S11 L2

Report Esercizio Malware Analysis

GiuliaSalani

INDICE

TRACCIA

Lo scopo dell'esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l'analisi statica. A tal proposito, con riferimento al malware chiamato «**Malware_U3_W3_L2**» presente all'interno della cartella «Esercizio_Pratico_U3_W3_L2» sul desktop della macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti, utilizzando IDA Pro.

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 variabili locali della funzione alla locazione di memoria 0x10001656?
4. Quanti sono, invece, i parametri della funzione sopra?

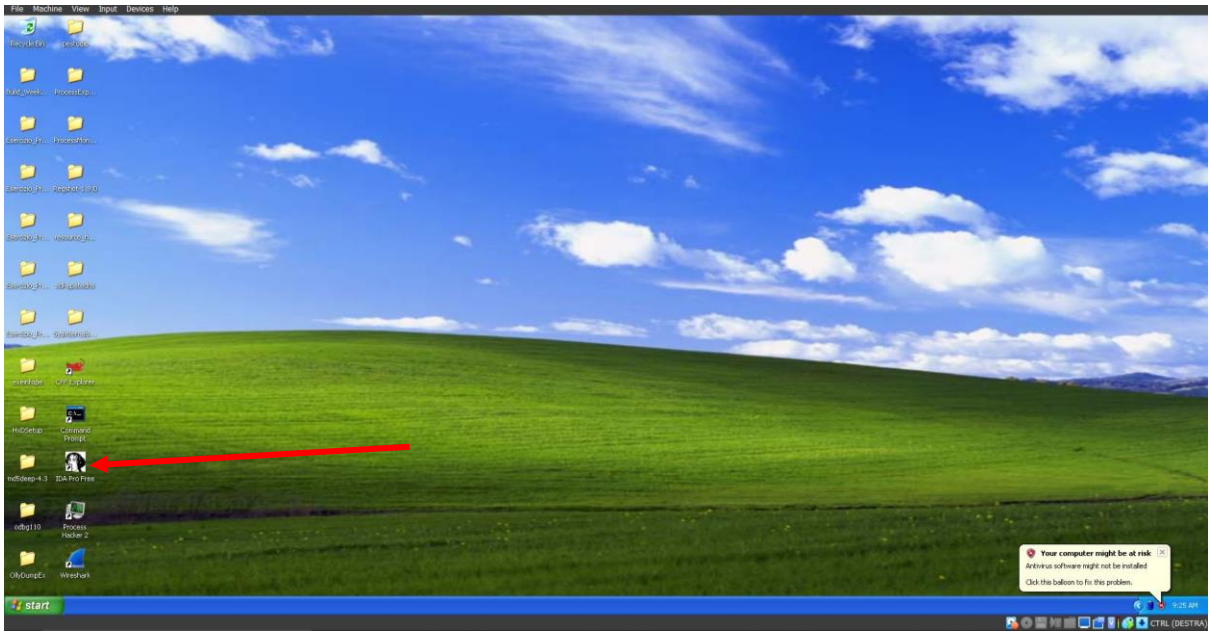
SVOLGIMENTO

DEFINIZIONE: IDA PRO

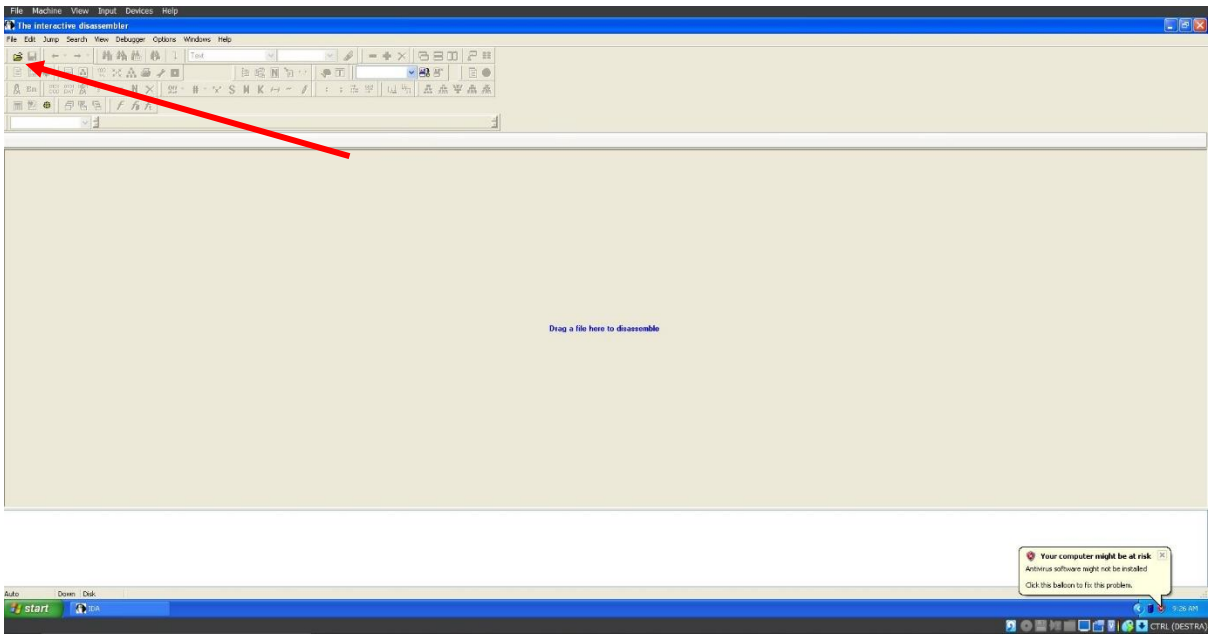
IDA Pro è uno **strumento di analisi malware e reverse engineering** che consente agli esperti di esaminare il codice binario di