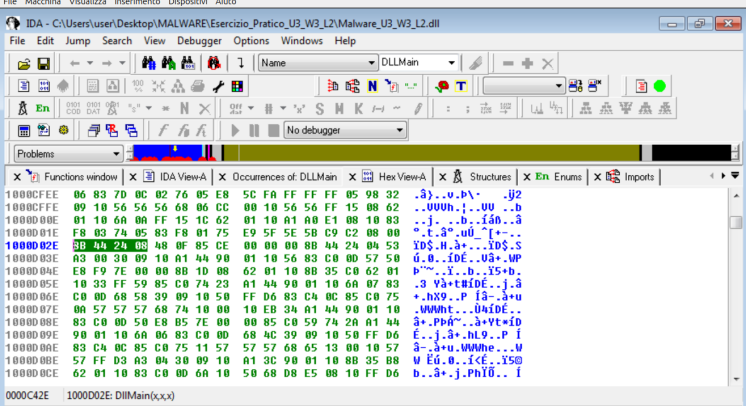
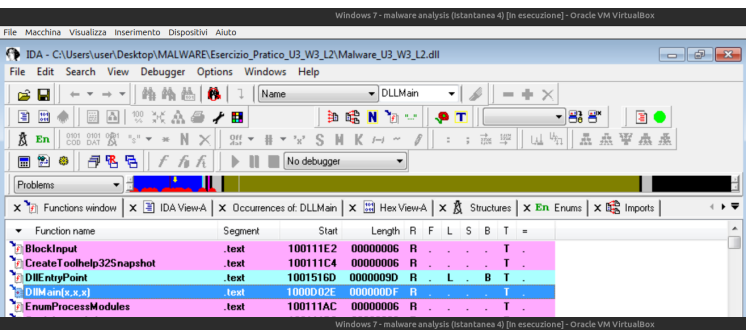


ANALISI STATICA AVANZATA: #IDA

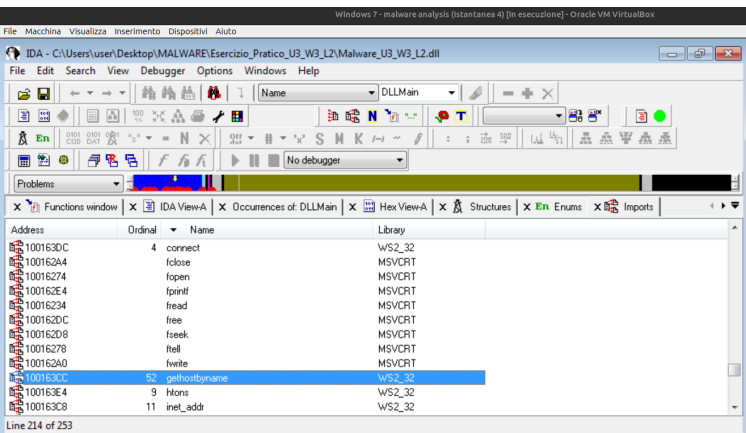
TRACCIA:

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).



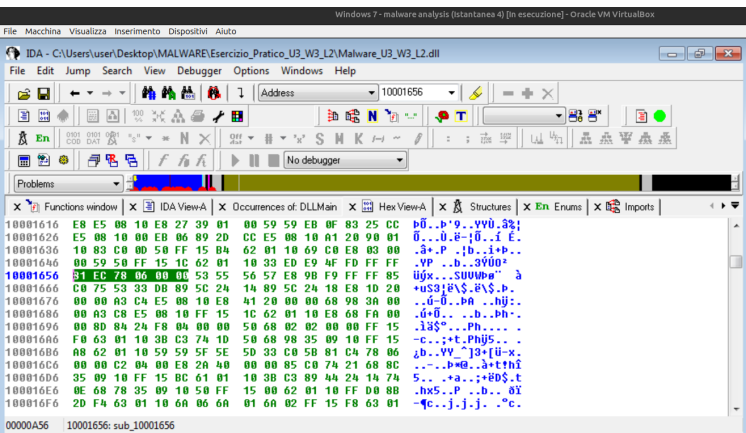
2. DALLA SCHEDA «IMPORTS» INDIVIDUARE LA FUNZIONE «GETHOSTBYNAME». QUAL È L'INDIRIZZO DELL'IMPORT?



