S9 – L2

Analisi Statica del Malware “notepad-classico.exe”

Introduzione:

Il presente esercizio ha come scopo l’**analisi del file *notepad-classico.exe* attraverso tecniche di analisi statica, senza eseguire il campione.**

L’attività si concentra sull’osservazione della struttura del file Portable Executable (PE), in particolare sulle **librerie importate (DLL)** e sulle **sezioni** che lo compongono, al fine di i**ndividuare eventuali elementi utili a comprenderne il possibile comportamento in ottica malware**. L’analisi viene svolta in un ambiente controllato e isolato, nel rispetto delle buone pratiche di sicurezza.

FASE 1) Scarico ed estraggo il campione

1. Scarico l’archivio dell’esercizio.
2. Lo estraggo con password **infected**.
3. Ottengo il file **notepad-classico.exe**.

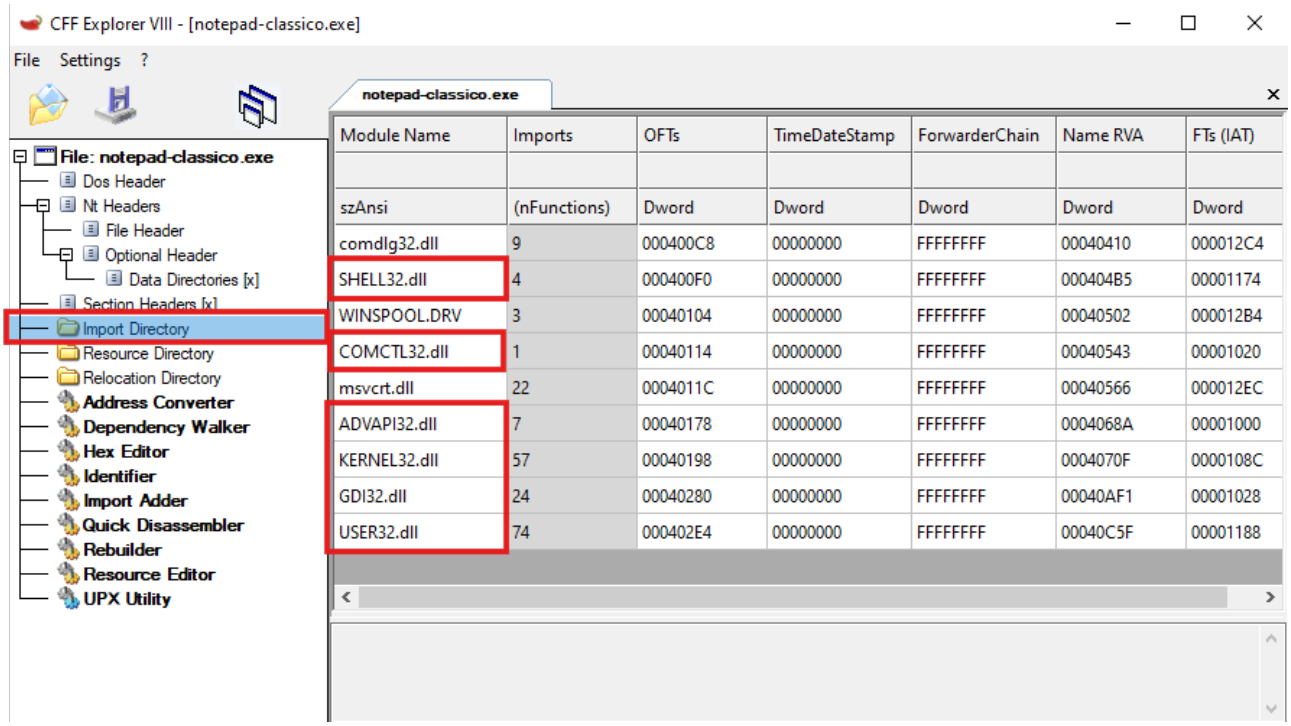
FASE 2) Apro il file con CFF Explorer

1. Avvio **CFF Explorer**.
2. Carico **notepad-classico.exe**.

FASE 3) Import Directory: elenco DLL importate + descrizione (richiesta ES)

1. In CFF Explorer vado su **Import Directory**.
2. Mi segno le **DLL importate**

- **GDI32.dll** → grafica base (testo/forme), tipico di app con interfaccia.
- **KERNEL32.dll** → funzioni base Windows (processi, memoria, file).
- **USER32.dll** → finestre, input tastiera/mouse, menu.
- **ADVAPI32.dll** → registro, sicurezza, servizi (possibili impostazioni/persistenza).
- **COMDLG32.dll** → finestre “Apri/Salva/Stampa/Trova”.
- **SHELL32.dll** → interazione con shell Windows (file/icone/associazioni).



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

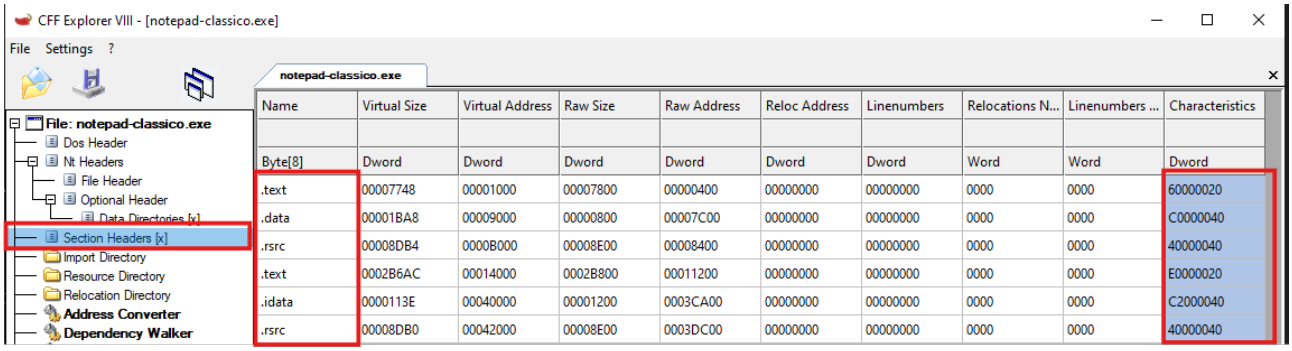
Output: pagina **Import Directory** con la lista DLL.

FASE 4) Sections: elenco sezioni + descrizione (richiesta ES)

1. In CFF Explorer controllo le **Sections** (sezione/headers).
2. Mi segno le sezioni interessate

- **.text** → codice eseguibile
- **.data** → dati globali/statici
- **.idata** → dati import (IAT / collegamento a DLL)
- **.rsrc** → risorse (icone, menu, stringhe UI)

3. **Controllo anomalie**: si nota **duplicazione di .text** (e anche .rsrc), indicatore forte di modifica/iniezione codice.



Output: tabella **Sections** dove si vedono i nomi (e l'eventuale duplicazione).

---

5) Conclusione:

"L'analisi statica di ***notepad-classico.exe*** **mostra che l'eseguibile è stato modificato: oltre alle importazioni coerenti con un'app Windows**, **presenta anomalie strutturali** (es. sezioni duplicate come *.text* e *.rsrc*). Questi elementi indicano la **presenza di codice aggiunto e sono compatibili con un comportamento trojan** (programma legittimo + payload nascosto)."