

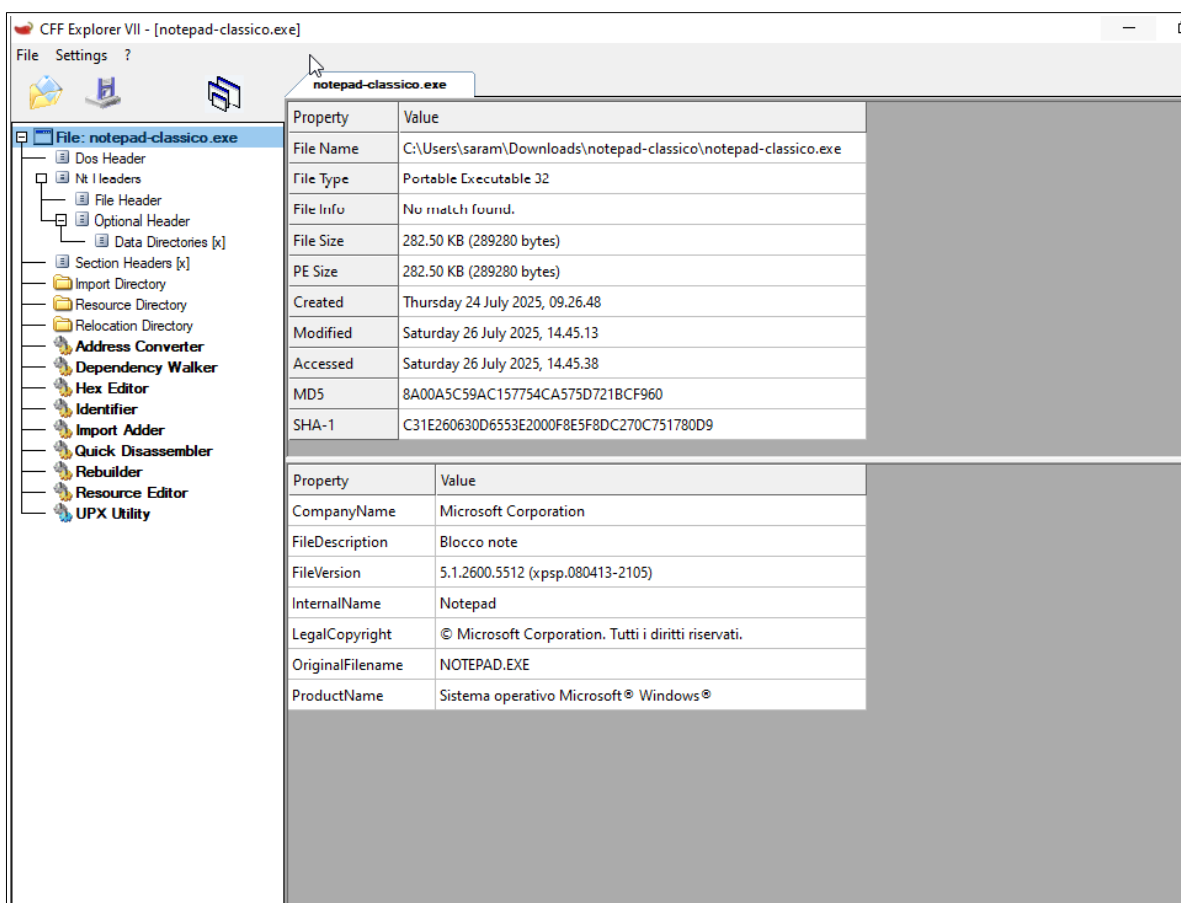
# Report W21D4 Analisi statica basica

In questo esercizio dovremo analizzare un file malevolo in maniera statica, senza quindi eseguire il file ma ricavando le informazioni solamente dal codice.

## Prerequisiti:

- VM di Windows 10,
- Strumenti per l'analisi statica dei file come CFF explorer,
- Isolamento della macchina dopo aver scaricato il file malevolo.

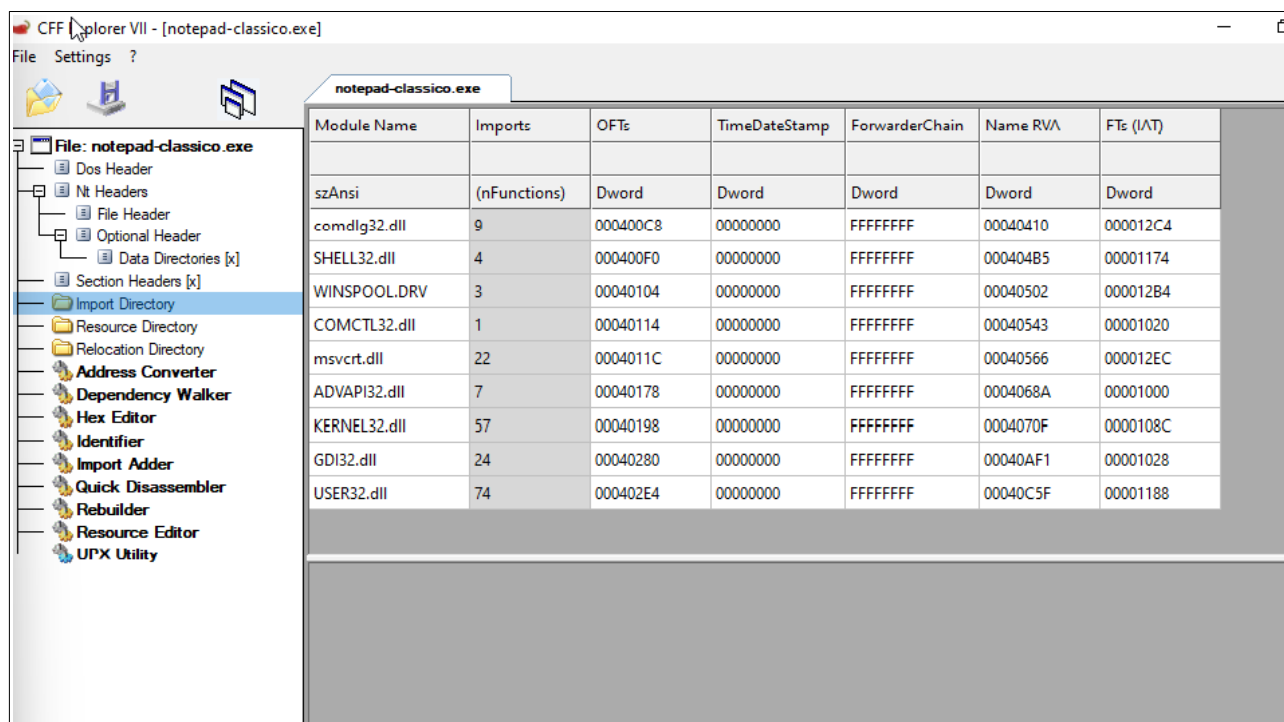
**Step 1** una volta scaricato il file ed averlo decompresso in un ambiente sicuro possiamo procedere all'analisi del file tramite CFF explorer.



## Step 2 Come da consegna andiamo ad analizzare le librerie importate dal file:

- **comdlg32.dll**: è una libreria di collegamento dinamico (Dynamic Link Library) di Windows che fornisce funzioni per le finestre di dialogo comuni, come quelle di apertura e salvataggio dei file. È utilizzata da molte applicazioni per interagire con l'utente, offrendo un'interfaccia standardizzata per queste operazioni.
- **SHELL32.dll**: è una libreria di collegamento dinamico (DLL) fondamentale per il sistema operativo Windows, responsabile della Shell, l'interfaccia utente grafica, che include elementi come il desktop, il menu Start, l'autoplay e la barra delle applicazioni. Questa libreria è essenziale e non dovrebbe essere rimossa.
- **WINSPOOL.DRV**: è un file DLL (Dynamic Link Library) del sistema operativo Windows che fa parte del driver dello spooler di stampa. È essenziale per la gestione della stampa.
- **COMCTL32.dll**: è un file di sistema principale di Windows che fornisce una libreria di elementi comuni dell'interfaccia utente per le applicazioni.
- **ADVAPI32.dll**: libreria di sistema di Windows usata dalle applicazioni per accedere a funzionalità avanzate del sistema operativo (sicurezza, registro di sistema, servizio di Windows, account utente, crittografia).
- **KERNEL32.dll**: libreria fondamentale di Windows per la gestione della memoria di sistema, I/O, gestione processi e thread.
- **GDI32.dll**: libreria per disegno grafico 2D, usata da applicazioni che devono mostrare contenuti visivi.
- **USER32.dll**: libreria core di qualsiasi applicazione Windows con interfaccia grafica che gestisce tutto ciò che riguarda l'interfaccia utente.

Tutte le librerie analizzate non risultano anomale per un'applicazione come Notepad.



