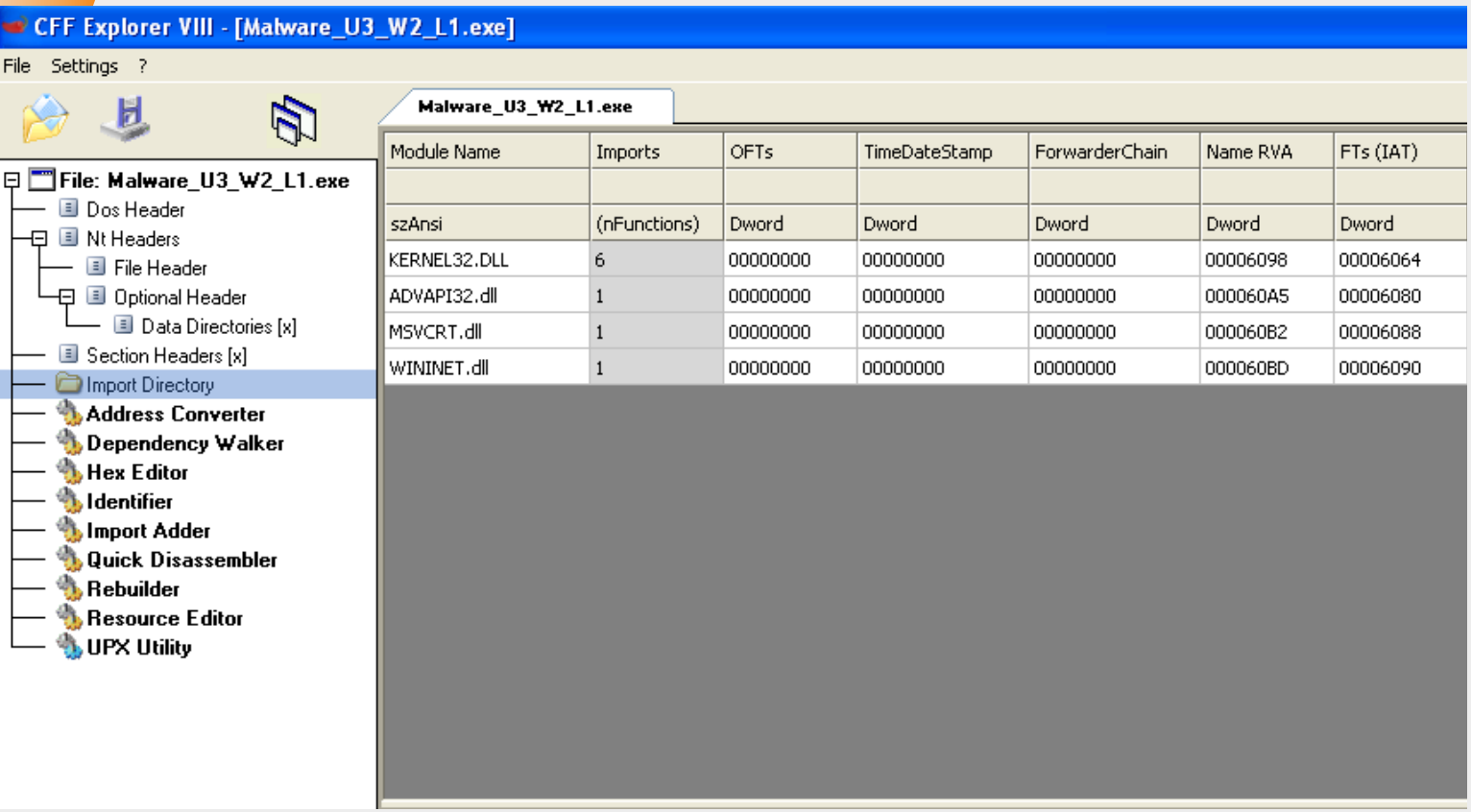
Traccia:

Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse
- Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte



Utilizzando **CFF Explorer** analizziamo librerie e funzioni importate dall'eseguibile che stiamo analizzando

Le librerie richiamate sono:

- kernel32.dll
- advapi32.dll
- wininet32.dll
- msvcrt.dll

Approfondimento:
DLL

un "Dynamic Link Library" o DLL è un tipo di file eseguibile in ambiente Windows che contiene codice e dati che possono essere utilizzati da più programmi contemporaneamente.

A differenza di un'applicazione autonoma, una DLL non può essere eseguita direttamente, ma fornisce funzionalità condivise che possono essere richiamate da diverse applicazioni.

***kernel32.dll*:**

- Fornisce funzioni di basso livello che gestiscono memoria, file, processi e altri aspetti fondamentali del sistema operativo.
- Include funzioni per la gestione dei processi, sincronizzazione, allocazione di memoria e la gestione delle eccezioni.
- È una delle DLL principali di Windows e molte altre DLL fanno riferimento a sue funzioni

***advapi32.dll*:**

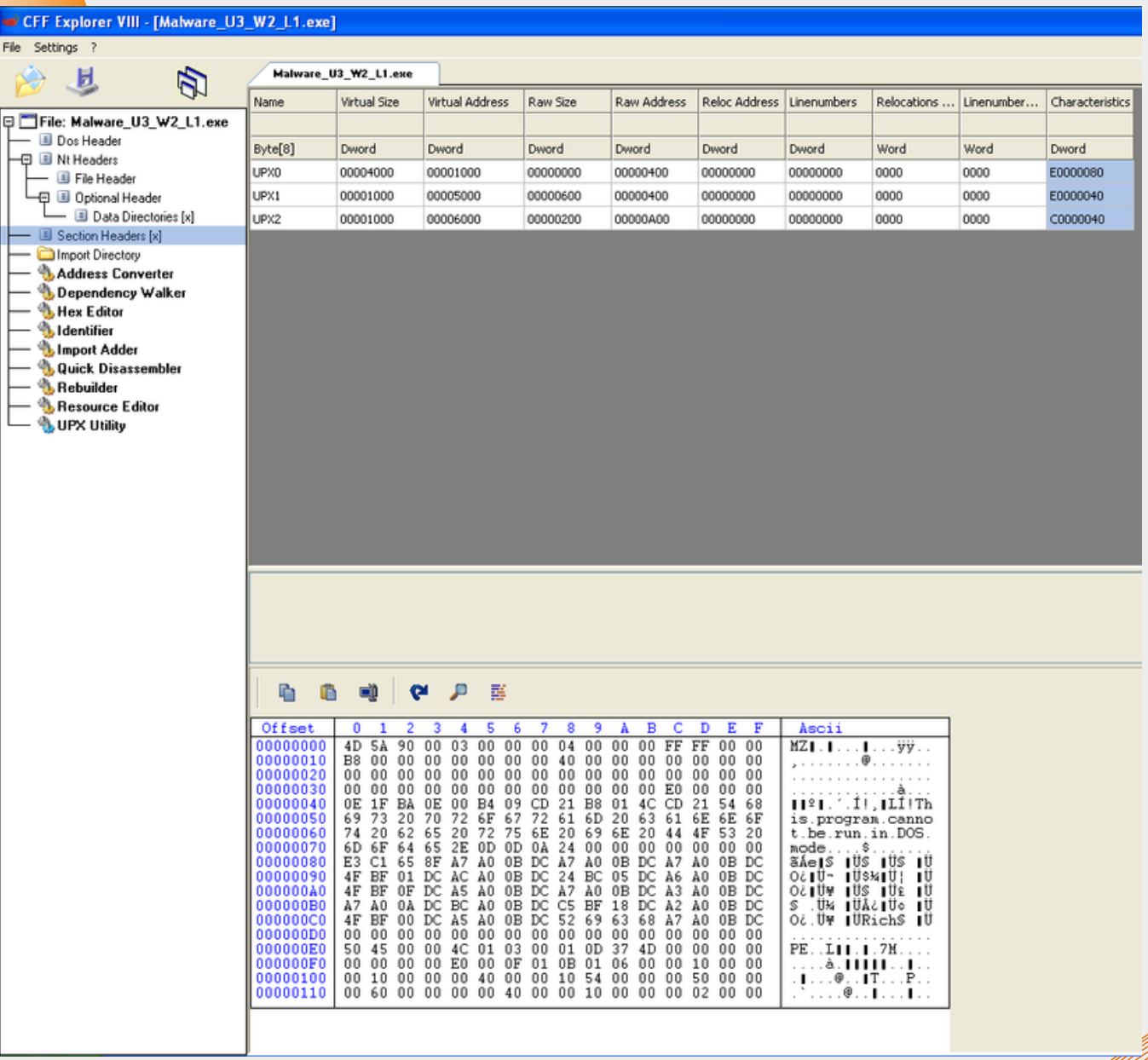
- Contiene funzioni per la gestione dei servizi, la sicurezza e le operazioni relative al registro di sistema.
- Fornisce un'interfaccia per interagire con il sottosistema di sicurezza di Windows.
- Include funzionalità per la gestione degli account utente, l'accesso alle informazioni sul sistema e la manipolazione del registro di sistema.

