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:** Eseguibile PE a 32-bit.
- **Compilazione:** 13 Aprile 2008 (Possibile *Time Stomping* per falsificare la data).

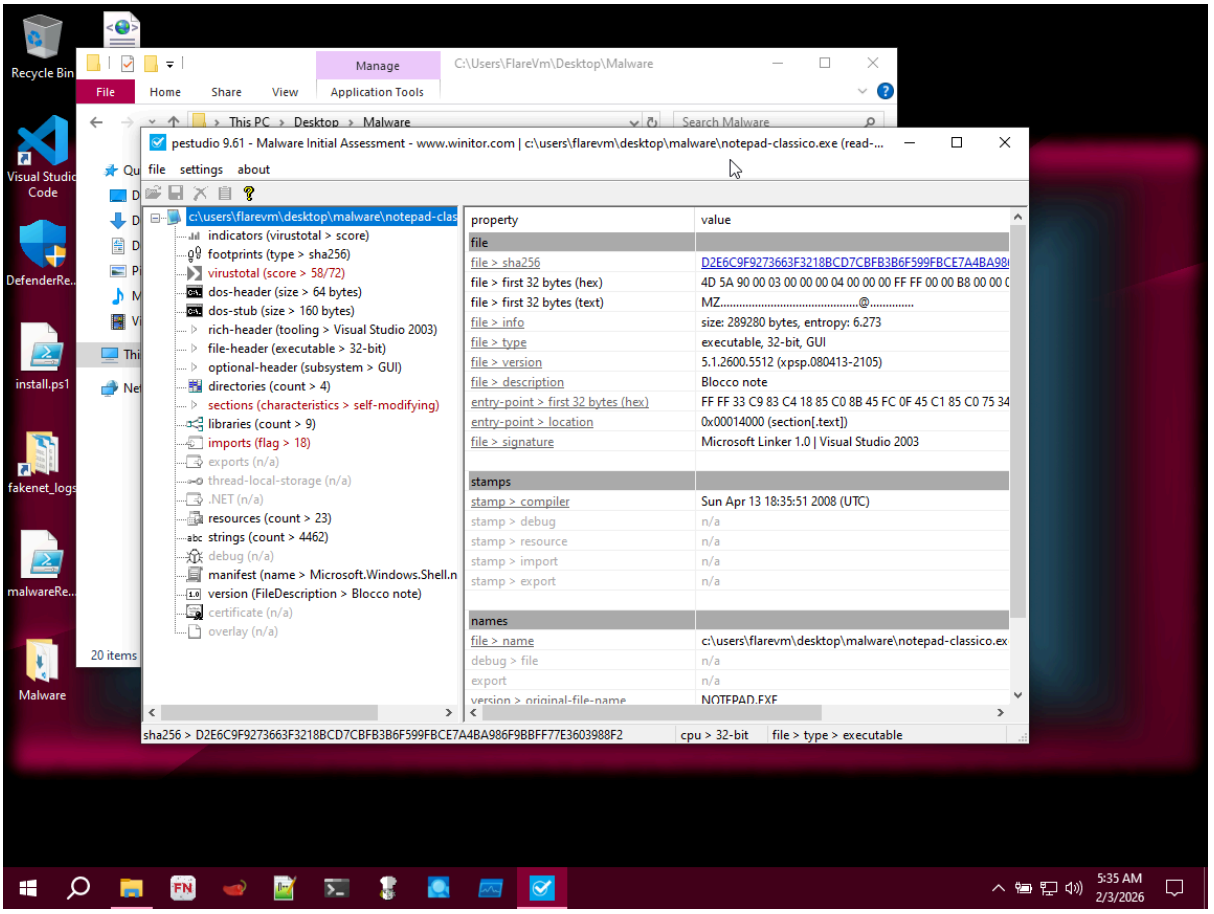


Fig. 1 - Panoramica iniziale di PEStudio che mostra il punteggio VirusTotal e l'avviso "self-modifying".

