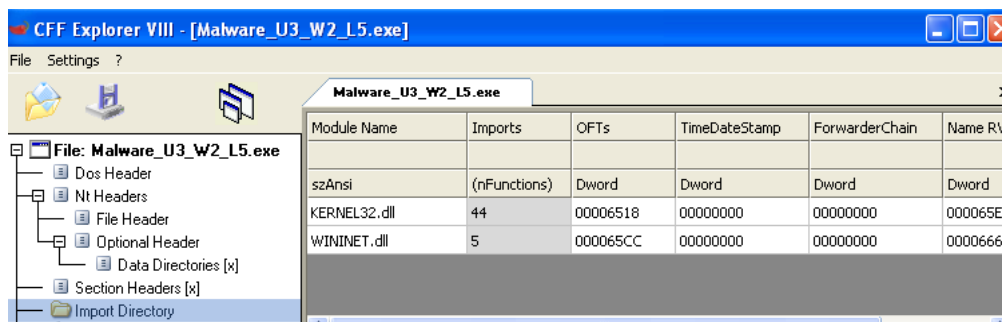


Report progetto settimanale

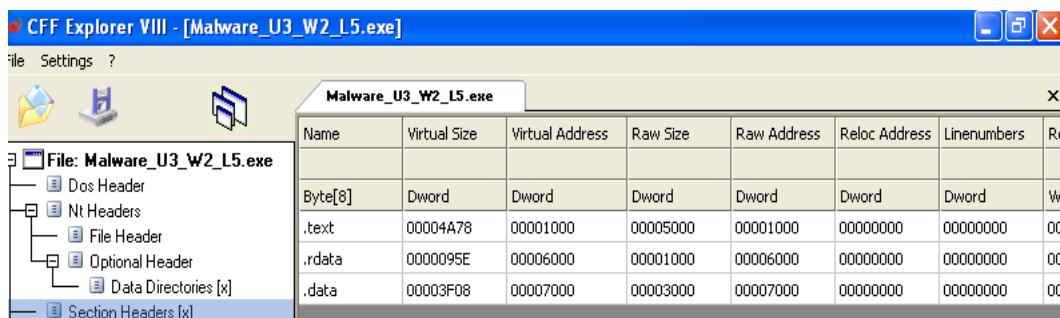
Analisi malware

Per svolgere i primi due quesiti ho utilizzato CFF Explorer per analizzare malware. CFF Explorer è un software che consente di analizzare gli eseguibili di Windows, attraverso l'uso di questo strumento, sono stato in grado di ottenere una lista dettagliata delle librerie importate dal malware e delle sezioni presenti nel suo codice.



wininet.dll: Fornisce funzionalità per la comunicazione di rete e l'accesso a risorse su Internet. È principalmente utilizzata per operazioni di networking come l'apertura di connessioni HTTP, il download di file, l'upload di dati.

kernel32.dll: Fornisce un'insieme di funzionalità di basso livello per la gestione dei processi, la gestione della memoria, le operazioni di input/output, la gestione dei file, la gestione degli errori e molte altre funzioni essenziali del sistema operativo. La libreria kernel32.dll è utilizzata da quasi tutti i programmi Windows e offre un'interfaccia per l'interazione con il sistema operativo.



La sezione **.text** contiene il codice eseguibile del programma. È la sezione in cui risiedono le istruzioni del programma, comprese le funzioni e i blocchi di codice. Questa sezione contiene il codice macchina tradotto dal codice sorgente durante la compilazione. L'esecuzione delle istruzioni nella sezione **.text** è ciò che permette al programma di eseguire le sue funzionalità.

La sezione **.rdata** contiene informazioni sulle librerie e le funzioni importate ed esportate dall'eseguibile.

La sezione **.data** contiene variabili globali e dati statici. Questa sezione viene utilizzata per memorizzare dati che possono essere modificati durante l'esecuzione del programma. Ad esempio, potrebbe contenere dati utente o altre informazioni che devono essere memorizzate e modificate nel corso dell'esecuzione del programma.

