

EPICODE-CS0124

S10/L1 - Pratica

Flaviano Sedici

Indice

1. Traccia	3
1.1. Definizioni	4
1.2. Analisi del Malware	4
1.2.1. Analisi delle librerie	4
1.2.2. Analisi delle sezioni.....	5
1.2.3. Analisi approfondita dell'Hash	7

Riferimenti e versioni

Responsabile del documento: Flaviano Sedici

Versionamento

Versione	Descrizione	Riferimento	Data
1.0	Redazione documento	Responsabile	25/03/2024

1. 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

1.1. Definizioni

Malware Analysis

L'analisi del malware è il processo di esame approfondito dei software dannosi per comprendere le loro funzionalità, comportamenti e impatti sui sistemi informatici. Include l'identificazione delle caratteristiche del malware, l'analisi del codice sorgente, l'esecuzione in un ambiente sicuro per osservarne il comportamento e lo sviluppo di contromisure e soluzioni di sicurezza per mitigare o neutralizzare la minaccia. L'analisi del malware è essenziale per comprendere e contrastare le sempre più sofisticate minacce informatiche e proteggere gli utenti e le organizzazioni dai danni causati dal software dannoso.

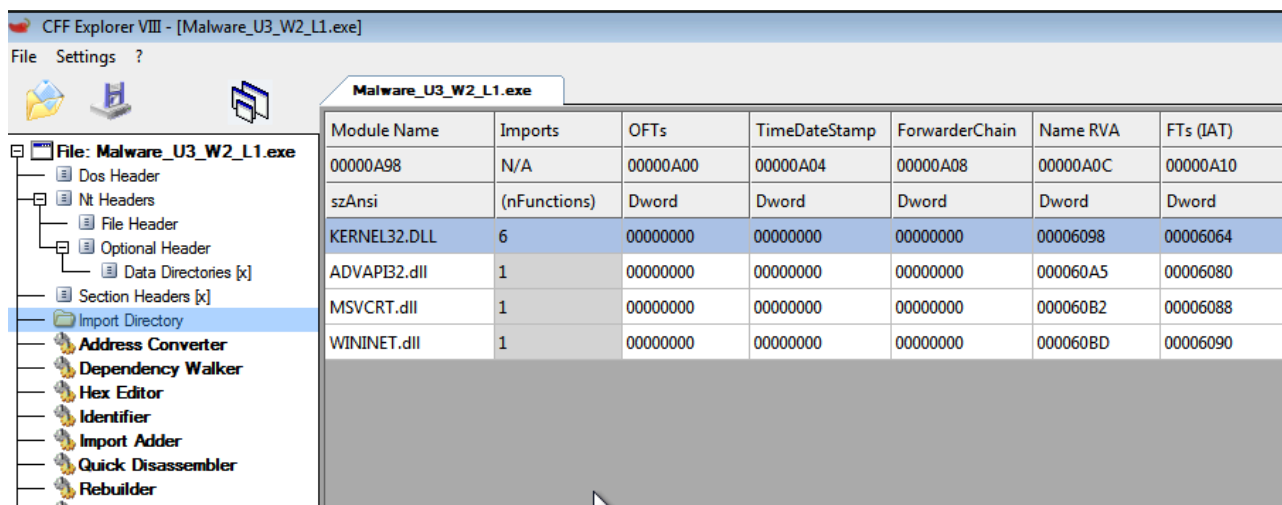
Libreria DLL

Una libreria DLL (Dynamic Link Library) è un file eseguibile di Windows che contiene funzioni e risorse condivise utilizzate da più programmi. Le DLL consentono il caricamento dinamico di codice in esecuzione, riducendo la duplicazione del codice e facilitando la gestione delle risorse comuni. Le applicazioni possono chiamare funzioni presenti nelle DLL per eseguire operazioni specifiche, migliorando l'efficienza e la modularità del software. Le DLL possono anche essere utilizzate per estendere le funzionalità del sistema operativo o fornire interfacce comuni per i driver di dispositivi hardware.

1.2. Analisi del Malware

1.2.1. Analisi delle librerie

Analizzando il malware fornito dalla traccia tramite l'utilizzo del software CFF Explorer, recandoci nella cartella "Import Directory", è possibile visionare l'elenco delle librerie che vengono richiamate dal malware.



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

Analisi delle librerie DLL

KERNEL32.DLL - libreria di sistema di Windows che fornisce funzioni essenziali per la gestione della memoria, la gestione dei file, l'accesso ai dispositivi hardware e altre operazioni di basso livello. È fondamentale per il funzionamento stabile del sistema operativo Windows.

ADVAPI32.dll - libreria di sistema di Windows che fornisce funzioni per la gestione degli account utente, la crittografia dei dati, la gestione delle autorizzazioni, i servizi di Windows e altre operazioni relative alla sicurezza e alla gestione dei dati sensibili nel sistema operativo Windows.

