

# Report Analisi Statica Malware: notepad-classico.exe

**Studente:** Nicola Cassandra

**Oggetto:** Analisi preliminare del campione `notepad-classico.exe`.

## 1. Introduzione e Identificazione del Campione

L'attività ha previsto l'analisi statica di un file eseguibile denominato `notepad-classico.exe`. Nonostante il nome e l'icona suggeriscano trattarsi del legittimo editor di testo di Windows ("Blocco note"), l'analisi preliminare rivela indicatori malevoli significativi.

Il file è stato analizzato all'interno di un ambiente virtualizzato sicuro (FlareVM) utilizzando il tool **PEStudio**.

**Dati identificativi rilevati:**

- **Nome File:** `notepad-classico.exe`
- **Rilevamento VirusTotal:** 58/72 (Alto tasso di malignità).
- **Tipologia:** Esecuibile PE a 32-bit.
- **Compilazione:** 13 Aprile 2008 (Possibile *Time Stomping* per falsificare la data).

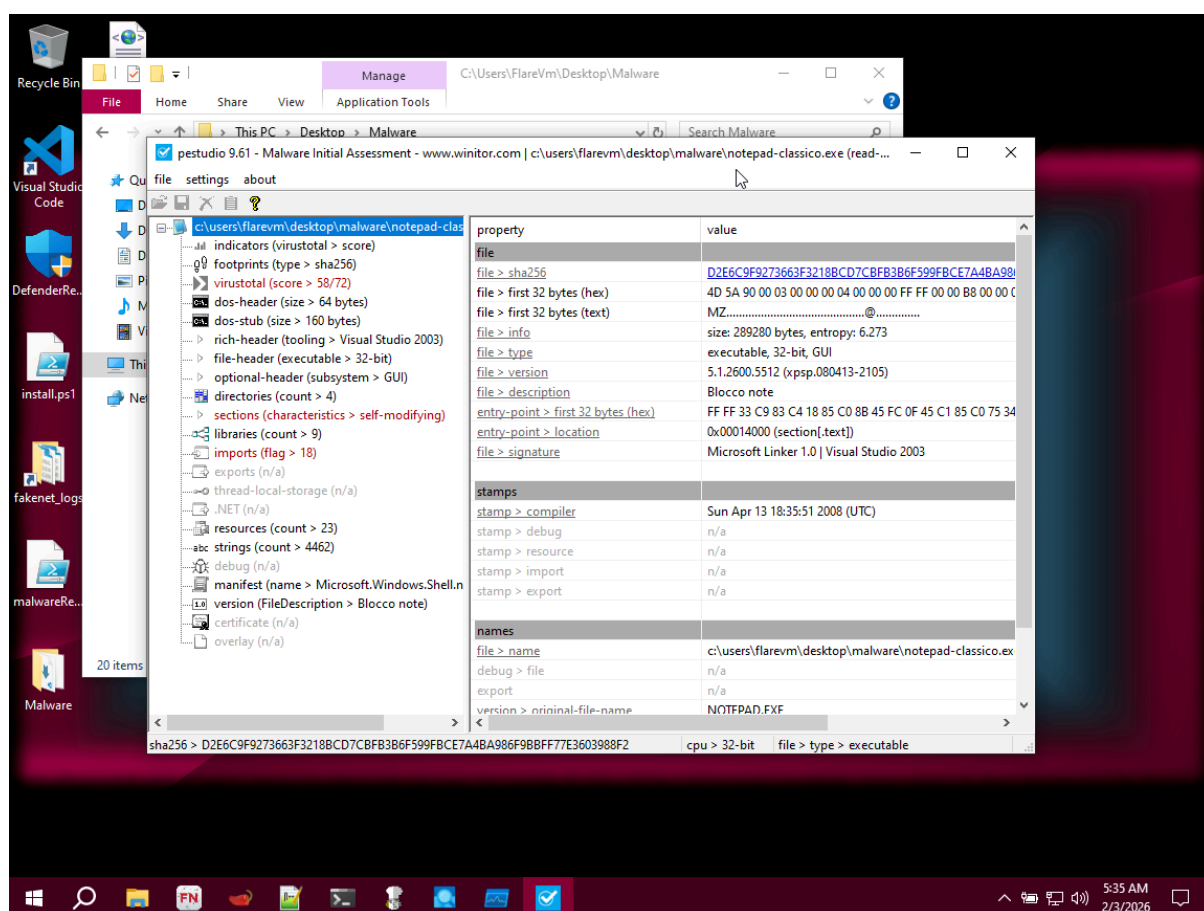


Fig. 1 - Panoramica iniziale di PESTudio che mostra il punteggio VirusTotal e l'avviso "self-modifying".

## 2. Analisi delle Librerie Importate (DLL)

L'analisi dell'Import Table rivela che il malware carica diverse librerie dinamiche (DLL) standard di Windows. Sebbene molte siano legittime, la loro combinazione suggerisce capacità offensive.

Le principali librerie identificate sono:

Libreria (DLL)	Descrizione	Potenziale Utilizzo Malevolo
<b>KERNEL32.dll</b>	Gestione core del sistema (file, memoria, processi).	Essenziale per operazioni di file system e manipolazione della memoria.
<b>ADVAPI32.dll</b>	Advanced Windows API (Registro, Servizi).	Utilizzata per ottenere persistenza (avvio automatico) modificando il Registro di Sistema.
<b>USER32.dll</b>	Interfaccia utente e gestione input.	Può essere usata per Keylogging (cattura tasti) o creare finestre ingannevoli.
<b>SHELL32.dll</b>	Gestione della Shell di Windows.	Permette l'esecuzione di comandi esterni o l'apertura di altri file.
<b>WINSPOOL.DRV</b>	Driver di stampa.	Importazione anomala per un semplice notepad; talvolta usata in tecniche di injection specifiche.

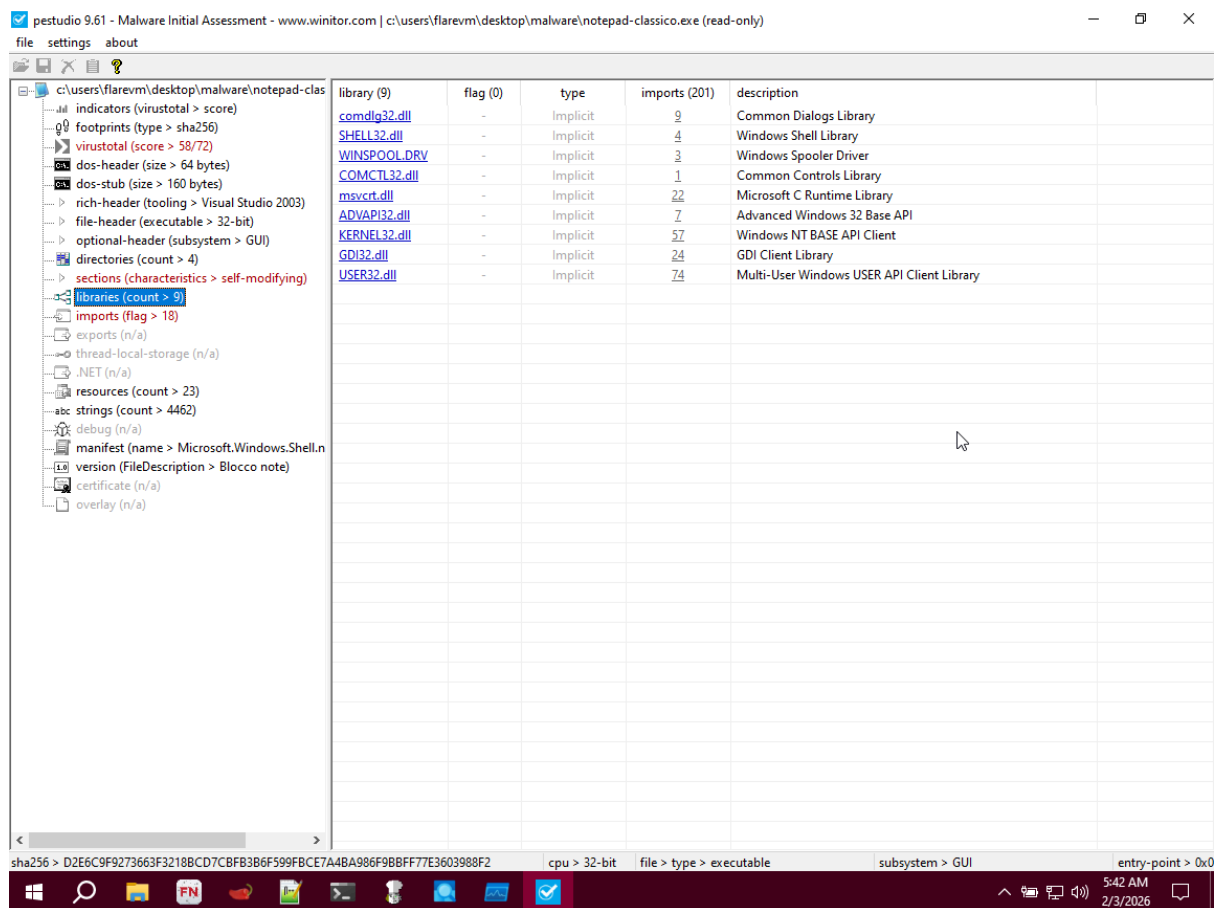


Fig. 2 - Elenco delle librerie importate visualizzate in PESTudio.

## Focus sulle Funzioni Sospette (Imports)

Approfondendo le funzioni specifiche importate da **KERNEL32.dll**, sono state evidenziate capacità critiche:

- **Manipolazione File:** **WriteFile**, **DeleteFileW**, **FindFirstFileW**. Il malware ha la capacità di cercare, creare e cancellare file sul disco, comportamento tipico di *dropper* o *wiper*.
- **Manipolazione Memoria:** **MapViewOfFile**, **UnmapViewOfFile**. Queste funzioni sono spesso indicatori di tecniche di **Process Injection** o di disimballaggio (unpacking) del codice in memoria.

c:\users\flarevm\desktop\malware\notepad-class	imports (201)	flag (18)	type	ordinal	first-thunk (IAT)	first-thunk-original (INT)	library
indicators (virustotal > score)	<a href="#">FoldStringW</a>	-	implicit	-	0x00040868	0x00040900	KERNEL32.dll
footprints (type > sha256)	<a href="#">CloseHandle</a>	-	implicit	-	0xD6FF5000	0x0004090E	KERNEL32.dll
virustotal (score > 58/72)	<a href="#">IstrcpvW</a>	-	implicit	-	0x89FC4D8B	0x0004091C	KERNEL32.dll
dos-header (size > 64 bytes)	<a href="#">ReadFile</a>	-	implicit	-	0x0096203D	0x00040928	KERNEL32.dll
dos-stub (size > 160 bytes)	<a href="#">CreateFileW</a>	-	implicit	-	0x895E5F01	0x00040934	KERNEL32.dll
rich-header (tooling > Visual Studio 2003)	<a href="#">IstrcmpiW</a>	-	implicit	-	0x0096241D	0x00040942	KERNEL32.dll
file-header (executable > 32-bit)	<a href="#">GetCurrentProcessId</a>	x	implicit	-	0x34E85B01	0x0004094E	KERNEL32.dll
optional-header (subsystem > GUI)	<a href="#">GetProcAddress</a>	-	implicit	-	0xC9000054	0x00040964	KERNEL32.dll
directories (count > 4)	<a href="#">GetCommandLineW</a>	-	implicit	-	0xCC004C2	0x00040976	KERNEL32.dll
sections (characteristics > self-modifying)	<a href="#">IstrcatW</a>	-	implicit	-	0xCCCCCCCC	0x00040988	KERNEL32.dll
libraries (count > 9)	<a href="#">FindClose</a>	-	implicit	-	0x1FE8006A	0x00040994	KERNEL32.dll
imports (flag > 18)	<a href="#">FindFirstFileW</a>	x	implicit	-	0xC2FFFFFF	0x000409A0	KERNEL32.dll
exports (n/a)	<a href="#">GetFileAttributesW</a>	-	implicit	-	0xCCCC001C	0x000409B2	KERNEL32.dll
thread-local-storage (n/a)	<a href="#">IstrcmpW</a>	-	implicit	-	0x8BCCCCC	0x000409C8	KERNEL32.dll
.NET (n/a)	<a href="#">MulDiv</a>	-	implicit	-	0xEC8B55FF	0x000409D4	KERNEL32.dll
resources (count > 23)	<a href="#">IstrcpvW</a>	-	implicit	-	0x08758B56	0x000409DE	KERNEL32.dll
strings (count > 4462)	<a href="#">LocalSize</a>	-	implicit	-	0x8B66C933	0x000409EA	KERNEL32.dll
debug (n/a)	<a href="#">GetLastError</a>	-	implicit	-	0xC985660E	0x000409F6	KERNEL32.dll
manifest (name > Microsoft.Windows.Shell.n	<a href="#">WriteFile</a>	x	implicit	-	0x8BFB8B57	0x00040A06	KERNEL32.dll