Analisi del codice assembly

- Creazione dello stack

```
push    ebp
mov     ebp, esp
```

- Confronto e salto condizionale, equivalente a `if (var_4 == 0)`

```
cmp     [ebp+var_4], 0
jz      short loc_40102B
```

- Pulizia e ripristino dello stack

```
mov     esp, ebp
pop     ebp
retn
```

Funzionalità possibile del programma

Il programma utilizza la funzione `InternetGetConnectedState` per verificare lo stato della connessione a Internet. Questa funzione ci da un valore che viene salvato nella variabile `[ebp+var_4]`. Il programma confronta il valore della variabile `[ebp+var_4]` con zero utilizzando l'istruzione `cmp` seguita da `jz` (jump if zero). Questo indica che il programma verifica se c'è una connessione a Internet.

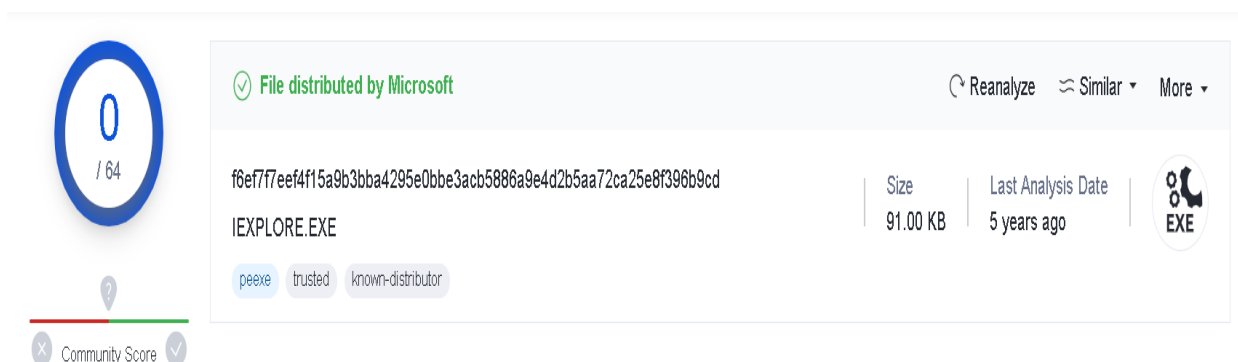
- Se il confronto dà esito positivo (cioè la connessione a Internet non è disponibile), il programma chiama la funzione `sub_40117F`, utilizzando la stringa "Error 1.1: No Internet\n".
- Se il confronto dà esito negativo (cioè la connessione a Internet è disponibile), il programma chiama la funzione `sub_40117F`, utilizzando la stringa "Success: Internet Connection\n".

Sembra che il programma stia verificando se è presente una connessione a Internet e sta gestendo le diverse situazioni. Potrebbe mostrare un messaggio appropriato all'utente in base allo stato della connessione a Internet o potrebbe eseguire ulteriori azioni in base a questa informazione.

