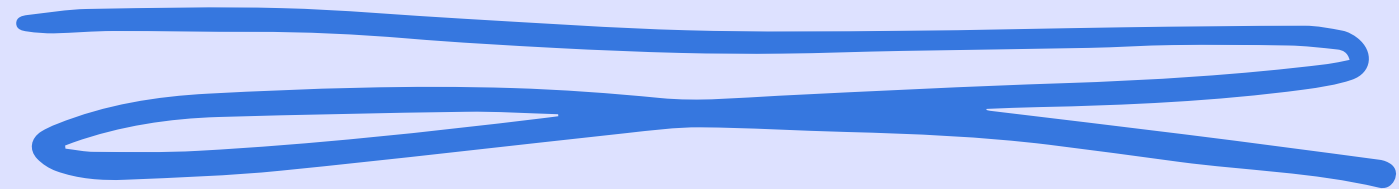


# S10 L1



## Malware Analysis

**Daniele Zizzi**

Ho effettuato l'analisi di un malware grazie al tool cffexplorer. Il tool in questione, permette di visualizzare le sezioni del malware, librerie e funzioni richiamate.

Qui sotto possiamo vedere il percorso, nome file, tipo file (PE eseguibile portabile), md5 e sha-1.

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, 14.31.03
MD5	8363436878404DA0AE3E46991E355B83
SHA-1	5A016FACBCB77E2009A01EA5C67B39AF209C3FCB

Property	Value
Empty	No additional info available

In import directory, troviamo le librei e funzioni richiamate.  
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 memoria e altro come chiamate per input/output, come nel linguaggio C

Wininet.dll: contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP

Module Name	Imports	OFTs	TimeStamp	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

Kernel32.dll

**LoadLibraryA** carica una libreria

**GetProcAddress** ottiene l'indirizzo di memoria di un processo

**Virtualprotect** consente di modificare le autorizzazioni di accesso per un segmento di memoria virtuale. Questa funzione può essere utilizzata per rendere una sezione di memoria leggibile, scrivibile o eseguibile.

**VirtualAlloc** alloca un segmento di memoria virtuale. Questa funzione può essere utilizzata per allocare memoria per un'immagine, un processo o un thread.

Se la funzione **VirtualFree** ha esito positivo, restituisce l'indirizzo del segmento di memoria virtuale allocato. In caso contrario, restituisce NULL.

**ExitProcess** Chiudi processo

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

ADVAPI32.dll

**CreateServiceA** crea un servizio

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006120	0000	CreateServiceA

# MSVCRT.dll exit termina il processo corrente

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006130	0000	exit

WININET.dll Viene utilizzata per inizializzare la DLL WinINet e per ottenere un handle Internet

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
N/A	00006136	0000	InternetOpenA

In section header, abbiamo le sezioni del file eseguibile.

- .text contiene le istruzioni che la cpu eseguirà
- .rdata contiene informazioni sulle librerie importate ed esportate
- .data contiene dati delle variabili globali


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

Dopo unpack

byte[]	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



La scansione virus total, attraverso la scansione del codice hash, mostra che è un trojan. Un trojan è un file eseguibile che, all'apparenza, è un file innocuo, ma al suo interno contiene del codice malevolo.



SUMMARY DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 16

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

Popular threat label

🚨 trojan.ulise/rogue

Threat categories

trojan

spywa

Family labels

ulise

rogue

troj

Security vendors' analysis ⓘ

Do you want to automate checks?

Ad-Aware	🚨 Gen:Variant.Ser.Ulise.216
AhnLab-V3	🚨 Trojan/Win32.StartPage.C26214
Alibaba	🚨 TrojanClicker:Win32/Tnega.2f275f7c
ALYac	🚨 Gen:Variant.Ser.Ulise.216
Antiy-AVL	🚨 Trojan/Win32.TSGeneric
Arcabit	🚨 Trojan.Ser.Ulise.216
Avast	🚨 Win32:AdwareX-gen [Adw]
AVG	🚨 Win32:AdwareX-gen [Adw]
Avira (no cloud)	🚨 TR/Rogue.7734716
BitDefender	🚨 Gen:Variant.Ser.Ulise.216
BitDefenderTheta	🚨 Gen:NN.ZexaF.36792.bmW@aG9@v0b
Bkav Pro	🚨 W32.AIDetectMalware
CrowdStrike Falcon	🚨 Win/malicious_confidence_100% (W)
Cybereason	🚨 Malicious.e49705

L'analisi del malware è molto importante, poichè permette di ottenere informazioni riguardo ad un file malevolo. Tool come cffexplorer e virus total, permettono di capire velocemente, il funzionamento del codice malevolo, mostrando tutte le chiamate alle funzioni e le librerie di sistema richiamate. Il malware in questione, scarica altri file malevoli sull'host vittima.