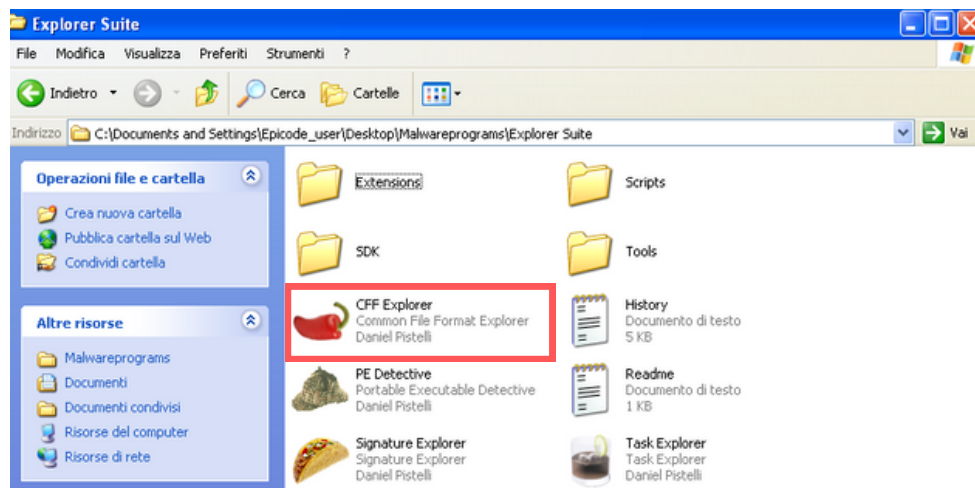


Malware analysis

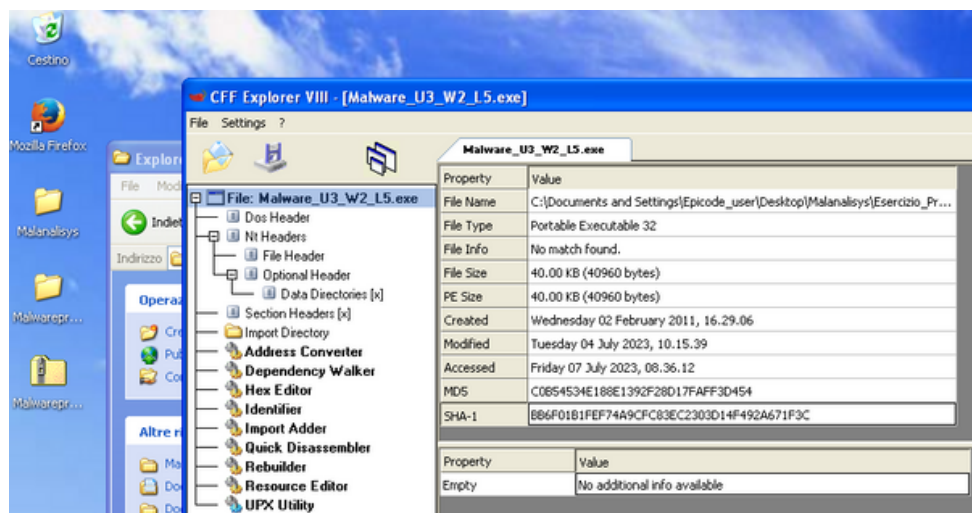
Esercizio 1

Librerie importate dal file .exe "Esercizio_pratico_U3_W2_L5"

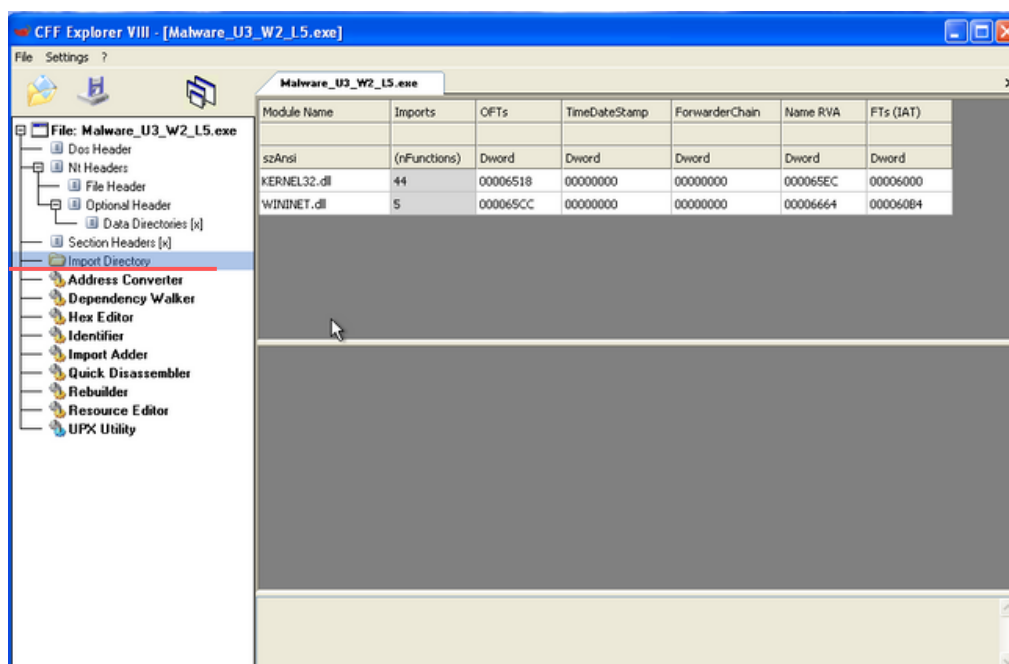
Per avviare l'analisi statica basica uso il tool **CFF EXPLORER**



