REPORT 17/01/2023 **LORENZO SCORBAIOLI**

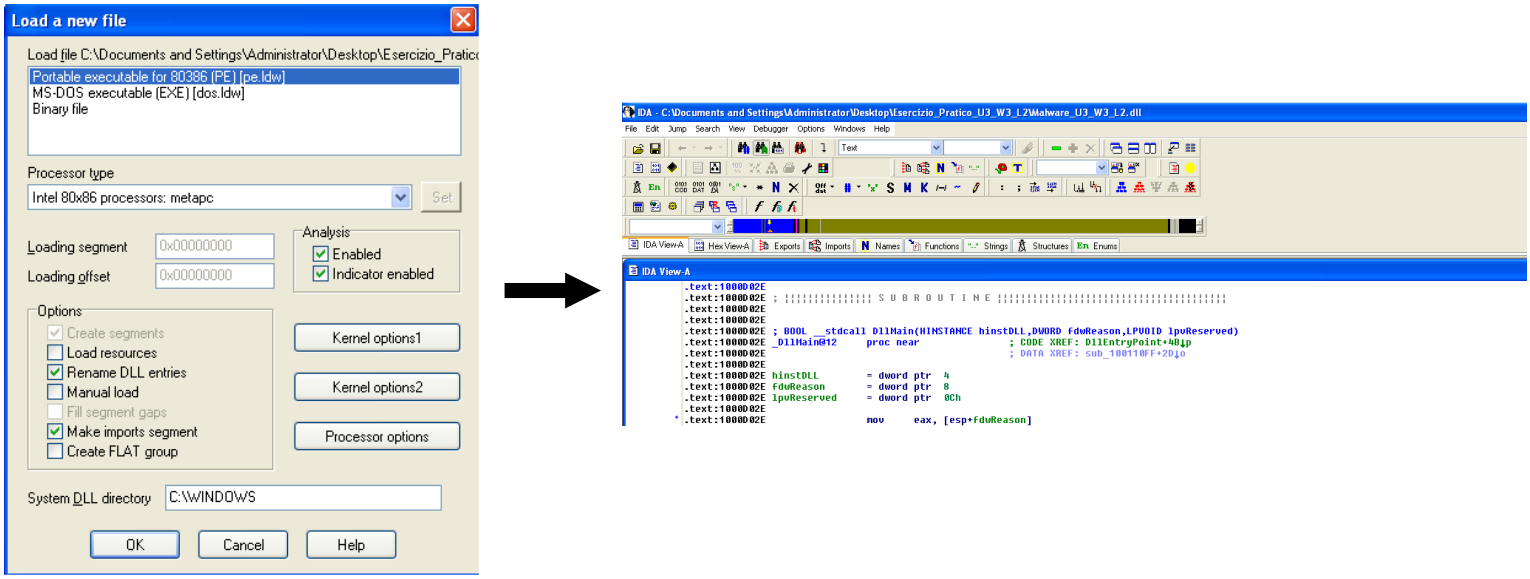
TASK:

Con riferimento al malware “Malware_U3_W3_L2” presente sulla macchina Windows XP rispondere ai seguenti quesiti:

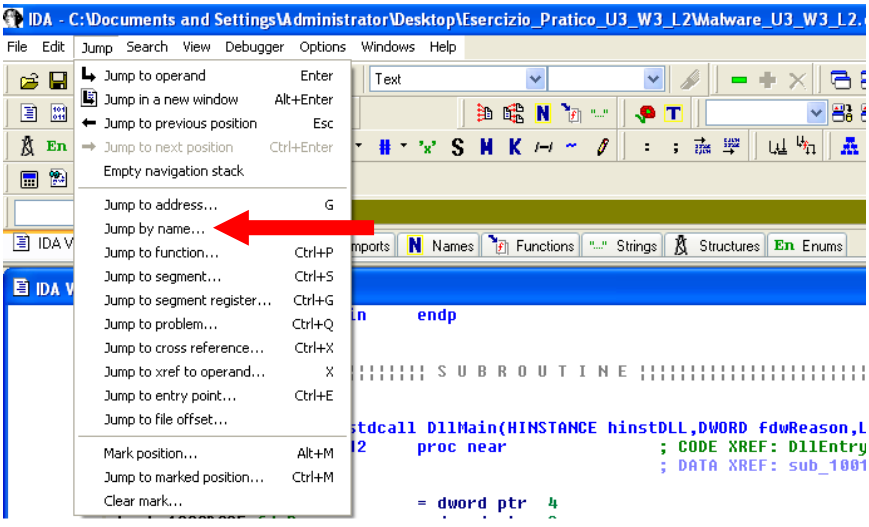
1. Individuare L’indirizzo della funzione DllMain
2. Dalla scheda “imports” individuare la funzione “gethostbyname”. Qual’è l’indirizzo dell’import’
3. Quante sono le varibili locali della funzione alla locazione di memoria “0x10001656”?
4. Quante sono invece i parametri della funzione al punto 3?
5. Inserire altre considerazioi macro livello sul malware (comportamento)

