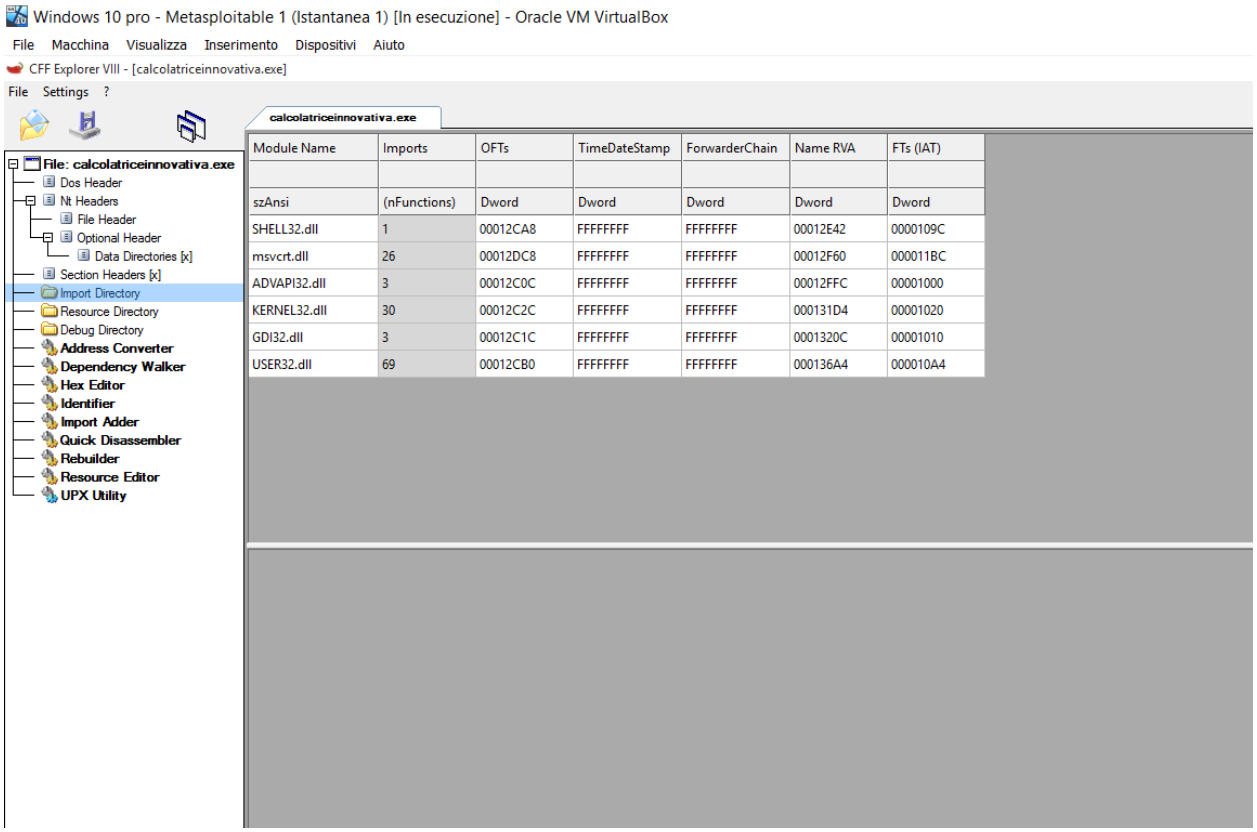
\calcolatriceinnovativa.exe - Descrizione librerie importate dal malware

Dump della tabella delle importazioni del malware denominato calcolatriceinnovativa.exe, visualizzato tramite CFF Explorer



Questa sezione del Portable Executable (PE) file contiene informazioni sulle librerie esterne (DLL) e sulle funzioni che il malware richiama per eseguire le sue operazioni.
Descrizione singole librerie importate con supporto AI:

1. SHELL32.dll

Descrizione: Questa libreria è una componente critica del sistema operativo Windows e fornisce API per interagire con la shell di Windows (ad esempio, per eseguire comandi di sistema, lavorare con file e directory, e gestire l'ambiente desktop).

