

Report Pratica S9-L2 – Analisi notepad-classico.exe

1. Introduzione

L'obiettivo di questa attività di laboratorio è analizzare il campione malware **notepad-classico.exe** al fine di comprenderne la struttura interna, il comportamento runtime e le potenziali capacità malevole.

L'analisi è stata condotta combinando **analisi statica** e **analisi dinamica**, al fine di individuare anomalie strutturali del formato PE e osservare il comportamento del campione in esecuzione controllata.

Tutte le operazioni sono state svolte all'interno di un **ambiente virtualizzato isolato (FLARE VM)**, configurato per garantire sicurezza e ripetibilità del test. Lo scopo finale è determinare la natura del campione e fornirne una classificazione tecnica basata sulle evidenze raccolte.

2. Informazioni sul campione analizzato

Il campione oggetto dell'analisi è un **file eseguibile Windows** denominato **notepad-classico.exe**. Il file è stato analizzato in un **ambiente virtualizzato isolato**, con l'obiettivo di identificarne le caratteristiche tecniche principali e predisporre le informazioni di base necessarie alle successive fasi di analisi statica e dinamica.

Contesto e Parametri di Analisi

- **Nome file:** notepad-classico.exe
- **Formato:** Portable Executable (PE) Windows
- **Strumento principale utilizzato:** CFF Explorer VIII
- **Ambiente di analisi:** FLARE VM (Windows isolato)
- **Strumenti principali utilizzati:**
 - CFF Explorer VIII (analisi statica)
 - Process Monitor
 - Process Explorer
 - Wireshark
 - FakeNet-NG

3. Analisi Statica

L'analisi statica è stata eseguita senza avviare il campione in esecuzione, con l'obiettivo di esaminare la struttura interna del file, le librerie importate, le sezioni del formato PE e gli indicatori testuali di potenziali funzionalità malevole.

Lo strumento principale utilizzato per questa fase è stato **CFF Explorer VIII**.

3.1 Librerie Importate (Import Address Table)

L'analisi della **Import Directory** tramite CFF Explorer ha permesso di individuare le principali librerie di sistema caricate staticamente dall'eseguibile.

notepad-classico.exe						
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

Figura 1 – Import Directory di notepad-classico.exe (CFF Explorer)

Librerie individuate

Libreria	Categoria funzionale	Ruolo operativo	Rilevanza per l'analisi malware
KERNEL32.dll	Core OS	Gestione processi, memoria, thread e file	Necessaria per l'esecuzione base del payload e del wrapper
USER32.dll	GUI	Gestione finestre e input utente	Coerente con la simulazione di comportamento legittimo

GDI32.dll	Grafica	Rendering testo e interfaccia	Supporta il mascheramento dell'applicazione
ADVAPI32.dll	Sistema avanzato	Accesso al registro e sicurezza	Potenzialmente utilizzabile per configurazioni e persistenza
COMDLG32.dll	Dialoghi standard	Finestre "Apri", "Salva", "Stampa"	Coerente con funzionalità Notepad
SHELL32.dll	Shell OS	Interazione con file system e shell	Supporta integrazione con ambiente Windows
COMCTL32.dll	UI avanzata	Componenti grafici standard	Rafforza l'aspetto di applicazione legittima
MSVCRT.dll	Runtime C	Funzioni base di memoria e I/O	Necessaria per il funzionamento del codice nativo
WINSPOOL.DRV	Printing	Gestione stampa	Compatibile con le funzionalità native di Notepad

Osservazione tecnica

La distribuzione delle librerie importate mostra un profilo fortemente orientato all'interfaccia grafica e all'integrazione con il sistema operativo, comportamento coerente con un'applicazione legittima. Questa caratteristica suggerisce l'utilizzo di una tecnica di mascheramento, in cui il malware mantiene attive le funzionalità originali del programma ospite per ridurre il sospetto dell'utente e mascherare l'esecuzione del payload malevolo.

