Adrian.Amarfii 13/01/2023
Report
Task

Traccia:

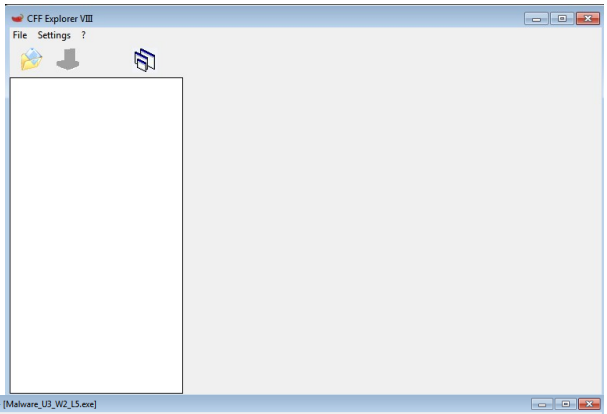
Con riferimento al file **Malware_U3_W2_L5** presente all'interno della cartella «**Esercizio_Pratico_U3_W2_L5**» sul desktop della macchina virtuale dedicata per l'analisi dei malware, rispondere ai seguenti quesiti:

- **1** Quali librerie vengono importate dal file eseguibile?
- **2** Quali sono le sezioni di cui si compone il file eseguibile del malware?

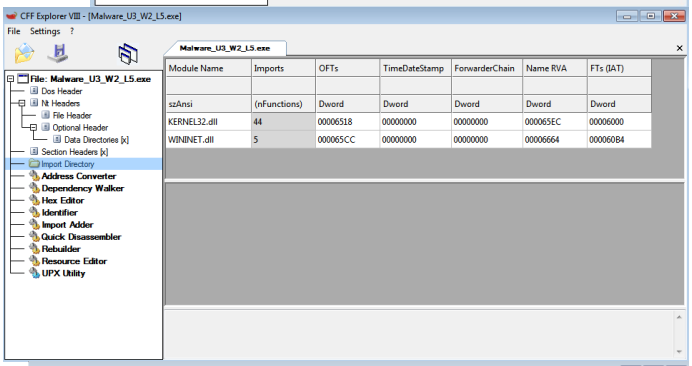
Con riferimento alla figura in slide 3, risponde ai seguenti quesiti:

- **3** Identificare i costrutti noti (creazione dello stack, eventuali cicli, costrutti)
- **4** Ipotizzare il comportamento della funzionalità implementata

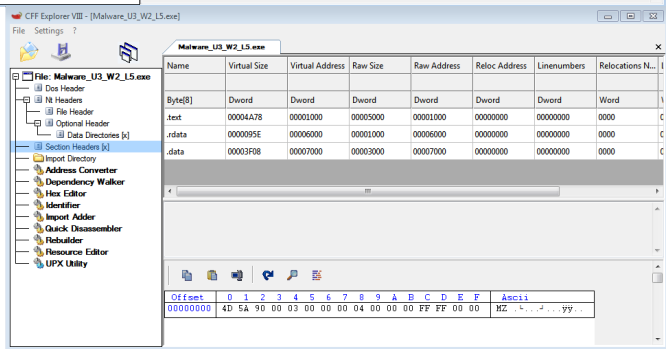
Cominciamo con l'avio della nostra macchina virtuale per analisi del malware e il tool da uitilizare è:CFF EXPLORER
Selezioniamo il file Malware_U3_W2_L5
e andiamo nello Import directory per vedere le librerie importate e nello Section Headers per vedere le sezioni di cui si compone il file eseguibile.



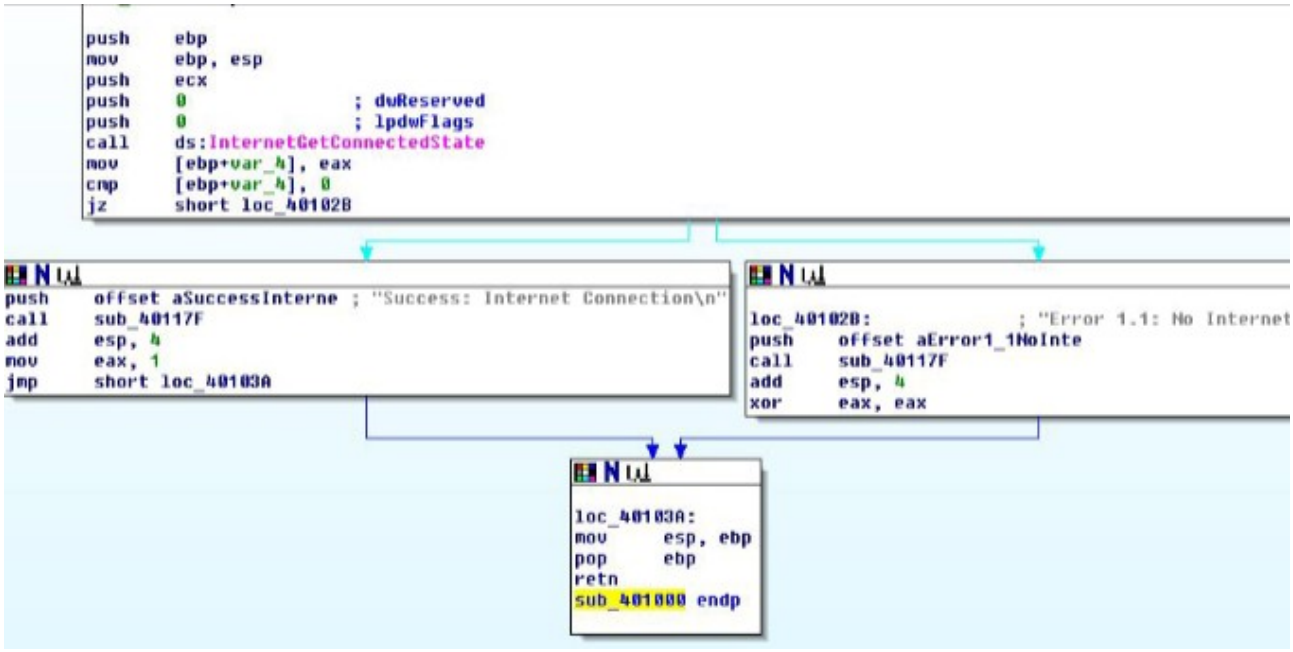
1Come possiamo vedere le librerie importate sono KERNEL32.DLL
WINNET.DLL-KERNEL → Contiene funzioni principali per interagire con il sistema operativo,WINNET → Per implementazioni di alcune protocoli di rete HTTP FTP NTP.



2Le sezione di cui si compone il file eseguibile sono:.TEXT,.RDATA,.DATA



3:



Andiamo a identificare 6 costrutti noti:

1→ push ebp
mov ebp,esp
(crezione stack)

2→ push ecx
push0 ;dwReserved
push 0 ;lpdwFlags
call ds:InternetGetConnectedState
(viene chiamata la funzione internetgetconnectedstate per controllare se il dispositivo è connesso ad internet)

3→ cmp [ebp+var_4],0
jz short loc_40102B
(If → controlla se il risultato è 0 se no salta al loc_40102B

4→ push offeset aSuccessInterne ; “Success:Internet Connection\n”
call sub_40117F
(chiamata funzione printf Success: Internet Connection)

5→ push offset aError1_1NoInte; “Success: Internet Connection\n”
call sub_40117F
(chiamata la funzione printf → Error1.1: Internet)

6→ mov esp ebp
pop ebp
(svuota stack)