---

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

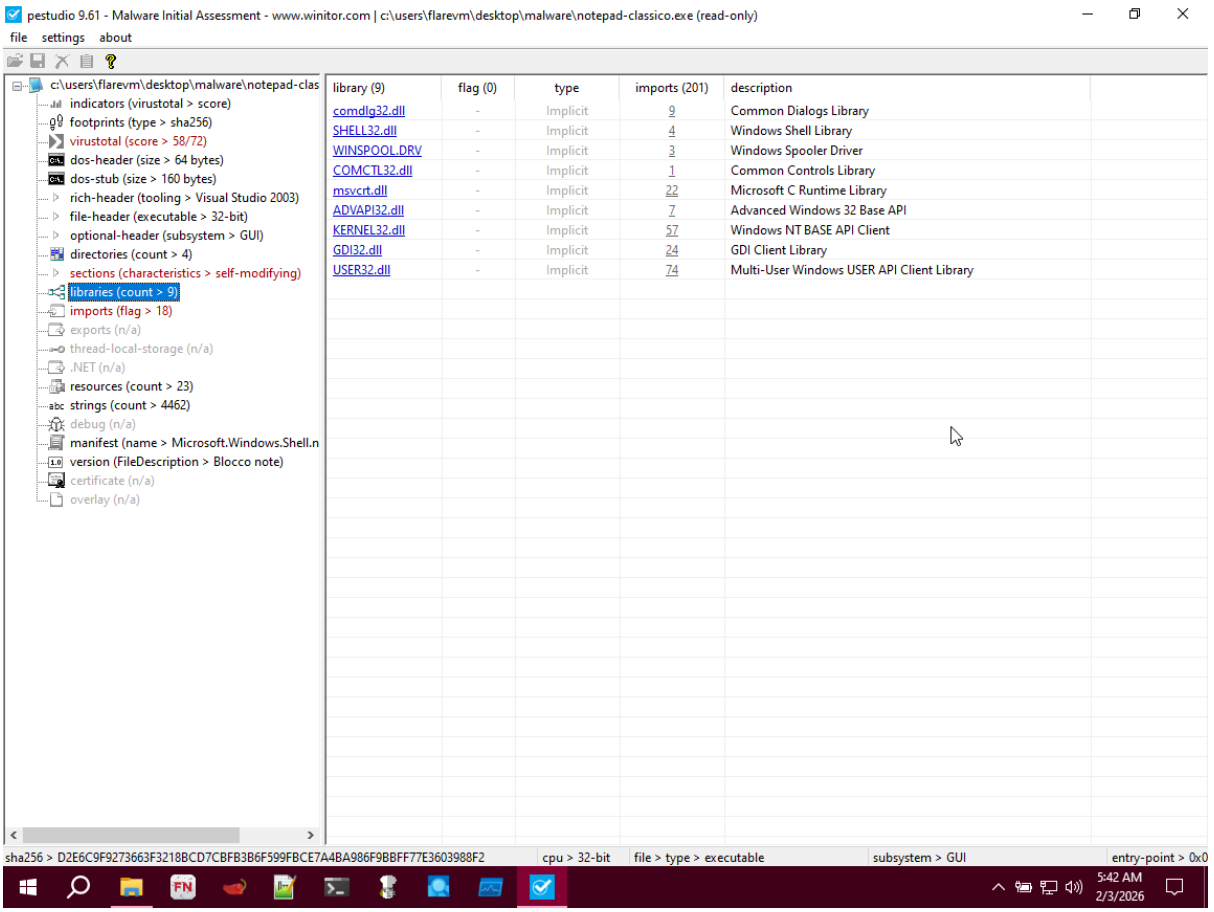
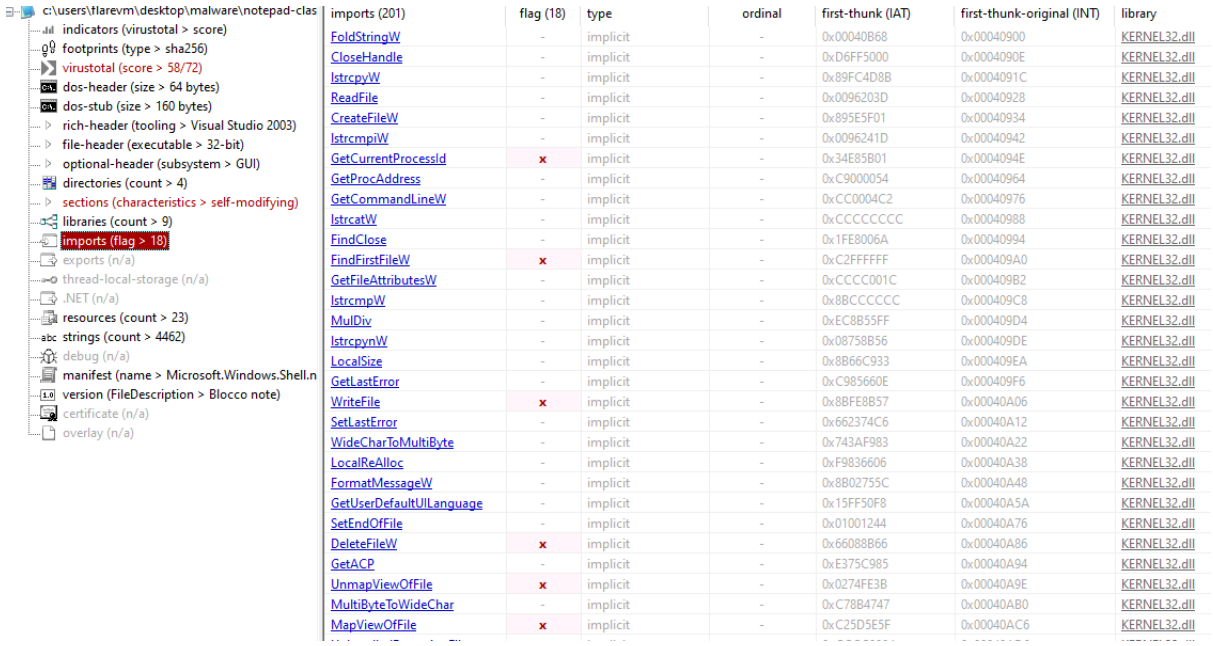


Fig. 2 - Elenco delle librerie importate visualizzate in PEStudio.

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.



imports (201)	flag (18)	type	ordinal	first-thunk (IAT)	first-thunk-original (INT)	library
FoldStringW	-	implicit	-	0x00040B68	0x00040900	KERNEL32.dll
CloseHandle	-	implicit	-	0xD6FF5000	0x0004090E	KERNEL32.dll
lstrcpyW	-	implicit	-	0x89FC4D8B	0x0004091C	KERNEL32.dll
ReadFile	-	implicit	-	0x0096203D	0x00040928	KERNEL32.dll
CreateFileW	-	implicit	-	0x895E5F01	0x00040934	KERNEL32.dll
lstrcmpiW	-	implicit	-	0x0096241D	0x00040942	KERNEL32.dll
GetCurrentProcessId	x	implicit	-	0x34E85B01	0x0004094E	KERNEL32.dll
GetProcAddress	-	implicit	-	0xC9000054	0x00040964	KERNEL32.dll
GetCommandLineW	-	implicit	-	0xCC0004C2	0x00040976	KERNEL32.dll
lstrcatW	-	implicit	-	0xCCCCCCCC	0x00040988	KERNEL32.dll
FindClose	-	implicit	-	0x1FE8006A	0x00040994	KERNEL32.dll
FindFirstFileW	x	implicit	-	0xC2FFFFFF	0x000409A0	KERNEL32.dll
GetFileAttributesW	-	implicit	-	0xCCCC001C	0x000409B2	KERNEL32.dll
lstrcmpW	-	implicit	-	0x8BCCCCCC	0x000409C8	KERNEL32.dll
MulDiv	-	implicit	-	0xEC8B55FF	0x000409D4	KERNEL32.dll
lstrcpynW	-	implicit	-	0x08758B56	0x000409DE	KERNEL32.dll
LocalSize	-	implicit	-	0x8B66C933	0x000409EA	KERNEL32.dll
GetLastError	-	implicit	-	0xC985660E	0x000409F6	KERNEL32.dll
WriteFile	x	implicit	-	0x8BFE8B57	0x00040A06	KERNEL32.dll
SetLastError	-	implicit	-	0x662374C6	0x00040A12	KERNEL32.dll
WideCharToMultiByte	-	implicit	-	0x743AF983	0x00040A22	KERNEL32.dll
LocalReAlloc	-	implicit	-	0xF9836606	0x00040A38	KERNEL32.dll
FormatMessageW	-	implicit	-	0x8B02755C	0x00040A48	KERNEL32.dll
GetUserDefaultUILanguage	-	implicit	-	0x15FF50F8	0x00040A5A	KERNEL32.dll
SetEndOfFile	-	implicit	-	0x01001244	0x00040A76	KERNEL32.dll
DeleteFileW	x	implicit	-	0x66088B66	0x00040A86	KERNEL32.dll
GetACP	-	implicit	-	0xE375C985	0x00040A94	KERNEL32.dll
UnmapViewOfFile	x	implicit	-	0x0274FE3B	0x00040A9E	KERNEL32.dll
MultiByteToWideChar	-	implicit	-	0xC78B4747	0x00040AB0	KERNEL32.dll
MapViewOfFile	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:

1. **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.
2. **Entropia Elevata:** Le sezioni di codice mostrano un'entropia superiore a 6.2, indicando che il contenuto è probabilmente compresso o cifrato ("Packed").
3. **Permessi RWX (Self-Modifying):** La Section[3] (.text) è marcata come **Self-modifying** e possiede i permessi di **Scrittura ed Esecuzione** (Write + Execute).

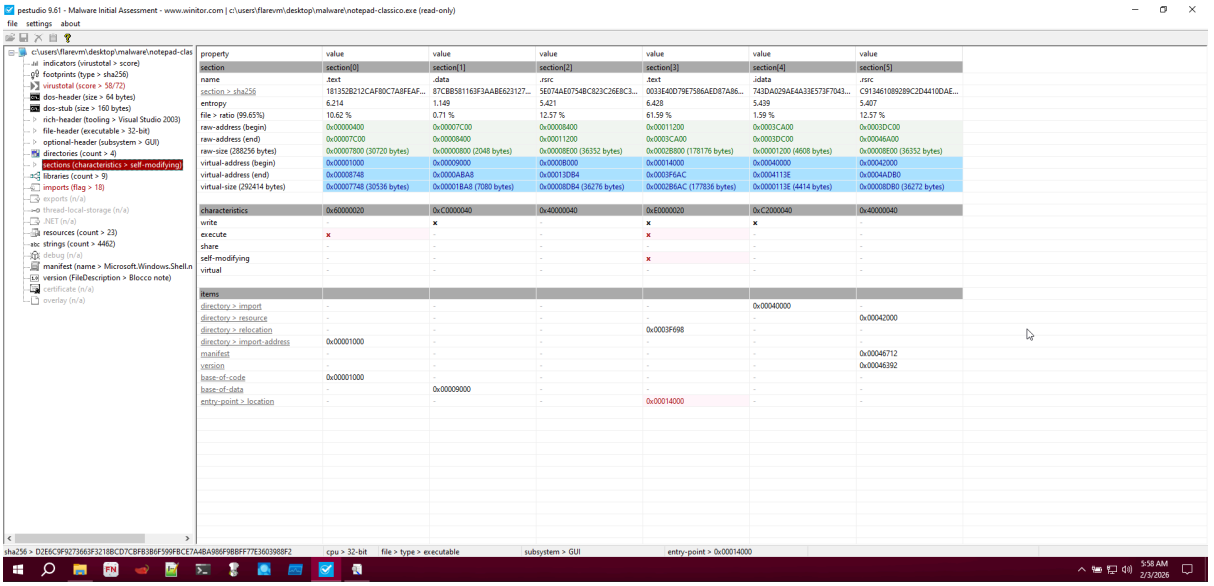


Fig. 4 - Tabella delle sezioni. Notare la sezione evidenziata con permessi di scrittura ed esecuzione e flag "self-modifying".

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	Lengtl	Info
160	278.718808	192.168.56.102	8.8.8.8	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64
161	280.737439	192.168.56.102	8.8.4.4	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64
162	282.756751	192.168.56.102	1.1.1.1	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64
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
165	288.788651	192.168.56.102	8.8.8.8	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64
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.loca
168	289.708013	192.168.56.1	224.0.0.251	MDNS	84	Standard query 0x0000 ANY Nicola._dosvc._tcp.loca
169	289.958867	192.168.56.1	224.0.0.251	MDNS	84	Standard query 0x0000 ANY Nicola._dosvc._tcp.loca
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
173	292.807862	192.168.56.102	1.1.1.1	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64
174	294.833683	192.168.56.102	1.0.0.1	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64
175	298.852745	192.168.56.102	8.8.8.8	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64
176	300.866934	192.168.56.102	8.8.4.4	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64
177	302.868357	192.168.56.102	1.1.1.1	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64
178	304.874943	192.168.56.102	1.0.0.1	ICMP	98	Echo (ping) request id=0x1739, seq=0/0, ttl=64

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.

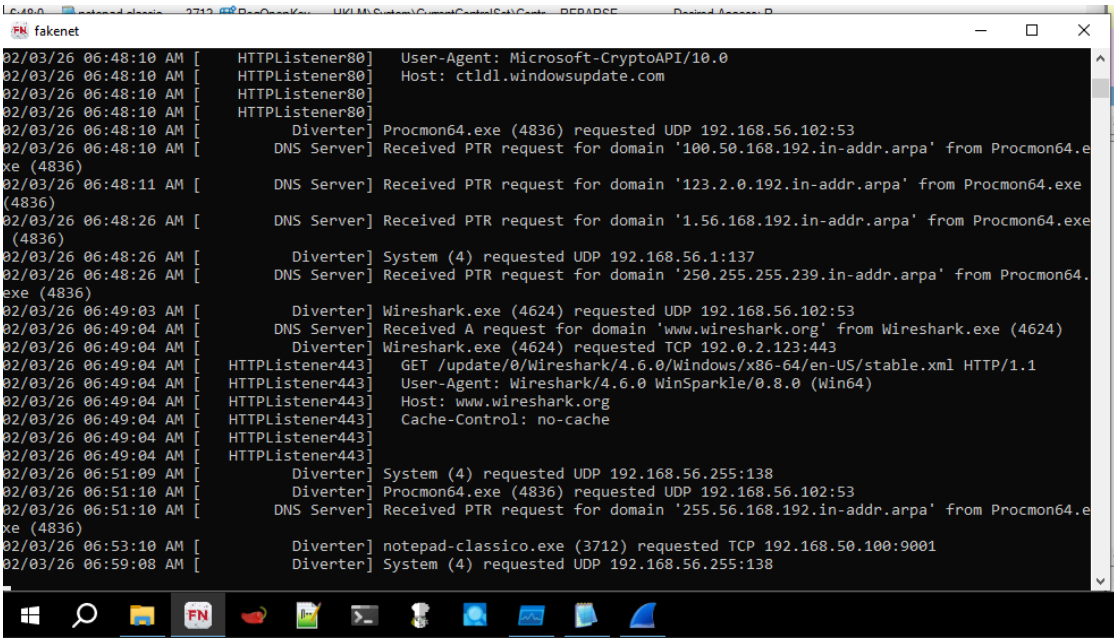


Fig. 2 - Dashboard di Analisi Completa è visibile la richiesta TCP sulla porta 9001 generata dal processo ID 3712.

---

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.

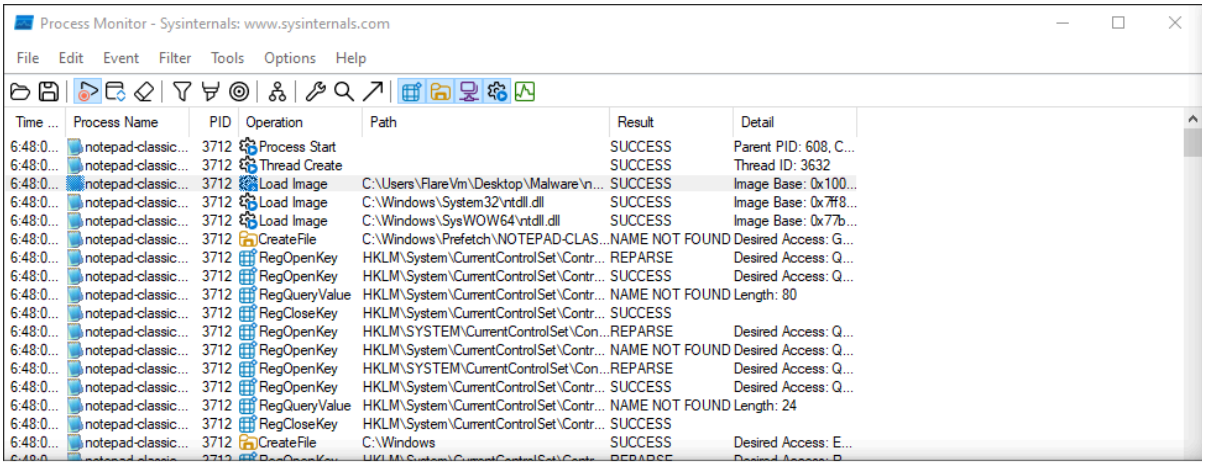


Fig. 3 - Process Monitor evidenzia le chiamate al registro di sistema e il caricamento delle DLL da parte del malware.

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.