3.2 Analisi della Struttura PE (Section Headers)

L'analisi delle intestazioni delle sezioni PE è stata effettuata tramite CFF Explorer al fine di individuare anomalie strutturali e modifiche riconducibili a tecniche di iniezione di codice.

notepad-classico.exe									
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

Figura 2 – Section Headers di notepad-classico.exe (CFF Explorer)

Struttura delle sezioni

Sezione	Funzione principale	Valutazione di sicurezza
.text (1)	Codice eseguibile originale dell'applicazione	Compatibile con eseguibile legittimo
.text (2)	Codice eseguibile aggiuntivo	Indicatore di iniezione di payload
.data	Dati globali e statici	Normale
.idata	Import Address Table	Normale
.rsrc (1)	Risorse grafiche originali	Normale
.rsrc (2)	Risorse aggiuntive	Anomalia Strutturale

Interpretazione tecnica

La presenza di **sezioni duplicate** *.text* e *.rsrc* rappresenta una chiara **anomalia strutturale**. Nei file PE legittimi è normalmente presente una singola sezione *.text* e una singola sezione *.rsrc*.

La duplicazione della sezione *.text* indica l'**iniezione di codice eseguibile aggiuntivo** all'interno dell'eseguibile originale. In questo contesto, la **prima sezione .text** è riconducibile al **codice legittimo di Notepad**, mentre la **seconda suggerisce fortemente la presenza di codice aggiuntivo malevolo**.

Analogamente, la duplicazione della sezione *.rsrc* suggerisce l'**aggiunta di risorse supplementari** associate al processo di **wrapping del malware**.

Questo pattern strutturale è tipico delle tecniche di **trojanizzazione tramite wrapping dell'eseguibile originale**, comunemente utilizzate per **incorporare payload malevoli** mantenendo **intatta la funzionalità apparente** del programma ospite.

3.3 Analisi delle Stringhe (Indicatori Statici di Comunicazione di Rete)

L'analisi delle stringhe effettuata tramite **Hex Editor di CFF Explorer** ha evidenziato la presenza di riferimenti diretti a librerie e funzioni di rete incorporate nel binario.

