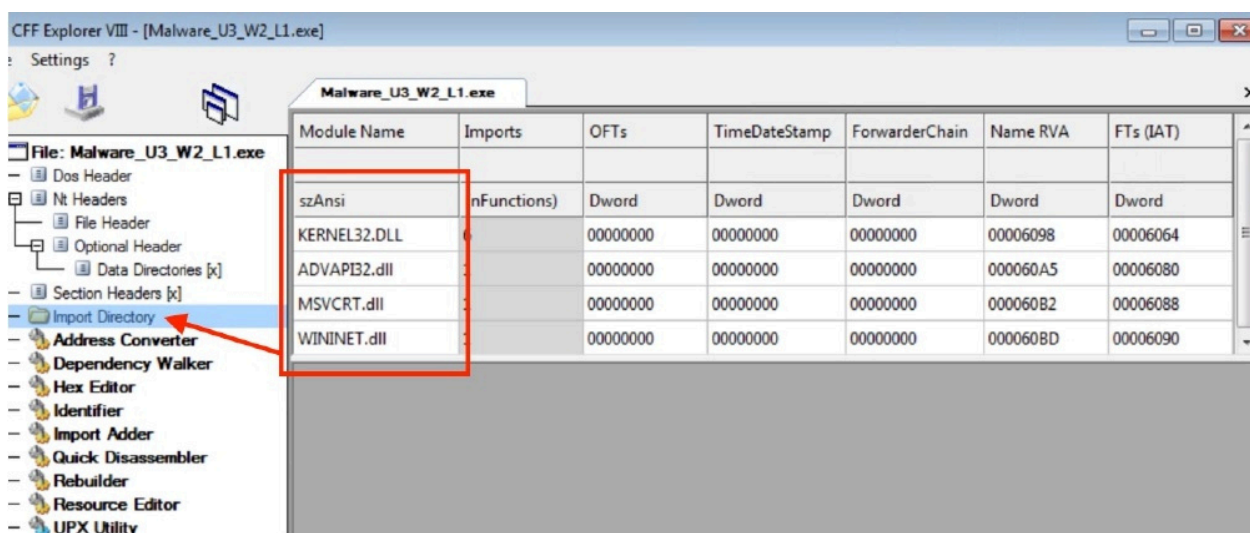


Analisi Malware 1

Librerie:



KERNEL32.DLL:

Contiene le funzioni principali per interagire con il sistema operativo, ad esempio: manipolazione dei file, la gestione della memoria. Questa libreria potrebbe essere utilizzata dal malware per:

- Manipolare file di sistema, gestire processi in background, o creare file temporanei.
- Eseguire codice in modalità kernel e utente, il che può includere l'iniezione di codice in altri processi o l'esecuzione di codice dannoso.
- Modificare le impostazioni di sicurezza

ADVAPI32.DLL:

Fornisce accesso a molte funzionalità avanzate del sistema operativo, come la gestione delle chiavi di registro, i servizi di sicurezza e le funzioni di autenticazione.

Con questa libreria il malware potrebbe:

- Leggere e scrivere nel registro di sistema, il che può essere utilizzato per persistere tra i riavvii, modificare impostazioni di sicurezza, o altre configurazioni di sistema.
- Effettuare una privilege escalation e ottenere accesso non autorizzato a dati riservati, sfruttando le funzioni di gestione degli utenti e dei privilegi di questa libreria.
- Modificare le politiche di sicurezza per permettere l'installazione di altri malware.

MSVCRT.DLL

È una libreria di runtime di Microsoft Visual C++ che fornisce funzioni C standard e funzionalità runtime a numerose applicazioni di Windows. Potrebbe consentire ad un malware di:

- Manipolare o elaborare file

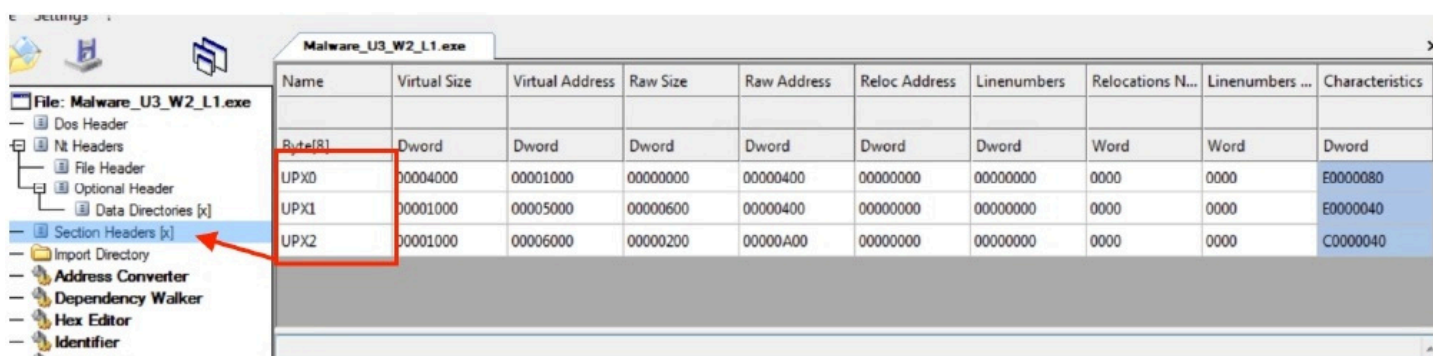
- Mascherare il comportamento del malware

WININET.DLL

Contiene le funzioni per l'implementazione di alcuni protocolli di rete come HTTP, FTP, NTP. Un malware potrebbe utilizzarla per:

- Scaricare ulteriori payload, inviare dati rubati a server di comando e controllo, o attaccare altre macchine sulla stessa rete.
- Può essere usata per manipolare cookie e sessioni di rete, questo potrebbe essere sfruttato per mantenere la persistenza del malware o per intercettare dati sensibili.

Selezioni:



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte(R)	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

Possiamo notare che sono file compressi con **UPX** per rendere più difficile l'analisi