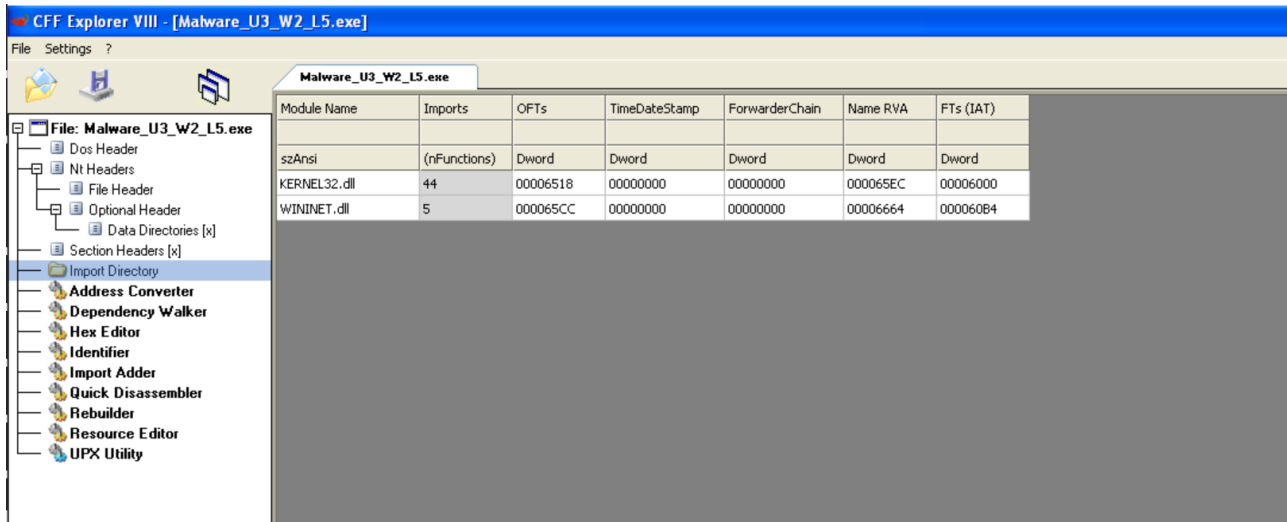


Analisi del malware e Assembly

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.

CFF Explorer VIII - [Malware_U3_W2_L5.exe]

File Settings ?

Malware_U3_W2_L5.exe

File: Malware_U3_W2_L5.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Addr
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F Ascii

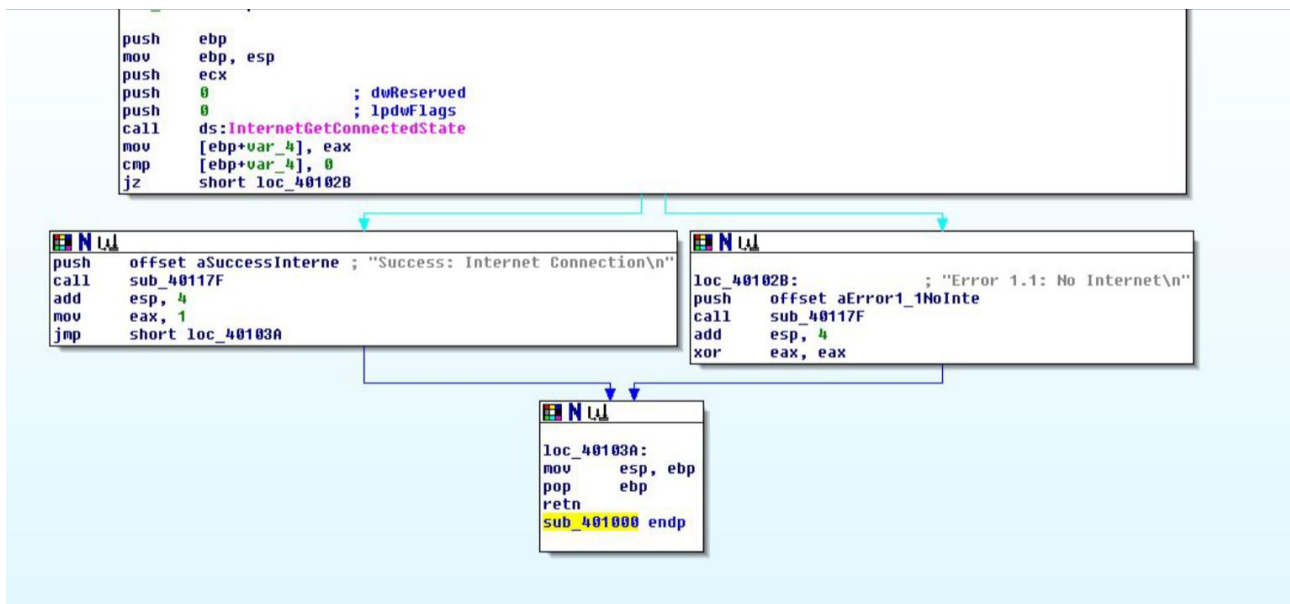
```

00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ|...|...yy..
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00000030 00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00 .....e.....
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 |||I.I!|LI!Th
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t.be.run.in.DOS.
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode...$.
00000080 49 29 7E 26 0D 48 10 75 0D 48 10 75 0D 48 10 75 I)~&.Hu.Hu.Hu
00000090 3B 6E 1B 75 0C 48 10 75 8E 54 1E 75 03 48 10 75 ;ntuHu!Tu!Hu
000000A0 3B 6E 1A 75 20 48 10 75 0D 48 10 75 0A 48 10 75 ;ntu.Hu.Hu.Hu
000000B0 6F 57 03 75 0E 48 10 75 0D 48 11 75 20 48 10 75 oWtuHu.Hu.Hu
000000C0 3B 6E 05 75 0C 48 10 75 52 69 63 68 0D 48 10 75 ;ntuHuRich.Hu
000000D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000000E0 00 00 00 00 00 00 00 00 50 45 00 00 4C 01 03 00 .....PE.L||
000000F0 A1 CC 49 4D 00 00 00 00 00 00 00 00 E0 00 0F 01 |IIX.....&.||
  
```

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:

<pre> push ebp mov ebp, esp </pre>	Creazione dello stack
<pre> push ecx push 0 ; dwReserved push 0 ; lpdwFlags call ds:InternetGetConnectedState cmp [ebp+var_4], 0 jz short loc_40102B </pre>	<p>I parametri sono passati sullo stack tramite le istruzioni push</p> <p>Ciclo if, in caso lo ZF sia impostato su 1 allora avverrà il salto</p>
<pre> push offset aSuccessInterne ; "Success: Internet Connection\n" call sub_40117F add esp, 4 mov eax, 1 jmp short loc_40103A </pre>	In questo caso, in cui lo ZF è 0, vuol dire che la connessione è attiva
<pre> loc_40102B: push offset aError1_1NoInte call sub_40117F add esp, 4 xor eax, eax </pre>	In questo caso, in cui lo ZF è 1, vuol dire che la connessione è disattivata
<pre> loc_40103A: mov esp, ebp pop ebp retn sub_401000 endp </pre>	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.