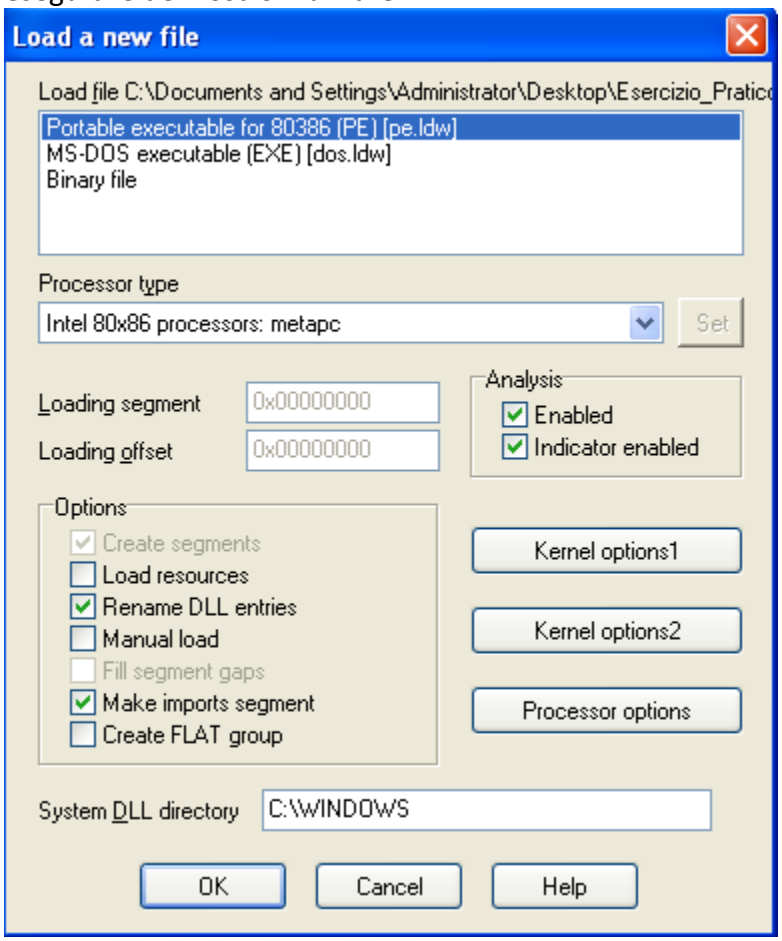
ANALISI STATICA CON IDA

FRANCESCO PERSICHETTI

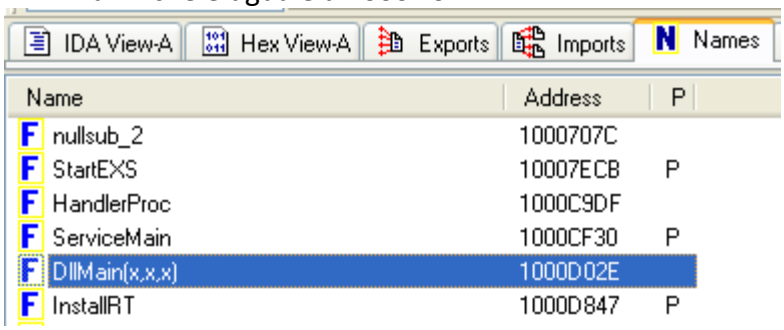
L'esercizio di oggi consiste nell'analizzare il codice malevolo con il dissambler IDA per svolgere i seguenti task:

1. Individuare l'indirizzo della funzione DLLMain
2. Dalla scheda imports individuare la funzione **"gethostbyname"** e il suo indirizzo
3. Quante sono le variabili della funzione alla locazione di memoria 0x10001656?
4. Quanti sono i parametri della stessa funzione al punto 3?
5. Considerazioni sul malware analizzato

1.
Per iniziare con l'analisi del malware utilizziamo il dissambler IDA con cui apriremo il codice eseguibile del nostro malware



Una volta aperto ci verrà restituito tutto il codice assembly del malware, con le varie funzioni importate. Se andiamo nella scheda “Names” del programma ci verranno elencate tutte le funzioni per nome, e noi andremo ad evidenziare ai fini del nostro task, l’indirizzo di memoria della funzione “DLLMain” che è uguale a **1000D02E**



2.

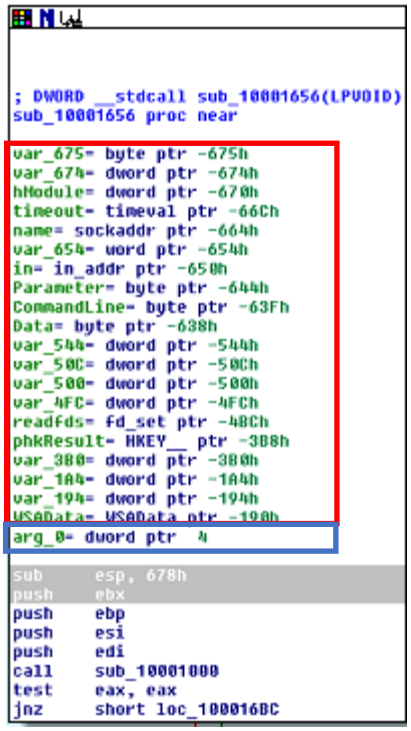
Sempre muovendosi tra le varie schede che ci sono nel programma, andiamo nella finestra “Imports” e andiamo ad individuare l’indirizzo di memoria della funzione “gethostbyname”. L’indirizzo è il seguente: 100163CC

3-4

Nella finestra “Functions” mettiamo nella barra di ricerca l’indirizzo di memoria **10001656** per andare a individuare la funzione corrispondente. Una volta trovata con il doppio click si aprirà tutto il codice inerente alla funzione con le relative variabili e parametri.

Variabili in rosso

Parametri in blu



5.
Dall'analisi più approfondita del codice sembra che questo malware si occupi di creare una backdoor sulla macchina vittima, come si può anche notare dai seguenti screen.