

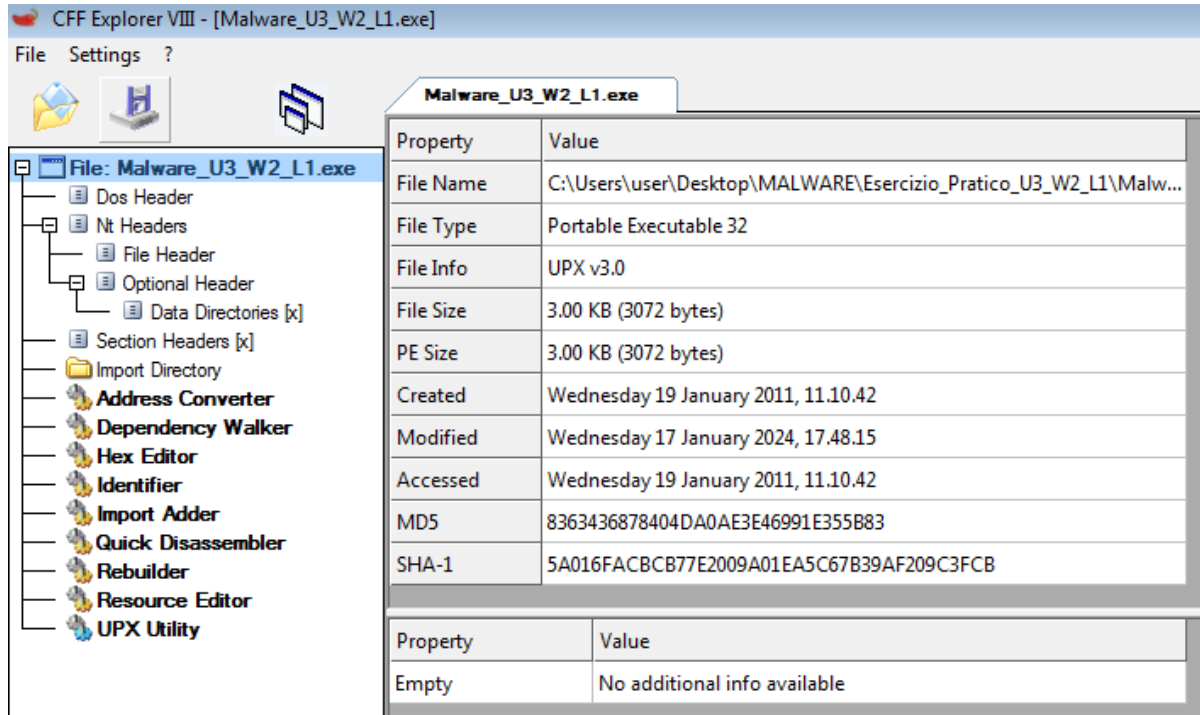
Pratica s10/L1

Traccia:

Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul Desktop della vostra macchina virtuale dedicata all'analisi dei malware, 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 essa
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte

Avvio CFF Explorer sul file «**Malware_U3_W2_L1.exe**»



In questa prima immagine, l'analisi riporta:

- Il nome del file;
- È un file eseguibile a 32bit;
- La dimensione del file;
- La data in cui è stato creato;
- I codici Hash MD5 e SHA-1.

Cartella «Section Headers»

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

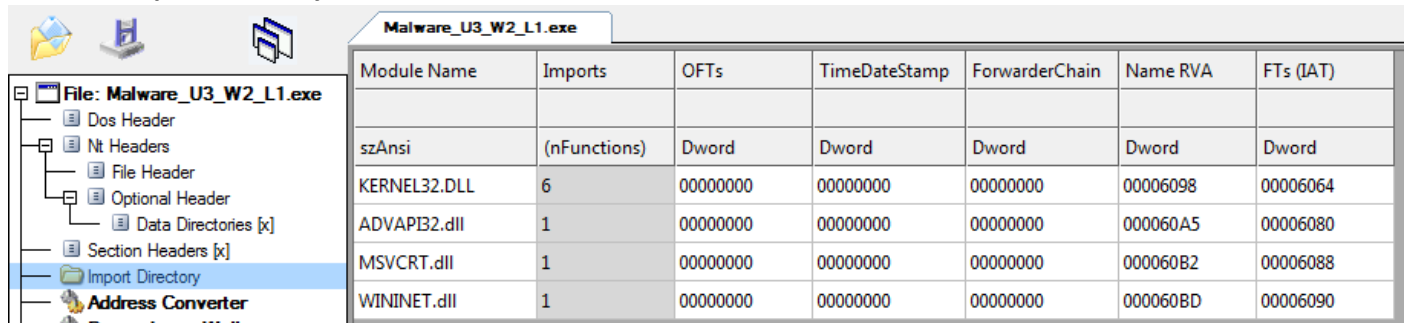
Sulla colonna Name vengono visualizzate le sezioni di cui è composto il file eseguibile.

Le sezioni sono i pakcet UPX0, UPX1 e UPX2, software compressi in grado di prendere il software binario, comprimerlo (rendendo illegibili le stringhe interne) e impacchettarlo con un programma in grado di decomprimerlo (Stub). I Packet proteggono il proprio codice da azioni di «**Reverse Engineering**», ma che vengono utilizzati per compilare le operazioni di «**Malware Analysis**».

Per ogni sezione vi è indicata anche:

- **Virtual Size:** lo spazio allocato di memoria;
- **Raw Size:** lo spazio allocato sul disco.

Cartella «Import Directory»



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

In questa cartella vengono visualizzate tutte le librerie e le funzioni utilizzate:

- **KERNEL32.DLL**: contiene le funzioni principali per interagire con il sistema operativo;
- **ADVAPI32.DLL**: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo;
- **MSVCRT.DLL**: contiene funzioni per la manipolazione stringhe (allocazione di memoria, chiamate per input/output etc.);
- **WININET.DLL**: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP.

Libreria «KERNEL32.DLL»

Module Name	Imports	OFTs	TimeDateStamp	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

Al suo interno vi sono 6 funzioni:

- **LoadLibraryA**: carica un modulo di una libreria nello spazio indirizzi del processo e restituisce un handle;
- **GetProcAddress**: per ottenere l'indirizzo di una funzione DLL;
- **VirtualProtect**: modifica la protezione di accesso di qualsiasi processo;
- **VirtualAlloc**: alloca memoria nello spazio indirizzi di un altro processo;
- **VirtualFree**: unisce un'area di pagina all'interno dello spazio indirizzi virtuale del processo chiamante;
- **ExitProcess**: termina il processo chiamante e tutti i relativi Thread.

Libreria «**ADVAPI32.DLL**»

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000AA5	N/A	00000A14	00000A18	00000A1C	00000A20	00000A24
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	00006120	0000	CreateServiceA

Contiene la funzione «**CreateServiceA**», crea un oggetto servizio e lo aggiunge al database di Gestione controllo del servizio specificato.

Libreria «**MSVCRT.DLL**»

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000AB2	N/A	00000A28	00000A2C	00000A30	00000A34	00000A38
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	00006130	0000	exit

Vi è la funzione «**exit**».

Libreria «WININET.DLL»

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000ABD	N/A	00000A3C	00000A40	00000A44	00000A48	00000A4C
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	00006136	0000	InternetOpenA

Contiene la funzione «**InternetOpenA**», indica alla DLL Internet di inizializzare le strutture di dati interne e prepararsi per le chiamate future dall'applicazione.

Analizzandolo su VirusTotal notiamo che questo file è riconosciuto da 55 vendors di antivirus.

55
/ 70

Community Score

55 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6

Malware_U3_W2_L1.exe

Size 3.00 KB | Last Analysis Date 22 hours ago | EXE

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

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 1 trojan.ulise/startpage

Threat categories trojan downloader

Family labels ulise startpage trojanclicker

Security vendors' analysis ⓘ

Do you want to automate checks?

AhnLab-V3	1 Trojan.Win32.StartPage.C26214	Alibaba	1 TrojanClicker.Win32/Generic.47e7b5e4
ALYac	1 Trojan.Startpage.3072	Antiy-AVL	1 Trojan.Win32.SGeneric
Arcabit	1 Trojan.Ser.Ulise.216	Avast	1 Win32:Malware-gen

È un Trojan, un malware ad accesso remoto che si nasconde all'interno del programma apparentemente innocuo, permettendo all'attaccante di poter mantenere il controllo remoto del computer, senza che il proprietario ne sia a conoscenza.

Conclusione:

Questo file crea Thread, manipola dei servizi, e comunica con la rete.