

Esercizio_S8_L2_Analisi_Malware

Consegna

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

<https://drive.google.com/file/d/1HNnJDSY7FbD1KHfRzA2wVNHhzTJndUD/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.

Facoltativo:

- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte ed elaborate con AI.
- Analisi Dinamica: Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

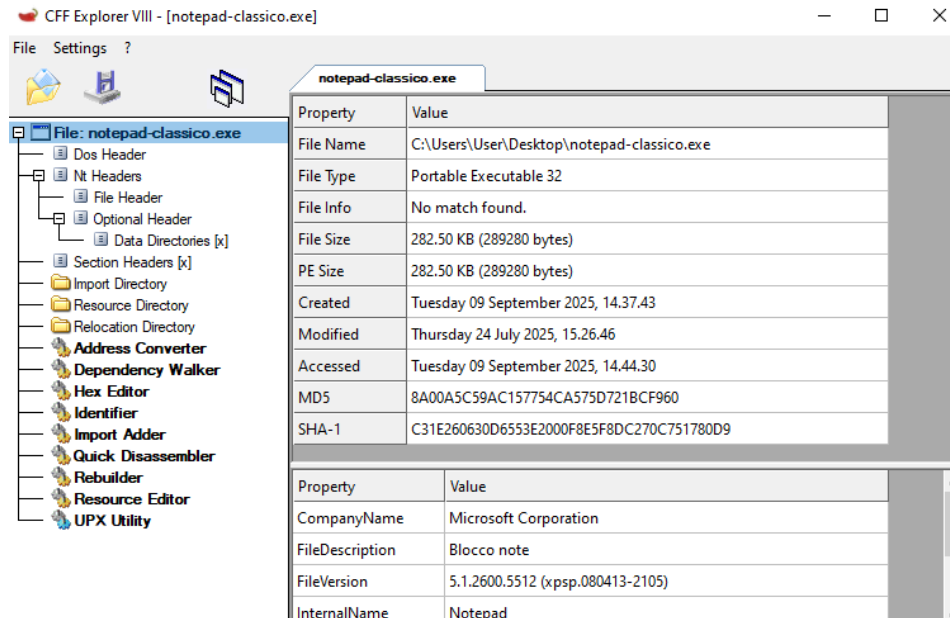
Setup Laboratorio

Per lo svolgimento di questo esercizio verrà utilizzata una VM con Windows 10 dedicata per l'appunto all'analisi di Malware.

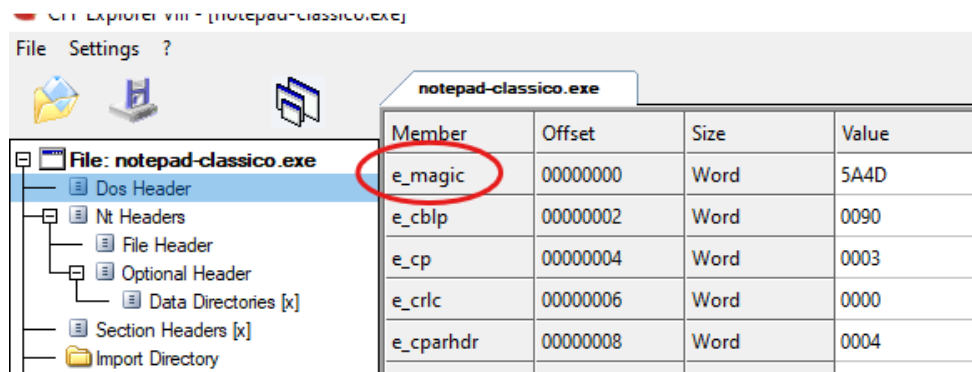
Nella macchina è stata installata la suite **FlareVM** per soddisfare qualunque sfida ci presenti il progetto di analisi.

