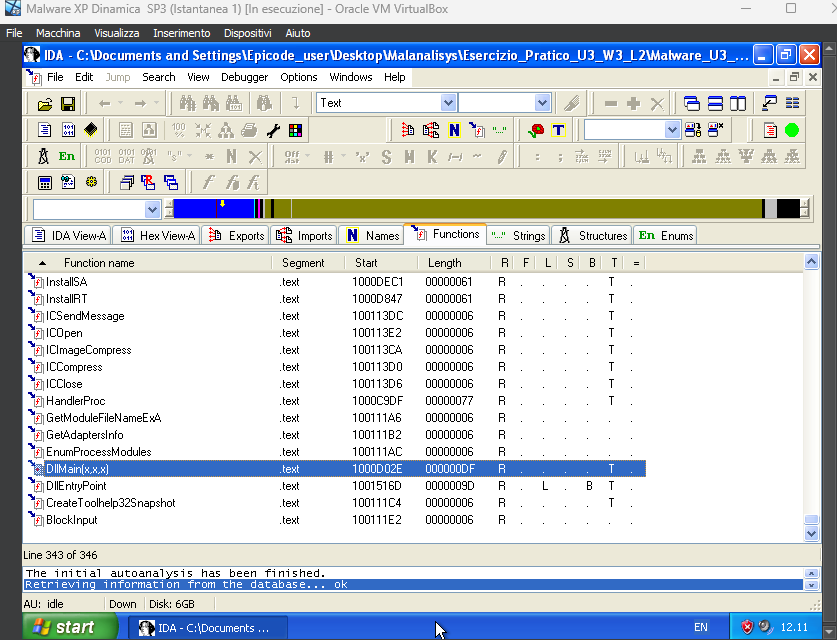
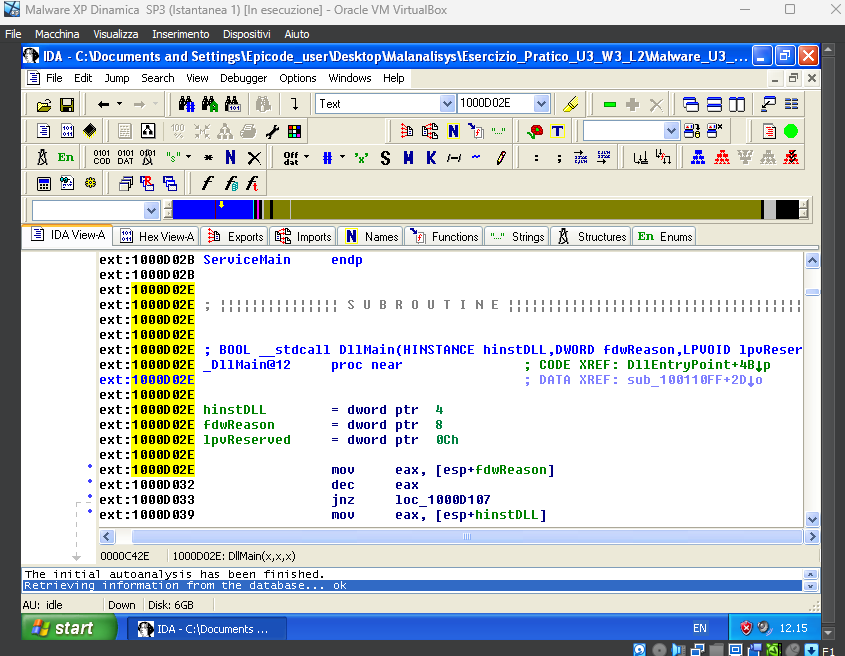
Pratica con IDA

