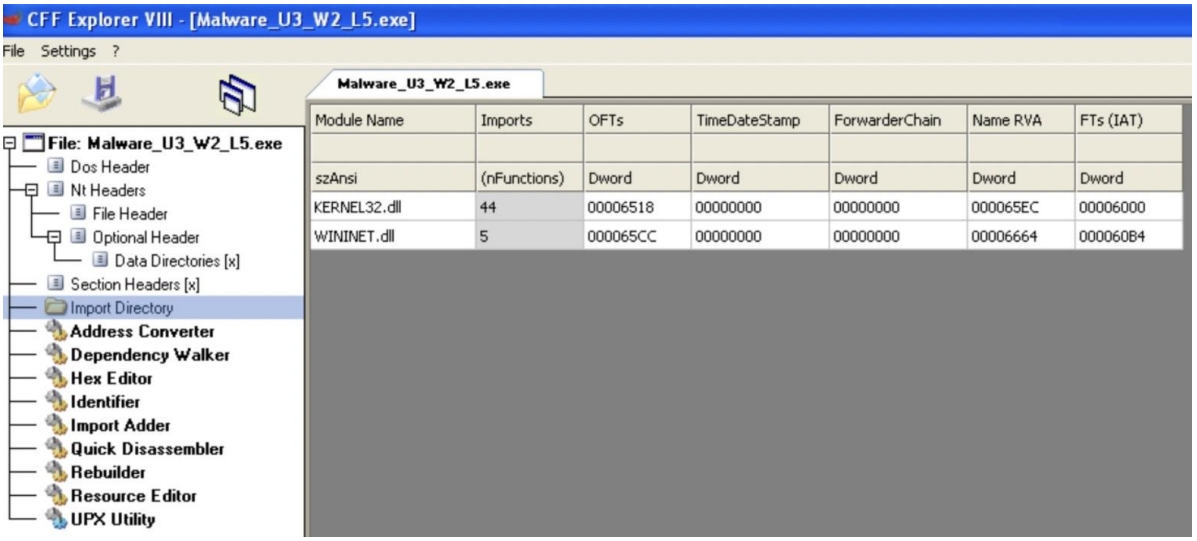
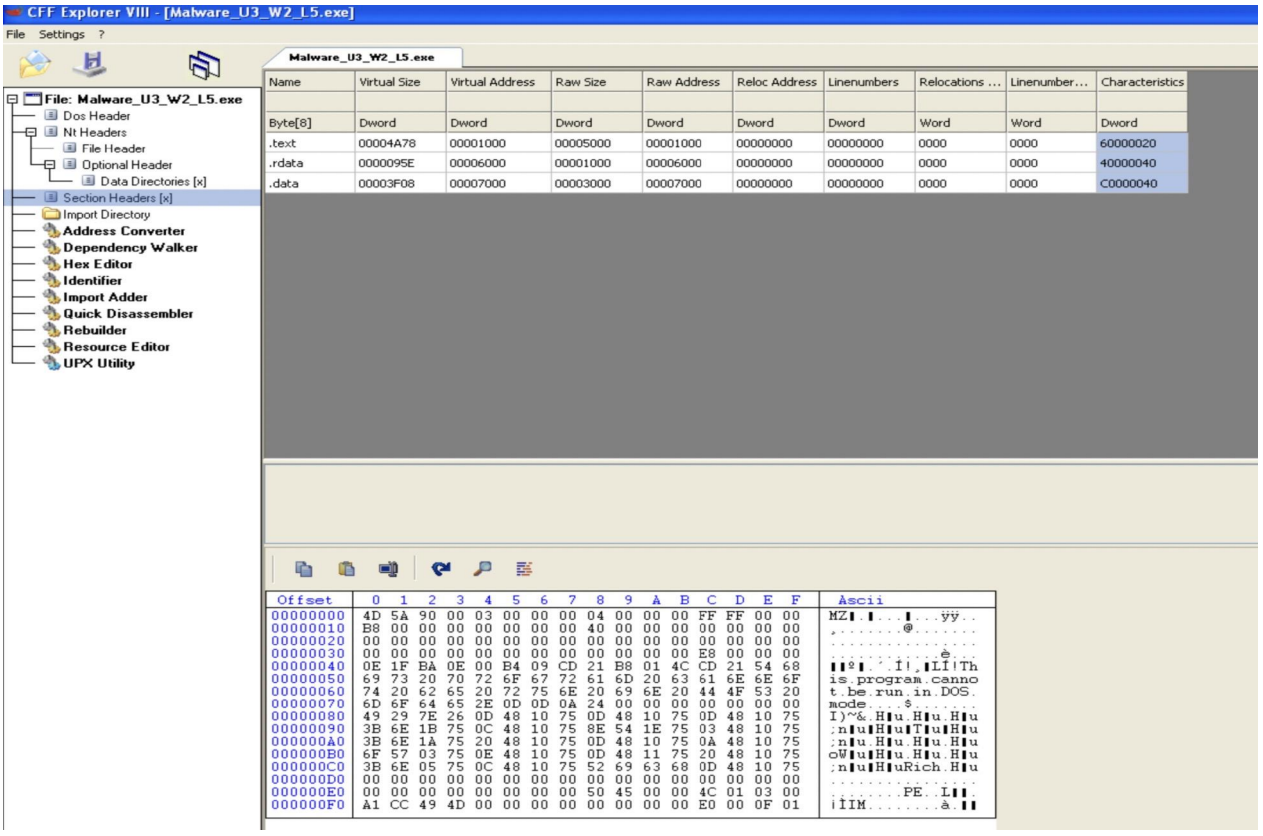
Tramite l'analisi statica basica andiamo a ricavare le informazioni sulle librerie e le sezioni del file PE

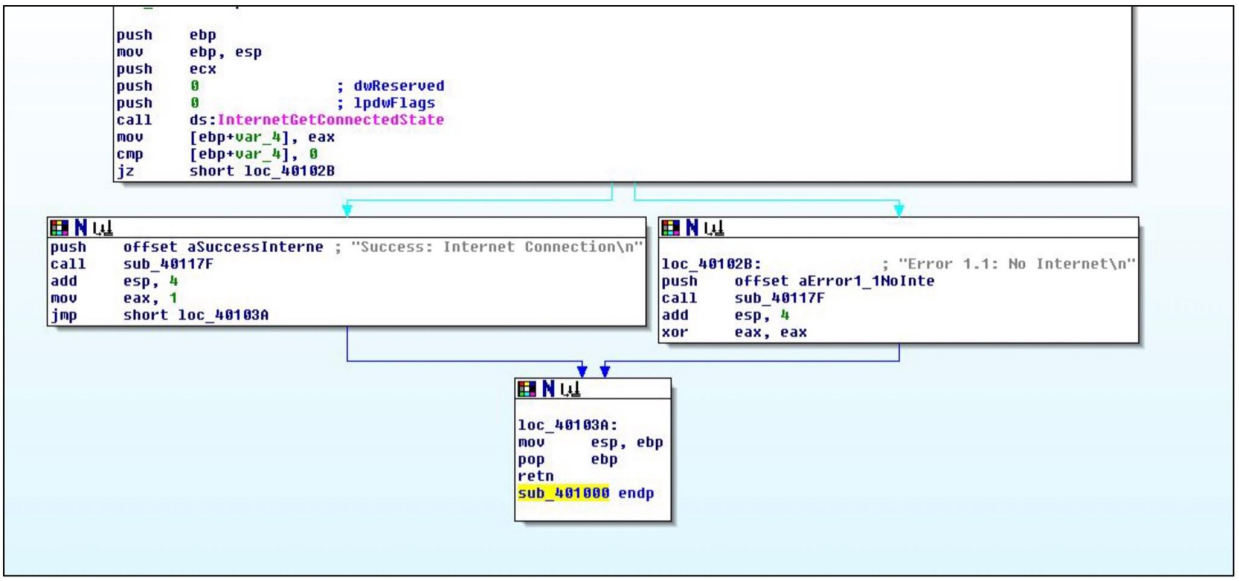


Come possiamo vedere dall'immagine le librerie utilizzate sono le seguenti:

KERNEL32.dll, che contiene le funzioni principali utili ad interagire con il sistema operativo
WININET.dll, che contiene le funzioni per l'utilizzo di alcuni protocolli di rete



Qui possiamo vedere le sezioni del file PE:
.text, contiene il codice che la CPU andrà ad eseguire una volta avviato il malware
.rdata, contiene le info riguardo le librerie è le funzioni da importare ed esportare dall'eseguibile
.data contiene le variabili globali del programma



Istruzioni	Descrizione
Push EBP Mov EBP, ESP	Creazione dello stack
Push ECX Push 0 ;dwReserved Push 0 ;lpdwFlags Call ds: InternetGetConnectedState	Passaggio dei parametri sullo stack tramite istruzioni push

Mov [ebp+var_4], eax
Cmp [ebp+var_4], 0
Jz short loc_40102B
	Ciclo if, se lo ZF è impostato su 1 avverrà il salto

Push offset a SuccessInterne; “Success: Internet Connection\n”
Call sub_40105F
Add esp, 4
Mov eax, 1
Jmp short loc_40103A
	caso 1, lo ZF è pari a 0 perciò la connessione è attiva

loc 40102B :"Error 1.1: No Internet\n' push offset aError1 1NoInte call sub 40117F add esp, 4 xor eax, eax	**caso 2**, lo ZF è pari a 1 perciò la connessione è disattiva
loc 40103A: mov esp, ebp pop ebp retn; sub 401000 endp	**Pulizia dello stack**

Analisi comportamentale

In seguito all'analisi fatte, si può dedurre che il malware andrà ad effettuare un tentativo di connessione ad Internet,
Una probabile motivazione a questo comportamento si può scoprire nel caso il malware cercasse di stabilire una connessione con un sito online per andare a scaricare altri malware in questo caso sarebbe identificato come **downloader**
oppure potrebbe una riuscito a nascondersi dentro il pc vittima, tentare una connessione ad internet ad ogni avvio permettendo il controllo remoto della macchia da parte di malintenzionati