Analisi IEXPLORE.exe

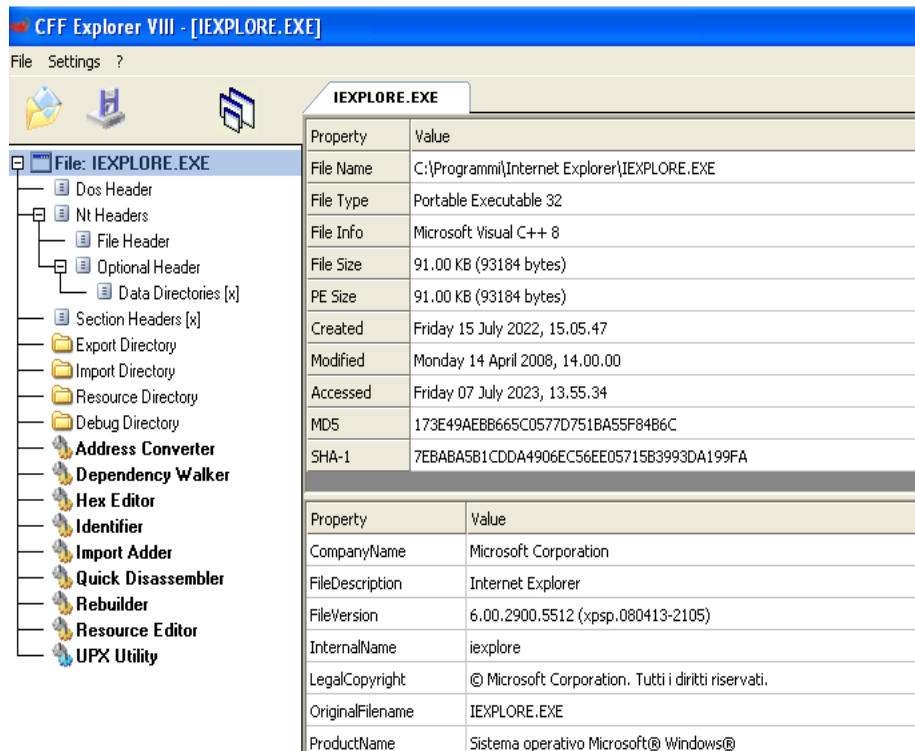
- Calcolo l'hash del file .exe e utilizzo Virustotal per effettuare un controllo

```
C:\Documents and Settings\Epicode_user\Documenti\Downloads\Malanalysis\md5deep-4
.3>md5deep "C:\Programmi\Internet Explorer\IEXPLORE.EXE"
173e49aebb665c0577d751ba55f84b6c C:\Programmi\Internet Explorer\IEXPLORE.EXE
```

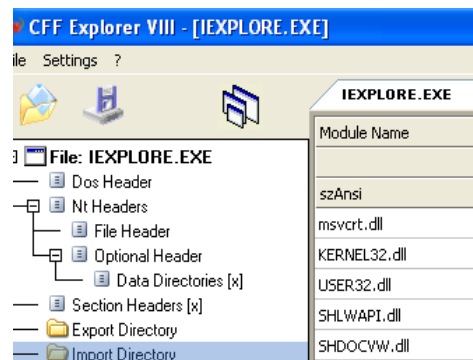


The screenshot shows the VirusTotal interface for the file `IEXPLORE.EXE`. On the left, there is a circular icon with the number '0' and a '64' bit indicator. Below it is a 'Community Score' section with a green checkmark. The main area displays the file's MD5 hash: `f6ef77eef4f15a9b3bba4295e0bbe3acb5886a9e4d2b5aa72ca25e8f396b9cd`. The file is identified as `IEXPLORE.EXE` and is marked as 'File distributed by Microsoft'. The size is listed as 91.00 KB, and the last analysis date is 5 years ago. The file type is 'EXE'. There are buttons for 'Reanalyze', 'Similar', and 'More'. The file is also labeled as 'peexe', 'trusted', and 'known-distributor'.

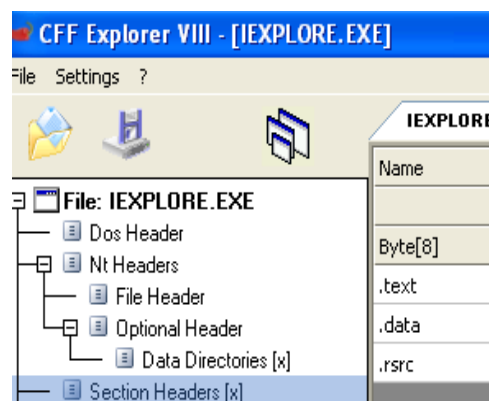
- Utilizzo CFF Explorer per ottenere informazioni sulle proprietà del file



