

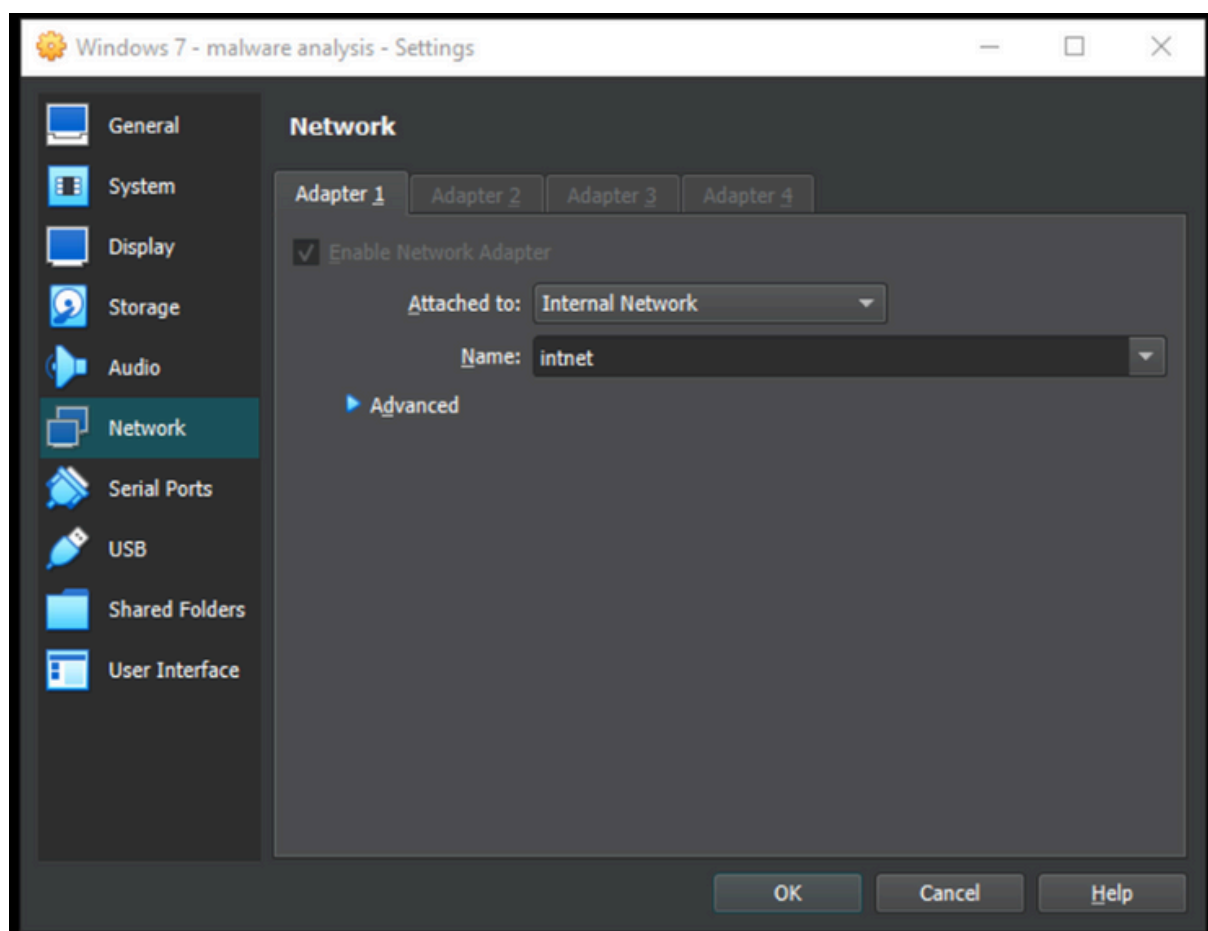
Ambiente di lavoro

Prima di iniziare ad analizzare i malware dobbiamo spostarci in un ambiente protetto.

La prima cosa da fare, per evitare una diffusione accidentale del malware e garantire la sicurezza della rete, è isolarci dalla stessa.

Proseguiamo, quindi, spostandoci in intranet, distaccandoci dalla rete “main” e prevenendo, così, una diffusione accidentale ad altri device.

Queste precauzioni sono necessarie soprattutto quando bisogna eseguire un’analisi statica prima ed una dinamica dopo (l’esercizio richiede solo l’analisi statica ma è buona prassi effettuare tutti gli step).

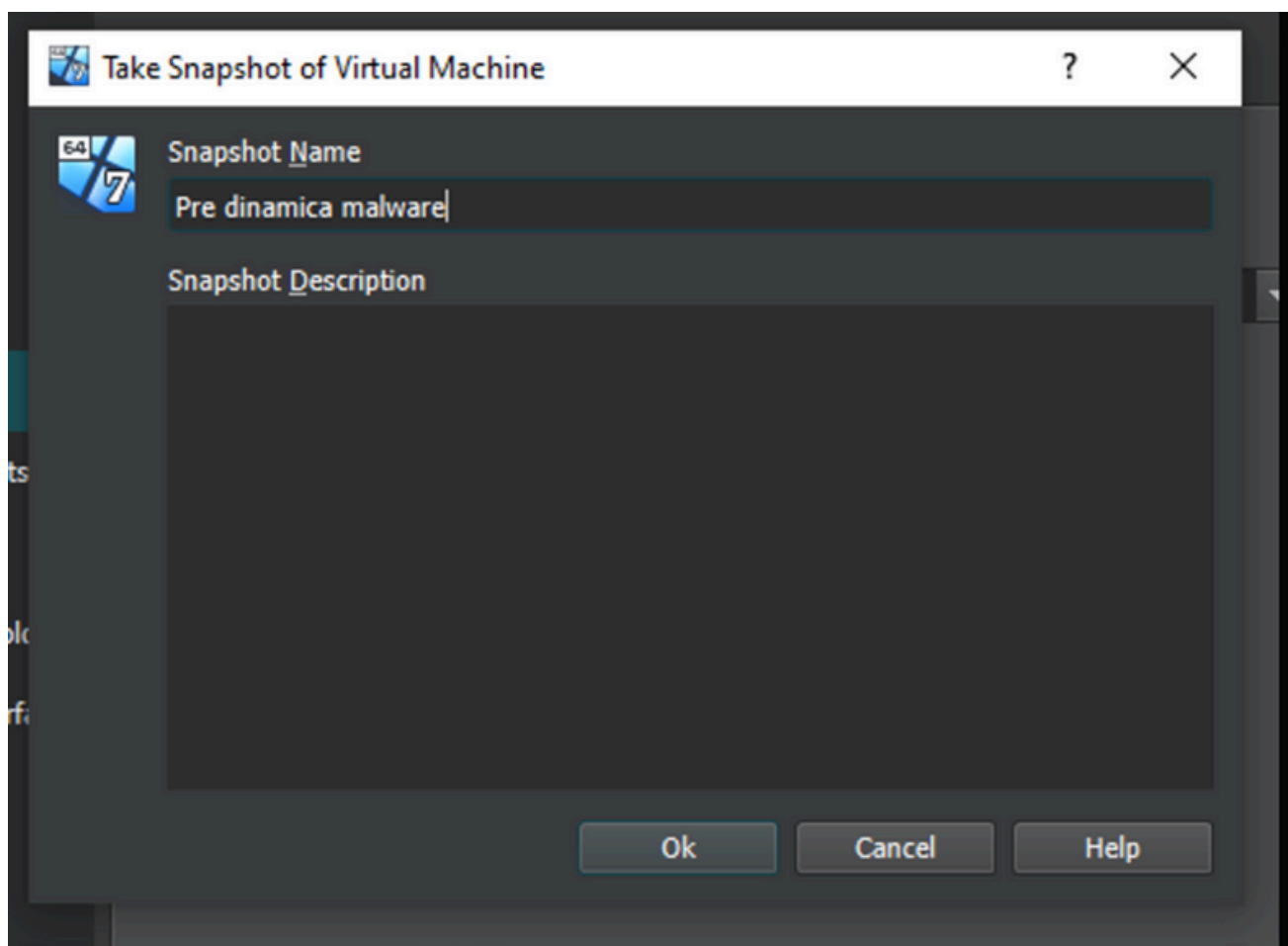


S10-L5 Analisi Malware

Emulo Francesco

La scelta, invece, di utilizzare una VM per l'analisi è doverosa in quanto, in questo modo, evitiamo eventuali danni al device host.

