Calcolatrice Innovativa

Utilizziamo Cff Explorer per capire bene la struttura del malware e le sue finalità. Andando sulla voce Resource Directory troviamo una sezione dei file PE che contiene risorse utilizzabili dal programma e troviamo: Icons: Il malware utilizza icone grafiche per rappresentare visivamnete il file eseguibile.

- **Menus:** Menù che possono essere utilizzati per costruire l'interfaccia grafica dell'applicazione, suggerisce che il file potrebbe avere un'interfaccia utente.
- **Dialogs:** Finestre di dialogo per interagire con l'utente.
- **String Tables:** Tabelle di stringhe che includono testo visibile nel programma, come messaggi d'errore o descrizioni.
- **Accelerators:** Tabelle di scorciatoie da tastiera che permettono di attivare funzioni specifiche.
- **Icon Groups:** Gruppi di icone utilizzati per rappresentare il programma in varie dimensioni
- **Version Info:** Informazioni sulla versione del file, che spesso includono nome dell'azienda, descrizione del prodotto, ecc. I malware a volte falsificano queste informazioni per sembrare legittimi.
- **Configuration FIles**: File di configurazione, spesso usati per salvare parametri o dettagli di esecuzione.

Si può pensare che le sue potenziali finalità sono mascherarsi come applicazione legittima usando risorse come icone o finestre di dialogo per sembrare un'applicazione normale, interagire con l'utente attraverso finestre o messaggi ingannandolo a fornire informazioni sensibili e nascondere payload. Utilizzando il software Cuckoo riusciamo a capire meglio che danni reca al nostro computer:

a. Modifica il registro del sistema alterando configurazioni critiche di Windows per persistere o danneggiare il sistema.
b. Utilizza la memoria RWX, ciò indica che il malware cerca di offuscare il suo funzionamento.
c. Ha un collegamento con la rete per comunicare con un server remoto avendo la possibilità di scaricare comandi o inviare dati esfiltrati.