***wininet.dll*:**

- Offre funzioni per la gestione delle operazioni di rete, inclusi protocolli come HTTP, FTP e altri.
- È coinvolta nella gestione delle connessioni Internet e fornisce un'interfaccia per le operazioni di navigazione e download.
- Utilizzata da molti programmi per interagire con il Web e le risorse Internet.

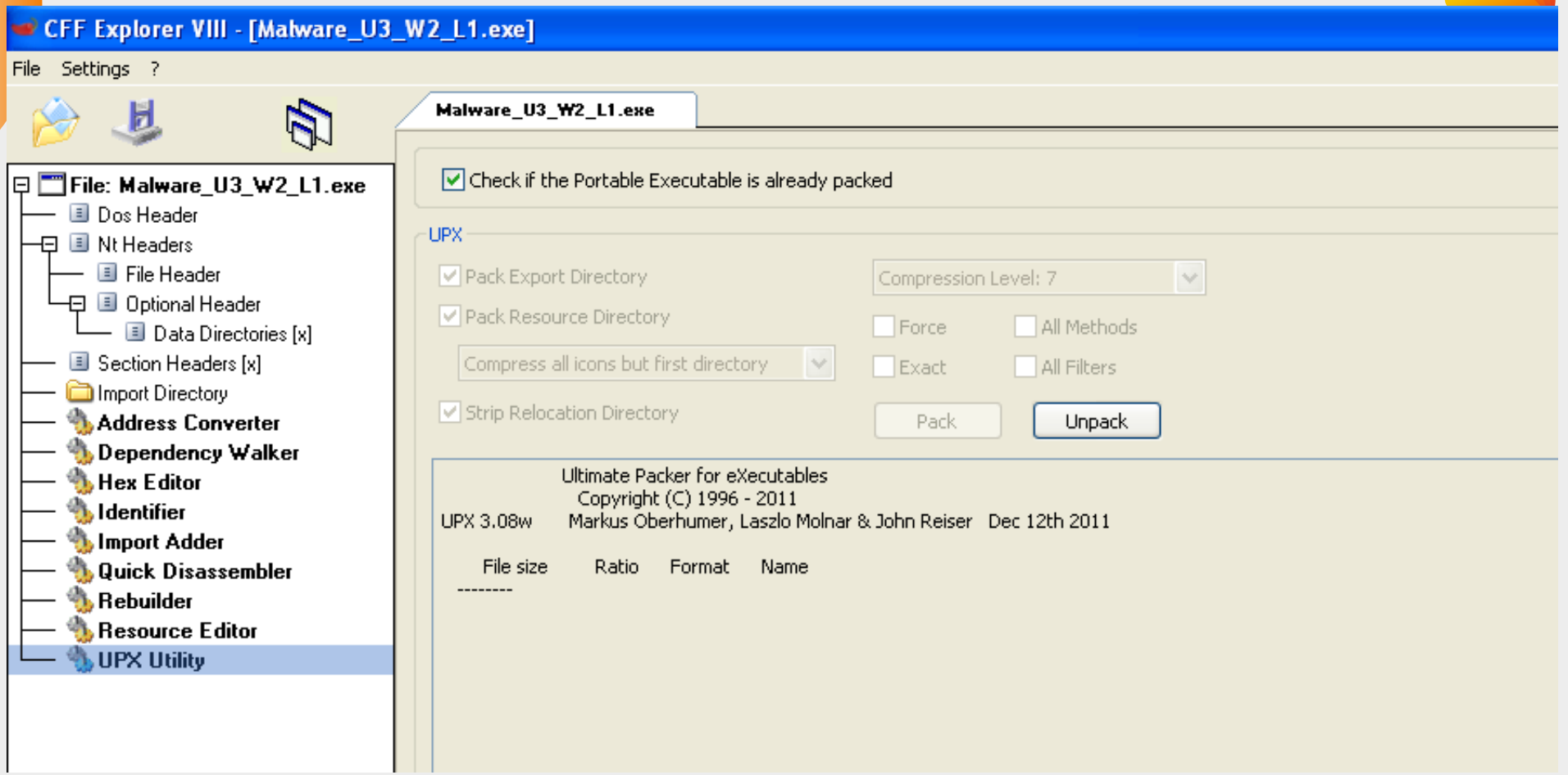
***MSVCRT.dll*:**

- La libreria di runtime di Microsoft Visual C++, che fornisce funzioni standard del linguaggio C.
- Contiene implementazioni delle funzioni standard della libreria C come quelle per la gestione della memoria, le stringhe, l'input/output e altre operazioni di base.
- È essenziale per l'esecuzione di programmi scritti in linguaggio C++ che utilizzano il compilatore Microsoft Visual C++.