Analisi Statica

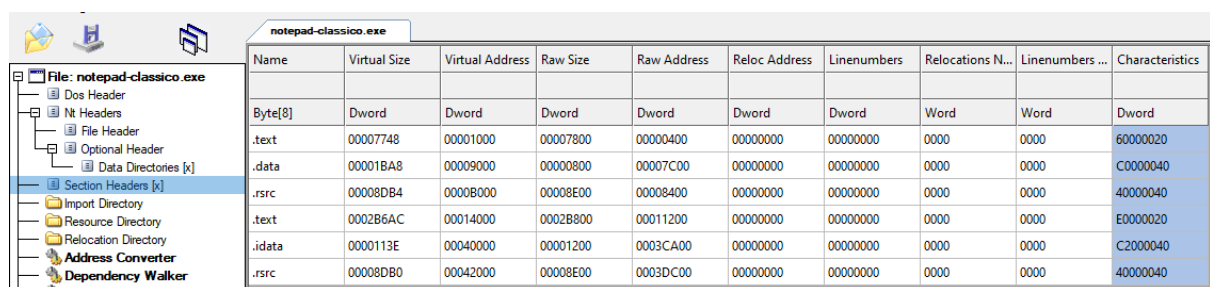
Ho iniziato l'analisi statica aprendo il presunto malware con CFF explorer.



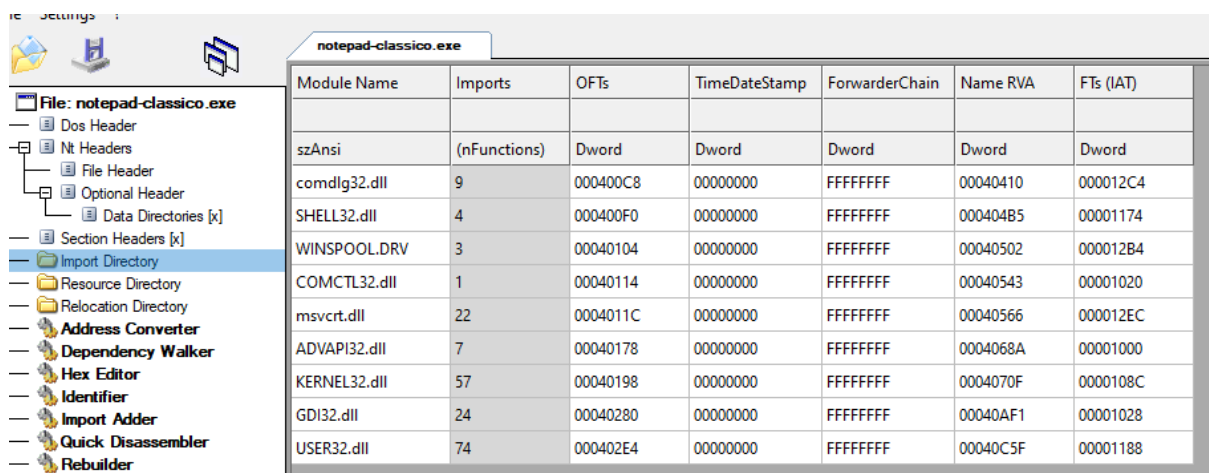
Una volta avviato, spostandosi nella sezione **Dos Header** è possibile visualizzare l'header **e_magic**, abbreviato MZ, che ci conferma che siamo dinanzi ad un eseguibile .exe:



Analizzando la **Section Header** possiamo invece notare quanto segue:



- Due **.text** → indica codice extra iniettato o struttura non standard (possibile packing parziale o sezione aggiunta manualmente).
- Due **.rsrc** → insolito: probabile uso come “contenitore nascosto” per altre risorse/payload.
- Le sezioni hanno permessi coerenti (eseguibile per **.text**, lettura/scrittura per **.data**), ma la duplicazione è un campanello d'allarme.



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

KERNEL32.dll

Contiene le API fondamentali di Windows: gestione processi/thread, file system, memoria. In un malware è usata per aprire/scrivere file, creare processi, allocare memoria.

ADVAPI32.dll

Fornisce funzioni per l'accesso al Registro di sistema, gestione dei servizi e sicurezza. Nei malware serve per ottenere persistenza (chiavi Run), modificare ACL, gestire privilegi.