Le virtual machine, inoltre, offrono la possibilità di effettuare delle istantanee (o snapshot), delle specie di punti di ripristino (o check-point) a cui poter ritornare una volta terminata l'analisi del malware in questione.



NB: Rientra nelle buone pratiche anche la disattivazione dei controller USB (alcuni malware possono utilizzare un dispositivo USB per propagarsi sull'host); e la rimozione delle cartelle condivise (stesso discorso, l'obiettivo è quello di confinarlo nel nostro laboratorio).

S10-L5 Analisi Malware

Emulo Francesco

Strumenti utili all'analisi statica

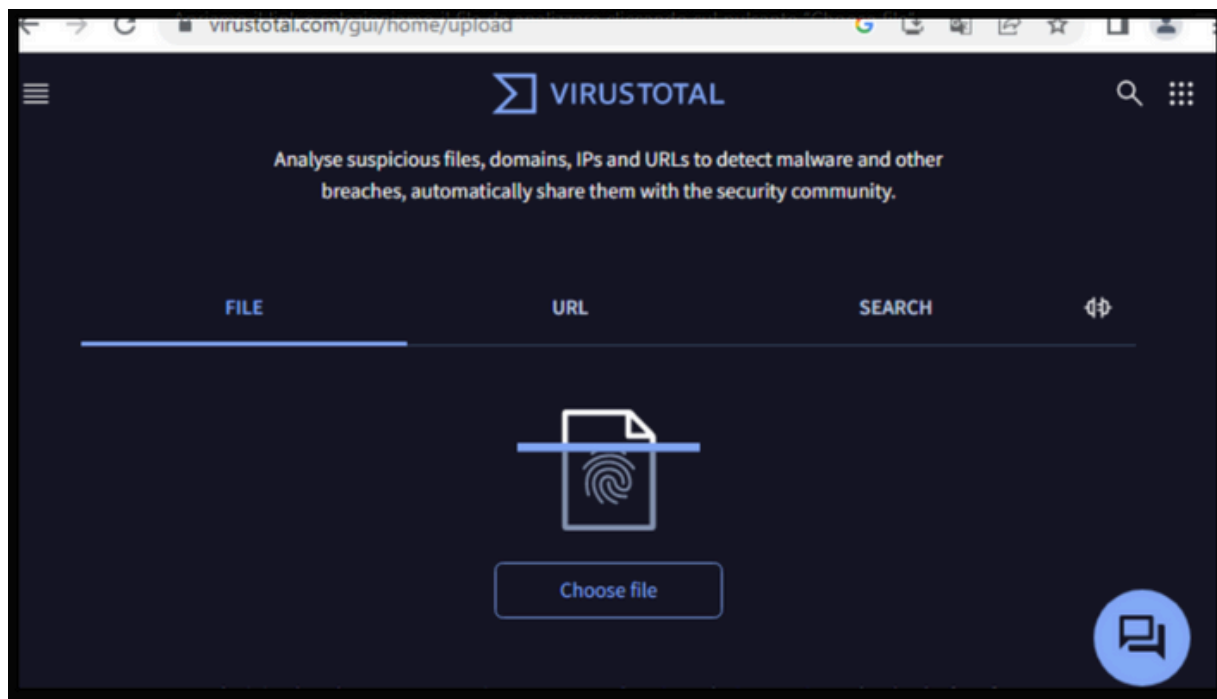
Dal momento che l'analisi statica non richiede il lancio del malware, durante questa analisi possiamo essere connessi alla rete (tool come virus total richiedono tale configurazione).

Per l'analisi statica utilizzeremo i seguenti tool:

- Virus Total
- CFF Explorer
- PE Explorer

Virus Total

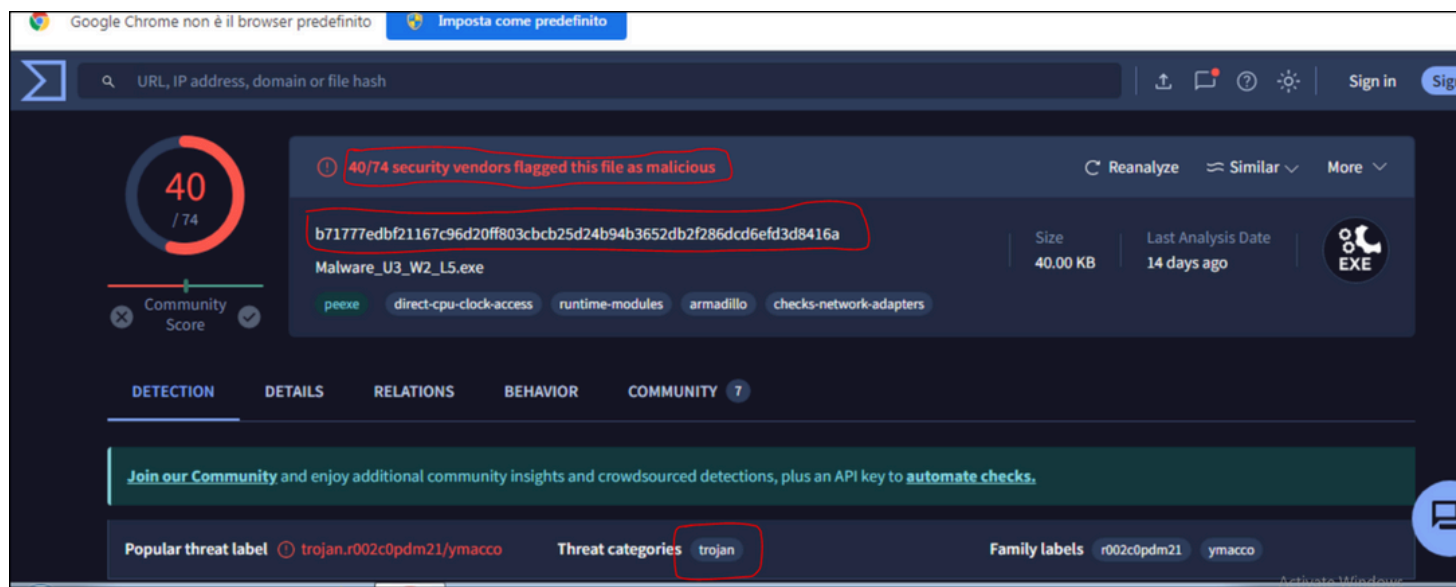
Andiamo sul nostro motore di ricerca e cerchiamo VirusTotal. Apriamo il link e selezioniamo il file da analizzare cliccando sul pulsante "Choose file".



S10-L5 Analisi Malware

Emulo Francesco

I risultati dell'analisi ci danno diverse informazioni importanti:



Il primo elemento cerchiato indica quanti vendors hanno flaggato questo exe come malware.

Il secondo elemento cerchiato è l'Hash (in SHA-256) utile ad identificare in modo univoco tale file (utile per permetterne il confronto con i file nel database e vedere se, eventualmente, sia già stato identificato come malware).

Il terzo elemento, infine, categorizza tale malware come Trojan.

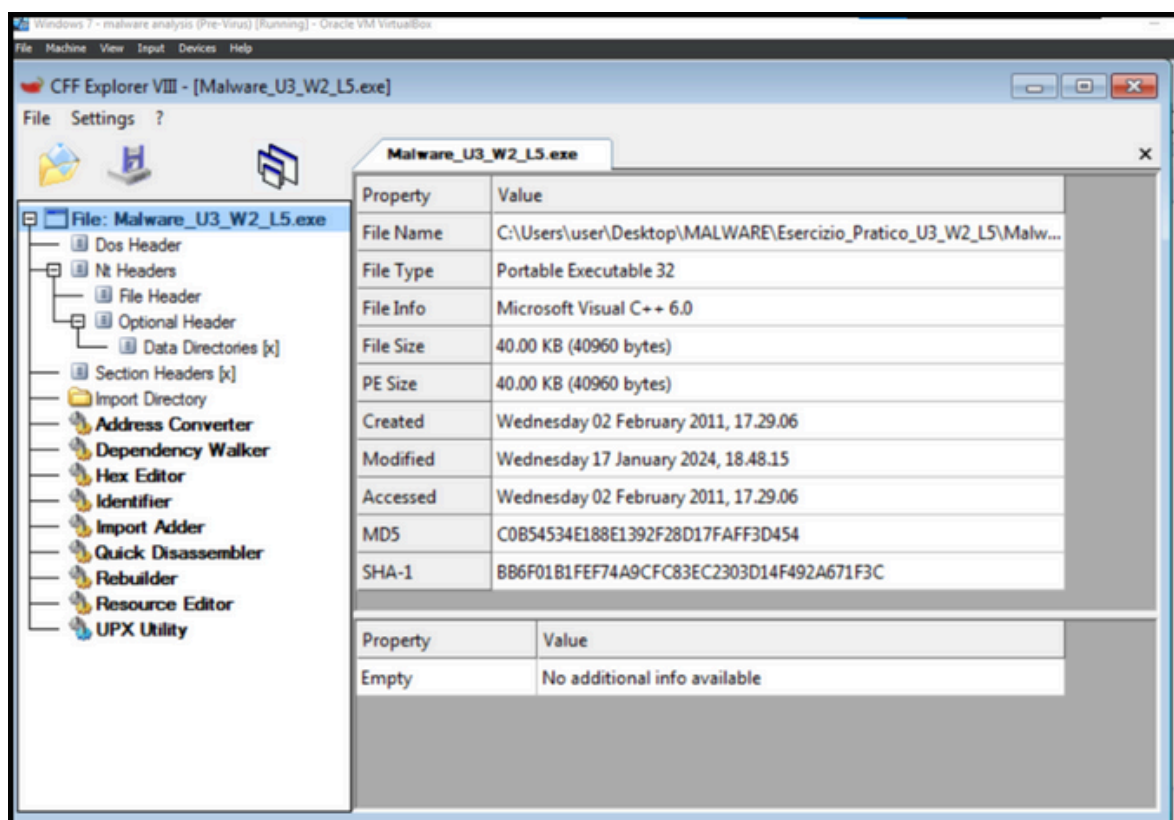
S10-L5 Analisi Malware

Emulo Francesco

CFF EXPLORER

Passiamo, ora, a comprendere come sia strutturato tale malware utilizzando il tool CFF Explorer (sempre analisi statica dato che non lanciamo ancora il malware).

Aperto il nostro malware tramite CFF possiamo ottenere delle prime informazioni:



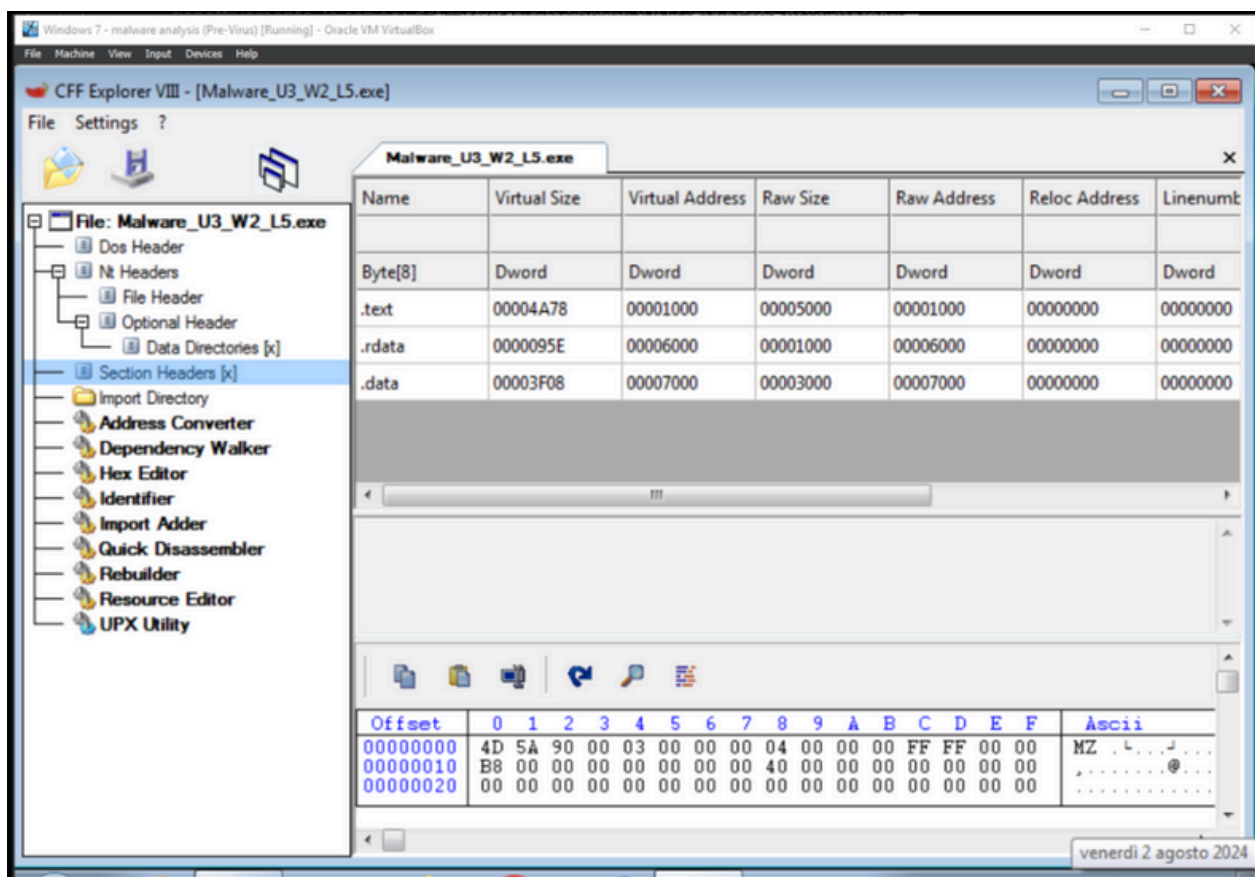
Vengono, nell'immagine sopra, evidenziati gli Hash in MD5 e SHA-1, oltre alla data di creazione.

Spostandoci nelle sezioni "Section Headers" ed "Import Directory" possiamo andare a visualizzare, rispettivamente, le sezioni del malware e le librerie (DLL) importate dallo stesso.

S10-L5 Analisi Malware

Emulo Francesco

Section Header



Analizziamo cosa significhino:

- **.text**, contiene il codice eseguibile del programma (le istruzioni eseguibili dalla CPU);
- **.rdata**, include le informazioni sulle librerie e le funzioni importate ed esportate (come intuibile dall'immagine sopra, sezione Pointing Directories), sono "read-only data".
- **.data**, contiene dati e variabili globali (questi dati possono essere letti e scritti durante l'esecuzione del programma).

S10-L5 Analisi Malware

Emulo Francesco

Import Directory

The screenshot shows the CFF Explorer VIII interface for the file Malware_U3_W2_L5.exe. The left pane displays a tree view of the file's structure, with 'Import Directory' selected. The right pane shows a table of imported modules.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC
WININET.dll	5	000065CC	00000000	00000000	00006664

The bottom of the window shows the Windows 7 taskbar with various application icons and a system clock indicating the date as venerdì 2 agosto 2024 and the time as 11:31.

S10-L5 Analisi Malware

Emulo Francesco

Analisi librerie

Analizziamo nel dettaglio le librerie importate:

- **Kernel32.DLL**
 - Importa 44 funzioni;
 - Questa libreria contiene le funzioni utili alla gestione della memoria, processi e thread, esaminiamone qualcuna:
 - **Sleep**: sospende l'esecuzione del thread corrente per un intervallo di tempo specificato;
 - **SetStdHandle**: imposta un handle per un processo;
 - **GetVersion**: stampa la versione del sistema operativo;
 - **ExitProcess**: termina il processo corrente;
 - **TerminateProcess**: termina un processo specificato;
 - **UnhandledExceptionFilter**: gestisce eccezioni non gestite;
 - **FreeEnvironmentStringsA**: libera la memoria allocata per le stringhe;
 - **WriteFile**: scrive dati in un file o in un output;
 - **GetLastError**: restituisce il codice di errore per l'ultima funzione chiamata che ha fallito;
 - **SetFilePointer**: imposta il puntatore del file nella posizione specificata.

