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* (così com'è, in esadecimale)

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

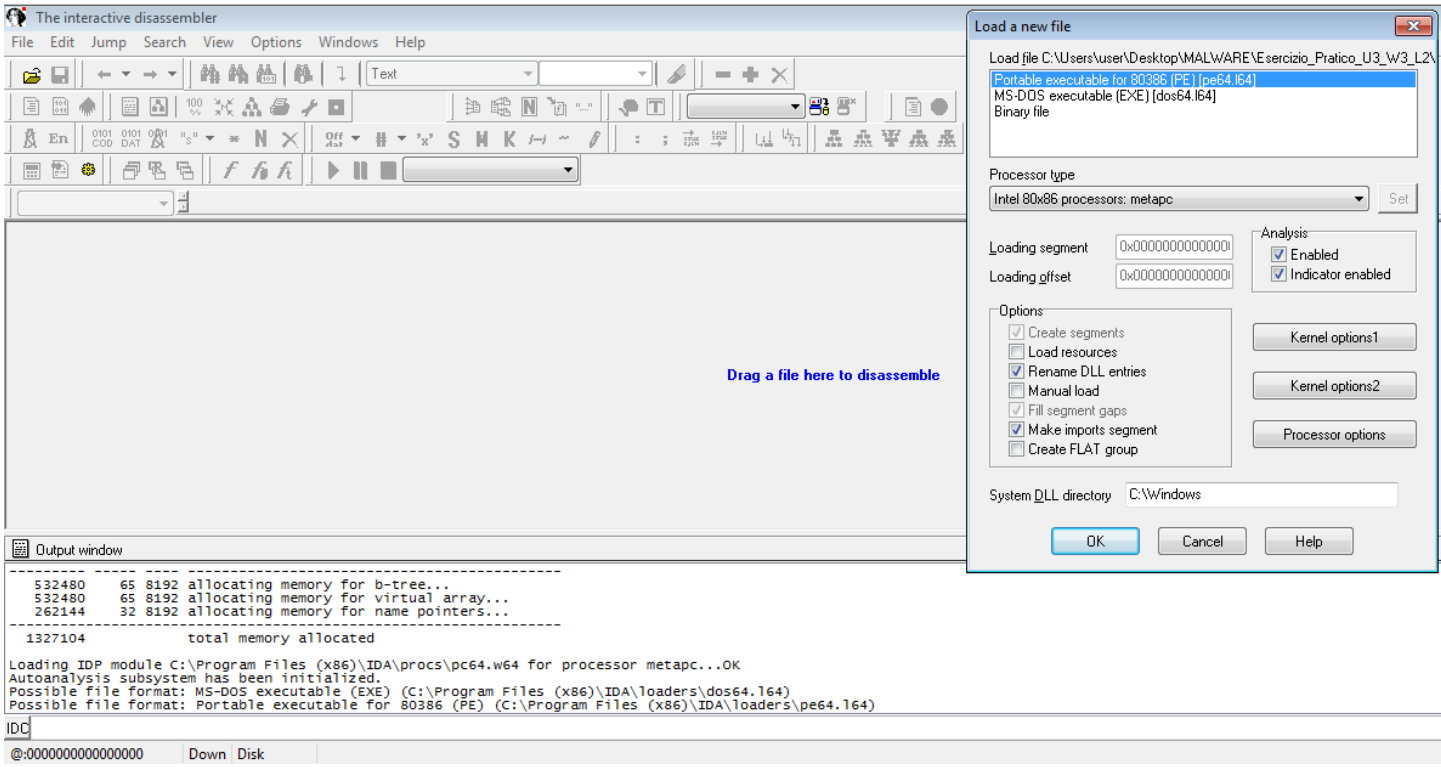
3. Quante sono le *variabili locali* della funzione alla locazione di memoria 0x10001656?

