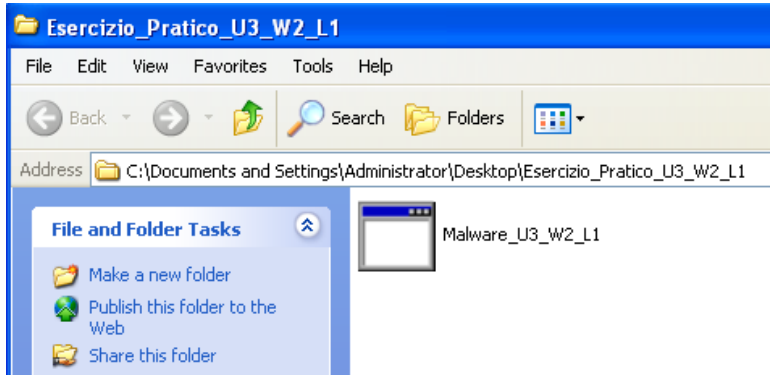
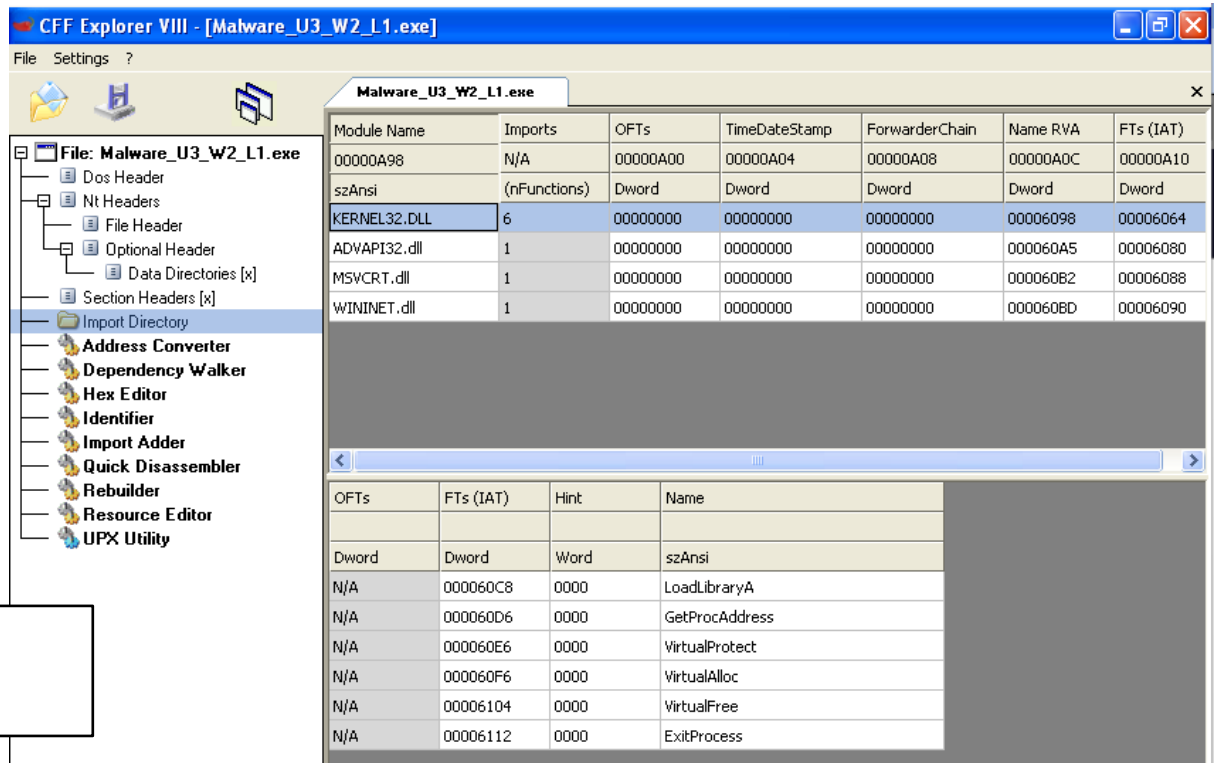
Esercizio 27-03

