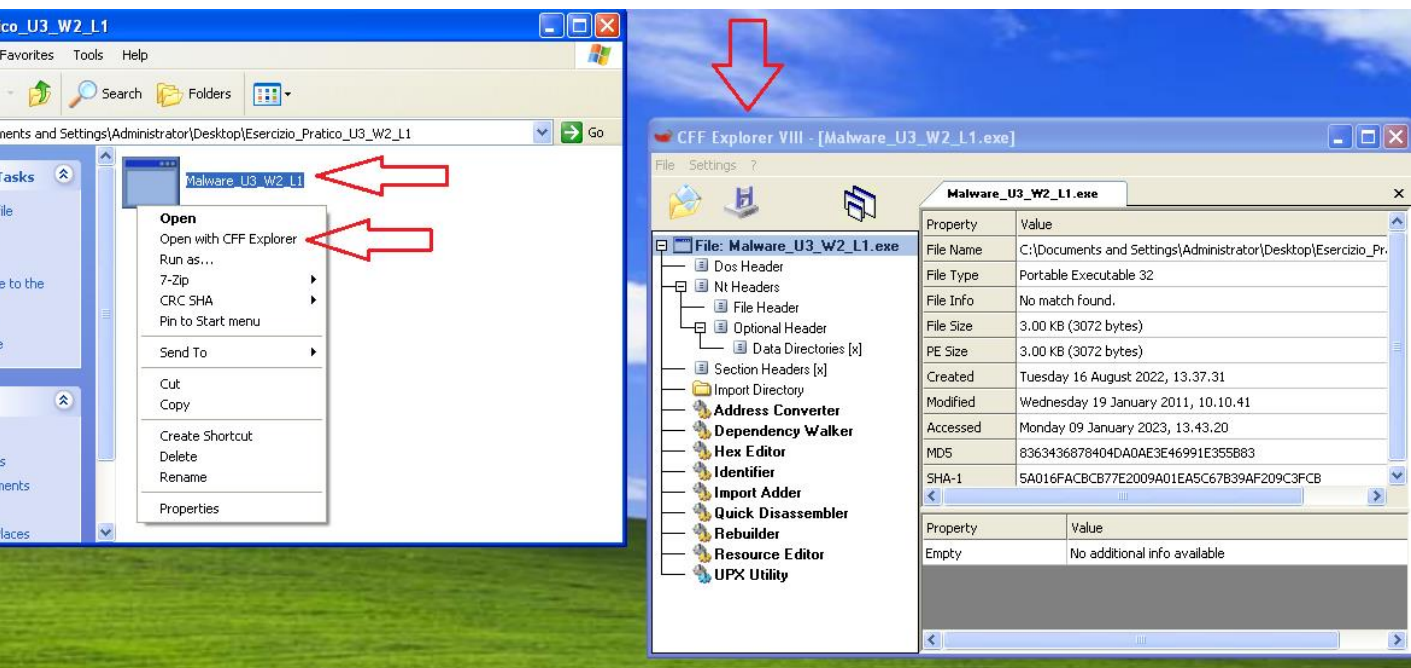


# Descrizione esercizio

- Indicare le librerie importate dal Malware e descriverle
- Indicare le sezioni di cui si compone il malware e descriverle
- Considerazione