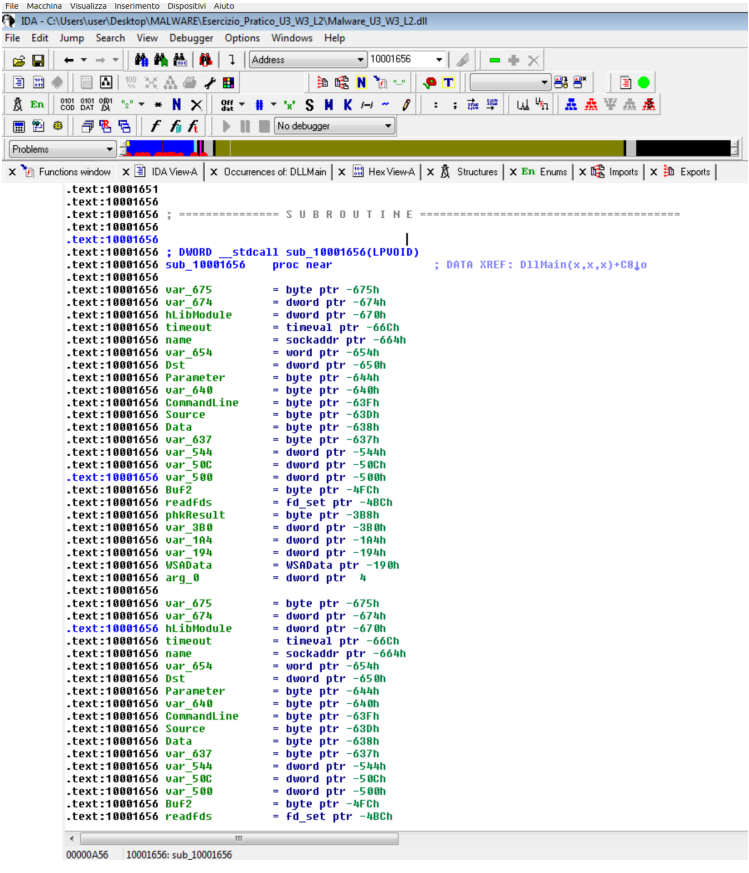
3. QUANTE SONO LE VARIABILI LOCALI DELLA FUNZIONE ALLA LOCAZIONE DI MEMORIA 0X10001656?

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**

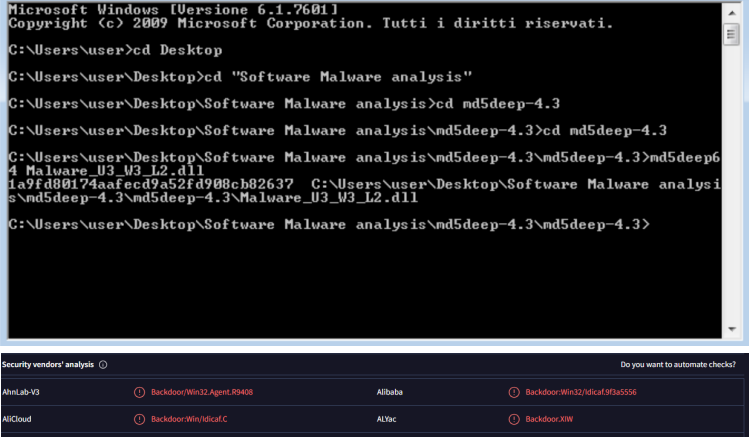
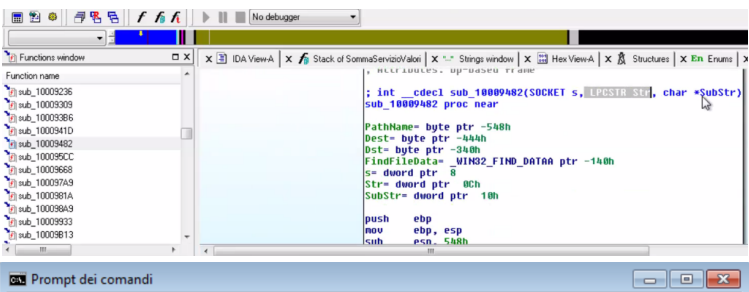
5. INSERIRE ALTRE CONSIDERAZIONI MACRO LIVELLO SUL MALWARE

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.

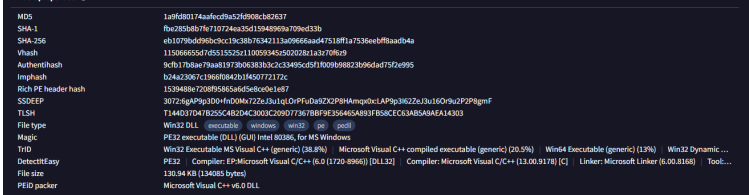
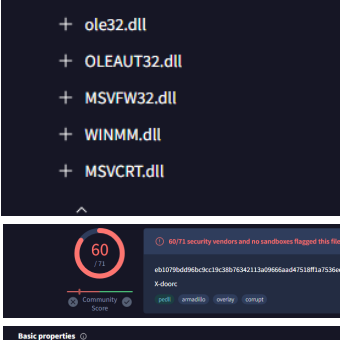
INOLTRE ANDANDO A VEDERE I PROCESSICHE CREA/UTILIZZA E LE LIBRERIE CHE IMPORTA POSSIAMO DEDURRE CHE CERCA DI MIMETIZZARSI COI PROCESSI COMUNI DI WINDOWS E RESTARE IN ASCOLTO LATENTE.

