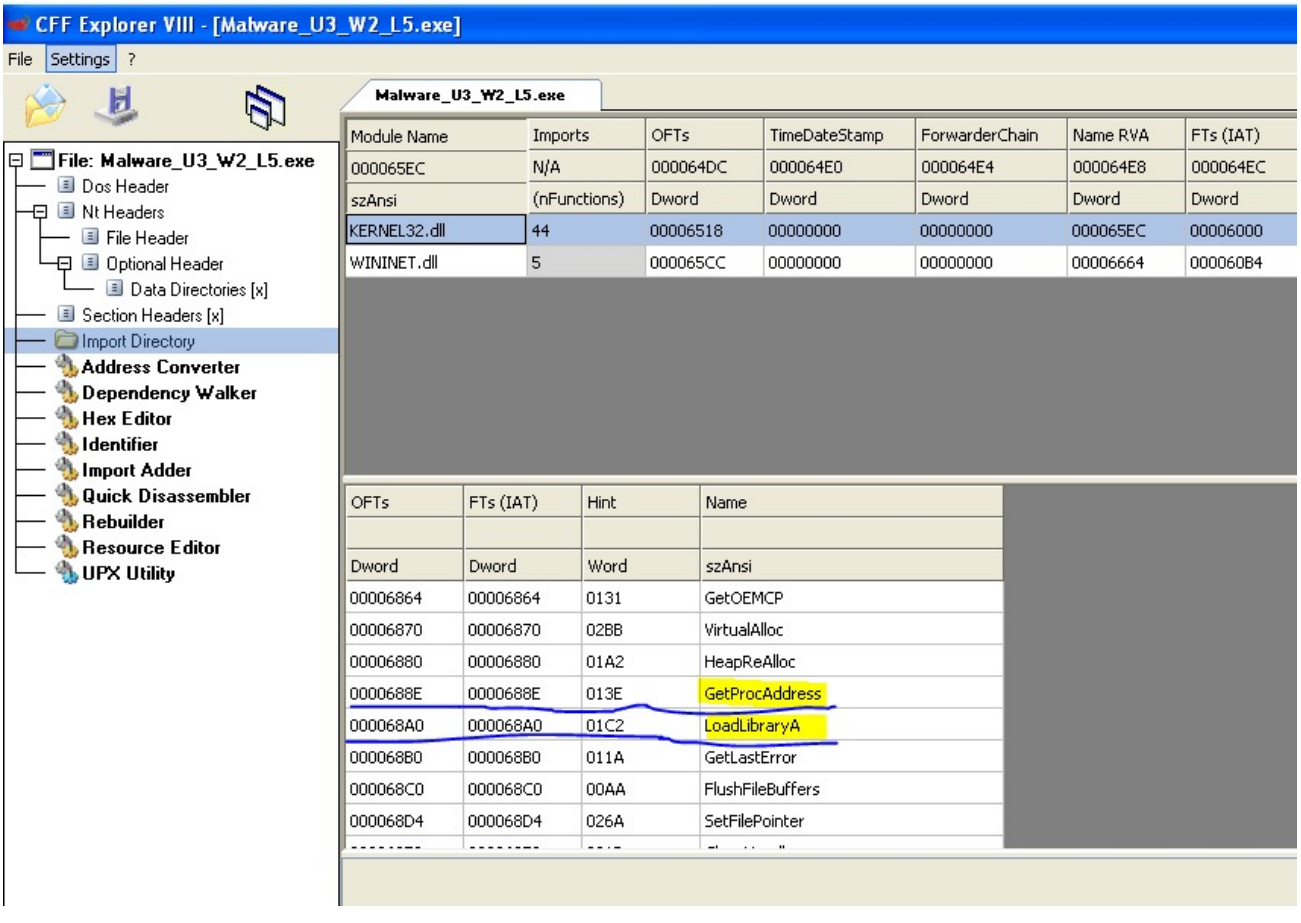
Progetto Week 10 - Fundamentals of Malware Analysis and reverse engineering

