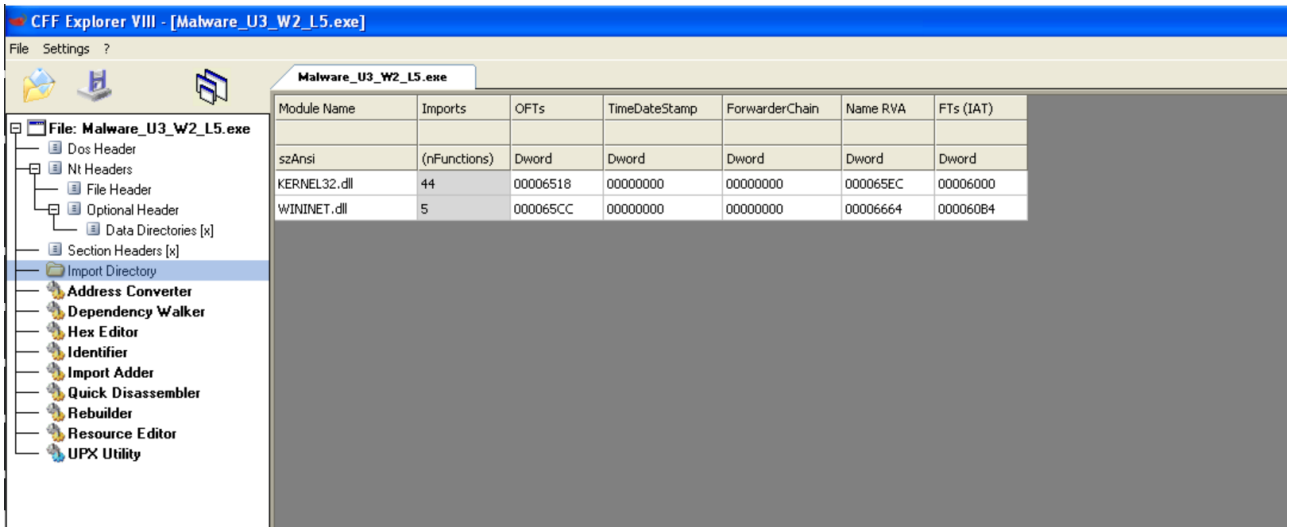
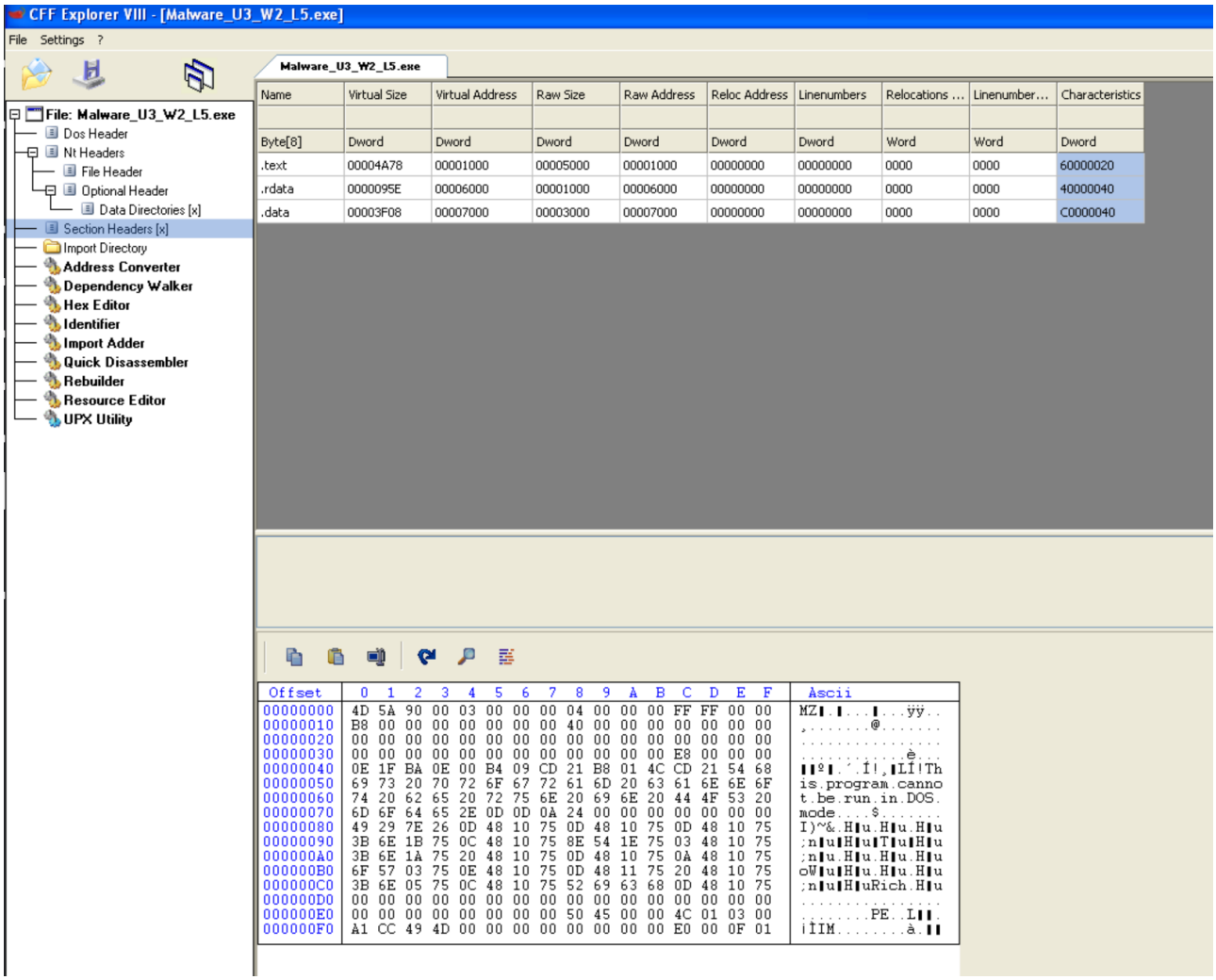
Analisi del malware e Assembly

Per iniziare si ricava le informazioni sulle librerie e le sezioni del file PE tramite l'*analisi statica basica*.



Le librerie utilizzate dal malware sono:

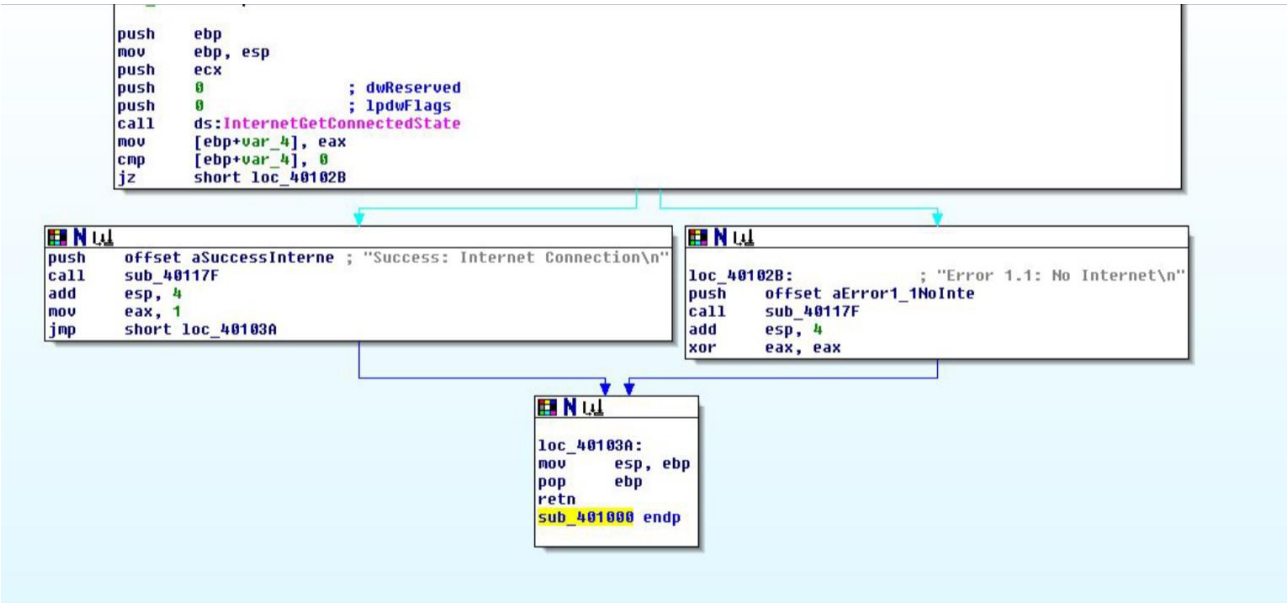
- ***Kernel32.dll***: contiene le funzioni principali per interagire con il sistema operativo.
- ***Wininet.dll***: contiene le funzioni per l'implementazione di alcuni protocolli di rete come http, FTP, NTP.



Le sezioni del file PE sono:

- ***.text***: contiene le righe di codice che la CPU eseguirà una volta che il software sarà avviato.
- ***.rdata***: include le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile.
- ***.data***: contiene dati/variabili globali del programma eseguibile.

Adesso si procede con un approfondimento tramite l'*analisi statica avanzata*.



Macrocategorie:

`push ebp` `mov ebp, esp`	Creazione dello stack

`push ecx`
`push 0 ; dwReserved`
`push 0 ; lpdwFlags`
`call ds:InternetGetConnectedState`
	I parametri sono passati sullo stack tramite le istruzioni push

`cmp [ebp+var_4], 0` `jz short loc_40102B`	Ciclo if, in caso lo ZF sia impostato su 1 allora avverrà il salto

`push offset aSuccessInterne ; "Success: Internet Connection\n"`
`call sub_40117F`
`add esp, 4`
`mov eax, 1`
`jmp short loc_40103A`
	In questo caso, in cui lo ZF è 0, vuol dire che 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`
	In questo caso, in cui lo ZF è 1, vuol dire che la connessione è disattivata

`loc_40103A:`
`mov esp, ebp`
`pop ebp`
`retn`
`sub_401000 endp`
	Rimozione e pulizia dello stack

Analisi comportamentale

Analizzando il malware si può affermare che stia cercando di verificare lo stato della connessione. Perciò si può ipotizzare che l'obiettivo del malware è di essere connesso ad internet e che quindi una delle sue altre funzionalità potrebbe essere

attivare la connessione in caso fosse disattivata; una probabile motivazione a questo comportamento potrebbe essere spiegato in caso il malware cercasse di connettersi ad un sito per scaricare altri malware, perciò sarebbe identificabile come downloader.

Difatti, andando a ricavare il codice hash tramite il tool CFF Explorer e poi inserendolo sul sito VirusTotal si può osservare che le ipotesi sono corrette.