S10-L5 Analisi Malware

Emulo Francesco

Analisi librerie

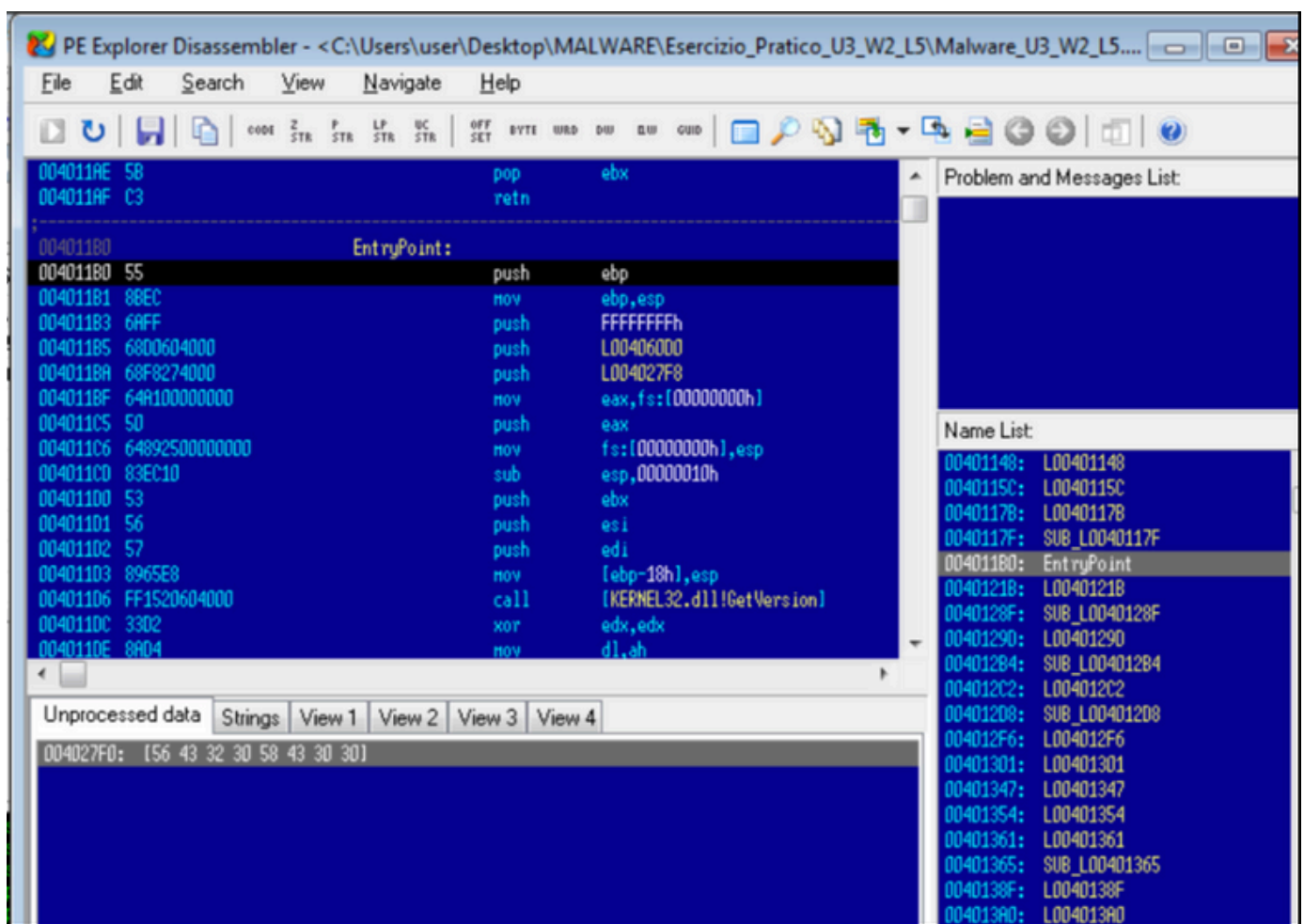
- ***Wininet.DDL***
 - Importa 5 funzioni;
 - Questa libreria fornisce funzioni per l'accesso ad internet ed il trasferimento di dati tramite protocolli HTTP ed FTP.
 - ***InternetOpenUrlA***: apre un'URL specifica e restituisce un handle;
 - ***InternetCloseHandle***: chiude un handle aperto precedentemente;
 - ***InternetReadFile***: legge dati da un handle;
 - ***InternetGetConnectedState***: determina lo stato della connessione Internet;
 - ***InternetOpenA***: inizializza l'utilizzo delle funzionalità Internet per l'applicazione;

S10-L5 Analisi Malware

Emulo Francesco

PE Explorer

Possiamo utilizzare, per comprendere meglio il malware in analisi, il programma PE Explorer che, caricato il file ed andando nella “Section Disassembler”, ci fornirà il codice in Assembly:



PE Explorer Disassembler - <C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L5\Malware_U3_W2_L5....

File Edit Search View Navigate Help

CODE Z STR P STR LP STR UC STR OFF SET BYTE WORD DIB DIB GUID

0040118E 5B pop ebx
0040118F C3 retn

00401180 EntryPoint:
00401180 55 push ebp
00401181 8BEC mov ebp,esp
00401183 6AFF push FFFFFFFFh
00401185 6800604000 push L00406000
0040118A 68F8274000 push L004027F8
0040118F 64A100000000 nov eax,fs:[00000000h]
004011C5 50 push eax
004011C6 64892500000000 nov fs:[00000000h],esp
004011C0 83EC10 sub esp,00000010h
00401100 53 push ebx
00401101 56 push esi
00401102 57 push edi
00401103 8965E8 mov [ebp-18h],esp
00401106 FF1520604000 call [KERNEL32.dll!GetVersion]
0040110C 33D2 xor edx,edx
0040110E 8A04 mov dl,ah

Problem and Messages List:

Name List:

00401148: L00401148
0040115C: L0040115C
00401178: L00401178
0040117F: SUB_L0040117F
00401180: EntryPoint
00401218: L00401218
0040128F: SUB_L0040128F
00401290: L00401290
004012B4: SUB_L004012B4
004012C2: L004012C2
00401208: SUB_L00401208
004012F6: L004012F6
00401301: L00401301
00401347: L00401347
00401354: L00401354
00401361: L00401361
00401365: SUB_L00401365
0040138F: L0040138F
004013A0: L004013A0

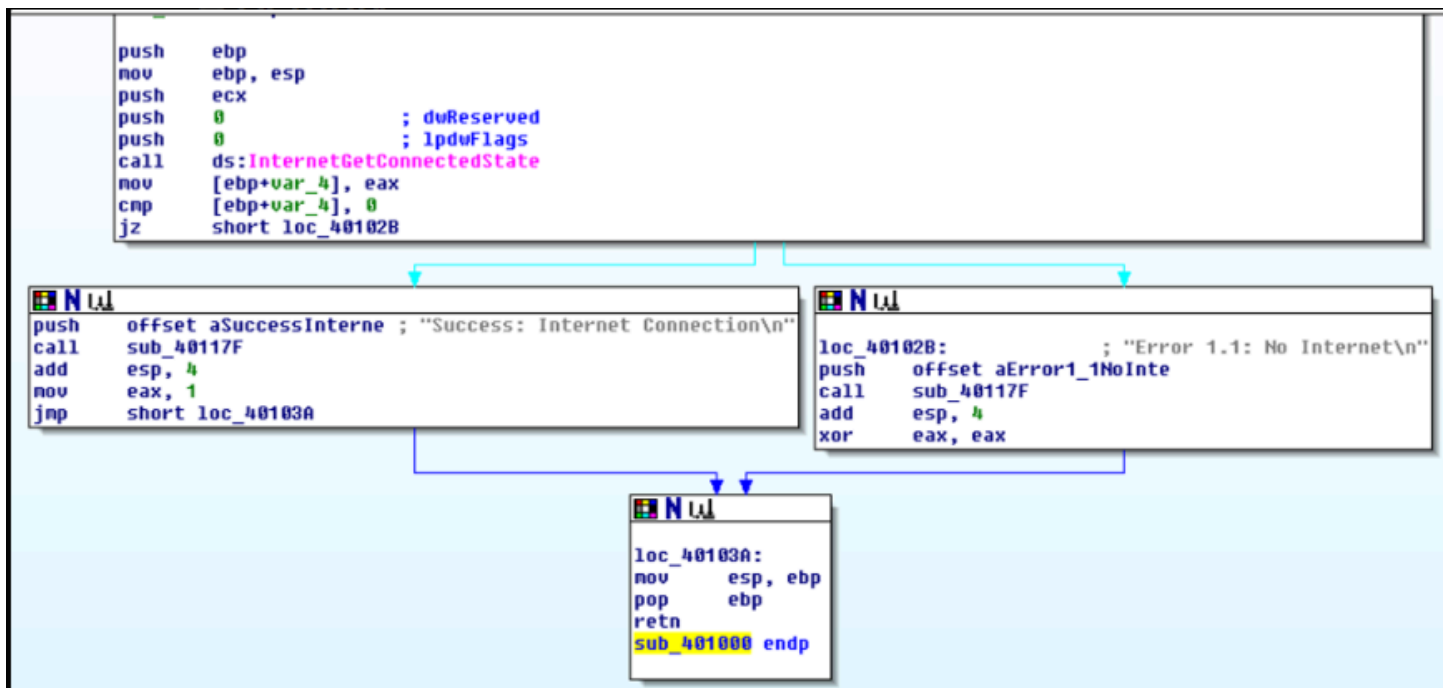
Unprocessed data Strings View 1 View 2 View 3 View 4

004027F0: [56 43 32 30 58 43 30 30]

S10-L5 Analisi Malware

Emulo Francesco

Assembly



- Analizziamo il codice blocco per blocco.

S10-L5 Analisi Malware

Emulo Francesco

Primo blocco di codice

La prima istruzione (in giallo) è quella utile alla creazione dello stack;

Il gruppo cerchiato, invece, è l'istruzione utile a richiamare la funzione (i push passano sullo stack i parametri);

L'ultima istruzione in giallo, è un IF (controllo condizionale).



```
push    ebp
mov     ebp, esp
push    ecx
push    0           ; dwReserved
push    0           ; lpdwFlags
call    ds:InternetGetConnectedState
mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0
jz      short loc_40102B
```

Nello specifico qui viene confrontato il valore nella variabile `ebp+var_4` con il contenuto di `eax`. Se sono uguali `jz` (ovvero jump if zero) salta in `loc_40102B`.

- ***push ebp*** salva il valore di `ebp` sullo stack
- ***mov ebp, esp*** copia il valore di `esp` in `ebp`
- ***push ecx***, salva il valore `ecx` sullo stack
- ***push 0*** salva 0 sullo stack, questo è seguito da un parametro di `InternetGetConnectedState`
- ***call ds:[funzione]*** chiama la funzione
- ***mov [ebp+var_4], eax*** copia il risultato della funzione nella variabile `ebp+var_4`
- ***cmp*** confronta il valore `ebp+var_4` con 0
- ***jz short loc_40102B*** se il confronto `cmp` è uguale a 0 allora salta a loc.


Da un punto di vista logico qui troviamo una diramazione del diagramma di flusso dato che dovremmo imboccare in un messaggio di successo o di errore.

Analizziamo il blocco 2 (successo) ed il blocco 3 (errore).

S10-L5 Analisi Malware

Emulo Francesco

Secondo blocco di codice



```
push    offset aSuccessInterne ; "Success: Internet Connection\n"  
call    sub_40117F  
add     esp, 4  
mov     eax, 1  
jmp     short loc_40103A
```

L'istruzione evidenziata serve per richiamare la funzione.
In questo caso stampiamo un messaggio di successo.

- ***push offset aSuccessInternet***, se vi è connessione pusha l'indirizzo della stringa "Success: internet connection" sullo stack
- ***call sub_40105F***, chiama una funzione per gestire il successo di connessione
- ***add esp, 4*** ripristina lo stack pointer
- ***mov eax, 1*** copia il valore 1 in eax, indica probabilmente un successo
- ***jmp short loc_40103A***, è un salto incondizionato

S10-L5 Analisi Malware

Emulo Francesco

Terzo blocco di codice

Come nell'immagine precedente.
In questo caso stampiamo un messaggio di errore.



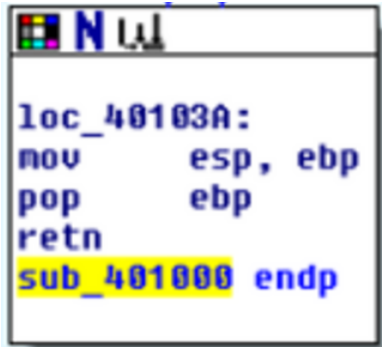
```
loc_40102B:                ; "Error 1.1: No Internet\n"
push    offset aError1_1NoInte
call    sub_40117F
add     esp, 4
xor     eax, eax
```

- **loc_40102B** è la destinazione per salti condizionali
- **push offset aError1**, operazione di somma, 4 in questo caso rimuove l'argomento dallo stack (pulisce)
- **add esp, 4** servono per pulire lo stack. Quando si incrementa di 4 (ogni variabile occupa 4 byte) viene rimosso l'argomento, ovvero il puntatore della stringa, dallo stack, ripristinano lo stack al suo stato precedente
- **xor eax**, XOR esegue un'operazione detta "XOR bit a bit" ove l'operando **eax** è sia origine che destinazione. Lo XOR di un numero con se stesso da sempre 0 e questa è una tecnica utile per azzerare un registro (alternativa a `mov eax, 0` in questo caso).

S10-L5 Analisi Malware

Emulo Francesco

Quarto blocco di codice



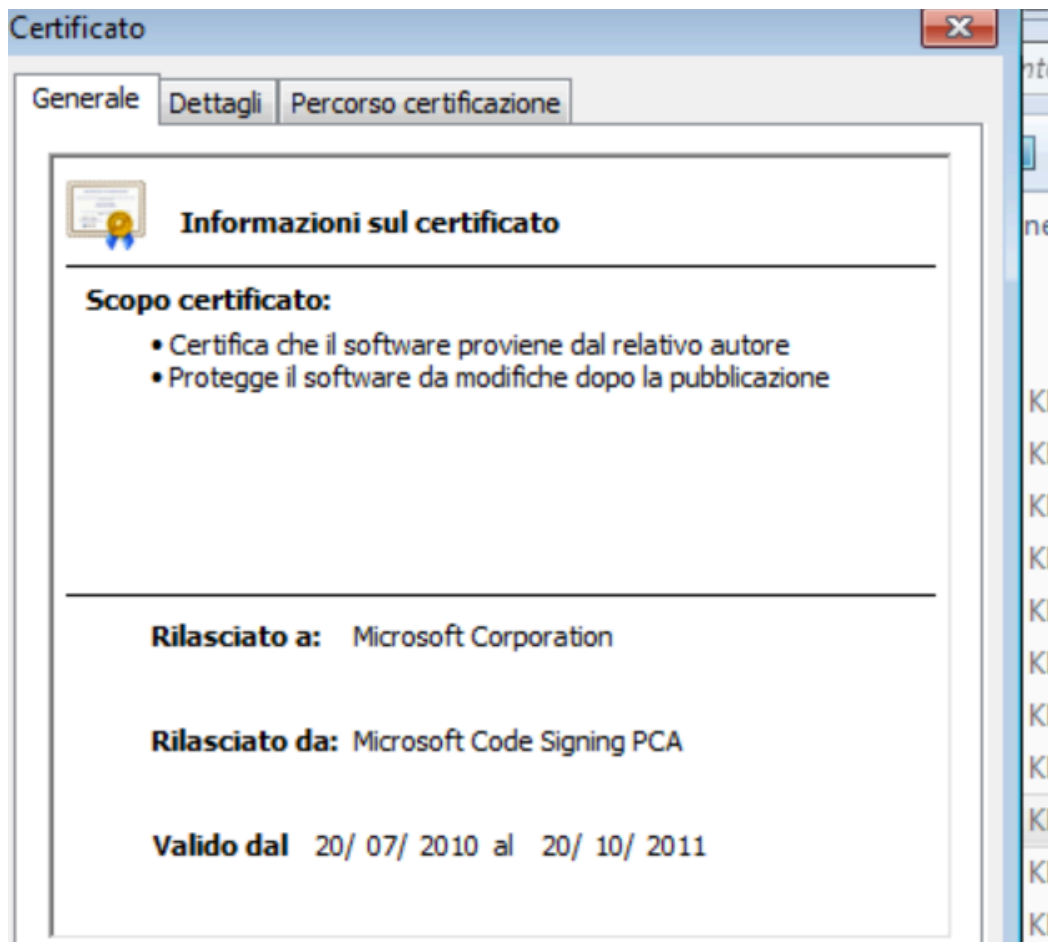
- **loc_40103A** è il punto di arrivo dei vari salti condizionali.
- **mov esp, ebp**, copia ebp in esp
- **pop** utile per rimuovere il valore in cima allo stack
- **retn**, rimuove l'indirizzo di ritorno dallo stack, ripristinando lo stato dello stack come era prima della chiamata alla funzione
- **sub_401000 endp**, indica la fine della funzione medesima.

