Analisi del malware

Controllare quali sono le librerie e le funzioni importate è fondamentale per capire lo scopo del malware infatti per rispondere ai primi due punti richiesti dal progetto utilizziamo il tool CFF EXPLORER che ci aiuta a controllae le funzioni importate ed esportate da un malware .

Il primo passaggio che facciamo è aprire CFF EXPLORER,
clicchiamo sull' icona a forma di cartella e scegliamo il file da caricare in questo caso "Malware_U3_W2_L5"

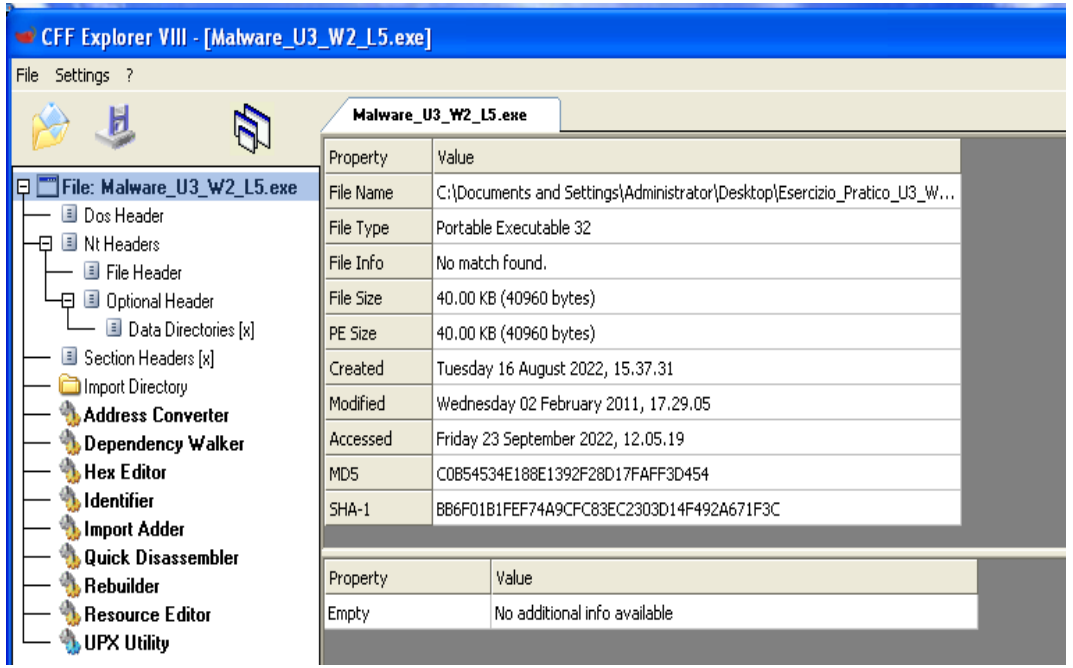
Una volta aperto il file,vediamo una descrizione generale del malware(img.1) .

Quello che ci interessa a noi e vedere le librerie e le funzioni importate , per questo ci digiriamo nella parte "Import directory"del menu a sinistra(img.2). Nella parte a destra ci viengono mostrate le informazioni sulle librerie importate. In questo caso abbiamo :