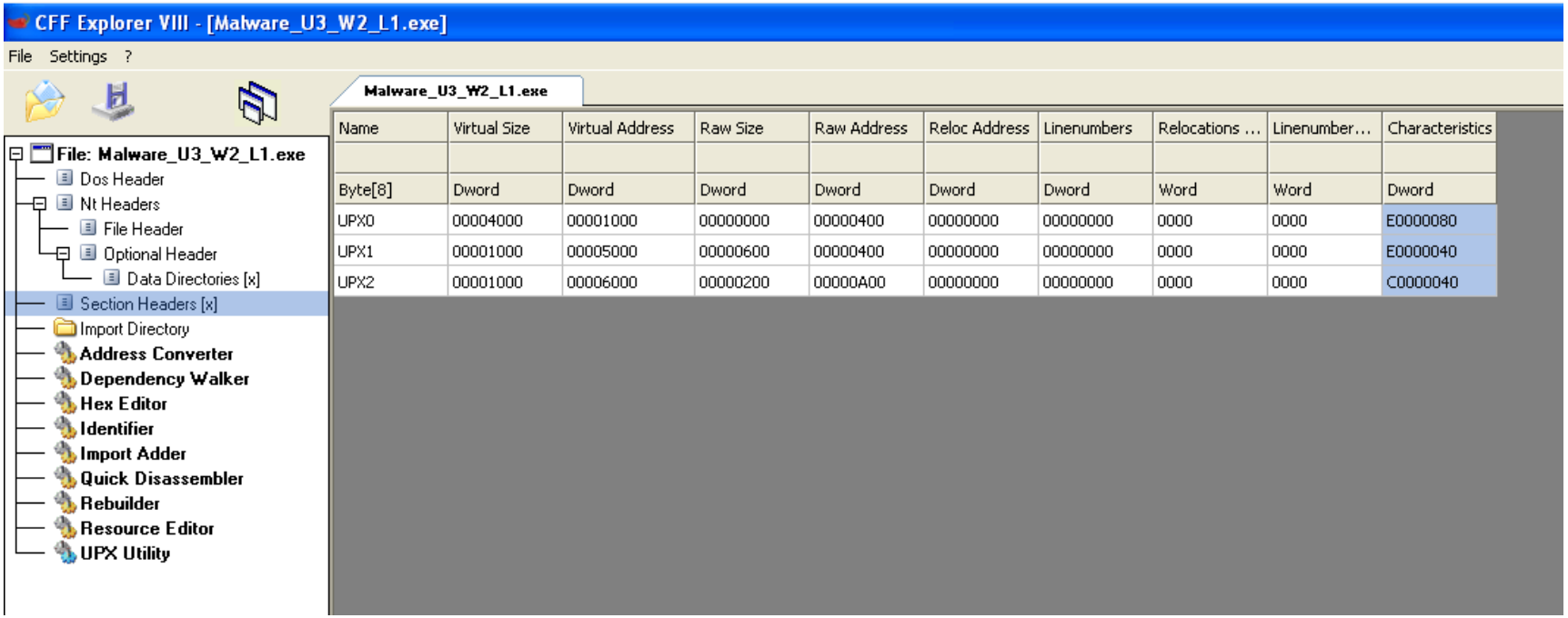
Traccia: come approfondimento pratico del concetto di analisi statica visto in lezione, analizzare il file eseguibile nella cartella "Esercizio_Pratico_U3_W2_L1" presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware e rispondere ai seguenti quesiti:

- 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 esse
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte



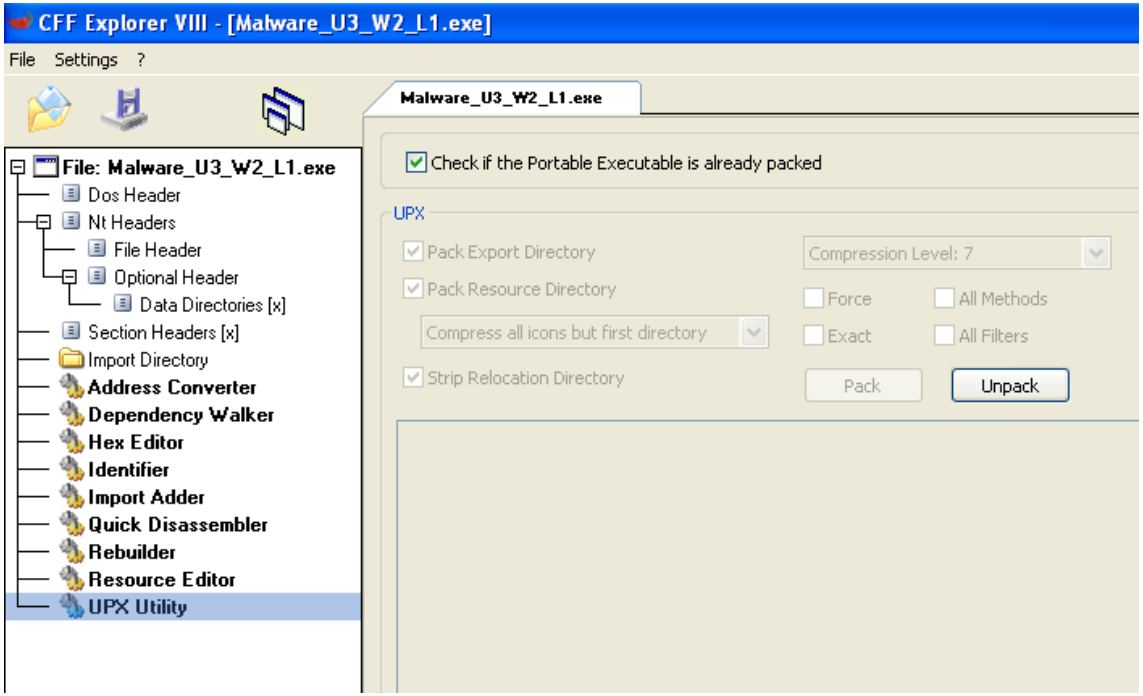


Spostandosi nella tab Import Directory si possono vedere le librerie importate dal malware