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00036230	6E	66	6F	00	00	57	53	32	5F	33	32	2E	64	6C	6C	00	nfo. WS2_32.dll
00036240	00	83	00	43	72	79	70	74	44	65	63	6F	64	65	4F	62	. CryptDecodeOb
00036250	6A	65	63	74	45	78	00	A4	00	43	72	79	70	74	49	6D	jectEx. CryptIm
00036260	70	6F	72	74	50	75	62	6C	69	63	4B	65	79	49	6E	66	portPublicKeyInf
00036270	6F	00	00	46	00	43	65	72	74	47	65	74	43	65	72	74	o. F.CertGetCert
00036280	69	66	69	63	61	74	65	43	6F	6E	74	65	78	74	50	72	ificateContextPr
00036290	6F	70	65	72	74	79	00	43	52	59	50	54	33	32	2E	64	operty.CRYPT32.d
000362A0	6C	6C	00	74	00	49	6E	74	65	72	6E	65	74	43	72	61	ll.t.InternetCra
000362B0	63	6B	55	72	6C	57	00	9A	00	49	6E	74	65	72	6E	65	ckUrlW. Interne
000362C0	74	43	6C	6F	73	65	48	61	6E	64	6C	65	00	72	00	49	tOpenW.k. Interne
000362D0	74	43	6C	6F	73	65	48	61	6E	64	6C	65	00	72	00	49	tCloseHandle.r. I
000362E0	6E	74	65	72	6E	65	74	43	6F	6E	6E	65	63	74	57	00	nternetConnectW.
000362F0	00	9F	00	49	6E	74	65	72	6E	65	74	52	65	61	64	46	. InternetReadF
00036300	69	6C	65	00	AF	00	49	6E	74	65	72	6E	65	74	53		ile. InternetS
00036310	65	74	4F	70	74	69	6F	6E	57	00	00	58	00	48	74	74	etOptionW.X.Htt
00036320	70	4F	70	65	6E	52	65	71	75	65	73	74	57	00	00	5E	pOpenRequestW.^
00036330	00	48	74	74	70	53	65	6E	64	52	65	71	75	65	73	74	.HttpSendRequest
00036340	57	00	00	5A	00	48	74	74	70	51	75	65	72	79	49	6E	W.Z.HttpQueryIn
00036350	66	6F	57	00	00	57	49	4E	49	4E	45	54	2E	64	6C	6C	foW. WININET.dll
00036360	00	09	00	57	69	6E	48	74	74	70	43	72	61	63	6B	55	...WinHttpCrackU
00036370	72	6C	00	0F	00	57	69	6E	48	74	74	70	4F	70	65	6E	rl. WinHttpOpen
00036380	00	07	00	57	69	6E	48	74	74	70	43	6C	6F	73	65	48	. WinHttpCloseH
00036390	61	6E	64	6C	65	00	00	08	00	57	69	6E	48	74	74	70	andle. WinHttp
000363A0	43	6F	6E	6E	65	63	74	00	00	15	00	57	69	6E	48	74	Connect. WinHt
000363B0	74	70	52	65	61	64	44	61	74	61	00	14	00	57	69	6E	tpReadData. Win
000363C0	48	74	74	70	51	75	65	72	79	4F	70	74	69	6F	6E	00	.HttpQueryOption
000363D0	00	1A	00	57	69	6E	48	74	74	70	53	65	74	4F	70	74	. WinHttpSetOpt
000363E0	69	6F	6E	00	00	10	00	57	69	6E	48	74	74	70	4F	70	ion. WinHttpOp
000363F0	65	6E	52	65	71	75	65	73	74	00	00	17	00	57	69	6E	enRequest. Win
00036400	48	74	74	70	53	65	6E	64	52	65	71	75	65	73	74	00	HttpSendRequest
00036410	00	16	00	57	69	6E	48	74	74	70	52	65	63	65	69	76	. WinHttpReceiv
00036420	65	52	65	73	70	6F	6E	73	65	00	00	13	00	57	69	6E	eResponse. Win
00036430	48	74	74	70	51	75	65	72	79	48	65	61	64	65	72	73	HttpQueryHeaders
00036440	00	0E	00	57	69	6E	48	74	74	70	47	65	74	50	72	6F	. WinHttpGetPro
00036450	78	79	46	6F	72	55	72	6C	00	0D	00	57	69	6E	48	74	xyForUrl. WinHt
00036460	74	70	47	65	74	49	45	50	72	6F	78	79	43	6F	6E	66	tpGetIEProxyConf
00036470	69	67	46	6F	72	43	75	72	72	65	6E	74	55	73	65	72	igForCurrentUser
00036480	00	57	49	4E	48	54	54	50	2E	64	6C	6C	00	EA	04	56	. WINHTTP.dll. @V
00036490	69	72	74	75	61	6C	41	6C	6C	6F	63	45	78	00	00	80	rtualAllocEx. I
000364A0	03	4F	70	65	6E	50	72	6F	63	65	73	73	00	C0	01	47	OpenProcess. @G
000364B0	65	74	43	75	72	72	65	6E	74	50	72	6F	63	65	73	73	etCurrentProcess
000364C0	00	02	02	47	65	74	4C	61	73	74	45	72	72	6F	72	00	. GetLastError.
000364D0	00	2E	05	57	72	69	74	65	50	72	6F	63	65	73	73	4D	. WriteProcessM
000364E0	65	6D	6F	72	79	00	00	52	00	43	6C	6F	73	65	48	61	emory. R.CloseHa

Figura 3 – Stringhe di rete individuate nel binario (CFF Explorer Hex Editor)

Interpretazione tecnica

La presenza delle stringhe **WININET.dll** e **HttpSendRequest** indica che il campione è progettato per utilizzare le API HTTP native di Windows per comunicazioni client-server.

Parallelamente, il riferimento a **WS2_32.dll** conferma il supporto alle comunicazioni TCP/IP a basso livello tramite socket.

Il fatto che tali API non risultino importate direttamente nella Import Address Table suggerisce l'utilizzo di **caricamento dinamico delle funzioni di rete**, tecnica comunemente adottata per ridurre la visibilità statica del comportamento malevolo e ostacolare l'analisi automatizzata.

3.4 Sintesi dell'Analisi Statica

L'analisi statica del campione **notepad-classico.exe** ha evidenziato numerosi indicatori riconducibili a un eseguibile compromesso.

In particolare sono state osservate:

- anomalie strutturali del formato PE
- duplicazione delle sezioni eseguibili
- presenza di indicatori statici di comunicazione di rete
- utilizzo di librerie GUI per mascheramento funzionale

Sulla base delle evidenze raccolte, il campione può essere **preliminarmente classificato come Trojan mascherato da applicazione legittima**, progettato per eseguire un payload aggiuntivo in background.

4. Analisi dinamica (Runtime Behavior Analysis)

L'analisi dinamica è stata condotta eseguendo il campione notepad-classico.exe all'interno di un ambiente controllato e isolato, con l'obiettivo di osservare il comportamento del malware a runtime e verificare le ipotesi formulate durante l'analisi statica.

