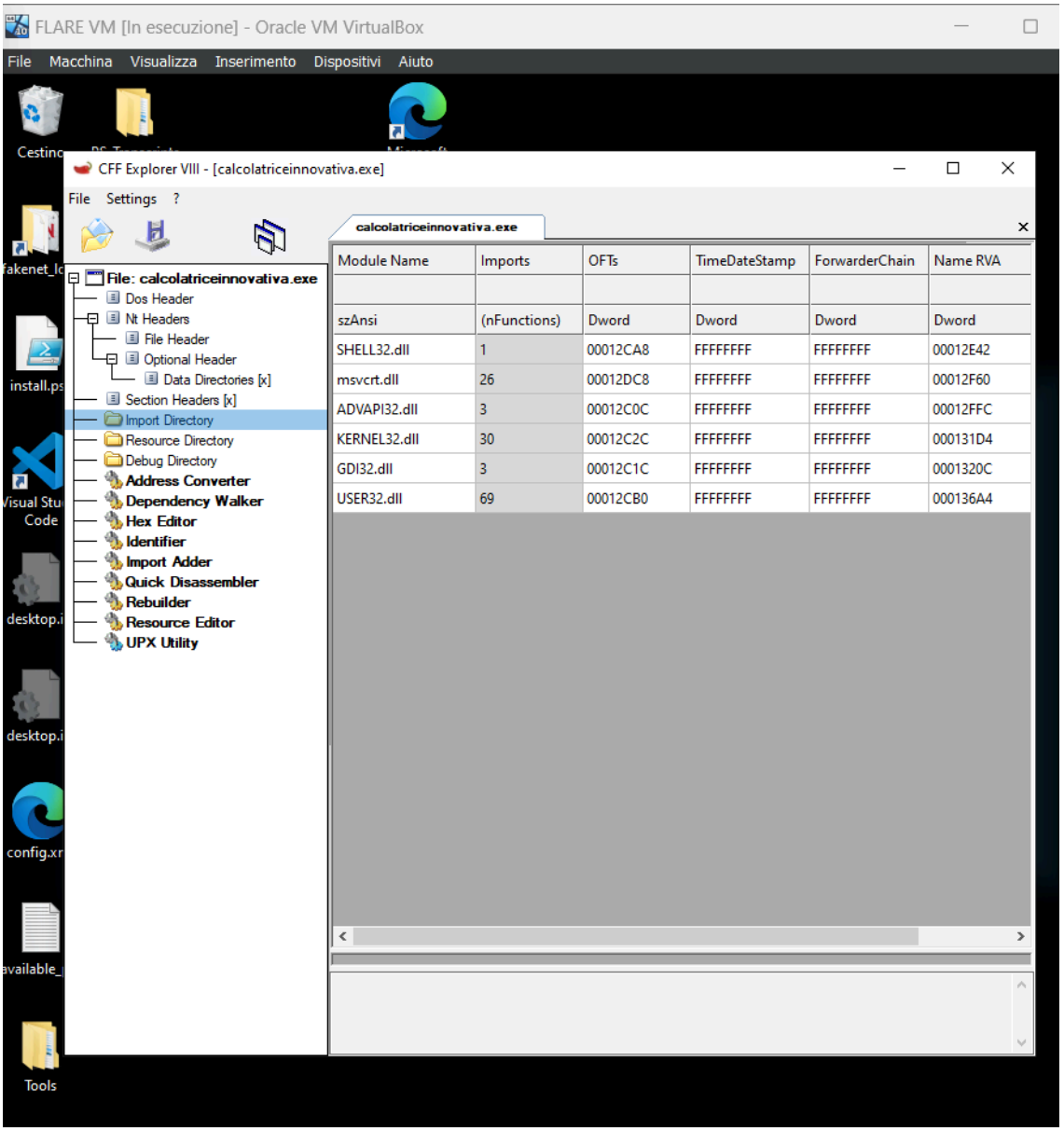
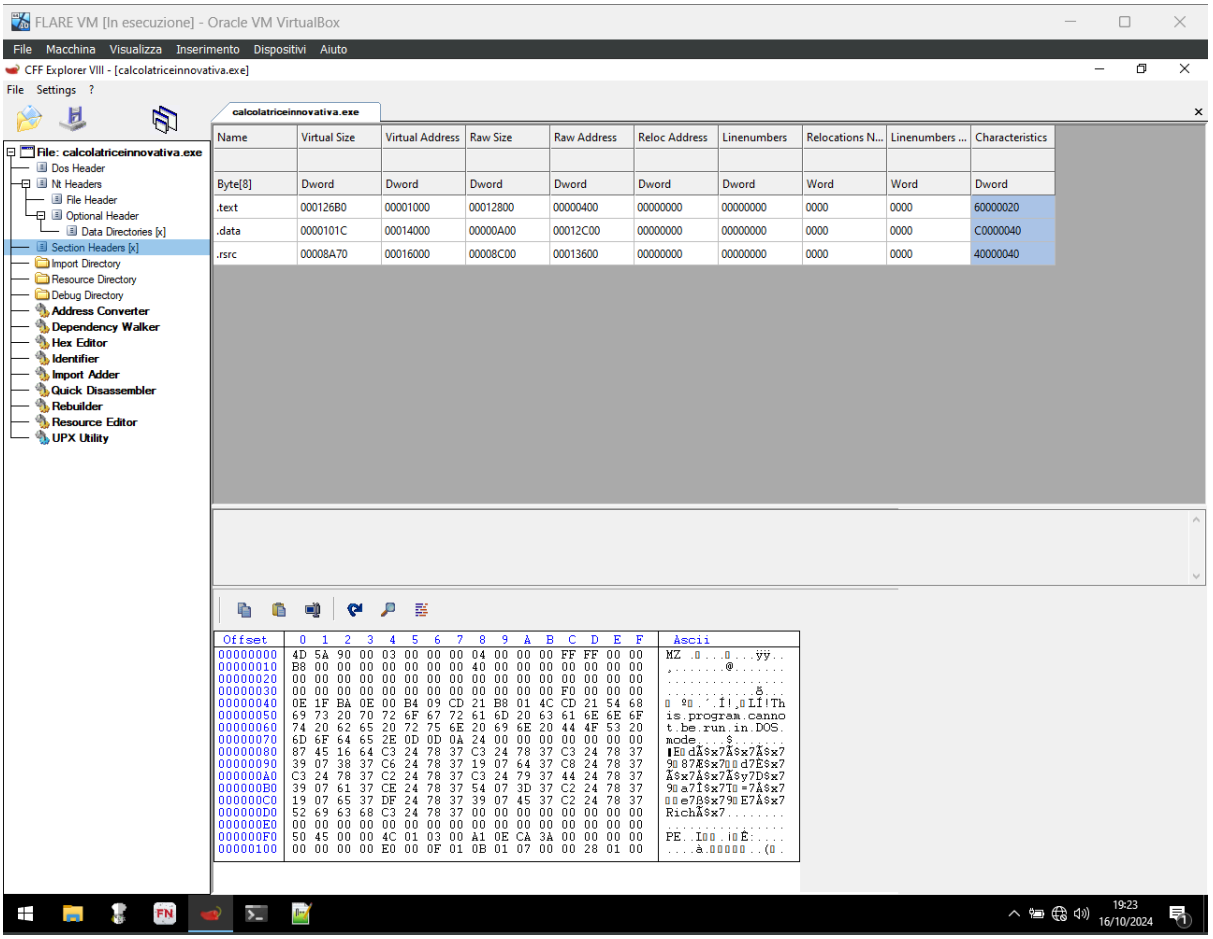

