

## Soluzione S10L1

Utilizzando CFF Explorer, osserviamo dalla sezione della directory di importazione che il malware U3\_W2\_L1 carica quattro librerie:

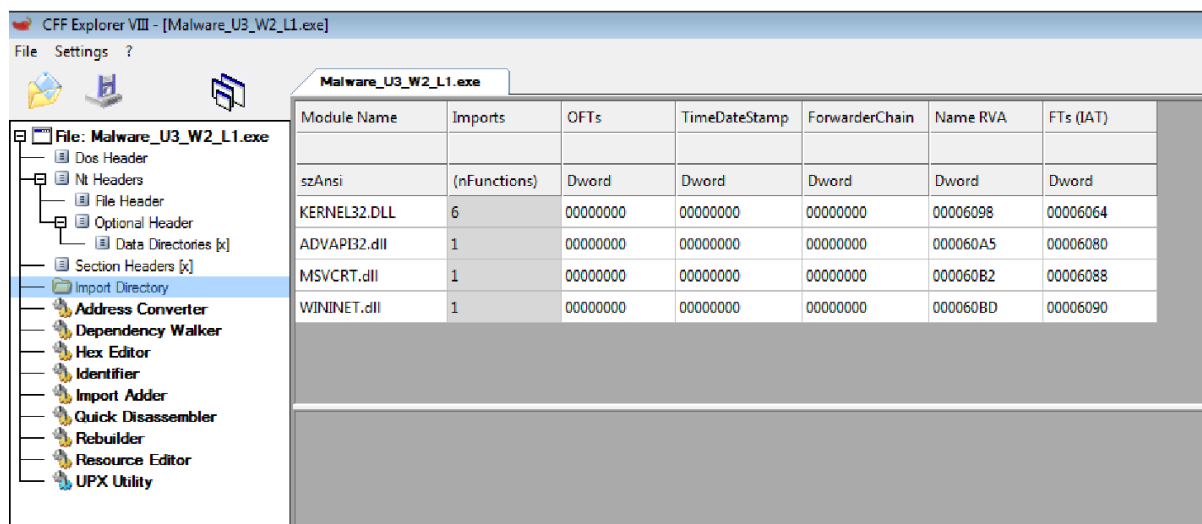
- **Kernel32.dll**, che contiene le funzioni principali del sistema operativo.
- **Advapi32.dll**, utilizzata per interagire con i registri e i servizi di Windows.
- **MSVCRT.dll**, una libreria C standard per operazioni di manipolazione delle stringhe e allocazione della memoria.
- **Wininet.dll**, che fornisce funzionalità di rete come FTP, NTP, HTTP.

## Soluzione – Sezioni del Malware

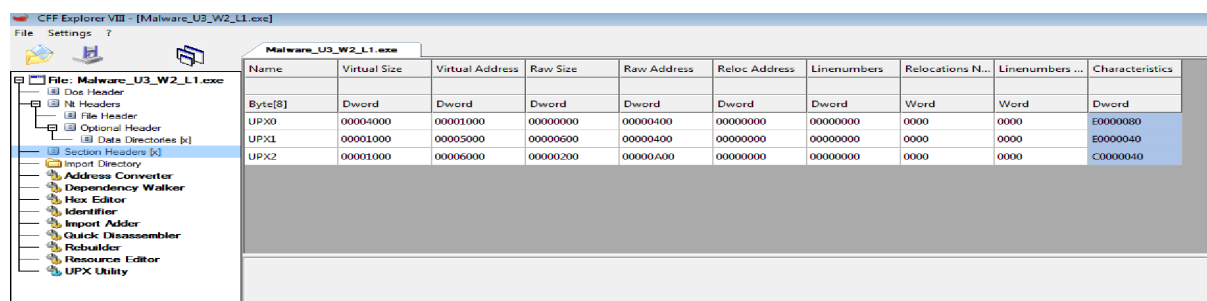
Esaminando la sezione «section header» tramite CFF Explorer, notiamo che l'eseguibile è suddiviso in tre sezioni. Tuttavia, il malware sembra aver offuscato i veri nomi delle sezioni, rendendo difficile determinare il loro scopo preciso.

## Soluzione – Considerazioni Finali

Questo malware si distingue per la sua complessità, poiché l'analisi statica di base non rivela molte informazioni sul suo comportamento. Ciò è confermato dalla presenza delle funzioni «LoadLibrary» e «GetProcAddress» tra quelle importate, suggerendo che il malware carica le librerie durante l'esecuzione (runtime), mascherando efficacemente le informazioni sulle librerie importate in anticipo.



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



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

CFF Explorer VIII - [Malware\_U3\_W2\_L1.exe]

File Settings ?

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

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, 12.10.42
Modified	Wednesday 17 January 2024, 18.48.15
Accessed	Wednesday 19 January 2011, 12.10.42
MD5	8363436878404DA0AE3E46991E355B83
SHA-1	5A016FACBCB77E2009A01EA5C67B39AF209C3FCB

Property	Value
Empty	No additional info available