- **Librerie importate**

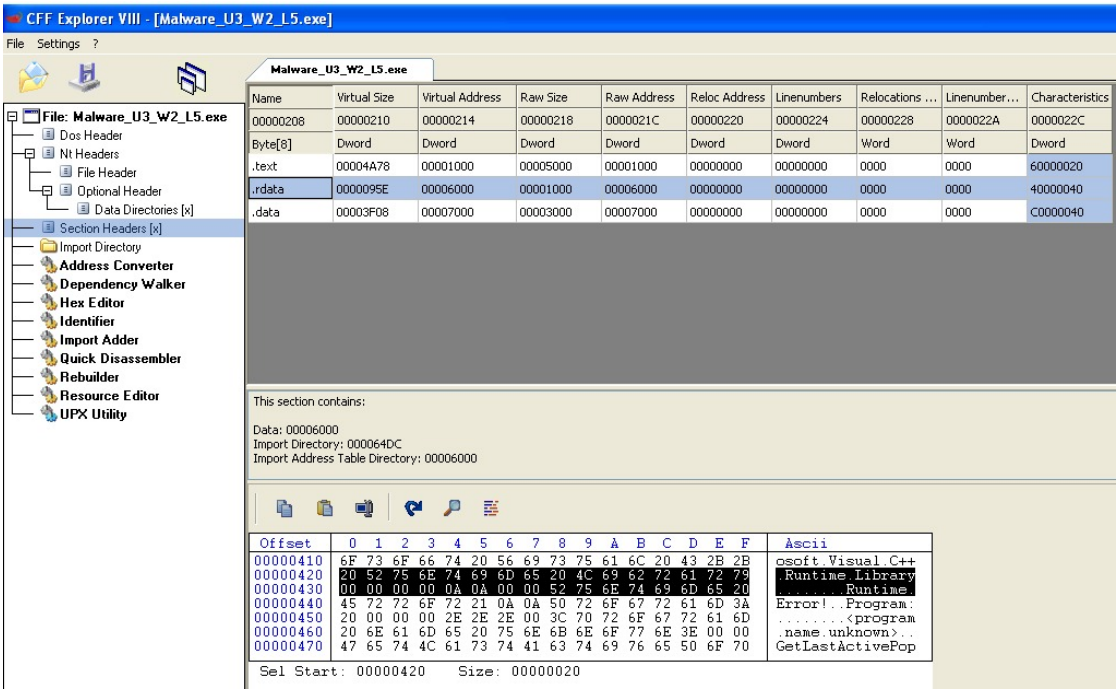
Possiamo verificare quali sono le librerie importate dal file eseguibile utilizzando CFF Explorer e selezionando **"import directory"**. Come possiamo vedere nella figura di seguito, le librerie importate sono due:
KERNEL32.dll, che contiene le funzioni principali per interagire con il sistema operativo (gestione file, memoria...)
WININET.dll, che contiene le funzioni di implementazione dei protocolli di rete (http, ftp, ntp...)



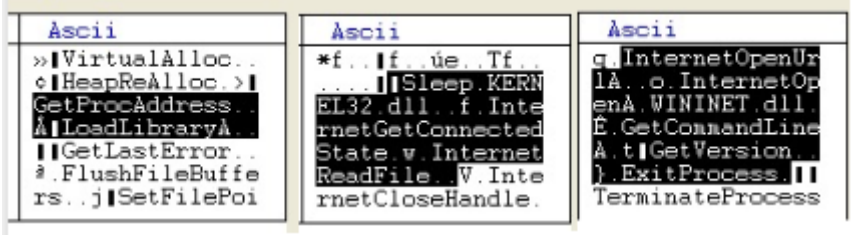
Analizzando le informazioni della libreria Kernel, possiamo notare la presenza di funzioni quali **"GetProcAddress"** e **"LoadLibraryA"**. Ciò ci fornisce una prima informazione sul malware: i**mporta le librerie "Runtime"** (ovvero, a tempo di esecuzione e, quindi, solo in caso di bisogno), nascondendo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