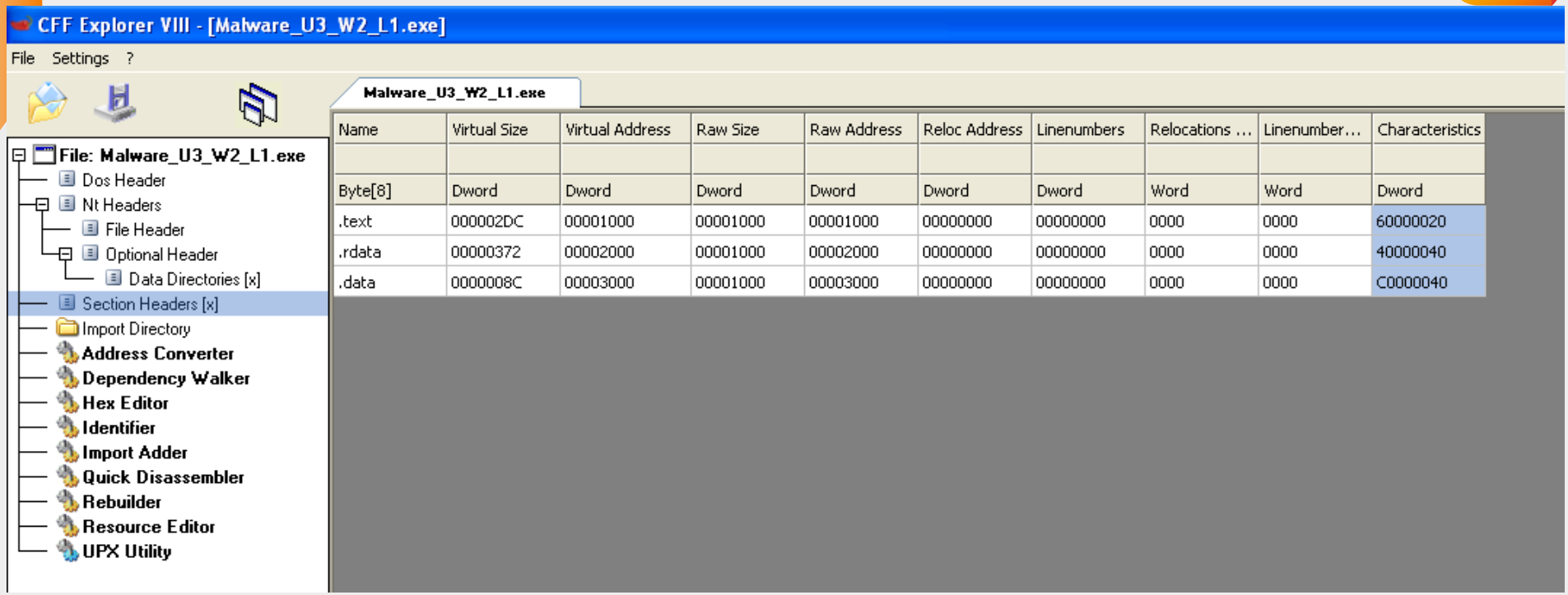


Con lo stesso tool possiamo continuare con l'analisi delle sezioni che compongono il malware

Le sezioni sono state compresse utilizzando il tool UPX, che comprime gli eseguibili rendendo inaccessibile il formato PE della sezione.



Per ovviare a questo problema, utilizziamo la funzione UPX utility per decomprimere il PE tramite il tasto “unpack”



