Librerie Importate

L'immagine mostra una schermata di CFF Explorer aperta su un file eseguibile ("calcolatriceinnovativa.exe") e, nello specifico, nella sezione "Import Directory". Qui possiamo vedere le librerie (DLL) importate dal malware e il numero di funzioni importate da ciascuna di esse. Le librerie importate e il numero di funzioni per ciascuna sono le seguenti:

1. **SHELL32.dll** - 1 funzione importata.
2. **msvcrt.dll** - 26 funzioni importate.
3. **ADVAPI32.dll** - 3 funzioni importate.
4. **KERNEL32.dll** - 30 funzioni importate.
5. **GDI32.dll** - 3 funzioni importate.
6. **USER32.dll** - 69 funzioni importate.

Queste librerie sono comunemente usate nei programmi Windows per diverse operazioni di sistema:

- **SHELL32.dll**: contiene funzioni per interfacciarsi con il file system e la shell di Windows.
- **msvcrt.dll**: è la libreria di runtime C di Microsoft e include funzioni di base per la gestione della memoria, stringhe, input/output e altro.
- **ADVAPI32.dll**: fornisce accesso a funzioni avanzate di Windows, come la gestione dei registri e la sicurezza.
- **KERNEL32.dll**: include funzioni di gestione di memoria, processi e thread, manipolazione di file e gestione del sistema.
- **GDI32.dll**: contiene funzioni grafiche per gestire e rappresentare immagini e testo.
- **USER32.dll**: fornisce funzioni per la gestione dell'interfaccia utente, come finestre, input dell'utente e messaggi di sistema.

L'uso di queste librerie è abbastanza tipico, ma il numero di funzioni importate, specialmente da **KERNEL32.dll** e **USER32.dll**, potrebbe indicare operazioni avanzate di sistema o interazioni con l'utente, che sono comuni nei malware per eseguire azioni specifiche sul sistema operativo.

Selezioni di cui si compone il Malware

L'immagine mostra la schermata di CFF Explorer nella sezione "Section Headers" del file eseguibile "calcolatriceinnovativa.exe". Questa sezione fornisce informazioni sulle diverse sezioni di cui si compone il file eseguibile. Ecco i dettagli delle sezioni elencate:

1. .text:
    - Virtual Size: `0x126B0` (75,184 bytes)
    - Virtual Address: `0x1000`
    - Raw Size: `0x12800` (75,776 bytes)
    - Raw Address: `0x400`

    - Descrizione: La sezione `.text` contiene il codice eseguibile del programma, ovvero le istruzioni che verranno eseguite dal processore. È la sezione principale per il codice del malware.
2. .data:
    - Virtual Size: `0x101C` (4,124 bytes)
    - Virtual Address: `0x14000`
    - Raw Size: `0xA00` (2,560 bytes)
    - Raw Address: `0x12C00`
    - Descrizione: La sezione `.data` contiene i dati inizializzati, ovvero variabili e strutture dati che il programma utilizza e che hanno un valore predefinito.
3. .rsrc:
    - Virtual Size: `0x8A70` (35,504 bytes)
    - Virtual Address: `0x16000`
    - Raw Size: `0x8C00` (35,840 bytes)
    - Raw Address: `0x13600`
    - Descrizione: La sezione `.rsrc` contiene le risorse del file, come icone, stringhe, immagini o altre informazioni che possono essere utilizzate dal programma. Nei malware, questa sezione può contenere anche dati crittografati o file di configurazione nascosti.

Riepilogo

Queste sezioni rappresentano la struttura base di molti file eseguibili Windows. La presenza delle sezioni `.text`, `.data`, e `.rsrc` è comune in molti programmi, ma il malware potrebbe sfruttare queste sezioni per contenere codice malevolo, dati crittografati o altri elementi utilizzati per compromettere il sistema ospitante.