

Analisi del Malware

notepad-classico.exe: con CFF Explorer

Profilo studente

data:03/02/2026

studente: Gabriel Giustinelli 15/06/2004

Epicode classe: CS0525

Cyber Security Specialist

progetto

Il progetto consiste nell'analisi tecnica dell'eseguibile `notepad-classico.exe` per verificarne l'integrità e identificare potenziali comportamenti malevoli. Nonostante il file si presenti con l'icona e i metadati del legittimo Blocco Note di Windows, l'indagine mira a scovare anomalie strutturali.

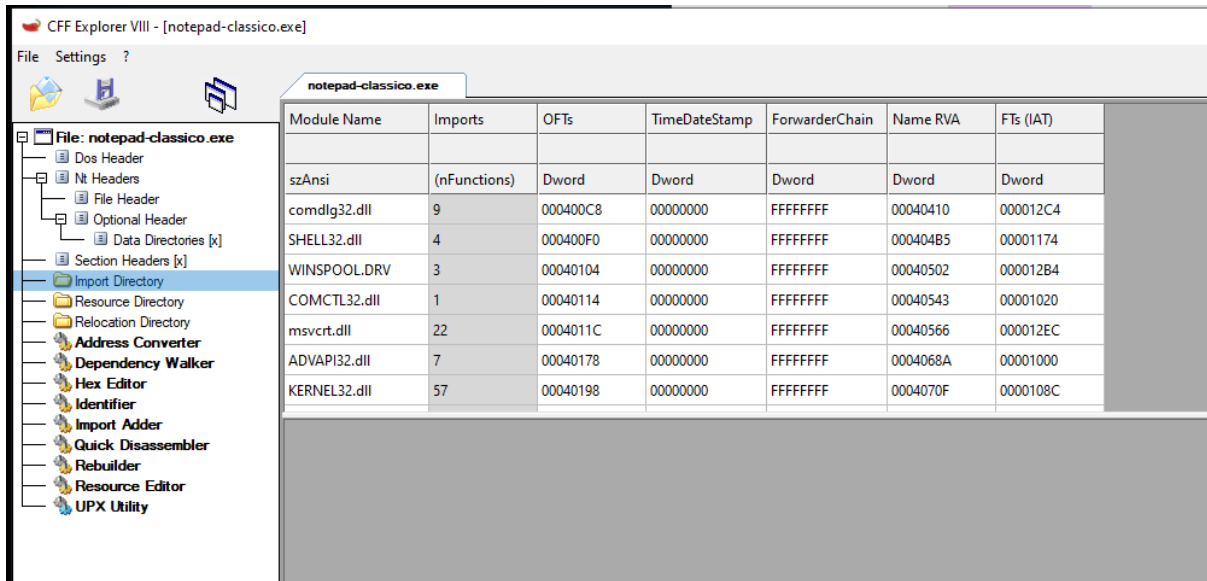
L'analisi è stata condotta tramite il software **CFF Explorer**, esaminando le librerie dinamiche (DLL) importate e la configurazione delle sezioni interne del file (sezioni PE) per determinare se il software originale sia stato alterato con l'inserimento di codice dannoso.

1. Librerie Importate (Imports)

L'analisi della *Import Directory* ha rivelato l'utilizzo di diverse librerie dinamiche (DLL). Di seguito sono elencate le principali con la relativa descrizione tecnica:

- **KERNEL32.dll**: Fornisce le API core di Windows per la gestione della memoria, dei processi e dei thread, oltre all'accesso fondamentale al file system.
- **ADVAPI32.dll**: Libreria critica che permette l'interazione con il Registro di sistema, la gestione degli account utente e il controllo dei servizi di sistema.
- **USER32.dll**: Gestisce tutti gli elementi dell'interfaccia utente (finestre, menu) e riceve gli input da tastiera e mouse.
- **GDI32.dll**: Utilizzata per le operazioni grafiche, come il rendering di testo e immagini sullo schermo.
- **SHELL32.dll**: Permette al programma di eseguire comandi tramite la shell di Windows e interagire con le cartelle di sistema.
- **MSVCRT.dll**: Libreria standard del runtime C, utilizzata per funzioni comuni di programmazione come l'allocazione di memoria e la manipolazione di stringhe.

- **COMDLG32.dll**: Contiene le finestre di dialogo standard (Apri/Salva), necessarie per simulare l'interfaccia del Blocco Note originale.



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

2. Analisi delle Sezioni

L'analisi dell'intestazione PE (*Section Headers*) evidenzia una struttura anomala composta dalle seguenti sezioni:

- **.text (doppia)**: La sezione principale del codice eseguibile. La presenza di una seconda sezione **.text** suggerisce l'inserimento di codice non originale o di un modulo malevolo aggiuntivo.
- **.data**: Area dedicata alle variabili globali e ai dati statici utilizzati durante l'esecuzione.
- **.rsrc (doppia)**: Contiene le risorse del file (icone, menu). La duplicazione di questa sezione è spesso usata per occultare file secondari o configurazioni del malware.
- **.idata**: Ospita la *Import Address Table* (IAT), ovvero i riferimenti alle funzioni esterne elencate nella sezione precedente.
- **.reloc**: Contiene i dati necessari per il rilocamento del codice in memoria (Base Relocation), essenziali per il corretto funzionamento su diverse configurazioni di sistema.

CFF Explorer VIII - [notepad-classico.exe]

File Settings ?

notepad-classico.exe

File: notepad-classico.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
- Section Headers [x]
 - Import Directory
 - Resource Directory
 - Relocation Directory
 - Address Converter
 - Dependency Walker
 - Hex Editor
 - Identifier
 - Import Adder
 - Quick Disassembler
 - Rebuilder
 - Resource Editor
 - UPX Utility

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

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ yy . .
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00 @
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	E0	00	00	00 a
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	0 40 LI!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is .program.canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t .be.run.in.DOS.
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode \$

Nota Tecnica Finale

"L'eseguibile analizzato è un esempio di **malware 'backdoored'** o infetto, progettato per camuffarsi da applicazione legittima (**Notepad.exe**) tramite il mascheramento dei metadati e delle icone. La struttura interna presenta evidenti anomalie, tra cui la duplicazione delle sezioni **.text** e **.rsrc**, tattica comunemente utilizzata per iniettare codice malevolo o payload compressi all'interno di un file originale. L'importazione di funzioni tramite **ADVAPI32.dll** suggerisce che il programma esegua operazioni non autorizzate sul Registro di sistema o sulla sicurezza degli account, rendendolo potenzialmente pericoloso per la persistenza nel sistema e per l'esfiltrazione di informazioni."