- **Sezioni del file eseguibile**

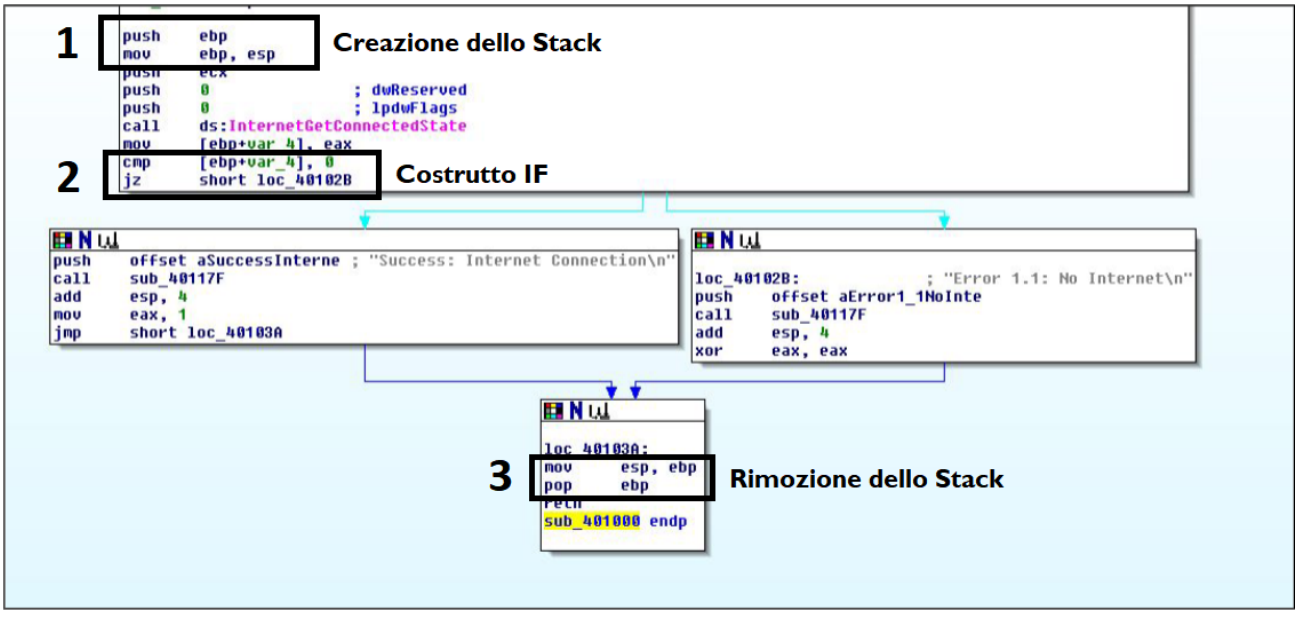
Continuando ad utilizzare il tool CFF Explorer, è possibile spostarsi su **"Section Headers"**. Il file ha 3 sezioni:
.text , che contiene le istruzioni che la CPU eseguirà all'avvio del software
.rdata , che contiene informazioni sulle librerie e sulle funzioni importate/esportate
.data , che contiene 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

