

# **REPORT TECNICO**

**ANALISI MALWARE**  
**notepad-classico.exe**

**Redatto da:** Nicolò Calì Cybersecurity Student

**Data:** 03/02/2026

## 1. Introduzione

Il presente documento riporta l'analisi tecnica del file eseguibile denominato "**notepad-classico.exe**".

L'obiettivo dell'analisi è comprendere la natura del file, identificarne le funzionalità potenzialmente malevole e documentare gli indicatori di compromissione.

L'analisi è stata condotta in un ambiente controllato (**FlareVM**) utilizzando metodologie di analisi statica e, successivamente, dinamica.

**Nome file:** notepad-classico.exe

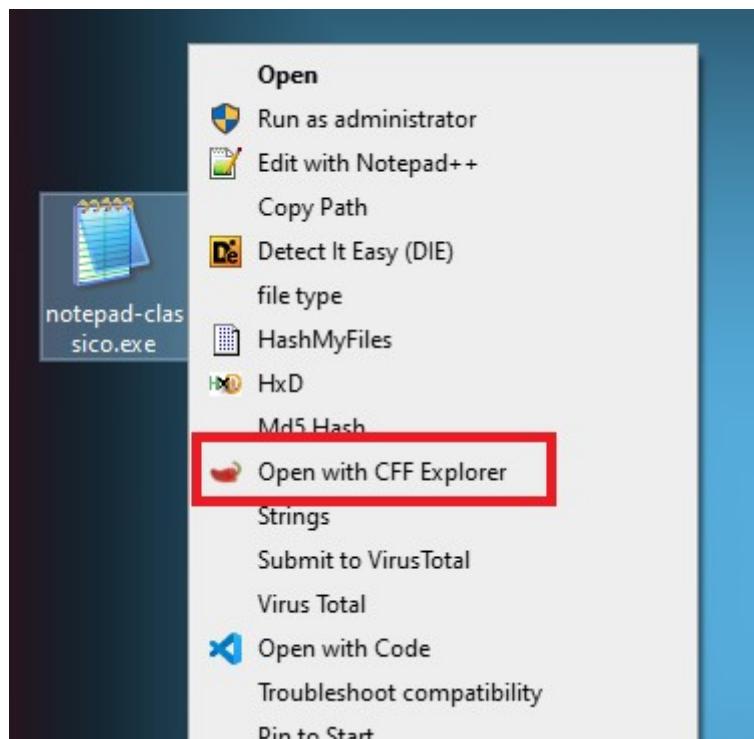
**Dimensione:** 626.95 KB

**Hash MD5:** EEA667929C0415EA0B74B7B9E9F9C23

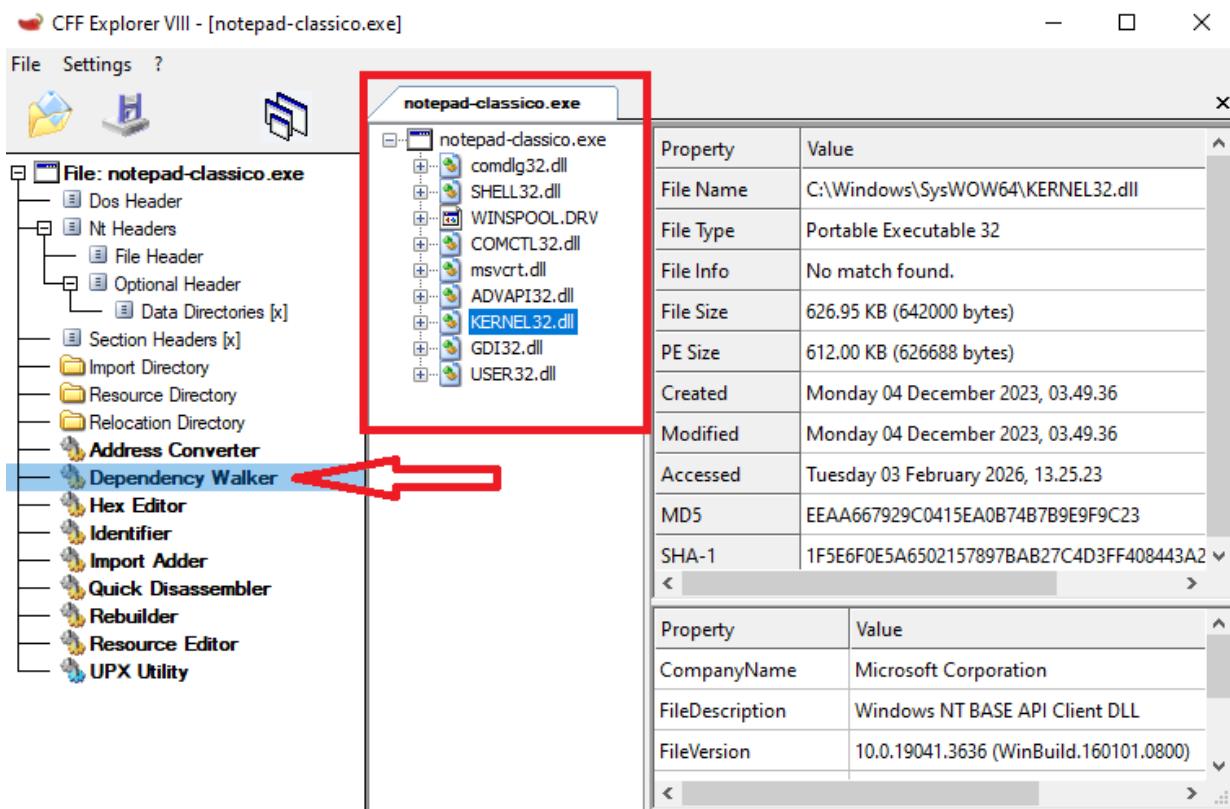
## 2. Analisi Statica - Librerie Importate

In questa sezione andremo ad analizzare le librerie importate dal malware, forniremo una descrizione di ognuna di esse e, per finire, andremo ad analizzare delle funzioni sospette racchiuse all'interno di queste librerie.

Per l'analisi utilizzerò il tool **CFF Explorer**.



Una volta che CFF Explorer si apre andiamo nella sezione "**Dipendancy Walker**" per vedere con facilità l'elenco delle Librerie utilizzate dal malware.



Capiamo il funzionamento di ognuna di esse:

- **comdlg32.dll** → Gestisce le finestre di dialogo comuni di Windows, come "Apri file", "Salva", o "Stampa". (Tipica di applicazioni con interfaccia grafica).
- **SHELL32.dll** → Fornisce funzioni per interagire con la shell di Windows, come l'apertura di file, l'esecuzione di programmi e la gestione delle icone.
- **WINSPOOL.DRV** → Contiene i driver e le funzioni per inviare documenti allo spooler di stampa (necessaria se il programma vuole stampare).
- **COMCTL32.dll** → Gestisce i controlli comuni dell'interfaccia utente moderna, come barre di stato, barre di avanzamento e tooltips.
- **msvcrt.dll** → È la libreria standard del C (Microsoft C Runtime); contiene funzioni base di programmazione come la gestione della memoria, stringhe e input/output.
- **ADVAPI32.dll** → **(Critica)** Gestisce funzionalità avanzate come il **Registro di Sistema**, i Servizi di Windows e gli account utente/sicurezza.
- **KERNEL32.dll** → **(Critica)** È il cuore del sistema operativo; gestisce la memoria, i file, i processi e i thread. Quasi ogni eseguibile dipende da questa.
- **GDI32.dll** → **(Graphics Device Interface)** Si occupa del disegno grafico di base: linee, curve, font e gestione dei colori sullo schermo.
- **USER32.dll** → Gestisce l'interfaccia utente di base: creazione e gestione delle finestre, mouse, tastiera e messaggi di sistema.

