

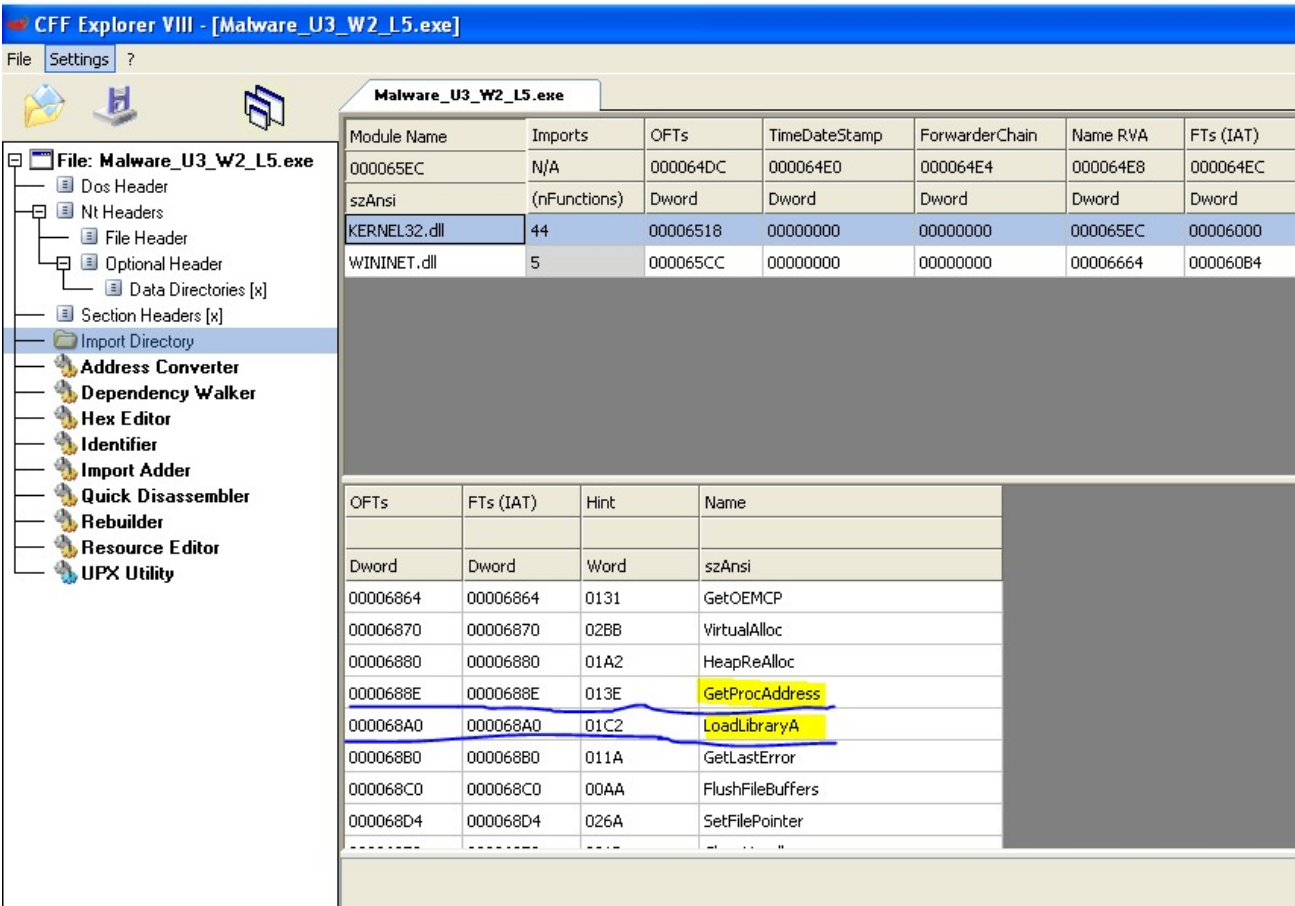
Progetto Week 10 - Fundamentals of Malware Analysis and reverse engineering

- Librerie importate

Possiamo verificare quali sono le librerie importate dal file eseguibile utilizzando CFF Explorer e selezionando **"import directory"**. Come possiamo vedere nella figura di seguito, le librerie importate sono due:

KERNEL32.dll, che contiene le funzioni principali per interagire con il sistema operativo (gestione file, memoria...)

WININET.dll, che contiene le funzioni di implementazione dei protocolli di rete (http, ftp, ntp...)

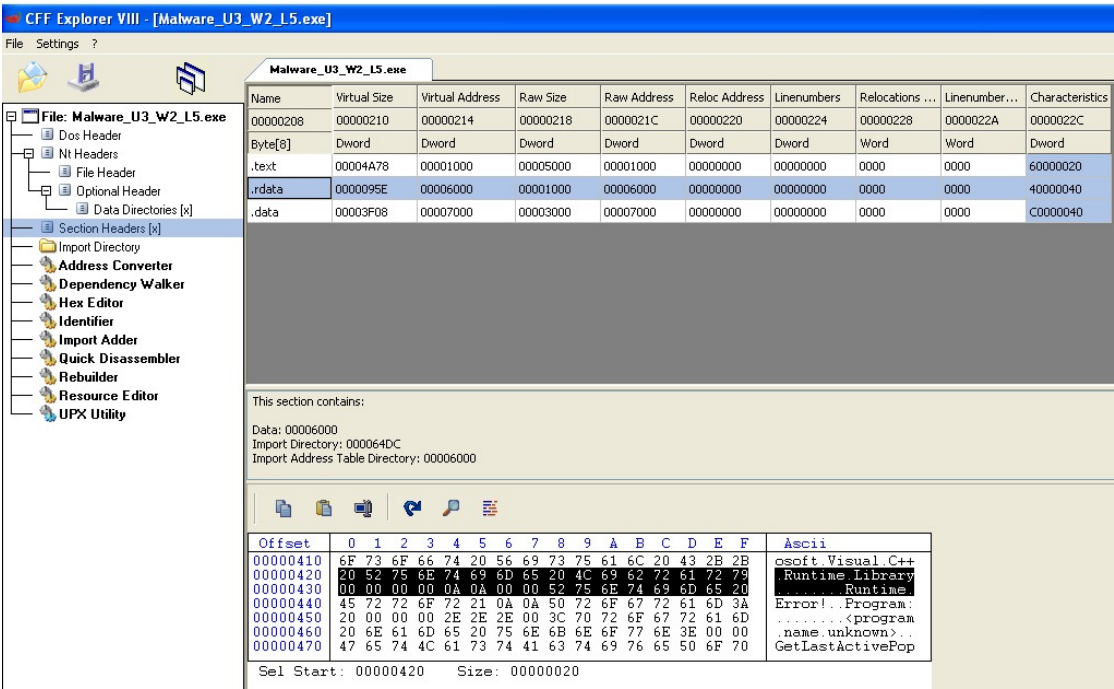


Analizzando le informazioni della libreria Kernel, possiamo notare la presenza di funzioni quali **"GetProcAddress"** e **"LoadLibraryA"**. Ciò ci fornisce una prima informazione sul malware: **importa le librerie "Runtime"** (ovvero, a tempo di esecuzione e, quindi, solo in caso di bisogno), nascondendo le informazioni sulle librerie importate a monte.

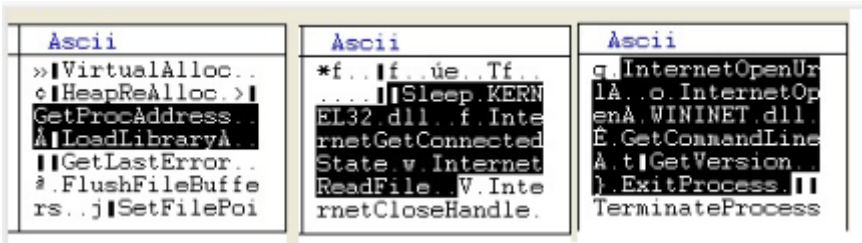
● Sezioni del file eseguibile

Continuando ad utilizzare il tool CFF Explorer, è possibile spostarsi su "Section Headers". Il file ha 3 sezioni:

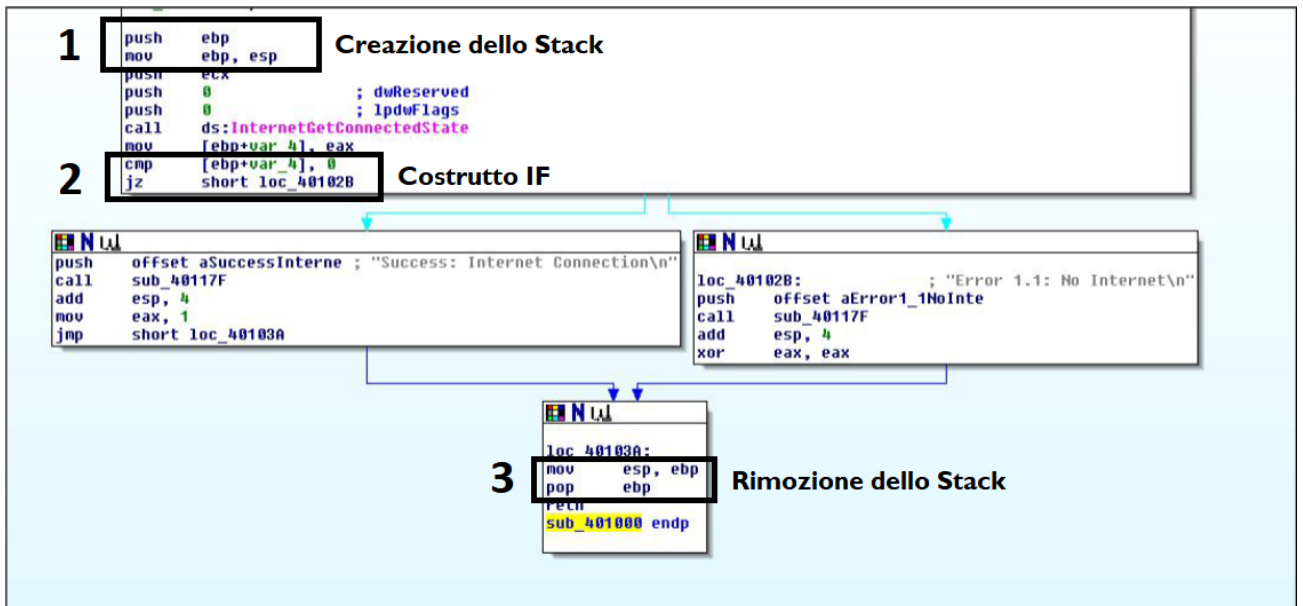
- .text , che contiene le istruzioni che la CPU eseguirà all'avvio del software
- .rdata , che contiene informazioni sulle librerie e sulle funzioni importate/esportate
- .data , che contiene i dati e le variabili del file eseguibile



- In particolar modo nella sezione .rdata possiamo ricavare le seguenti indicazioni sui possibili comportamenti del malware (E' opportuno specificare che non si tratta di informazione certe e precise, ma di indicazioni)
- importa una libreria runtime (confermando quanto avevamo già visto su "import directory"). Ciò possiamo denotarlo anche da "GetProcAddress"
 - "Load Library" indica che il malware può caricare una libreria di sistema in memoria
 - "Sleep" è una funzione di sistema che sospende l'esecuzione della libreria "kernel32.dll"
 - Se il computer è connesso a internet ("InternetgetConnected"), il malware può leggere i dati da un risorsa internet.
 - InternetOpenUrl è una funzione di sistema che viene utilizzata per aprire una connessione Internet e ottenere l'handle di una risorsa



- Identificare i costrutti noti del file in Assembly



- Ipotesi del comportamento della funzionalità implementata

Dopo aver creato lo stack, il codice istruisce di eseguire un check di connessione, per verificare se la macchina è connessa o meno ad Internet.

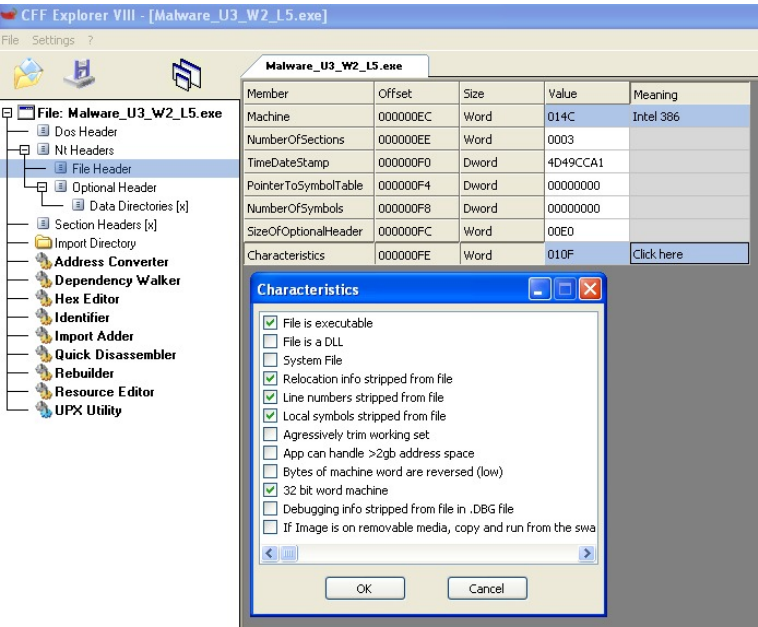
-Se il parametro restituito da "InternetgetConnectedState" $\neq 0$, la funzione stamperà a schermo un messaggio di successo: "Success: Internet Connection"