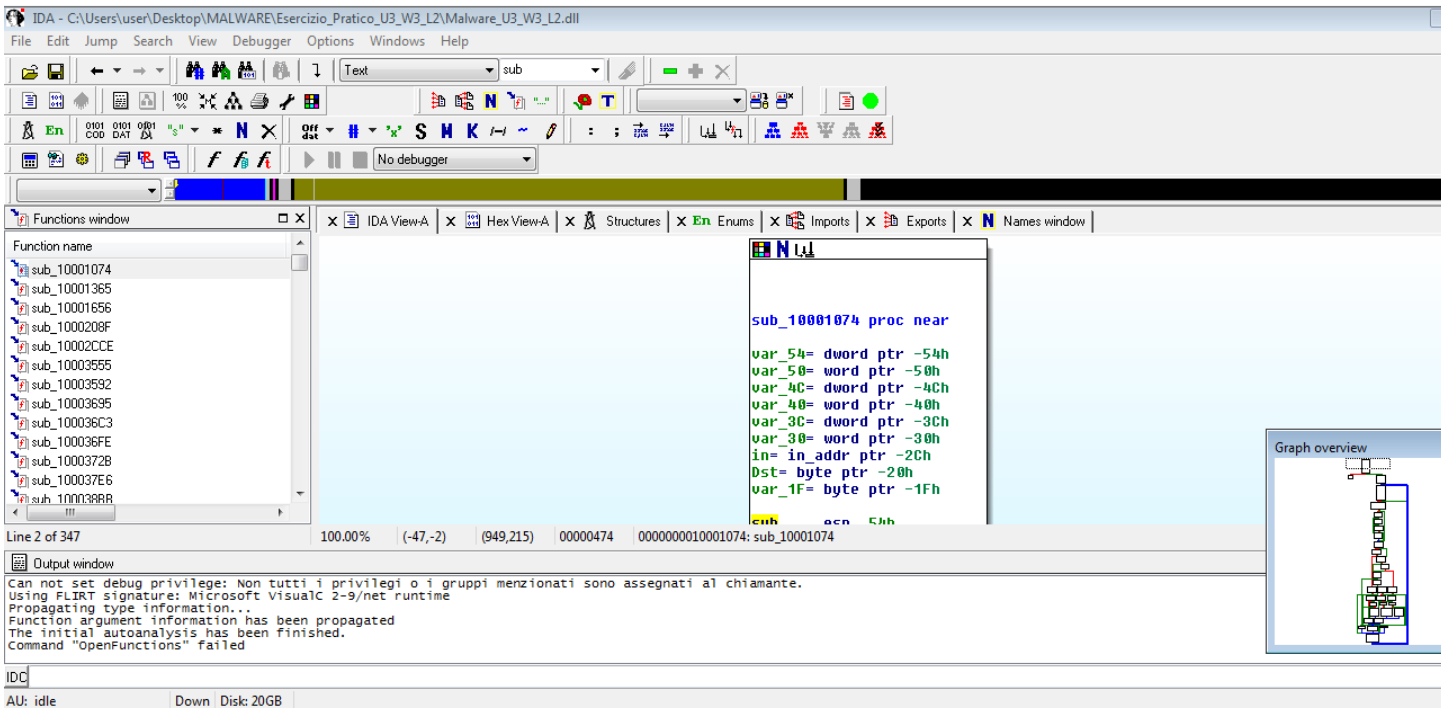
4. Quanti sono, invece, i *parametri* della funzione sopra?

5. Inserire altre considerazioni macro livello sul malware (comportamento).

Premessa → **IDA Pro** è uno degli strumenti più noti e potenti per *l'analisi e il reverse engineering di software binario*. È un ambiente interattivo che consente agli analisti di esaminare il codice assembly, analizzare la struttura e il flusso del programma, identificare funzioni, variabili e stringhe, nonché comprendere il comportamento del software.

