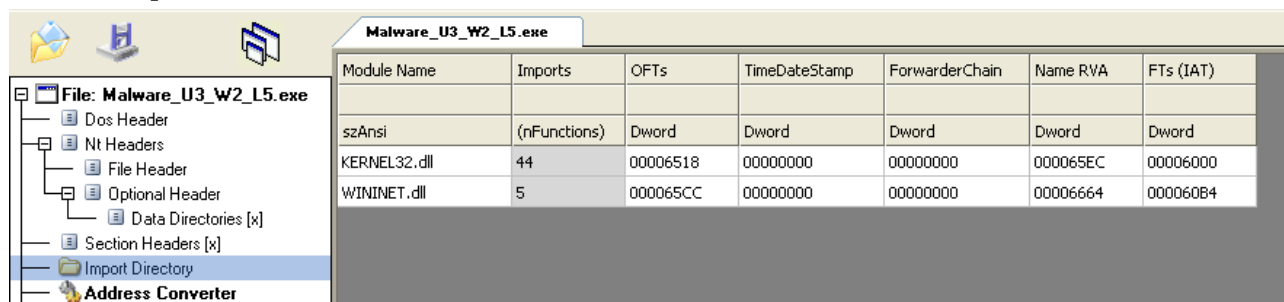


Per trovare le librerie importate apriamo il malware con cff explorer e andiamo sulla sezione “import directory” dove troviamo le librerie che il malware importa.

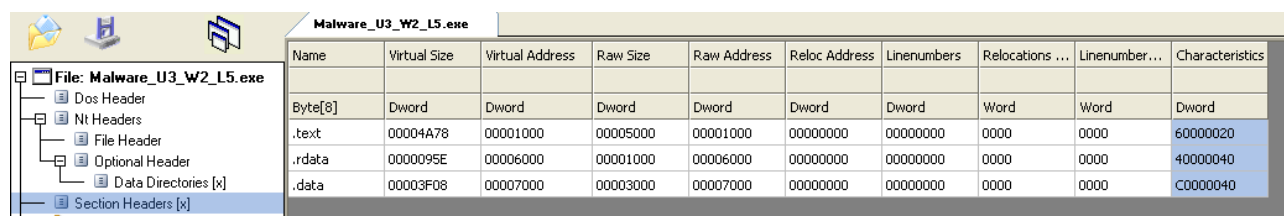
kernel32.dll: è il Microsoft Windows Kernel più importante. La funzionalità che richiama la maggior parte delle funzioni delle finestre è collegata a questo DLL del nocciolo in qualche modo.

wininet.dll è un modulo che contiene le funzioni Internet-relative usate dalle applicazioni di Windows. Nota: wininet.dll è un processo che il Trojan di Troj/Zlob-AO prova a travestire in se come nell'ambito di vero nome trattato di %systemroot% \ mscornet.exe. Questo processo è un rischio per la sicurezza e dovrebbe essere rimosso dal vostro sistema.



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

Per trovare le sezione dobbiamo spostarci su “section headers”



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

.text: la sezioni text contiene le istruzioni che la cpu eseguirà una volta che il software sarà avviato.

.rdata: la sezione rdata include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile, informazione che possiamo ricavare con cff explorer.

.data: la sezione data contiene tipicamente i dati / le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Chiamando la funzione `InternetGetConnectedState()` della libreria `wininet.dll` di Windows. Questa funzione viene utilizzata per verificare la connessione a Internet. Dopo aver chiamato questa funzione, il codice compara il valore restituito con 0 e salta a `loc_40102b` se il valore è uguale a 0.

```
push    ebp
mov     ebp, esp
push    ecx
push    0          ; dwReserved
push    0          ; lpdwFlags
call    ds:InternetGetConnectedState
mov     [ebp+var_4], eax
cmp     [ebp+var_4], 0
jz      short loc_40102B
```

Se il valore restituito è diverso da 0, allora il codice salta a `loc_40103a` e imposta il registro `eax` a 1. Questo potrebbe significare che la connessione a Internet è stata verificata con successo e il codice sta continuando con la sua esecuzione normale.

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

D'altra parte, se il valore restituito è uguale a 0, il codice salta a `loc_40102b` e stampa un messaggio di errore "error 1.1: no internet" utilizzando la funzione `sub_40117f()`. In questo caso, il registro `eax` viene azzerato (`XOR eax, eax`). Ciò potrebbe significare che il codice sta gestendo un errore di connessione a Internet e sta interrompendo la sua esecuzione.

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

La prima istruzione, "`mov esp, ebp`", ripristina il puntatore dello stack (ESP) al valore che aveva prima dell'inizio della funzione, eliminando così gli elementi dello stack creati durante l'esecuzione della funzione.

La successiva istruzione "`pop ebp`" ripristina il registro EBP al valore che aveva prima dell'inizio della funzione. Questo è importante poiché EBP viene utilizzato come puntatore di base per accedere ai parametri e alle variabili locali della funzione. Infine, l'istruzione "`retn`" restituisce il controllo al chiamante della funzione, saltando all'indirizzo di ritorno salvato nello stack.

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