Una volta aperto il tool vado a caricare al suo interno "Esercizio_pratico_U3_W2_L5.exe", dove nella schermata iniziale vengono riportate varie informazioni tra cui la data di creazione, l'hash ecc.



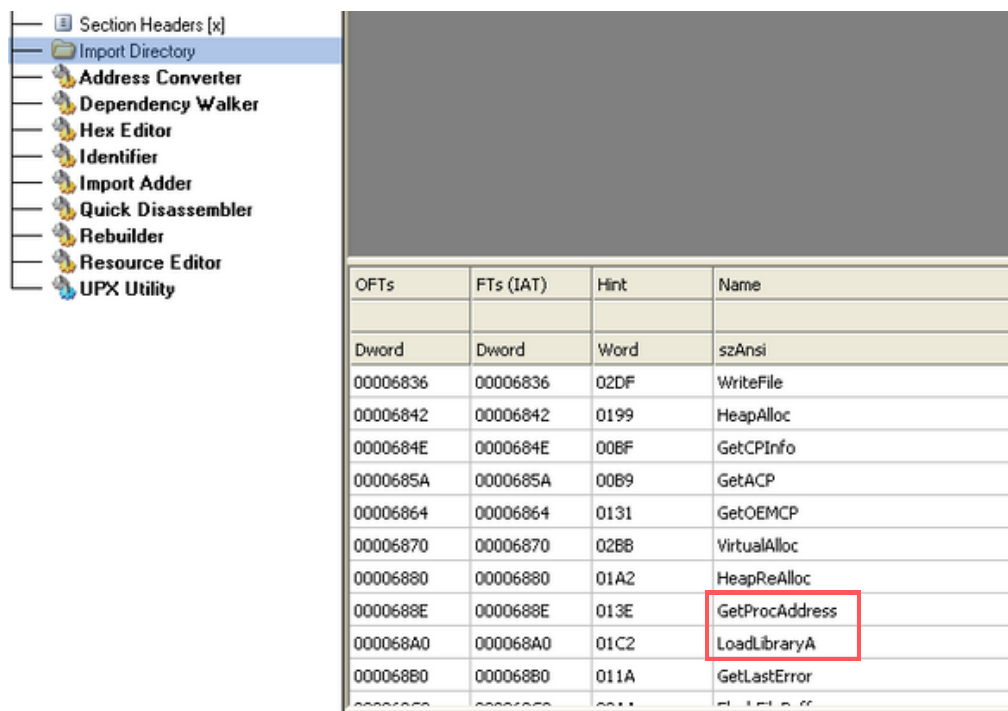
Per controllare le librerie caricate mi sposto su import directory



In questa sezione possiamo notare che sono caricate due librerie ovvero:

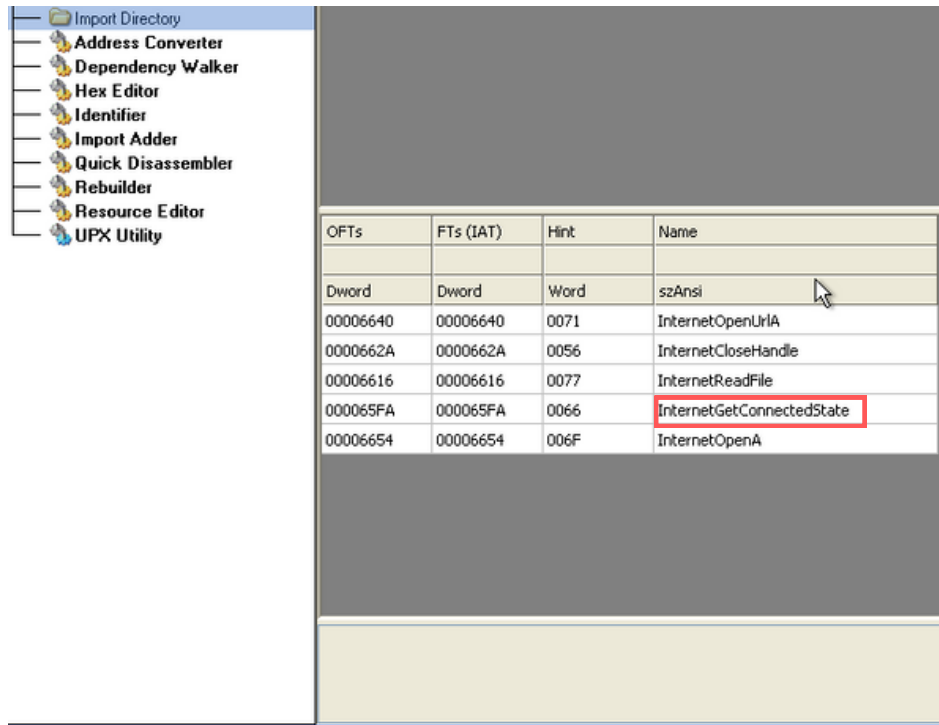
- **KERNEL32.DLL**: contiene funzioni principali per interagire con il sistema operativo
- **WININET.DLL**: contiene delle funzioni per alcuni protocolli di rete come HTTP FTP NTP

