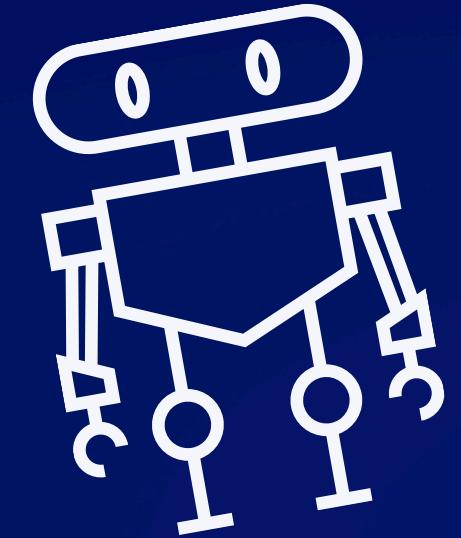


MALWARE ANALYSIS



Andando ad analizzare il malware con CFF Explorer notiamo subito che importa 4 librerie.

The screenshot shows the CFF Explorer interface with the title bar "CFF Explorer VIII - [Malware_U3_W2_L1.exe]". The menu bar includes "File", "Settings", and "?". The toolbar has icons for opening files, saving, and other utilities. The left sidebar shows the file structure of "Malware_U3_W2_L1.exe", including the Dos Header, Nt Headers, File Header, Optional Header, Data Directories, Section Headers, Import Directory, and several utility tools like Address Converter, Dependency Walker, Hex Editor, Identifier, Import Adder, Quick Disassembler, Rebuilder, Resource Editor, and UPX Utility. The main window displays a table titled "Malware_U3_W2_L1.exe" with the following data:

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

Kernel32.dll è una libreria di sistema fondamentale di Windows che gestisce operazioni di basso livello nel sistema operativo, come la gestione della memoria, dei processi e dei thread. È cruciale per il funzionamento di molte applicazioni Windows.

I malware utilizzano Kernel32.dll per eseguire operazioni fondamentali come creare processi nascosti, manipolare la memoria, leggere e scrivere file sensibili, e controllare risorse di sistema senza destare sospetti.



Advapi32.dll

Advapi32.dll è una libreria di sistema di Windows che fornisce funzionalità avanzate per la gestione delle operazioni di sicurezza e delle politiche di accesso, oltre a servizi di sistema come il registro di Windows. I malware utilizzano Advapi32.dll per ottenere e modificare i privilegi di sicurezza, manipolare il registro di Windows per persistenza e configurazione, e gestire i servizi di sistema per nascondersi o per eseguire attività malevole.

MSVCRT.dll

MSVCRT.dll è la libreria runtime di Microsoft Visual C++ che fornisce funzioni standard del linguaggio C, come gestione delle stringhe, input/output, allocazione della memoria e altre funzioni di runtime.

I malware utilizzano MSVCRT.dll per eseguire operazioni standard del linguaggio C, come manipolazione delle stringhe, gestione della memoria e operazioni di input/output necessarie per il funzionamento del codice malevolo.

Wininet.dll

Wininet.dll è una libreria di sistema di Windows che fornisce funzionalità per l'accesso a Internet e alle risorse di rete, come il supporto per i protocolli HTTP e FTP.

I malware utilizzano Wininet.dll per comunicare con server remoti, esfiltrare dati, scaricare ulteriori componenti malevoli o ricevere istruzioni da un server di comando e controllo (C2).

Sezioni

andando ad analizzare le sezioni del malware vediamo che il loro nome è nascosto, quindi possiamo dedurre che il malware sta utilizzando tecniche avanzate per evitare il rilevamento e l'analisi.

Nascondere i nomi delle sezioni rende più difficile per gli analisti di sicurezza identificare e comprendere il comportamento del malware.

The screenshot shows the OllyDbg debugger interface. On the left, the file structure tree displays the file 'Malware_U3_W2_L1.exe' with its various sections and headers. The 'Section Headers [x]' node is currently selected. On the right, a table provides detailed information about the sections:

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	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

Conclusioni

Il malware in analisi dimostra un alto livello di sofisticazione, utilizzando tecniche avanzate per nascondere i nomi delle sue sezioni per evitare il rilevamento sia da parte degli analisti di sicurezza che degli strumenti antivirus..

L'importazione di librerie critiche come Kernel32.dll, Advapi32.dll, MSVCRT.dll e Wininet.dll evidenzia le sue capacità di interagire profondamente con il sistema operativo, gestire la sicurezza e le risorse di sistema, eseguire operazioni standard del linguaggio C e comunicare con risorse di rete.