CFF Explorer VII - [notepad-classico.exe]

File Settings ?

notepad-classico.exe

Module Name	Imports	OFf	TimeDateStamp	ForwarderChain	Name RVA	File (L/T)
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

**Step 3** Andiamo ad analizzare le sezioni che compongono il file. Possiamo notare che le sezioni .text e .rsrc sono doppie.

- **.text**: contiene il codice eseguibile compilato del programma, cioè le istruzioni che verranno poi eseguite dalla CPU.
- **.data**: contiene i dati inizializzati in fase di compilazione.
- **.rsrc**: contiene le risorse incorporate nel file eseguibile ovvero dati non eseguibili che l'applicazione può usare durante l'esecuzione.
- **.idata**: contiene le informazioni sulle dll esterne e le funzioni che l'eseguibile vuole usare.

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

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 . . . . .
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	. . . . .
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	. . . . .
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program cannot
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	0A	24	00	00	00	00	00	00	00	00	mode. . . . .
00000080	EC	85	5B	A1	A8	E4	35	F2	A8	E4	35	F2	A8	E4	35	F2	i i i ' a 5 0 ' a 5 0 ' a 5 0
00000090	6B	EB	3A	F2	A9	E4	35	F2	6B	EB	55	F2	A9	E4	35	F2	ke o a 5 0 ke U o a 5 0
000000A0	6B	EB	68	F2	EB	E4	35	F2	A8	E4	34	F2	63	E4	35	F2	ke h o a 5 0 a 4 c c a 5 0
000000B0	6B	EB	6B	F2	A9	E4	35	F2	6B	EB	6A	F2	BF	E4	35	F2	ke k o a 5 0 ke j o a 5 0

Andando ad approfondire il contenuto delle sezioni doppie, in particolar modo di quelle .text, la prima contiene codice legittimo legato all'applicazione Notepad, la seconda invece contiene codice malevolo.

Ci possiamo rendere conto immediatamente del fatto che siano due sezioni diverse, in quanto l'ascii è completamente diverso, così come i valori delle sezioni come virtual size e virtual address, ecc.

## Prima sezione .text:

- Virtual size: 00007748
- Virtual address: 00001000
- Raw size: 00007800
- Raw address: 00000400
- Characteristics: 60000020

notepad-classico.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
000001D8	000001E0	000001E4	000001E8	000001EC	000001F0	000001F4	000001F8	000001FA	000001FC
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

This section contains:  
Import Address Table Directory: 00001000

Find String: http Find Reset  
☐ Match Case ☐ Unichrome  
Hex Find  
Status: String not found

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	98	06	04	00	AC	06	04	00	BA	06	04	00	CA	06	04	00	00000000
00000010	DA	06	04	00	EE	06	04	00	FE	06	04	00	00	00	00	00	00000010
00000020	50	05	04	00	00	00	00	00	FC	0A	04	00	06	0B	04	00	00000020
00000030	12	0B	04	00	1C	0B	04	00	28	0B	04	00	34	0B	04	00	00000030
00000040	4C	0B	04	00	58	0B	04	00	68	0B	04	00	78	0B	04	00	00000040
00000050	84	0B	04	00	90	0B	04	00	9E	0B	04	00	B0	0B	04	00	00000050
00000060	BE	0B	04	00	CE	0B	04	00	E4	0B	04	00	F4	0B	04	00	00000060
00000070	06	0C	04	00	12	0C	04	00	1C	0C	04	00	2E	0C	04	00	00000070
00000080	42	0C	04	00	50	0C	04	00	00	00	00	00	1C	07	04	00	00000080
00000090	32	07	04	00	42	07	04	00	5C	07	04	00	6C	07	04	00	00000090

## Seconda sezione .text:

- Virtual size: 0002B6AC
- Virtual address: 00014000
- Raw size: 0002B800
- Raw address: 00011200
- Characteristics: E0000020

notepad-classico.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
00000250	00000258	0000025C	00000260	00000264	00000268	0000026C	00000270	00000272	00000274
Byte[8]		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

This section contains:  
Code Entry Point: 00014000  
Relocation Directory: 0003F698

Find String: http Find Reset  
☐ Match Case ☐ Unicode  
Hex Find  
Status: String found