Selezionando la libreria **kernel32.dll** possiamo notare che importa LoadlibraryA e GetProcAddress



La funzione **LoadLibraryA** e la funzione **GetProcAddress** sono utilizzate a tempo di esecuzione (runtime). L'eseguibile richiama la libreria solo quando ha bisogno di utilizzare una specifica funzione, durante l'esecuzione del file. Questo comportamento è ampiamente analizzato da malware che, allo stesso modo, chiamano una determinata funzione solo quando necessario per risultare meno invasivi e rilevabili possibile.

Selezionando la libreria **Wininet.dll** possiamo notare che importa **InternetGetConnectedState**

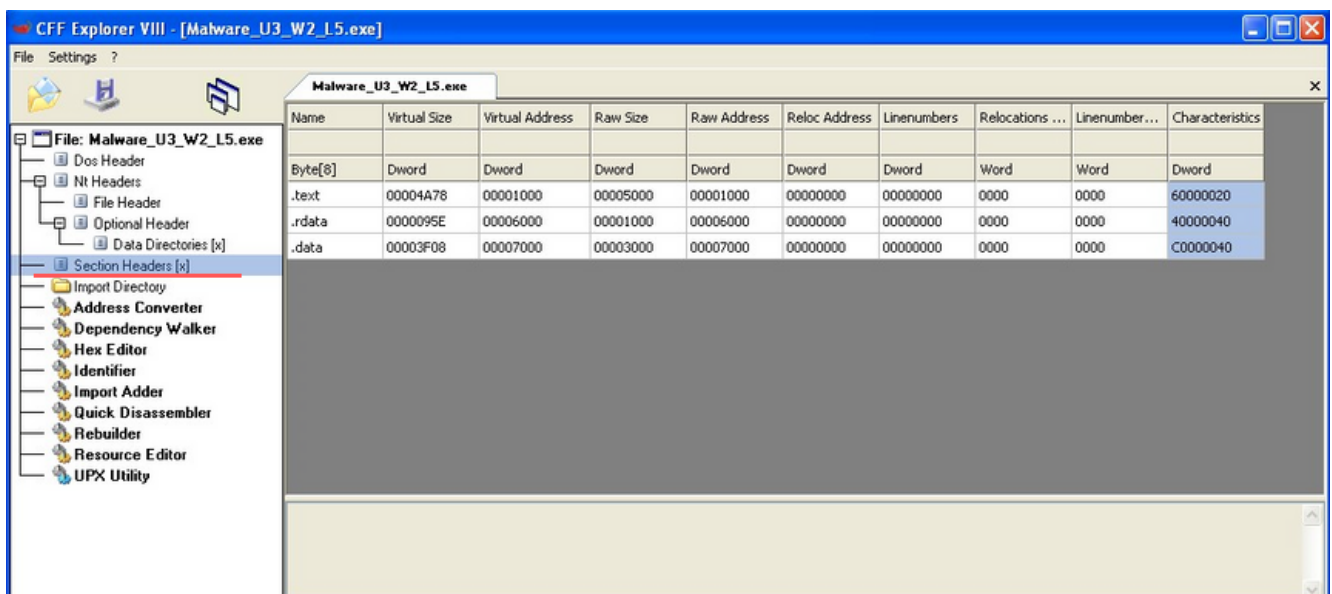


InternetGetConnectedState: Verifica se una macchina ha accesso ad internet.

