

ANALISI STATICA BASICA

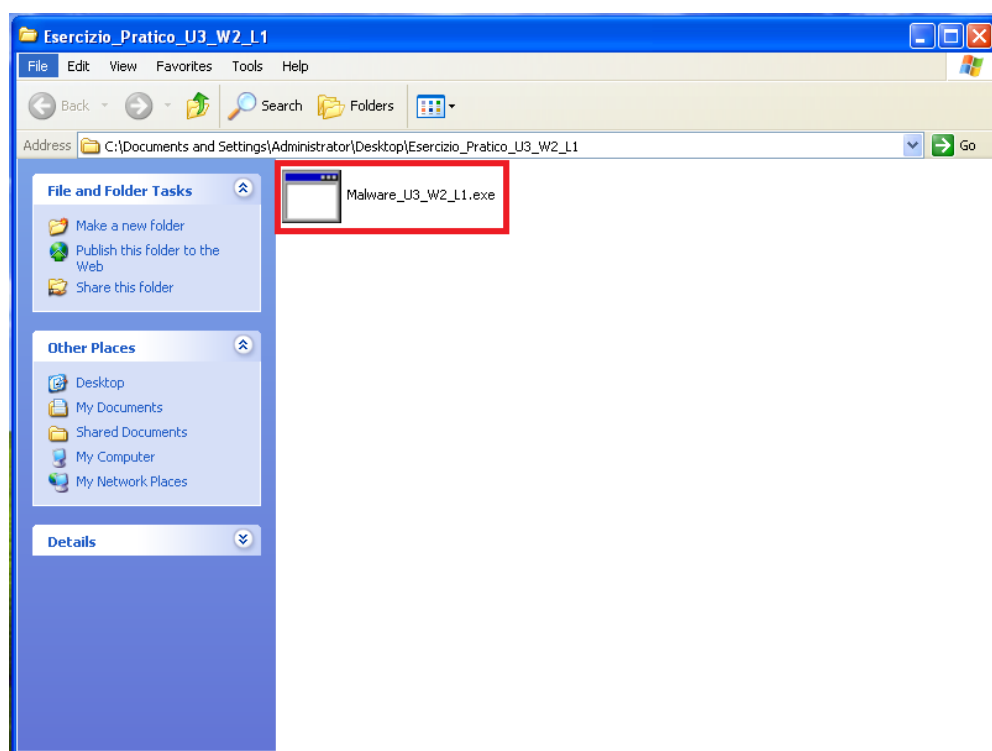
Analisi del malware *Malware_U3_W2_L1.exe*

Tasks

1. Identificazione delle **librerie** importate dal malware *Malware_U3_W2_L1.exe*
2. Identificazione delle **sezioni** di cui si compone il malware
3. Considerazioni finali sul malware in analisi

1. Identificazione delle **librerie** importate dal malware *Malware_U3_W2_L1.exe*

Le attività odierne sono incentrate sull'analisi del file eseguibile di test *Malware_U3_W2_L1.exe*.



Procediamo dunque all'analisi del malware utilizzando il tool **CFF Explorer**:

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

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	Tuesday 10 January 2023, 02.13.12
MD5	8363436878404DA0AE3E46991E355B83
SHA-1	5A016FACBCB77E2009A01EA5C67B39AF209C3FCB

Property Value

Empty	No additional info available
-------	------------------------------

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

Possiamo subito notare che, al caricamento del file, tra i dettagli spiccano due hash in formato MD5 e SHA-1, che ci saranno utili in seguito. Spostandoci nella sezione “**Import Directory**”, possiamo identificare le librerie importate dal malware:

CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
00000A98	N/A	00000A00	00000A04	00000A08	00000A0C	00000A10
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

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

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

Come si vede, le librerie sono:

Kernel32.dll – libreria piuttosto comune che contiene le funzioni principali per interagire con il sistema operativo, es. manipolazione del file, gestione della memoria

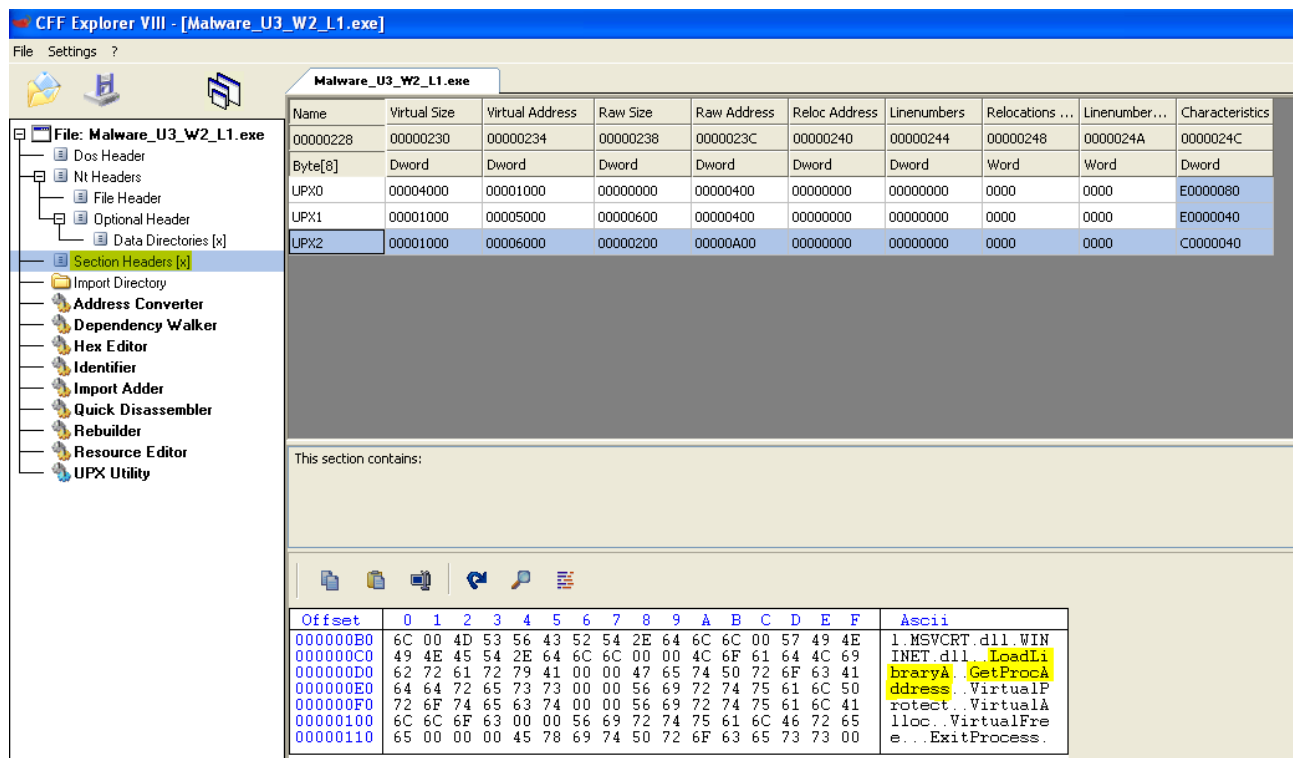
Advapi32.dll – libreria che contiene le funzioni per interagire con i servizi ed i registri di un sistema operativo Microsoft

Wininet.dll – libreria che contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP (network time protocol)

Selezionando la libreria Kernel32.dll, notiamo che tra le funzioni al suo interno sono presenti **LoadLibraryA** e **GetProcAddress**: ciò implica che la modalità di importazione è **A TEMPO DI ESECUZIONE (RUNTIME)**. L'eseguibile, dunque, richiama la libreria SOLAMENTE quando ha necessità di utilizzare una determinata funzione. Questo comportamento è ampiamente analizzato dai malware, che chiamano una determinata funzione all'occorrenza per risultare meno invasivi e rilevabili possibile.

2. Identificazione delle sezioni di cui si compone il malware

Spostandoci all'interno della sezione "Section Headers", possiamo identificare le sezioni UPX0, UPX1 e UPX2. In particolare, selezionando UPX2 possiamo identificare le chiamate alle già citate funzioni **LoadLibraryA** e **GetProcAddress**.



CFF Explorer VIII - [Malware_U3_W2_L1.exe]

File Settings ?

Malware_U3_W2_L1.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
00000228	00000230	00000234	00000238	0000023C	00000240	00000244	00000248	0000024A	0000024C
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

This section contains:

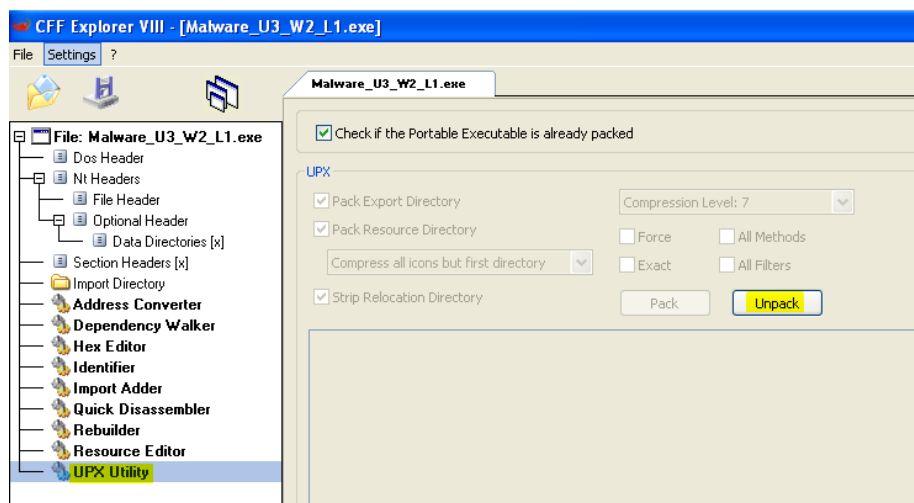
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
000000B0	6C	00	4D	53	56	43	52	54	2E	64	6C	6C	00	57	49	4E	1.MSVCRT.dll.WIN
000000C0	49	4E	45	54	2E	64	6C	6C	00	00	4C	6F	61	64	4C	69	INET.dll..LoadLi
000000D0	62	72	61	72	79	41	00	00	47	65	74	50	72	6F	63	41	braryA..GetProcA
000000E0	64	64	72	65	73	73	00	00	56	69	72	74	75	61	6C	50	ddress..VirtualP
000000F0	72	6F	74	65	63	74	00	00	56	69	72	74	75	61	6C	41	rotect..VirtualA
00000100	6C	6C	6F	63	00	00	56	69	72	74	75	61	6C	46	72	65	lloc..VirtualFre
00000110	65	00	00	00	45	78	69	74	50	72	6F	63	65	73	73	00	e...ExitProcess.

Adesso spostiamoci sulla sezione **UPX Utility**: procedendo all'estrazione con "unpack" abbiamo accesso alle seguenti sezioni:

.text – contiene istruzioni (righe di codice) che la CPU eseguirà quando il software sarà avviato. Generalmente questa è l'UNICA sezione di un file eseguibile che viene eseguita dalla CPU perché tutte le altre sezioni contengono dati o info a supporto

.rdata – contiene informazioni sulle librerie e le funzioni importate ed esportate dall'eseguibile

.data – contiene dati/variabili globali del programma eseguibile, che devono essere quindi disponibili da qualsiasi parte del programma (una variabile è globale quando non è definita all'interno di una funzione, ma è globalmente dichiarata ed è quindi accessibile da qualsiasi funzione dell'eseguibile)



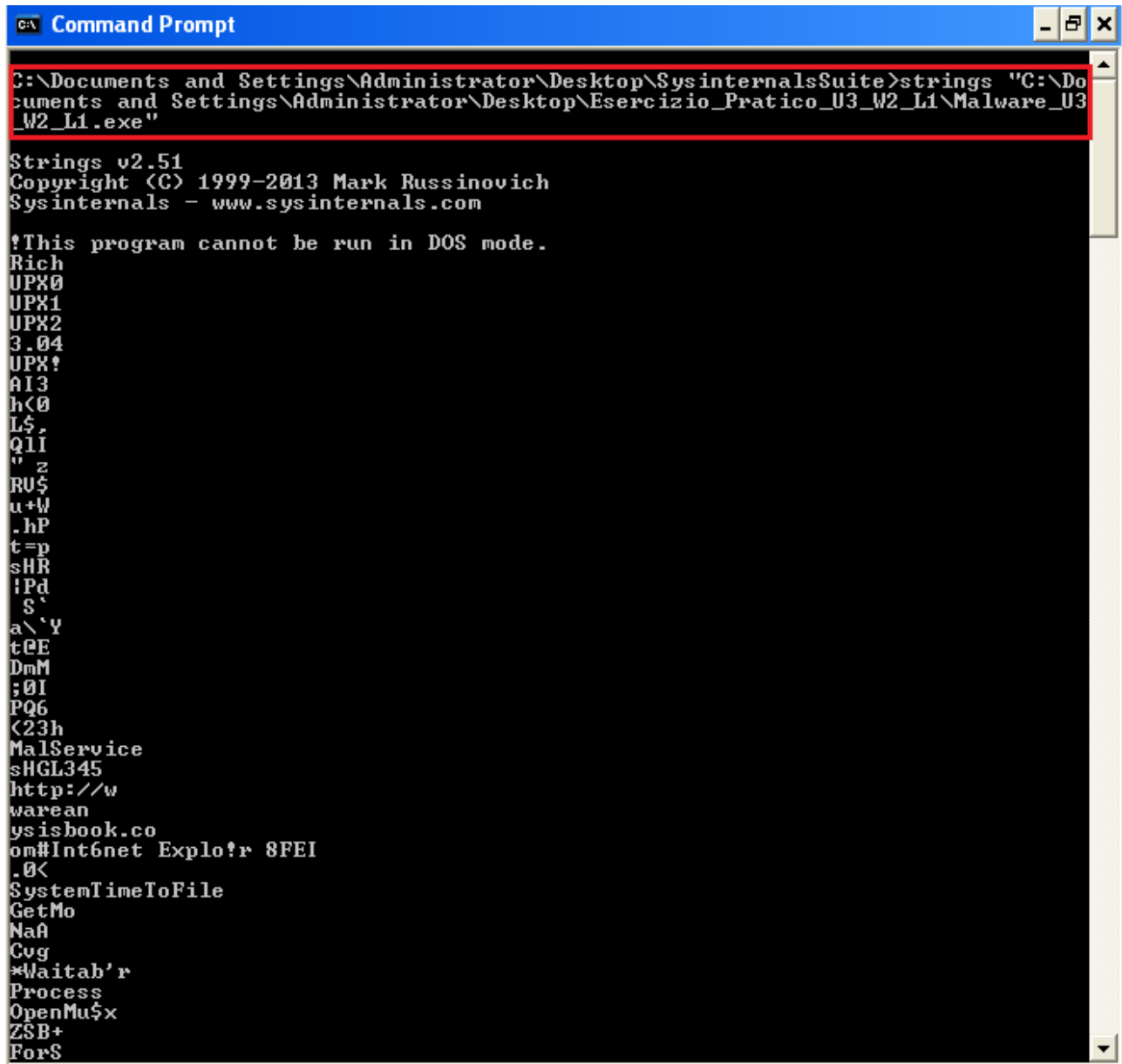
The screenshot shows the CFF Explorer VIII interface for the file 'Malware_U3_W2_L1.exe'. The left sidebar lists various tools, with 'Section Headers [x]' highlighted. The main window displays a table of section headers. The table has columns for Name, Virtual Size, Virtual Address, Raw Size, Raw Address, Reloc Address, Linenumbers, Relocations, Linenumbers, and Characteristics. The sections listed are .text, .rdata, and .data.

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations	Linenumbers	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

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
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
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	!! 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.

Ulteriori verifiche

Da prompt dei comandi, utilizziamo il comando **strings** per accedere alle stringhe all'interno dell'eseguibile:



```
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
!Pd
S`
a\`y
t@E
DmM
;0I
PQ6
<23h
MalService
sHGL345
http://w
warean
ysisbook.co
om#Int6net Explo!r 8FEI
.0<
SystemTimeToFile
GetMo
NaA
Cug
*Waitab'r
Process
OpenMu$x
ZSB+
For$
```


```
C:\ Command Prompt
*Waitab'r
Process
OpenMu$X
Z$B+
For$
ing
ObjectU4
[Urtb
CtrlDisp ch
SCM
8_e
Xcpt
mArg
sus
5nm@_
t_fd
i9H
m<e
9.p
vty
dll137n
olfp
PEL
dW!6
.4t
lB'.rd
@.&
0'0
_~S
u A
GIu
PTj
vPTPSH
KERNEL32.DLL
ADVAPI32.dll
MSUCRT.dll
WININET.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
CreateServiceA
exit
InternetOpenA
C:\Documents and Settings\Administrator\Desktop\SysinternalsSuite>_
```

Come si vede, è possibile identificare tra le stringhe presenti le librerie importate dall'eseguibile e le relative chiamate ad alcune funzioni già viste nei test precedenti.

Adesso ricaviamo l'hash md5 del file utilizzando il comando **md5deep**:

```
C:\ Select Command Prompt
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"
8363436878404da0ae3e46991e355b83 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>
```

Successivamente, sfrutteremo l’hash appena ricavato per eseguire una ricerca sul database **VirusTotal**, che ci restituisce i seguenti risultati:




Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE

URL

SEARCH



8363436878404da0ae3e46991e355b83

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your **Sample submission with the security community**. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

53 / 71

X Community Score ✓

53 security vendors and no sandboxes flagged this file as malicious

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6


3.00 KB

2023-01-04 20:55:55 UTC

Lab01-02.exe

Size

5 days ago



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

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 30 +

Security vendors' analysis

AhnLab-V3	Trojan/Win32.StartPage.C26214	Alibaba	TrojanClicker.Win32/Generic.1ba980f
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
Baidu	Win32.Trojan-Clicker.Agent.ad	BitDefender	Gen:Variant.Ser.Ulise.216
BitDefenderTheta	Gen:NN.ZexaF.36158.amGfaWi867f	ClamAV	Win.Malware.Agent-6350563-0
Comodo	Malware@#22epuiwih8vym	Cybereason	Malicious.878404

Come si vede, 53 vendors su 71 identificano il file come un malware di tipo Trojan, dandoci un’ulteriore conferma della natura malevola dell’eseguibile appena analizzato.

3. Considerazioni finali sul malware in analisi

Alla luce delle analisi appena condotte sul malware, possiamo concludere che

- il malware è stato configurato per sfruttare una connettività di tipo HTTP/FTP/NTP grazie all'importazione della libreria Wininet.dll
- interagisce con il sistema operativo tramite la libreria Kernel32.dll
- non è possibile identificare con precisione tramite la sola analisi statica il dettaglio delle operazioni svolte dal malware: come abbiamo visto, la presenza delle funzioni **LoadLibrary** e **GetProcAddress** segnala che il caricamento di alcune funzioni avviene e può essere identificato solo durante l'esecuzione del malware. Si rende dunque necessaria un'analisi dinamica per avere più dettagli ed osservare da vicino il comportamento del file.