-Se il parametro restituito da "InternetgetConnectedState" = 0, la funzione stamperà a schermo un messaggio di errore "Error 1.1: No Internet"

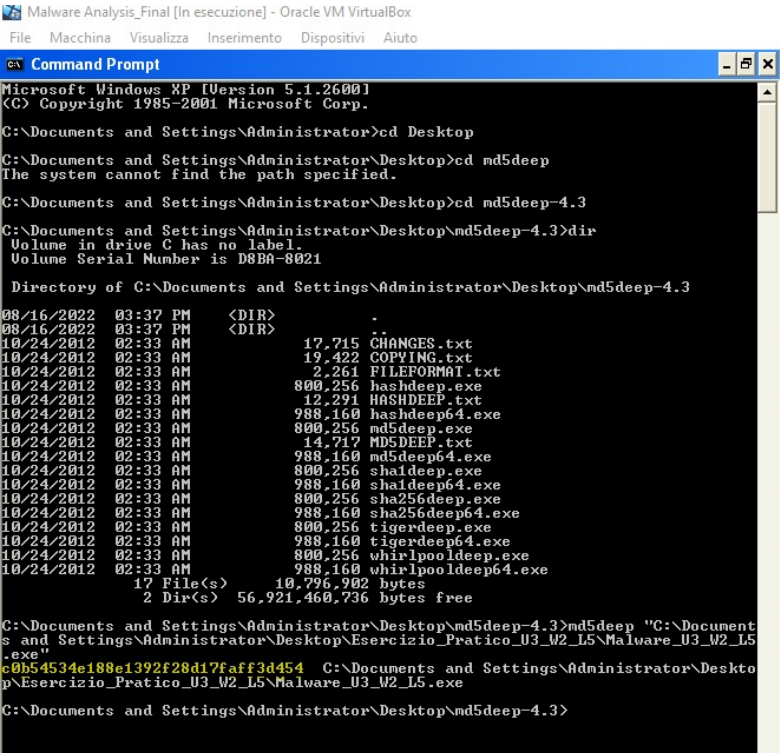
Infine il codice chiude lo stack

Approfondimenti: ricerca di altre informazioni sul malware

- In **File Header** possiamo vedere delle informazioni generiche sull'eseguibile



- Utilizzando **md5deep** posso calcolare l'hash dell'eseguibile e usare lo stesso per ottenere, anzitutto, la conferma che si tratti di un malware e, auspicabilmente, maggiori informazioni sul comportamento dello stesso.



L'hash dell'eseguibile è il codice evidenziato in giallo nella figura qui sopra.

Inserendo l'hash in analisi in "anyrun", 2 risultati su 10 lo identificano come un malware: un risultato non molto soddisfacente.

Public submissions			
c0b54534e188e1392f28d17faff3d454			
 Windows 7 Professional 32bit	✓		No threats detected
27 December 2022, 06:00			Lab06-02.exe PE32 executable (console) intel 80386, for MS Windows
 Windows 7 Professional 32bit	✓		No threats detected
23 August 2022, 22:02			Lab06-02.exe PE32 executable (console) intel 80386, for MS Windows
 Windows 7 Professional 32bit	✓		Malicious activity
09 February 2022, 23:54			Lab06-02.exe PE32 executable (console) intel 80386, for MS Windows
 Windows 7 Professional 32bit	✓		No threats detected
05 September 2020, 05:57			Lab06-02.exe PE32 executable (console) intel 80386, for MS Windows
 Windows 7 Professional 32bit	✓		Malicious activity
04 April 2020, 16:52			Lab06-02.exe PE32 executable (console) intel 80386, for MS Windows
 Windows 7 Professional 32bit	✓		No threats detected
17 November 2019, 19:00			Lab06-02.exe PE32 executable (console) intel 80386, for MS Windows
 Windows 7 Professional 32bit	✓		No threats detected
01 November 2019, 13:32			Lab06-02.exe PE32 executable (console) intel 80386, for MS Windows