Esercizio 2

Sezioni del file .exe "Esercizio_pratico_U3_W2_L5"

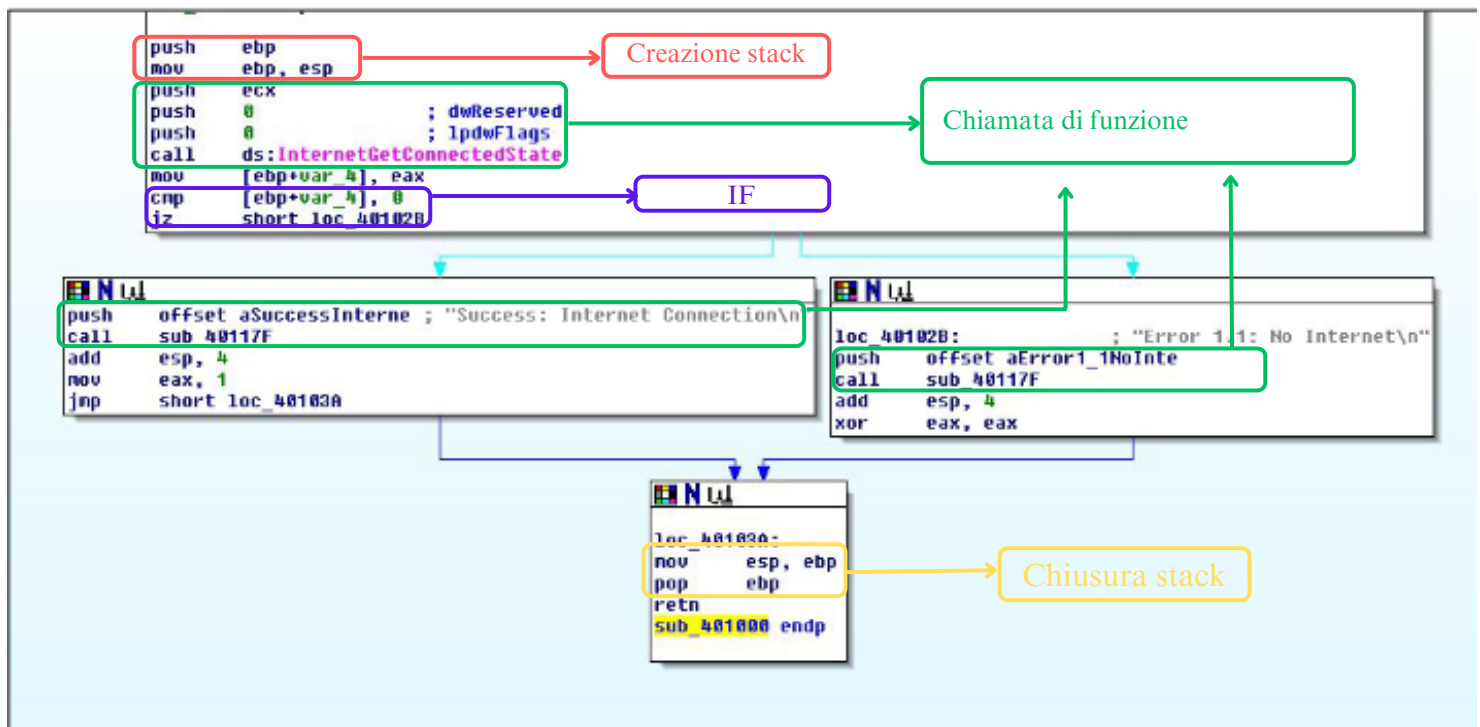
Utilizzando sempre **CFF EXPLORER** mi sposto nella sezione Headers dove trovo le seguenti sezioni



- **.text:** contiene le istruzioni che la CPU esegue una volta che il software verrà avviato.
- **.rdata:** contiene informazioni sulle librerie e le funzioni importate ed esportate dall'eseguibile
- **.data:** contiene variabili globali del programma .exe, che devono essere disponibili da qualsiasi parte del programma

Esercizio 3

Identificazione dei costrutti noti



Esercizio 4

Ipotesi del comportamento

Inizialmente il programma crea uno stack per le variabili locali.

Ci sono due puntatori: **EBP** (Extended Base Pointer) dove punta alla base dello stack ed **ESP** (Extended Stack Pointer) che punta alla cima dello stack.

Successivamente attraverso la funzione `InternetGetConnectedState` verifica se la macchina ha accesso ad internet.

Con l'IF presumo che il software stamperà a schermo un messaggio dello stato di connessione.

Se è presente una connessione internet, il programma andrà avanti e aumenterà il valore dello stack (`add esp, 4`) ovvero, aggiunge 4 al registro ESP (Stack Pointer), spostandosi di 4 byte.

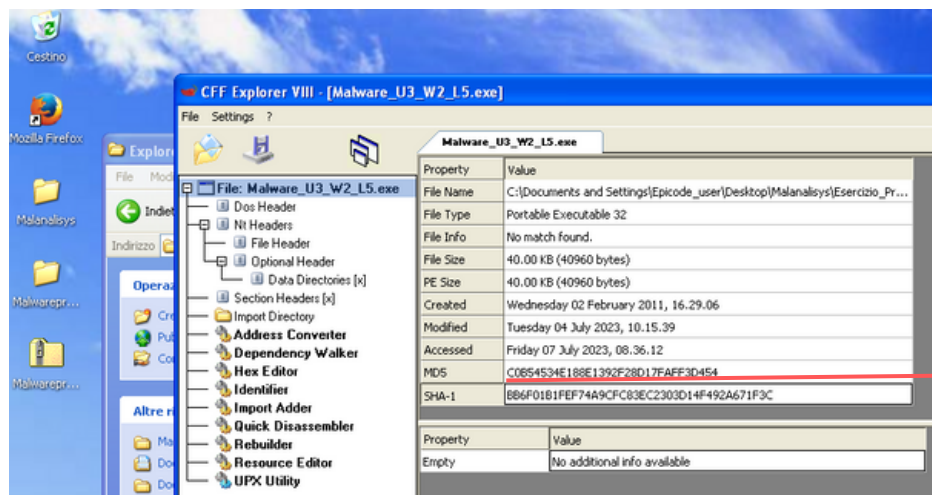
In caso di mancata connessione ad Internet, viene reinizializzato a 0 il valore del registro `eax` (`xor eax, eax`).