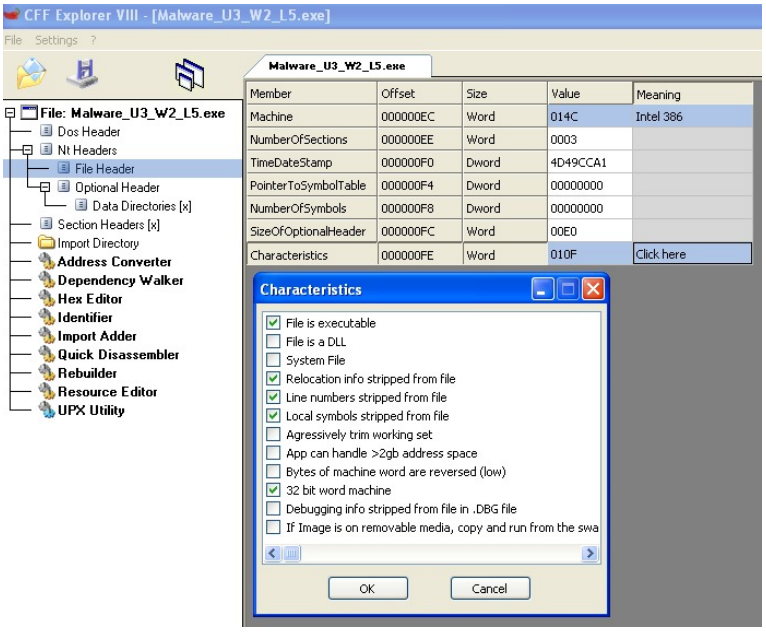


- Ipotesi del comportamento della funzionalità implementata

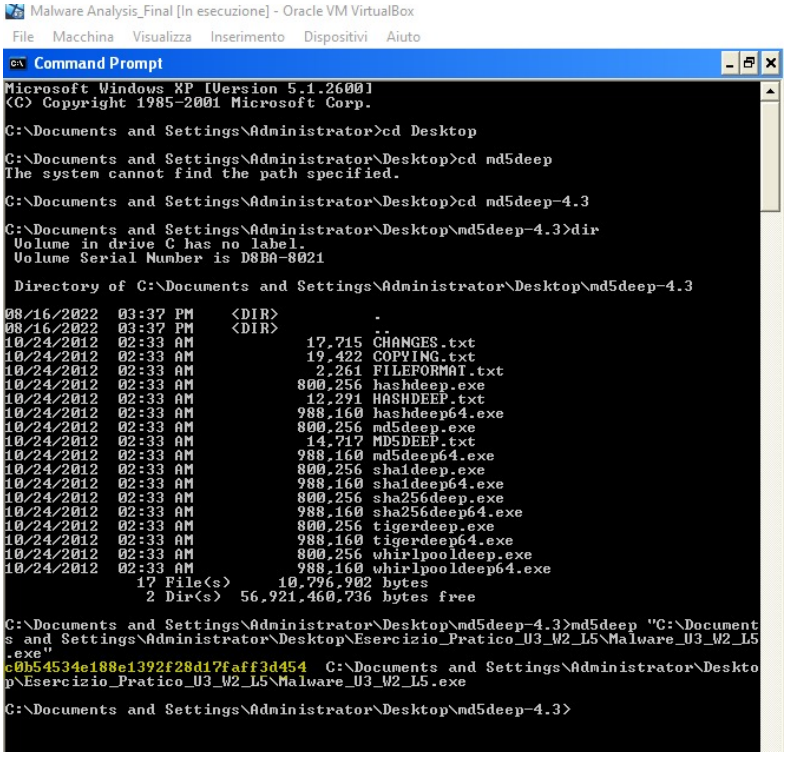
Dopo aver creato lo stack, il codice istruisce di eseguire un check di connessione, per verificare se la macchina è connessa o meno ad Internet.
-Se il parametro restituito da "InternetgetConnectedState" ≠ 0, la funzione stamperà a schermo un messaggio di successo: "Success: Internet Connection"
-Se 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



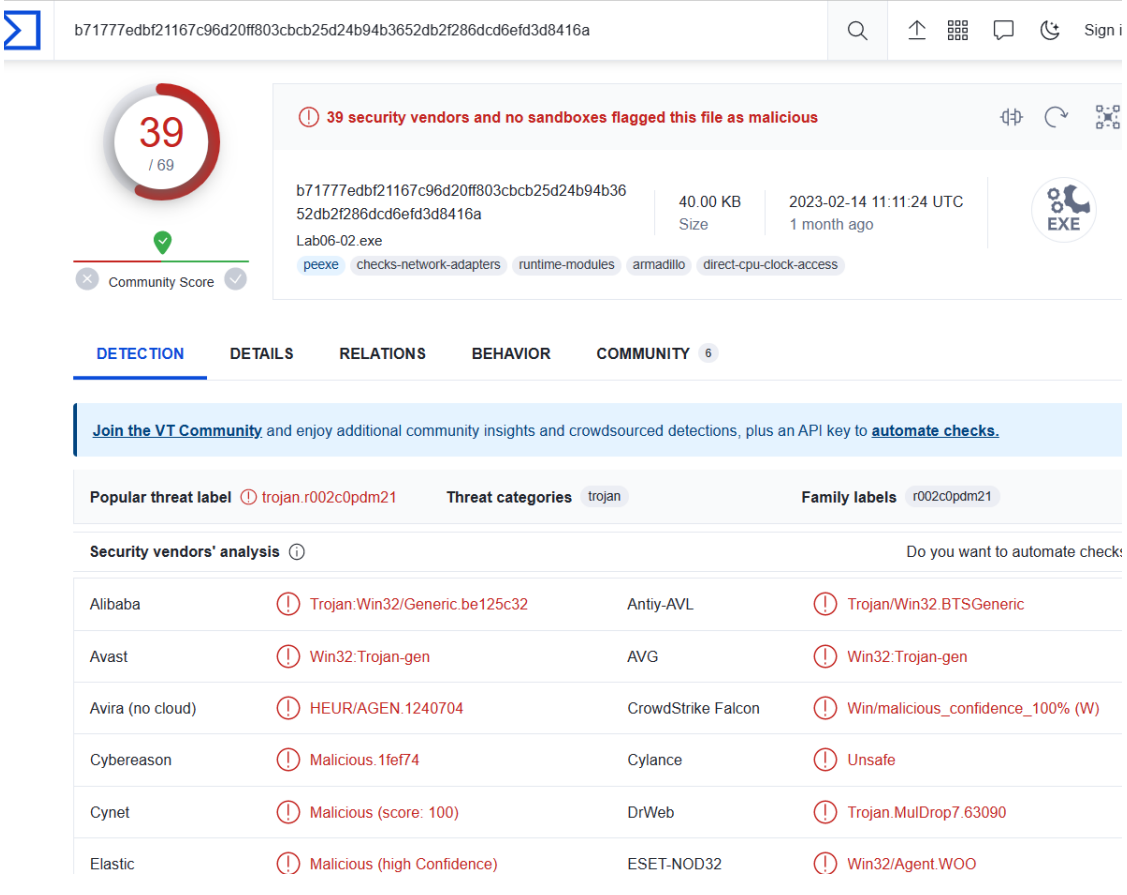
- Utilizzando **md5deep** posso calcolare l'hash dell'eseguibile e usare lo stesso per ottenere, anzitutto, la conferma che si tratti di un malware e, auspicabilmente, maggiori informazioni sul comportamento dello stesso.