Successivamente, inserisco l'hash su **VirusTotal** e scopro che si tratta, molto presumibilmente, di un **Trojan**

39

/ 69

Community Score

39 security vendors and no sandboxes flagged this file as malicious

b71777edbf21167c96d20ff803cbcb25d24b94b3652db2f286dcd6efd3d8416a

40.00 KB

2023-02-14 11:11:24 UTC

Size

1 month ago

Lab06-02.exe

peexe checks-network-adapters runtime-modules armadillo direct-cpu-clock-access

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 6

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.r002c0pdm21

Threat categories trojan

Family labels r002c0pdm21

Security vendors' analysis

Do you want to automate check:

Alibaba	Trojan.Win32/Generic.be125c32	Antiy-AVL	Trojan/Win32.BTSGeneric
Avast	Win32:Trojan-gen	AVG	Win32:Trojan-gen
Avira (no cloud)	HEUR/AGEN.1240704	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.1fef74	Cylance	Unsafe
Cynet	Malicious (score: 100)	DrWeb	Trojan.MulDrop7.63090
Elastic	Malicious (high Confidence)	ESET-NOD32	Win32/Agent.WOO

Elastic	! Malicious (high Confidence)	ESET-NOD32	! Win32/Agent.WOO
F-Secure	! Heuristic.HEUR/AGEN.1240704	Fortinet	! W32/Agent.WOO!tr
GData	! Win32.Trojan.Agent.DZ3C1W	Google	! Detected
Ikarus	! Trojan.Win32.Agent	Lionic	! Trojan.Win32.Generic.4!c
Malwarebytes	! Trojan.Agent.PMA	MAX	! Malware (ai Score=97)
McAfee	! GenericRXAA-AAIC0B54534E188	McAfee-GW-Edition	! Artemis!Trojan
Microsoft	! Trojan:Win32/Ymacro.AAB7	NANO-Antivirus	! Trojan.Win32.Agent.dveq!k
Palo Alto Networks	! Generic.ml	Rising	! Trojan.Agent!8.B!E (TFE:5:W5kRu0pS...
Sangfor Engine Zero	! Trojan.Win32.Agent.Vffk	Symantec	! ML.Attribute.HighConfidence
TACHYON	! Trojan/W32.Agent.40960.ESE	Tencent	! Malware.Win32.Gencirc.115cdf77
Trellix (FireEye)	! Generic.mg.c0b54534e188e139	TrendMicro	! TROJ_GEN.R002C0PDM21
TrendMicro-HouseCall	! TROJ_GEN.R002C0PDM21	VBA32	! Suspected Of Trojan.Downloader.gen
VirIT	! Trojan.Win32.Agent5.CRS	Webroot	! W32.Malware.Heur
Xcitium	! Malware@#13bka6m1o8w1f	Yandex	! Trojan.GenAsa!zclt79pGSs

- Alternativamente, sarebbe stato possibile ricavare l'**MD5** dell'eseguibile direttamente sulla sezione "**Dependency Walker**" di CFF Explorer, per poi inserire l'MD5 su Virustotal. Coincide con l'hash, dunque è inutile cercarlo nuovamente su VirusTotal.

CFF Explorer VIII - [Malware_U3_W2_L5.exe]

Settings ?

File: Malware_U3_W2_L5.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Malware_U3_W2_L5.exe

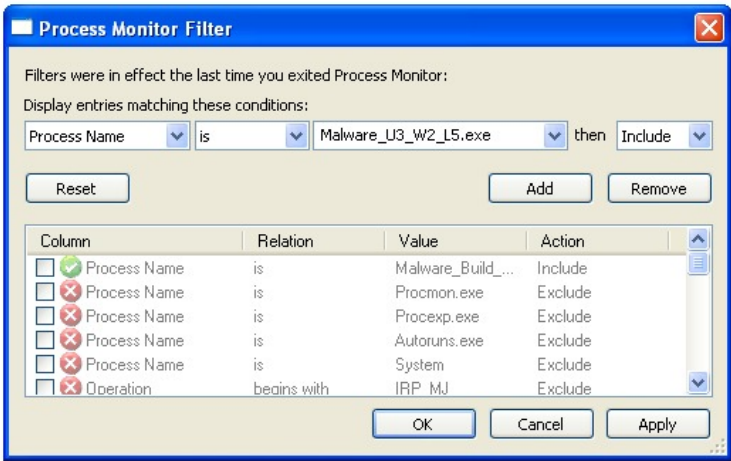
- Malware_U3_W2_L5.exe
 - KERNEL32.dll
 - WININET.dll

