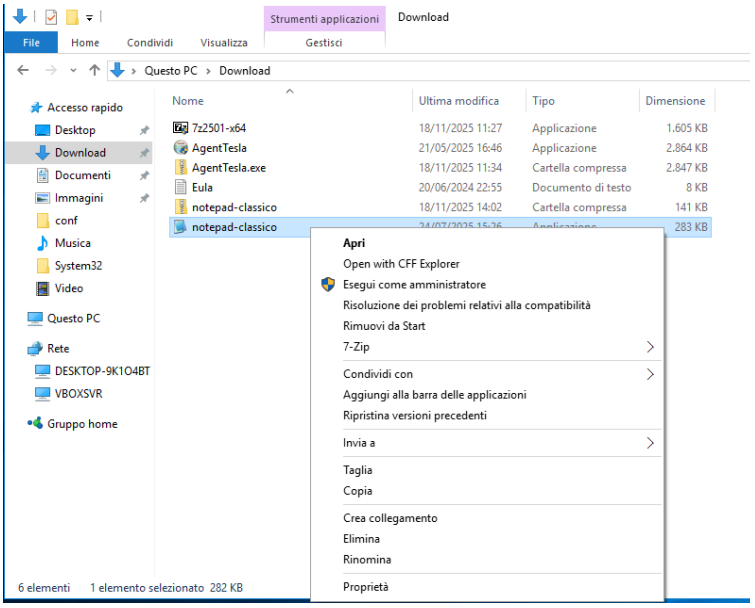
UNIT3 S9/L2 - ANALISI STATICA + DINAMICA MALWARE

Rispondere ai seguenti quesiti, con riferimento al file eseguibile notepad-classico.exe

● *Indicare le librerie importate dal malware, fornendo una descrizione per ognuna di esse tramite AI;*
● *Indicare le sezioni di cui si compone il malware, fornendo una descrizione per ognuna di essa tramite AI.*
opzionale:
● *Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte ed elaborate con AI.*
● *Analisi Dinamica: Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.*

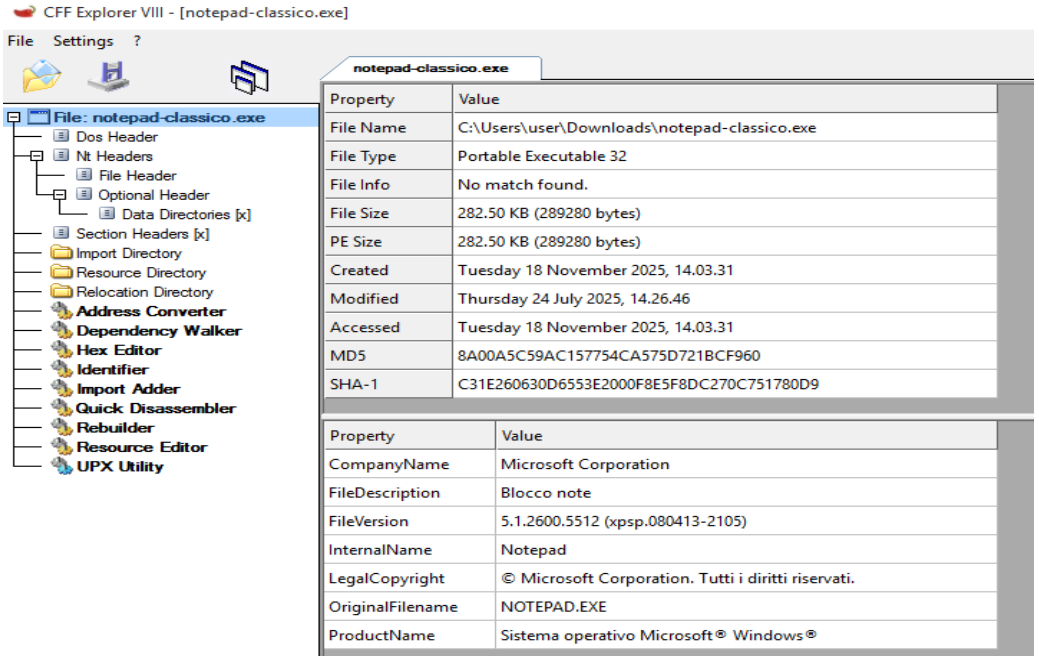
Esercizio:

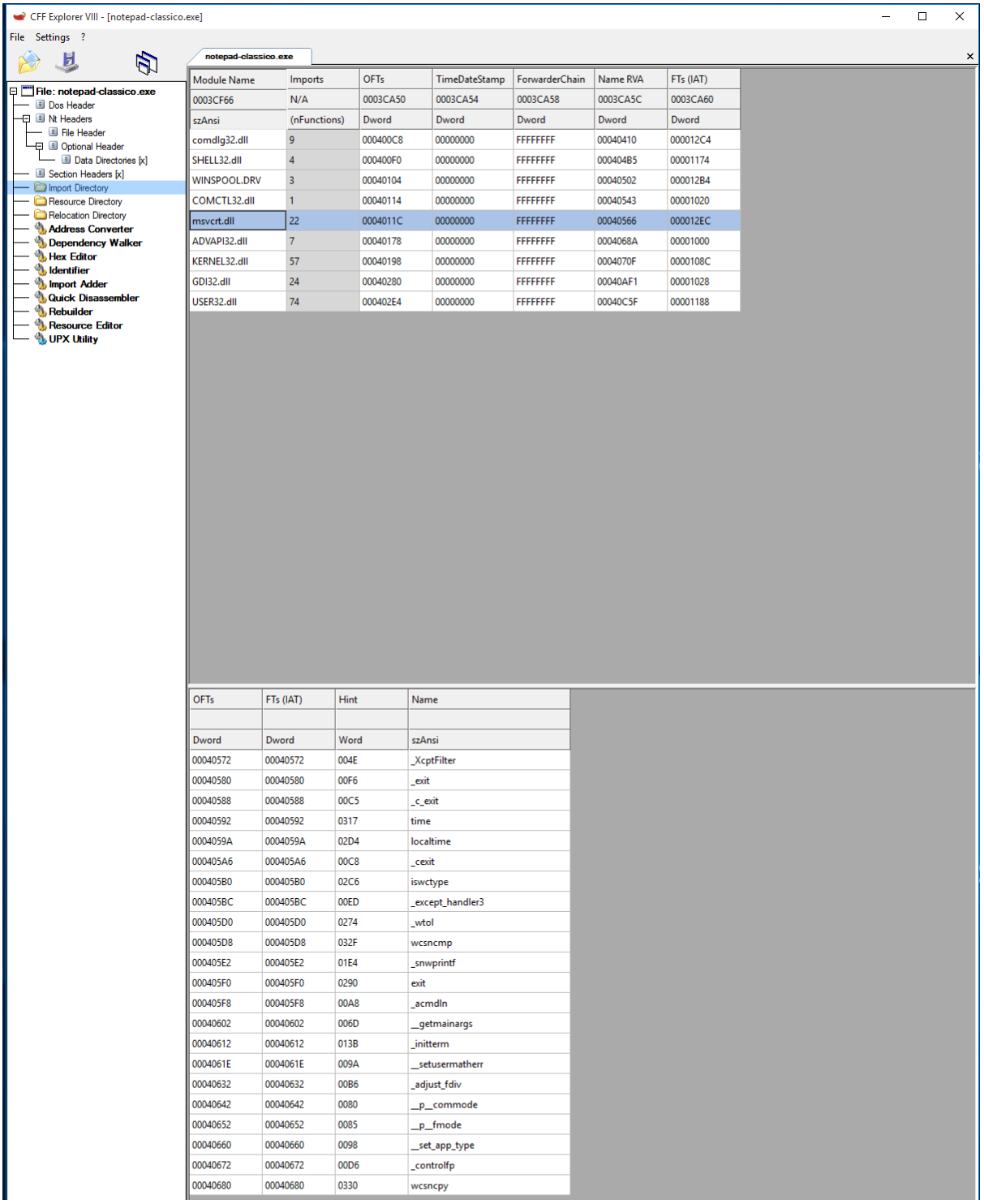
scarico il file notepad-classic.exe



Per eseguire l'analisi statica apro il programma con CFF explorer.

la pagina iniziale presentata è la seguente:





(è possibile vedere le **librerie importate** tramite “import directory”)

KERNEL32.dll

- Funzione: È la libreria centrale e più essenziale di Windows (Core Kernel).
- Ruolo: Gestisce le funzioni fondamentali del sistema operativo, come l'allocazione e gestione della memoria, la creazione e sincronizzazione di processi e thread, e l'accesso di basso livello al file system e all'hardware.
- Significato per il Malware: È richiesta per qualsiasi operazione base, dalla semplice esecuzione di codice alla manipolazione avanzata dei processi.

USER32.dll

- Funzione: Gestisce l'interfaccia utente (User Interface - UI).
- Ruolo: Fornisce le API per la creazione e la gestione di finestre, menu, cursori, icone e per l'elaborazione degli input da mouse e tastiera.
- Significato per il Malware: Utilizzata per interagire con il desktop, creare finestre nascoste o messaggi (anche per phishing), o intercettare l'input dell'utente (keylogging).

GDI32.dll

- Funzione: Gestisce le funzioni di interfaccia per dispositivi grafici (Graphics Device Interface).
- Ruolo: Contiene le API per l'output grafico, permettendo al programma di disegnare sullo schermo, stampare documenti, gestire font e manipolare grafica bidimensionale.
- Significato per il Malware: Raramente usata per la logica malevola pura, ma è necessaria se il malware deve visualizzare messaggi grafici, creare screenshot, o manipolare l'output grafico.

ADVAPI32.dll

- Funzione: Fornisce servizi di sicurezza avanzati e API di accesso al Registro.
- Ruolo: Gestisce l'accesso e la manipolazione del Registro di sistema (per la persistenza), i servizi Windows, i diritti di sicurezza (es. token) e le funzionalità di crittografia.
- Significato per il Malware: Essenziale per stabilire la persistenza (eseguirsi automaticamente all'avvio) scrivendo chiavi nel Registro, per elevare i privilegi o per utilizzare funzioni di crittografia e hashing.

SHELL32.dll

- Funzione: Gestisce le operazioni della shell di Windows.
- Ruolo: Fornisce API per interagire con l'ambiente desktop, il file system e per eseguire programmi. Funzioni comuni includono ShellExecute (per lanciare altri eseguibili), la gestione delle cartelle speciali e delle icone.
- Significato per il Malware: Usata per eseguire file, spostarsi nel file system, accedere a directory speciali o aprire URL.

---

msvcrt.dll

- Funzione: È la libreria di runtime del compilatore Microsoft Visual C++ (C RunTime Library).

- Ruolo: Implementa le funzioni standard del linguaggio C e C++, come la manipolazione delle stringhe (strcpy), le operazioni matematiche, l'input/output (printf/scanf) e la gestione della memoria dinamica (malloc/free).
- Significato per il Malware: Necessaria se il codice è stato scritto in C/C++ e utilizza funzioni standard.

COMDLG32.dll

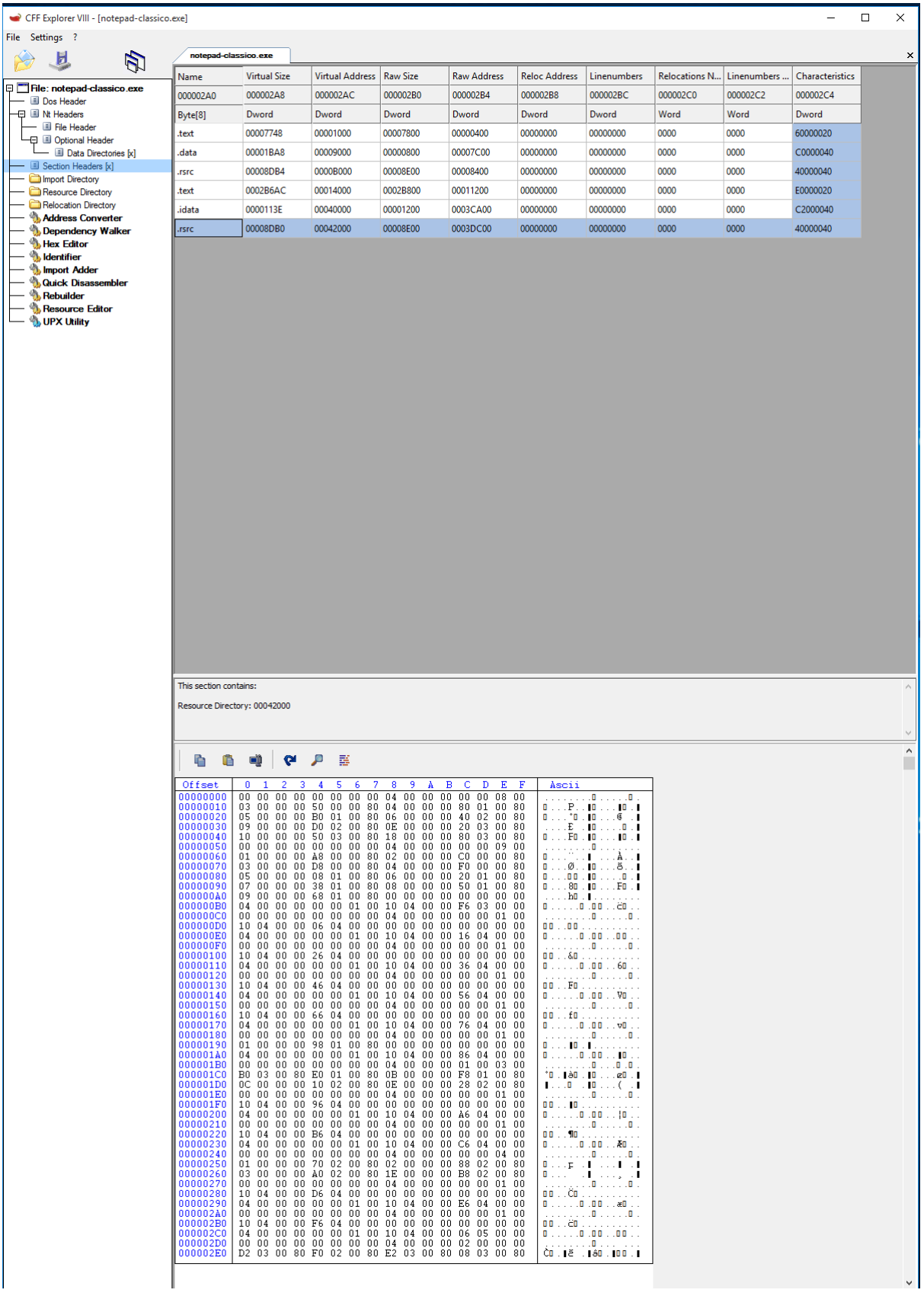
- Funzione: Gestisce le finestre di dialogo comuni (Common Dialog Boxes).
- Ruolo: Fornisce le API per visualizzare le finestre di dialogo standard di Windows, come la finestra "Apri File" (GetOpenFileName), "Salva File" o "Stampa".
- Significato per il Malware: Potrebbe essere usata per cercare file sul sistema o per ingannare l'utente visualizzando finestre familiari.

COMCTL32.dll

- Funzione: Gestisce i controlli comuni (Common Controls Library).
- Ruolo: Contiene le API per elementi di interfaccia utente più complessi e moderni, come barre di avanzamento, barre degli strumenti, schede e Tree View.
- Significato per il Malware: Necessaria se il malware ha un'interfaccia utente grafica più elaborata (sebbene molti malware siano headless e non ne abbiano bisogno).

WINSPOOL.DRV

- Funzione: Driver e libreria di gestione dello spooler di stampa.
- Ruolo: Controlla l'accesso alle funzionalità di stampa e al servizio Print Spooler.
- Significato per il Malware: I malware che importano funzioni da WINSPOOL.DRV a volte lo fanno per sfruttare vulnerabilità nel servizio di spooler di stampa (storicamente sfruttato per l'elevazione dei privilegi, come in attacchi "PrintNightmare").



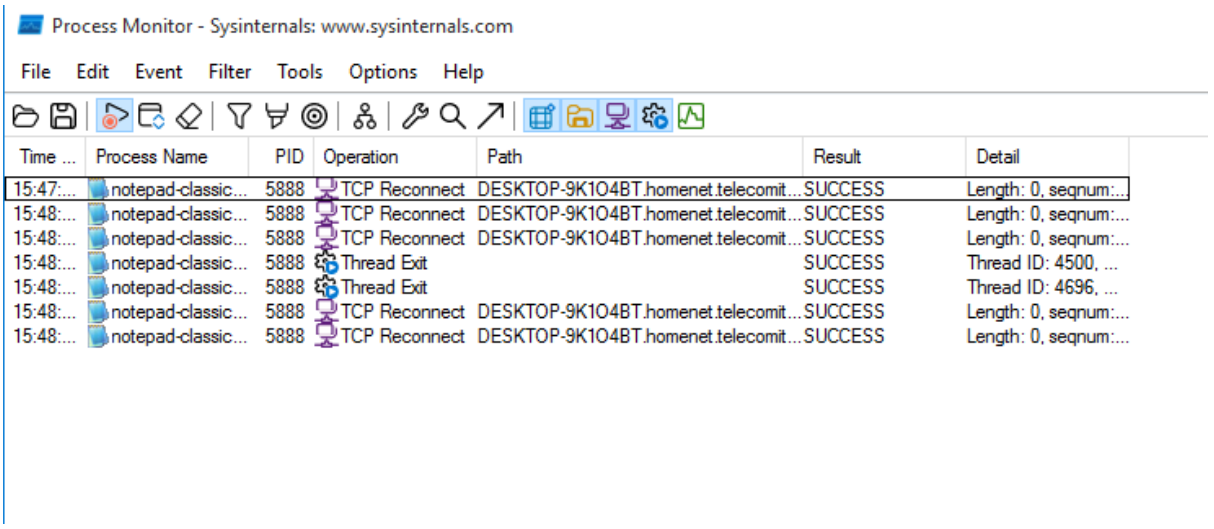
(le sezioni di cui si compone il malware è possibile trovarla sotto **sections headers**)
Si possono identificare cinque sezioni principali. Queste sezioni sono standard per i file **PE (Portable Executable)** di Windows e contengono diversi tipi di dati e codice.

1. **data**: Questa sezione contiene dati inizializzati e dati non inizializzati che il programma utilizza durante l'esecuzione. Include variabili globali o statiche che sono state inizializzate a un valore specifico nel codice sorgente. Significato in un Malware: I malware spesso usano .data per memorizzare stringhe critiche, URL di C2 (Command and Control), indirizzi IP codificati, chiavi crittografiche o configurazioni hardcoded che vengono lette all'avvio. Le caratteristiche (C0000040) indicano generalmente che la sezione è leggibile e scrivibile.
2. **rdata**: Descrizione: Questa sezione contiene dati di sola lettura (Read-only data). Include dati costanti, stringhe letterali (come i messaggi di errore), informazioni di debug o i metadati del file. Significato in un Malware: È spesso usata per memorizzare la Import Address Table (IAT), i nomi delle funzioni API importate, o stringhe costanti utilizzate dal malware. Le caratteristiche (40000040) indicano che la sezione è leggibile ma non scrivibile, rendendo i dati sicuri dalla modifica durante l'esecuzione.
3. **text**: Questa è la sezione più importante. Contiene il codice eseguibile effettivo (le istruzioni) del programma. Quando il sistema carica il file, l'esecuzione inizia tipicamente dal punto di ingresso (Entry Point) situato in questa sezione. Significato in un Malware: Contiene la logica operativa del malware: l'esecuzione delle API per iniettare codice, la crittografia dei file, la comunicazione di rete, ecc. Le caratteristiche (60000020) indicano che la sezione è leggibile ed eseguibile.
4. **idata**: Questa sezione contiene le risorse del programma, come icone, cursori, bitmap, menu, dialoghi, manifesti del programma (versioni) e stringhe di risorse non critiche. Significato in un Malware: I malware spesso usano la sezione .rsrc per nascondere dati binari importanti:
   Un payload iniettabile (come una DLL o un altro eseguibile) viene archiviato qui per essere estratto e iniettato in un altro processo.
   Chiavi crittografiche o altri dati di configurazione vengono nascosti tra i dati binari di risorse apparentemente innocue.
   L'hash dump mostrato nello screenshot in basso è proprio il contenuto della sezione .rsrc (Resource Directory), dove si notano blocchi di byte potenzialmente utili.
5. **rsrc**: Questa sezione contiene le informazioni necessarie per la rilocazione del codice e dei dati del programma. È usata quando il loader di Windows non può caricare il file all'indirizzo di memoria preferito specificato nell'intestazione PE e deve adattare gli indirizzi interni.Significato in un Malware: Il fatto che questa sezione sia presente indica che il file è un eseguibile standard. L'assenza di questa sezione in un PE non dinamico è spesso un indicatore di tecniche di anti-analisi o compattazione/packing, poiché un file con rilocazioni eliminate (strippate) è più difficile da analizzare.

Considerazioni finali:
Il file in analisi presenta le caratteristiche di un malware di tipo Remote Access Trojan (RAT) o un info-stealer, grazie alla sua capacità di eseguire logica complessa (.text), manipolare i servizi e la persistenza (ADVAPI32, KERNEL32), e potenzialmente evadere i controlli di sicurezza (ntdll.dll).

Analisi dinamica:
avviamo il “programma” e attiviamo anche procmon come strumento per l’analisi dinamica è possibile vedere una sfilza di dati.

cercando quindi filtrare solo i dati con “notepad” nel “process name” è possibile vedere come ci siano continue richieste di connessione tcp all’indirizzo IP 192.168.50.100 e una chiusura di thread



Analisi con Cuckoo: