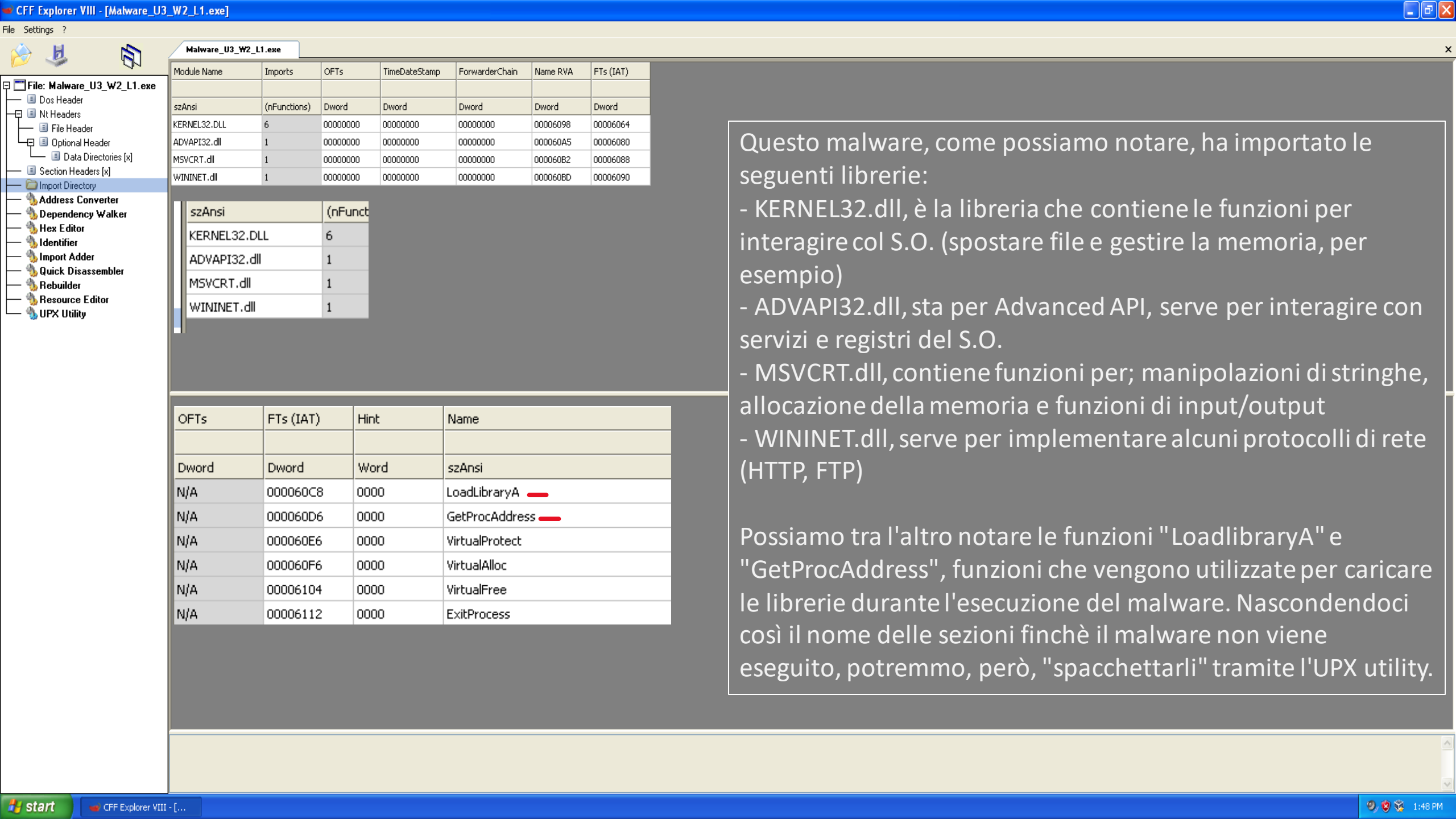


Questo malware, come possiamo notare, ha importato le seguenti librerie:

- KERNEL32.dll, è la libreria che contiene le funzioni per interagire col S.O. (spostare file e gestire la memoria, per esempio)
- ADVAPI32.dll, sta per Advanced API, serve per interagire con servizi e registri del S.O.
- MSVCRT.dll, contiene funzioni per; manipolazioni di stringhe, allocazione della memoria e funzioni di input/output
- WININET.dll, serve per implementare alcuni protocolli di rete (HTTP, FTP)

Possiamo tra l'altro notare le funzioni "LoadlibraryA" e "GetProcAddress", funzioni che vengono utilizzate per caricare le librerie durante l'esecuzione del malware. Nascondendoci così il nome delle sezioni finchè il malware non viene eseguito, potremmo, però, "spacchettarli" tramite l'UPX utility.

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

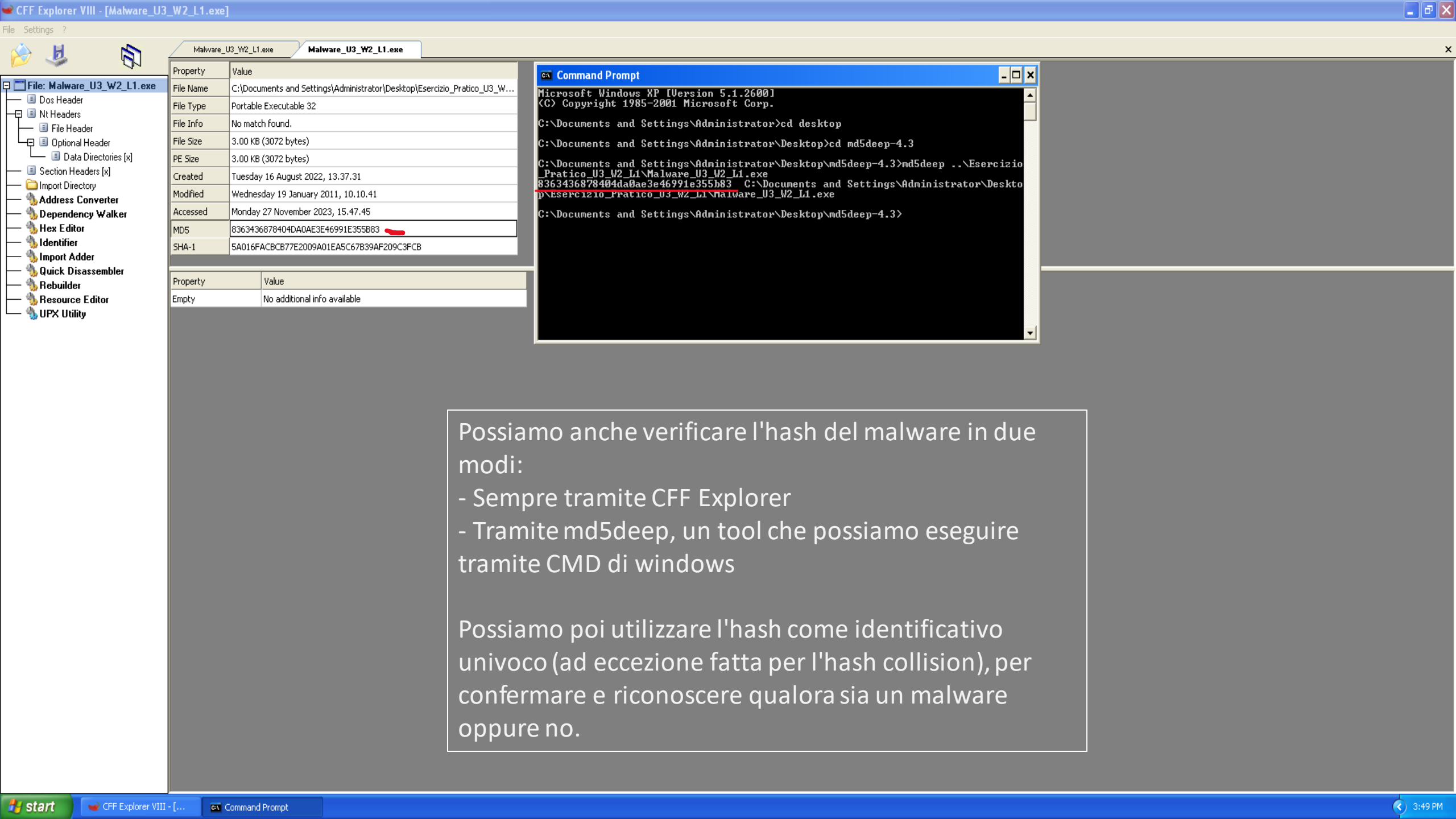
- File: Malware_U3_W2_L1.exe
  - Dos Header
  - Nt Headers
    - File Header
    - Optional Header
      - Data Directories [x]
  - Section Headers [x]
  - Import Directory
  - Address Converter
  - Dependency Walker
  - Hex Editor
  - Identifier
  - Import Adder
  - Quick Disassembler
  - Rebuilder
  - 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	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

Come possiamo notare le sezioni sono adesso visibili, andiamole ad esaminare:
- .text, contiene le istruzioni che la CPU andrà ad eseguire ogni volta che il programma verrà avviato.
- .rdata, include tutte le informazioni e le librerie importate/esportate dal programma.
- .data, include i dati e le variabili a cui il programma deve "attingere" in qualsiasi situazione.

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▮.▮...▮...ÿÿ..
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	E0	00	00	00	............à...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	▮▮º▮.´.Í!¸▮LÍ!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....$.......
00000080	E3	C1	65	8F	A7	A0	0B	DC	A7	A0	0B	DC	A7	A0	0B	DC	ãÁe▮§ ▮Ü§ ▮Ü§ ▮Ü
00000090	4F	BF	01	DC	AC	A0	0B	DC	24	BC	05	DC	A6	A0	0B	DC	O¿▮Ü¬ ▮Ü$¼▮Ü¦ ▮Ü
000000A0	4F	BF	0F	DC	A5	A0	0B	DC	A7	A0	0B	DC	A3	A0	0B	DC	O¿▮Ü¥ ▮Ü§ ▮Ü£ ▮Ü
000000B0	A7	A0	0A	DC	BC	A0	0B	DC	C5	BF	18	DC	A2	A0	0B	DC	§ .Ü¼ ▮ÜÅ¿▮Ü¢ ▮Ü
000000C0	4F	BF	00	DC	A5	A0	0B	DC	52	69	63	68	A7	A0	0B	DC	O¿.Ü¥ ▮URich§ ▮Ü
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000000E0	50	45	00	00	4C	01	03	00	01	0D	37	4D	00	00	00	00	PE..L▮▮.▮.7M....
000000F0	00	00	00	00	E0	00	0F	01	0B	01	06	00	00	10	00	00	....à.▮▮▮▮..▮...
00000100	00	20	00	00	00	00	00	00	90	11	00	00	00	10	00	00	....▮▮...▮..
00000110	00	20	00	00	00	00	40	00	00	10	00	00	00	10	00	00	..... @..▮...▮..
00000120	04	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00	▮.......▮.......

start | CFF Explorer VIII - [... | Command Prompt | 4:29



Possiamo anche verificare l'hash del malware in due modi:

- Sempre tramite CFF Explorer
- Tramite md5deep, un tool che possiamo eseguire tramite CMD di windows

Possiamo poi utilizzare l'hash come identificativo univoco (ad eccezione fatta per l'hash collision), per confermare e riconoscere qualora sia un malware oppure no.