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00025110	65	74	4F	70	74	69	6F	6E	57	00	00	58	00	08	74	74	etOptionW...X Htt
00025120	70	4F	70	65	6E	52	65	71	75	65	73	74	57	00	00	5E	pOpenRequestW...^
00025130	00	48	74	74	70	53	65	6E	64	52	65	71	75	65	73	74	.HttpSendRequest
00025140	57	00	00	5A	00	48	74	74	70	51	75	65	72	79	49	6E	W...Z.HttpQueryin
00025150	66	6F	57	00	00	57	49	4E	49	4E	45	54	2E	64	6C	6C	foW...WININET.dll
00025160	00	09	00	57	69	6E	48	74	74	70	43	72	61	63	6B	55	...WinHttpCrackU
00025170	72	6C	00	0F	00	57	69	6E	48	74	74	70	4F	70	65	6E	rl...WinHttpOpen
00025180	00	07	00	57	69	6E	48	74	74	70	43	6C	6F	73	65	48	...WinHttpCloseH
00025190	61	6E	64	6C	65	00	00	08	00	57	69	6E	48	74	74	70	andle...WinHttp
000251A0	43	6F	6E	6E	65	63	74	00	00	15	00	57	69	6E	48	74	Connect...WinHt

Pos: 0002511D

Analizzando l'Ascii tramite lo strumento di ricerca di CFF explorer possiamo notare come siano presenti parole come http, create thread, internet connect, ecc. tutti indicatori che l'applicazione è sospetta.

Troveremo anche la libreria WININET.dll e ws2\_32.dll, entrambe librerie sospette in quanto servono per effettuare conessioni ad internet, cosa che un'applicazione come Notepad non dovrebbe normalmente fare.

Find String: ws2\_32 Find Match Case Unicode Reset

Hex Find

Status: String found

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00025030	6E	66	6F	00	00	51	53	32	5F	33	32	2E	64	6C	6C	00	nfo..WS2_32.dll
00025040	00	83	00	43	72	79	70	74	44	65	63	6F	64	65	4F	62	..CryptDecodeOb
00025050	6A	65	63	74	45	78	00	A4	00	43	72	79	70	74	49	6D	jectEx..CryptIm
00025060	70	6F	72	74	50	75	62	6C	69	63	4B	65	79	49	6E	66	portPublicKeyInf
00025070	6F	00	00	46	00	43	65	72	74	47	65	74	43	65	72	74	o..F.CertGetCert
00025080	69	66	69	63	61	74	65	43	6F	6E	74	65	78	74	50	72	ificateContextPr
00025090	6F	70	65	72	74	79	00	43	52	59	50	54	33	32	2E	64	operty.CRYPT32.d
000250A0	6C	6C	00	74	00	49	6E	74	65	72	6E	65	74	43	72	61	ll..t..InternetCra
000250B0	63	6B	55	72	6C	57	00	9A	00	49	6E	74	65	72	6E	65	ckUriW..I..Interne
000250C0	74	4F	70	65	6E	57	00	6B	00	49	6E	74	65	72	6E	65	tOpenW..k..Interne

Sel Start: 00025034 Size: 0000000C

Find String: Wininet Find Match Case Unicode Reset

Hex Find

Status: String found

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00025150	66	6F	57	00	00	57	49	4E	49	4E	45	54	2E	64	6C	6C	foW..WININET.dll
00025160	00	09	00	57	69	6E	48	74	74	70	43	72	61	63	6B	55	..WinHttpCrackU
00025170	72	6C	00	0F	00	57	69	6E	48	74	74	70	4F	70	65	6E	rl..WinHttpOpen
00025180	00	07	00	57	69	6E	48	74	74	70	43	6C	6F	73	65	48	..WinHttpCloseH
00025190	61	6E	64	6C	65	00	00	08	00	57	69	6E	48	74	74	70	andle..WinHttp
000251A0	43	6F	6E	6E	65	63	74	00	00	15	00	57	69	6E	48	74	Connect..WinHt
000251B0	74	70	52	65	61	64	44	61	74	61	00	14	00	57	69	6E	tpReadData..Win
000251C0	48	74	74	70	51	75	65	72	79	4F	70	74	69	6F	6E	00	HttpQueryOption.
000251D0	00	1A	00	57	69	6E	48	74	74	70	53	65	74	4F	70	74	..WinHttpSetOpt
000251E0	69	6F	6E	00	00	10	00	57	69	6E	48	74	74	70	4F	70	ion..WinHttpOp

Sel Start: 0002515F Size: 0000000D

## Facoltativo

In conclusione il malware che abbiamo preso in esame è un trojan in quanto si presenta come un'applicazione legittima (Notepad) ma in realtà nasconde un payload malevolo che esegue connessioni verso l'esterno per fornire potenzialmente il controllo della macchina infetta ad attori malevoli.