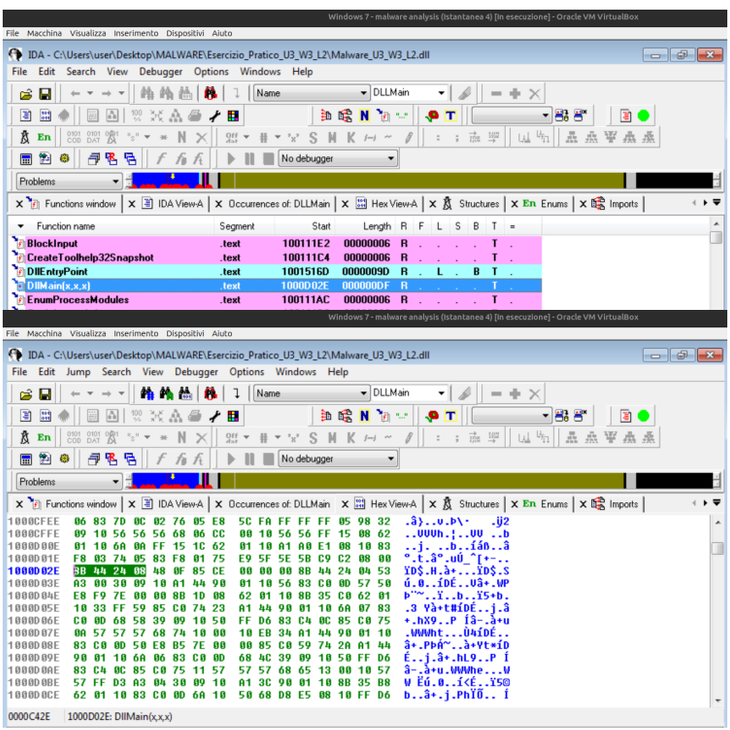
ANALISI STATICA AVANZATA:

#IDA

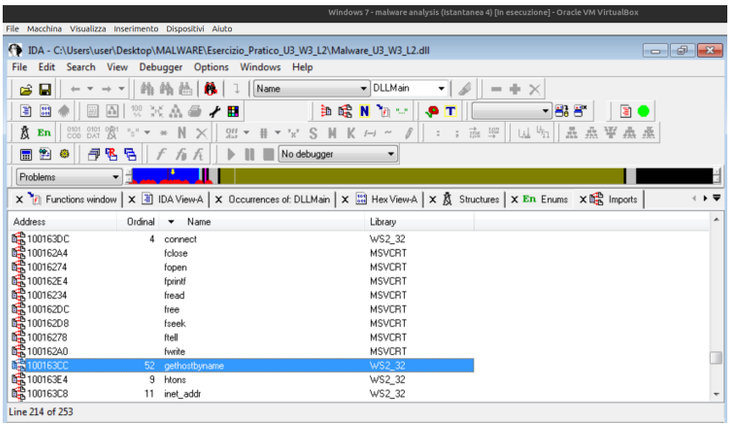
TRACCIA:

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).



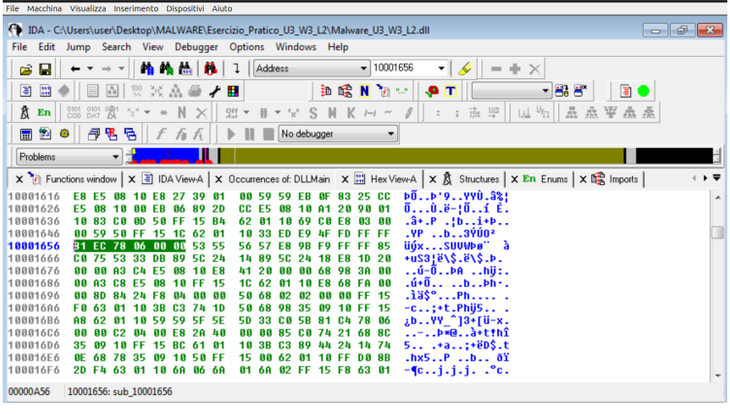
2. DALLA SCHEDA «**IMPORTS**» INDIVIDUARE LA FUNZIONE «**GETHOSTBYNAME**». QUAL È L'INDIRIZZO DELL'IMPORT?



