

PRATICA S9L2:

Traccia:

Rispondere ai seguenti quesiti, con riferimento al file eseguibile notepad-classico.exe contenuto in questo file compresso:

<https://drive.google.com/file/d/1HNnJDSY7FbD1KHfiRzA2wVNHhzTJndUD/view?usp=s>
haring

- Indicare le **librerie** importate dal malware, fornendo una descrizione per ognuna di esse tramite AI;
- Indicare le **sezioni** di cui si compone il malware, fornendo una descrizione per ognuna di essa tramite AI.

Suggerimento: ChatGPT (o altri LLM) possono ricevere in input degli screenshot da analizzare e cerca librerie caricate dinamicamente nei testi del codice.

LIBRERIE MALWARE

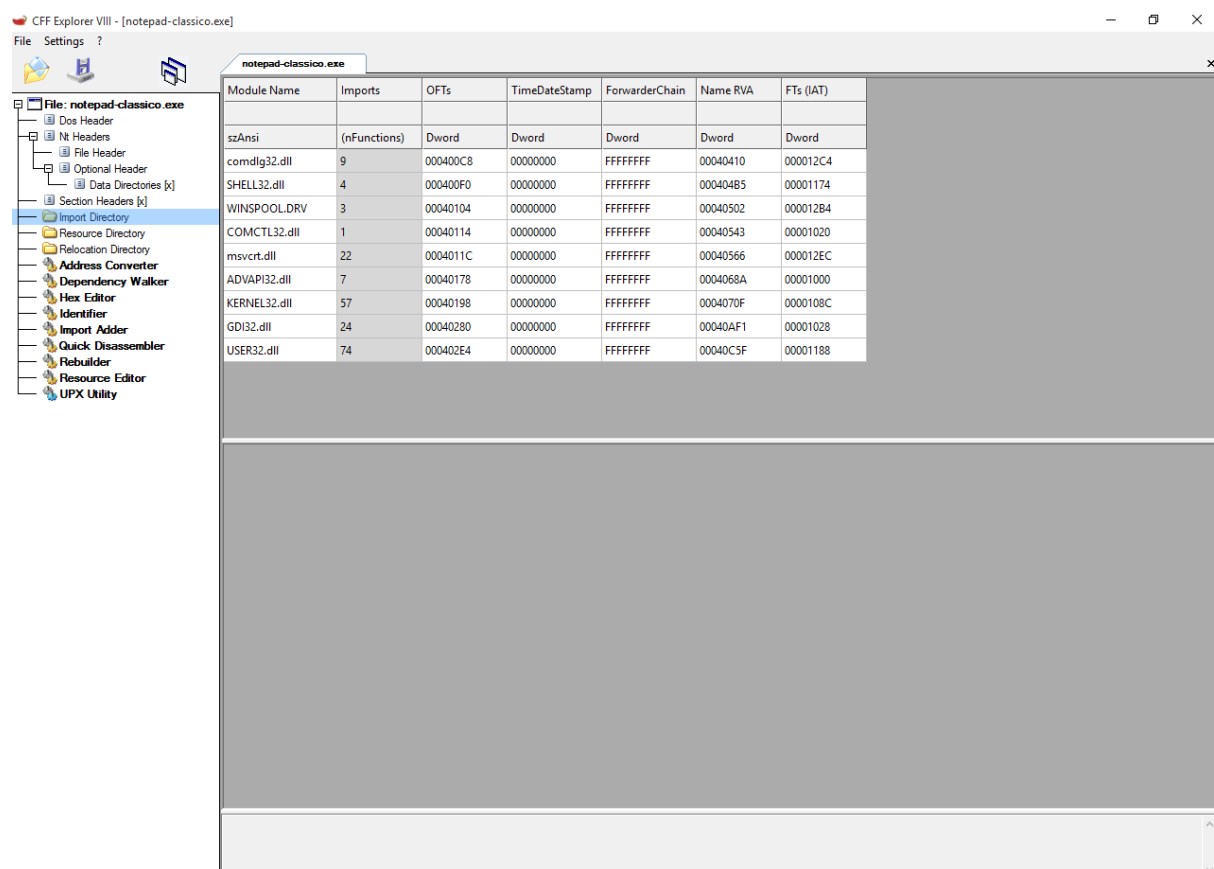
Ho aperto **CFF Explorer VII** e ho caricato *notepad++.exe* per analizzare la sua struttura interna. Mi sono concentrato sulla **Import Directory**, che mostra tutte le **DLL** (librerie dinamiche) da cui l'eseguibile dipende. Questo passaggio è fondamentale per capire quali funzionalità esterne vengono utilizzate e come il programma interagisce con il sistema operativo.

Ecco le librerie che ho trovato, con una breve descrizione di ciascuna:

- **comdlg32.dll:** è la libreria che si occupa delle finestre di dialogo comuni. Quando apri un file, salvi un documento o scegli una stampante, è lei che gestisce quella finestra che ti permette di navigare tra le cartelle. È una sorta di ponte tra l'applicazione e il file system.
- **SHELL32.dll:** è il cuore dell'interfaccia grafica di Windows. Contiene le funzioni che permettono di visualizzare il desktop, le icone, le cartelle e di interagire con Esplora risorse. Se pensi a tutto ciò che rende Windows "Windows" dal punto di vista visivo, questa libreria è la regista.
- **COMCTL32.dll:** fornisce i controlli grafici avanzati. Parliamo di elementi come le barre di scorrimento, le liste a discesa, le schede e altri componenti che rendono le finestre interattive e funzionali. È come il set di strumenti che gli sviluppatori usano per costruire interfacce utente moderne.
- **msvcrt.dll:** è la libreria runtime del linguaggio C di Microsoft. Contiene funzioni fondamentali per la gestione delle stringhe, dei numeri, dell'input/output e della

memoria. È utilizzata da moltissimi programmi, soprattutto quelli scritti in C o C++, per eseguire operazioni di base.

- **ADVAPI32.dll:** gestisce le funzioni avanzate legate alla sicurezza, ai servizi di Windows e al registro di sistema. Se un programma deve accedere a informazioni sugli utenti, modificare chiavi di registro o interagire con i servizi di sistema, passa da questa libreria.
- **KERNEL32.dll:** è il nucleo operativo del sistema. Gestisce la memoria, i processi, i thread, i file e le operazioni di input/output. È una delle librerie più critiche: praticamente ogni programma che gira su Windows la utilizza per comunicare con l'hardware e il sistema operativo.
- **GDI32.dll:** è responsabile della grafica. Si occupa di disegnare sullo schermo: linee, forme, testo, immagini. È la libreria che permette a Windows di visualizzare contenuti grafici in modo efficiente, sia nelle applicazioni che nell'interfaccia utente.
- **USER32.dll:** gestisce l'interazione con l'utente. È lei che controlla le finestre, i pulsanti, le caselle di testo, la tastiera e il mouse. Ogni volta che clicchi, digiti o interagisci con un programma, USER32 è coinvolta nel processo.



CFF Explorer VIII - [notepad-classico.exe]

File Settings ?

notepad-classico.exe

Module Name	Imports	OFs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
comdlg32.dll	9	000400C8	00000000	FFFFFFFF	00040410	000012C4
SHELL32.dll	4	000400F0	00000000	FFFFFFFF	000404B5	00001174
WINSPOOL.DRV	3	00040104	00000000	FFFFFFFF	00040502	000012B4
COMCTL32.dll	1	00040114	00000000	FFFFFFFF	00040543	00001020
msvcrt.dll	22	0004011C	00000000	FFFFFFFF	00040566	000012EC
ADVAPI32.dll	7	00040178	00000000	FFFFFFFF	0004068A	00001000
KERNEL32.dll	57	00040198	00000000	FFFFFFFF	0004070F	0000108C
GDI32.dll	24	00040280	00000000	FFFFFFFF	00040AF1	00001028
USER32.dll	74	000402E4	00000000	FFFFFFFF	00040C5F	00001188

SEZIONI MALWARE

Sempre con **CFF Explorer VII** sono andato a vedere la **Section Headers**, dove sono elencate tutte le sezioni principali del file eseguibile. Le sezioni del file PE sono:

- **.text:** Questa è la parte più importante: contiene il **codice eseguibile** vero e proprio. Sono le istruzioni che la CPU esegue. Se voglio modificare il comportamento del programma o analizzare cosa fa, è qui che vado a cercare. È una sezione in sola lettura e marcata come eseguibile.
- **.data:** Qui ci sono i **dati modificabili**, come le variabili globali e statiche. Durante l'esecuzione, il programma può leggere e scrivere in questa sezione. Se ci sono contatori, flag, buffer o strutture che cambiano nel tempo, probabilmente stanno qui.
- **.rsrc:** Questa sezione contiene tutte le **risorse** del programma: icone, immagini, menu, dialoghi, stringhe localizzate. Non è eseguibile, ma è fondamentale per la parte visiva e interattiva. Se il programma ha una GUI, molto di quello che vedo a schermo viene da qui.
- **.idata:** Questa è la **Import Directory**, dove il programma tiene traccia delle **funzioni esterne** che usa, prese da DLL di sistema o da librerie personalizzate. È qui che vedo quali API vengono chiamate e da quali moduli. Se voglio capire le dipendenze o analizzare il comportamento a livello di sistema, questa sezione è cruciale.

