



# CONSEGNA S10-L1

analisi malware statica



# INDICE

- Traccia (pg.3)
- Librerie importate dal malware e spiegazione (pg.4->5)
- Sezioni in cui si divide il malware più spiegazione (pg.6)
- Considerazioni finali (pg.7)



### Traccia:

Nella lezione teorica del mattino, abbiamo visto come recuperare informazioni su un malware tramite l'analisi statica basica.

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

FILE MODIFICHE VISUALIZZA IMPOSTAZIONI DISPOSITIVI AIUTO

**CFF Explorer VIII - [Malware\_U3\_W2\_L1.exe]**

File Settings ?

Malware\_U3\_W2\_L1.exe


File: Malware\_U3\_W2\_L1.exe

- Dos Header
- Nt Headers
  - File Header
  - Optional Header
  - Data Directories [x]
- Section Headers [x]
- Import Directory

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

come si può notare nello screenshot le librerie importate sono 4:

- KERNEL32.DLL = La KERNEL32.dll è cruciale per l'esecuzione dei programmi su piattaforma Windows, offrendo servizi di base come l'allocazione di memoria, l'accesso al Registro di sistema e la sincronizzazione dei processi. La sua presenza e corretta funzionalità sono vitali per il corretto operato del sistema operativo e delle applicazioni che ne fanno uso.

- 
- ADVAPI32.dll= La libreria ADVAPI32.dll è un componente chiave nei sistemi operativi Windows, contenente funzioni avanzate per la gestione di servizi, sicurezza e registri di sistema. Essa supporta operazioni come l'autenticazione degli utenti, l'accesso ai servizi di crittografia, la gestione degli eventi del sistema e la manipolazione del Registro di sistema.
  - MSVCRT.dll=La libreria MSVCRT.dll è una componente critica nei sistemi operativi Windows e contiene funzioni di runtime della libreria C standard di Microsoft Visual C++. Questa DLL (Dynamic Link Library) è fondamentale per l'esecuzione di programmi sviluppati con il compilatore Microsoft Visual C++. La presenza e il corretto funzionamento di MSVCRT.dll sono cruciali per l'esecuzione di programmi basati su Visual C++ nei sistemi Windows.
  - WININET.dll=WININET.dll è ampiamente utilizzata da applicazioni Windows per supportare operazioni di navigazione web, scaricare dati da Internet e interagire con risorse online. La corretta funzionalità di questa libreria è cruciale per le applicazioni che dipendono da connessioni di rete e interazioni su Internet su piattaforma Windows.

Possiamo notare che tutte le librerie importate riguardano i sistemi principali della macchina windows ovvero sono essenziali per il corretto funzionamento del sistema

CFF Explorer VIII - [Malware\_U3\_W2\_L1.exe]

File Settings ?

Malware\_U3\_W2\_L1.exe

File: Malware\_U3\_W2\_L1.exe

- Dos Header
- Nt Headers
  - File Header
  - Optional Header
    - Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter
- Dependency Walker

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

nella section Headers possiamo trovare le parti che compongono il malware e sono

- UPX= (Ultimate Packer for eXecutables) è uno strumento di compressione e decompressione di eseguibili, progettato per ridurre le dimensioni dei file eseguibili e migliorare la distribuzione del software. In relazione a un malware potrebbe indicare una versione o una configurazione specifica associata a pratiche illegali di modifica di file eseguibili per scopi dannosi.



## Considerazioni finali

Per quanto riguarda il malware in se non si può essere sicuri di che tipo di malware si tratta in quanto l'analisi svolta e' statica e ciò non permette di vedere il programma in azione, però possiamo dedurre dai vari nomi dei file e dal fatto che ci siano librerie atte ad attaccare il sistema della macchina target che probabilmente si tratta di un attacco DDoS in quanto il programma presenta diversi eseguibili che potrebbero andare a sovraccaricare un determinato servizio così da renderlo irraggiungibile