

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 Addr

Quick Disassembler

Rebuilder

Resource Editor

UPX Utility

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000	00006098	00006064
ADVAPI32.dll	1	00000000	00000000	00000000	000060A5	00006080
MSVCRT.dll	1	00000000	00000000	00000000	000060B2	00006088
WININET.dll	1	00000000	00000000	00000000	000060BD	00006090

szAnsi

(nFunctions)

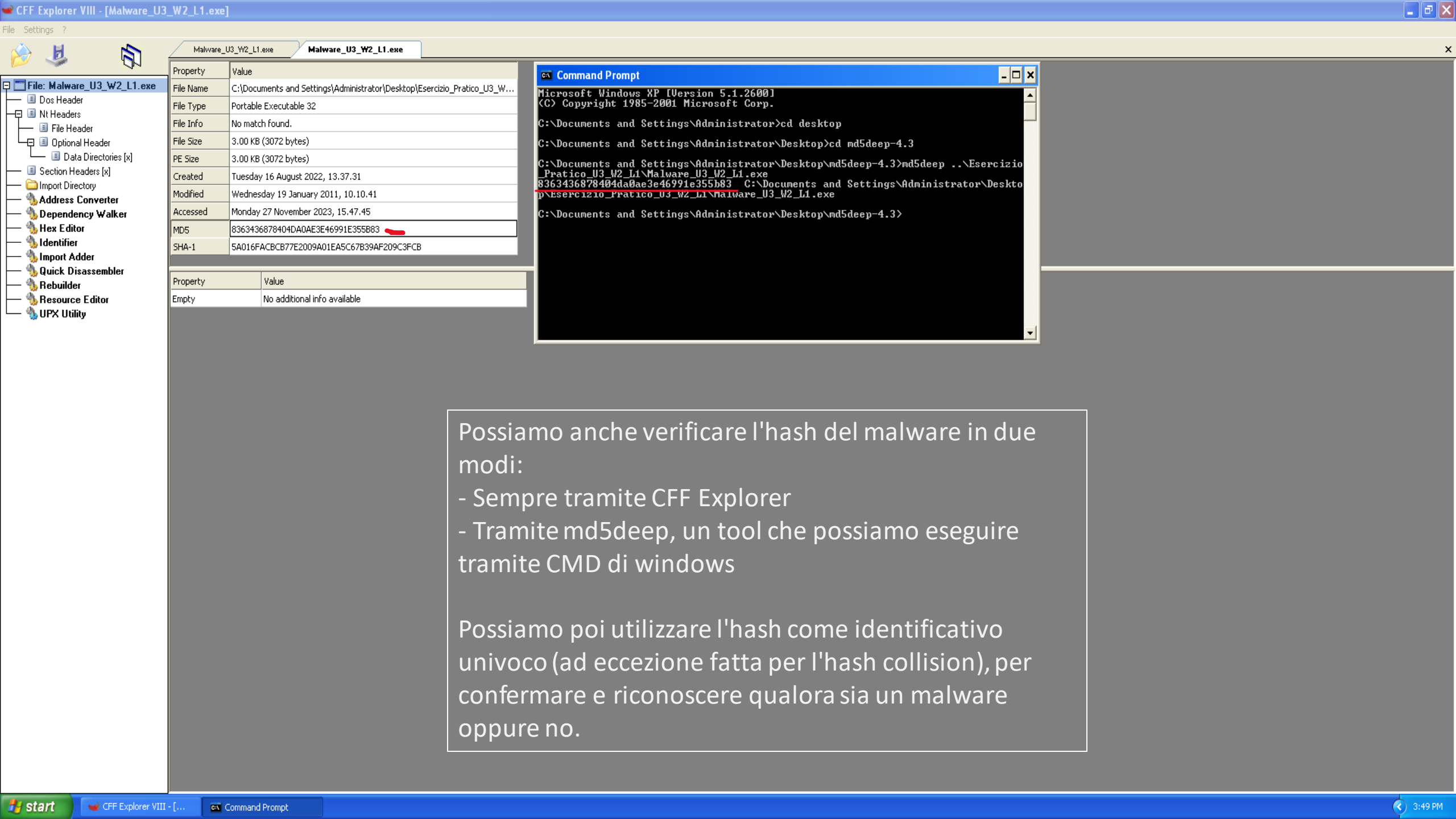
KERNEL32.DLL	6
ADVAPI32.dll	1
MSVCRT.dll	1
WININET.dll	1

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	000060C8	0000	LoadLibraryA
N/A	000060D6	0000	GetProcAddress
N/A	000060E6	0000	VirtualProtect
N/A	000060F6	0000	VirtualAlloc
N/A	00006104	0000	VirtualFree
N/A	00006112	0000	ExitProcess

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



Property	Value
File Name	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W...
File Type	Portable Executable 32
File Info	No match found.
File Size	3.00 KB (3072 bytes)
PE Size	3.00 KB (3072 bytes)
Created	Tuesday 16 August 2022, 13.37.31
Modified	Wednesday 19 January 2011, 10.10.41
Accessed	Monday 27 November 2023, 15.47.45
MD5	8363436878404DA0AE3E46991E355B83
SHA-1	5A016FACBCB77E2009A01EA5C67B39AF209C3FCB
Property	Value
Empty	No additional info available

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd desktop
C:\Documents and Settings\Administrator\Desktop>cd md5deep-4.3
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>md5deep ..\Esercizio
_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe
8363436878404da0ae3e46991e355b83  C:\Documents and Settings\Administrator\Deskt
o\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>
```

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.