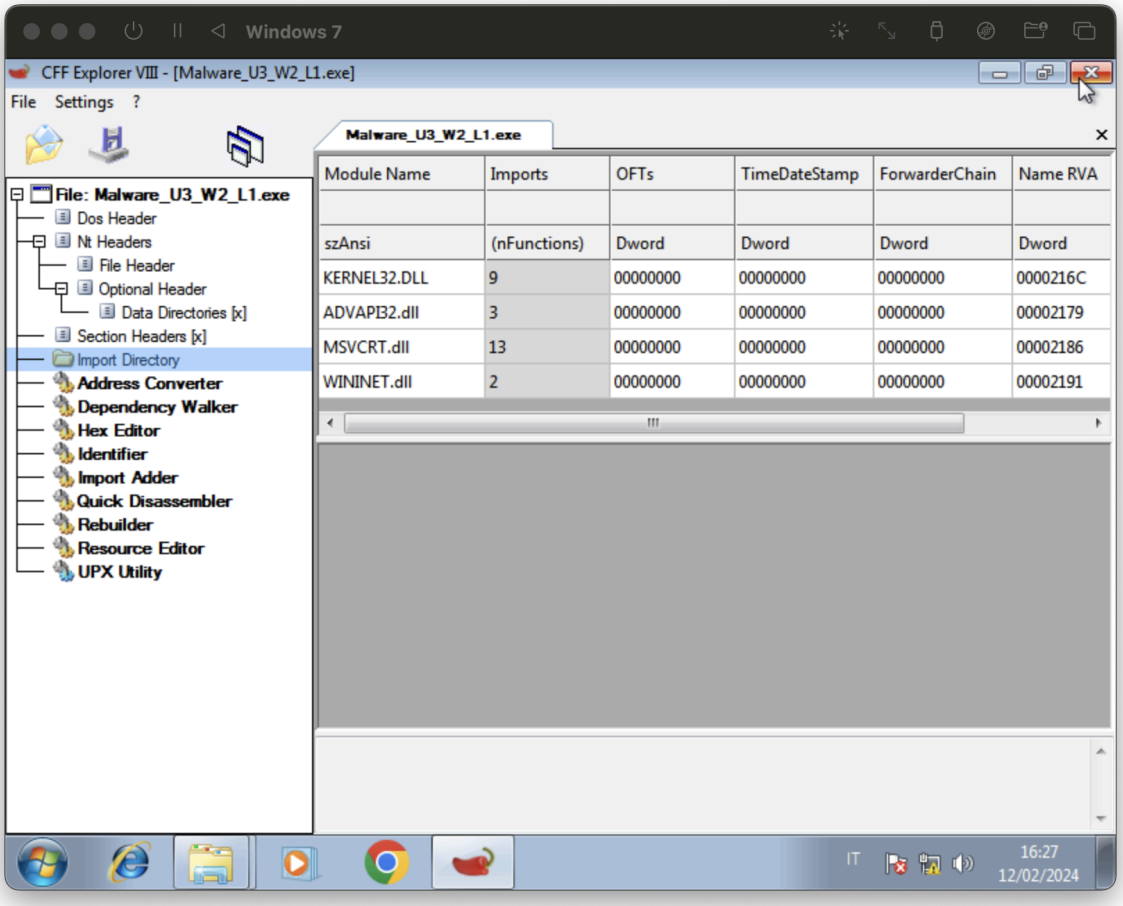
Analisi statica basica malware

Dopo aver analizzato il malware con CFF Explorer questo è quello che ne abbiamo ricavato:



Possiamo notare alcune librerie presenti ed ecco una piccola descrizione per ognuna:

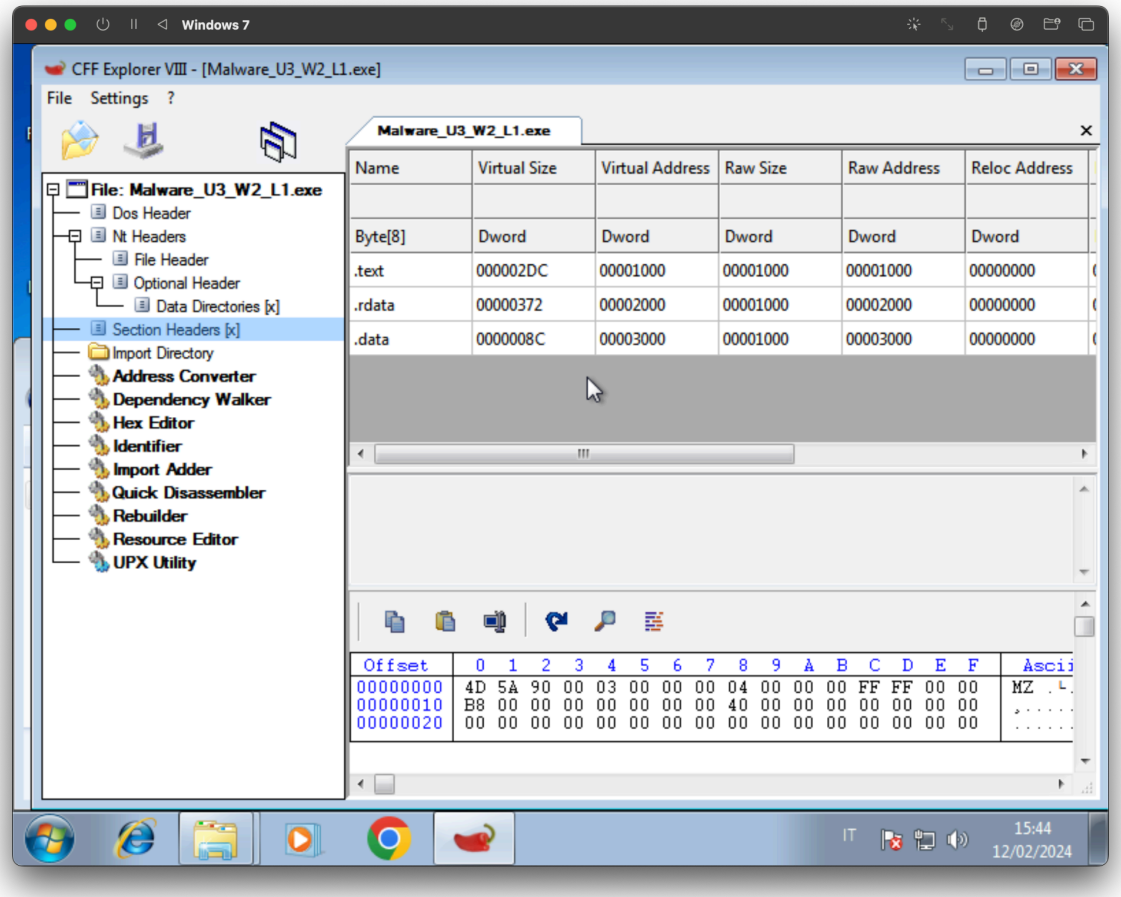
Kernel32.dll: contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria

Advapi32.dll: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo

WSock32.dll e Ws2_32.dll: contengono le funzioni di network, come le socket, le funzioni connect, bind. Ogni malware che utilizza funzionalità di rete caricherà certamente una di queste librerie

Wininet.dll:contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP

E possibile inoltre estrapolare le funzioni del file PE:



Le funzioni sono:

.text: contiene le istruzioni (le righe di codice) che la CPU eseguirà una volta che il software sarà avviato. Generalmente questa è l'unica sezione di un file eseguibile che viene eseguita dalla CPU, in quanto tutte le altre sezioni contengono dati o informazioni a supporto.

.rdata: include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che come abbiamo visto possiamo ricavare con CFF Explorer.

.data: contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma. Una variabile si dice globale quando non è definita all'interno di un contesto di una funzione, ma bensì è globalmente dichiarata ed è di conseguenza accessibile da qualsiasi funzione all'interno dell'eseguibile.

Dalle informazioni estratte dal malware, è evidente che il malware è progettato per interagire direttamente con il sistema operativo e sfruttare le sue funzionalità fondamentali.

Inoltre, l'analisi delle sezioni di un file eseguibile fornisce informazioni preziose sul suo funzionamento interno. La sezione .text contiene le istruzioni eseguibili del programma, mentre le sezioni .rdata e .data contengono rispettivamente informazioni sulle librerie e le funzioni importate/esportate e dati/variabili globali del programma.

Queste informazioni suggeriscono che il malware è progettato per eseguire operazioni sofisticate e potenzialmente dannose sul sistema compromesso, sfruttando le funzionalità di rete e le risorse del sistema operativo.