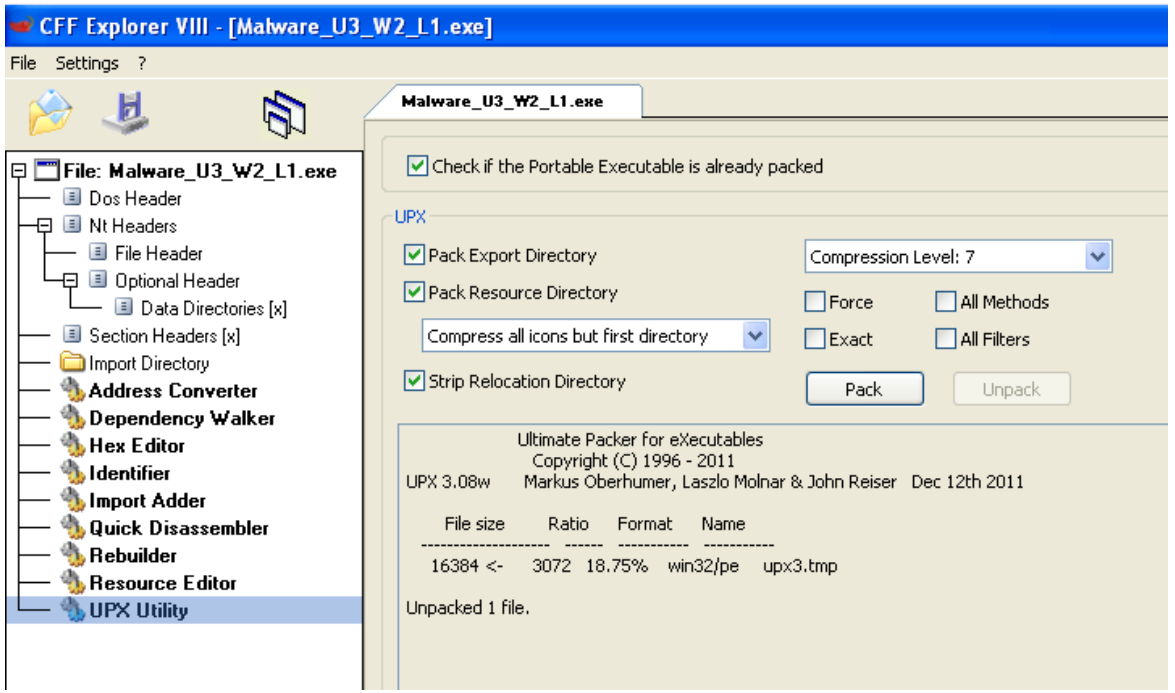


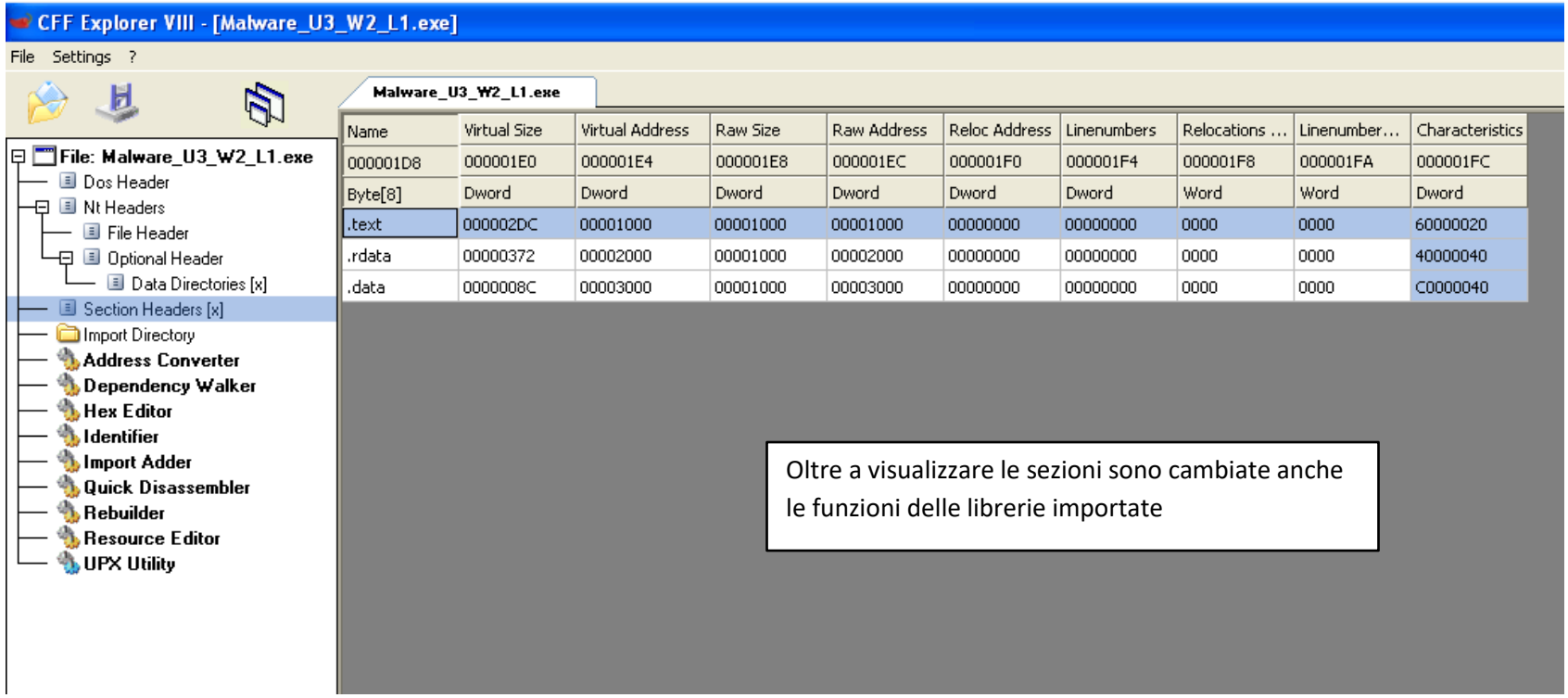
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
UPX0	00004000	00001000	00000000	00000400	00000000	00000000	0000	0000	E0000080
UPX1	00001000	00005000	00000600	00000400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

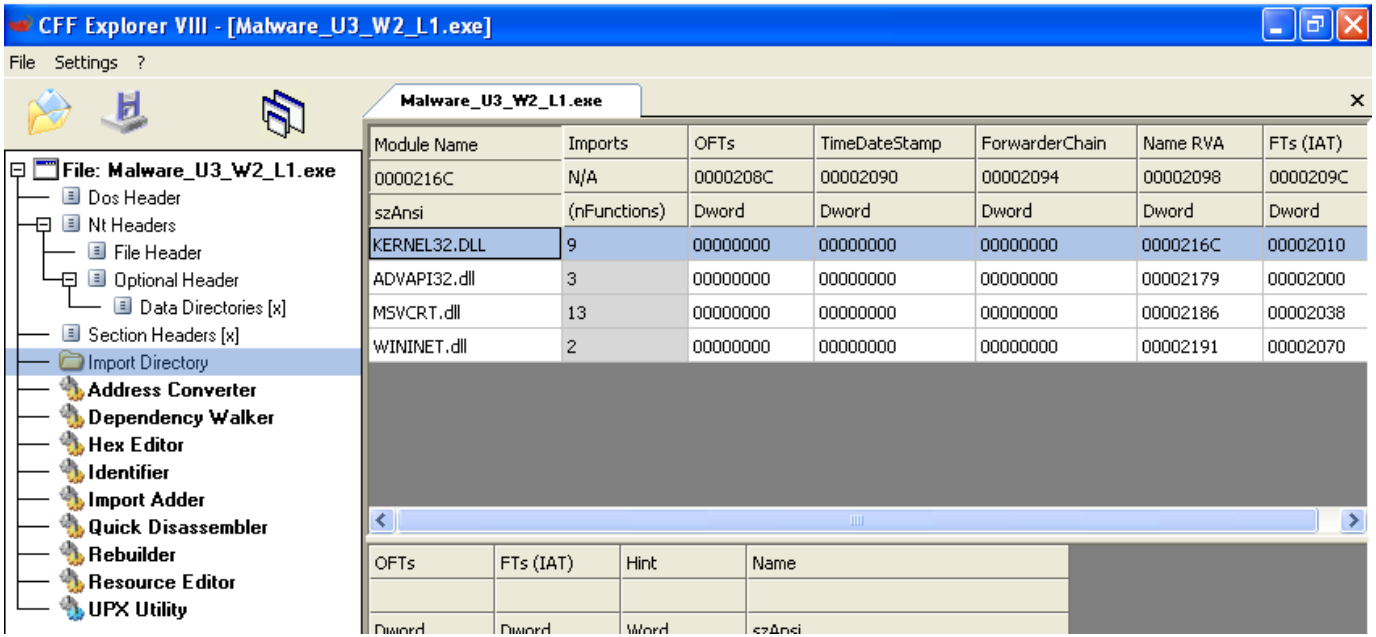
Nel tab Section Headers [x] vediamo le sezioni del malware, che risultano però compresse



Decompressione del malware (Unpack) dal tab UPX Utility, così da poter visualizzare le sezioni dello stesso




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
000001D8 | 000001E0 | 000001E4 | 000001E8 | 000001EC | 000001F0 | 000001F4 | 000001F8 | 000001FA | 000001FC
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
Oltre a visualizzare le sezioni sono cambiate anche le funzioni delle librerie importate


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
Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT)
0000216C | N/A | 0000208C | 00002090 | 00002094 | 00002098 | 0000209C
szAnsi | (nFunctions) | Dword | Dword | Dword | Dword | Dword
KERNEL32.DLL | 9 | 00000000 | 00000000 | 00000000 | 0000216C | 00002010
ADVAPI32.dll | 3 | 00000000 | 00000000 | 00000000 | 00002179 | 00002000
MSVCRT.dll | 13 | 00000000 | 00000000 | 00000000 | 00002186 | 00002038
WININET.dll | 2 | 00000000 | 00000000 | 00000000 | 00002191 | 00002070
OFTs | FTs (IAT) | Hint | Name
Dword | Dword | Word | szAnsi

Il malware importa le seguenti librerie:

- KERNEL32.DLL: libreria contenente le funzioni principali per interagire con il sistema operativo (es. Manipolazione dei file, gestione memoria). È un processo di sistema necessario perchè il PC funzioni correttamente, non lo si deve rimuovere.

- ADVAPI32.DLL: libreria che contiene le funzioni per interagire coi servizi ed i registri del sistema operativo Microsoft. La versione a 32 bit di questo file è responsabile del riavvio e dell'arresto del sistema, del registro di Windows, della gestione degli account utente e dell'avvio, dell'arresto e della creazione dei servizi Windows

- MSVCRT.DLL: libreria contenente funzioni per la manipolazione stringhe, allocazione memoria e altro come chiamate per input/output in stile linguaggio C.

- WININET.DLL (DLL = Dinamic Link Library): libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Il malware si compone delle seguenti sezioni:

- UPX0 => .text: contiene il codice che la CPU eseguirà una volta che il software sarà avviato. È l'unica sezione di un file eseguibile che viene eseguita dalla CPU.

- UPX1 => .rdata: include generalmente le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile.

- UPX2 => .data: contiene i dati/ le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.

Utilizzo del comando md5deep "percorso_del_malware" per ottenerne l'hash, seguentemente fatto analizzare da VirusTotal

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

C:\Documents and Settings\Administrator>cd Desktop\md5deep-4.3

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>md5deep "C:\Document
s and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1
.exe"
8363436878404da0ae3e46991e355b83  C:\Documents and Settings\Administrator\Deskto
p\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>_
```

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Sign in

50 / 69

Community Score

50 security vendors and no sandboxes flagged this file as malicious

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
Lab01-02.exe

peexe | checks-disk-space | via-tor | detect-debug-environment | idle | long-sleeps | upx | checks-user-input

3.00 KB
Size

2023-03-27 14:14:41 UTC
34 minutes ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY 30 +

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.ulise/trojanclicker

Threat categories trojan | downloader

Family labels ulise | trojanclicker | r002c0dhd20

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan/Win32.StartPage.C26214	Alibaba	TrojanClicker:Win32/Generic.1baf980f
ALYac	Trojan.Startpage.3072	Antiy-AVL	Trojan/Win32.SGeneric
Arcabit	Trojan.Ser.Ulise.216	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	TR/Downloader.Gen

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

C:\Documents and Settings\Administrator>cd Desktop\md5deep-4.3

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>md5deep "C:\Document
s and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1
.exe"
8363436878404da0ae3e46991e355b83  C:\Documents and Settings\Administrator\Deskto
p\Esercizio_Pratico_U3_W2_L1\Malware_U3_W2_L1.exe

C:\Documents and Settings\Administrator\Desktop\md5deep-4.3>_
```

Analisi del malware con comando “strings”

```
C:\Documents and Settings\Administrator\Desktop\SysinternalsSuite>strings "C:\Do
cuments 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!
AI3
h<0
L$,
Q1I
" z
RV$
u+W
.hP
t=p
sHR
!Pd
 $`
a\`Y
t@E
DmM
;0I
PQ6
<23h
MalService
sHGL345
```

```
http://w
warean
ysisbook.co
om#Int6net Explo!r 8FEI
.0<
SystemTimeToFile
GetMo
NaA
Cvg
*Waitab'r
Process
OpenMu$x
ZSB+
ForS
ing
ObjectU4
[Vrtb
CtrlDisp ch
SCM
8_e
Xcpt
mArg
sus
5nm@_
t_fd
i9H
m<e
9,p
vty
dll37n
olfp
PEL
dW!6
.4t
lB`.rd
@.&
0'0
_~S
u A
GIu
PTj
```

```
XPTPSW
KERNEL32.DLL
ADVAPI32.dll
MSVCRT.dll
WININET.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
CreateServiceA
exit
InternetOpenA
```

Stringhe ottenute in output

Conclusione

Il malware è un Trojan.