1)

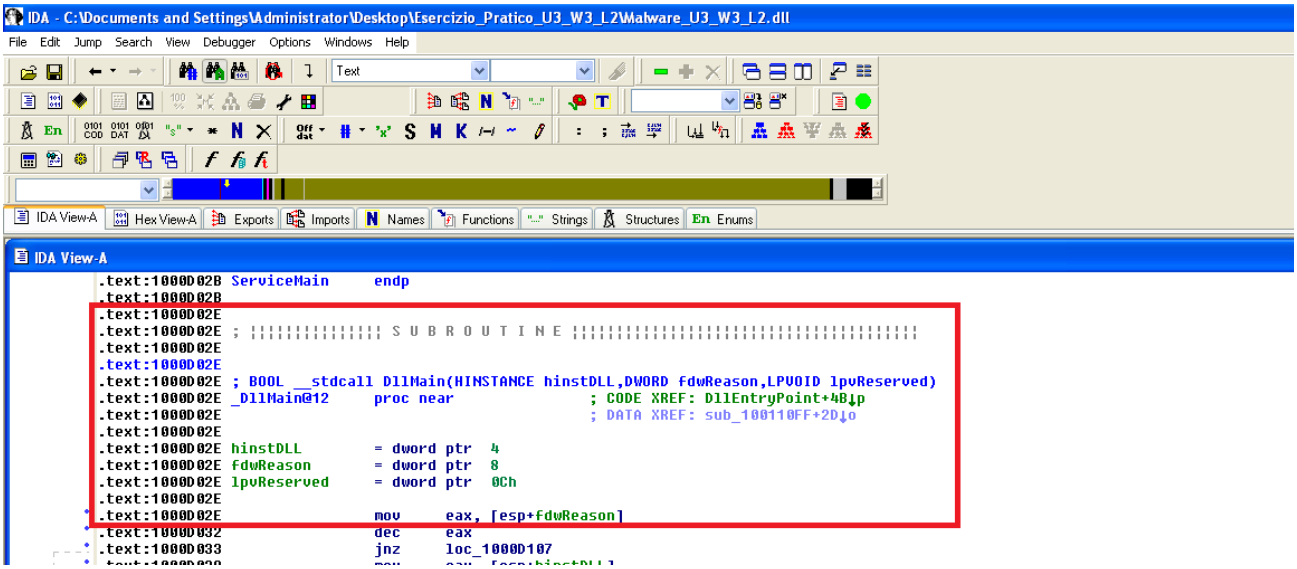
Dopo avere aperto il Malware indicato in traccia con il programma IDA Pro lasciando le impostazioni di base ho ottenuto questa schermata:



A questo punto sono andato a cercare tramite la funzione jump by name la funzione DllMain:

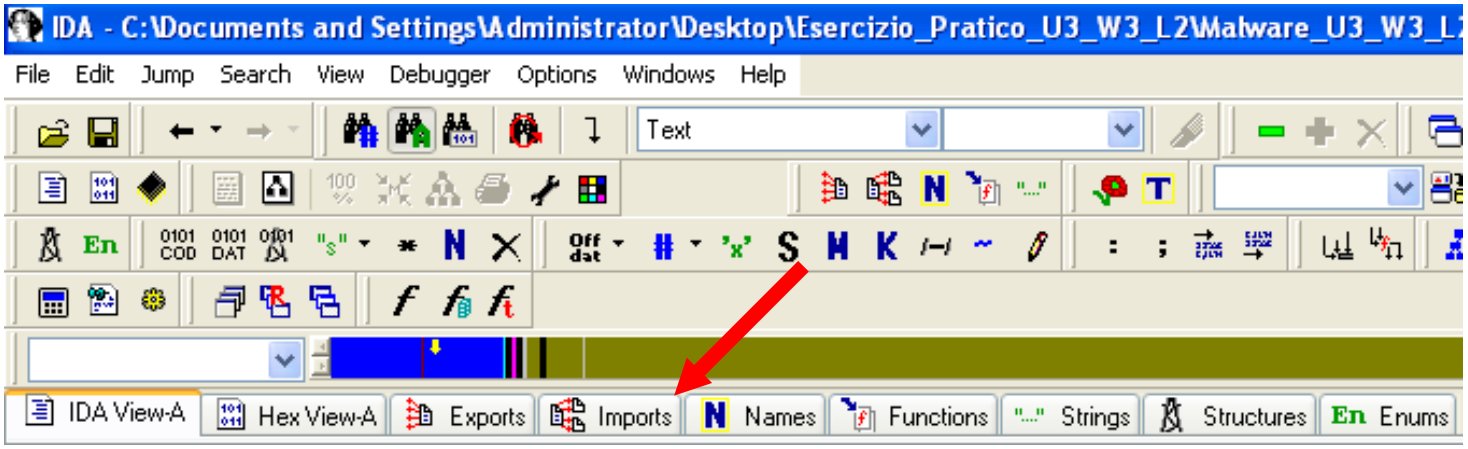


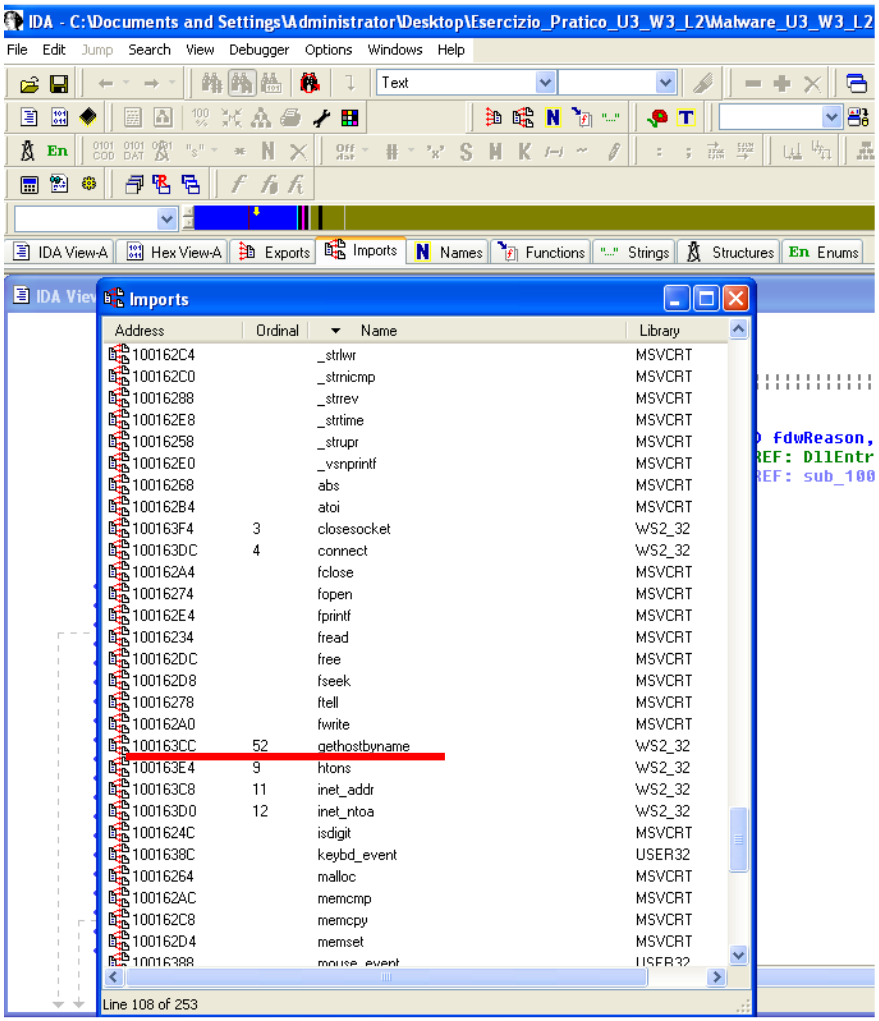
Il risultato della mia ricerca mi ha portato a questa schermata:



2)

A questo punto mi sono spostato sulla scheda “imports” per andare ad individuare la funzione “gethostbyname”:

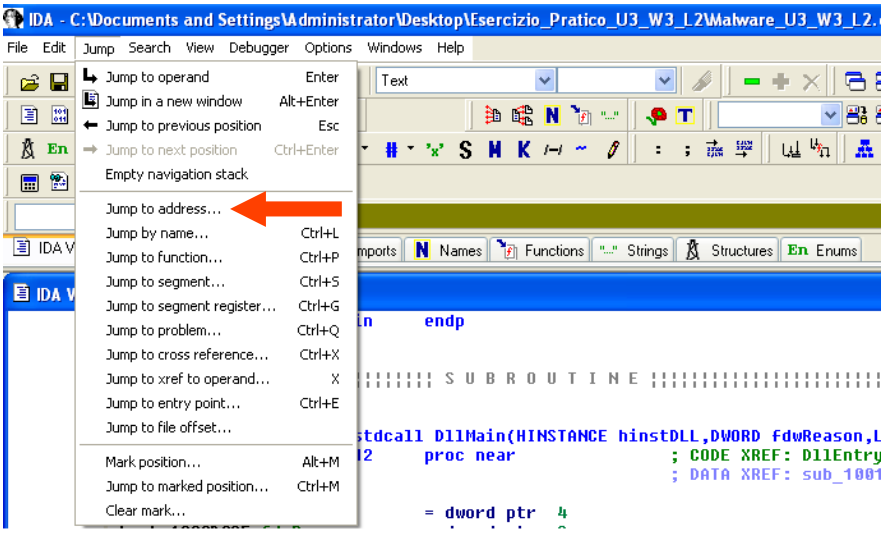




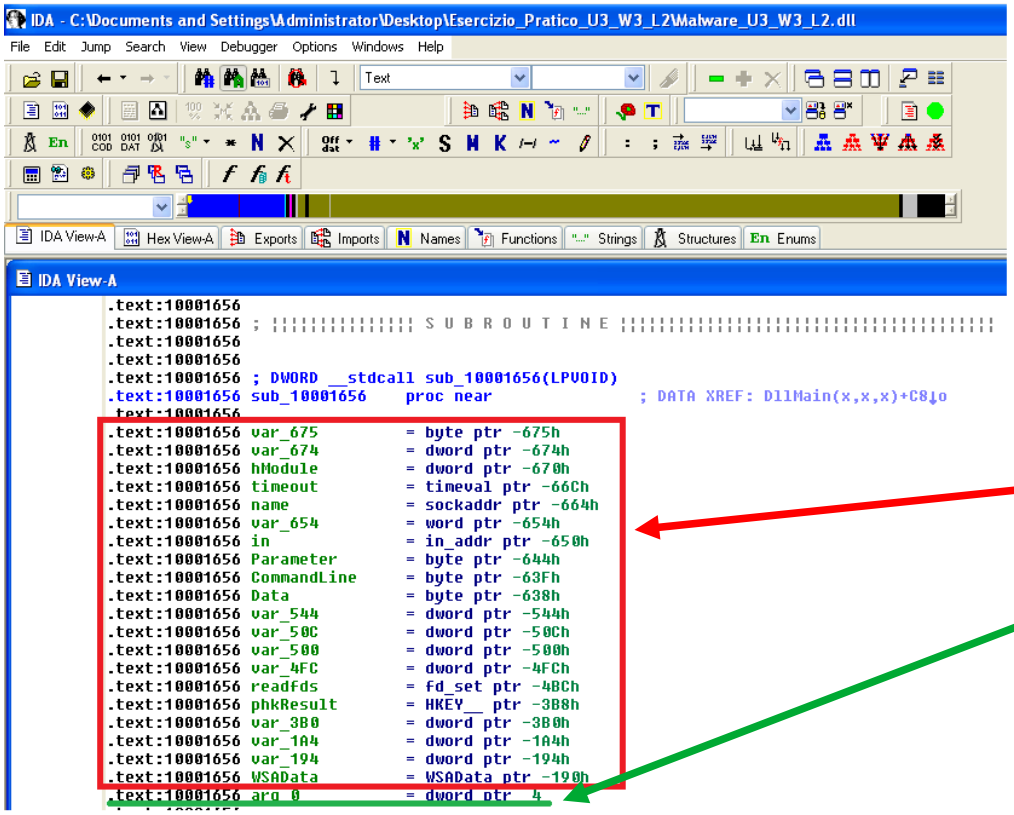
Come possiamo vedere dall'immagine qui sopra tale funzione è localizzata all'indirizzo di memoria 0x100163CC.

