

S9L2

Traccia:

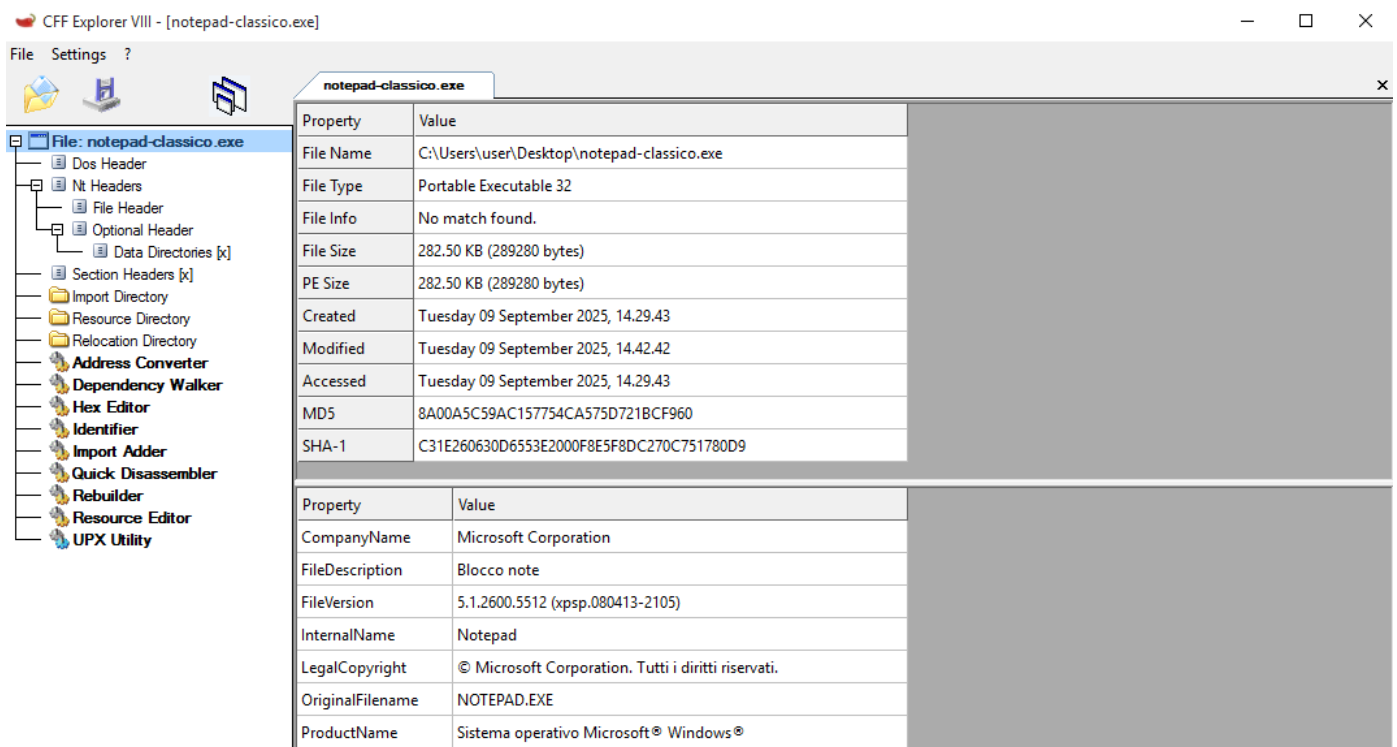
Rispondere ai seguenti quesiti, con riferimento al file eseguibile **notepad-classico.exe** contenuto in questo [file compresso](https://drive.google.com/file/d/1HNnJDSY7FbD1KHfiRzA2wVNHhzTJndUD/view?usp=sharing):

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

- 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.

L'esercizio di oggi si concentra sull'analisi malware, per farlo useremo CFF Explorer. E' stato fornito un file compresso **notepad-classico.exe**, che al suo interno contiene un malware, tramite l'ausilio di CFF cercheremo di identificare le **librerie** e le **sezioni**, descrivendo ognuna di esse.



Property	Value
File Name	C:\Users\user\Desktop\notepad-classico.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	282.50 KB (289280 bytes)
PE Size	282.50 KB (289280 bytes)
Created	Tuesday 09 September 2025, 14.29.43
Modified	Tuesday 09 September 2025, 14.42.42
Accessed	Tuesday 09 September 2025, 14.29.43
MD5	8A00A5C59AC157754CA575D721BCF960
SHA-1	C31E260630D6553E2000F8E5F8DC270C751780D9

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Blocco note
FileVersion	5.1.2600.5512 (xpsp.080413-2105)
InternalName	Notepad
LegalCopyright	© Microsoft Corporation. Tutti i diritti riservati.
OriginalFilename	NOTEPAD.EXE
ProductName	Sistema operativo Microsoft® Windows®

Dopo aver aperto il malware con CFF, andiamo sulla sezione **Import directory**, questa sezione elenca tutte le **DLL** e le funzioni che il programma importa ed esegue.

Module Name	Imports	Size	Imported Name	Imported Name	Imported Name	Imported Name	Imported Name
szAnsi	(nFunctions)	Dword	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	

comdlg32.dll: Questa DLL gestisce le **finestre di dialogo comuni** (Common Dialog Boxes), come quelle per l'apertura, il salvataggio o la stampa di file.

SHELL32.dll: Questa libreria fornisce funzionalità relative alla **Shell di Windows**, che include elementi come il desktop, il menu Start e la gestione dei file e delle cartelle. È fondamentale per la gestione delle operazioni del sistema operativo.

WINSPOOL.DRV: Questa DLL è il driver di spooling della stampante di Windows e gestisce tutte le **funzionalità di stampa**.

COMCTL32.dll: Questa libreria fornisce i **controlli comuni** (Common Controls) di Windows, come pulsanti, caselle di testo, barre di scorrimento e altre interfacce utente standard.

msvcrt.dll: Questa DLL è la **Microsoft Visual C++ Runtime Library**, che contiene funzioni essenziali per i programmi scritti in C e C++. Include le funzioni per l'input/output di base, la gestione della memoria e altre operazioni di runtime.

ADVAPI32.dll: Questa libreria fornisce funzioni **avanzate dell'API di Windows**, come la gestione del registro di sistema, dei servizi e della sicurezza. È cruciale per le operazioni che richiedono privilegi o interazioni a un livello più profondo del sistema. **Le sue funzioni sono spesso usate per rendere persistente il malware nel sistema.**

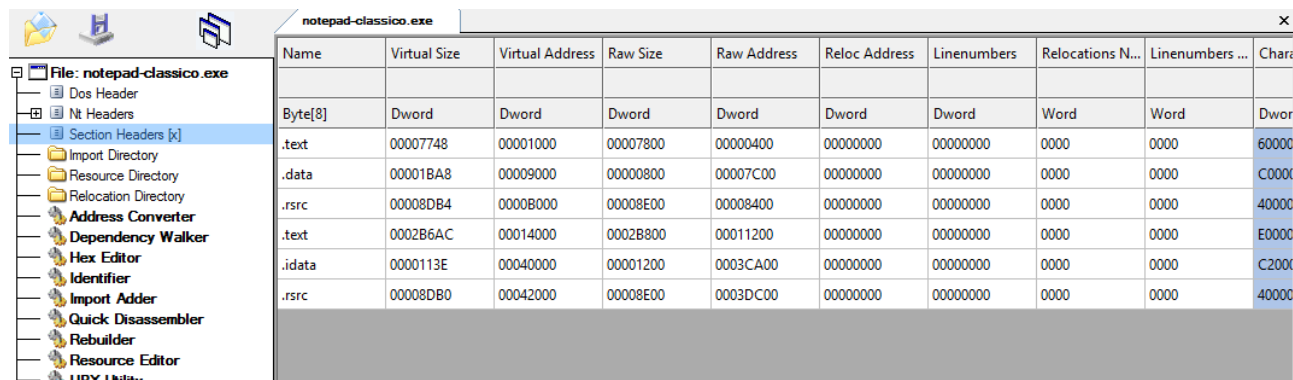
KERNEL32.dll: Questa è una delle librerie più importanti di Windows. Contiene le **funzioni del kernel**, che gestiscono l'accesso e la gestione della memoria, i processi e i thread. È la libreria principale per il funzionamento di base del sistema operativo. **Questa libreria è critica per il malware perché contiene funzioni che possono manipolare i processi e la memoria del sistema.**

GDI32.dll: Questa DLL fornisce le funzioni del **Graphic Device Interface (GDI)** per le operazioni grafiche di base, come il disegno di linee, poligoni e testo sullo schermo.

USER32.dll: Questa libreria gestisce l'**interfaccia utente**, inclusa la creazione e la gestione delle finestre, l'elaborazione dei messaggi di input (come quelli del mouse e della tastiera) e l'interazione generale con l'utente.

Per quanto riguarda le **sezioni**, possiamo trovarle in **Selection Headers [x]**.

In un'analisi di malware, un aspetto cruciale è controllare i nomi e le proprietà delle sezioni. I malware usano spesso tecniche per eludere il rilevamento (**nomi di sezioni atipici** come .evil, .malware, **alta entropia** che suggerisce contenuti **compressi o criptati**)



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Chara
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dwor
.text	00007748	00001000	00007800	00000400	00000000	00000000	0000	0000	60000
.data	00001BA8	00009000	00000800	00007C00	00000000	00000000	0000	0000	C0000
.rsrc	00008DB4	0000B000	00008E00	00008400	00000000	00000000	0000	0000	40000
.text	0002B6AC	00014000	0002B800	00011200	00000000	00000000	0000	0000	E0000
.idata	0000113E	00040000	00001200	0003CA00	00000000	00000000	0000	0000	C2000
.rsrc	00008DB0	00042000	00008E00	0003DC00	00000000	00000000	0000	0000	40000

Analisi delle sezioni

Normalmente, un file eseguibile ha una singola istanza per ogni sezione, come **.text**, **.data** e **.rsrc**. In questo caso, vediamo che le sezioni sono duplicate;

.text (prima istanza): Questa sezione è la prima e principale del file. Ha una **dimensione virtuale** di 00007748 e una **dimensione grezza (raw)** di 00007800. Questa sezione contiene il **codice eseguibile** del programma. Il flag "Characteristics" 60000020 indica che la sezione contiene codice, è eseguibile e leggibile.

.data (prima istanza): Questa sezione contiene le **variabili inizializzate** e i **dati globali** del programma. Il flag "Characteristics" C0000040 indica che è scrivibile, leggibile e contiene dati inizializzati.

.rsrc (prima istanza): Questa sezione contiene le **risorse del programma**, come le icone e i menu. Il flag 40000040 indica che è leggibile e contiene dati inizializzati.

.text (seconda istanza): Questa è la prima anomalia. Un eseguibile normale non dovrebbe avere due sezioni .text. Questo potrebbe suggerire una tecnica di offuscamento o di **compressione del codice** utilizzata da un packer o da un malware. Il flag E0000020 indica che è eseguibile, leggibile e **scrivibile**, una combinazione insolita e sospetta, tipica dei malware che auto-modificano il proprio codice in memoria.

.data (seconda istanza): Anche questa è una sezione **.data** duplicata, il che è un'altra anomalia. Il flag C0000040 è simile a quello della prima istanza.

.rsrc (seconda istanza): Sezione **.rsrc** duplicata. Il flag 40000040 è simile a quello della prima istanza.

La presenza di sezioni duplicate, in particolare quella **.text** che è anche **scrivibile**, è un forte segnale di comportamento anomalo. Se questo file non è stato impacchettato da un programma legittimo, è molto probabile che si tratti di un **malware**.