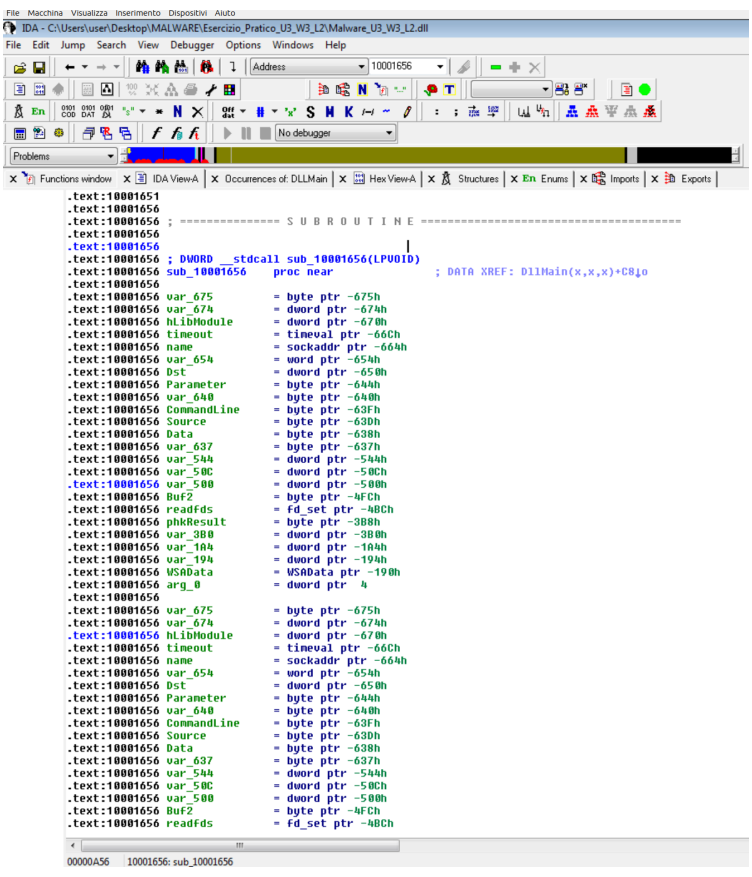
3. QUANTE SONO LE **VARIABILI LOCALI** DELLA FUNZIONE ALLA LOCAZIONE DI MEMORIA **0X10001656**?

4. QUANTI SONO, INVECE, I **PARAMETRI** DELLA FUNZIONE SOPRA?

CERCANDO L'INDIRIZZO DELLA FUNZIONE DIRETTAMENTE DALLA TAB DI RICERCA INSERENDO ADDRESS + NUMERO REGISTRO POSSIAMO ANDARE A VEDERE UNA SERIE DI INFORMAZIONI



VARIABILI:



VARIABILI LOCALI: LE VARIABILI LOCALI IN UNA FUNZIONE ASSEMBLY SONO TIPICAMENTE ALLOCATE NELLO STACK. QUESTO È SPESSO FATTO ATTRAVERSO ISTRUZIONI DI TIPO PUSH ALL'INIZIO DI UNA FUNZIONE O CON UN'ISTRUZIONE SUB CHE AUMENTA IL PUNTATORE DELLO STACK (SP) PER CREARE SPAZIO.

PARAMETRI: SOLITAMENTE I PARAMETRI SONO PASSATI AI REGISTRI O ATTRAVERSO L'USO DELLO STACK PRIMA DELLA CHIAMATA DELLA FUNZIONE. I COMMENTI NEL CODICE POSSONO FORNIRE INDICAZIONI SU DOVE E QUANTI PARAMETRI SONO PASSATI.

LE ETICHETTE COME "ARG_0", "ARG_9", "VAR_54" ECC. SONO VISIBILI, POSSIAMO IPOTIZZARE CHE "ARG_" POSSA RIFERIRSI A PARAMETRI E "VAR_" A VARIABILI LOCALI.

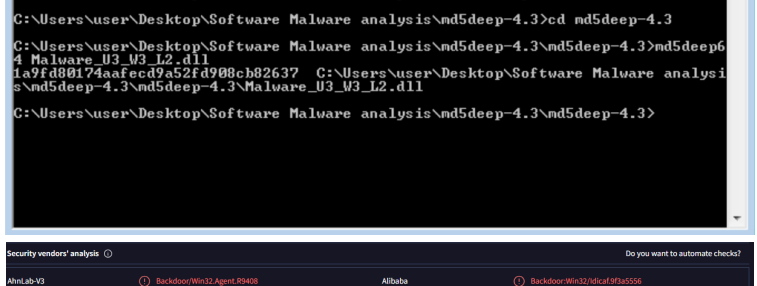
NELL'ASSEMBLY, LE ETICHETTE CHE INIZIANO CON VAR_ TENDONO A INDICARE VARIABILI LOCALI, MENTRE QUELLE CHE INIZIANO CON ARG_ INDICANO ARGOMENTI O PARAMETRI PASSATI ALLA FUNZIONE.

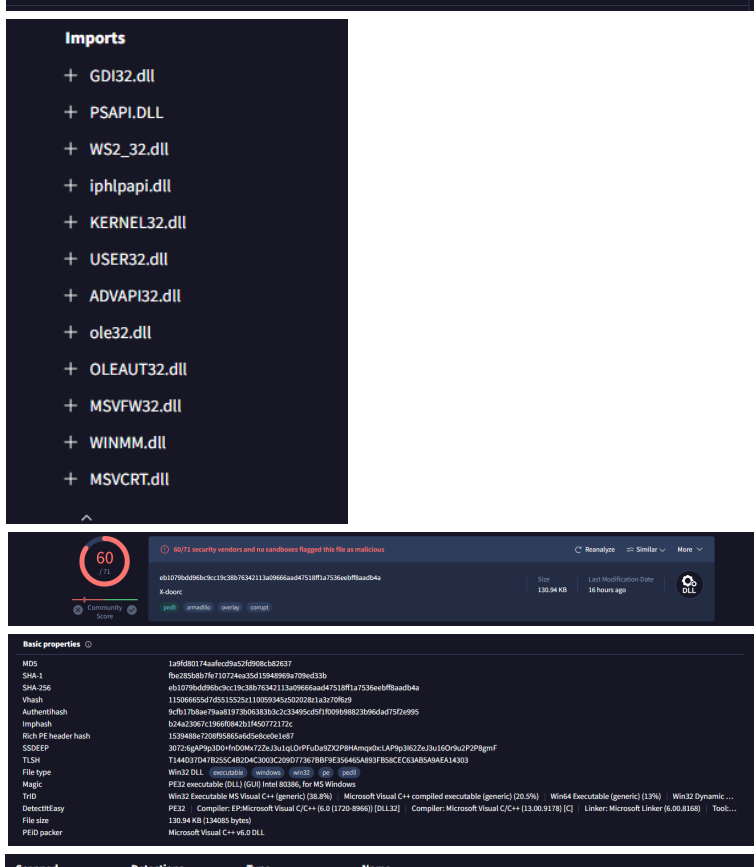
VALORI OFFSET: GLI OFFSET (COME VAR_54H) SONO UTILIZZATI PER ACCEDERE A DATI SPECIFICI SULLO STACK. GLI OFFSET NEGATIVI RISPETTO ALL'INDIRIZZO BASE DEL FRAME DELLA FUNZIONE (AD ESEMPIO EBP SU X86) DI SOLITO INDICANO VARIABILI LOCALI, MENTRE GLI OFFSET POSITIVI INDICANO PARAMETRI.

IN QUESTO CASO LE VARIABILI LOCALI IN EVIDENZA CHE POSSIAMO RILEVARE AD UN'OCCHIATA SONO 11: VAR_194, VAR_1A4, VAR_3B6, VAR_544 ,VAR_56C, VAR_58C, VAR_637, VAR_646, VAR_654, VAR_674, VAR_675; MENTRE IL PARAMETRO È UNO ED È ARG_0

5. INSERIRE ALTRE CONSIDERAZIONI MACRO LIVELLO SUL MALWARE

RILEVANDO L'HASH CON MD5DEEP64 ED ANDANDOLO AD INSERIRE SU VIRUS TOTAL SI POSSONO TROVARE MOLTE INFORMAZIONI RIGUARDO AL MALWARE IN QUESTIONE, CHE IN SOSTANZA È UN BACKDOOR/TROJAN HORSE.
INOLTRE ANDANDO A VEDERE I PROCESSICHE CREA/UTILIZZA E LE LIBRERIE CHE IMPORTA POSSIAMO DEDURRE CHE CERCA DI MIMETIZZARSI COI PROCESSI COMUNI DI WINDOWS E RESTARE IN ASCOLTO LATENTE.
TROVIAMO TANTE FUNZIONI, ED È FACILE PERDERSI SENZA UNA CONOSCENZA APPROFONDITA.
AD ESEMPIO C'È UNA FUNZIONE CHE ECRCA DI METTERSI IN ASCOLTO O RICEVERE UNA STRINGA / OPPURE USER_AGENT MOZILLA CHE CERCA DI COLLEGARSI MAGARI SIMULANDO UNA RICHIESTA HTTP CHE PROVIENE DA UN BROWSER (FARÀ UN GET... ECC), UNA FUNZIONE CHE VA A CERCARE UN DEVICE VIDEO, MAGARI VA A CERCARE DEGLI ESEGUIBILI... ECC.





Scanned	Detections	Type	Name
2023-10-10	57 / 66	ZIP	704138bec89cf9e7f00fbce100dbc09cf133d16dc0203806392f0e153c43c68c.zip
2023-09-04	30 / 49	ZIP	Malware Analysis Resources.zip
2024-04-03	51 / 65	ZIP	Malware_U3_W3_L2.zip
2023-01-25	56 / 65	ZIP	--master.zip
2024-02-13	61 / 70	Win32 EXE	TJprojMain
2023-05-09	55 / 64	ZIP	Cmulator-0.2.1.zip
2020-12-20	51 / 64	ZIP	Practical-Malware-Analysis-Labs.zip
2023-09-02	52 / 63	ZIP	PracticalMalwareAnalysis-Labs.exe.zip
2021-12-29	34 / 54	RAR	chapter_5.rar
2022-12-03	41 / 61	RAR	4fb9859ece666c158455f74fcc63d800b9601c92b3e2040a3096b63952dbf7ff
2024-01-31	52 / 62	ZIP	ZARARLI.zip
2023-09-01	53 / 65	ZIP	lab1.zip
2023-04-18	51 / 64	ZIP	PracticalMalwareAnalysis-Labs-master.zip
2023-12-02	57 / 66	ZIP	Files2Examine_F2023(2).zip
2023-10-01	55 / 72	Win32 EXE	7fc045e3c4eb624e7505df106a9f3241.virus
2024-04-02	62 / 70	Win32 EXE	PracticalMalwareAnalysis-Labs.exe
2023-01-10	30 / 50	ZIP	Malanalisys.zip
2020-11-27	55 / 65	ZIP	Practical Malware Analysis Labs.zip
2023-09-12	56 / 65	ZIP	Practical Malware Analysis Labs.zip
2024-04-01	57 / 66	ZIP	Practical Malware Analysis Lab Files.zip