3-4)

Ho utilizzato sempre il comando jump ma questa volta sono andato a cercare l'indirizzo di memoria di mio interesse: 0x10001656



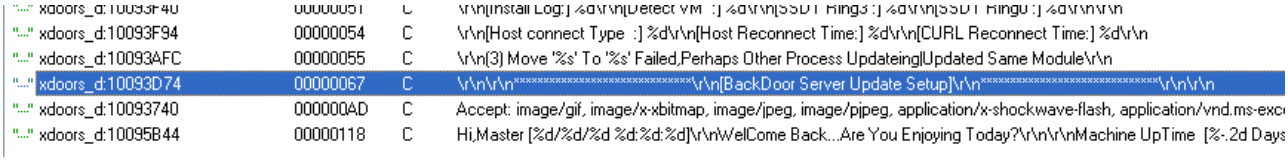
Una volta effettuato questo jump ho ottenuto questa schermata:



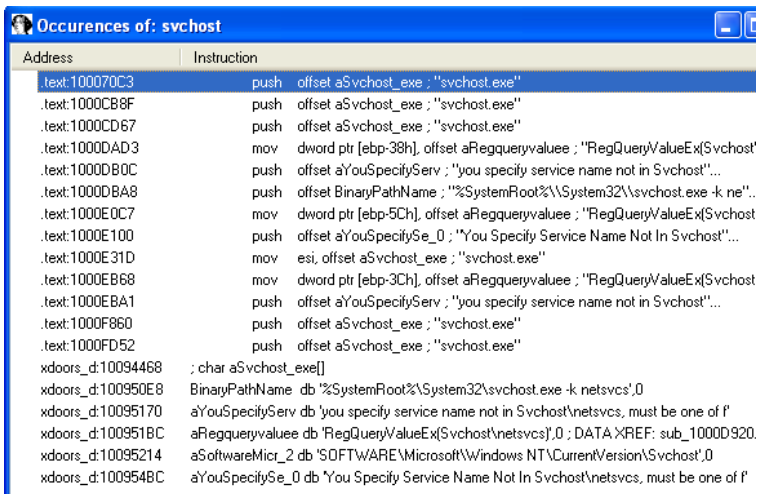
Nel riquadro rosso possiamo vedere le variabili locali della funzione, mentre sottolinato in verde l'unico argomento della funzione.

5)

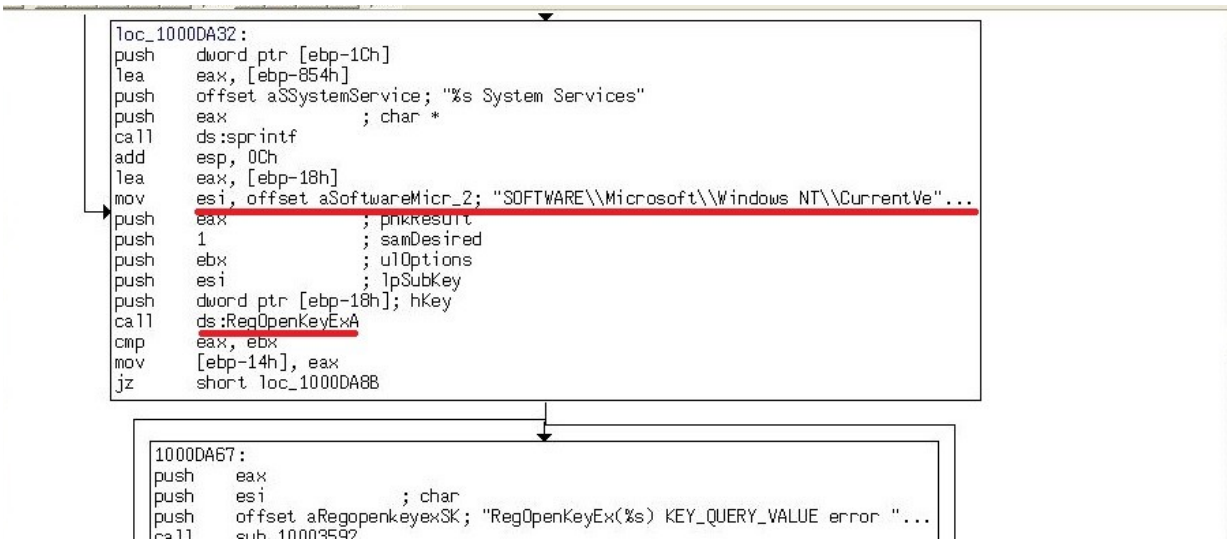
Dall'analisi del codice, coadiuvata dall'utilizzo di virustotal.com, sono giunto alla conclusione che questo malware si occupa di creare una backdoor nella macchina infetta. A sostegno di questa mia ipotesi ho riscontrato questa stringa nel codice:



Inoltre ho riscontrato una manipolazione del servizio svchost.exe per porre il processo in background per essere meno rintracciabile:



Ottiene la persistenza andando a modificare le chiavi di registro come possiamo vedere dall'immagine qui sotto:



E inoltre penso che vada ad aprire una remote shell data: