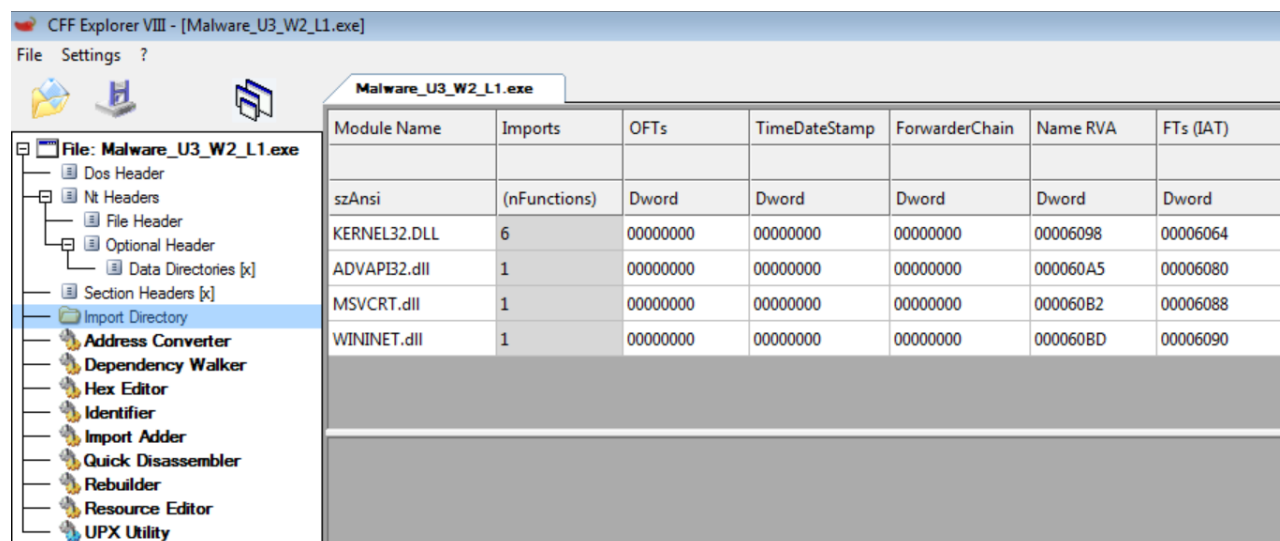


# Relazione Malware

Utilizzando CFF Explorer, osserviamo dalla sezione "import directory" che il malware U3\_W2\_L1 importa quattro librerie:



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

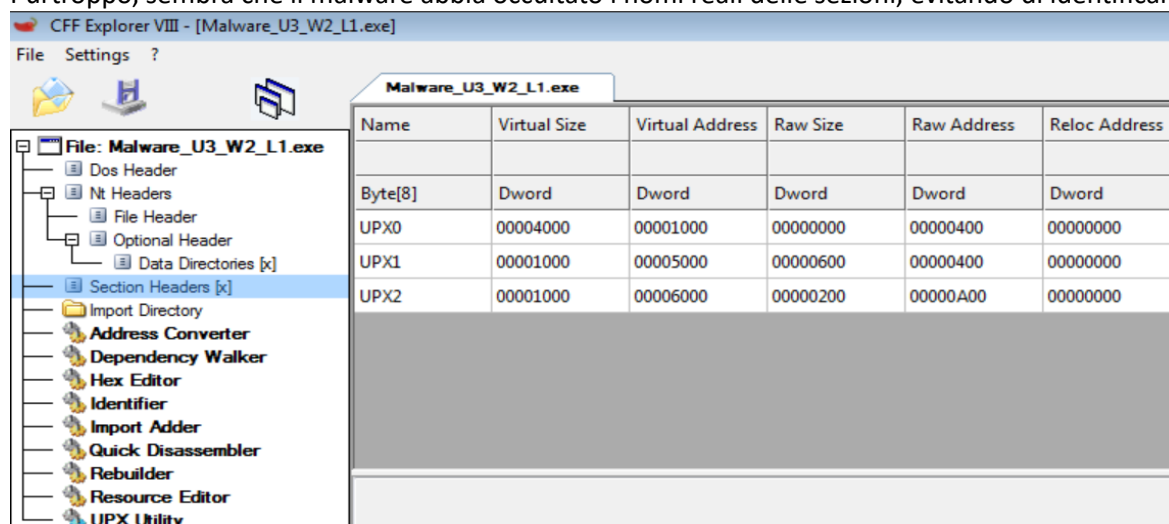
**Kernel32.dll:** Contiene le funzioni principali del sistema operativo, come la gestione della memoria, l'accesso ai file e la gestione dei processi e thread. È una libreria fondamentale per l'esecuzione di molte operazioni a livello di sistema

**Advapi32.dll:** Fornisce funzioni avanzate per la gestione dei registri di Windows, la sicurezza, le autorizzazioni e la gestione dei servizi. Include anche funzioni per la gestione delle chiavi di registro e la configurazione dei servizi di sistema

**Msvcrt.dll:** È una libreria standard del C runtime di Microsoft, utilizzata per la manipolazione delle stringhe, l'allocazione della memoria, le operazioni matematiche e l'input/output dei file. È essenziale per molte applicazioni scritte in linguaggio C e C++

**Wininet.dll:** Include funzioni per la gestione delle comunicazioni di rete attraverso protocolli come HTTP, FTP e NTP. È utilizzata per implementare servizi di rete, inclusi download e upload di file, navigazione web e sincronizzazione di orologi di rete

Da CFF Explorer, nella sezione "section header", vediamo che l'eseguibile è composto da tre sezioni. Purtroppo, sembra che il malware abbia occultato i nomi reali delle sezioni, evitando di identificarne il tipo



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

## Conclusione

Si tratta di un malware che non permette di ottenere molte informazioni sul suo comportamento tramite un'analisi statica di base. Questo è confermato dalla presenza delle funzioni "LoadLibrary" e "GetProcAddress" tra le funzioni importate, suggerendo che il malware importa le librerie durante il runtime, celando così le informazioni sulle librerie importate in precedenza

Malware_U3_W2_L1.exe				
Module Name	Imports	OFTs	TimeStamp	ForwarderChain
00000A98	N/A	00000A00	00000A04	00000A08
szAnsi	(nFunctions)	Dword	Dword	Dword
KERNEL32.DLL	6	00000000	00000000	00000000
ADVAPI32.dll	1	00000000	00000000	00000000
MSVCRT.dll	1	00000000	00000000	00000000
WININET.dll	1	00000000	00000000	00000000
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	