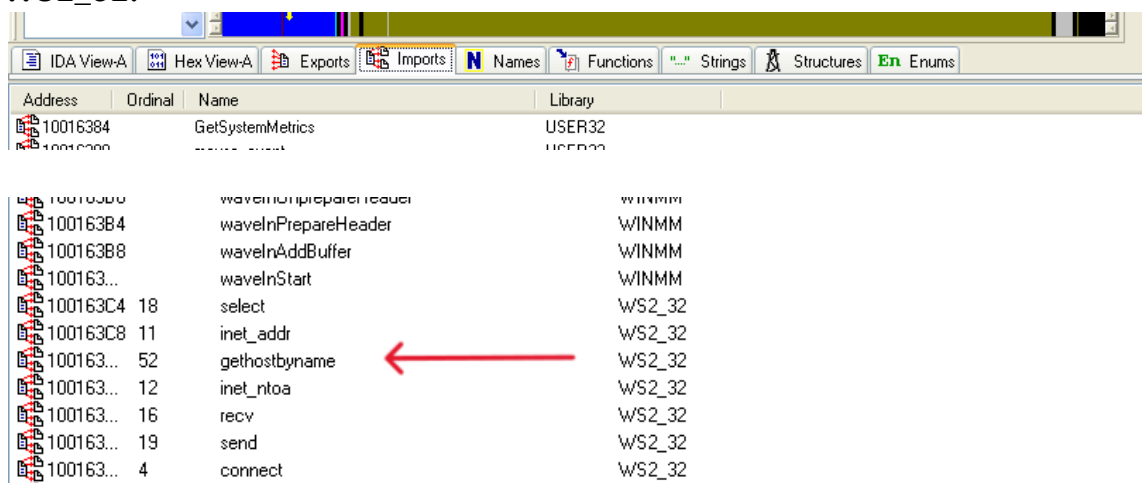
### Ida Static Analysis

- 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"

```
; DWORD __stdcall sub_10001656(LPVOID)
sub_10001656 proc near

var_675= byte ptr -675h
var_674= dword ptr -674h
hModule= dword ptr -670h
timeout= timeval ptr -66Ch
name= sockaddr ptr -664h
var_654= word ptr -654h
in= in_addr ptr -650h
Parameter= byte ptr -644h
CommandLine= byte ptr -63Fh
Data= byte ptr -638h
var_544= dword ptr -544h
var_50C= dword ptr -50Ch
var_500= dword ptr -500h
var_4FC= dword ptr -4FCh
readfds= fd_set ptr -4BCh
phkResult= HKEY__ ptr -3B8h
var_3B0= dword ptr -3B0h
var_1A4= dword ptr -1A4h
var_194= dword ptr -194h
WSAData= WSAData ptr -190h
arg_0= dword ptr 4

sub     esp, 678h
push    ebx
push    ebp
push    esi
push    edi
call    sub_10001000
test    eax, eax
jnz     short loc_1000168C
```

- 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.