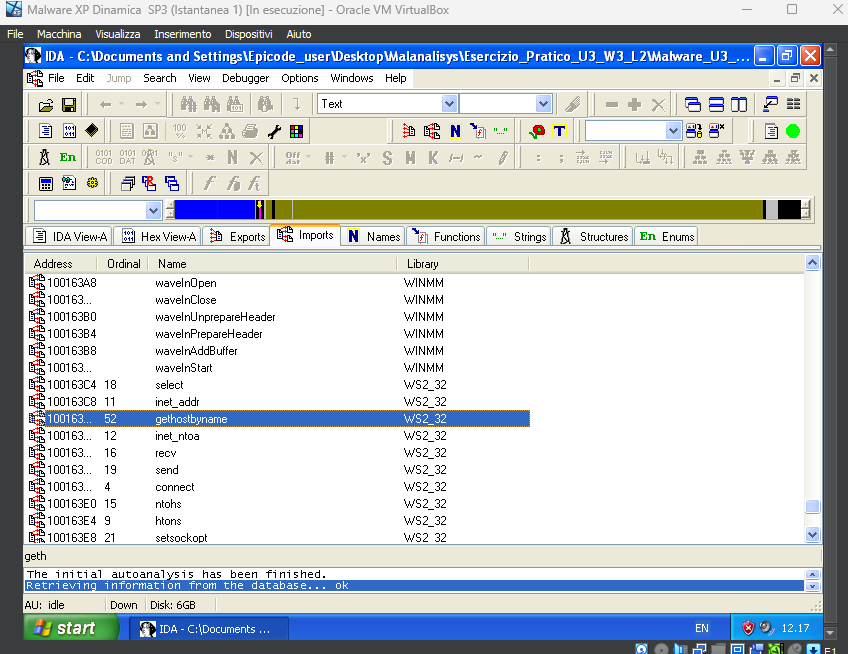
Utilizzando il malware “Esercizio\_Pratico\_U3\_W3\_L2” cerchiamo di soddisfare le seguenti domande:

* Individuare l’indirizzo della funzione DLLMain
* Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l’indirizzo dell’import? Cosa fa la funzione?
* Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?
* Quanti sono, invece, i parametri della funzione sopra?
* Considerazioni di macro-livello sul malware.

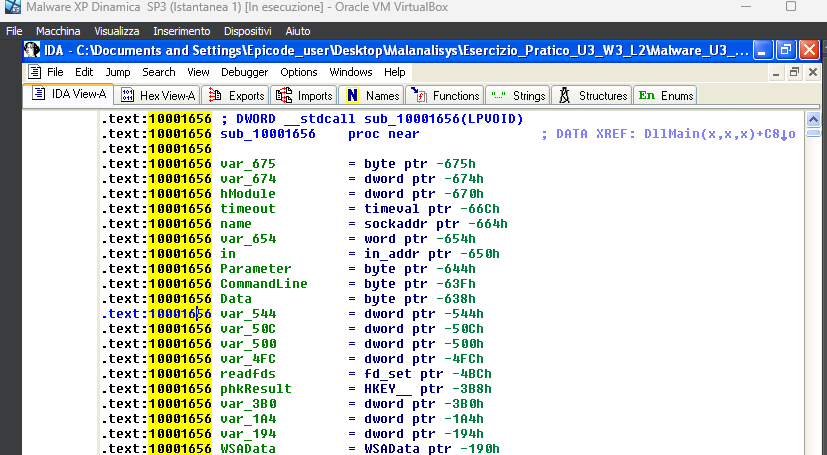




Filtrando dalla finestra Functions il nome della funzione possiamo identificare la funzione “dllMain” con l’indirizzo 1000D02E, dopodiché si può notare nello specifico la funzione nella sezione IDA View-A



Dalla finestra Imports filtriamo tra i risultati e troviamo la funzione gethostbyname nella libreria WS2\_32 all’indirizzo 100163CC. La funzione gethostbyname è utilizzata dal malware per consentire di stabilire una connessione a un server remoto per ricevere istruzioni, inviare dati o ricevere aggiornamenti.



Queste sono tutte variabili locali all’indirizzo 10001656 della funzione Dllmain:

Da “var\_675” a “WSAData”



Invece in quest’ultima riga si può notare l’unico parametro della funzione Dllmain

“arg\_0”

Si può notare come il malware importi delle librerie e funzioni che servono per stabilire una connessione ad Internet, per questo possiamo ipotizzare ad un malware di tipo downloader che una volta avviato vada a scaricare funzioni e pacchetti malevoli.

Per scrupolo possiamo anche andare ad analizzare la barra di navigazione del codice cercando qualche indizio nei dati come un server o un URL di collegamento.

In questo modo troviamo un’istruzione che chiarisce il comportamento del malware una volta per tutte; infatti, come si può vedere in figura il malware cercherà di creare una connessione con il server Backdoor. Possiamo dunque ipotizzare che il malware in realtà vada ad installare una backdoor all’interno del sistema infetto.