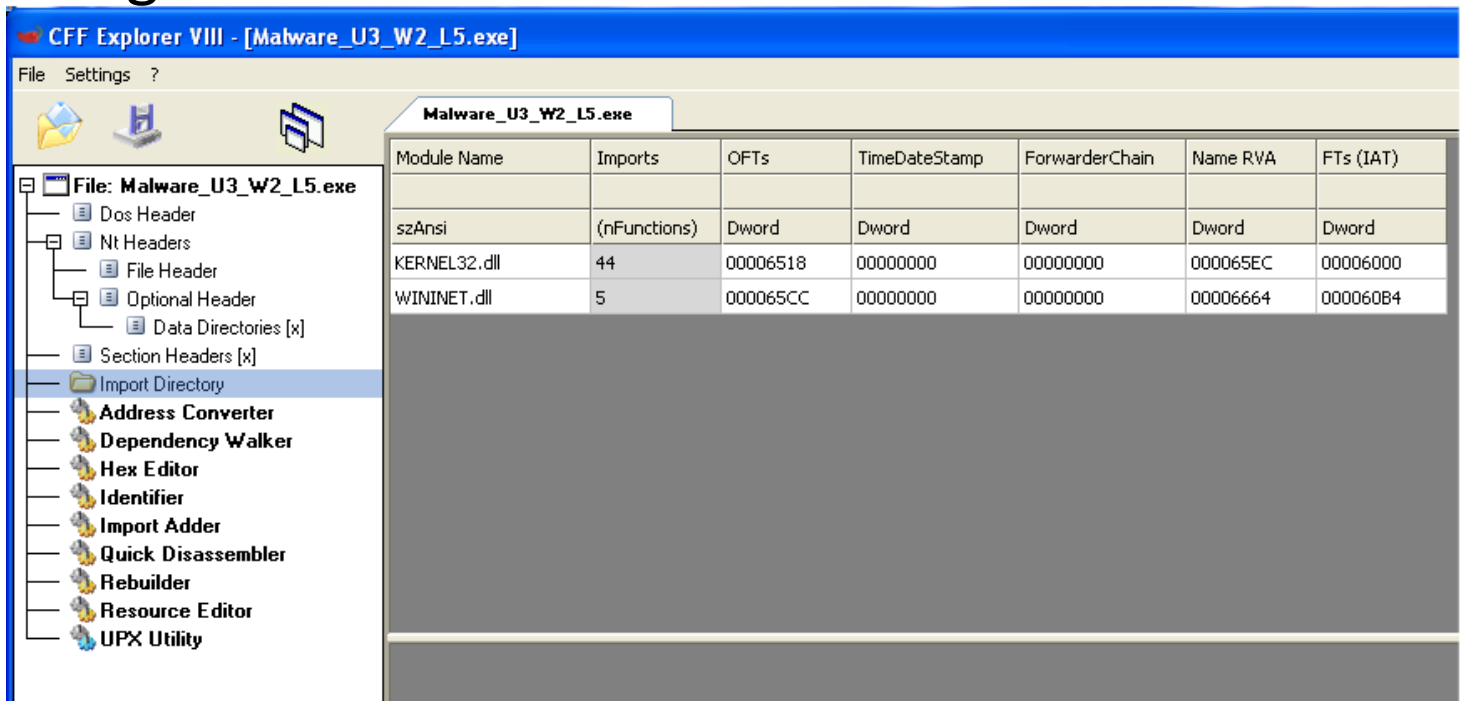
KERNEL32.dll - libreria comune che contiene funzioni principali per la manipolazione dei file ,la gestione della memoria.