4.1 Esecuzione del campione e comportamento osservabile

All'avvio del file notepad-classico.exe, l'applicazione mostra un comportamento pienamente coerente con il **Notepad legittimo**, presentando regolarmente l'interfaccia grafica dell'editor di testo e risultando utilizzabile dall'utente senza anomalie evidenti.

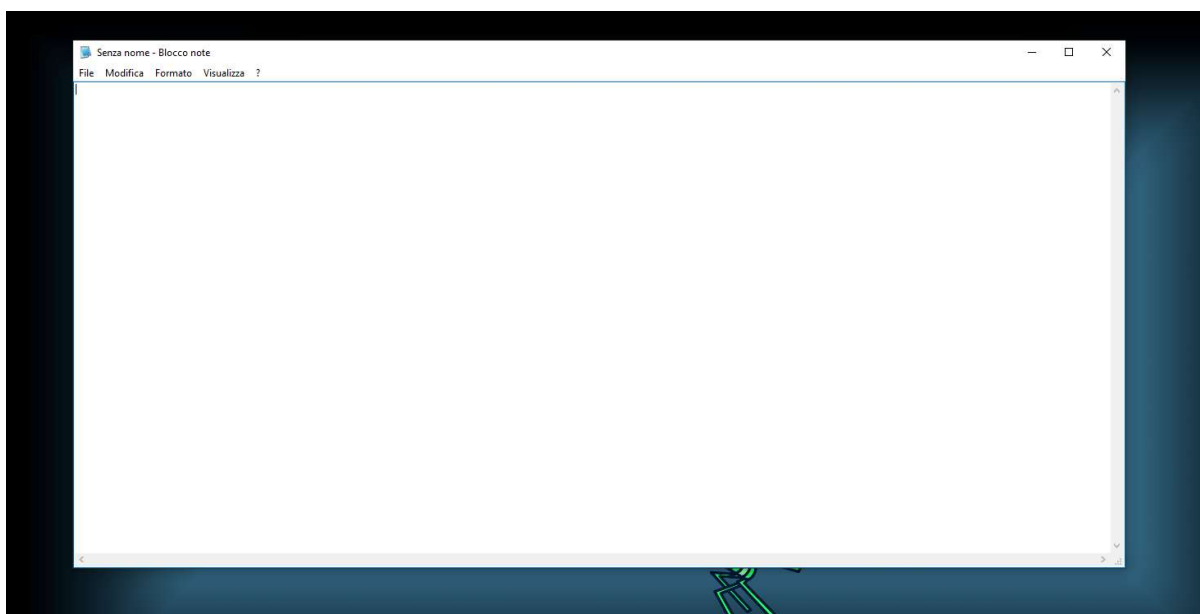


Figura 4 – Avvio dell'applicazione notepad-classico.exe (interfaccia Notepad)

Osservazione tecnica

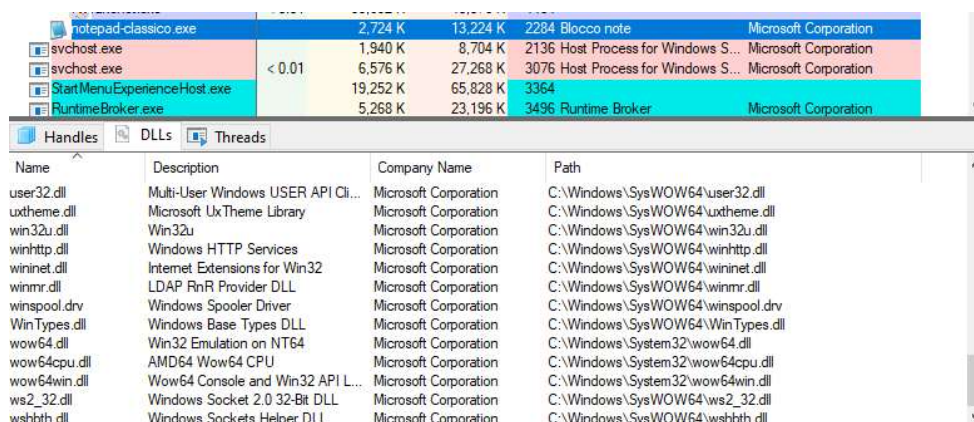
Il mantenimento del comportamento funzionale dell'applicazione ospite conferma l'adozione di una tecnica di **mascheramento**, in cui il malware preserva l'esperienza utente per ridurre il sospetto e nascondere l'esecuzione del payload in background.

