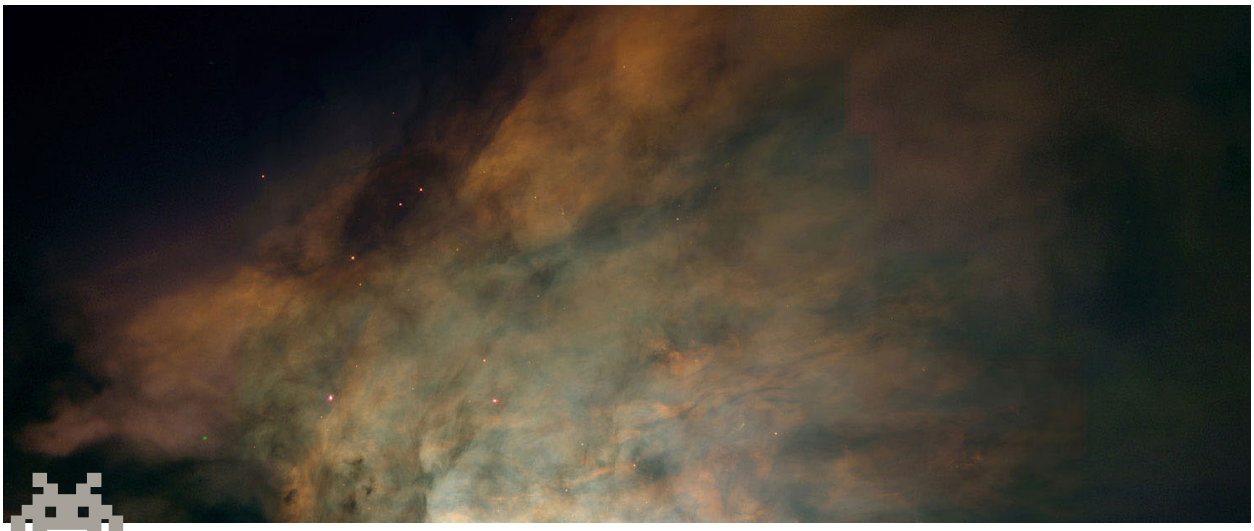
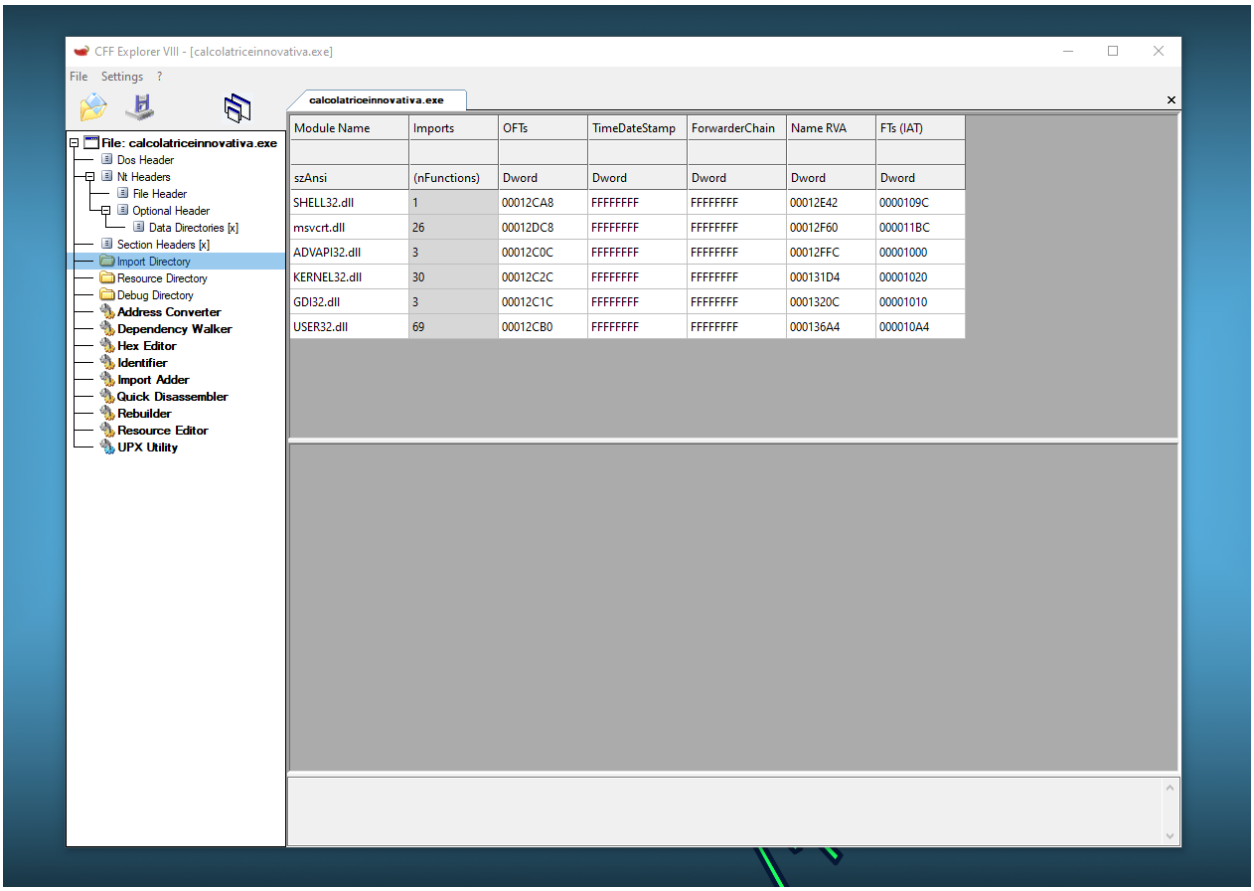


Analisi statica W22D4 CALCOLATRICE INNOVATIVA



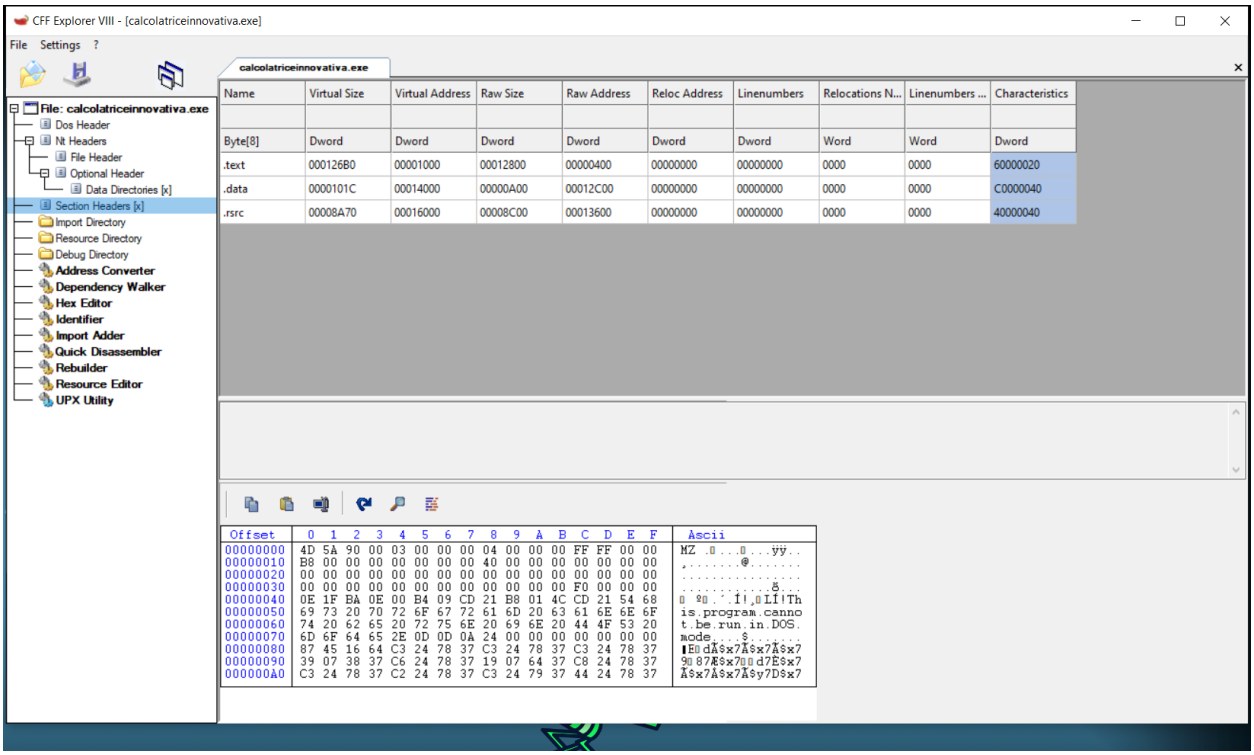
Librerie Importate

Le librerie DLL (Dynamic-Link Libraries) elencate sono quelle che il malware utilizza per le sue funzioni. Ecco una breve descrizione per ognuna di esse:

1. **SHELL32.dll**
    - Questa libreria gestisce molte funzioni di interfaccia utente di Windows, come l'apertura di finestre, la gestione dei file tramite Esplora risorse e altre operazioni legate all'ambiente grafico. Il fatto che venga importata suggerisce che il malware possa interagire con l'interfaccia di Windows o manipolare file.
2. **msvcrt.dll**
    - È la libreria del runtime del C di Microsoft. Contiene funzioni per la gestione di memoria, input/output, gestione delle stringhe e altro. Se il malware importa questa libreria, potrebbe eseguire operazioni di base

come lettura e scrittura di file, gestione della memoria o manipolazione di stringhe.

3. **ADVAPI32.dll**
    - Fornisce accesso a funzioni di Windows avanzate, come la gestione del registro di sistema, la sicurezza e la gestione dei servizi. Il malware potrebbe usare questa libreria per modificare chiavi di registro, gestire servizi di Windows o eseguire altre operazioni amministrative.
4. **KERNEL32.dll**
    - Questa libreria è fondamentale per la gestione di operazioni di base come input/output, gestione della memoria, thread e gestione dei processi. Se importata dal malware, indica che eseguirà operazioni a basso livello, come la creazione o modifica di file, l'esecuzione di processi o la gestione della memoria.
5. **GDI32.dll**
    - Questa libreria fornisce funzioni per la grafica e l'output visivo in Windows. Il malware potrebbe usare GDI32 per creare, manipolare o mostrare elementi grafici, suggerendo una possibile componente visiva o manipolazione grafica.
6. **USER32.dll**
    - Contiene funzioni legate alla gestione dell'interfaccia utente di Windows, come la gestione di finestre, messaggi, menu e altre interazioni con l'utente. Il malware potrebbe interagire con l'utente attraverso finestre o messaggi pop-up.



Sezioni del Malware

1. **.text**
    - **Descrizione**: Questa sezione contiene il codice eseguibile del malware. La sua dimensione virtuale è di 0x12680, il che indica che il codice vero e proprio occupa un discreto spazio in memoria. Il malware viene eseguito tramite le istruzioni contenute in questa sezione, e quindi è fondamentale analizzare il comportamento che implementa. In questa sezione si trovano spesso chiamate a funzioni di sistema o librerie esterne come quelle importate (es. `SHELL32.dll`, `msvcrt.dll`).
2. **.data**
    - **Descrizione**: Questa sezione contiene dati globali, come variabili inizializzate e non inizializzate che il malware utilizza durante l'esecuzione. La dimensione virtuale di questa sezione è 0x14000, e la sua dimensione fisica (Raw Size) è 0xA00. Questo spazio viene riservato per la gestione di dati che il malware utilizza in fase di esecuzione, come puntatori, strutture o buffer.
3. **.rsrc**

- **Descrizione**: La sezione delle risorse (`.rsrc`) contiene dati statici non eseguibili come icone, immagini, stringhe, e altre risorse necessarie per l'interfaccia grafica o altre funzionalità. Qui, il malware potrebbe nascondere anche elementi malevoli, come payload aggiuntivi. La dimensione virtuale di questa sezione è 0x7800 e la sua dimensione fisica è 0x8C00. Spesso questa sezione viene esaminata per rilevare eventuali payload criptati o offuscati.

Conclusione

L'analisi delle sezioni del malware rivela che:

- **La sezione** `.text` contiene il codice vero e proprio del malware, che rappresenta il core delle operazioni malevole.
- **La sezione** `.data` gestisce i dati necessari durante l'esecuzione.
- **La sezione** `.rsrc` potrebbe contenere risorse o anche dati nascosti come payload o comandi che vengono eseguiti a runtime.

Questo tipo di strutturazione è comune nei malware, e ogni sezione ha il suo ruolo nel completare le funzionalità malevole. Per un'analisi più approfondita, bisognerebbe eseguire un disassemblaggio o un'analisi dinamica del file.