Come da istruzione per lo svolgimento dell'esercizio, eseguiamo IDA sulla nostra macchina virtuale ed analizziamo il Malware_U3_W3_L2:

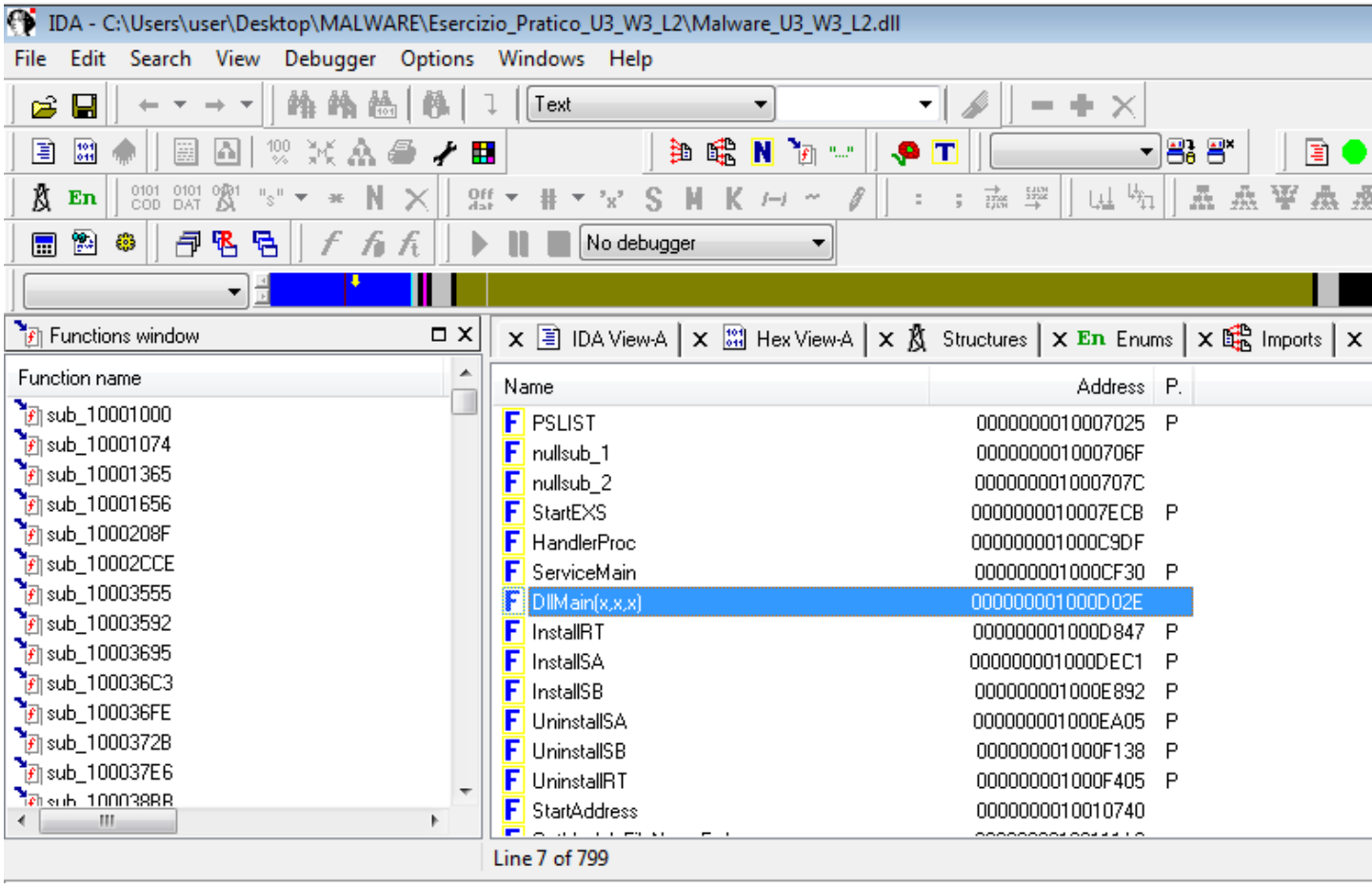




Presenta un’interfaccia molto intuitiva, utile per approcciarsi ad una prima esperienza di analisi. Andiamo quindi a rispondere ai quesiti dell’esercizio.