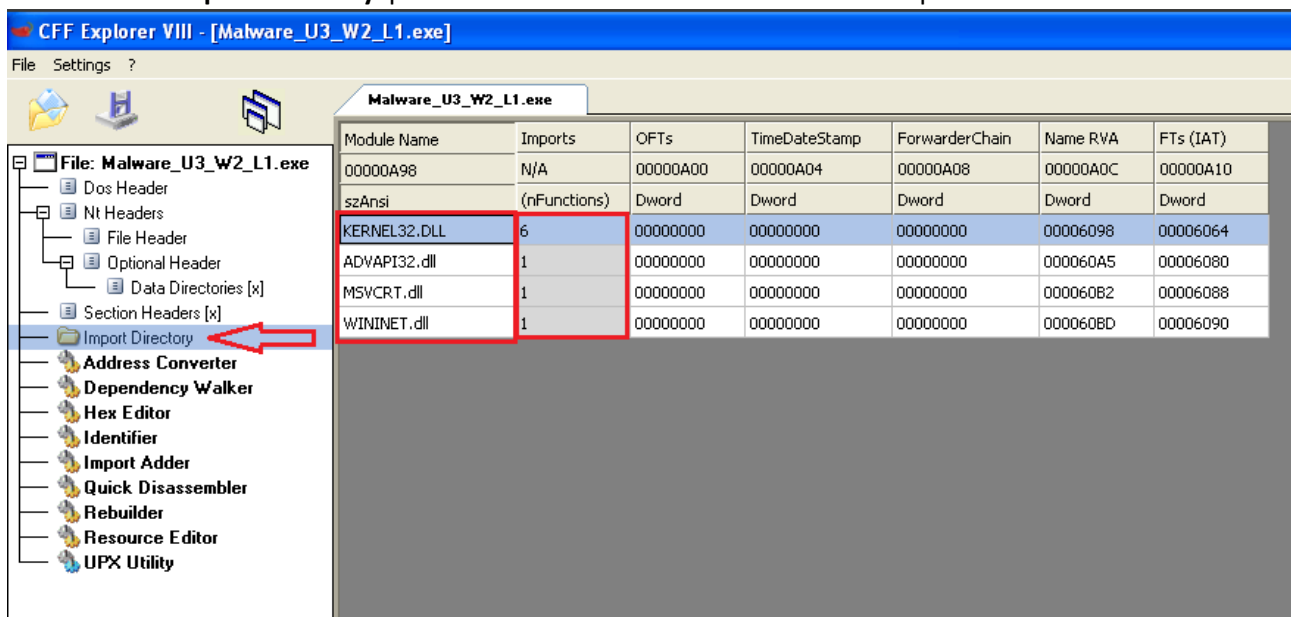
## Analisi Statica

La prima cosa da fare sarà quello di analizzare il file Richiesto – **Malware\_U3\_W2\_L1** – tramite il nostro Tool per le analisi dinamica, ovvero **CFF Explorer**



Come possiamo vedere ci basterà cliccare con il tasto destro del Mouse sul nostro file e cliccare su **Open With CFF Explorer**, in questo modo il Malware verrà caricato nel programma.

Selezionando **Import Directory** potremmo vedere le Librerie e le funzioni importate



Come possiamo vedere troviamo:

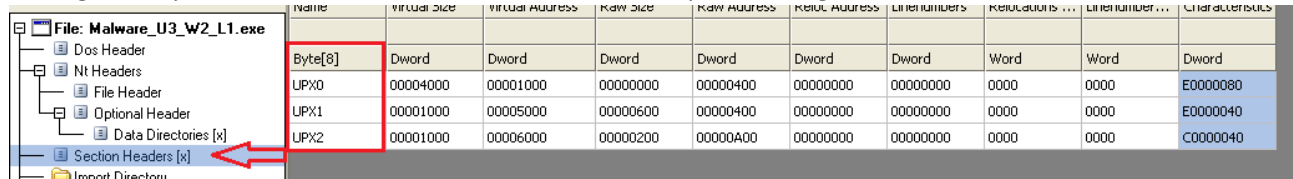
**KERNEL32.DLL:** Serve a garantire il corretto funzionamento di Windows e dei suoi Programmi

**ADVAPI32.DLL:** Contiene funzioni per interagire con i servizi ed i registri del sistema operativo

**MSVCRT.DLL:** Contiene funzioni per la manipolazione stringhe, allocazione memoria e altro.

**WININET.DLL:** Libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come http, FTP e Ntp

Proseguendo possiamo controllare le sezioni di cui è composto l'eseguibile:



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc. Address	Reloc. Address	Reloc. Address	Reloc. Address	Reloc. Address	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400	00000000	00000000	0000	0000	0000	E0000040
UPX2	00001000	00006000	00000200	00000A00	00000000	00000000	0000	0000	0000	C0000040

Possiamo notare, sulla nostra destra, come si compone:

UPX0\UPX1\UPX2 , anche chiamati Packer, che sono dei file oscurati e compressi.

Possiamo comunque constatare che

**UPX0 è .text :** Contiene le righe di codice che la CPU eseguirà una volta avviato.

**UPX1 è .Rdata:** che richiama le librerie e le loro funzioni

**UPX2 è .data:** Contiene i dati e le variabili globali del programma.

## ExeinfoPE

[illegible]

Abbiamo anche cercato l'MD5 del nostro file, ovvero la stringa alfanumerica unica per identificare il file, utilizzando il tool in riga di comando: MD5DEEP-4.3

```
Command Prompt
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 "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe"
C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1: No such file or directory
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>md5deep "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe"
3363436878404da0ae3e46991e355b83 C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe
C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>
```

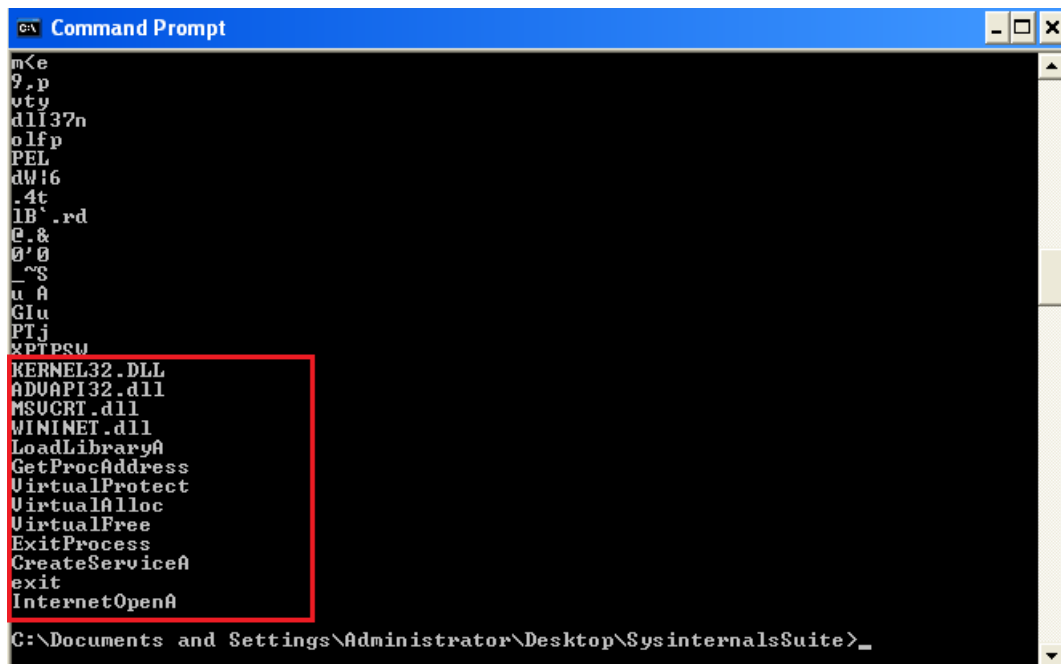
Con il risultato che ci verrà mostrato in immagine, ovvero l'Md5.

C'è anche un altro modo per recuperare informazioni dalla stringhe contenute all'interno degli eseguibili, in questo caso possiamo utilizzare il comando STRING che ci potrà permettere di estrapolare diverse informazioni utili.

```
Command Prompt
C:\Documents and Settings\Administrator\Desktop\SysinternalsSuite>strings "C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe"

Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
Rich
UPX0
UPX1
UPX2
3.04
UPX!
A13
h<0
L$,
Q1I
" z
RU$
u+W
.hP
t=p
sHR
iPd
S`Y
a\`Y
t@E
DmM
;0I
```



```
C:\> Command Prompt
m<e
9.p
vty
dll37n
olfp
PEL
dW!6
.4t
!B'.rd
@.&
@'0
~S
u A
GIu
PTj
xPTPSW
KERNEL32.DLL
ADVAPI32.dll
MSUCRT.dll
WININET.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
CreateServiceA
exit
InternetOpenA
C:\Documents and Settings\Administrator\Desktop\SysinternalsSuite>
```

La considerazione finale è che il file non va aperto.

## Conclusione

Siamo giunti alla conclusione che si tratti di un Trojan. Un Malware che solitamente viene nascosto all'interno di un programma e installandosi inconsapevolmente ne computer della vittima, così da creare anche un accesso diretto per la manipolazione di diversi file e funzioni.

Link

[VirusTotal - File - c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6](https://www.virustotal.com/file/c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6/analysis/1544444444/)