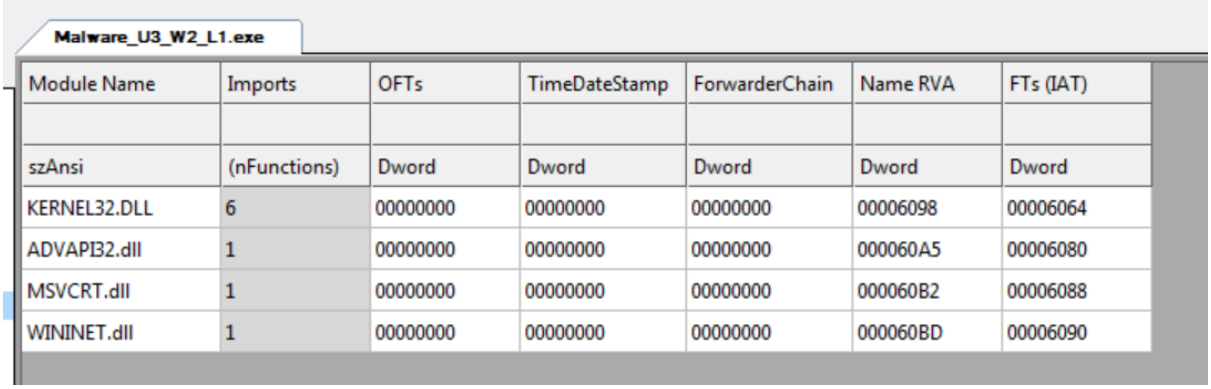
ANALISI DELLE LIBRERIE IMPORTATE
Attraverso l'uso del programma CFF EXPLORER, è possibile condurre una preliminare analisi dei componenti del malware. Nella sezione Directory di Importazione, è possibile esaminare le librerie utilizzate dal malware, consentendo di dedurre alcune delle sue funzionalità principali.


Malware_U3_W2_L1.exe

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

Kernel32.dll: Essenziale in ambienti Windows, fornisce funzioni fondamentali per la gestione della memoria, dei file, degli errori e dei processi, garantendo il corretto funzionamento dei programmi su piattaforma Windows.

Advapi32.dll: Offre funzioni avanzate per la gestione della sicurezza, la manipolazione dei servizi di sistema, la registrazione degli eventi e altre operazioni critiche, essenziale per il funzionamento di vari programmi in un ambiente Windows.

Msvcrt.dll: Associata al compilatore Microsoft Visual C++, questa libreria fornisce funzioni di runtime per programmi scritti in linguaggio C/C++, inclusa la gestione della memoria, la manipolazione delle stringhe e altre funzioni di supporto, garantendo l'esecuzione corretta delle applicazioni dipendenti da questa libreria di runtime.

Wininet.dll: Libreria di sistema su piattaforme Windows dedicata alla gestione delle operazioni di rete e della connettività Internet, fondamentale per applicazioni come browser web e altri programmi che richiedono l'accesso a risorse online.

ANALISI DELLE SEZIONI MALWARE
Sempre nella sezione sinistra di CFF EXPLORER, spostandoci su Section Headers, è possibile visualizzare le sezioni che compongono il malware. Si possono individuare 3 sezioni:

UPX0
UPX1
UPX2

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

Sembra che il malware abbia nascosto il nome originale delle sezioni, quindi non è possibile identificarle.

CONSIDERAZIONI FINALI
Si tratta chiaramente di un malware abbastanza sofisticato, poiché cerca di nascondere il più possibile le informazioni sul suo comportamento. Tuttavia, un'analisi più dettagliata delle librerie suggerisce l'utilizzo di Load Library e Get Process Address, indicando un caricamento in runtime delle librerie e nascondendo quelle utilizzate.