programmi eseguibili. Fornisce una visualizzazione dettagliata del codice assembly, facilitando l'analisi delle istruzioni e la comprensione del flusso di controllo. La **creazione automatica di grafici del flusso di controllo e la capacità di identificare automaticamente le funzioni** semplificano l'analisi. IDA Pro supporta numerosi tipi di file eseguibili e offre funzionalità avanzate come decompilazione, debugging remoto e scripting per l'automazione delle attività. È uno strumento essenziale per gli analisti di malware e gli esperti di sicurezza per comprendere il comportamento interno di software dannoso.

PREPARAZIONE

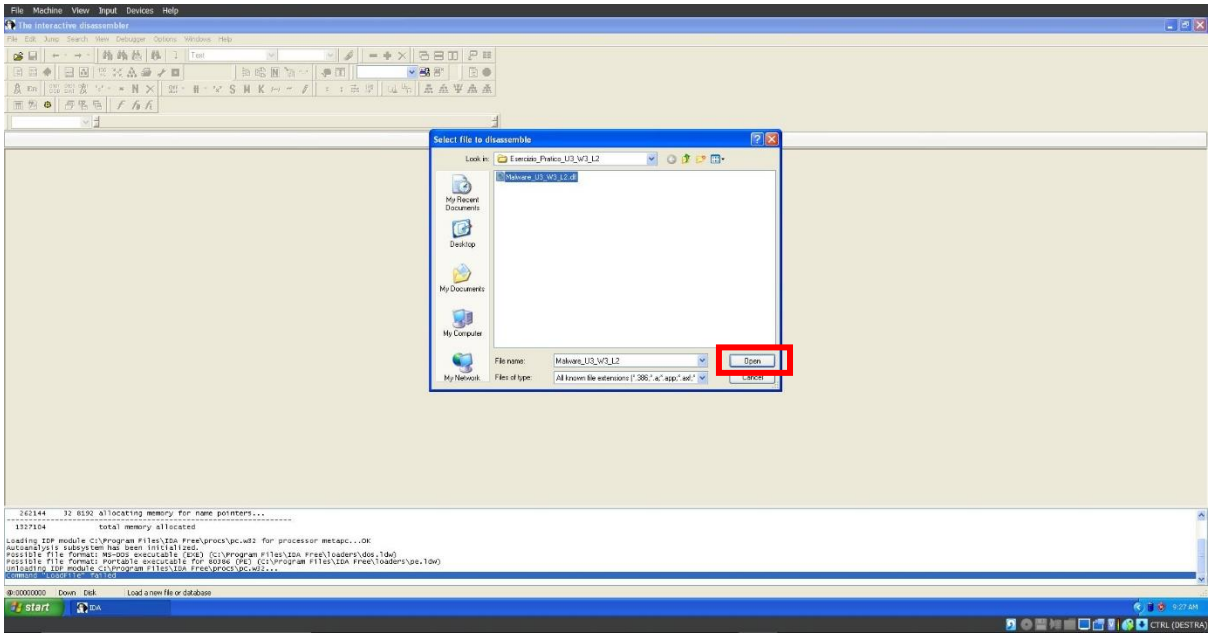
Come prima cosa, prepariamo il software e carichiamo il malware oggetto dell'analisi odierna. Apriamo la macchina virtuale e individuiamo IDA pro sul desktop:



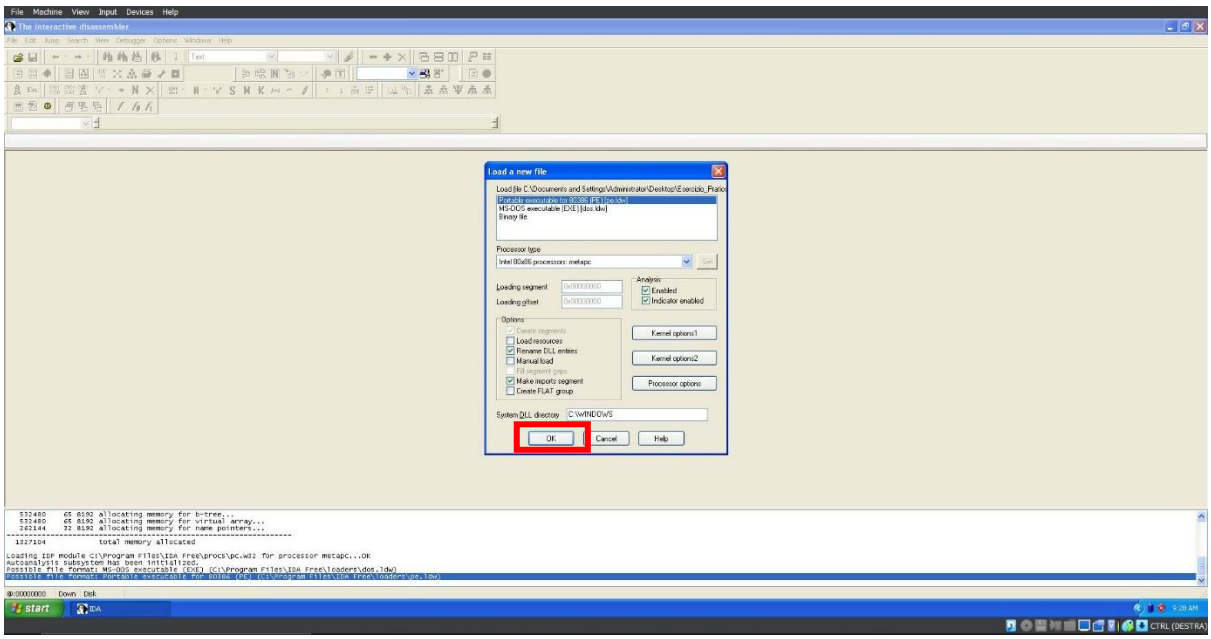
Clicchiamo l'icona a forma di cartella in alto a sinistra:



Selezioniamo il file da analizzare e clicchiamo su open:



Confermiamo a IDA che desideriamo aprire il formato PE:

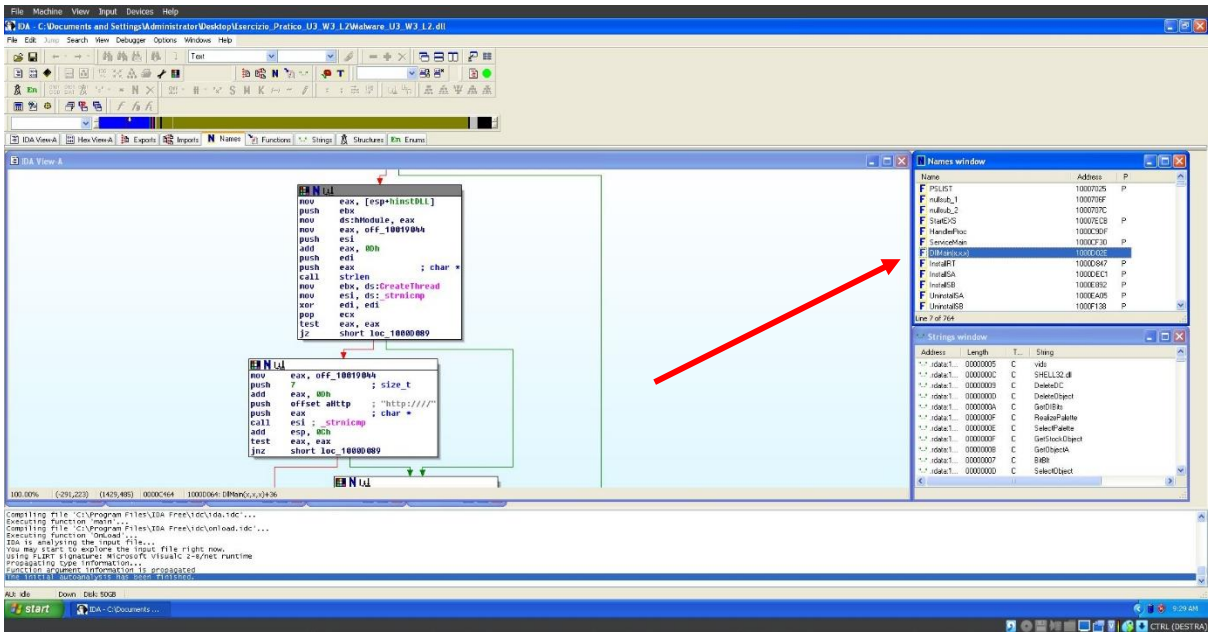


Ora possiamo affrontare le consegne.

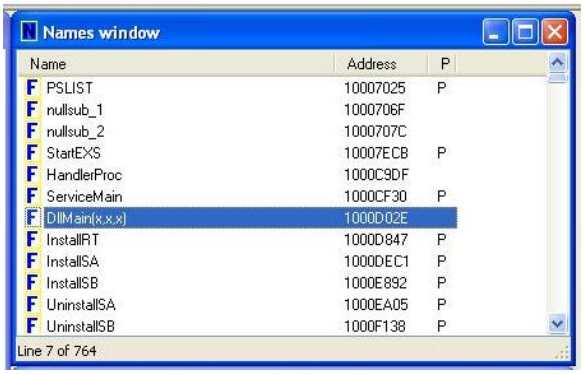
QUESITO 1

Individuare l'indirizzo della funzione DLLMain

Al caricamento del malware sul software, notiamo subito sulla destra la finestra Names Windows. A metà elenco individuiamo DLLMain e di fianco il suo indirizzo:



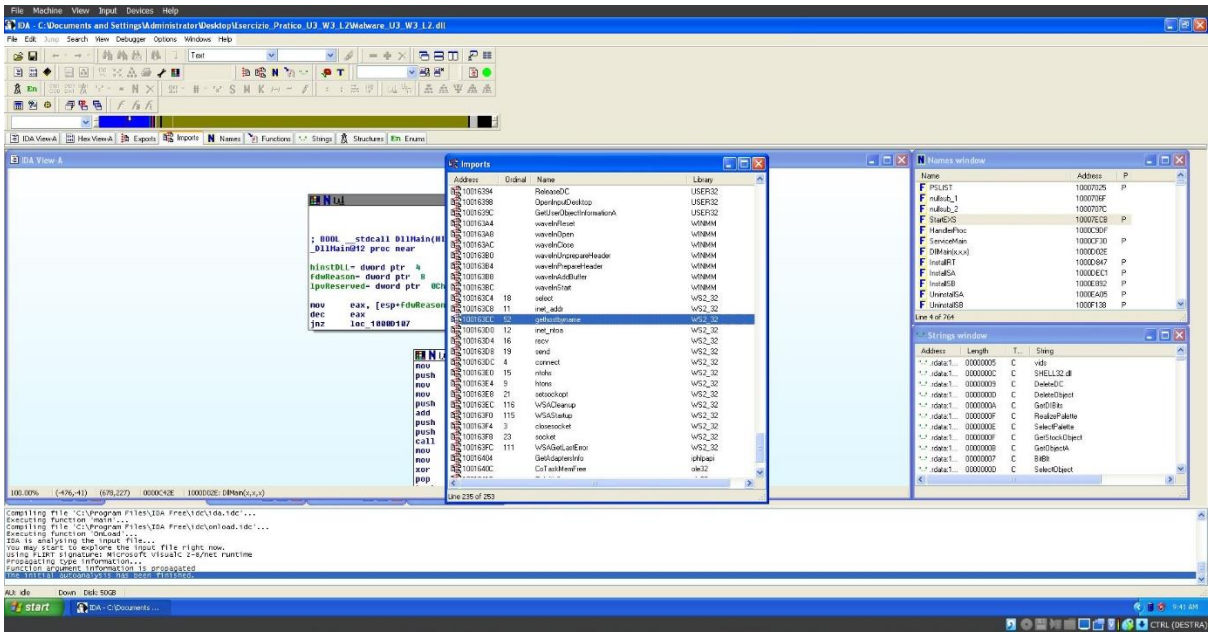
L'indirizzo è 1000D02E:



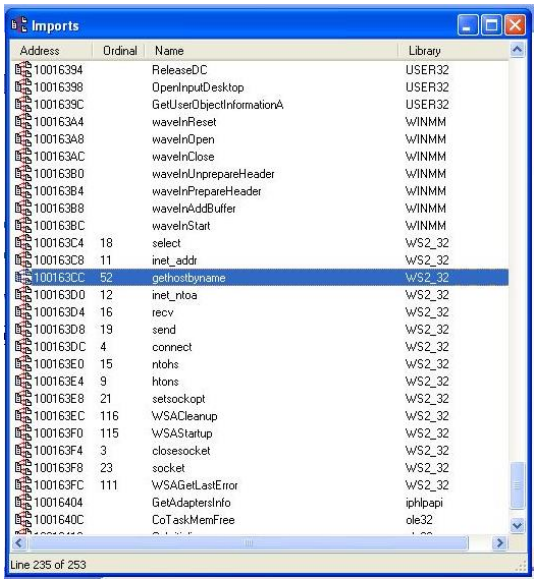
QUESITO 2

Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l'indirizzo dell'import?

Selezioniamo la scheda "imports", che risulta già aperta. Scorriamo la lista fino ad individuare il nome gethostbyname:



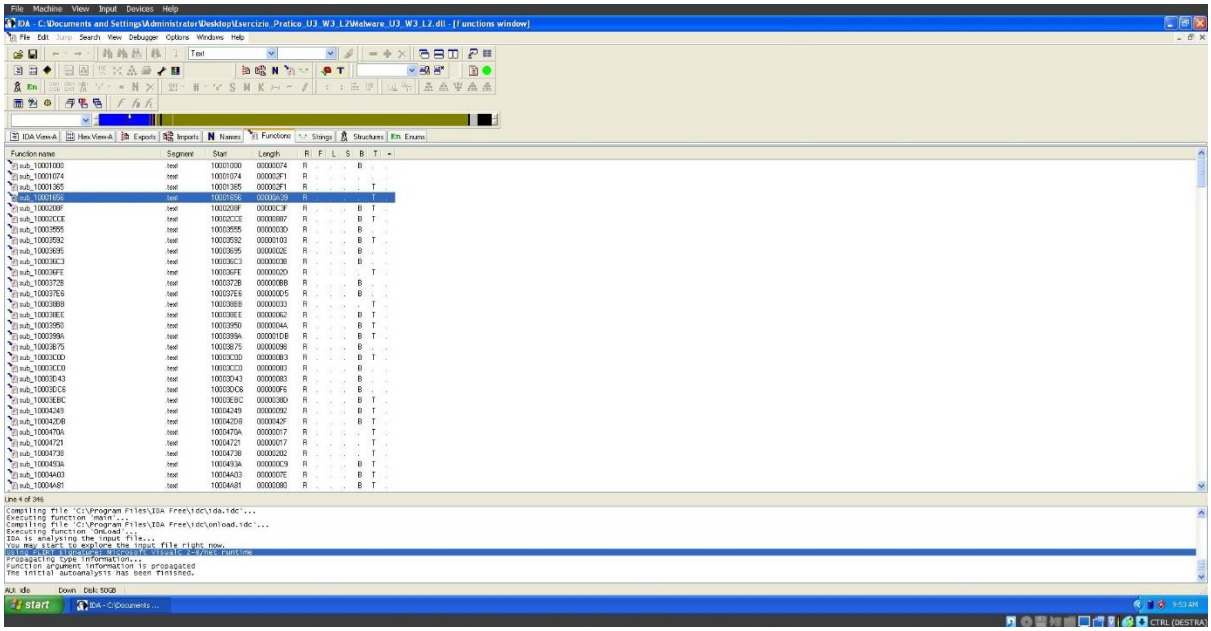
Così possiamo individuare l'indirizzo che è 100163CC:



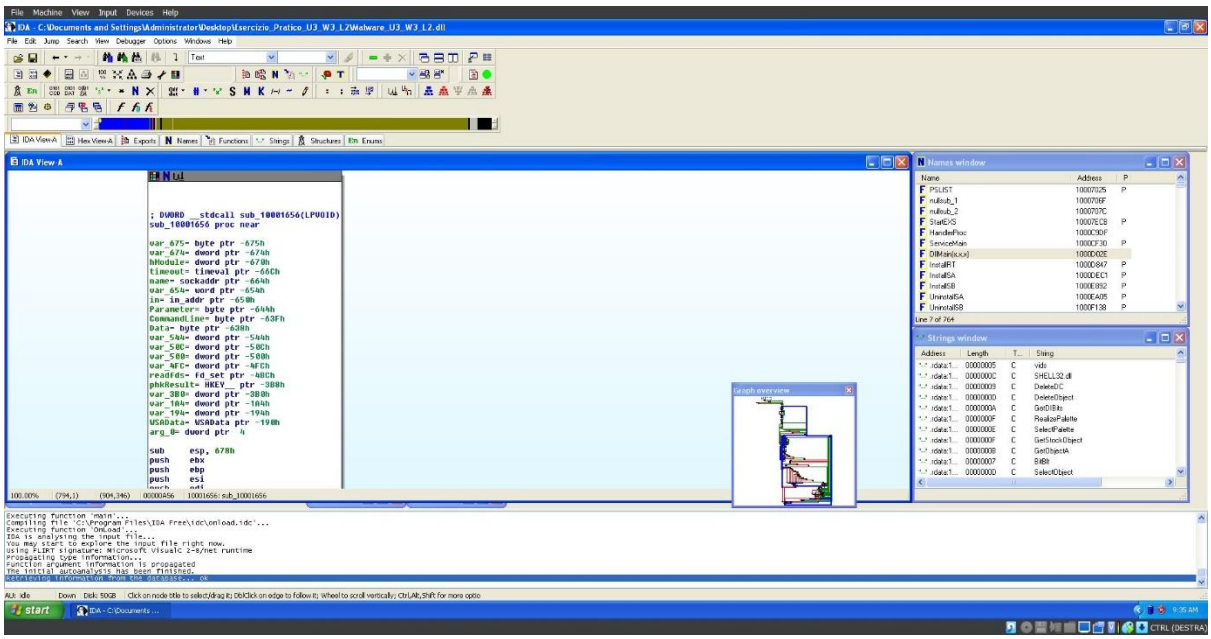
QUESITO 3

Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?

Apriamo la scheda "Functions" e cerchiamo l'indirizzo 0x10001656:



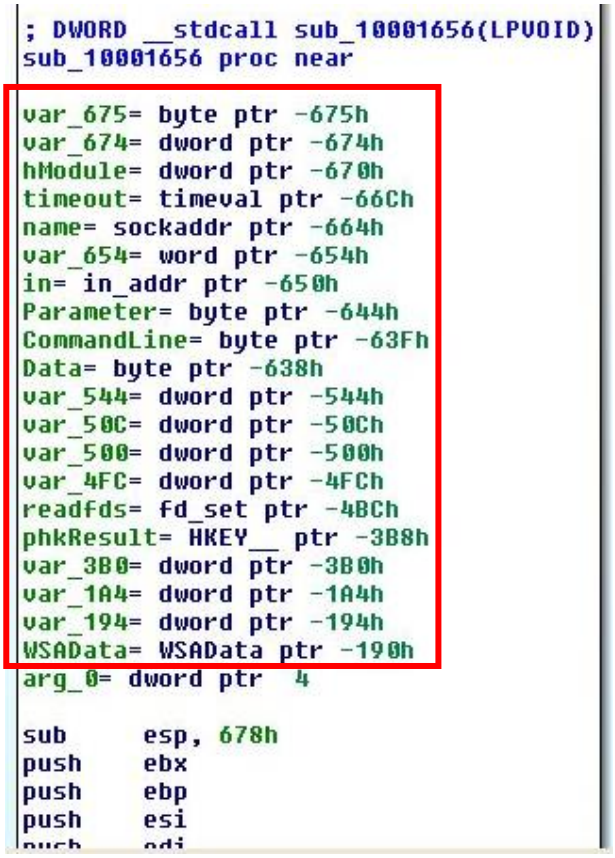
Con un doppio clic atterriamo sul IDA View A per quell'indirizzo:



Partendo dalla definizione teorica per cui:

- Le variabili sono ad un offset negativo rispetto al registro EBP
- I parametri si trovano ad un offset positivo rispetto ad EBP

Individuiamo 20 variabili con offset negativo:



QUESITO 4

Quanti sono, invece, i parametri della funzione sopra?

Vi è una sola riga con offset negativo, dunque il parametro è uno: