Traccia:

Rispondere ai seguenti quesiti, con riferimento al file eseguibile:

C:\Users\user\Desktop\Malware\calcolatriceinnovativa.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.

Suggerimento: ChatGPT (o altri LLM) possono ricevere in input degli screenshot da analizzare.

Utilizzando CFF Explorer, vediamo dalla sezione import directory che il malware importa 6 librerie:

● **SHELL32.dll:** Fornisce funzioni per l'interfaccia utente di Windows e operazioni di sistema.

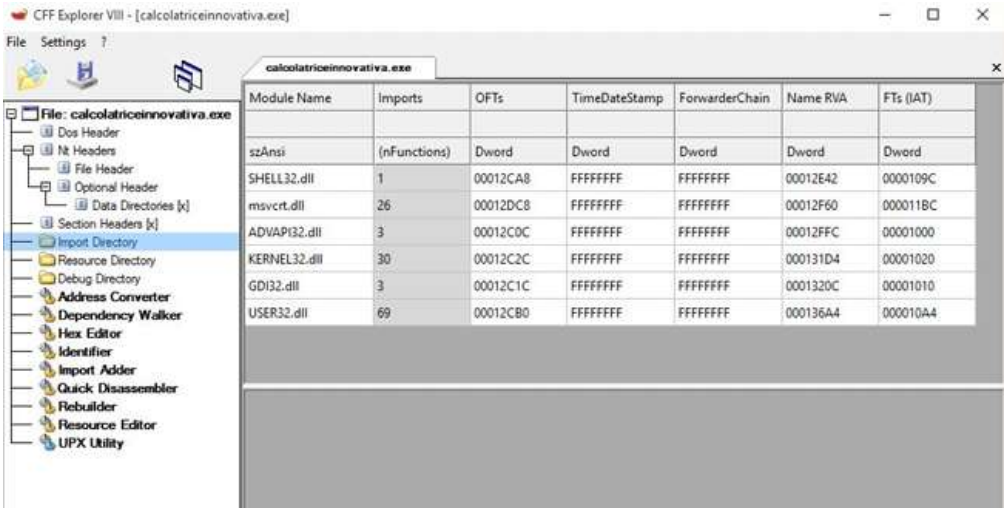
● **msvcrt.dll:** La libreria runtime di Microsoft Visual C++, che fornisce funzioni standard C.

● **ADVAPI32.dll**: Contiene funzioni per servizi, registro di sistema e gestione della sicurezza.

● **KERNEL32.dll:** Libreria core di Windows che gestisce memoria, processi e thread.

● **GDI32.dll:** Graphic Device Interface, per funzioni di disegno e grafica di base.

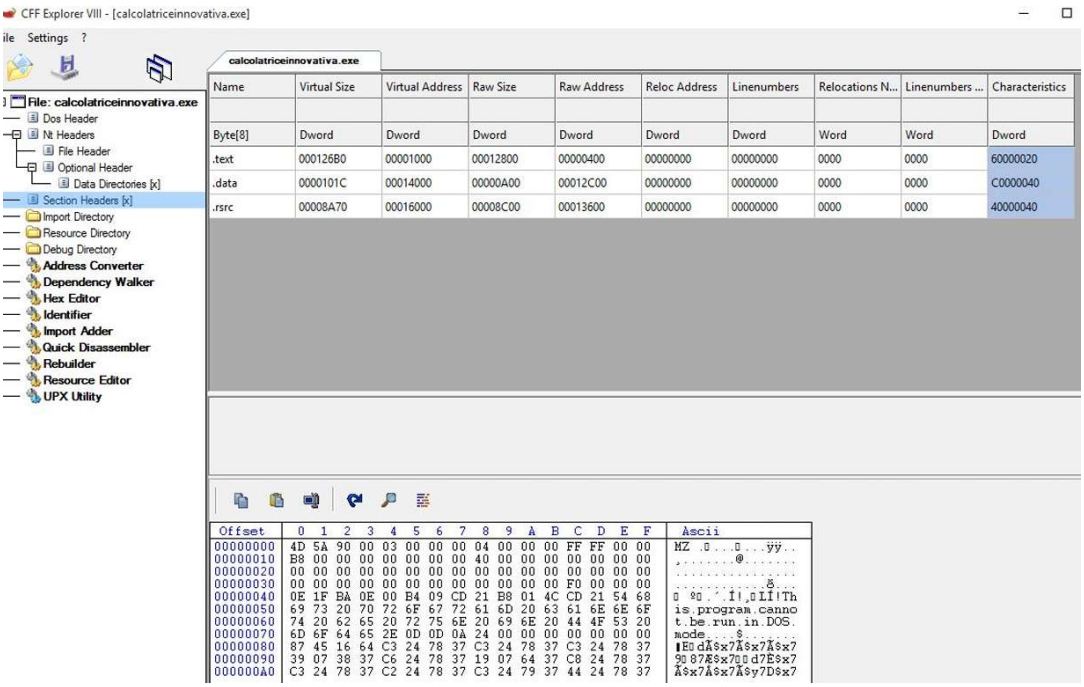
● **USER32.dll**: Gestisce l'interfaccia utente di Windows, come finestre, messaggi e controlli.



● La sezione **.text** contiene il codice eseguibile del programma.

● La sezione **.data** contiene dati inizializzati e globali.

● La sezione **.rsrc** contiene le risorse del programma come icone, menu, stringhe, ecc.



Facoltativo:

● Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte ed elaborate con AI.

● **Mascheramento**: Il malware si presenta come una calcolatrice innovativa, probabilmente per ingannare gli utenti e farli eseguire il file.

● **Tecniche di evasione:**

- Contiene codice probabilmente compresso o crittografato, indicando tentativi di offuscamento.
- La sezione .text del file PE è eseguibile e probabilmente contiene codice compresso (rapporto di compressione zlib < 0.3).
- Mostra poca attività quando eseguito, possibilmente per evitare il rilevamento.
- Potrebbe tentare di rilevare se viene eseguito in una macchina virtuale per ostacolare l'analisi.

● **Funzionalità di accesso remoto:** si rileva la presenza di funzionalità di accesso remoto.

● **Cattura di input**: Crea un oggetto DirectInput, spesso utilizzato per catturare l'input da tastiera.

● **Attività di rete:**
Comunica con l'indirizzo IP 192.168.1.80, segnalato come malevolo.

● **Tecniche MITRE ATT&CK:**

- T1027.002 e T1027: Offuscamento di file o informazioni, incluso il packing del software.
- T1056: Cattura di input.
- T1518.001: Possibile rilevamento di software di sicurezza.
- T1082: Possibile raccolta di informazioni sul sistema.

Questo malware sembra essere progettato per stabilire un accesso remoto al sistema infetto, catturare input dell'utente (possibilmente per rubare credenziali), e raccogliere informazioni sul sistema. Utilizza varie tecniche di evasione per evitare il rilevamento e l'analisi. La sua connessione con Metasploit suggerisce che potrebbe essere parte di un attacco più ampio o utilizzato come punto di ingresso per ulteriori compromissioni.