version (FileDescription > Blocco note)	<a href="#">SetLastError</a>	-	implicit	-	0x662374C6	0x00040A12	KERNEL32.dll
certificate (n/a)	<a href="#">WideCharToMultiByte</a>	-	implicit	-	0x743AF983	0x00040A22	KERNEL32.dll
overlay (n/a)	<a href="#">LocalReAlloc</a>	-	implicit	-	0xF9836606	0x00040A38	KERNEL32.dll
	<a href="#">FormatMessageW</a>	-	implicit	-	0x8B02755C	0x00040A48	KERNEL32.dll
	<a href="#">GetUserDefaultUILanguage</a>	-	implicit	-	0x15FF50F8	0x00040A5A	KERNEL32.dll
	<a href="#">SetEndOfFile</a>	-	implicit	-	0x01001244	0x00040A76	KERNEL32.dll
	<a href="#">DeleteFileW</a>	x	implicit	-	0x66088B66	0x00040A86	KERNEL32.dll
	<a href="#">GetACP</a>	-	implicit	-	0xE375C985	0x00040A94	KERNEL32.dll
	<a href="#">UnmapViewOfFile</a>	x	implicit	-	0x0274FE38	0x00040A9E	KERNEL32.dll
	<a href="#">MultiByteToWideChar</a>	-	implicit	-	0xC78B4747	0x00040AB0	KERNEL32.dll
	<a href="#">MapViewOfFile</a>	x	implicit	-	0xC25D5E5F	0x00040AC6	KERNEL32.dll

Fig. 3 - Funzioni importate sospette (flagged) evidenziate dal tool.

### 3. Analisi delle Sezioni e Struttura PE

L'analisi delle sezioni (Sections Header) è la parte che fornisce le prove più evidenti della natura malevola del file. Sono state riscontrate anomalie strutturali che non sono presenti nel software legittimo.

#### Anomalie Riscontrate:

- Sezioni Duplicate:** Sono presenti due sezioni nominate **.text** e due **.rsrc**. Questo è un chiaro segnale di manipolazione del file PE per nascondere il payload reale.
- Entropia Elevata:** Le sezioni di codice mostrano un'entropia superiore a 6.2, indicando che il contenuto è probabilmente compresso o cifrato ("Packed").
- Permessi RWX (Self-Modifying):** La **Section[3]** (.text) è marcata come **Self-modifying** e possiede i permessi di **Scrittura ed Esecuzione** (Write + Execute).

pestdio 9.61 - Malware Initial Assessment - www.wintr.com | c:\users\flawm\desktop\malware\notepad-classico.exe (read-only)

file settings about

pestdio 9.61 - Malware Initial Assessment - www.wintr.com | c:\users\flawm\desktop\malware\notepad-classico.exe (read-only)

property	value	value	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]	section[4]	section[5]
name	.text	.data	.rsrc	.text	.data	.rsrc
name	18135B212CAF8C7A8FEAF...	87C8B581163F3AA8623127...	5E074AE07548C823C26E8C...	0033E40079E7586AED07A86...	743DAD29AE4A33E573F7043...	C913461089289C2D44100AE...
entropy	6.214	1.149	5.421	6.428	5.439	5.407
file > ratio (99.65%)	10.62 %	0.71 %	12.57 %	61.59 %	1.59 %	12.57 %
raw-address (begin)	0x00000400	0x00007C00	0x00008400	0x00011200	0x0003CA00	0x0003DC00
raw-address (end)	0x00007C00	0x00008400	0x00011200	0x0003CA00	0x0003DC00	0x00046A00
raw-size (288256 bytes)	0x00007800 (30720 bytes)	0x00000800 (2048 bytes)	0x00008E00 (36352 bytes)	0x00002800 (178176 bytes)	0x00001200 (4608 bytes)	0x00008E00 (36352 bytes)
virtual-address (begin)	0x00001000	0x00009000	0x0000B000	0x00014000	0x00040000	0x00042000
virtual-address (end)	0x00007800	0x0000A800	0x00013800	0x0003F600	0x00041100	0x00044A00
virtual-size (292416 bytes)	0x00007740 (30536 bytes)	0x00007BA8 (7080 bytes)	0x00008D84 (36276 bytes)	0x000028A4 (17788 bytes)	0x0000113E (4414 bytes)	0x00008D80 (36272 bytes)
Characteristics	0x50000020	0xC0000040	0x40000040	0xE0000020	0xC0000040	0x40000040
write	-	x	-	x	x	-
execute	x	-	-	x	-	-
share	-	-	-	-	-	-
self-modifying	-	-	-	x	-	-
virtual	-	-	-	-	-	-
Items						
directory > import	-	-	-	-	0x00040000	-
directory > resource	-	-	-	-	-	0x00042000
directory > relocation	-	-	-	0x0003F600	-	-
directory > import-address	0x00001000	-	-	-	-	-
manifest	-	-	-	-	-	0x00046712
version	-	-	-	-	-	0x00046382
base-of-code	0x00001000	-	-	-	-	-
base-of-data	-	0x00008000	-	-	-	-
entry-point > location	-	-	-	0x00014000	-	-

sha256 > D2E6C9F9273663F3218BCD7CBF8384F599F8CE7A4BA896F98BF77E3603988F2

cpu > 32-bit

file > type > executable

subsystem > GUI

entry-point > 0x00014000

5:58 AM 2/3/2025

Fig. 4 - Tabella delle sezioni. Notare la sezione evidenziata con permessi di scrittura ed esecuzione e flag "self-modifying".

## Interpretazione Tecnica:

La coesistenza di permessi di scrittura ed esecuzione viola la regola di sicurezza **W^X** (Write XOR Execute). Questo suggerisce che il malware utilizzi un **Packer**. All'avvio, un piccolo pezzo di codice (stub) decifrerà il vero malware scrivendolo nella sezione **.text** per poi eseguirlo.

# Analisi Dinamica: Comportamento Runtime di `notepad-classico.exe`

**Oggetto:** Analisi del comportamento di rete e di sistema del campione in ambiente controllato (FlareVM).

**Strumenti utilizzati:** Process Monitor, FakeNet-NG, Wireshark.

## 1. Fase di Inizializzazione e Verifica Connettività (Connectivity Check)

Immediatamente dopo l'esecuzione, il malware non manifesta subito comportamenti ostili, ma esegue una verifica preliminare per accertarsi di essere connesso a Internet. Questa è una comune tecnica di **Evasione**: se il malware non riceve risposta (perché è in una sandbox offline), spesso termina l'esecuzione per non farsi analizzare.

Dall'analisi del traffico di rete tramite **Wireshark**, si osserva una sequenza di richieste **ICMP (Ping)** verso server DNS pubblici ad alta affidabilità:

- **Google Public DNS:** 8.8.8.8 ;  
8.8.4.4.
- **Cloudflare DNS:** 1.1.1.1 ;  
1.0.0.1.

La sequenza dei ping è rapida e ripetuta, confermando che il codice malevolo attende una risposta "Echo Reply" prima di procedere alla fase successiva dell'infezione.

No.	Time	Source	Destination	Protocol	Length	Info
160	278.718808	192.168.56.102	8.8.8.8	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64 (i
161	280.737439	192.168.56.102	8.8.4.4	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64 (i
162	282.756751	192.168.56.102	1.1.1.1	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64 (i
163	283.746982	192.168.56.1	192.168.56.255	UDP	86	57621 → 57621 Len=44
164	284.761151	192.168.56.102	1.0.0.1	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64 (i
165	288.788651	192.168.56.102	8.8.8.8	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64 (i
166	289.455158	192.168.56.1	224.0.0.251	MDNS	449	Standard query response 0x0000 PTR Nicola._dosvc._
167	289.457540	192.168.56.1	224.0.0.251	MDNS	84	Standard query 0x0000 ANY Nicola._dosvc._tcp.loc
168	289.708013	192.168.56.1	224.0.0.251	MDNS	84	Standard query 0x0000 ANY Nicola._dosvc._tcp.loc
169	289.958867	192.168.56.1	224.0.0.251	MDNS	84	Standard query 0x0000 ANY Nicola._dosvc._tcp.loc
170	290.209660	192.168.56.1	224.0.0.251	MDNS	509	Standard query response 0x0000 PTR, cache flush N
171	290.210350	192.168.56.1	224.0.0.251	MDNS	454	Standard query response 0x0000 SRV, cache flush 0
172	290.799599	192.168.56.102	8.8.4.4	ICMP, --	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64 (i
173	292.807862	192.168.56.102	1.1.1.1	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64 (i
174	294.833683	192.168.56.102	1.0.0.1	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64 (i
175	298.852745	192.168.56.102	8.8.8.8	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64 (i
176	300.866934	192.168.56.102	8.8.4.4	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64 (i
177	302.868357	192.168.56.102	1.1.1.1	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64 (i
178	304.874943	192.168.56.102	1.0.0.1	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64 (i

Fig. 1 - Dettaglio Wireshark: Sequenza di richieste Echo (Ping) verso DNS Google e Cloudflare.

## 2. Fase di "Call Home" (Comando e Controllo)

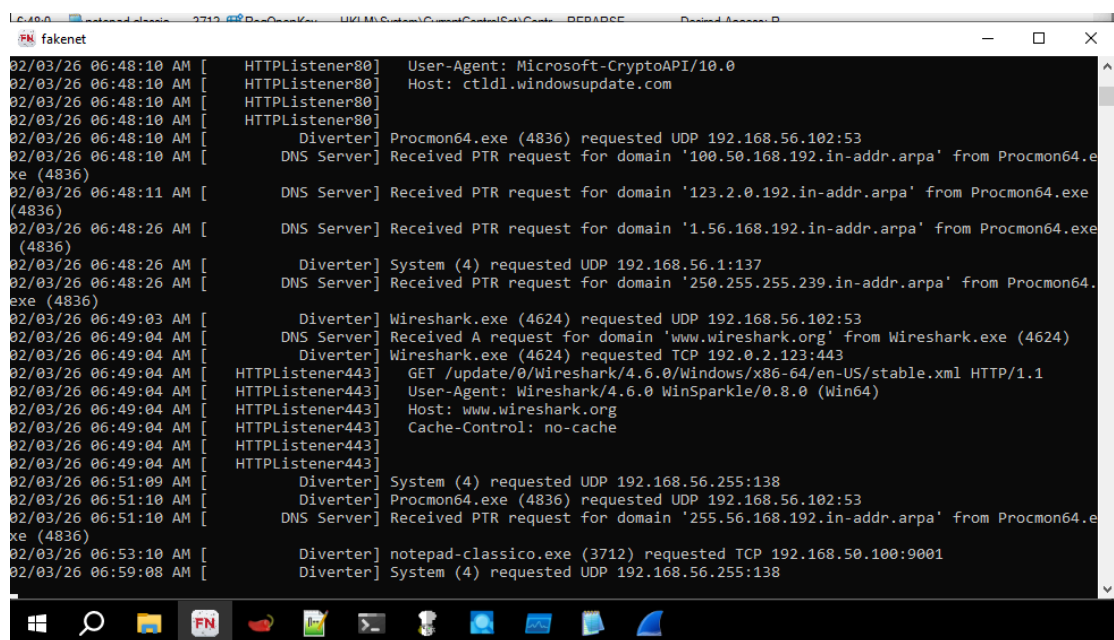
Una volta che il malware "crede" di essere online (grazie alla simulazione di rete fornita da FakeNet-NG), rivela la sua vera natura tentando di stabilire una connessione verso il server dell'attaccante (C2).

Dalla console di **FakeNet-NG**, abbiamo intercettato con successo questa comunicazione critica:

- **Processo:** `notepad-classico.exe` (PID 3712).
- **Protocollo:** TCP.
- **Destinazione Intercettata:** `192.168.56.108` (indirizzo IP simulato o reindirizzato).
- **Porta di Destinazione:** **9001**.

L'utilizzo della porta **9001** è un forte Indicatore di Compromissione (IoC). Non è una porta standard per traffico web (80/443), ma è frequentemente utilizzata da:

- Tool di accesso remoto (RAT).
- Client della rete **Tor**.
- Reverse Shells.



```
02/03/26 06:48:10 AM [ HTTPListener80] User-Agent: Microsoft-CryptoAPI/10.0
02/03/26 06:48:10 AM [ HTTPListener80] Host: ctldl.windowsupdate.com
02/03/26 06:48:10 AM [ HTTPListener80]
02/03/26 06:48:10 AM [ HTTPListener80]
02/03/26 06:48:10 AM [ Diverter] Procmon64.exe (4836) requested UDP 192.168.56.102:53
02/03/26 06:48:10 AM [ DNS Server] Received PTR request for domain '100.50.168.192.in-addr.arpa' from Procmon64.exe (4836)
02/03/26 06:48:11 AM [ DNS Server] Received PTR request for domain '123.2.0.192.in-addr.arpa' from Procmon64.exe (4836)
02/03/26 06:48:26 AM [ DNS Server] Received PTR request for domain '1.56.168.192.in-addr.arpa' from Procmon64.exe (4836)
02/03/26 06:48:26 AM [ Diverter] System (4) requested UDP 192.168.56.1:137
02/03/26 06:48:26 AM [ DNS Server] Received PTR request for domain '250.255.255.239.in-addr.arpa' from Procmon64.exe (4836)
02/03/26 06:49:03 AM [ Diverter] Wireshark.exe (4624) requested UDP 192.168.56.102:53
02/03/26 06:49:04 AM [ DNS Server] Received A request for domain 'www.wireshark.org' from Wireshark.exe (4624)
02/03/26 06:49:04 AM [ Diverter] Wireshark.exe (4624) requested TCP 192.0.2.123:443
02/03/26 06:49:04 AM [ HTTPListener443] GET /update/0/Wireshark/4.6.0/Windows/x86-64/en-US/stable.xml HTTP/1.1
02/03/26 06:49:04 AM [ HTTPListener443] User-Agent: Wireshark/4.6.0 WinSparkle/0.8.0 (Win64)
02/03/26 06:49:04 AM [ HTTPListener443] Host: www.wireshark.org
02/03/26 06:49:04 AM [ HTTPListener443] Cache-Control: no-cache
02/03/26 06:49:04 AM [ HTTPListener443]
02/03/26 06:51:09 AM [ Diverter] System (4) requested UDP 192.168.56.255:138
02/03/26 06:51:10 AM [ Diverter] Procmon64.exe (4836) requested UDP 192.168.56.102:53
02/03/26 06:51:10 AM [ DNS Server] Received PTR request for domain '255.56.168.192.in-addr.arpa' from Procmon64.exe (4836)
02/03/26 06:53:10 AM [ Diverter] notepad-classico.exe (3712) requested TCP 192.168.50.100:9001
02/03/26 06:59:08 AM [ Diverter] System (4) requested UDP 192.168.56.255:138
```

*Fig. 2 - Dashboard di Analisi Completa è visibile la richiesta TCP sulla porta 9001 generata dal processo ID 3712.*

### 3. Fase di Interazione con il Sistema (Host-Based Indicators)

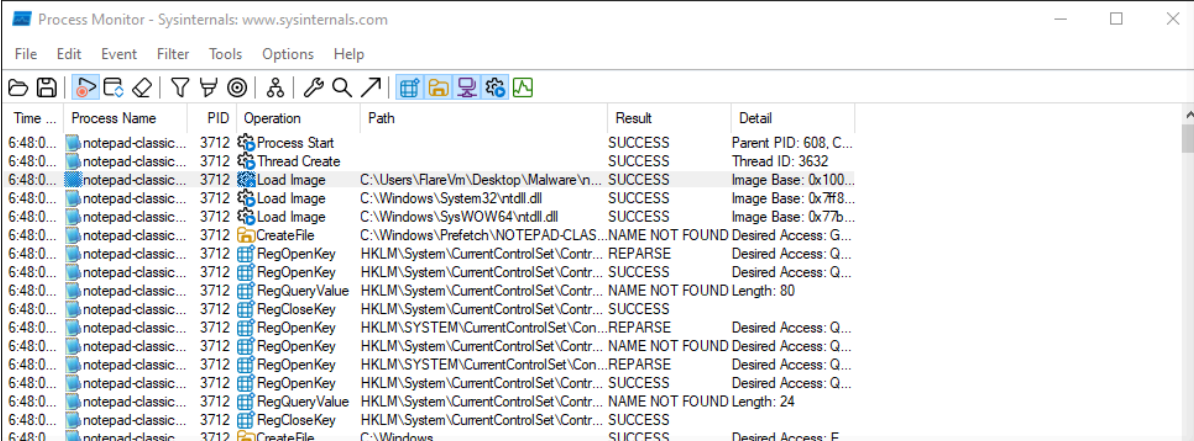
Parallelamente all'attività di rete, il malware interagisce con il sistema operativo ospite. Utilizzando **Process Monitor (Procmon)**, è stato isolato il comportamento del processo `notepad-classico.exe` (PID 3712).

Il tracciamento evidenzia numerose operazioni sul **Registro di Sistema**:

- **Operazioni:** `RegOpenKey`, `RegQueryValue`, `RegCloseKey`.
- **Target:** `HKLM\System\CurrentControlSet\...`

L'accesso ripetuto a queste chiavi suggerisce due possibili intenti:

1. **Fingerprinting:** Il malware raccoglie informazioni sulla configurazione del sistema per decidere quale payload scaricare.
2. **Persistenza:** Tenta di verificare o modificare le chiavi di avvio automatico per garantirsi l'esecuzione al prossimo riavvio.



Time ...	Process Name	PID	Operation	Path	Result	Detail
6:48:0...	notepad-classic...	3712	Process Start		SUCCESS	Parent PID: 608, C...
6:48:0...	notepad-classic...	3712	Thread Create		SUCCESS	Thread ID: 3632
6:48:0...	notepad-classic...	3712	Load Image	C:\Users\FlareVm\Desktop\Malware\...	SUCCESS	Image Base: 0x100...
6:48:0...	notepad-classic...	3712	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7f8...
6:48:0...	notepad-classic...	3712	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77b...
6:48:0...	notepad-classic...	3712	CreateFile	C:\Windows\Prefetch\NOTEPAD-CLAS...	NAME NOT FOUND	Desired Access: G...
6:48:0...	notepad-classic...	3712	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Q...
6:48:0...	notepad-classic...	3712	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
6:48:0...	notepad-classic...	3712	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
6:48:0...	notepad-classic...	3712	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
6:48:0...	notepad-classic...	3712	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
6:48:0...	notepad-classic...	3712	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Q...
6:48:0...	notepad-classic...	3712	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Q...
6:48:0...	notepad-classic...	3712	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Q...
6:48:0...	notepad-classic...	3712	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
6:48:0...	notepad-classic...	3712	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
6:48:0...	notepad-classic...	3712	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
6:48:0...	notepad-classic...	3712	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: P...

*Fig. 3 - Process Monitor evidenzia le chiamate al registro di sistema e il caricamento delle DLL da parte del malware.*

## Conclusioni sul Funzionamento

Il comportamento dinamico conferma che `notepad-classico.exe` è un **Malware Beaconing/Dropper**. Il suo ciclo di funzionamento è:

1. **Verifica:** Controlla la presenza di internet (Ping Google/Cloudflare).
2. **Attivazione:** Se online, apre un canale di comunicazione TCP sulla porta **9001** verso il server di controllo.
3. **Installazione:** Interagisce con il registro di sistema per profilare la macchina o garantirsi la persistenza.



L'attività su porta non standard (9001) e i check di connettività multipli lo classificano come una minaccia attiva progettata per esfiltrare dati o ricevere comandi remoti.