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

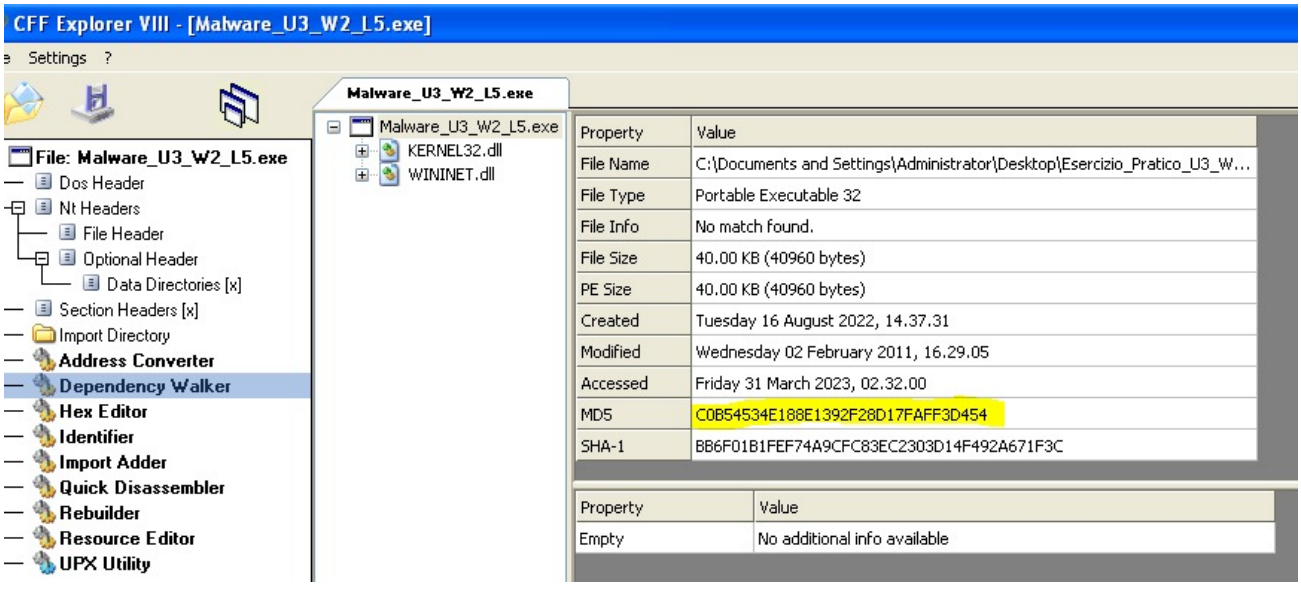
Inserendo l'hash in analisi in "**anyrun**", 2 risultati su 10 lo identificano come un malware: un risultato non molto soddisfacente.