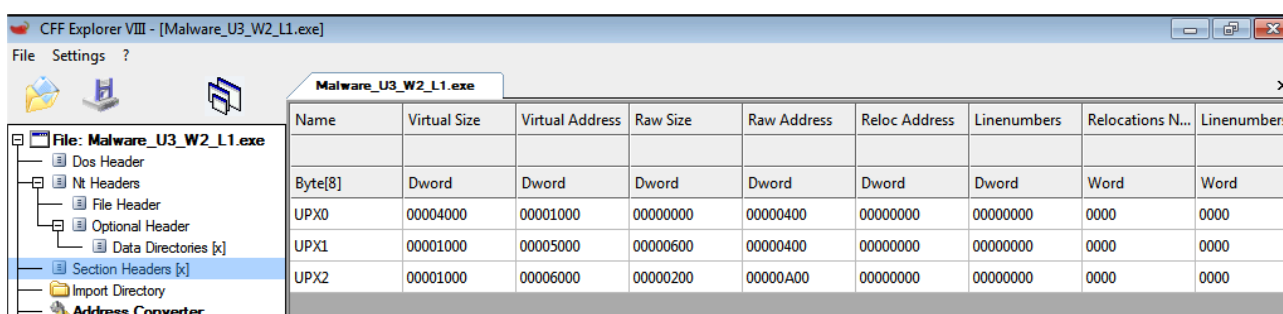
MSVCRT.dll - libreria di sistema di Windows che fornisce funzioni di runtime per le applicazioni C/C++ compilate con il compilatore Microsoft Visual C++. Include funzioni per la gestione della memoria, l'input/output, le stringhe e altre operazioni di base. È essenziale per l'esecuzione delle applicazioni Windows.

WININET.dll - libreria di sistema di Windows che fornisce funzionalità per l'accesso a Internet dalle applicazioni Windows. Include funzioni per la gestione delle connessioni HTTP, HTTPS e FTP, l'invio e la ricezione di dati su Internet e altre operazioni di rete. È essenziale per le applicazioni web e Internet.

1.2.2. Analisi delle sezioni

Durante l'analisi delle sezioni, notiamo come i creatori del Malware hanno nascosto il vero nome delle sezioni.

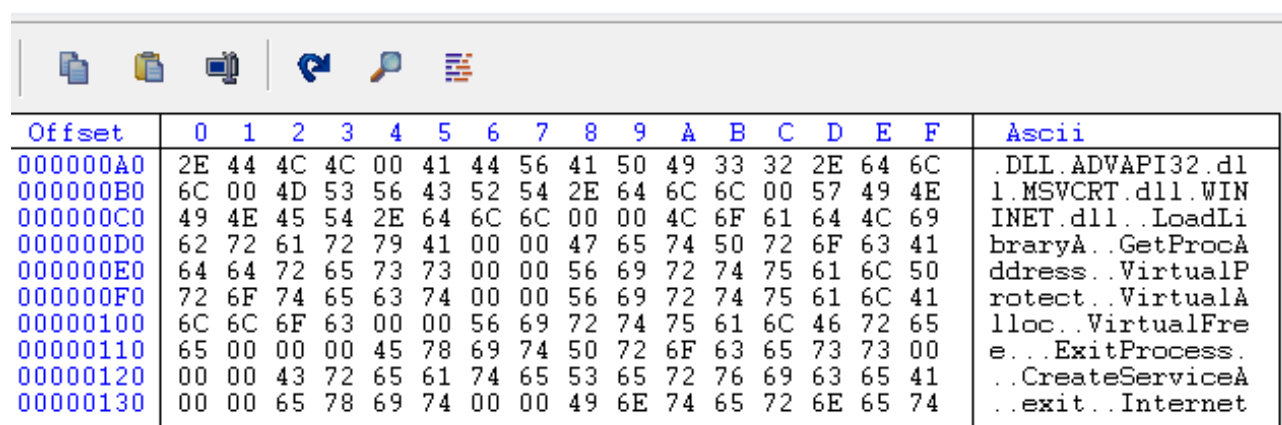
Non siamo quindi in grado di comprendere esattamente di che tipo di sezioni si tratti.



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

Analisi delle sezioni

Analizzando brevemente il codice ASCII, si evince come al suo interno siano presenti le librerie già identificate più alcuni comandi scritti in chiaro.



Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
000000A0	2E	44	4C	4C	00	41	44	56	41	50	49	33	32	2E	64	6C	.DLL.ADVAPI32.dll
000000B0	6C	00	4D	53	56	43	52	54	2E	64	6C	6C	00	57	49	4E	l.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.
00000120	00	00	43	72	65	61	74	65	53	65	72	76	69	63	65	41	..CreateServiceA
00000130	00	00	65	78	69	74	00	00	49	6E	74	65	72	6E	65	74	..exit..Internet

Analisi ASCII

Anche utilizzando il comando strings sul file, non rileviamo ulteriori informazioni oltre a quelle già estratte grazie a CFF Explorer.



```
0'0  
~S  
u A  
Glu  
PTj  
XPTPSW  
KERNEL32.DLL  
ADVAPI32.dll  
MSUCRT.dll  
WININET.dll  
LoadLibraryA  
GetProcAddress  
VirtualProtect  
VirtualAlloc  
VirtualFree  
ExitProcess  
CreateServiceA  
exit  
InternetOpenA  
C:\Users\user\Desktop\Software Malware analysis\SysinternalsSuite>
```

Analisi del file tramite il comando Strings

Vediamo però che sono riconoscibili le seguenti chiamate a seguito del caricamento delle librerie:

GetProcAddress - potrebbe indicare un comportamento dinamico del caricamento di funzioni, utilizzato per eludere la rilevazione e l'analisi statica del malware.

VirtualProtect - potrebbe riferirsi a una chiamata di sistema Windows utilizzata per modificare i permessi di accesso alla memoria virtuale di un processo in esecuzione.

VirtualAlloc - potrebbe indicare che il malware sta cercando di allocare spazio di memoria per eseguire codice dannoso o nascondere la sua presenza, modificando dinamicamente lo spazio di indirizzamento del processo infetto.

VirtualFree - potrebbe essere utilizzata per rilasciare risorse di sistema acquisite in modo dannoso e mascherare le proprie attività.

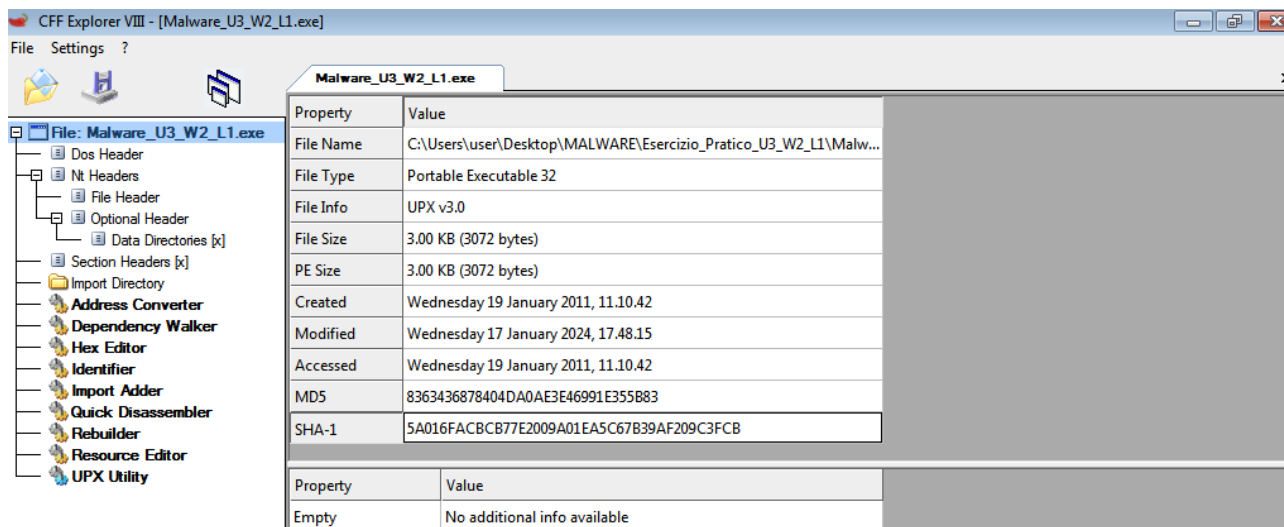
CreateService - potrebbe riferirsi alla creazione di un nuovo servizio nel sistema operativo Windows. Questo servizio consentirebbe al malware di eseguire operazioni dannose in background, come il mantenimento della persistenza, la raccolta di informazioni o l'esecuzione di altri moduli del malware.

InternetOpen - potrebbe essere utilizzata per scopi dannosi al fine di stabilire connessioni con un server di comando e controllo o per scaricare payload dannosi da server remoti.

Si può dedurre che il malware sia assimilabile ad un Trojan finalizzato al mantenimento di un accesso o volto al download di ulteriore codice malevolo.

