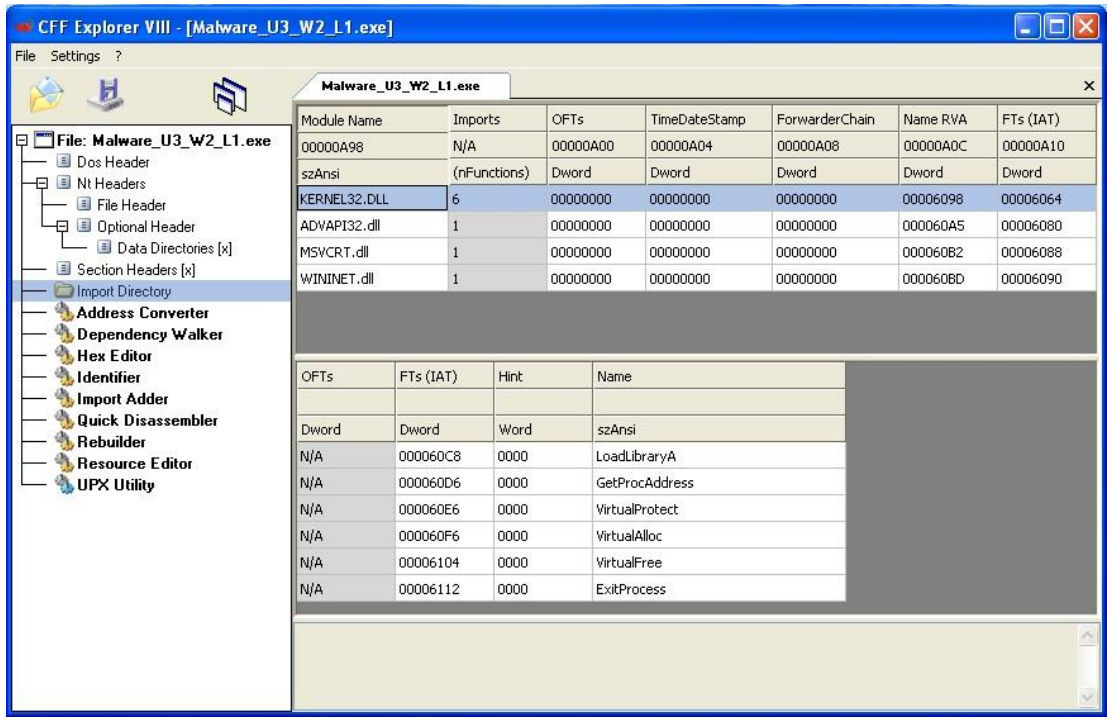
Security Operation

azioni preventive

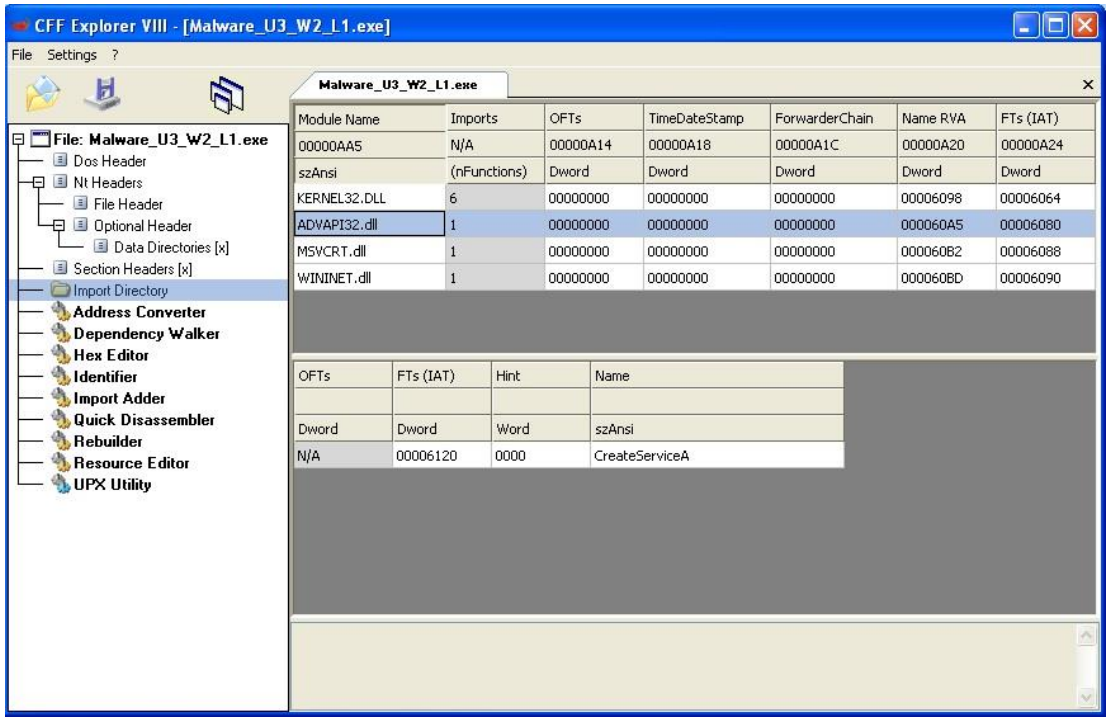
Malware_U3_W2_L1

Orlando Tangari