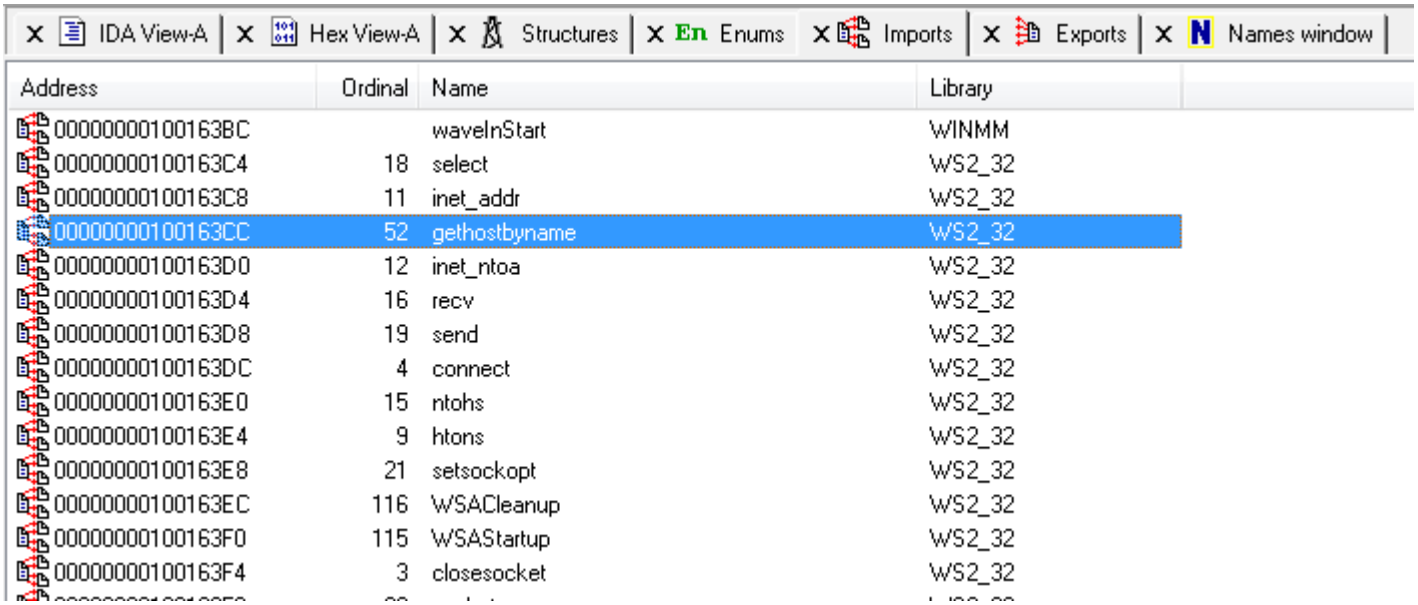
1.----------

Per individuare l'indirizzo DLLMain apriamo la finestra *Names Widow* [N], cerchiamo il nome di interesse e il rispettivo indirizzo. In questo caso **1000D02E:**