S10-L5 Analisi Malware

Emulo Francesco

Traccia Bonus

La prima cosa che possiamo fare è andare a vedere il certificato di autenticità facendo tasto destro sull'applicativo, proprietà, **firme digitali**, informazione sul certificato.



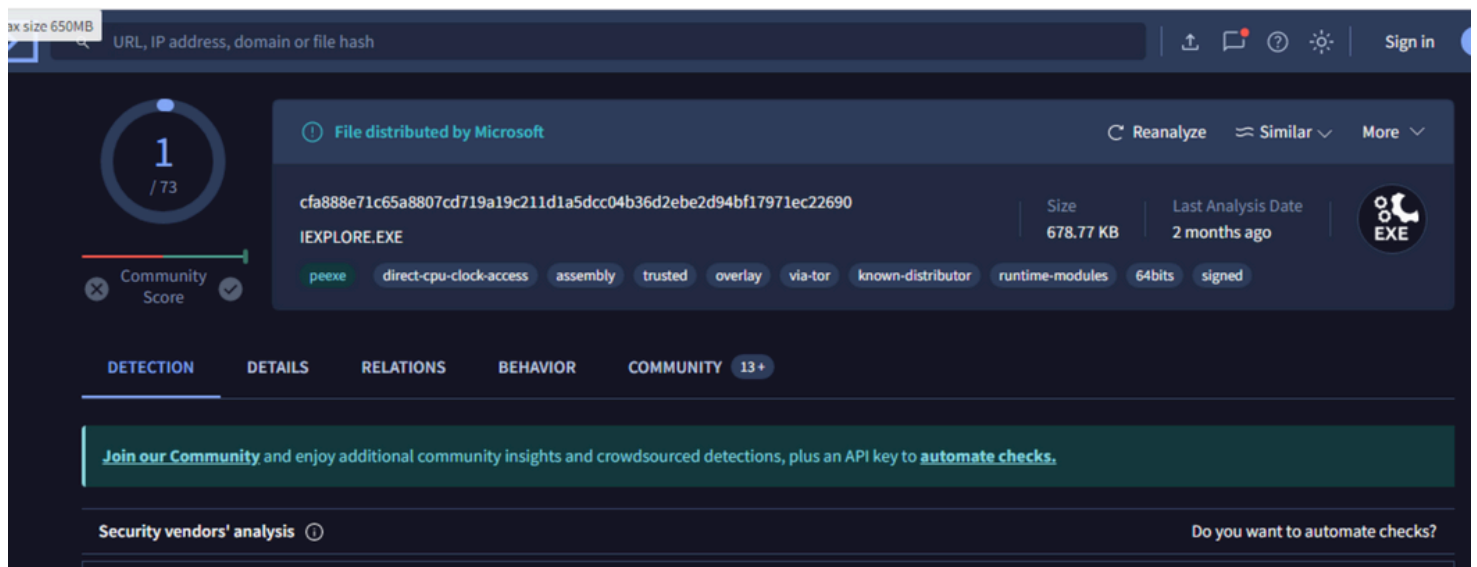
Da qui possiamo vedere chi ha rilasciato l'applicativo e quando.

S10-L5 Analisi Malware

Emulo Francesco

Traccia Bonus

Andiamo a fare il check su ViruTotal



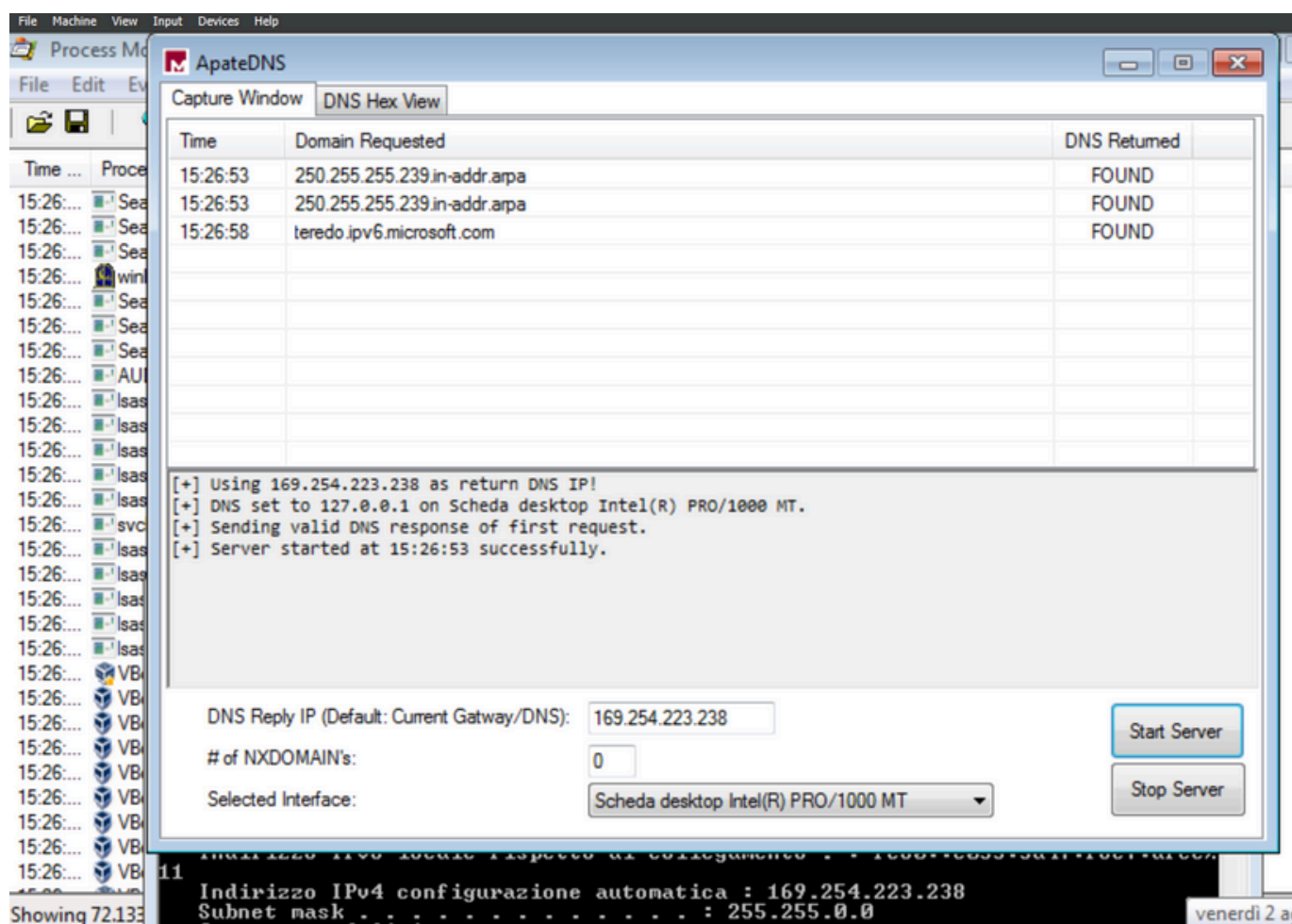
Non sembra essere inserito nel database dei malware flaggati, questa non è una prova di non malevolenza dato che potrebbe essere, anche se improbabile, un nuovo malware. Proseguiamo con le analisi.