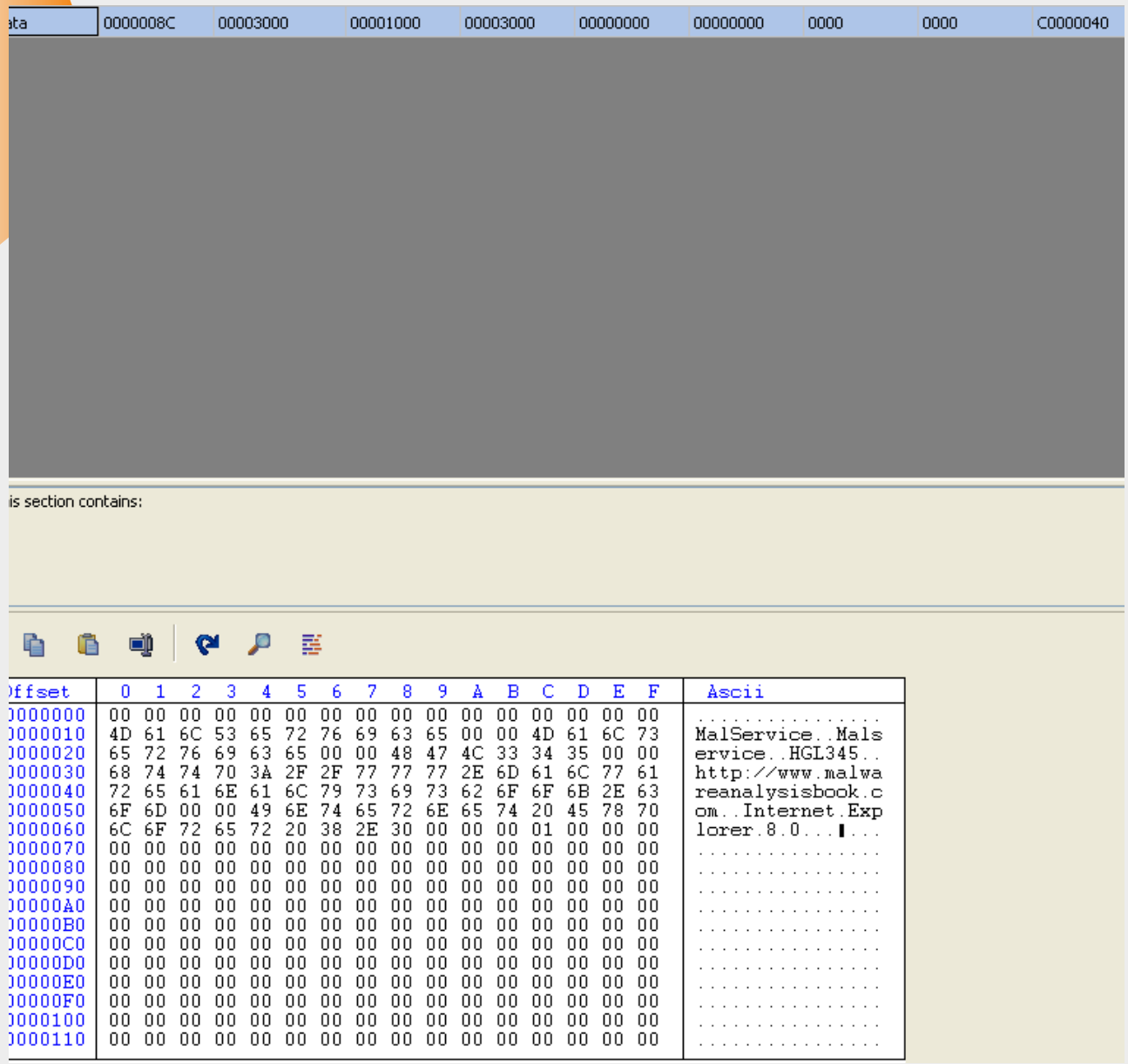
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000002DC	00001000	00001000	00001000	00000000	00000000	0000	0000	60000020
.rdata	00000372	00002000	00001000	00002000	00000000	00000000	0000	0000	40000040
.data	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000	C0000040