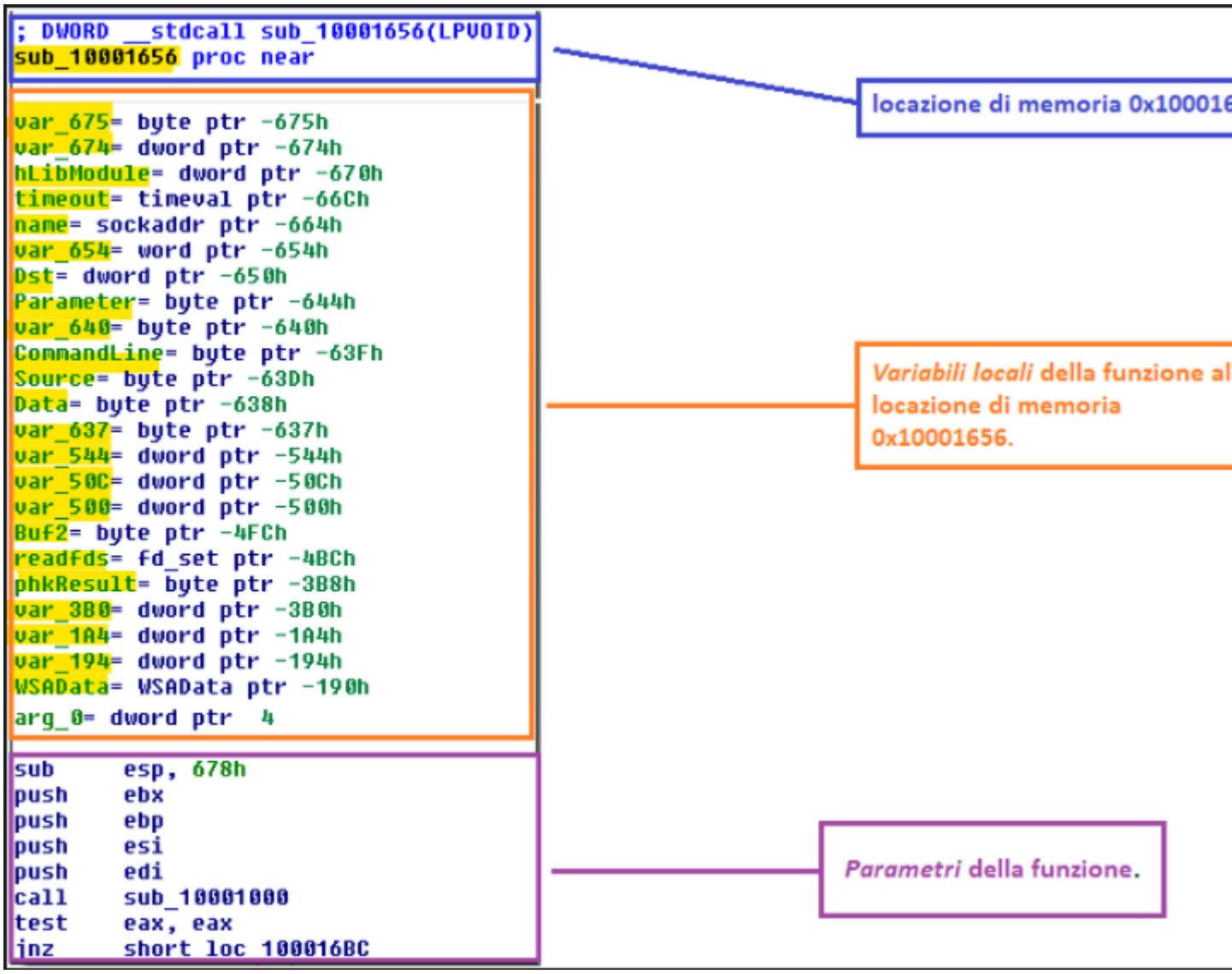
2.----------|

Dalla scheda import, individuiamo la funzione "*gethostbyname*" come richiesto, individuiamo l'indirizzo, in questo caso **100163CC**, e la libreria che ci permette di capire cosa fa la funzione. In questo caso **WS2_32**, una libreria di sistema di Microsoft Windows che fornisce funzionalità per la programmazione di socket e la comunicazione di rete. Questa libreria è fondamentale per lo sviluppo di applicazioni che richiedono comunicazione di rete, come ad esempio applicazioni client-server, applicazioni web, applicazioni che utilizzano protocolli di rete come TCP/IP o UDP, e così via:



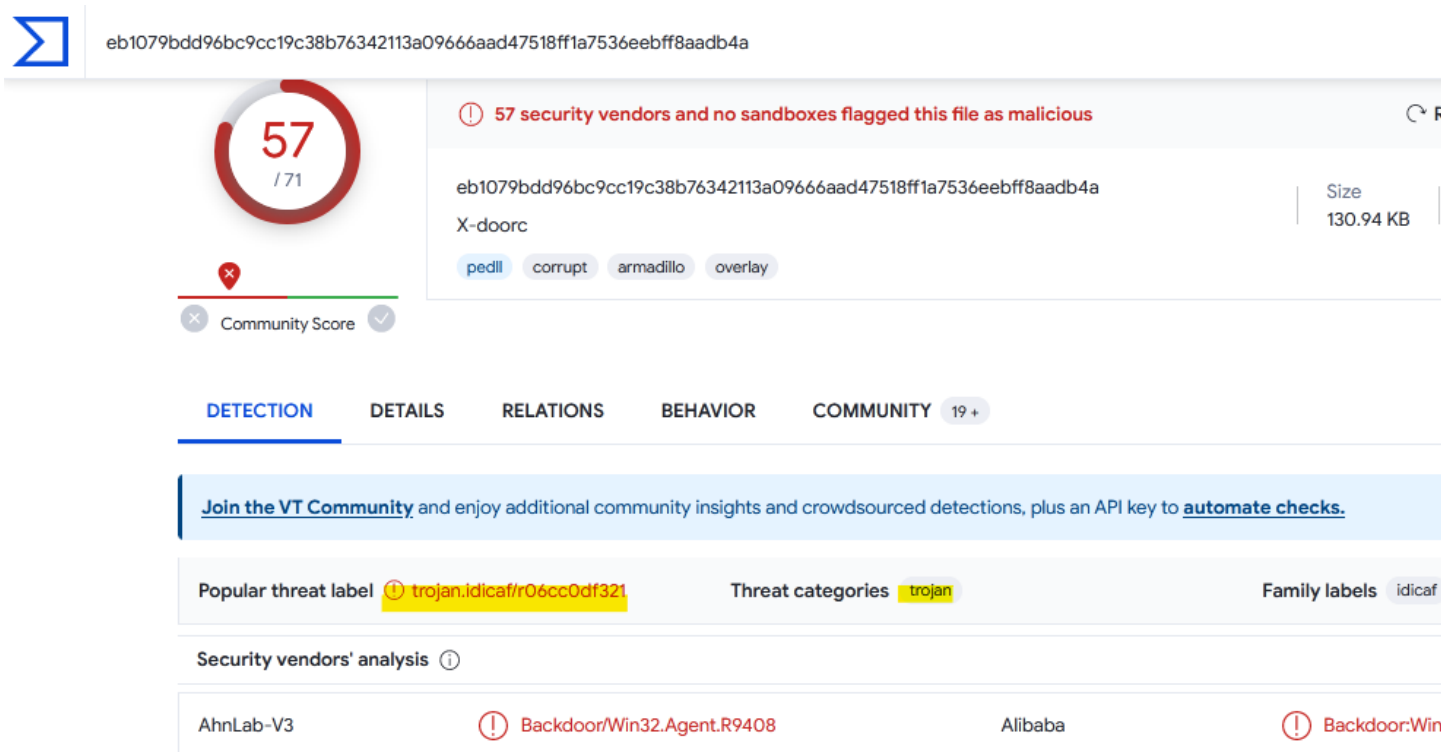
3/4.----------|

Per risponde agli ultimi due quesiti, nel pannello a sinistra, la *Functions widow*, cerchiamo la locazione di memoria **10001656,** facciamo doppio click ed individuiamo, nella sezione *IDA View A* che ci appare, le **variabili locali** e i **parametri** della funzione in oggetto:



5.----------|

Per "*informazioni a livello macro sui malware*", si intende una panoramica generale dei diversi tipi di malware, delle loro caratteristiche e delle tendenze nel panorama della sicurezza informatica. Uno dei metodi già visti in precedenza, prevede l'utilizzo di **Virus Total**, un servizio online gratuito che fornisce analisi di malware e sospetti di malware utilizzando una vasta gamma di motori antivirus e strumenti di scansione:



Gli utenti possono caricare file o inserire URL per essere analizzati da più di 70 motori antivirus e altre tecnologie di rilevamento di minacce. VirusTotal fornisce un rapido riepilogo delle risposte dei vari motori antivirus e consente agli utenti di esaminare i risultati dettagliati delle scansioni.