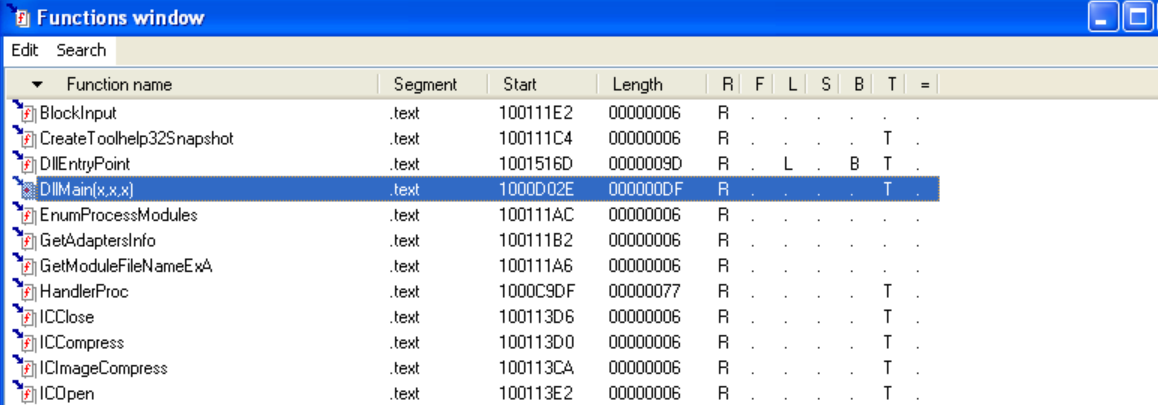
Esercizio 2 Settimana 11

Oggi andremo ad effettuare un’analisi statica avanzata di un malware usando IDAPRO 5.

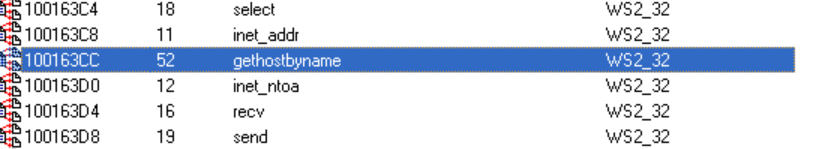
Dovremo andare a rispondere alle seguenti domande:

* Individuare l’indirizzo della funzione DLLMain(così com’è, in esadecimale)
* Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l’indirizzo dell’import? Cosa fa la funzione?
* Quante sono le variabili locali della funzionealla locazione di memoria 0x10001656?
* Quanti sono, invece, i parametri della funzione sopra?
* Inserire altre considerazioni macro livello sul malware (comportamento)

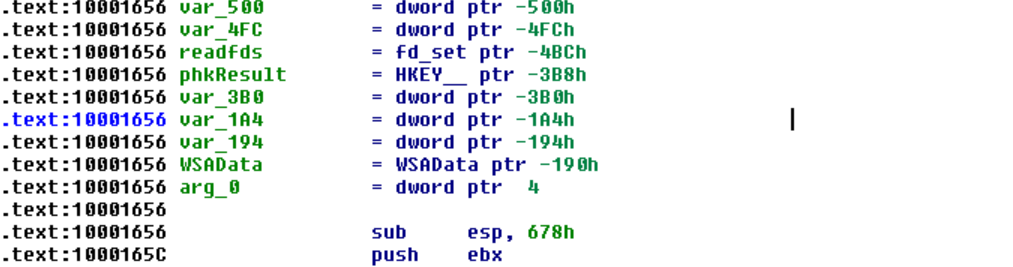
Per rispondere alla prima domanda, sarà sufficiente andare sulla scheda “Functions” del nostro programma e cercare DLLMain, questo sarà il risultato:



Per la seconda domanda, invece, ci sposteremo nella sezione “imports” del programma andando a ricercare gethostbyname, per poi trovare anche il suo indirizzo:



Per la terza e la quarta domanda torneremo alla vista con testo. Faremo un jump (dalle opzioni) all’indirizzo indicato e troveremo questa parte di codice:



Tutto ciò che ha un offset negativo (il risultato dell’operazione logica) sarà considerato variabile, mentre ciò che avrà offset positivo sarà considerato variabile. Pertanto, solo arg\_0 è una variabile e tutto il resto è parametro.

Per quanto riguarda l’ultima domanda, potremmo usare l’hash del file per andare a cercare su virustotal di che malware stiamo parlando. Facendo quest’operazione, arriveremo a capire che questo malware potrebbe essere una backdoor.