Funzione Importata (1 funzione):
Il malware utilizza una funzione da questa DLL, che può essere legata a operazioni di file system, come aprire/eseguire file o manipolare cartelle.

2. msvcrt.dll

Descrizione: Questa libreria fornisce le funzionalità del runtime C di Microsoft, necessarie per l'esecuzione di applicazioni scritte in C/C++. Include funzioni per la gestione della memoria, input/output, stringhe, matematica, e altro.

Funzioni Importate (26 funzioni):
L'uso intensivo di msvcrt.dll indica che il malware potrebbe fare largo uso di funzioni standard del C/C++, come gestione di buffer, manipolazione di stringhe o operazioni matematiche, cruciali per le sue operazioni di base.

3. ADVAPI32.dll

Descrizione: Questa libreria fornisce accesso a numerosi servizi di sistema, come la gestione delle chiavi di registro di Windows, servizi di sicurezza, gestione delle sessioni e controllo degli account utente.

Funzioni Importate (3 funzioni):
L'importazione di funzioni da ADVAPI32.dll può indicare che il malware modifica impostazioni di sistema o di registro, o interagisce con i privilegi di sicurezza per eseguire operazioni privilegiate o nascondere la sua presenza.

4. KERNEL32.dll

Descrizione: Kernel32.dll è uno dei componenti principali di Windows, fornendo un'ampia gamma di funzioni di base per la gestione della memoria, dei thread, e delle operazioni di input/output.

Funzioni Importate (30 funzioni):
Il grande numero di funzioni importate da Kernel32.dll suggerisce che il malware fa ampio uso di funzionalità di basso livello del sistema operativo, come la creazione di nuovi processi, la manipolazione di file, la gestione di memoria e la gestione dei thread. Queste funzioni sono spesso cruciali per la persistenza e l'esecuzione di codice malevolo.

5. GDI32.dll

Descrizione: Questa libreria contiene le funzioni grafiche di Windows, usate per disegnare grafici e testi sullo schermo. È usata per manipolare oggetti grafici e interagire con i dispositivi di output (come lo schermo).

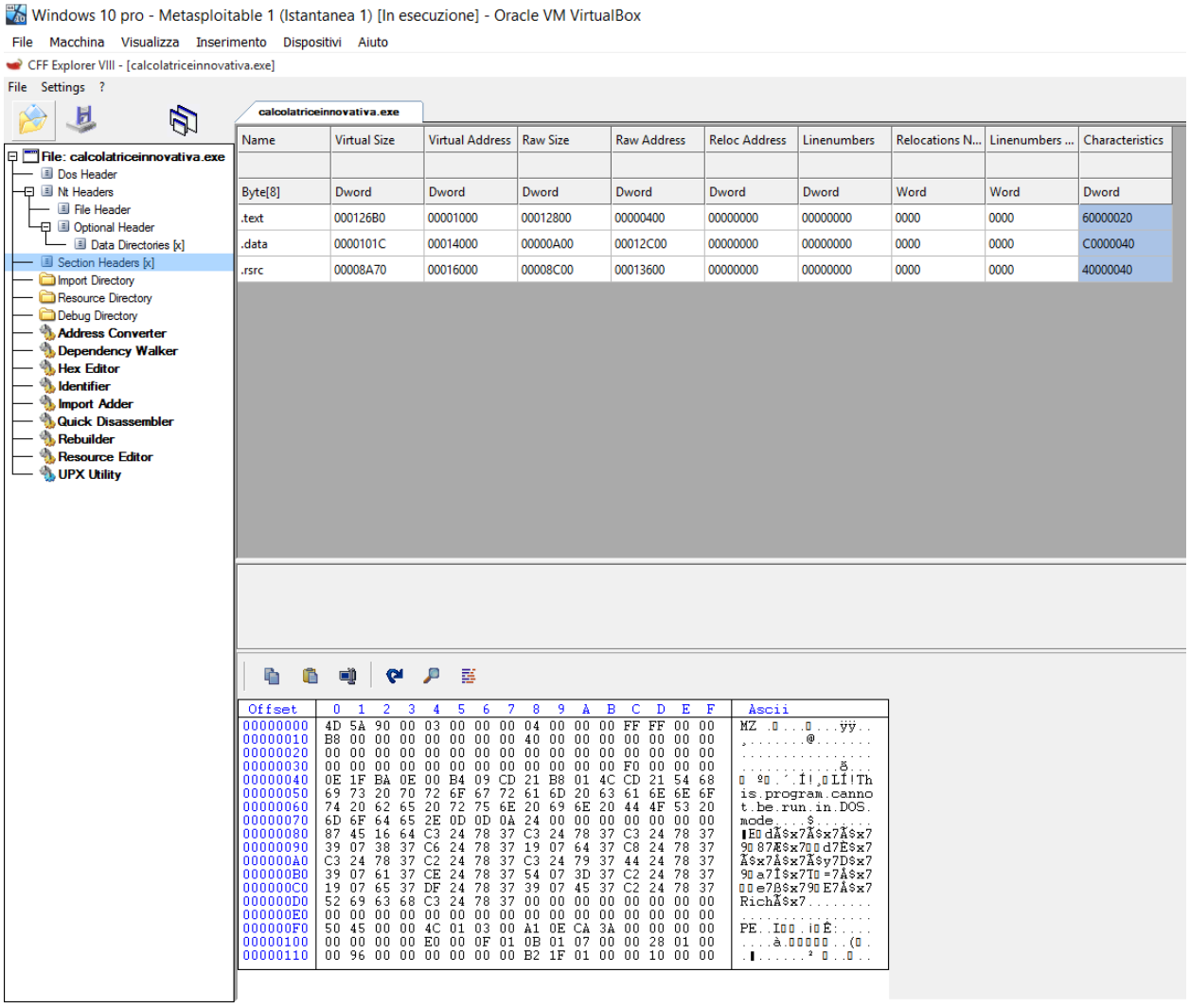
Funzioni Importate (3 funzioni):
Anche se meno comune nei malware standard, l'importazione di GDI32.dll suggerisce che il malware potrebbe avere una componente grafica o manipolare elementi visivi, magari per visualizzare interfacce false o nascondere la sua presenza con elementi visivi.

6. USER32.dll

Descrizione: Questa libreria gestisce la maggior parte delle funzionalità relative all'interfaccia utente in Windows. Fornisce funzioni per la gestione di finestre, messaggi, tastiere, mouse e altro.

Funzioni Importate (69 funzioni):
Il malware importa un numero significativo di funzioni da USER32.dll, indicando che interagisce pesantemente con l'interfaccia utente di Windows. Questo potrebbe significare che simula interazioni utente, come clic di mouse o pressioni di tasti, o crea finestre fittizie per ingannare l'utente e nascondere le sue attività.

\calcolatriceinnovativa.exe - Descrizione sezioni del malware



1. Sezione .text

- **Virtual Size**: 0x12680 (75,776 bytes)
- **Virtual Address**: 0x1000
- **Raw Size**: 0x12800 (75,776 bytes)
- **Raw Address**: 0x400
- **Characteristics**: 0x60000020 (Memoria eseguibile, in sola lettura)

Descrizione:

La sezione **.text** è probabilmente la più critica nel contesto di un malware, poiché contiene il codice eseguibile vero e proprio. In questa sezione risiedono tutte le istruzioni che verranno

eseguite quando il file viene caricato in memoria. Il codice malevolo che compie le azioni distruttive o nascoste si trova solitamente qui.

Funzioni comuni nel malware:

- **Iniezione di codice**: Tecniche di evasione come l'iniezione di codice in processi legittimi possono essere ospitate in questa sezione.
- **Persistenza**: Il codice che stabilisce la persistenza del malware nel sistema, per esempio modificando chiavi di registro o installando servizi, viene eseguito da qui.
- **Payload principale**: L'esecuzione del payload malevolo che potrebbe includere attività come furto di dati, esfiltrazione, o download di altri malware.