In conclusione il malware, se ha una connessione ad internet può avere molteplici funzionalità come:

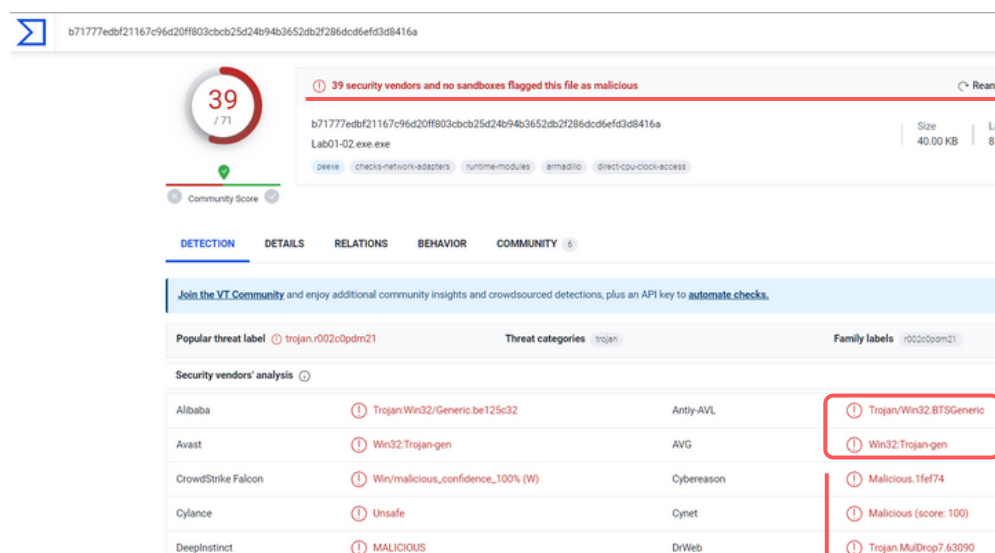
- Una Backdoor
- Download di file verso server web
- Upload di file malevoli

Di conseguenza potremmo essere di fronte ad un trojan, downloader o una backdoor

Per confermare la mia ipotesi inserisco l'hash dato da CFF EXPLORER su Virus Total



Preso l'hash da CFF EXPLORER lo inserisco su Virus Total.



39 vendors ci segnalano che il software è malevolo

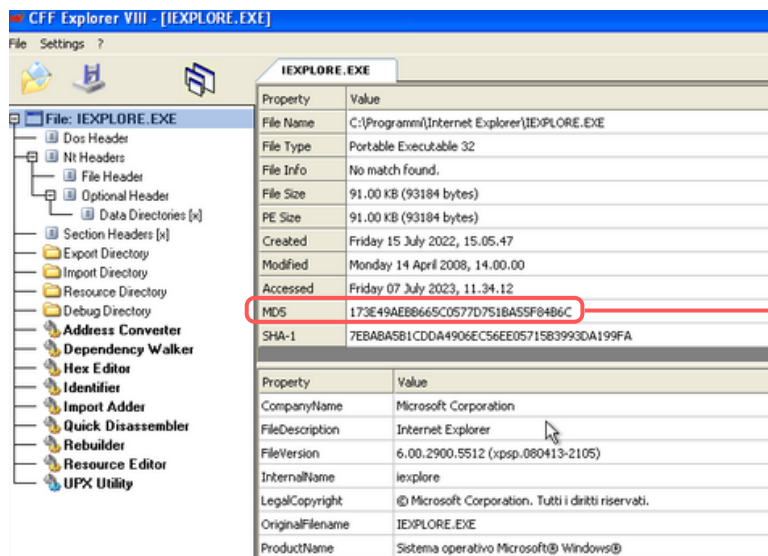
Segnalato come un Trojan

<https://www.virustotal.com/gui/file/b71777edbf21167c96d20ff803cbcb25d24b94b3652db2f286dcd6efd3d8416a>