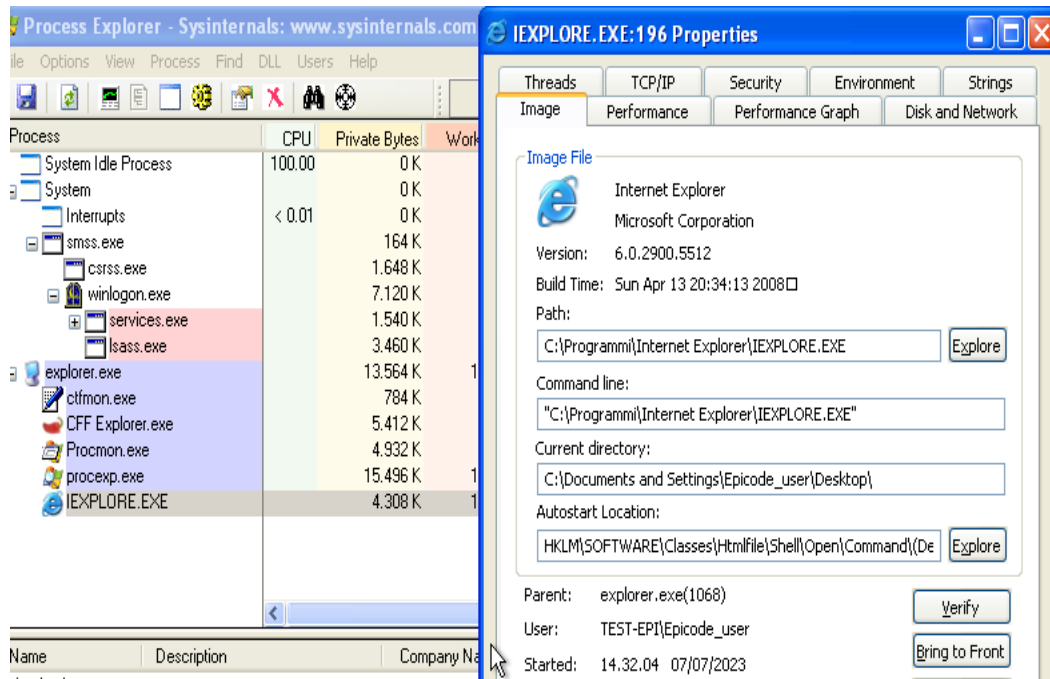
- Analizzo le librerie importate. Si può notare che le librerie sono legittime, in particolare **SHDOCVW.dll** libreria associata al browser web di Windows



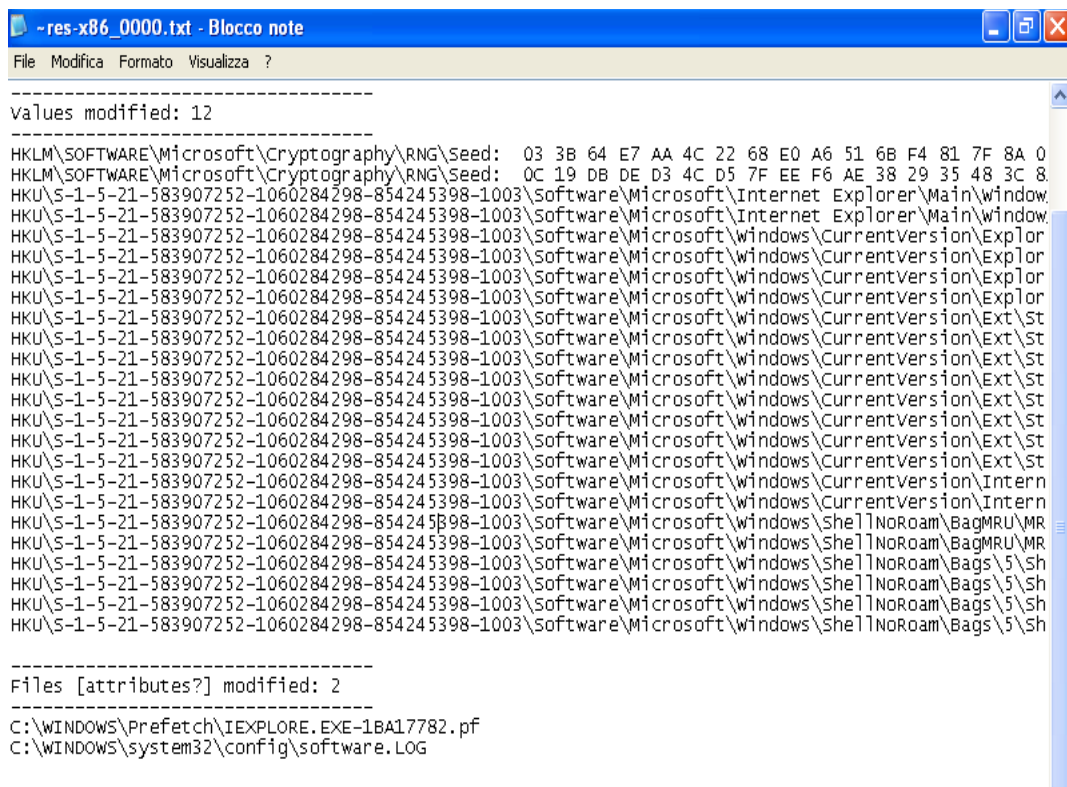
- Analizzo le sezioni, anche in questo caso non risultano sezioni sospette