Property	Value
File Name	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W...
File Type	Portable Executable 32
File Info	No match found.
File Size	40.00 KB (40960 bytes)
PE Size	40.00 KB (40960 bytes)
Created	Tuesday 16 August 2022, 14.37.31
Modified	Wednesday 02 February 2011, 16.29.05
Accessed	Friday 31 March 2023, 02.32.00
MD5	C0B54534E188E1392F28D17FAFF3D454
SHA-1	BB6F01B1FEF74A9CFC83EC2303D14F492A671F3C

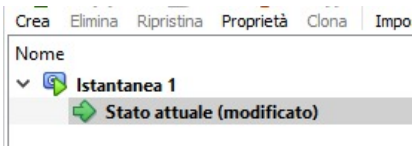
Property	Value
Empty	No additional info available

- Infine, con **Procmon** si può effettuare un'analisi basica dinamica per verificare se le informazioni ricavate fino a questo momento combaciano

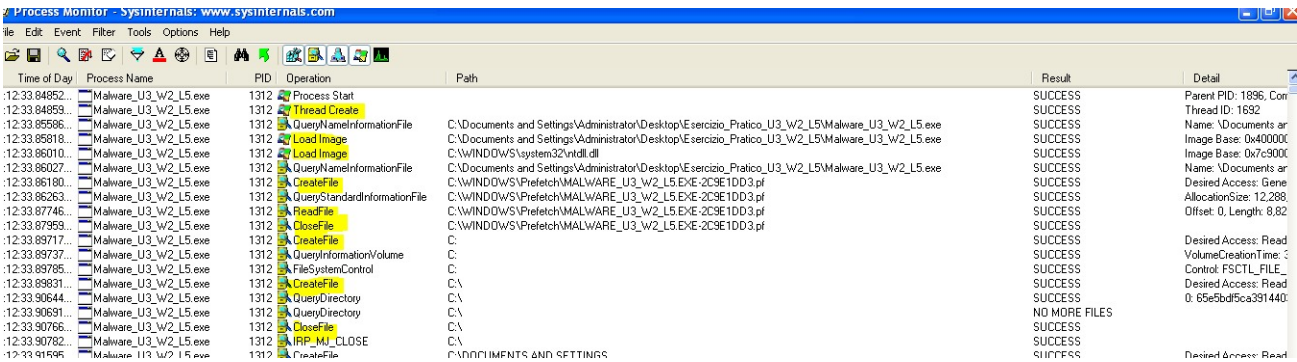
Imposto il filtro



Prima di eseguire il file, mi assicuro che l'ambiente virtuale non comunichi in alcun modo con la macchina host e provvedo a creare un'istantanea sulla macchina virtuale, di modo da poter ripristinare facilmente lo stato della macchina, in caso di danni arrecati dall'esecuzione del malware.



Avvio la detection: dalla comparazione delle operations con i path relativi, il comportamento del Trojan sarà più chiaro.



Le azioni osservate (l'apertura, lettura e scrittura di file; la creazione di mappature di file; l'accesso al Registro di sistema; il caricamento di immagini) sono spesso associate ai **Trojan di accesso remoto (RAT)** o ai **Trojan di furto di informazioni**, che cercano di accedere ai dati del sistema e rubare informazioni sensibili come credenziali di accesso e informazioni personali.

Inoltre, il fatto che il Trojan esegua queste operazioni in modo continuo suggerisce che stia cercando di rimanere attivo sul sistema per il maggior tempo possibile e forse tentando di evitare la rilevazione da parte dei software di sicurezza.

- Ulteriori tool utili per analizzare il comportamento del malware sono:
 1. **Process Explorer**, utile per vedere quali processi sono stati creati o terminati dal malware
 2. **RegShot**, per comparare le chiavi di registro prima e dopo l'esecuzione del malware.
 3. **ApateDNS**, per simulare un server DNS ed intercettare le richieste dal malware ai domini Internet
 4. **Wireshark**, per monitorare tutto il traffico di rete generato dal malware, sia verso Internet, sia, eventualmente, verso la rete interna