Esercizio 5

Valutazione del file eseguibile IEXPLORE

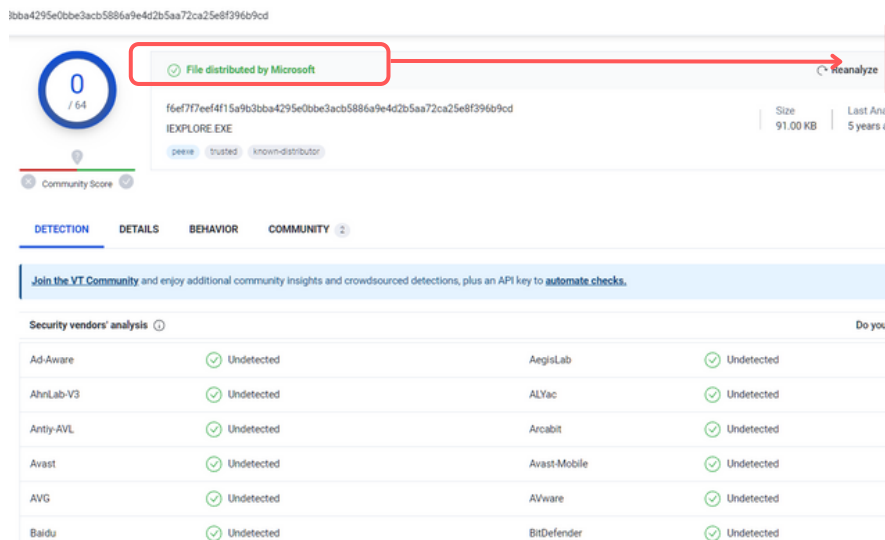
Inizialmente apro il file su CFF EXPLORER dove posso leggere l'hash e confrontarlo su virus total



Preso l'hash da ECC EXPLORER lo inserisco su Virus Total.

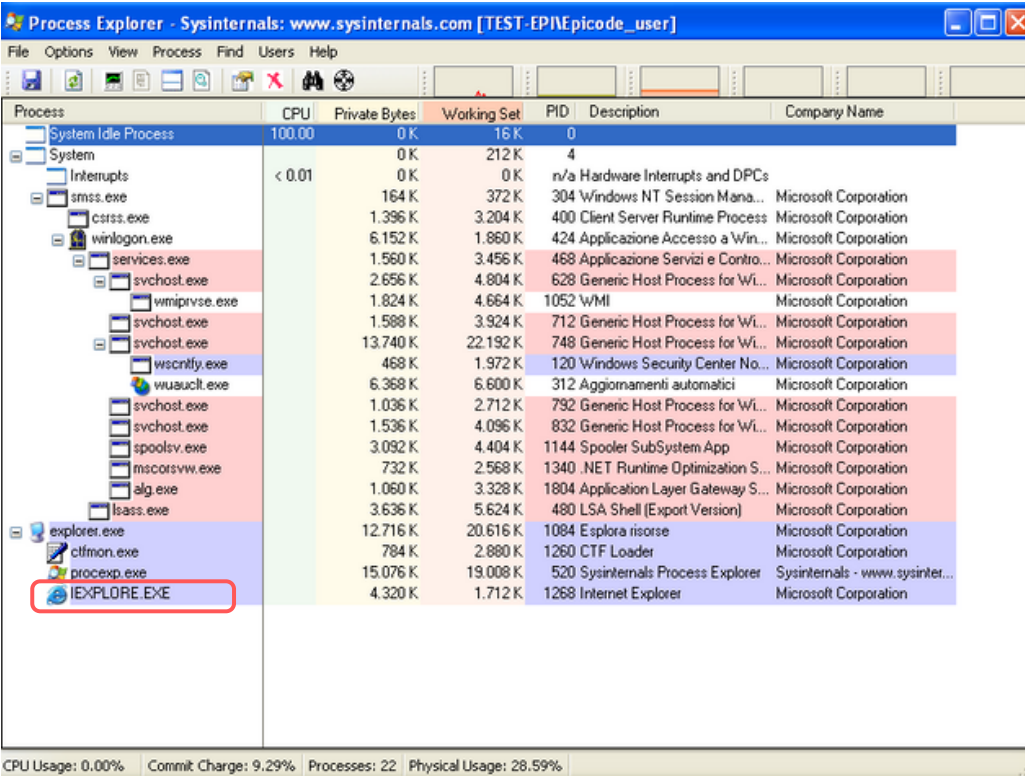
Come si può notare nessuno lo ha segnalato come software malevolo.

In più Virus Total conferma che il file è distribuito da Microsoft.