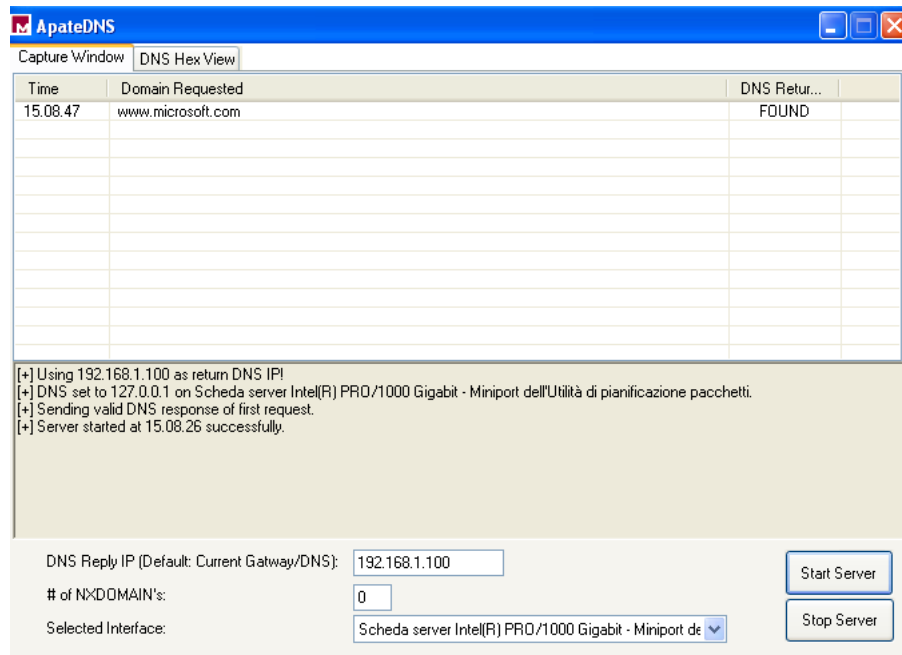
- Utilizzo Process Explorer per visualizzare i processi che si avviano dopo l'esecuzione del file .exe. Viene avviato solo un processo che dal percorso risulta essere conforme al programma



- Analizzo le modifiche alle chiavi di registro tramite Regshot, non risultano modifiche al registro potenzialmente dannose



- Utilizzo ApatеDNS per verificare se il programma effettua connessioni di rete verso server sconosciuti o indesiderati



In base ai risultati dei vari strumenti utilizzati, non sono emersi motivi di preoccupazione riguardo al programma IEXPLORE.exe. Non sono state riscontrate attività dannose o sospette che possano indicare la presenza di un malware o minacce nel programma.