Il valore 0x60000020 delle caratteristiche indica che questa sezione è **eseguibile** e in **sola lettura**, che è tipico per una sezione di codice.

Qui si trovano le istruzioni assembly che eseguono il comportamento del malware, incluse potenziali routine per comunicare con un server remoto o attivare funzionalità malevole.

Possibile Tecniche di MITRE ATT&CK:

- **T1105** (Data Staged): Potrebbe caricare dati da o verso un server C2 (Command and Control).
- **T1041** (Exfiltration Over C2 Channel): Il codice potrebbe includere routine per comunicazioni di rete con server esterni per il furto di informazioni.

2. Sezione .data

- **Virtual Size**: 0x400 (1,024 bytes)
- **Virtual Address**: 0x14000
- **Raw Size**: 0x400 (1,024 bytes)
- **Raw Address**: 0x12C00
- **Characteristics**: 0xC0000040 (Memoria leggibile e scrivibile)

Descrizione:

La sezione **.data** è utilizzata per memorizzare **dati variabili inizializzati**. Nel contesto di un malware, questa sezione può essere utilizzata per memorizzare una serie di informazioni essenziali per il funzionamento del programma.

Possibili utilizzi del malware:

- **Configurazioni e informazioni statiche**: Dati di configurazione del malware, come indirizzi IP di comando e controllo (C2), chiavi crittografiche, o variabili che definiscono il comportamento del malware.
- **Buffer e variabili globali:** Se il malware esegue manipolazioni di memoria o gestisce flussi di dati, potrebbe usare questa sezione per allocare buffer temporanei o globali.

Le caratteristiche di questa sezione (0xC0000040) indicano che è **leggibile** e **scrivibile**, una proprietà che la rende idonea per la memorizzazione di variabili e dati utilizzati durante l'esecuzione del programma.

Non è tipicamente una sezione critica per il codice eseguibile, ma può includere dati importanti per la configurazione della comunicazione di rete o per l'inizializzazione del malware.

Potenziale Tecniche MITRE ATT&CK:

- **T1071.001** (Application Layer Protocol): Potrebbe memorizzare configurazioni di comunicazione via HTTP/HTTPS per interagire con C2.

3. Sezione .rsrc

- **Virtual Size:** 0xA700 (42,240 bytes)
- **Virtual Address:** 0x16000
- **Raw Size:** 0x13600 (79,872 bytes)
- **Raw Address:** 0x13000
- **Characteristics:** 0x40000040 (Memoria leggibile)

Descrizione:

La sezione **.rsrc** è utilizzata per contenere le **risorse** del programma. Queste possono includere icone, immagini, stringhe, informazioni della GUI, e altre risorse utilizzate dall'applicazione. Nei malware, questa sezione può essere utilizzata in modi particolari.

Funzioni comuni nel malware:

- **Payload nascosto**: Molti malware nascondono file eseguibili aggiuntivi, shellcode, o altri tipi di payload malevolo nella sezione .rsrc, spesso crittografati o offuscati, che vengono poi estratti ed eseguiti in un secondo momento.
- **Certificati fasulli**: Alcuni malware utilizzano questa sezione per includere certificati digitali fasulli, al fine di apparire legittimi.
- **File aggiuntivi**: Potrebbero essere presenti file di configurazione, stringhe per visualizzare messaggi di errore finti, o altri dati utili durante l'attacco.

Le caratteristiche di questa sezione (0x40000040) indicano che è **leggibile**, e non eseguibile o scrivibile, tipico per una sezione che contiene risorse statiche.

In alcuni casi, questa sezione può nascondere file binari aggiuntivi o oggetti utilizzati dal malware.

Possibili Tecniche di MITRE ATT&CK:

- **T1027** (Obfuscated Files or Information): Potrebbe contenere dati cifrati o compressi per nascondere il reale payload del malware o le informazioni di configurazione.

Interpretazione Tecnica delle Sezioni:

1. **.text** – È la sezione chiave, contenente il codice eseguibile malevolo. Da qui viene eseguito tutto il codice necessario per compromettere il sistema bersaglio, inclusi payload per furto di informazioni o esecuzione di codice dannoso.
2. **.data** – Questa sezione viene utilizzata per gestire dati dinamici. Può contenere variabili e buffer necessari per le operazioni runtime del malware, come la gestione di configurazioni o di dati temporanei.
3. **.rsrc** – È una sezione spesso sfruttata dai malware per nascondere componenti aggiuntivi o file malevoli crittografati, pronti per essere decriptati ed eseguiti quando necessario.

In base alle informazioni raccolte dall'analisi delle sezioni e delle librerie importate dal malware calcolatriceinnovativa.exe, possiamo concludere che si tratta di un malware potenzialmente sofisticato, costruito con cura per eseguire azioni malevole in maniera furtiva e resiliente.

Considerazioni Finali:

- **Importazioni Critiche:** Il malware si affida a diverse librerie di sistema fondamentali, come **KERNEL32.dll** e **USER32.dll**, che forniscono funzioni essenziali per la manipolazione del file system, della memoria e delle interfacce grafiche. L'uso di queste librerie indica che il malware potrebbe interagire direttamente con il sistema operativo, manipolando risorse cruciali, come file o processi di sistema, o persino iniettando codice in applicazioni legittime per nascondersi.
- **Potenziale Persistenza:** L'inclusione di librerie come **ADVAPI32.dll** suggerisce che il malware potrebbe avere capacità di interagire con il Registro di sistema, possibilmente per stabilire persistenza, alterando chiavi di avvio automatico o modificando configurazioni di sicurezza per garantire che venga eseguito a ogni riavvio del sistema infetto.

- **Struttura del Malware:**
    - La **sezione .text** contiene il cuore del codice eseguibile, probabilmente ben offuscato per evitare rilevamenti antivirus.
    - La sezione .data suggerisce la presenza di variabili o buffer necessari durante l'esecuzione del malware, potenzialmente utilizzati per memorizzare dati temporanei o persino dati rubati.
    - La **sezione .rsrc** potrebbe nascondere payload secondari o componenti crittografati che verranno estratti ed eseguiti successivamente. Questa tecnica è spesso utilizzata per superare i controlli di sicurezza iniziali e scaricare ulteriori moduli malevoli in fasi avanzate dell'infezione.
- **Comportamento Offensivo:** Il fatto che il malware importi funzioni da **SHELL32.dll** e **msvcrt.dll** implica la capacità di eseguire comandi di shell e manipolare stringhe e buffer in memoria. Questo è tipico di malware che scaricano ulteriori payload, comunicano con server di comando e controllo (C2), o manipolano processi a livello locale.

Sintesi del Potenziale di Minaccia:

Il malware calcolatriceinnovativa.exe sembra essere stato progettato per essere altamente funzionale e versatile. Potrebbe essere in grado di:

- **Scaricare ed eseguire altri malware** o moduli malevoli nascosti nella sezione risorse.
- **Stabilire persistenza** per garantirsi una presenza duratura nel sistema, sopravvivendo a riavvii.
- **Comunicare con server remoti**, potenzialmente per esfiltrare dati sensibili o ricevere istruzioni dall'attaccante.
- **Compromettere le difese di sicurezza locali** attraverso l'uso di API di basso livello, disabilitando protezioni o modificando configurazioni cruciali.

In conclusione, questo malware rappresenta una minaccia significativa per la sicurezza del sistema infetto. L'uso combinato di tecniche di evasione, persistenza e offuscamento del payload suggerisce che è stato creato con l'obiettivo di compromettere il sistema e mantenere un accesso nascosto e prolungato. È raccomandabile intraprendere un'analisi più approfondita e, se necessario, procedere con la disinfezione del sistema colpito.