4.2 Analisi dei processi e delle librerie caricate

Durante l'esecuzione del campione, l'analisi tramite Process Explorer ha evidenziato che il processo notepad-classico.exe carica dinamicamente librerie di rete precedentemente individuate durante l'analisi statica.

In particolare sono state osservate le seguenti DLL:

- WS2_32.dll
- WININET.dll



Name	Description	Company Name	Path
user32.dll	Multi-User Windows USER API Cli...	Microsoft Corporation	C:\Windows\SysWOW64\user32.dll
uxtheme.dll	Microsoft UxTheme Library	Microsoft Corporation	C:\Windows\SysWOW64\uxtheme.dll
win32u.dll	Win32u	Microsoft Corporation	C:\Windows\SysWOW64\win32u.dll
winhttp.dll	Windows HTTP Services	Microsoft Corporation	C:\Windows\SysWOW64\winhttp.dll
wininet.dll	Internet Extensions for Win32	Microsoft Corporation	C:\Windows\SysWOW64\wininet.dll
winmr.dll	LDAP RnR Provider DLL	Microsoft Corporation	C:\Windows\SysWOW64\winmr.dll
winspool.drv	Windows Spooler Driver	Microsoft Corporation	C:\Windows\SysWOW64\winspool.drv
WinTypes.dll	Windows Base Types DLL	Microsoft Corporation	C:\Windows\SysWOW64\WinTypes.dll
wow64.dll	Win32 Emulation on NT64	Microsoft Corporation	C:\Windows\System32\wow64.dll
wow64cpu.dll	AMD64 Wow64 CPU	Microsoft Corporation	C:\Windows\System32\wow64cpu.dll
wow64win.dll	Wow64 Console and Win32 API L...	Microsoft Corporation	C:\Windows\System32\wow64win.dll
ws2_32.dll	Windows Socket 2.0 32-Bit DLL	Microsoft Corporation	C:\Windows\SysWOW64\ws2_32.dll
wshbth.dll	Windows Sockets Helper DLL	Microsoft Corporation	C:\Windows\SysWOW64\wshbth.dll

Figura 5 – Librerie di rete caricate dal processo notepad-classico.exe (Process Explorer)

Interpretazione tecnica

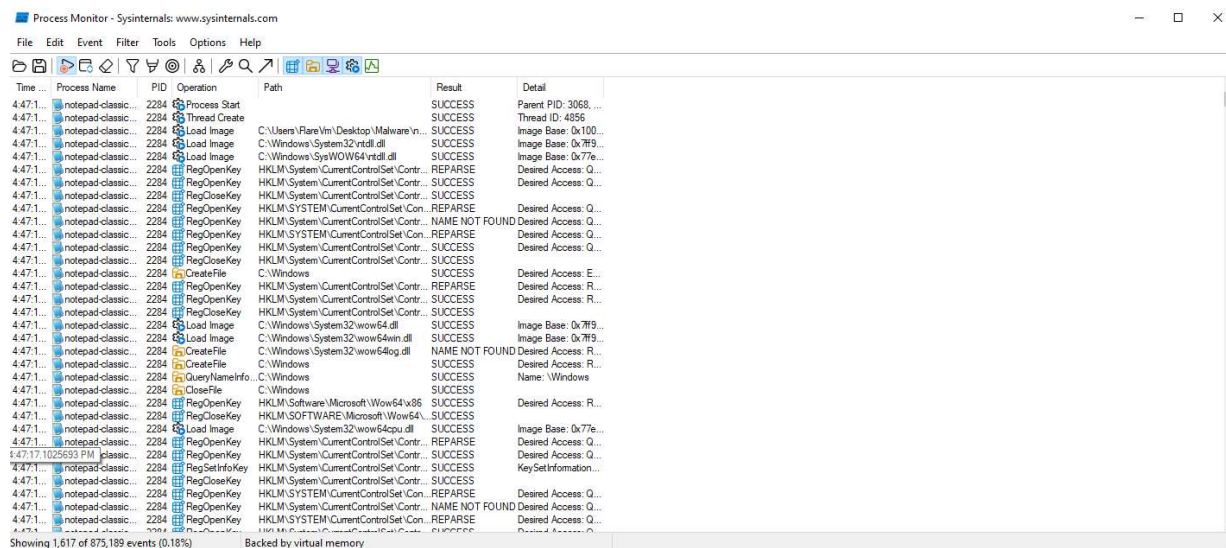
Il caricamento runtime delle librerie **WS2_32.dll** e **WININET.dll** conferma operativamente la presenza delle funzionalità di comunicazione di rete individuate staticamente tramite Hex Editor.

La corrispondenza tra indicatori statici (stringhe embedded nel binario) e comportamento runtime rafforza l'ipotesi di un **caricamento dinamico delle API di rete**, tecnica comunemente utilizzata per ridurre la visibilità statica delle capacità di comunicazione del malware.

4.3 Attività su file system e registro

L'analisi tramite Process Monitor, filtrata sul processo notepad-classico.exe, ha evidenziato numerose operazioni di:

- apertura e lettura di chiavi di registro
- accesso a directory di sistema
- caricamento dinamico di librerie



The screenshot displays the Process Monitor application window, showing a detailed log of system events for the process 'notepad-classico.exe'. The interface includes a menu bar (File, Edit, Event, Filter, Tools, Options, Help) and a toolbar with various icons for filtering and viewing events. The main pane is a table with columns: Time, Process Name, PID, Operation, Path, Result, and Detail. The log shows a sequence of operations including Process Start, Thread Create, Load Image (for various DLLs like ntdll.dll, user32.dll, and GDI32.dll), RegOpenKey, RegCloseKey, CreateFile, and QueryNameInfo. The results are mostly 'SUCCESS', with some 'REPARSE' and 'NAME NOT FOUND' entries. The status bar at the bottom indicates 'Showing 1,617 of 875,189 events (0.18%)' and 'Backed by virtual memory'.

Time	Process Name	PID	Operation	Path	Result	Detail
4:47:1...	notepad-classico...	2284	Process Start		SUCCESS	Parent PID: 3068, ...
4:47:1...	notepad-classico...	2284	Thread Create		SUCCESS	Thread ID: 4856
4:47:1...	notepad-classico...	2284	Load Image	C:\Users\Fare\Win\Desktop\Malware'n...	SUCCESS	Image Base: 0x100...
4:47:1...	notepad-classico...	2284	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x779...
4:47:1...	notepad-classico...	2284	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x779...
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
4:47:1...	notepad-classico...	2284	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
4:47:1...	notepad-classico...	2284	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
4:47:1...	notepad-classico...	2284	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
4:47:1...	notepad-classico...	2284	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
4:47:1...	notepad-classico...	2284	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x779...
4:47:1...	notepad-classico...	2284	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x779...
4:47:1...	notepad-classico...	2284	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
4:47:1...	notepad-classico...	2284	CreateFile	C:\Windows	SUCCESS	Desired Access: R...
4:47:1...	notepad-classico...	2284	QueryNameInfo	C:\Windows	SUCCESS	Name: \Windows
4:47:1...	notepad-classico...	2284	CloseFile	C:\Windows	SUCCESS	
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\Software\Microsoft\Wow64\...	SUCCESS	Desired Access: R...
4:47:1...	notepad-classico...	2284	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64...	SUCCESS	
4:47:1...	notepad-classico...	2284	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x77e...
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
4:47:1...	notepad-classico...	2284	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
4:47:1...	notepad-classico...	2284	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
4:47:1...	notepad-classico...	2284	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...

Figura 6 – Attività su file system e registro (Process Monitor)

Osservazione tecnica

Le operazioni osservate risultano in larga parte compatibili con il comportamento di un'applicazione Windows legittima. Tuttavia, considerate congiuntamente al caricamento dinamico delle API di rete e all'attività di comunicazione osservata, contribuiscono a delineare il comportamento di un **wrapper malevolo** che esegue codice aggiuntivo in background.

4.4 Attività di rete osservata

Durante l'esecuzione del campione, il traffico di rete è stato monitorato tramite **Wireshark** e **FakeNet-NG**.