Ci concentreremo principalmente su **KERNEL32.dll**, per andare a visualizzare le funzioni contenute all'interno di questa specifica libreria ci sposteremo sulla sezione “**Import Directory**”.

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name
0003D10F	N/A	0003CA78	0003CA7C	0003CA80	0003
szAnsi	(nFunctions)	Dword	Dword	Dword	Dwo
<b>KERNEL32.dll</b>	<b>57</b>	<b>00040198</b>	<b>00000000</b>	<b>FFFFFF</b>	<b>0004</b>
GDI32.dll	24	00040280	00000000	FFFFFF	0004
USER32.dll	74	000402E4	00000000	FFFFFF	0004

OFTs	FTs (IAT)	Hint	Name
0003CC64	00000558	0003D486	0003D488
Dword	Dword	Word	szAnsi
00040A76	00040A76	0300	SetEndOfFile
00040A86	00040A86	0082	<b>DeleteFileW</b>
00040A94	00040A94	00F6	GetACP
00040A9E	00040A9E	035E	UnmapViewOfFile
00040A9F	00040A9F	00C7	FindFirstFileW

Le funzioni presenti nella libreria dimostrano alcuni comportamenti potenzialmente dannosi che il **malware** sarà in grado di avere.

Tra quelle visionate precedentemente notiamo:

- **CreateFileW/WriteFile**: Il malware può creare nuovi file o scrivere codice all'interno di file esistenti (magari per infettarli o per salvare dati rubati).
- **DeleteFileW**: Ha la capacità di cancellare file (comportamento tipico di un wiper o di un malware che vuole eliminare le proprie tracce).
- **FindFirstFileW**: Cerca file nel sistema (spesso usato per mappare il computer della vittima).

**Nota tecnica:** La "W" finale sta per **"Wide"**, indicando che la funzione supporta i caratteri **Unicode**.

Adesso procediamo ad esaminare la libreria “**ADVAPI32.dll** ” e le funzioni in esso incluse per vedere anche qui se esistono delle funzioni potenzialmente pericolose che il malware potrebbe utilizzare.

Module Name	Imports	OFTs	TimeStamp	ForwarderChain	Name RVA	FTs (IAT)
0003D08A	N/A	0003CA64	0003CA68	0003CA6C	0003CA70	0003CA74
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
SHELL32.dll	4	000400F0	00000000	FFFFFF	000404B5	00001174
WINSPOOL.DRV	3	00040104	00000000	FFFFFF	00040502	000012B4
COMCTL32.dll	1	00040114	00000000	FFFFFF	00040543	00001020
msvcrtdll	22	0004011C	00000000	FFFFFF	00040566	000012EC
<b>ADVAPI32.dll</b>	<b>7</b>	<b>00040178</b>	<b>00000000</b>	<b>FFFFFF</b>	<b>0004068A</b>	<b>00001000</b>
KERNEL32.dll	57	00040198	00000000	FFFFFF	0004070F	0000108C
GDI32.dll	24	00040280	00000000	FFFFFF	00040AF1	00001028

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00040698	00040698	01EF	RegQueryValueExW
000406AC	000406AC	01CA	RegCloseKey
000406BA	000406BA	01D0	RegCreateKeyW
000406CA	000406CA	0139	IsTextUnicode
000406DA	000406DA	01EE	RegQueryValueExA
000406EE	000406EE	01E4	RegOpenKeyExA
000406FE	000406FE	01FC	RegSetValueExW

Le funzioni che iniziano con “**Reg**” fanno riferimento alle **Registry**, ovvero il Registro di sistema.

Il **Registro di Sistema** è un enorme database dove Windows salva le impostazioni.

Le funzioni particolarmente interessanti sono:

- **RegCreateKeyW**: Crea una nuova "cartella" (chiave) nel registro.
- **RegSetValueExW**: Scrive un valore dentro una chiave.

### Perche risultano “Sospette”?

Spesso i malware usano RegSetValueExW per scrivere il proprio percorso in chiavi di avvio automatico. In questo modo, **ottengono la Persistenza**: ogni volta che accendi il computer, Windows legge quella chiave e avvia il virus automaticamente.

### 3. Analisi Statica - Sezioni del File

In questa fase continueremo ad effettuare un'analisi statica del malware al fine di esaminare nel dettaglio le sezioni di cui si compone, fornendo una descrizione per ognuna di esse.

Per questa ulteriore analisi utilizzeremo sempre CSS Explorer spostandoci però nel menu “**Section Headers**”.

Qui prenderemo in esame le tre colonne riportate nell'immagine sottostante:

- **Name** → Identifica l'etichetta della sezione (come .text per il codice o .rsrc per le risorse), permettendo di riconoscere il tipo di contenuto ospitato.
- **Virtual Size** → Indica la dimensione effettiva che la sezione occuperà una volta caricata nella memoria volatile (RAM) del sistema.
- **Raw Size** → Indica la dimensione fisica che la sezione occupa all'interno del file salvato sul disco rigido.

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...
000001D8	000001E0	000001E4	000001E8	000001EC	000001F0	000001F4	000001F8
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word
.text	00007748	00001000	00007800	00000400	00000000	00000000	0000
.data	00001BA8	00009000	00000800	00007C00	00000000	00000000	0000
.rsrc	00008DB4	0000B000	00008E00	00008400	00000000	00000000	0000
.text	0002B6AC	00014000	0002B800	00011200	00000000	00000000	0000
.idata	0000013E	00040000	00001200	0003CA00	00000000	00000000	0000
.rsrc	00008DB0	00042000	00008E00	0003DC00	00000000	00000000	0000

Per prima cosa sono andato a confrontare le **Virtual Size** con le **Raw Size**.

Se il Virtual Size è molto più grande del Raw Size, significa che c'è del codice “**compresso**” che esplode quando il programma parte.

La sezione **.data** ha una Virtual Size (1BA8) che è un po' più grande della Raw Size (800), ma non è una differenza così enorme.

Esaminando però la colonna **Name** notiamo qualcosa di anomalo: **le sezioni tendono a ripetersi** (sono presenti due .txt o due .rsrc).

Questa ridondanza non è conforme agli standard dei compilatori legittimi. È un forte indicatore che l'eseguibile è stato manipolato post-compilazione. È altamente probabile che il file sia stato "**packato**" (compresso/offuscato) o infettato, e che le sezioni duplicate contengano il **payload malevolo** che verrà estratto o eseguito in memoria, separatamente dal codice originale del "Notepad".

## 4. Analisi Dinamica

In questa fase passeremo da un analisi Statica ad una **Dinamica** ed osserveremo in tempo reale come il programma interagisce con il sistema operativo: quali file crea, quali chiavi di registro tocca e se prova a comunicare con l'esterno.

Dal momento che dovremo avviare il malware è importante assicurarsi che la macchina **FlareVM** non sia connessa ad internet.

Per effettuare l'analisi utilizziamo i seguenti tool:

- **Process Monitor** che si occupa di registrare ogni singolo accesso ai file ed al registro di sistema.
- **FakeNet-NG** che si occupa di simulare internet.

Su Process Monitor assicuriamoci di applicare correttamente i filtri in modo da vedere solamente i Log inerenti al malware **notepad-classico.exe**.

The screenshot shows the 'Process Monitor Filter' dialog box. At the top, there is a search bar with dropdown menus for 'Architecture' and 'Value', and a 'then' dropdown set to 'Include'. Below the search bar are 'Reset' and 'Add/Remove' buttons. The main area is a table with columns: Column, Relation, Value, and Action. A red arrow points to the first row where 'Process N...' is checked, 'is' is selected as the relation, 'notepad-classico...' is the value, and 'Include' is the action. The table contains several rows of filter conditions, mostly starting with a red 'X' and 'Exclude' action, indicating they are currently disabled. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Column	Relation	Value	Action
Process N...	is	notepad-classico...	Include
Process N...	is	Procmon.exe	Exclude
Process N...	is	Procexp.exe	Exclude
Process N...	is	Autoruns.exe	Exclude
Process N...	is	Procmon64.exe	Exclude
Process N...	is	Procexp64.exe	Exclude
Process N...	is	System	Exclude
Operation	begins with	IRP_MJ_	Exclude
Operation	begins with	FASTIO_	Exclude
Result	begins with	FAST IO	Exclude
Path	ends with	pagefile.sys	Exclude
Path	ends with	\$Mft	Exclude
Path	ends with	CMA Mir	Exclude

Avviamo **Fakenet** dal terminale tramite il comando **fakenet**.

```
PyInstaller\loader\pyimod02_importers.py:378: UserWarning: You are using cryptography on a 32-bit Python on a 64-bit Windows Operating System. Cryptography will be significantly faster if you switch to using a 64-bit Python.

[FAKENETNG]
[FAKENETNG]

Version 3.5

Developed by FLARE Team
Copyright (C) 2016-2024 Mandiant, Inc. All rights reserved.

02/03/26 03:44:36 PM [           Divterer] Loaded configuration file: C:\tools\fakenet\fakenet3.5\configs\default.ini
02/03/26 03:44:36 PM [           Divterer] Capturing traffic to packets_20260203_154436.pcap
02/03/26 03:44:36 PM [           Divterer] WARNING: No gateways configured!
02/03/26 03:44:37 PM [           Divterer] Setting gateway 192.168.56.1 on interface Ethernet
02/03/26 03:44:37 PM [           Divterer] WARNING: No DNS servers configured!
02/03/26 03:44:38 PM [           Divterer] Failed to set DNS 192.168.56.101 on interface Ethernet.
02/03/26 03:44:38 PM [           Divterer] netsh failed with error: b'The service has not been started.\r\n\r\n\r\n\r\n\r\n'
02/03/26 03:44:38 PM [           Divterer] Cannot fix DNS
02/03/26 03:44:38 PM [           Divterer] Please configure a DNS server in order to allow network resolution.
02/03/26 03:44:38 PM [           Divterer] Failed calling GetBestInterface
Root "Trusted Root Certification Authorities"
Signature matches Public Key
Certificate "fakenet_flare" added to store
```

## 4.1 Registry Activity

L'analisi con Process Monitor ha evidenziato tentativi di interazione con chiavi sensibili del Registro di Sistema.

Time ...	Process Name	PID	Operation	Path	Result	Detail
3:47:0...	notepad-classic...	4620	RegQueryKey	HKLM\	SUCCESS	Query: HandleTag...
3:47:0...	notepad-classic...	4620	RegQueryKey	HKLM\	SUCCESS	Query: Name
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\Software\WOW6432Node\Micr...	REPARSE	Desired Access: R...
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\SOFTWARE\Microsoft\Rpc	SUCCESS	Desired Access: R...
3:47:0...	notepad-classic...	4620	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Rpc	SUCCESS	KeySetInformation...
3:47:0...	notepad-classic...	4620	RegQueryValue	HKLM\SOFTWARE\Microsoft\Rp... NAME NOT FOUND Length: 16		
3:47:0...	notepad-classic...	4620	RegCloseKey	HKLM\SOFTWARE\Microsoft\Rpc	SUCCESS	
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\System\CurrentControlSet\Serv... REPARSE		Desired Access: R...
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\System\CurrentControlSet\Serv... NAME NOT FOUND Desired Access: R...		
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\System\CurrentControlSet\Serv... REPARSE		Desired Access: R...
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\System\CurrentControlSet\Serv... NAME NOT FOUND Desired Access: R...		
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\System\CurrentControlSet\Contr... REPARSE		Desired Access: R...
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\System\CurrentControlSet\Contr... SUCCESS		Desired Access: R...
3:47:0...	notepad-classic...	4620	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr... SUCCESS		KeySetInformation...
3:47:0...	notepad-classic...	4620	RegQueryValue	HKLM\System\CurrentControlSet\Contr... SUCCESS		Type: REG_SZ, Le...
3:47:0...	notepad-classic...	4620	RegCloseKey	HKLM\System\CurrentControlSet\Contr... SUCCESS		
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\System\Setup	SUCCESS	Desired Access: R...
3:47:0...	notepad-classic...	4620	RegSelInfoKey	HKLM\SYSTEM\Setup	SUCCESS	KeySetInformation...
3:47:0...	notepad-classic...	4620	RegQueryValue	HKLM\SYSTEM\Setup\OOBEInProgress	SUCCESS	Type: REG_DWO...
3:47:0...	notepad-classic...	4620	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS	
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\SYSTEM\Setup	SUCCESS	Desired Access: R...
3:47:0...	notepad-classic...	4620	RegSetInfoKey	HKLM\SYSTEM\Setup	SUCCESS	KeySetInformation...
3:47:0...	notepad-classic...	4620	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupIn... SUCCESS		Type: REG_DWO...
3:47:0...	notepad-classic...	4620	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS	
3:47:0...	notepad-classic...	4620	RegQueryKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Query: HandleTag...
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND Desired Access: Q...	
3:47:0...	notepad-classic...	4620	RegQueryKey	HKLM\	SUCCESS	Query: HandleTag...
3:47:0...	notepad-classic...	4620	RegQueryKey	HKLM\	SUCCESS	Query: Name
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\Software\WOW6432Node\Polic...	REPARSE	Desired Access: R...
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\...	NAME NOT FOUND Desired Access: R...	
3:47:0...	notepad-classic...	4620	RegQueryKey	HKLM\	SUCCESS	Query: HandleTag...
3:47:0...	notepad-classic...	4620	RegQueryKey	HKLM\	SUCCESS	Query: Name
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\Software\WOW6432Node\Micr...	REPARSE	Desired Access: Q...
3:47:0...	notepad-classic...	4620	RegOpenKey	HKLM\SOFTWARE\Microsoft\Rpc	SUCCESS	Desired Access: Q...
3:47:0...	notepad-classic...	4620	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Rpc	SUCCESS	KeySetInformation...

**Comportamento osservato:** Sono state rilevate operazioni di apertura e interrogazione (**RegOpenKey**, **RegQueryKey**) verso il ramo **HKLM** (HKEY\_LOCAL\_MACHINE), specificamente in percorsi come HKLM\SYSTEM\Setup e HKLM\SOFTWARE\Microsoft\Rpc.

**Analisi:** L'accesso al ramo HKLM suggerisce che il malware tenta di interagire con le configurazioni globali del sistema, piuttosto che limitarsi a quelle dell'utente corrente. Questo comportamento richiede solitamente privilegi elevati e può indicare tentativi di evasione, persistenza o modifica delle impostazioni di sicurezza.

## 4.2 File System Activity

L'analisi dei log di Process Monitor ha permesso di osservare come il malware interagisce con il file system durante la sua esecuzione.

Process Monitor - Sysinternals: www.sysinternals.com						
Time ...	Process Name	PID	Operation	Path	Result	Detail
3:47:2...	notepad-classic...	4620	CreateFile	Mapp...C:\Windows\System32\en-US\user32.d...	SUCCESS	SyncType: SyncTy...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\WinSxS\x86_microsoft.win...	SUCCESS	Offset: 668,672, Le...
3:47:2...	notepad-classic...	4620	CreateFile	C:\Users\flarevm\Desktop\dwmapi.dll	NAME NOT FOUND	Desired Access: R...
3:47:2...	notepad-classic...	4620	CreateFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Desired Access: R...
3:47:2...	notepad-classic...	4620	QueryBasicInfor...	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	CreationTime: 12/4...
3:47:2...	notepad-classic...	4620	CloseFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	
3:47:2...	notepad-classic...	4620	CreateFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Desired Access: R...
3:47:2...	notepad-classic...	4620	CreateFileMapp...	C:\Windows\SysWOW64\dwmapi.dll	FILE LOCKED WI...	SyncType: SyncTy...
3:47:2...	notepad-classic...	4620	QueryStandardI...	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	AllocationSize: 143...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Offset: 0, Length: 4...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Offset: 1,024, Leng...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Offset: 123,904, Le...
3:47:2...	notepad-classic...	4620	CreateFileMapp...	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	SyncType: SyncTy...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Offset: 66,560, Len...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Offset: 96,256, Len...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Offset: 104,448, Le...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Offset: 104,960, Le...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Offset: 97,280, Len...
3:47:2...	notepad-classic...	4620	CloseFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Offset: 33,792, Len...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 95,232, Len...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 398,336, Le...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 504,832, Le...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 472,064, Le...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 439,296, Le...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 619,520, Le...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 431,104, Le...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 660,480, Le...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 4,404,224, ...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 66,560, Len...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 2,003,968, ...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 1,356,800, ...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 1,881,088, ...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 2,958,336, ...
3:47:2...	notepad-classic...	4620	ReadFile	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Offset: 3,077,120, ...

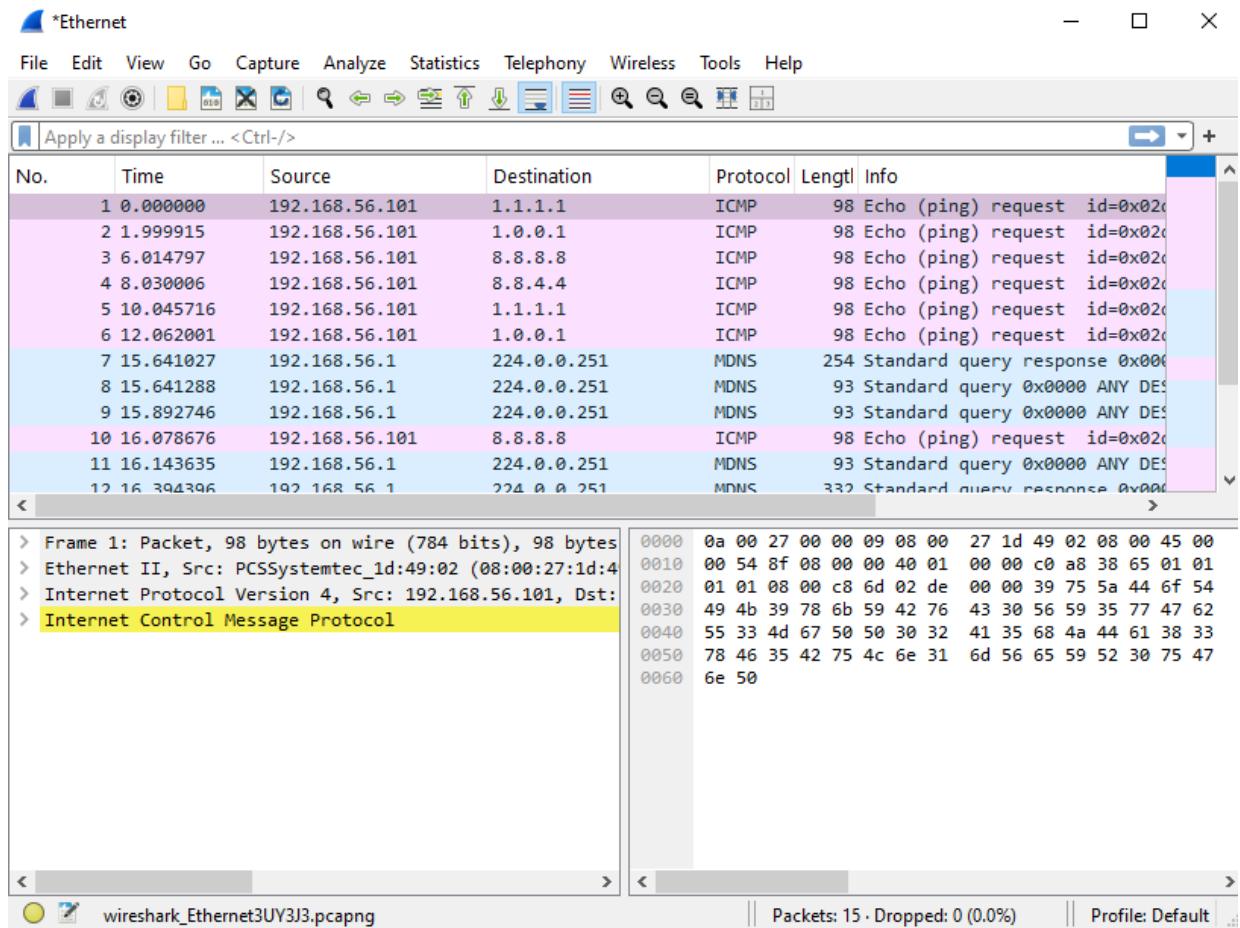
**Comportamento osservato:** Sono state rilevate numerose operazioni di lettura (ReadFile) e apertura (CreateFile) relative a librerie di sistema, come dwmapi.dll e windows.storage.dll.

**Analisi:** È stato notato un tentativo di caricamento della DLL dwmapi.dll direttamente dalla directory di esecuzione (C:\Users\flarevm\Desktop\),

terminato con esito NAME NOT FOUND, seguito dal caricamento corretto dalla cartella di sistema SysWOW64.

### 4.3 Network Activity

Durante l'esecuzione, il malware ha generato traffico di rete immediato, rilevato tramite Wireshark.



**Comportamento osservato:** Il processo notepad-classico.exe ha inviato richieste ICMP (Ping) verso indirizzi IP pubblici specifici:

- 8.8.8.8 (Google DNS)
- 1.1.1.1 (Cloudflare DNS)

**Analisi:** Questo comportamento non è coerente con un normale editor di testo. Si tratta verosimilmente di un **Connectivity Check**: il malware verifica se la macchina

infetta ha accesso a Internet attivo, probabilmente come pre-requisito per scaricare ulteriori payload o contattare un server di Comando e Controllo.

## 6. Conclusione e Considerazioni

Sulla base dell'analisi effettuata, il campione notepad-classico.exe è classificato come **malevolo**.

Nonostante il camuffamento da applicazione legittima (Notepad), il file presenta indicatori di compromissione (**IOC**) critici:

- **Offuscamento:** La presenza di sezioni duplicate (.text, .rsrc) indica l'uso di software di packing per nascondere il codice originale.
- **Persistenza:** I tentativi di scrittura nel Registro di Sistema (HKLM) dimostrano l'intenzione di radicarsi nel sistema operativo.
- **Comportamento di Rete:** Il connectivity check verso DNS pubblici (8.8.8.8, 1.1.1.1) all'avvio è tipico dei malware che necessitano di comunicare con l'esterno.

Le caratteristiche osservate suggeriscono che il malware agisca come un **Dropper** o un **Downloader**. Il suo obiettivo primario non sembra essere il danneggiamento diretto immediato, bensì garantire la persistenza e verificare la connessione internet, presumibilmente per scaricare ed eseguire ulteriori payload malevoli in una fase successiva.