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.



| Security vendors' analysis | | | Do you want to automate checks? |
|----------------------------|-----------------------------------|--------------|---------------------------------|
| AhnLab-V3 | Backdoor/Win32.Agent.R9408 | Alibaba | Backdoor/Win32/Idcal/93a5556 |
| AliCloud | Backdoor/Win/Idcal.C | ALYac | Backdoor.XIW |
| Antiy-AVL | Trojan/Backdoor/Win32.Agent | Arcabit | Backdoor.XIW |
| Avast | Win32.Agent-OLH [Trj] | AVG | Win32.Agent-OLH [Trj] |
| Avira (no cloud) | BOS/Agent.two.134160 | BitDefender | Backdoor.XIW |
| Bkav Pro | W32.Common.983E47C | ClamAV | Win.Trojan.Idcal/9937585-0 |
| CrowdStrike Falcon | Win/malicious_confidence_100% (W) | Cylance | Unsafe |
| Cynet | Malicious (score: 100) | DeepInstinct | MALICIOUS |
| DrWeb | BackDoor.Siggen.47995 | Elastic | Malicious (high Confidence) |
| Emisoft | Backdoor.XIW (B) | eScan | Backdoor.XIW |
| ESET-NOD32 | A Variant Of Win32/Idcal.C | Fortinet | W32/Idcal.Kitr |
| GData | Backdoor.XIW | Google | Detected |
| Gridinsoft (no cloud) | Trojan.Heur.02016020 | Ikarus | Virus.Win32.Agent.OLH |
| Jiangmin | Backdoor/Agent.cejo | K7AntiVirus | Trojan (004c48271) |
| K7GW | Trojan (004c48271) | Kaspersky | Backdoor.Win32.Agent.kwa |
| Kingsoft | Win32.Hack.Agent.kwa | Lionic | Trojan.Win32.QQPass.logG |



| Basic properties | | File type | |
|---------------------|--|---|---|
| MD5 | 1a9fd80174aafec9a52fd908cb82637 | Win32 DLL | executable (windows) (win32) (pe) (peidl) |
| SHA-1 | fbe2850b7fe710724ea35d15948969a709ed33b | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows | Win32 Executable (generic) (38.8%) |
| SHA-256 | eb1079bdc96bc9cc19c38b76342113a09666aad47518f1a7536eebf8aad4a | PE32+ Compiler: Microsoft Visual C/C++ (6.0 (L1720-8966)) [DLL32] | Compiler: Microsoft Visual C/C++ (13.00.9178) [C] |
| Vhash | 115066655d7d5515525z110059345z02028z1a3z70f6z9 | Linker: Microsoft Linker (6.00.8168) | Tool... |
| Imphash | 9cfb17b8ae79aa81973b06383b3c2c3495c5f1f009b98823b96dad75f2e995 | | |
| Rich PE header hash | b24a23067c196f0842b13450772172c | | |
| SSDEEP | 1539489e7208f95865a6d5e8oe0e1e87 | | |
| File type | Win32 DLL | | |
| Trid | PE32 executable (DLL) (GUI) Intel 80386, for MS Windows | | |
| DetectItEasy | Win32 Executable MS Visual C++ (generic) (38.8%) | | |
| PEID packer | Microsoft Visual C++ v6.0 DLL | | |

| Scanned | Detections | Type | Name |
|------------|------------|-----------|---|
| 2023-10-10 | 57 / 66 | ZIP | 704138bec89cf9e7f00fbc100dbc09cf133d16dc0203806392f0e153c43c68c.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 | Cumulator-0.2.1.zip |
| 2020-12-20 | 51 / 64 | ZIP | Practical-Malware-Analysis-Labs.zip |
| 2023-09-02 | 51 / 63 | ZIP | PracticalMalwareAnalysis-Labs.exe.zip |
| 2021-12-29 | 34 / 54 | RAR | chapter_5.rar |
| 2022-12-03 | 41 / 61 | RAR | 4fb9859ece666c158455f74fcc63d800b9601c92b3e2040a3096b63952dbf7f |
| 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 | Malanalysis.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 |