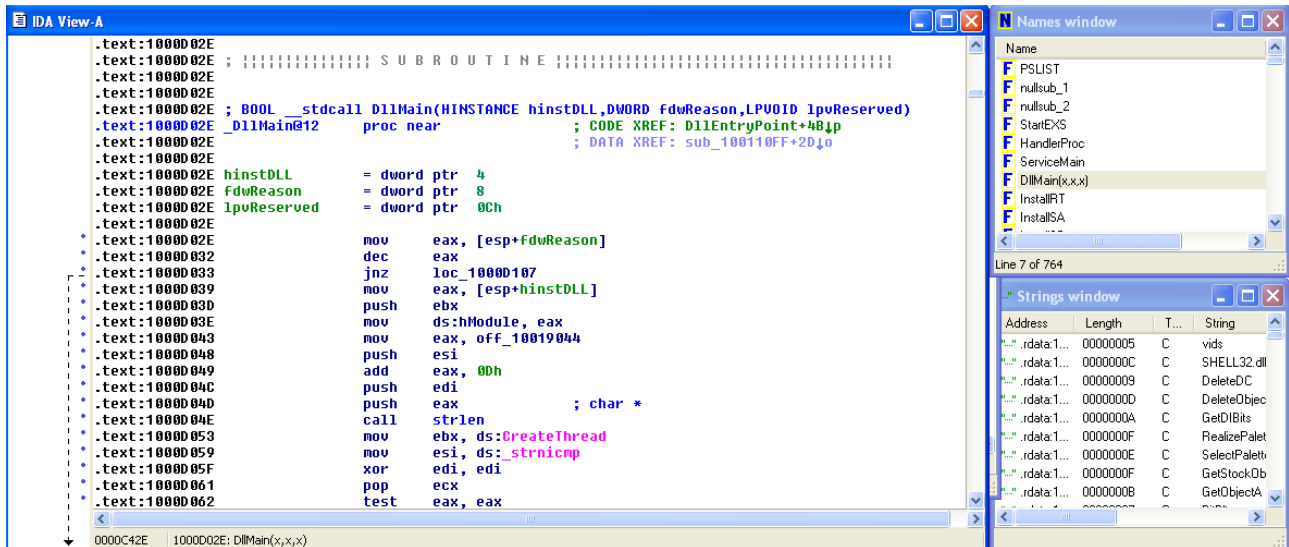


## PRATICA S11L2

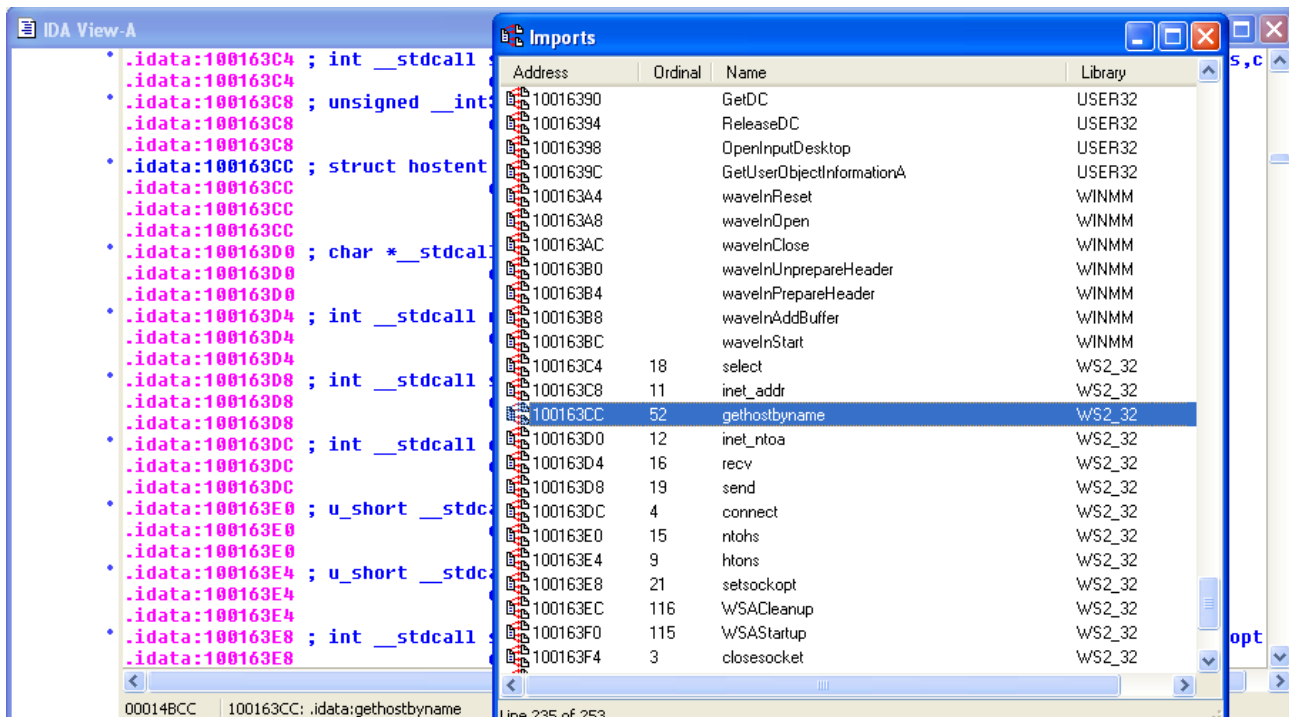
### 1) Individuare l'indirizzo della funzione DLLMAIN

Possiamo individuare la funzione richiesta dalla tab “names” di IDA pro:



Dallo screen vediamo che l'indirizzo è 1000D02E

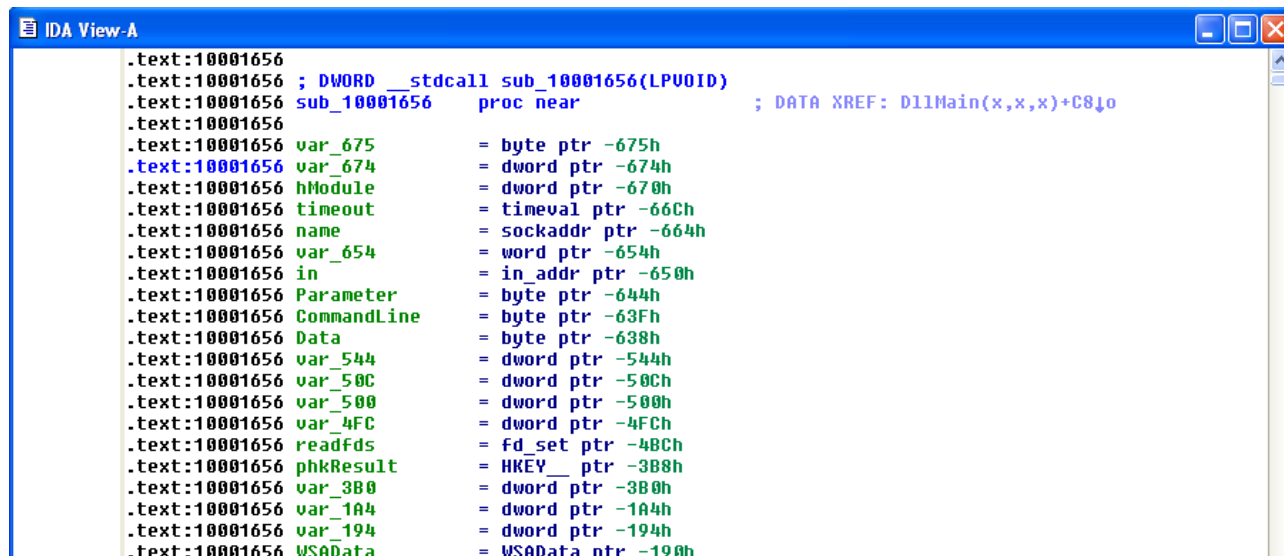
### 2) Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import? Cosa fa la funzione?



Selezionando la funzione richiesta, possiamo vedere che il suo indirizzo è 100163CC. Dalla documentazione di windows online possiamo recuperare le informazioni sul funzionamento di tale funzione, che restituisce un indirizzo ip dato un nome host appartenente ad un host database.

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

Inseriamo l'indirizzo indicato nel campo "jump to address" presente sulla scheda in alto. Le variabili utilizzate dalla funzione sono quelle in figura:



```
IDA View-A
.text:10001656
.text:10001656 ; DWORD __stdcall sub_10001656(LPVOID)
.text:10001656 sub_10001656 proc near ; DATA XREF: DllMain(x,x,x)+C840
.text:10001656
.text:10001656 var_675 = byte ptr -675h
.text:10001656 var_674 = dword ptr -674h
.text:10001656 hModule = dword ptr -670h
.text:10001656 timeout = timeval ptr -66Ch
.text:10001656 name = sockaddr ptr -664h
.text:10001656 var_654 = word ptr -654h
.text:10001656 in = in_addr ptr -650h
.text:10001656 Parameter = byte ptr -644h
.text:10001656 CommandLine = byte ptr -63Fh
.text:10001656 Data = byte ptr -638h
.text:10001656 var_544 = dword ptr -544h
.text:10001656 var_50C = dword ptr -50Ch
.text:10001656 var_500 = dword ptr -500h
.text:10001656 var_4FC = dword ptr -4FCh
.text:10001656 readfds = fd_set ptr -4BCh
.text:10001656 phkResult = HKKEY ptr -3B8h
.text:10001656 var_380 = dword ptr -380h
.text:10001656 var_1A4 = dword ptr -1A4h
.text:10001656 var_194 = dword ptr -194h
.text:10001656 WSADATA = WSADATA ptr -190h
```

4) Quanti sono, invece, i parametri della funzione sopra?

Sempre nella stessa scheda, vediamo che l'unico parametro è arg0:

```
.text:10001656 arg_0 = dword ptr 4
```

5) Dalla macro-analisi del codice, vediamo che il malware fa uso di diverse funzioni per utilizzare i socket di windows, gestire le comunicazioni di rete, leggere e modificare le chiavi di registro, connettersi ad un host remoto, inviare e ricevere dati. Aspettandosi quindi di ricevere comunicazioni in ingresso, si può presupporre che si tratti di una backdoor