Tornando alla sezione “section headers” possiamo procedere ad analizzare le sezioni trovate:

.text: La sezione "text" comprende le istruzioni, ovvero le linee di codice, che la CPU eseguirà una volta avviato il software. Di solito, questa è l'unica sezione di un file eseguibile che la CPU esegue, poiché tutte le altre sezioni contengono dati o informazioni di supporto.

.rdata: La sezione "rdata" contiene informazioni sulle librerie e sulle funzioni importate o esportate dall'eseguibile.

.data: La sezione "data" contiene i dati o le variabili globali del programma eseguibile. Si noti che una variabile viene considerata globale quando non è definita all'interno del contesto di una funzione, ma è dichiarata globalmente e, di conseguenza, è accessibile da qualsiasi funzione dell'eseguibile.



ata	0000008C	00003000	00001000	00003000	00000000	00000000	0000	0000	C0000040

is section contains:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
0000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000010	4D	61	6C	53	65	72	76	69	63	65	00	00	4D	61	6C	73	MalService..Mals
0000020	65	72	76	69	63	65	00	00	48	47	4C	33	34	35	00	00	ervice..HGL345..
0000030	68	74	74	70	3A	2F	2F	77	77	77	2E	6D	61	6C	77	61	http://www.malwa
0000040	72	65	61	6E	61	6C	79	73	69	73	62	6F	6F	6B	2E	63	reanalysisbook.c
0000050	6F	6D	00	00	49	6E	74	65	72	6E	65	74	20	45	78	70	om..Internet.Exp
0000060	6C	6F	72	65	72	20	38	2E	30	00	00	00	01	00	00	00	lorer.8.0...▌...
0000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
0000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....

analizzando ogni sezione, ci rendiamo conto che .text e .rdata sono crittate e indecifrabili, tuttavia abbiamo scoperto tramite .data che il malware si connette, dopo aver creato un servizio “MalService HGL345”, all’url “http://www.malwareanalysisbook.com”