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



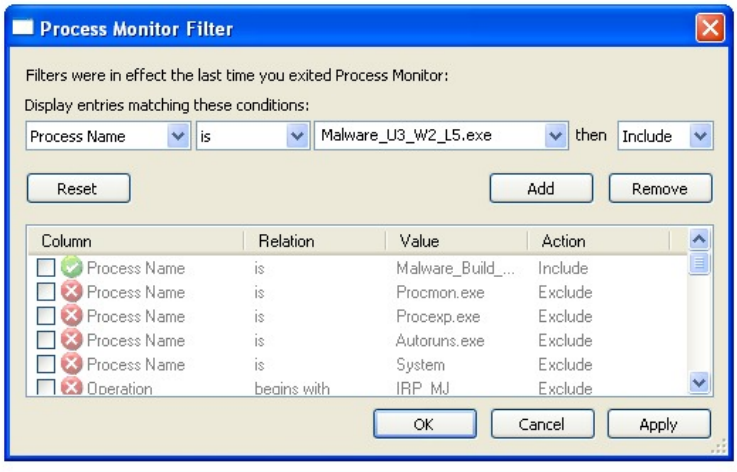
Elastic	Malicious (high Confidence)	ESET-NOD32	Win32/Agent.WOO
F-Secure	Heuristic.HEUR/AGEN.1240704	Fortinet	W32/Agent.WOO!tr
GData	Win32.Trojan.Agent.DZ3C1W	Google	Detected
Ikarus	Trojan.Win32.Agent	Lionic	Trojan.Win32.Generic.4!c
Malwarebytes	Trojan.Agent.PMA	MAX	Malware (ai Score=97)
McAfee	GenericRXAA-AAIC0B54534E188	McAfee-GW-Edition	Artemis!Trojan
Microsoft	Trojan:Win32/Ymacco.AAB7	NANO-Antivirus	Trojan.Win32.Agent.dveqxk
Palo Alto Networks	Generic.ml	Rising	Trojan.Agentt!8.B1E (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.GenAsaIzc/tt79pGSs

- 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.

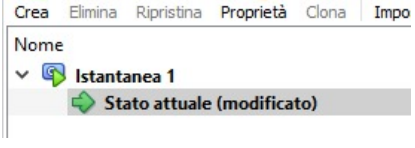


- Infine, con **Procmon** si puo effettuare un'analisi basica dinamica per verificare se le informazioni ricavate fino a questo momento combaciano

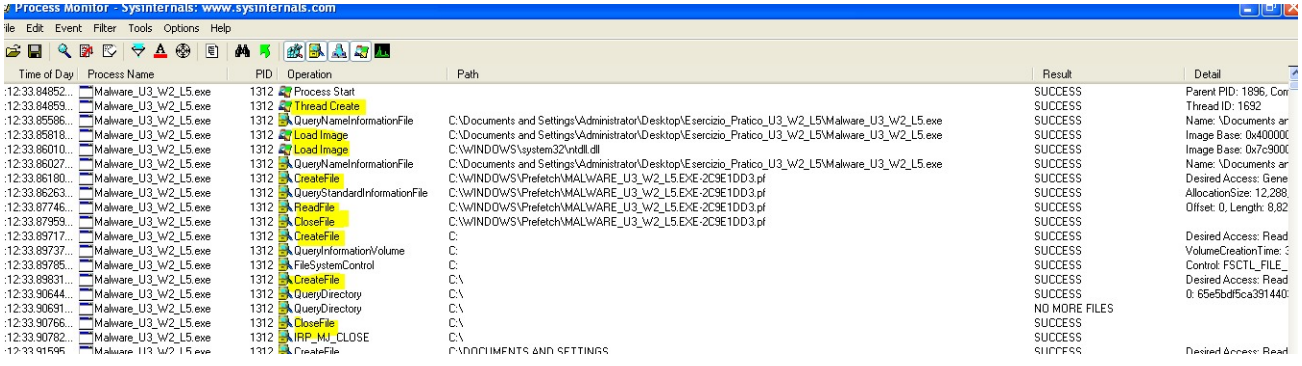
  Imposto il filtro



  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 piu 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