WININET.dll - libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, NTP, FTP

- Img.1



- Img.2

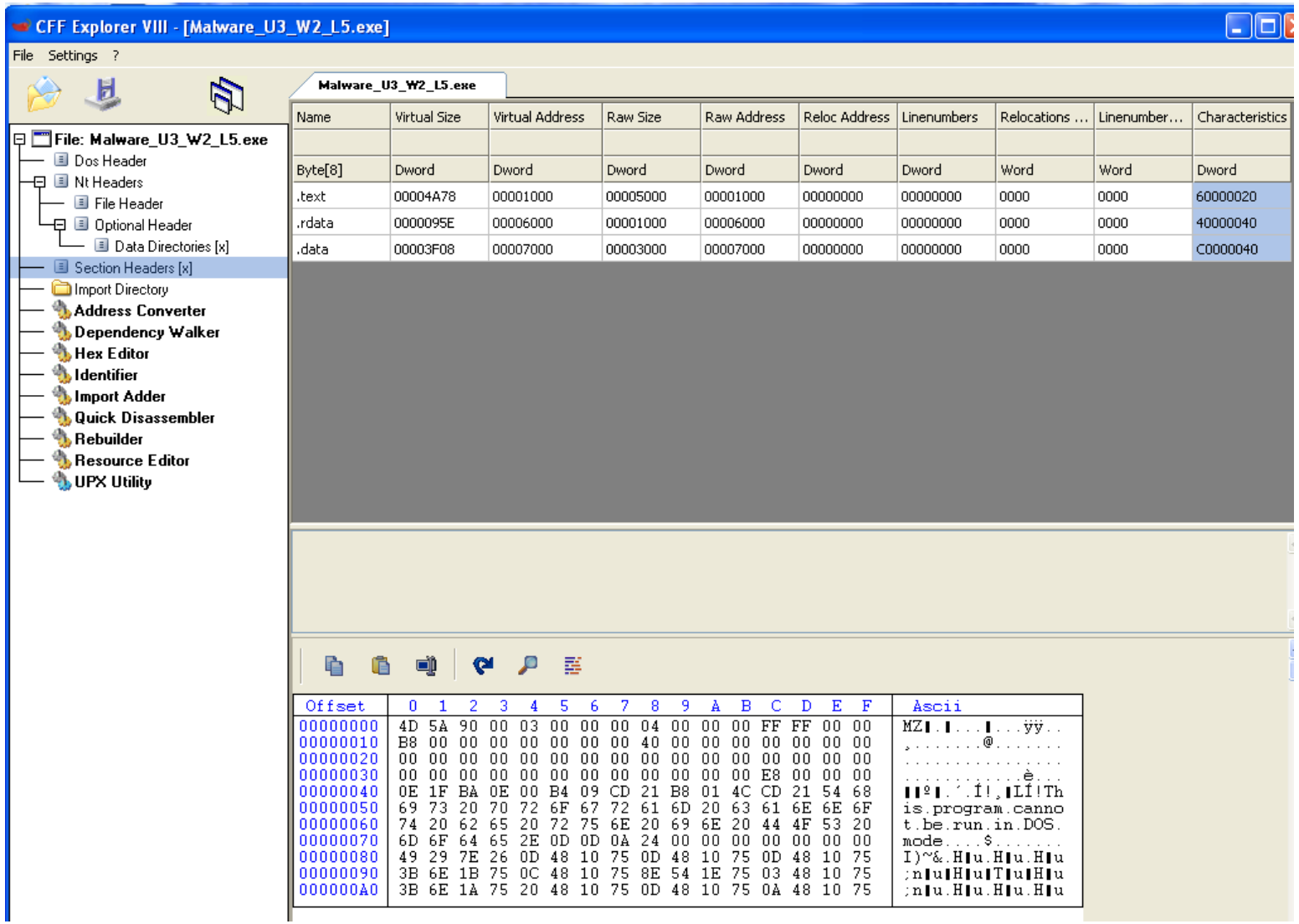


Il secondo punto ci chiede le sezioni di cui si compone il malware , per questo sempre dal menu a sinistra andiamo nella sezione "Section headers",il quale ci mostra le informazioni circa le sezioni di cui si compone l'eseguibile, in questo caso è fromato da tre sezioni .

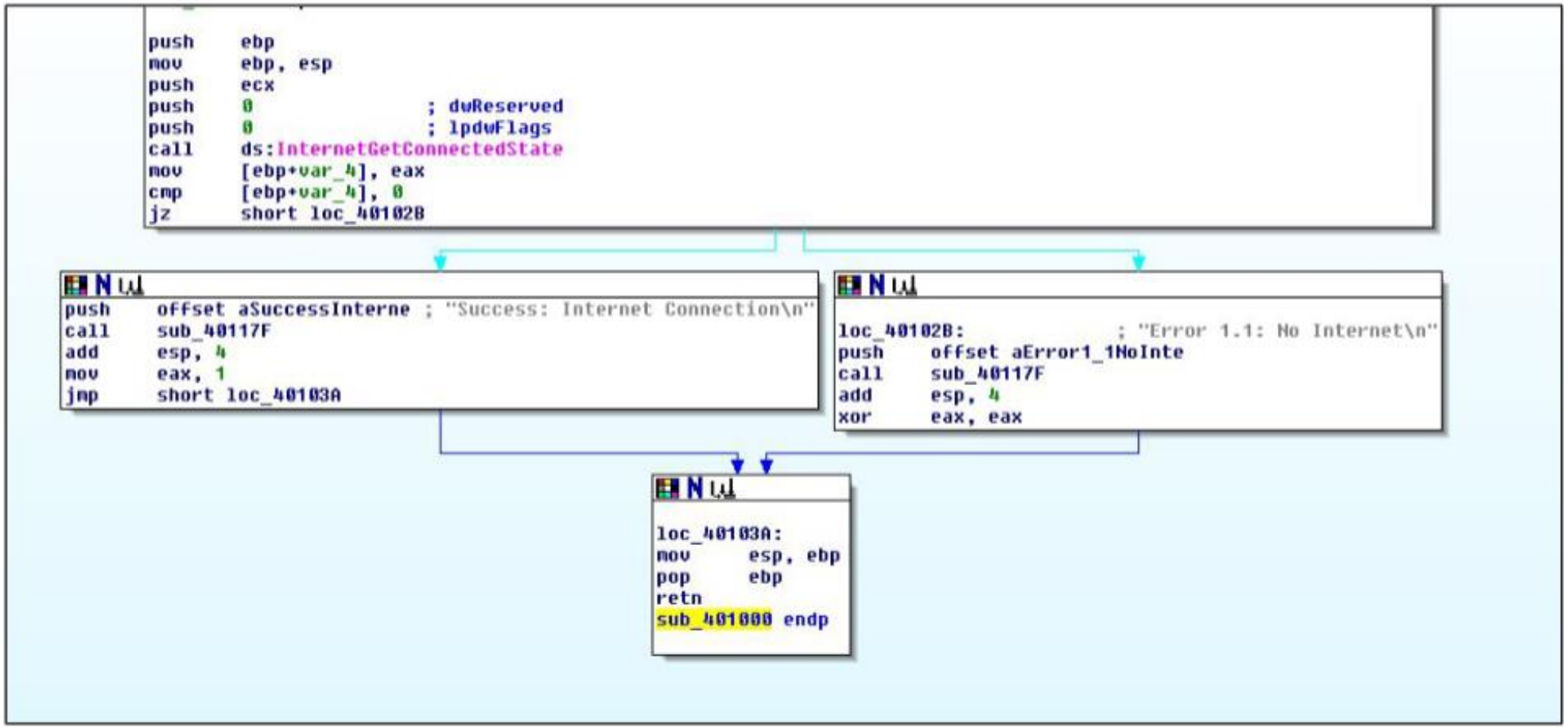
.TEXT - contiene le righe di codice che la CPU eseguira una volta avviato il software

.RDATA - include le informazioni circa le librerie e funzioni importate

.DATA - contiene dati/variabili globali del programma eseguibile.



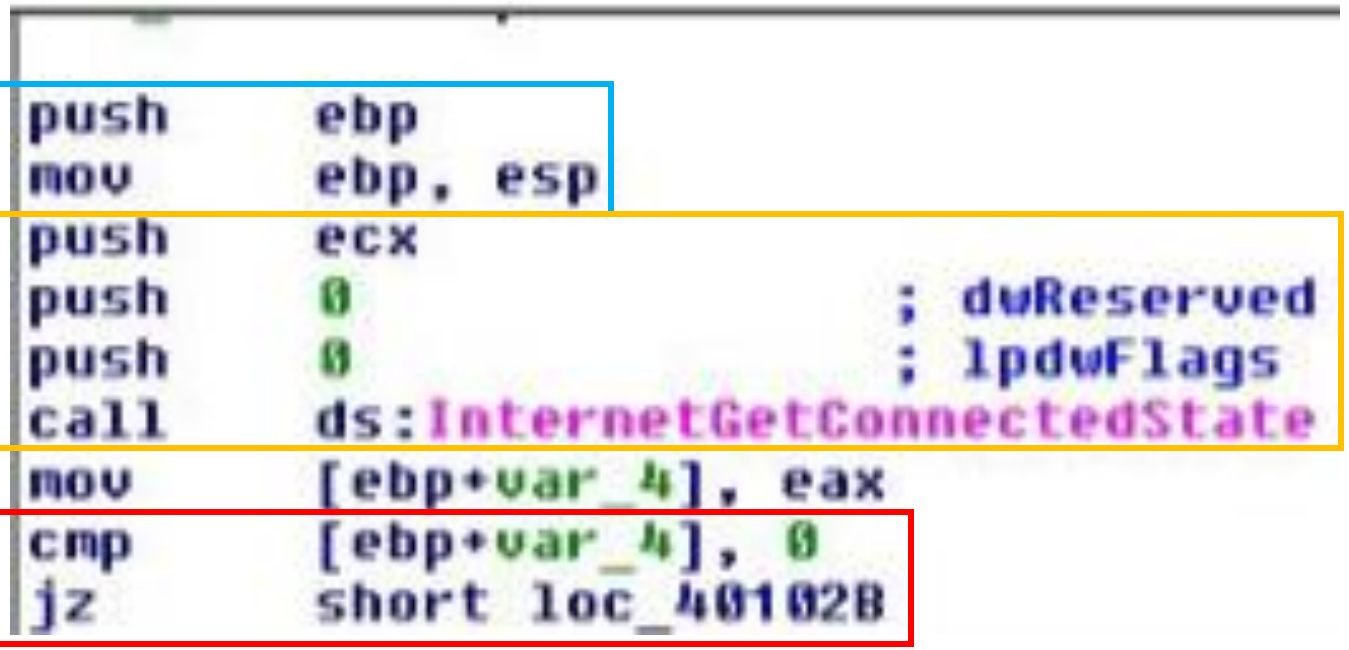
Linguaggio Assembly



Creazione dello stack

Chiamata di funzione. I parametri sono passati sullo stack tramite le istruzioni push

Ciclo IF



Possibili output del ciclo IF, Se il valore di ritorno (return) della funzione è diverso da 0, allora vuol dire che c'è una connessione attiva.

Con il "push of set "ci dice che la connessione a internet è attiva

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

Con il "push of set aError1"ci dice che la connessione non c'è

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

Chiude il ciclo e ripulisce lo stack

```
loc_40103A:
mov     esp, ebp
pop     ebp
retn
sub_401000 endp
```

La funzionalità implementata

Il malware chiama la funzione "internetgetconnectedstate" e ne controlla con un «if» il valore di ritorno. Se il valore di ritorno (return) della funzione è diverso da 0, allora vuol dire che c'è una connessione attiva. Possiamo dunque dedurre che il malware in questione è un downloader perché tenta la connessione a internet per poi scaricare altri malware .