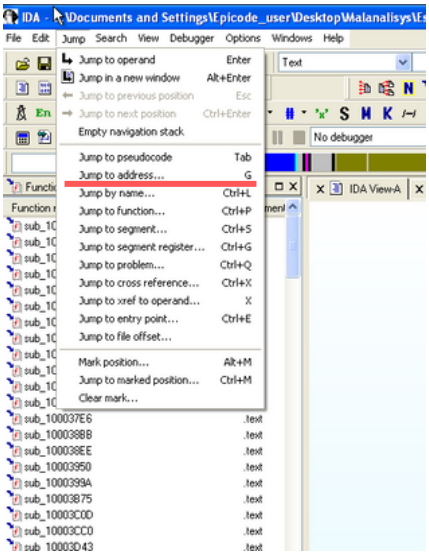
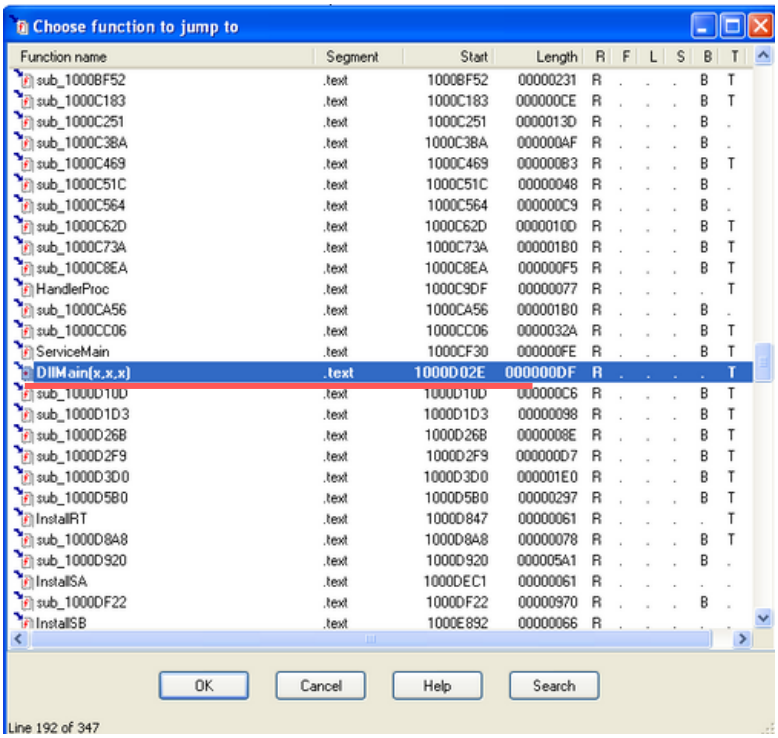
1. Individuazione dell'indirizzo della funzione DLLMain

Inizialmente individuiamo l'indirizzo della funzione DLLMain. Per farlo, apriamo il menù "Jump", "Jump to function" e cerchiamo la funzione la funzionalità "Search":

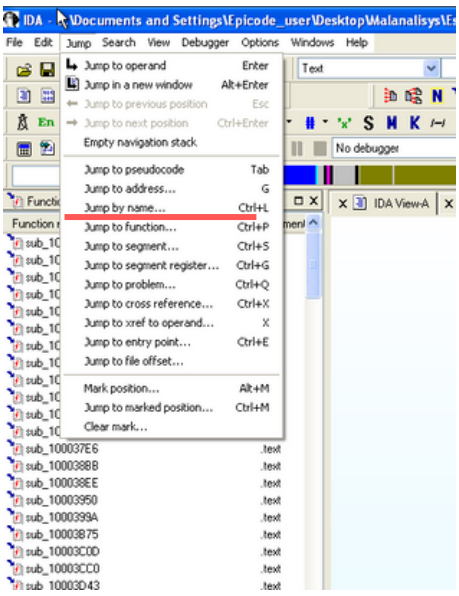


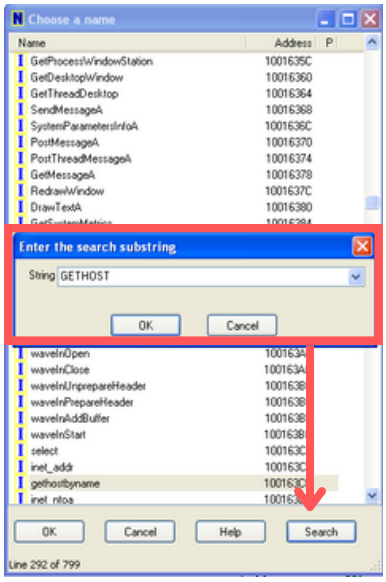


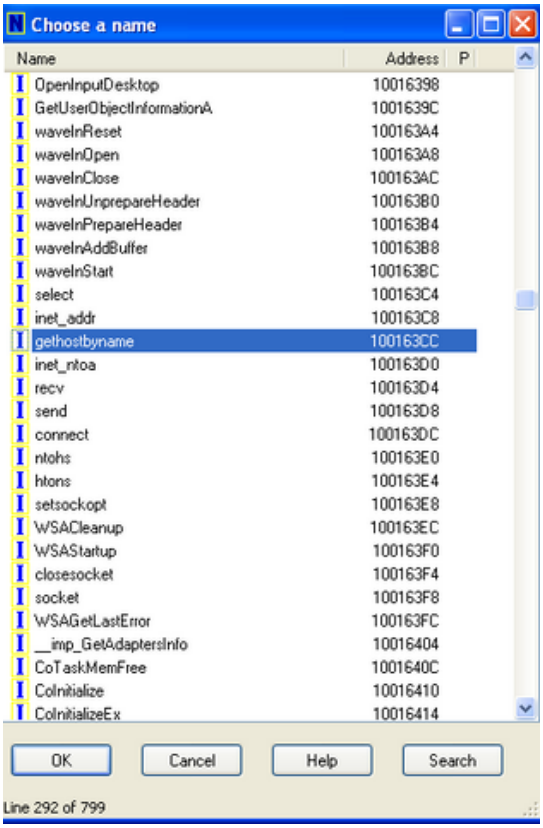
Abbiamo identificato la funzione DLLMain; l'indirizzo di memoria ad essa associato è 1000D02E.

2. Individuazione dell'indirizzo di import della funzione gethostbyname

Adesso individuo la funzione gethostbyname, presente tra le funzioni importate dall'eseguibile . Scelgo funzionalità jump by name e ricercare il nome della funzione cliccando su "Search":

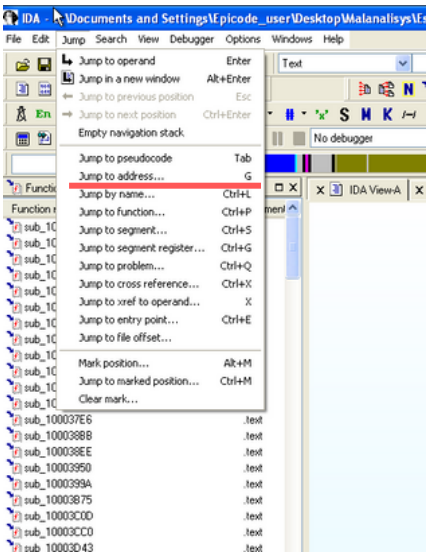


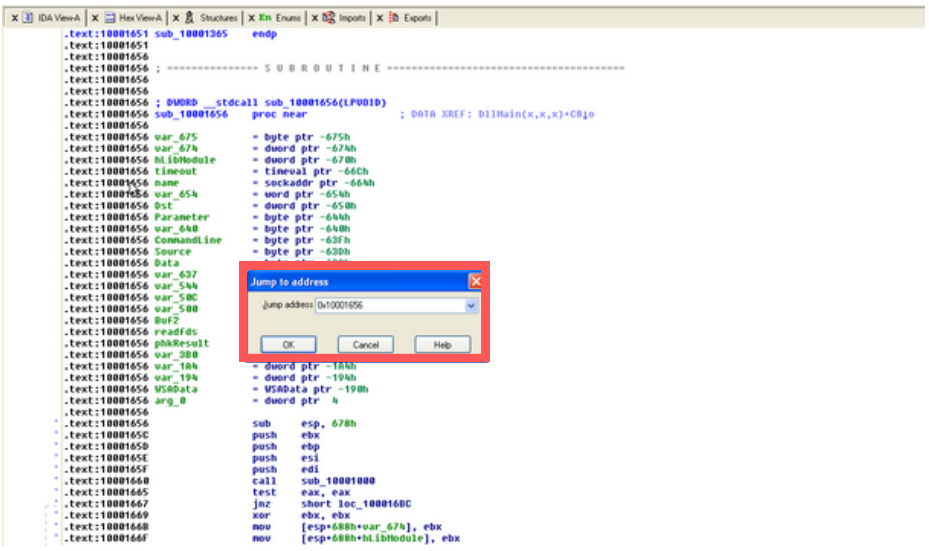


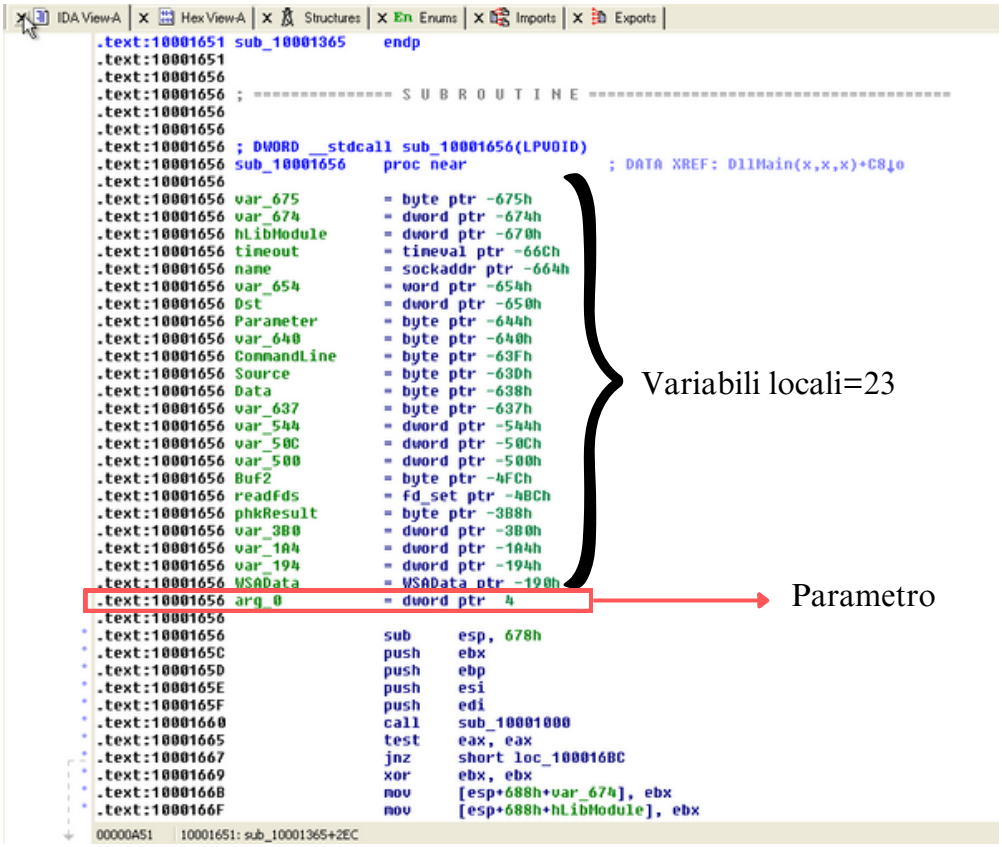


Ho individuato la funzione ricercata, presente all'indirizzo di memoria 1001063CC

3. Quantificazione delle variabili locali e dei parametri della funzione alla locazione di memoria 0x10001656

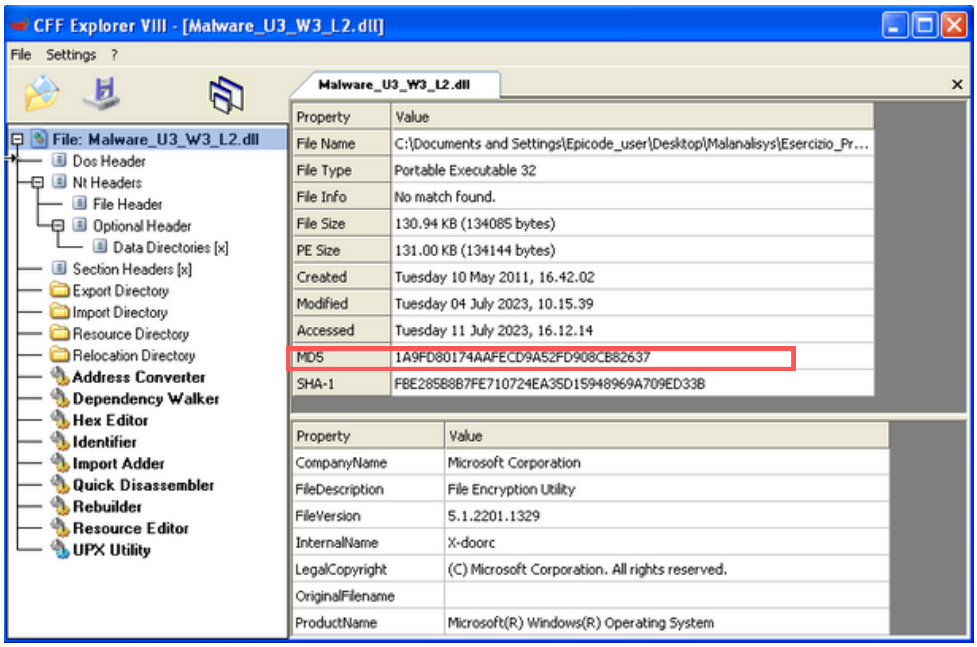




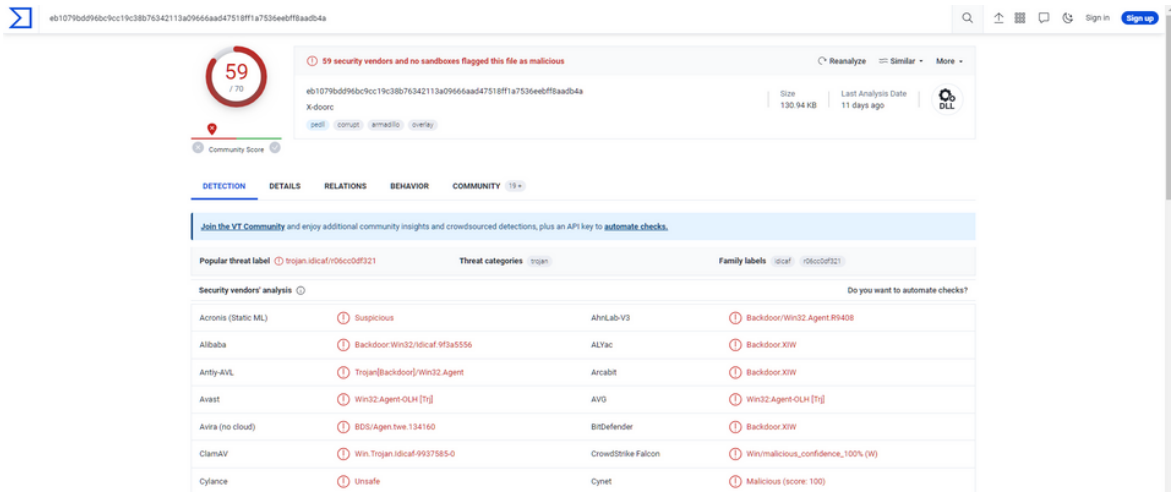


4. Considerazioni macro-livello circa il comportamento del malware

Inizialmente trovo l'hash del malware con CFF EXPLORER

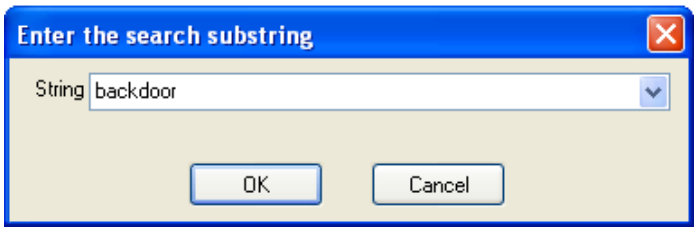


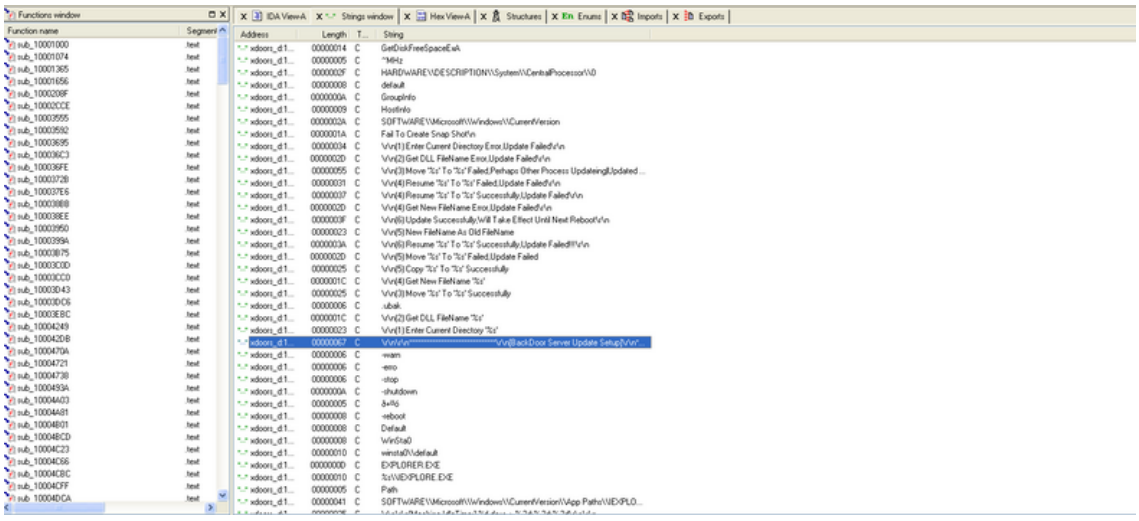
Una volta trovato l'hash del file lo inserisco su virus total

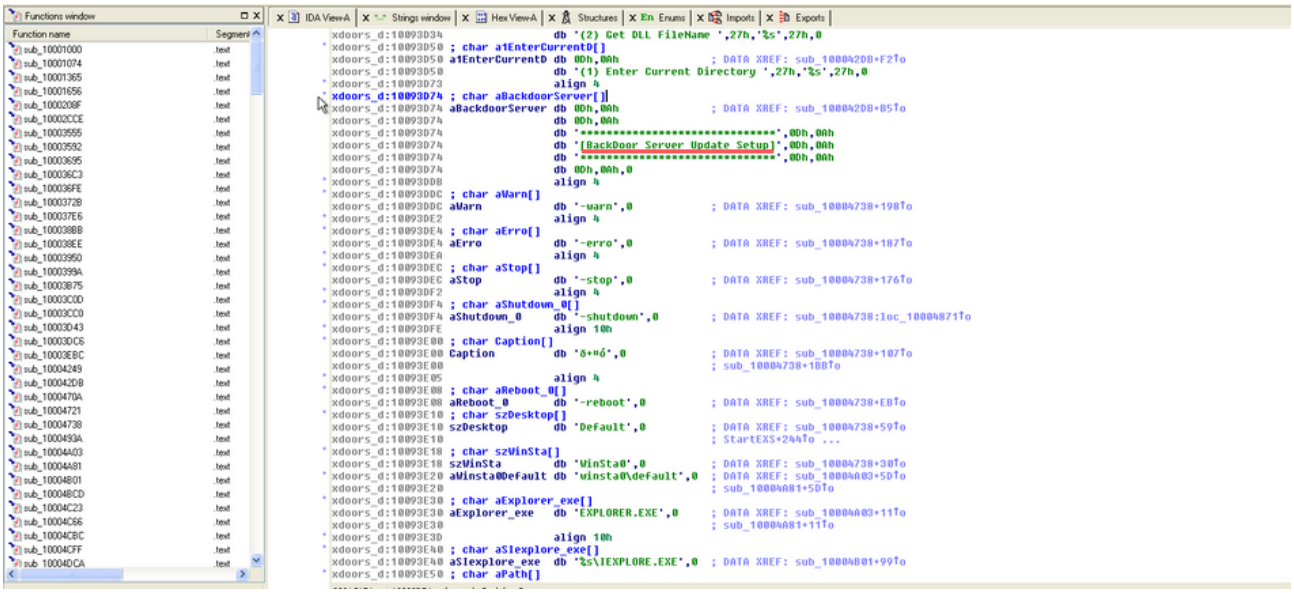


59 vendors su 70 dicono che è un file malevolo.
Come possiamo vedere nella figura precedente il file è una backdoor

Dopo l'analisi di virus total ho provato a cercare la parola backdoor nelle stringhe






Functions window
Function name
IDA View-A
Strings window
Hex View-A
Structures
Enums
Imports
Exports
xdoors_d:10093D74 aBackdoorServer db 0Dh,0Ah ; DATA XREF: sub_10004208+B5↑o
xdoors_d:10093D74 db 0Dh,0Ah
xdoors_d:10093D74 db "**********",0Dh,0Ah
xdoors_d:10093D74 db "[BackDoor Server Update Setup]",0Dh,0Ah
xdoors_d:10093D74 db "**********",0Dh,0Ah
xdoors_d:10093D74 db 0Dh,0Ah,0

}