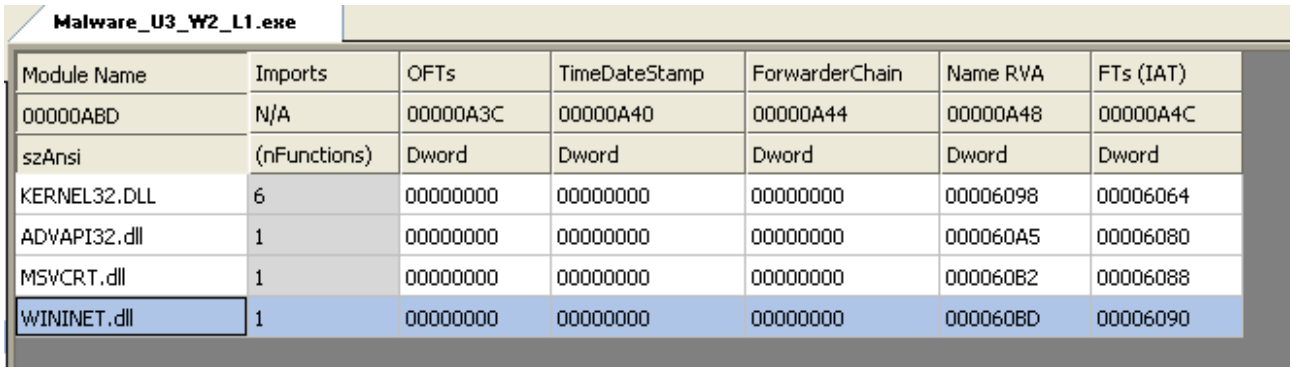
S10 LEZIONE 1

Con riferimento al file eseguibile contenuto nella cartella «Esercizio_Pratico_U3_W2_L1» presente sul desktop della vostra macchina virtuale dedicata all'analisi dei malware, rispondere ai seguenti quesiti:

- Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse;
- Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa;
- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte;

Il file Esercizio_Pratico_U3_W2_L1 analizzato con **CFF Explorer** mostra che il malware importa le seguenti librerie:

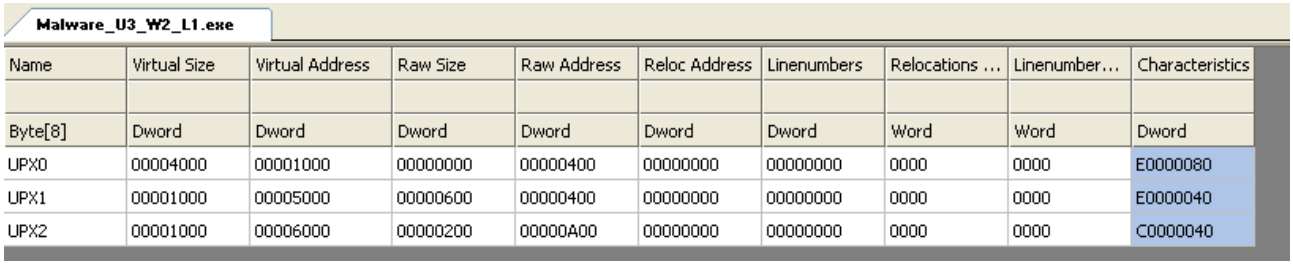


Malware_U3_W2_L1.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00000ABD	N/A	00000A3C	00000A40	00000A44	00000A48	00000A4C
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:** è una libreria di windows che fornisce accesso alle funzionalità di base del sistema operativo (accesso ai file, gestione della memoria, esecuzione thread).
- **ADVAPI32.dll:** un'altra libreria che fornisce accesso alle funzionalità di sicurezza del sistema operativo (autenticazione, autorizzazione e accesso a registro di sistema)
- **MSVCRT.dll:** è una libreria di runtime di C e C++ che fornisce funzioni per la gestione della memoria, input e output e alu.
- **WININET.dll:** libreria windows che fornisce accesso alle funzionalità di rete (connessione siti web, download file e invio mail)

Le seguenti funzioni invece compongono il malware:



Malware_U3_W2_L1.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	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

- **UPX0:** rappresenta la dimensione della sezione *.txt*, contiene il codice eseguibile del malware, è pertanto responsabile dell'esecuizione delle azioni dannose.

- **UPX1:** rappresenta la dimensione della sezione *.data*, contiene i dati statici del malware, ovvero dati che non cambiano durante l'esecuzione (stringhe e costanti)
- **UPX2:** rappresenta la dimensione totale del malware

Considerazione finale:

La presenza di librerie come **WININET.dll**, **DVAPI32.dll**, **KERNEL32.DLL** e **MSVCRT.dll**, in questo contesto suggerisce che il malware potrebbe sfruttare una varietà di funzionalità del sistema operativo Windows per eseguire attività dannose.

Comunicazione e controllo remoto:

Utilizza 'WININET' per stabilire connessioni con server remoti, consentendo al malware di ricevere istruzioni dal server di comando e controllo
Sfrutta 'ADVAPI32' per gestire l'autenticazione e l'autorizzazione, cercando di ottenere privilegi elevati o compromettere l'accesso a risorse di sistema.

Propagazione e persistenza:

Sfrutta 'KERNEL32' per manipolare file e directory, copiando se stesso in posizioni specifiche, creando servizi o modificando le impostazioni di avvio del sistema.

Criptazione e manipolazione dati:

Utilizza 'ADVAPI32' per operazioni di crittografia e decrittografia, nascondendo il proprio codice o manipolando dati sensibili.
Potrebbe utilizzare 'MSVCRT' per gestire operazioni di input/output e manipolare dati in memoria

Attività di rete e download:

Sfrutta 'WININET' per scaricare ulteriori componenti dannosi da server remoti, inoltre potrebbe eseguire attacchi di phishing e monitorare attività di rete dell'utente.

Elusione e camuffamento:

Sfrutta 'KERNEL32' per manipolare processi e thread, cercando di evitare la rilevazione antivirus o interrompendo processi di sicurezza
Utilizza 'ADVAPI32' per manipolare il registro di sistema, nascondendo tracce o configurandosi in modo da avviarsi automaticamente con il sistema.