Nel corso della cattura sono stati osservati:

- pacchetti UDP multicast diretti all'indirizzo 239.255.255.250:1900 (SSDP)
- pacchetti UDP broadcast associati a meccanismi di discovery e name resolution (ARP, NBNS)

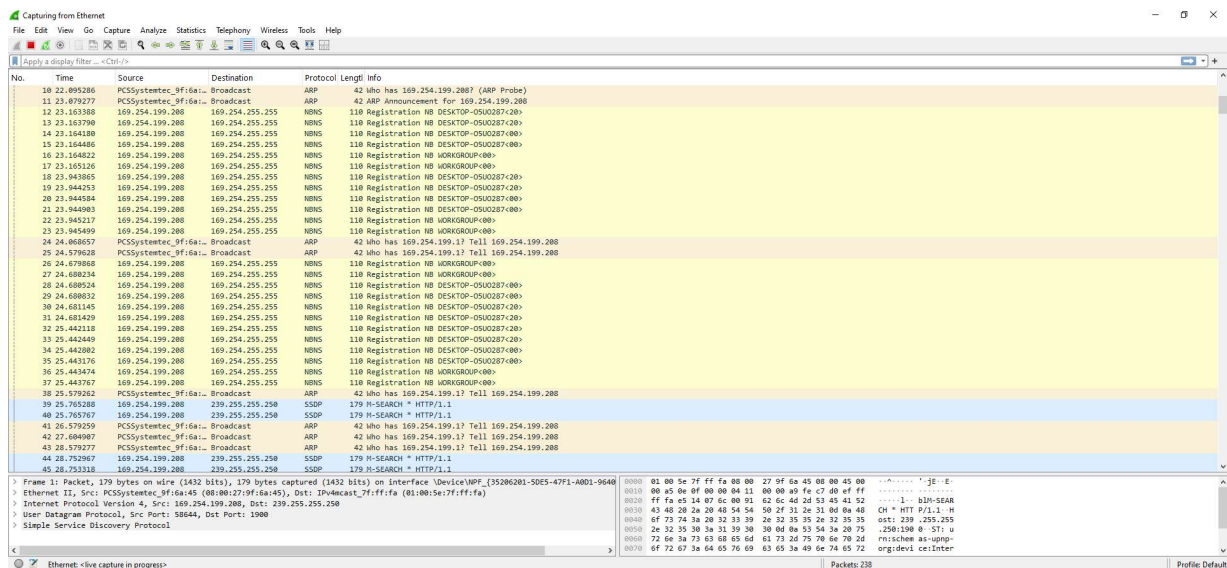


Figura 7 – Traffico di rete osservato (Wireshark)

Osservazione tecnica

Il traffico di rete osservato è riconducibile a normali operazioni di avvio e inizializzazione delle funzionalità di rete del sistema, come la ricerca di dispositivi o servizi presenti nella rete locale.

Non sono state osservate comunicazioni dirette verso server remoti né scambi di dati riconducibili a un controllo attivo dall'esterno. Tuttavia, la presenza di questo traffico indica che il processo analizzato attiva effettivamente le funzionalità di rete, in modo coerente con le API di comunicazione individuate nell'analisi statica e caricate durante l'esecuzione.

4.5 Sintesi dell'Analisi Dinamica

L'analisi dinamica ha confermato le ipotesi formulate durante la fase statica.

In particolare è stato osservato che:

- il campione mantiene un comportamento apparente legittimo
- il processo carica dinamicamente librerie di rete
- vengono inizializzate comunicazioni di rete intercettate dall'ambiente sandbox
- il comportamento osservato è coerente con una tecnica di mascheramento funzionale

Sulla base delle evidenze raccolte, il comportamento runtime del campione risulta coerente con quello di un **Trojan mascherato da applicazione legittima**, progettato per operare in modo discreto e a basso profilo.

5. Conclusione Finale

L'analisi del campione **notepad-classico.exe**, condotta tramite analisi statica e dinamica, ha permesso di identificarne la natura e il comportamento operativo.

L'analisi statica ha evidenziato **anomalie strutturali del formato PE**, in particolare la duplicazione delle sezioni .text e .rsrc, riconducibili a tecniche di **trojanizzazione e wrapping**. L'analisi delle stringhe ha inoltre confermato la presenza, direttamente nel binario, di riferimenti alle API di rete **WS2_32.dll** e **WININET.dll**, indicativi di capacità di comunicazione HTTP.

L'analisi dinamica ha confermato tali evidenze, mostrando che il campione mantiene un comportamento apparentemente legittimo, caricando a runtime le librerie di rete individuate staticamente e inizializzando attività di rete intercettate dall'ambiente sandbox.

Nel complesso, le evidenze raccolte consentono di classificare il campione come un **Trojan mascherato da applicazione legittima**, coerente con un contesto di laboratorio e privo di meccanismi avanzati di evasione o persistenza.