



LUCA GASPARI

# Malware Analysis

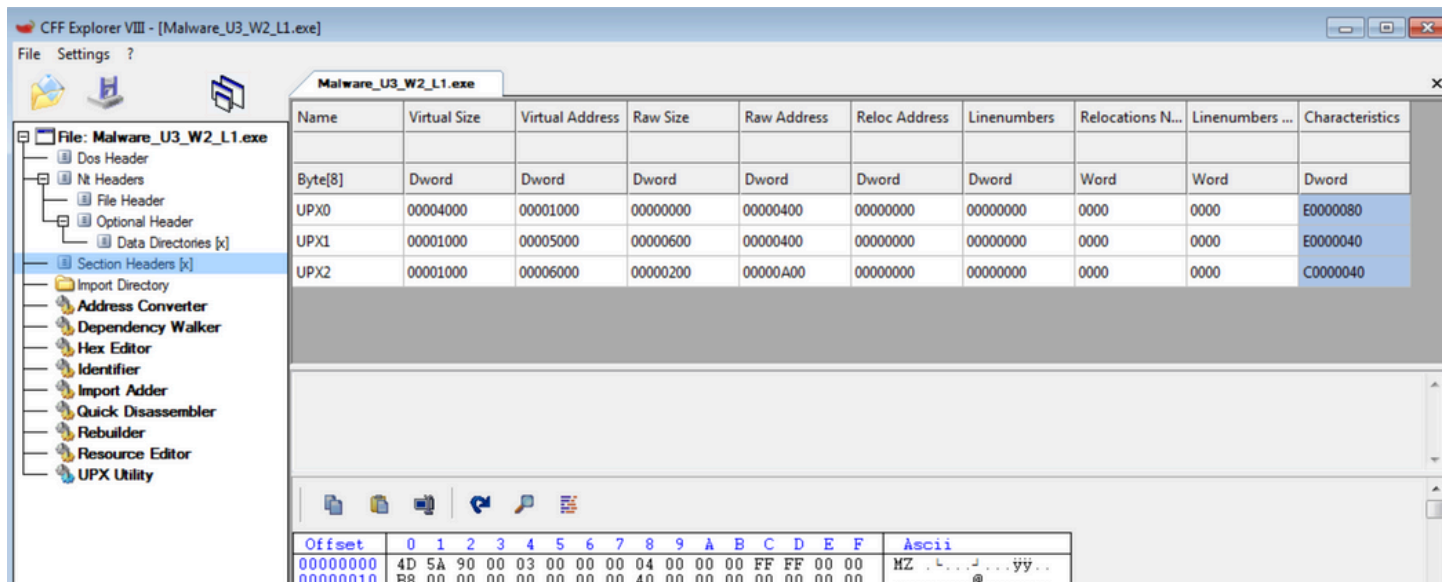
2024

# Introduzione

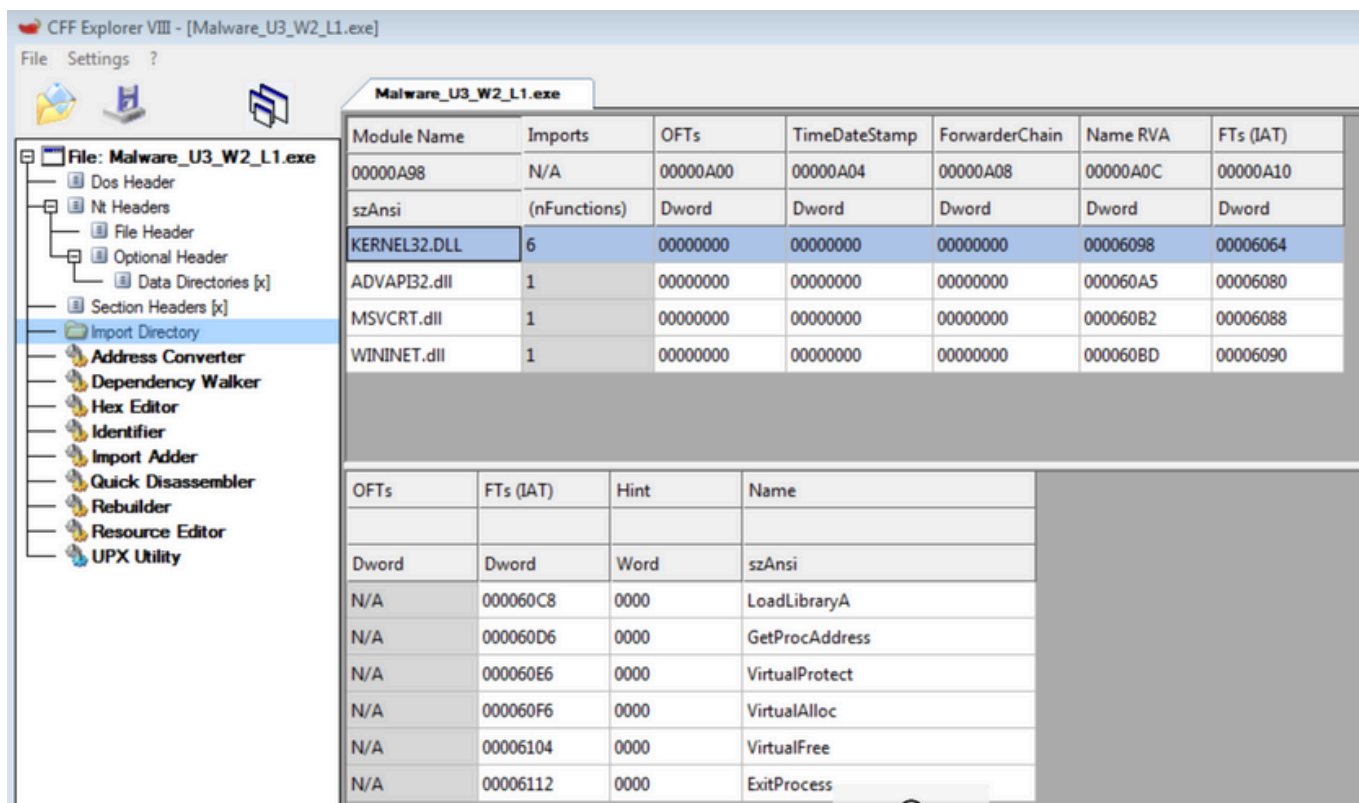
La **malware analysis**, o analisi del malware, è il processo di studiare e comprendere il comportamento, la funzionalità e l'impatto di software malevolo, comunemente noto come malware. Questo processo è cruciale per la cybersecurity poiché consente ai professionisti di identificare, mitigare e proteggere i sistemi informatici dalle minacce informatiche.

Il malware può presentarsi in molte forme diverse, inclusi virus, worm, trojan, ransomware, spyware e adware, ognuno con caratteristiche e scopi distinti. Alcuni malware sono progettati per rubare informazioni sensibili, altri per danneggiare o interrompere operazioni di sistema, e altri ancora per prendere il controllo di sistemi informatici a scopi nefasti.

Quindi è una comprensione approfondita delle capacità e delle modalità operative del malware, che consente la creazione di contromisure efficaci. Queste possono includere aggiornamenti alle firme antivirus, implementazione di patch di sicurezza, e lo sviluppo di strategie di risposta agli incidenti.



## Librerie Importate e Funzioni



The screenshot shows the CFF Explorer VIII interface for the file Malware\_U3\_W2\_L1.exe. The left sidebar displays the file's structure, with 'Import Directory' selected. The main window shows a table of imported modules and a detailed view of the imported functions from 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

### KERNEL32.DLL:

è una delle librerie di sistema più critiche di Windows. Fornisce la maggior parte delle funzioni di gestione della memoria, processi e thread, gestione dei file e delle operazioni di I/O. Le funzioni importate da questa libreria indicano che il malware potrebbe eseguire diverse operazioni fondamentali per il suo funzionamento.

Andando più nello specifico di questa libreria troviamo le funzioni:

**LoadLibraryA**, ha la funzione di caricare una libreria DLL specificata nel processo chiamante, questa funzione è essenziale per il malware perché consente di caricare ulteriori moduli DLL necessari per eseguire operazioni specifiche.

**GetProcAddress**, ha la funzione di recuperare l'indirizzo di una funzione esportata o di una variabile da una DLL caricata. Utilizzato in combinazione con LoadLibraryA, permette al malware di chiamare funzioni specifiche all'interno delle DLL caricate dinamicamente.

### **ADVAPI32.dll**

Questa libreria fornisce funzioni avanzate di gestione delle applicazioni, inclusi i servizi di registro di sistema, sicurezza e controllo delle sessioni di login.

### **MSVCRT.dll**

è la libreria di runtime del C per Microsoft Visual Studio, contiene funzioni della libreria standard del C utilizzate per la manipolazione di stringhe, l'allocazione di memoria e altre operazioni di runtime.

### **WININET.dll**

fornisce funzionalità di accesso a Internet per applicazioni che utilizzano HTTP e FTP.

## **Considerazioni finali**

Il malware analizzato utilizza una combinazione di funzioni da diverse librerie di sistema critiche per eseguire operazioni di rete, manipolazione della memoria e interazione con il registro di sistema. La presenza di LoadLibraryA e GetProcAddress indica che il malware è progettato per essere modulare, caricando e utilizzando dinamicamente altre librerie necessarie per la sua esecuzione. Questo approccio rende il malware più flessibile e più difficile da rilevare, in quanto può adattarsi a diverse situazioni caricando solo le componenti necessarie in base all'ambiente in cui viene eseguito. La compressione tramite UPX suggerisce inoltre che il malware cerca di evitare il rilevamento riducendo le sue dimensioni e alterando la sua firma binaria.