S10-L5 Analisi Malware

Emulo Francesco

Traccia Bonus

Possiamo passare su Procmon ed ApacheDNS e vedere se tenta, una volta avviato, ad accedere a directory non standard o se avvia comunicazioni di rete sospette. Ricorda che questa è un'analisi dinamica, quindi mettili in intranet per sicurezza



Non sembra fare richieste malevoli o non canoniche

S10-L5 Analisi Malware

Emulo Francesco

Traccia Bonus

Passiamo ad utilizzare RegShot

Effettuiamo il primo shot, lanciamo il programma, secondo shot, compariamo i risultati per apprezzare le modifiche nelle chiavi di registro.

```
-res-x86 - Blocco note
File Modifica Formato Visualizza ?

Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2024/8/2 13:33:49 , 2024/8/2 13:34:57
Computer: USER-PC , USER-PC
Username: user , user

-----
Keys added: 27

HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hiv
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\hiv
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\hiv\OpenWithList
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\hiv
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist01202408022024
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagsMRU\31
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\48\ComDlg
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\95\Shell\{5C4F28B5-F869-4E84-8E60-F11D897C5C7}\{5C4F28B5-F869-4E84-8E60-F11D897C5C7}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\96\Shell\{5C4F28B5-F869-4E84-8E60-F11D897C5C7}\{5C4F28B5-F869-4E84-8E60-F11D897C5C7}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\{0B2BAAE8-0042-4DCA-A44D-3E8F}\{0B2BAAE8-0042-4DCA-A44D-3E8F}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\{0B2BAAE8-0042-4DCA-A44D-3E8F}\{0B2BAAE8-0042-4DCA-A44D-3E8F}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\ComDlg\{FBB3477E-C9E4-4B3B-A2B4-D3F}\{FBB3477E-C9E4-4B3B-A2B4-D3F}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\97
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\97\Shell
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagsMRU\31
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\48\ComDlg
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\95\Shell\{5C4F28B5-F869-4E84-8E60-F11D897C5C7}\{5C4F28B5-F869-4E84-8E60-F11D897C5C7}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\96\Shell\{5C4F28B5-F869-4E84-8E60-F11D897C5C7}\{5C4F28B5-F869-4E84-8E60-F11D897C5C7}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\{0B2BAAE8-0042-4DCA-A44D-3E8F}\{0B2BAAE8-0042-4DCA-A44D-3E8F}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\Shell\{0B2BAAE8-0042-4DCA-A44D-3E8F}\{0B2BAAE8-0042-4DCA-A44D-3E8F}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\AllFolders\ComDlg\{FBB3477E-C9E4-4B3B-A2B4-D3F}\{FBB3477E-C9E4-4B3B-A2B4-D3F}
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\97
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\97\Shell

-----
values added: 109
```

```

00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count\{
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Count\{
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings: 46 00 00 00 34
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings: 46 00 00 00 35
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\Nodeslots: 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\Nodeslots: 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRULISTEX: 00 00 00 00 02 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRULISTEX: 00 00 00 00 03 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\3\MRULISTEX: 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\3\MRULISTEX: 00 00 00 00 01 00 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\Nodeslots: 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\Nodeslots: 02 02 02 02 02 02 02 02 02
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRULISTEX: 00 00 00 00 02 00 00 00 03 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\MRULISTEX: 00 00 00 00 03 00 00 00 02 00 00
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\3\MRULISTEX: 00 00 00 00 FF FF FF FF
HKU\S-1-5-21-3771313050-58705377-3452663501-1001\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\3\MRULISTEX: 00 00 00 00 01 00 00 00 FF FF FF
-----
Total changes: 159

```

Analizziamo le chiavi principali

S10-L5 Analisi Malware

Emulo Francesco

Traccia Bonus

- ComDlg32\OpenSavePidlMRU\hiv
- Explorer\FileExts\.hiv
- Explorer\RecentDocs\.hiv

Queste chiavi registrano i file recenti aperti o salvati dall'utente, con estensione .hiv.

Mantengono traccia delle ultime attività sui file per facilitarne l'accesso rapido.

- Internet Settings\5.0\Cache\Extensible
Cache\MSHist012024080220240803

Questa chiave riguarda la cache del browser Internet Explorer. Memorizza informazioni sui siti web visitati dall'utente per migliorare le prestazioni del browser e l'accesso rapido ai siti web.

- Shell\BagMRU
- Shell\Bags

Queste chiavi tengono traccia delle cartelle aperte di recente e delle impostazioni di visualizzazione delle cartelle.

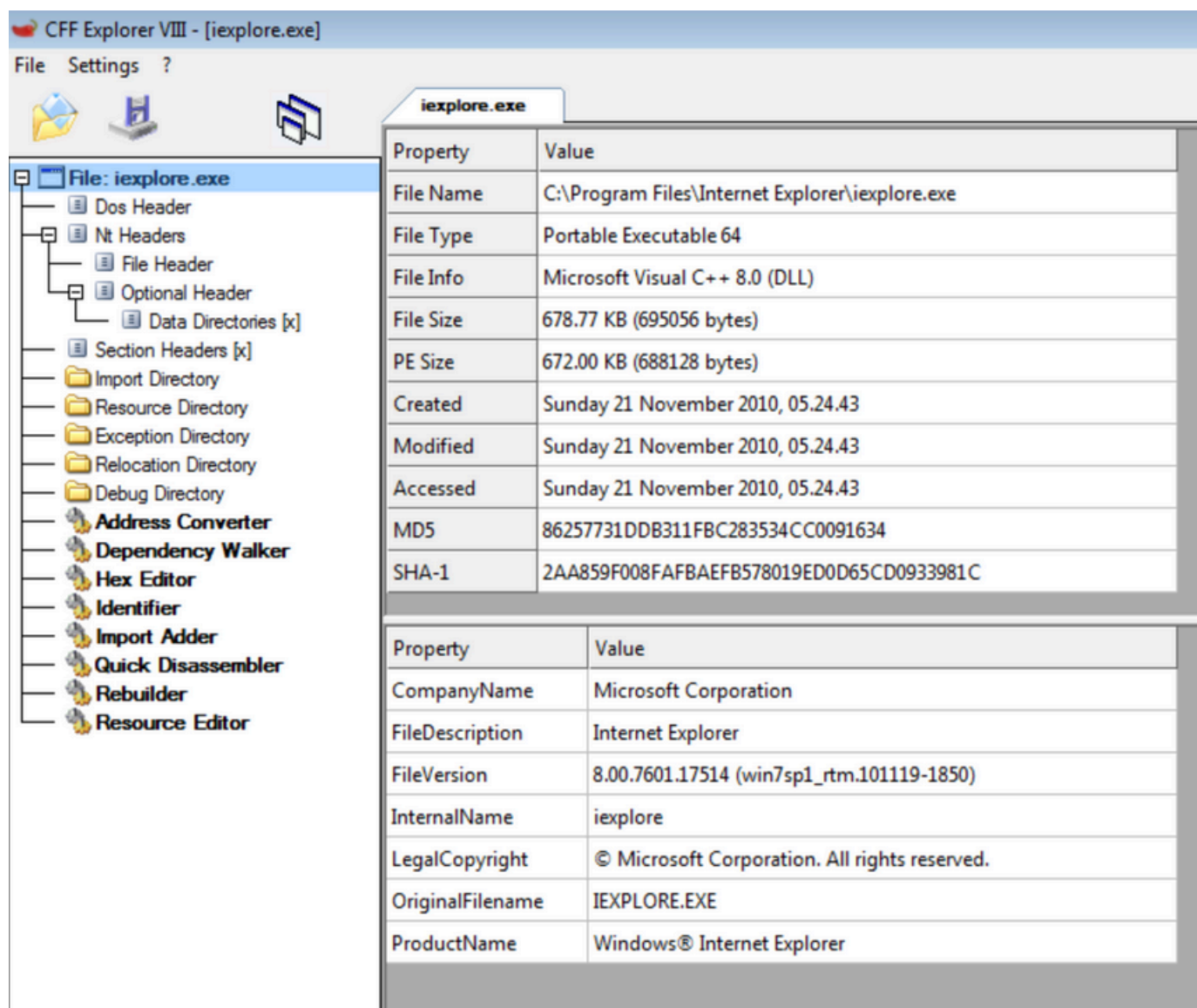
Aiutano Windows a ricordare come l'utente preferisce visualizzare il contenuto delle cartelle.