USER32.dll

API per interfaccia grafica e input utente (finestre, pulsanti, tastiera, mouse). In ambito malevolo può essere usata per **keylogging**, manipolazione di finestre o interazioni simulate.

GDI32.dll

Gestione grafica (disegno testi, immagini, interfacce). Normalmente legittima, ma in malware può essere usata per “camuffarsi” da applicazione normale o manipolare schermate.

SHELL32.dll	Funzioni legate all'interfaccia shell di Windows (esecuzione programmi, apertura URL, accesso a file/cartelle speciali). Malware la usa per aprire file, lanciare comandi o eseguire script.
COMDLG32.dll	Gestione delle finestre di dialogo standard (Apri/Salva file). Può indicare che il malware mostra interfacce ingannevoli per far credere all'utente che stia usando un programma legittimo.
COMCTL32.dll	Fornisce i "controlli comuni" (liste, bottoni, toolbar). Usata spesso in GUI; un malware può sfruttarla per sembrare un'applicazione Windows reale.
WINSPOOL.DRV	API per stampa. È insolito in un malware, ma può essere sfruttata per interagire con spooler e stampanti oppure come "copertura" per un binario che imita Notepad.
MSVCRT.dll	Runtime C standard: funzioni di libreria (stringhe, memoria, I/O). Sempre presente nei programmi compilati in C; nei malware fornisce funzioni utili per manipolazione dati e rete (es. sprintf , malloc).

Considerazioni generali

- La presenza di librerie grafiche (USER32, GDI32, COMCTL32, COMDLG32) → cerca di camuffarsi come applicazione con GUI (in linea con il nome "notepad-classico").
- L'uso di ADVAPI32 → probabile interazione con Registro o servizi → indizio di possibili tecniche di persistenza.
- WINSPOOL.DRV è piuttosto sospetta: non è comune in un Notepad normale, potrebbe indicare abuso di componenti di sistema per comportamenti non documentati.
- MSVCRT + KERNEL32 sono base, ma la combinazione con librerie di shell e registro suggerisce funzionalità oltre a un semplice editor di testo.

ANALISI DINAMICA

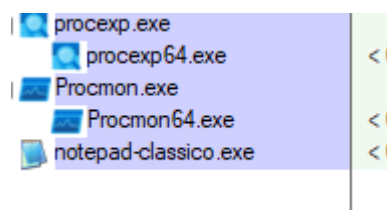
Per procedere ad un'analisi dinamica ho avviato due software:

Esegui → [procmon](#)

Esegui → [procexp](#)

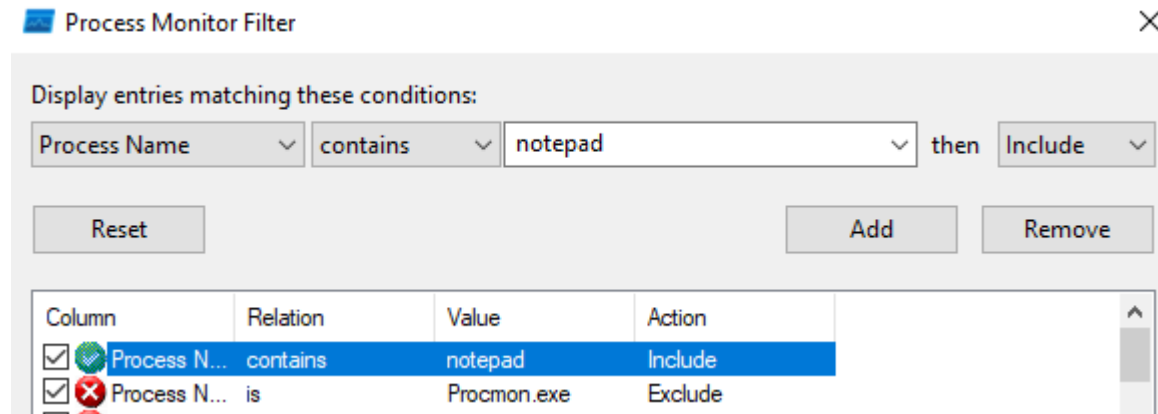
Ho poi eseguito il malware **notepad-classico.exe**

Osservando process explorer notiamo subito che il malware non avvia processi figli.



Non essendoci nulla di interessante passiamo dunque a process monitor.

Iniziamo filtrando i processi per nome:



Passiamo ora ad analizzare quanto eseguito dal malware filtrando tra le varie sezioni disponibili in procmon.

Processi e Threads

Time	Process Name	PID	Operation	Path	Result	Details
15:05:...	notepad-classic...	5912	Process Start		SUCCESS	Parent PID: 3264, Command line: "C:\Users\User\Desktop...
15:05:...	notepad-classic...	5912	Thread Create		SUCCESS	Thread ID: 4228
15:05:...	notepad-classic...	5912	Load Image	C:\Users\User\Desktop\notepad-classi...	SUCCESS	Image Base: 0x1000000, Image Size: 0x4adb0
15:05:...	notepad-classic...	5912	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7fba6fd0000, Image Size: 0x1f8000
15:05:...	notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77560000, Image Size: 0x1a4000
15:05:...	notepad-classic...	5912	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Query Value
15:05:...	notepad-classic...	5912	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Query Value
15:05:...	notepad-classic...	5912	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
15:05:...	notepad-classic...	5912	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
15:05:...	notepad-classic...	5912	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Query Value

Tra i punti più interessanti, emerge quanto segue:

- Il malware ci conferma venire eseguito come processo singolo (**notepad-classico.exe**, PID 5912).
- Non crea processi figli (niente **cmd.exe** o **powershell.exe**), genera però numerosi thread interni (**Thread Create** e **Thread Exit** in Procmon).

Questo indica che tutta la logica malevola gira dentro lo stesso processo, rendendo l'eseguibile più stealth rispetto a spawnare processi visibili.

Registro di Sistema

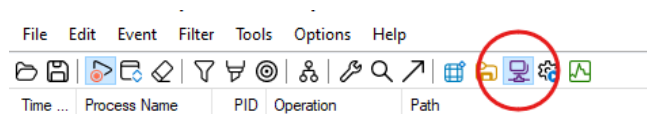
notepad-classic...	5912	Process Start		SUCCESS
notepad-classic...	5912	Thread Create		SUCCESS
notepad-classic...	5912	Load Image	C:\Users\User\Desktop\notepad-classico.exe	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\System32\wow64.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\comdlg32.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS
notepad-classic...	5912	Thread Create		SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\combase.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\urlbase.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\pccrt4.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\SHCore.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\win32u.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\gdi32full.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\msvc_p_win.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS
notepad-classic...	5912	Thread Create		SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\bcrypt.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\WinSxS\x86_microsoft.windows.com...	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\winspool.drv	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS
notepad-classic...	5912	Thread Create		SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\crypt32.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\wininet.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\winhttp.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\msctf.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\oleaut32.dll	SUCCESS
notepad-classic...	5912	Load Image	C:\Windows\SysWOW64\mswsock.dll	SUCCESS

All'interno della sezione relativa al registro di sistema notiamo diverse operazioni interessanti quanto sospette:

- Chiavi Session Manager
(HKLM\System\CurrentControlSet\Control\Session Manager): controlli su DEP, heap, exception handling → il malware valuta le protezioni anti-exploit.
- Resource Policies / SideBySide: verifica configurazioni di caricamento DLL → legato a possibili side-loading.
- FileSystem: lettura di opzioni come LongPathsEnabled, NtfsDisableLastAccessUpdate → possibili tecniche per compatibilità o evasione log.
- Policies\Microsoft\Windows\Safer\CodeIdentifiers: verifica se esistono Software Restriction Policies/AppLocker.
- HKCU\Software\Microsoft\CTF: scritture e query → servizi input/IME → indizio di possibili capacità di keylogging.
- Microsoft\Ole: query a chiavi COM/OLE → probabile abuso di automation COM.