Libreria KERNEL32.DLL

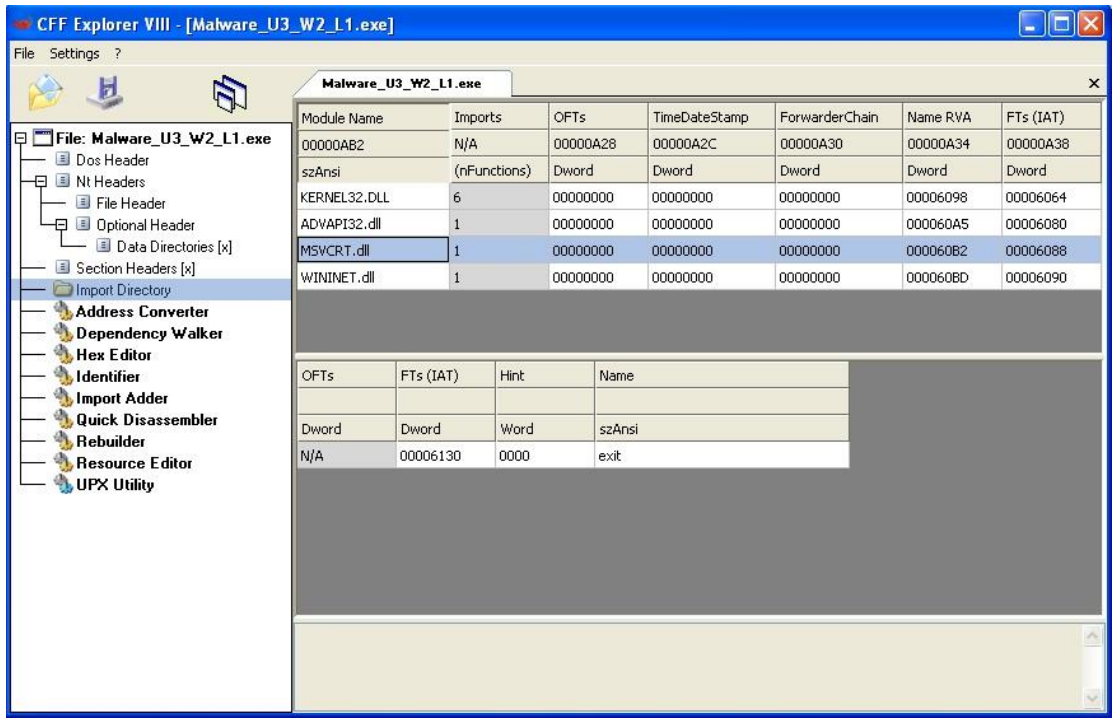
Libreria contenente le funzioni principali per interagire con il sistema operativo.



Libreria ADVAPI32.dll

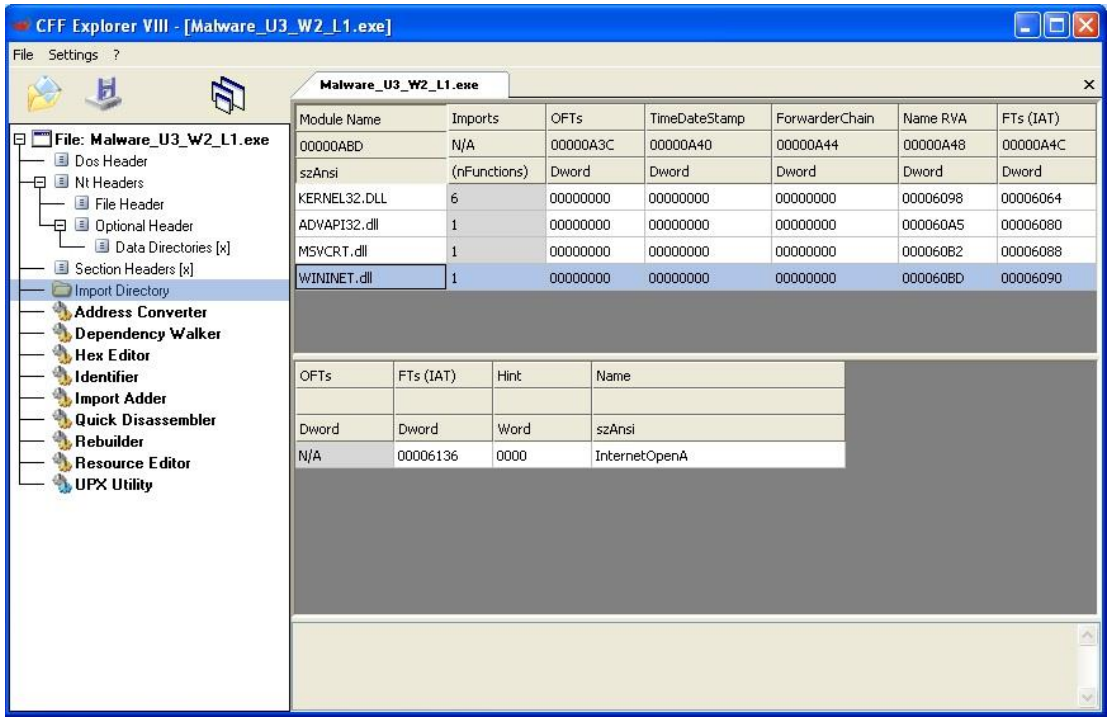
Libreria contenente le funzioni per interagire con i servizi ed i registri del sistema operativo Microsoft.

Librerie importate dal malware (part. 1)



Libreria MSVCRT.dll

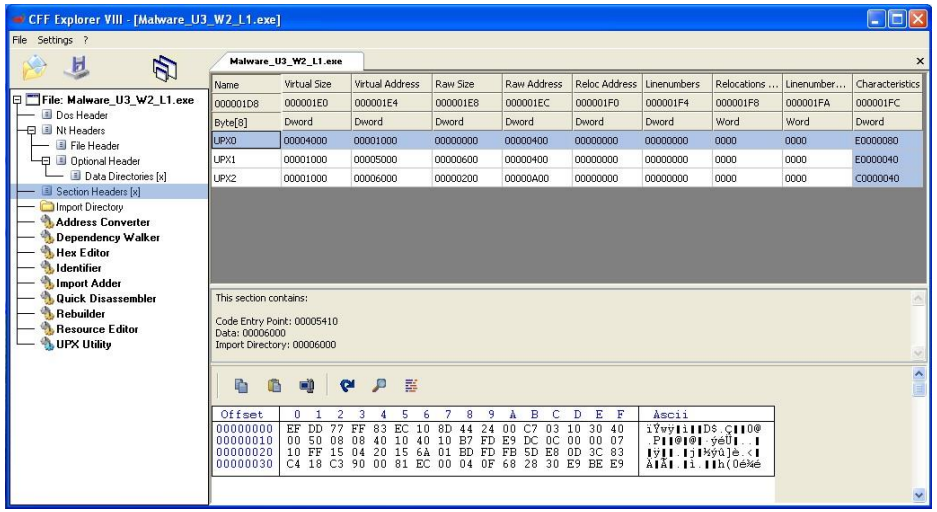
Libreria contenete le funzioni per manipolare stringhe, allocazione memoria e chiamate per input/output in stile linguaggio C.



Libreria WININET.dll

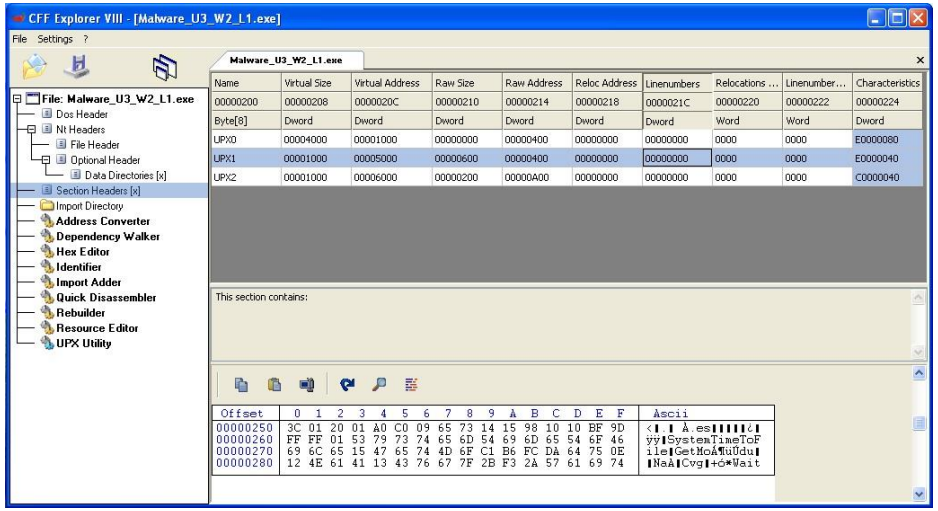
Libreria contenente le funzioni per implementare alcuni protocolli di rete come: HTTP, FTP, NTP.

Librerie importate dal malware (part. 2)



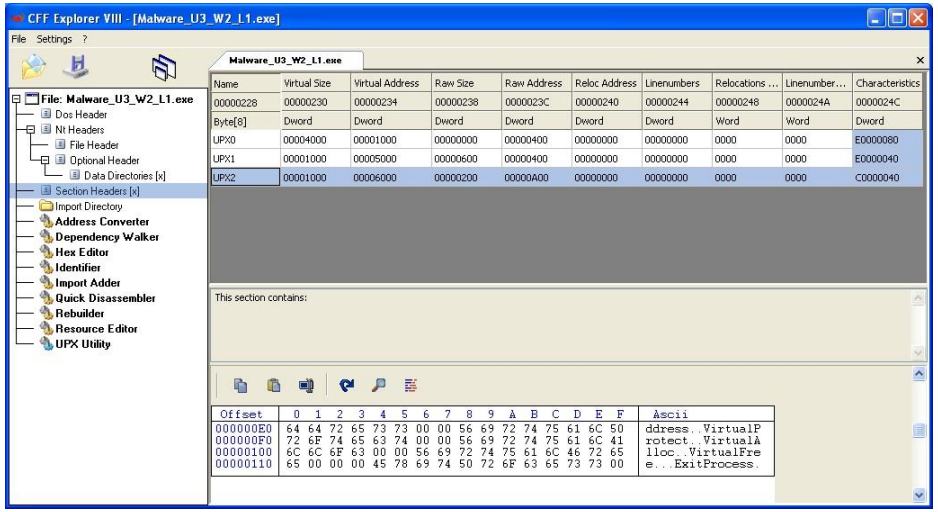
Sezione UPX0

Unione delle sezioni UX1 e UX2 ed essendo tutti e tre dei *packer*, strumenti di tipo UPX, risulta difficile l'analisi di un eseguibile.



Sezione UPX1

Potrebbe essere una sezione *data* visto che contiene dati/variabili del programma eseguibile.



Sezione UPX2

Potrebbe essere una sezione *rdata* visto che include informazioni sulle librerie e le funzioni importanti.

Sezioni in cui si compone il malware

Dall’analisi statica basica, si è giunti alla conclusione che, il malware Malware_U3_W2_L1, crei un oggetto sulla macchina vittima per stabilire una connessione di tipo: HTTP, o FTP, o NTP ma, viste le sezioni UPX di cui è composto, lo fa con uno strato di offuscamento.

Considerazioni finali