1.2.3. Analisi approfondita dell'Hash

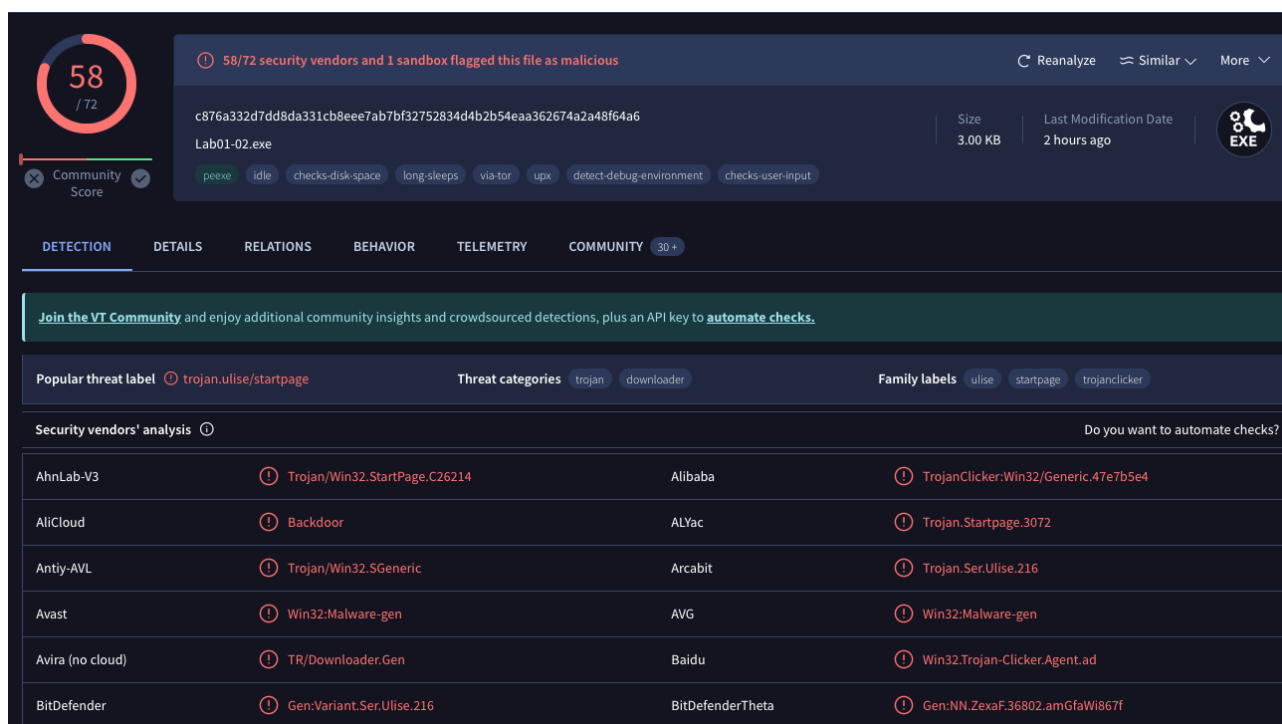
Proseguendo nell'analisi tramite l'utilizzo dell'hash sul portale Virus Total, possiamo notare come da molti enti indipendenti il malware venga identificato nello specifico come un Trojan.



The screenshot shows the CFF Explorer VIII interface. The left pane displays the file structure, including sections like Dos Header, PE Headers, and Section Headers. The right pane shows the file properties for 'Malware_U3_W2_L1.exe'.

Property	Value
File Name	C:\Users\user\Desktop\MALWARE\Esercizio_Pratico_U3_W2_L1\Malw...
File Type	Portable Executable 32
File Info	UPX v3.0
File Size	3.00 KB (3072 bytes)
PE Size	3.00 KB (3072 bytes)
Created	Wednesday 19 January 2011, 11.10.42
Modified	Wednesday 17 January 2024, 17.48.15
Accessed	Wednesday 19 January 2011, 11.10.42
MD5	8363436878404DA0AE3E46991E355B83
SHA-1	5A016FACBCB77E2009A01EA5C67B39AF209C3FCB

Estrazione dell'HASH



The screenshot shows the VirusTotal analysis page for the file 'Lab01-02.exe'. The page displays a community score of 58/72, indicating it is malicious. The file is identified as a Trojan (TrojanClicker) and is flagged by 58/72 security vendors. The page also shows a list of security vendors and their specific detections.

File Information:

- File Name: Lab01-02.exe
- Size: 3.00 KB
- Last Modification Date: 2 hours ago
- File Type: EXE

Security vendors' analysis:

Vendor	Detection
AhnLab-V3	Trojan/Win32.StartPage.C26214
AllCloud	Backdoor
Antiy-AVL	Trojan/Win32.SGeneric
Avast	Win32:Malware-gen
Avira (no cloud)	TR/Downloader.Gen
BitDefender	Gen:Variant.Ser.Ulisse.216

Verifica dell'HASH su Virus Total