In sintesi, il malware analizza l'ambiente di sicurezza e le configurazioni, adattandosi per bypassare restrizioni.

Network



La sezione network non presenta alcuna attività tuttavia, dall'analisi di DLL caricate, si osserva:

- ws2_32.dll → stack TCP/IP

- **wininet.dll, winhttp.dll** → funzioni per HTTP/HTTPS

Questo conferma che il malware ha capacità di **comunicazione in rete**, anche se nella sessione monitorata non sono comparsi tentativi di connessione diretta (probabile che richieda condizioni specifiche o trigger utente).

File System

15:05:...	notepad-classic...	5912	CreateFile	C:\Windows
15:05:...	notepad-classic...	5912	QueryOpen	C:\Windows\System32\wow64log.dll
15:05:...	notepad-classic...	5912	CreateFile	C:\Windows
15:05:...	notepad-classic...	5912	QueryNameInfo...	C:\Windows
15:05:...	notepad-classic...	5912	CloseFile	C:\Windows
15:05:...	notepad-classic...	5912	CreateFile	C:\Users\User\Desktop
15:05:...	notepad-classic...	5912	ReadFile	C:\Users\User\Desktop\notepad-classico.exe
15:05:...	notepad-classic...	5912	CreateFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0..
15:05:...	notepad-classic...	5912	QueryOpen	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0..
15:05:...	notepad-classic...	5912	CreateFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0..
15:05:...	notepad-classic...	5912	CreateFileMapp...	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0..
15:05:...	notepad-classic...	5912	CreateFileMapp...	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0..
15:05:...	notepad-classic...	5912	CloseFile	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0..
15:05:...	notepad-classic...	5912	QueryOpen	C:\Users\User\Desktop\WINSPOOL.DRV
15:05:...	notepad-classic...	5912	QueryOpen	C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0..
15:05:...	notepad-classic...	5912	QueryOpen	C:\Windows\SysWOW64\winspool.drv

- Accessi in lettura a numerose DLL di sistema (**kernel32.dll, user32.dll, gdi32.dll, comctl32.dll**, ecc.) → coerente con GUI.
- Attività sospette:
 - Apertura e lettura del file utente **NTUSER.DAT**, che contiene il registro personale → anomalo per un editor di testo.
 - Numerosi accessi e FileMapping su **winspool.drv** (spooler di stampa) → potenziale tecnica di DLL side-loading o injection.
 - Accessi a file in **WinSxS** e **SystemResources**.

Sintesi del Comportamento

- **Camuffamento:** si presenta con GUI simile a Notepad, caricando librerie grafiche (USER32, GDI32, COMCTL32).
- **Stealth:** non crea processi figli → tutto resta confinato nel proprio processo con thread multipli.
- **Persistenza/Evasione:** interagisce con registro (chiavi Policies, CTF, Session Manager) per modificare configurazioni e valutare protezioni attive.
- **Spionaggio:** accesso a **NTUSER.DAT** + uso di **imm32.dll** e chiavi CTF → possibili funzioni di keylogging o raccolta dati utente.
- **Rete:** presenza di librerie di comunicazione → può collegarsi a server remoti (C2) per inviare o ricevere dati.
- **Tecniche avanzate:** abusi di **winspool.drv** con file mapping → indizio di injection o DLL hijacking.

Conclusione

Il campione **notepad-classico.exe** è probabilmente un trojan camuffato da applicazione legittima.

Si finge un Notepad ma svolge attività sospette: controlla le protezioni di sistema, manipola il registro, accede a file utente critici, e carica librerie di rete. Non lascia tracce evidenti nel process tree ma usa thread interni per eseguire codice malevolo.

Il comportamento osservato è compatibile con malware che mira a:

- stabilire persistenza,
- raccogliere informazioni sull'utente (potenzialmente anche input da tastiera),
- e comunicare con server remoti tramite HTTP/HTTPS.