<https://www.virustotal.com/gui/file/f6ef7f7eef4f15a9b3bba4295e0bbe3acb5886a9e4d2b5aa72ca25e8f396b9cd>

Avvio Process Explorer che da in output un'analisi dettagliata di tutti i processi in esecuzione

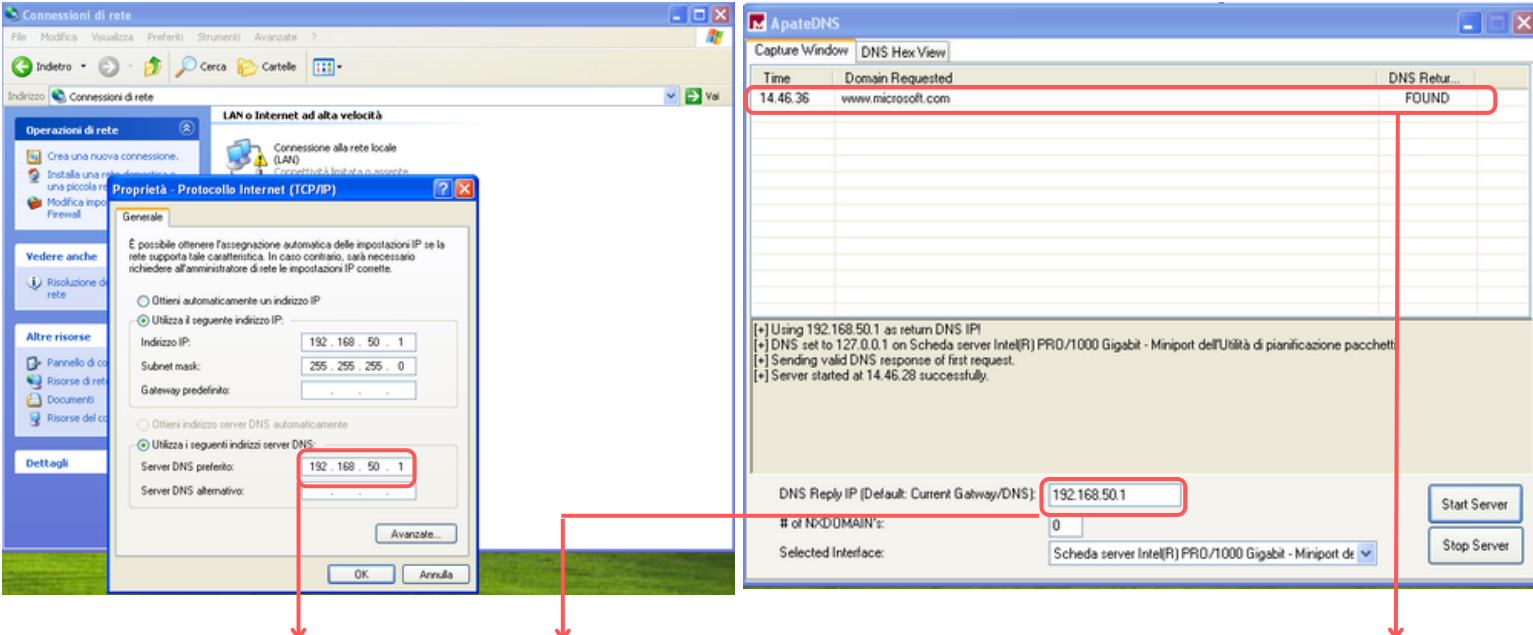


Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	100.00	0 K	16 K	0		
System		0 K	212 K	4		
Interrupts	< 0.01	0 K	0 K		n/a Hardware Interrupts and DPCs	
smss.exe		164 K	372 K	304	Windows NT Session Mana...	Microsoft Corporation
csrss.exe		1.396 K	3.204 K	400	Client Server Runtime Process	Microsoft Corporation
winlogon.exe		6.152 K	1.860 K	424	Applicazione Accesso a Win...	Microsoft Corporation
services.exe		1.560 K	3.456 K	468	Applicazione Servizi e Contro...	Microsoft Corporation
svchost.exe		2.656 K	4.804 K	628	Generic Host Process for Wl...	Microsoft Corporation
wmiiprvse.exe		1.824 K	4.664 K	1052	WMI	Microsoft Corporation
svchost.exe		1.588 K	3.924 K	712	Generic Host Process for Wl...	Microsoft Corporation
svchost.exe		13.740 K	22.192 K	748	Generic Host Process for Wl...	Microsoft Corporation
wscntfy.exe		468 K	1.972 K	120	Windows Security Center No...	Microsoft Corporation
wuauclt.exe		6.368 K	6.600 K	312	Aggiornamenti automatici	Microsoft Corporation
svchost.exe		1.036 K	2.712 K	792	Generic Host Process for Wl...	Microsoft Corporation
svchost.exe		1.536 K	4.096 K	832	Generic Host Process for Wl...	Microsoft Corporation
spoolsv.exe		3.092 K	4.404 K	1144	Spooler SubSystem App	Microsoft Corporation
mscorsvw.exe		732 K	2.568 K	1340	.NET Runtime Optimization S...	Microsoft Corporation
alg.exe		1.060 K	3.328 K	1804	Application Layer Gateway S...	Microsoft Corporation
lsass.exe		3.636 K	5.624 K	480	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe		12.716 K	20.616 K	1084	Esplora risorse	Microsoft Corporation
ctfmon.exe		784 K	2.880 K	1260	CTF Loader	Microsoft Corporation
processp.exe		15.076 K	19.008 K	520	Sysinternals Process Explorer	Sysinternals - www.sysinter...
IEXPLORE.EXE		4.320 K	1.712 K	1268	Internet Explorer	Microsoft Corporation

