Esercizio Malware

Abbiamo aperto un file eseguibile **"notepad-classico.exe"** con CFF Explorer e nella sezione Import Directory, vengono mostrate le librerie (DLL) importate dal programma. Ecco una descrizione dettagliata di ogni libreria, con particolare attenzione al loro possibile utilizzo da parte di un malware.

szAnsi: Sembra essere un riferimento interno a una funzione di conversione stringhe ANSI. Non è una libreria di sistema standard. Potrebbe essere usata per manipolare stringhe, decodificare dati o gestire comunicazioni in formato testuale.

comdlg32.dll: Fornisce le Common Dialog Boxes di Windows, come finestre per Apri, Salva, selezione font e colori. Il malware potrebbe usarla per mostrare finestre apparentemente legittime e ingannare l'utente.

SHELL32.dll: Contiene funzioni per interagire con l'**interfaccia grafica di Windows** e gestire **file, cartelle, collegamenti** e altre risorse del sistema. Un malware può sfruttarla per copiare/spostare file, aprire cartelle, creare collegamenti o manipolare l'Esplora risorse.

WINSPOOL.DRV: Gestisce le **code di stampa** e le funzioni per inviare dati alla stampante. Potrebbe essere sfruttata per rubare documenti inviati in stampa o nascondere dati in lavori di stampa.

COMCTL32.dll: Contiene i **controlli grafici comuni** di Windows (bottoni, liste, barre di scorrimento, ecc.). Potrebbe essere utilizzata per creare **finte finestre** o interfacce per trarre in inganno l'utente.

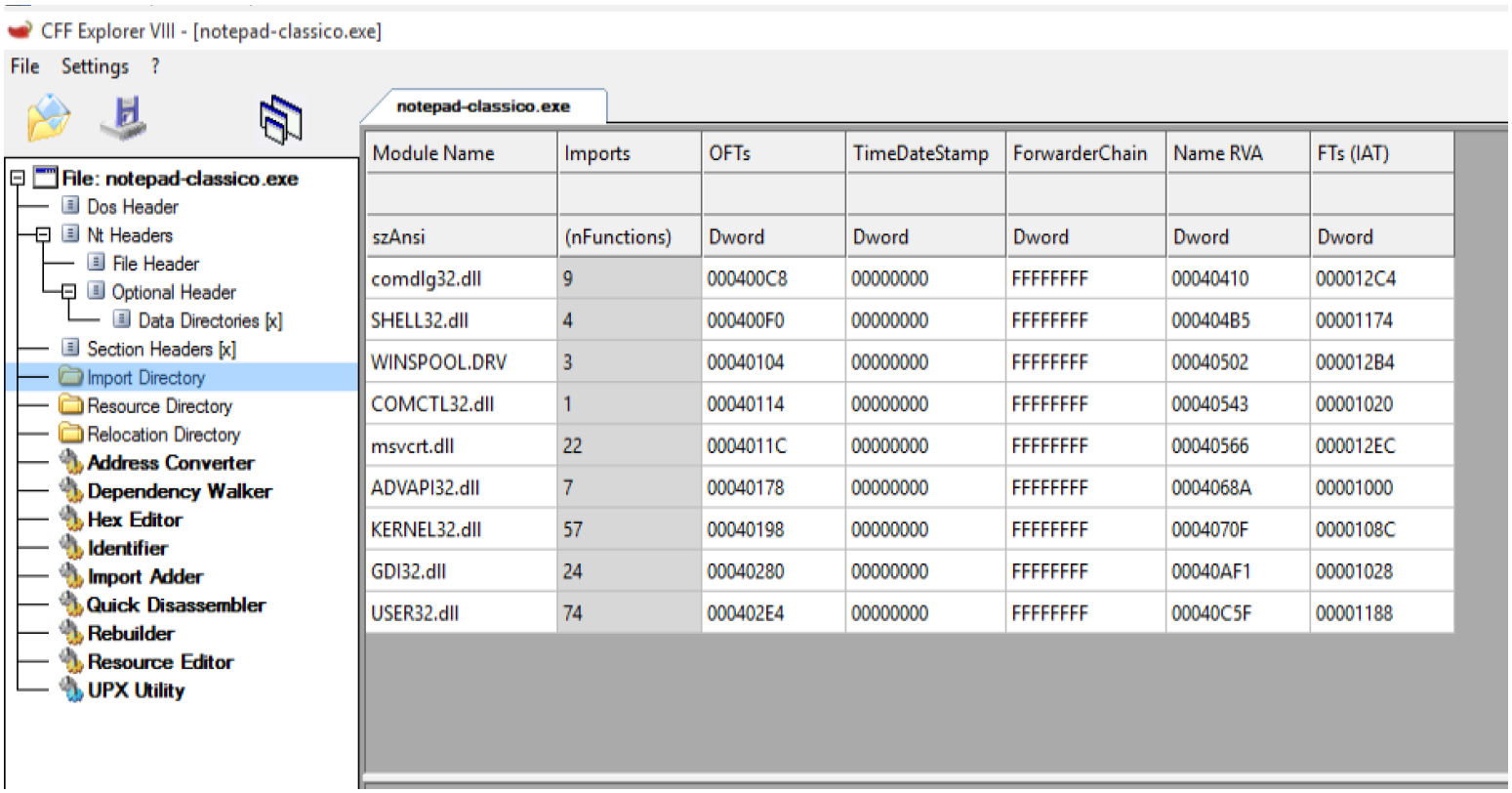
msvcrt.dll: La **Microsoft Visual C Runtime Library** fornisce funzioni base per la gestione di **stringhe, memoria, I/O, matematica** e altro. Un malware la usa spesso per funzioni generali, come leggere/scrivere file, allocare memoria o manipolare buffer.

ADVAPI32.dll: Contiene funzioni avanzate per la gestione di **servizi Windows, registro di sistema, token di sicurezza** e criptografia. Potrebbe essere usata per **modificare il registro**, installare servizi malevoli o alterare i permessi di sicurezza.

KERNEL32.dll: La libreria principale per interagire con il **kernel di Windows**. Contiene funzioni per **processi, thread, memoria, file e I/O**. Essenziale per malware: può creare processi nascosti, leggere/scrivere file, iniettare codice o terminare antivirus.

GDI32.dll: Gestisce la **grafica** e il **disegno di elementi su schermo**: testi, immagini, finestre, ecc. Potrebbe essere sfruttata per **catturare schermate**, visualizzare falsi messaggi o alterare l'interfaccia grafica.

USER32.dll: Contiene funzioni per gestire **interfaccia grafica, input dell'utente, finestre e messaggi di sistema**. Spesso usata dai malware per **intercettare input da tastiera** (keylogging), simulare click o creare popup falsi.

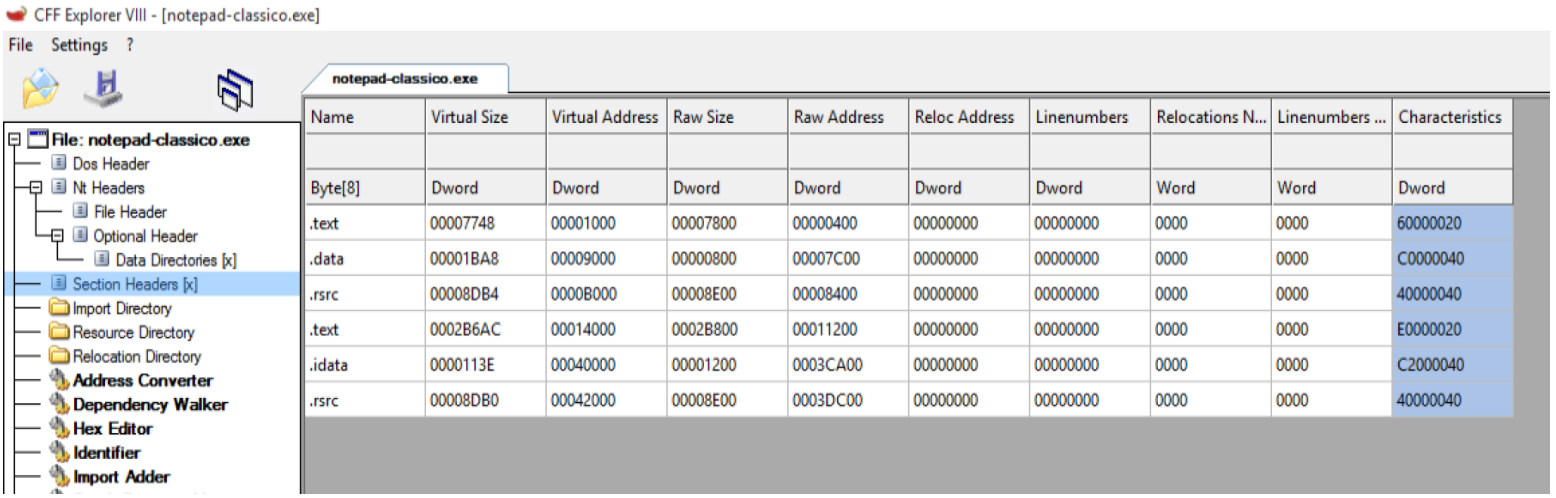


Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
comdlg32.dll	9	000400C8	00000000	FFFFFFFF	00040410	000012C4
SHELL32.dll	4	000400F0	00000000	FFFFFFFF	000404B5	00001174
WINSPOOL.DRV	3	00040104	00000000	FFFFFFFF	00040502	000012B4
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

Ora vedo la tabella delle **Section Headers** del file **notepad-classico.exe** aperto con **CFF Explorer**.
Questa sezione mostra le diverse **sezioni del file PE** (Portable Executable), che contengono **codice, dati, risorse e importazioni**.
Sezioni trovate nel file:

Sezione	Descrizione	Possibile utilizzo da parte del malware
.text	Contiene il **codice eseguibile principale** del programma. È la sezione dove si trovano le istruzioni che la CPU esegue.	Il malware può inserire qui **payload malevolo**, codice per keylogging, furto dati o connessioni remote.

.data	Contiene **dati statici e variabili globali** che il programma usa in lettura/scrittura.	Un malware può usarla per **memorizzare configurazioni**, **token**, **chiavi di decrittazione** o persino URL dei server C2.
.rsrc *(prima)*	Contiene le **risorse del programma**, come icone, immagini, cursori, menu e file incorporati.	I malware spesso nascondono qui **payload criptati**, eseguibili aggiuntivi o dati per l'esecuzione successiva (**fileless malware**).
.text *(seconda, sospetta)*	È anomalo trovare **due sezioni .text**: potrebbe contenere **codice offuscato o iniettato**.	Potrebbe essere usata per **eseguire funzioni malevole**, come exploit, download di payload aggiuntivi o evasione antivirus.
.idata	Contiene la **Import Directory**, ossia le informazioni sulle librerie (DLL) e le API che il programma richiama.	Nel malware è cruciale perché mostra **quali funzioni di sistema vengono usate**: ad esempio `CreateProcess`, `InternetOpenUrl`, `RegSetValueEx`, ecc.
.rsrc *(seconda)*	Presenza insolita di **due sezioni .rsrc**: spesso usata per nascondere **payload cifrati**, immagini che in realtà contengono codice, oppure chiavi di decrittazione.	Potrebbe indicare **packing o offuscamento avanzato**, tipico dei malware che cercano di bypassare gli antivirus.



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00007748	00001000	00007800	00000400	00000000	00000000	0000	0000	60000020
.data	00001BA8	00009000	00000800	00007C00	00000000	00000000	0000	0000	C0000040
.rsrc	00008DB4	0000B000	00008E00	00008400	00000000	00000000	0000	0000	40000040
.text	0002B6AC	00014000	0002B800	00011200	00000000	00000000	0000	0000	E0000020
.idata	0000113E	00040000	00001200	0003CA00	00000000	00000000	0000	0000	C2000040
.rsrc	00008DB0	00042000	00008E00	0003DC00	00000000	00000000	0000	0000	40000040