S10-L5 Analisi Malware

Emulo Francesco

Traccia Bonus

Passiamo ad utilizzare CFF



File: iexplore.exe

Property	Value
File Name	C:\Program Files\Internet Explorer\iexplore.exe
File Type	Portable Executable 64
File Info	Microsoft Visual C++ 8.0 (DLL)
File Size	678.77 KB (695056 bytes)
PE Size	672.00 KB (688128 bytes)
Created	Sunday 21 November 2010, 05.24.43
Modified	Sunday 21 November 2010, 05.24.43
Accessed	Sunday 21 November 2010, 05.24.43
MD5	86257731DDB311FBC283534CC0091634
SHA-1	2AA859F008FAFBAEFB578019ED0D65CD0933981C

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Internet Explorer
FileVersion	8.00.7601.17514 (win7sp1_rtm.101119-1850)
InternalName	iexplore
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	IEXPLORE.EXE
ProductName	Windows® Internet Explorer

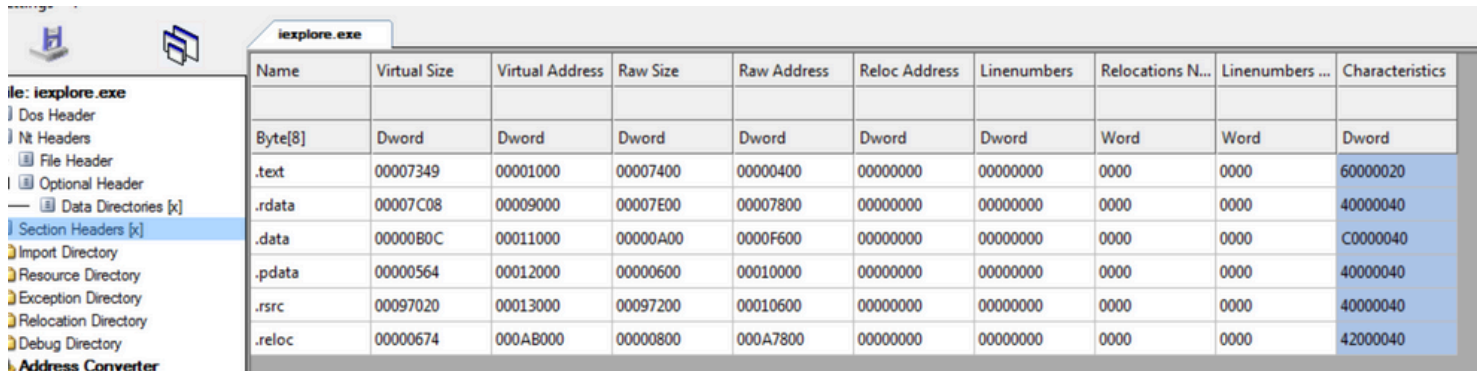
Qui possiamo vedere altre generalità che ne confermano l'autenticità; potremmo confrontare questi Hash con quelli ufficiali della Microsoft per ulteriori conferme.

S10-L5 Analisi Malware

Emulo Francesco

Traccia Bonus

Analizziamo Header e Librerie



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00007349	00001000	00007400	00000400	00000000	00000000	0000	0000	60000020
.rdata	00007C08	00009000	00007E00	00007800	00000000	00000000	0000	0000	40000040
.data	00000B0C	00011000	00000A00	0000F600	00000000	00000000	0000	0000	C0000040
.pdata	00000564	00012000	00000600	00010000	00000000	00000000	0000	0000	40000040
.rsrc	00097020	00013000	00097200	00010600	00000000	00000000	0000	0000	40000040
.reloc	00000674	000AB000	00000800	000A7800	00000000	00000000	0000	0000	42000040

.text .rdata e .data sono stati analizzati nell'esercizio precedente.

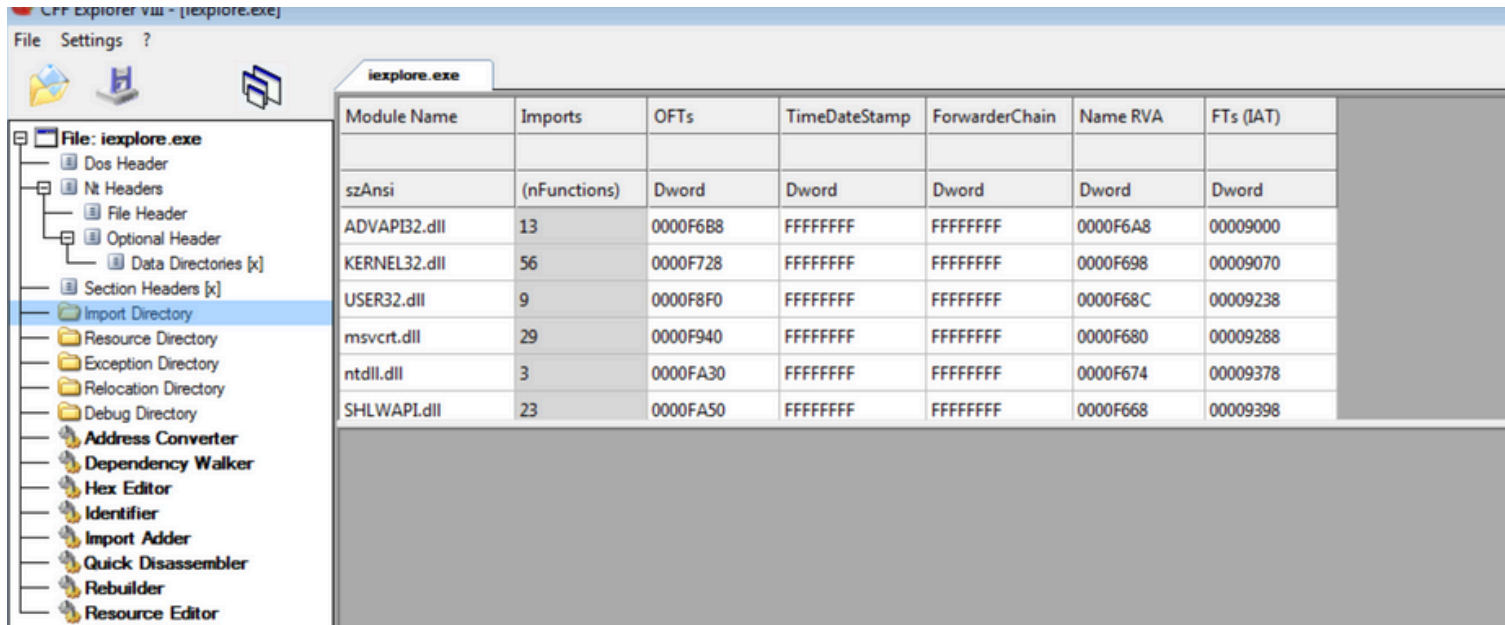
- **.pdata**, contiene informazioni circa le procedure di chiamata di funzione e gestione degli errori;
- **.rsrc**, contiene risorse del programma come cursori, stringhe e menu;
- **.reloc**, contiene informazioni di rilocalizzazione.

S10-L5 Analisi Malware

Emulo Francesco

Traccia Bonus

Analizziamo Header e Librerie



- **ADVAPI32.dll**, utile per le funzioni avanzate di API di Windows
- **USER32.dll**, gestisce le informazioni inerenti l'interfaccia utente di Windows e la gestione delle finestre
- **msvcrt.dll**, fornisce funzioni standard di C runtime
- **ntdll.dll**, ha funzioni di basso livello del kernel
- **SHLWAPI.dll**, fornisce funzioni di supporto per la manipolazione di stringhe, percorsi, registri etc.

S10-L5 Analisi Malware

Emulo Francesco

Conclusione

iexplore.exe, probabilmente è autentico, non è un malware; sembra essere una versione di Internet Explorer.

Le librerie e le chiavi con cui interagisce sono strettamente associate alle funzionalità di Internet Explorer, avvalorando quanto intuito.