CPU Usage: 0.00% Commit Charge: 9.29% Processes: 22 Physical Usage: 28.59%

Come possiamo notare nella figura precedente avviando IEXPLORE.EXE avvia solo quel processo e nient'altro che potrebbe essere malevolo

Avvio ApateDNS per simulare un server e può intercettare le richieste de malware effettuate su domini internet



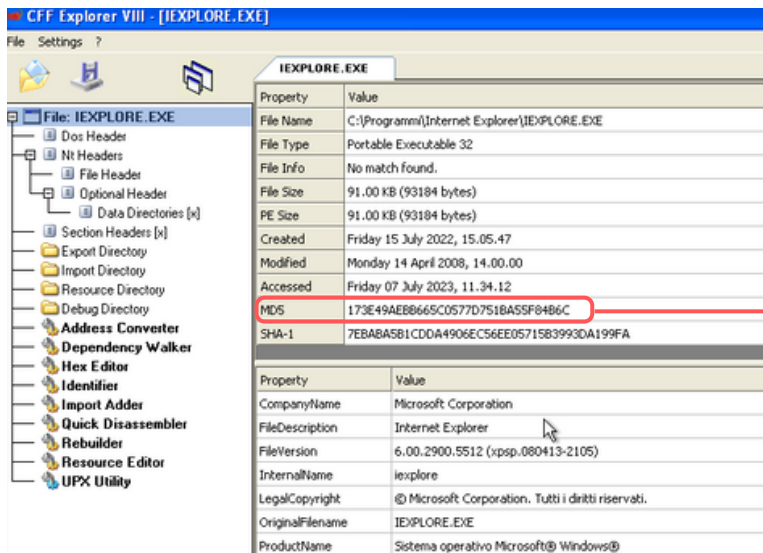
The left screenshot shows the 'Internet Protocol (TCP/IP)' properties window. The 'General' tab is selected, and the 'Obtain an IP address automatically' option is chosen. The 'Obtain DNS server address automatically' option is also selected. The IP address is 192.168.50.1 and the DNS server is 192.168.50.1.

The right screenshot shows the ApateDNS interface. The 'Capture Window' tab is selected, and a DNS request for 'www.microsoft.com' is captured at 14.46.36. The 'DNS Reply IP' is set to 192.168.50.1. The 'Start Server' button is visible.

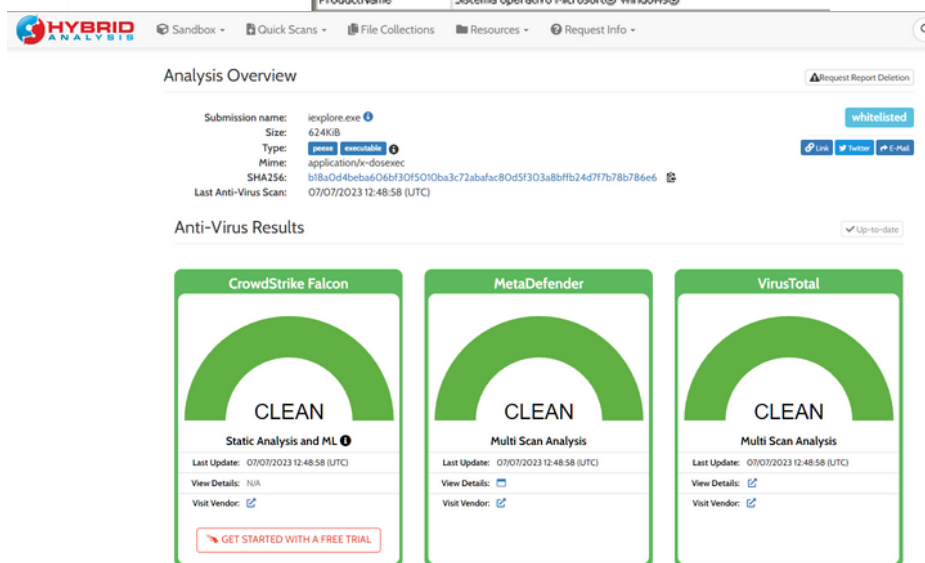
Configuro il server DNS impostandolo al seguente indirizzo ip: 192.168.50.1

Aprendo IEXPLORE.EXE Possiamo notare che non fa nessuna richiesta anomala

Infine come ultima verifica utilizzo **hybrid analysis**



Preso l'hash da CFF EXPLORER lo inserisco su hybrid analysis.



Anche hybrid analysis ci conferma la sicurezza del file eseguibile

<https://www.hybrid-analysis.com/sample/b18a0d4beba606bf30f5010ba3c72abafac80d5f303a8bffb24d7f7b78b786e6>

In conclusione dico al neo dipendente del reparto tecnico che non è un file malevolo e può utilizzarlo tranquillamente