FLARE VM [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CFF Explorer VIII - [calcolatriceinnovativa.exe]
File Settings ?
calcolatriceinnovativa.exe
File: calcolatriceinnovativa.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Resource Directory
Debug Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA
szAnsi | (nFunctions) | Dword | Dword | Dword | Dword
SHELL32.dll | 1 | 00012CA8 | FFFFFFFF | FFFFFFFF | 00012E42
msvcrt.dll | 26 | 00012DC8 | FFFFFFFF | FFFFFFFF | 00012F60
ADVAPI32.dll | 3 | 00012C0C | FFFFFFFF | FFFFFFFF | 00012FFC
KERNEL32.dll | 30 | 00012C2C | FFFFFFFF | FFFFFFFF | 000131D4
GDI32.dll | 3 | 00012C1C | FFFFFFFF | FFFFFFFF | 0001320C
USER32.dll | 69 | 00012CB0 | FFFFFFFF | FFFFFFFF | 000136A4
Tools



Il file eseguibile `calcolatriceinnovativa.exe` importa diverse librerie.

SHELL32.dll: fornisce funzioni per gestire e interagire con il file system, come l'apertura, l'eliminazione e l'esecuzione di file. Può anche gestire operazioni di shell come la creazione di finestre di dialogo o l'avvio di processi.

Potrebbe essere utilizzata per eseguire comandi di sistema o manipolare file sul computer infetto.

msvcrt.dll: questa è una libreria del runtime di Microsoft C, contenente funzioni standard della libreria C come gestione della memoria, input/output e manipolazione di stringhe.

Potrebbe servire per gestire operazioni basilari di memoria e input/output, essenziali per la funzionalità del malware.

ADVAPI32.dll: contiene API avanzate per interagire con il registro di sistema e gestire servizi di sicurezza, inclusi processi e thread di sicurezza, manipolazione delle chiavi del registro e controllo degli accessi.

Spesso è utilizzata dai malware per manipolare chiavi di registro, installare servizi nascosti o ottenere privilegi amministrativi.

KERNEL32.dll: fornisce molte delle API di base per la gestione di memoria, file, processi, e comunicazioni di sistema.

Essenziale per la gestione dei processi del malware, la manipolazione della memoria e il controllo dei file. Molti malware utilizzano KERNEL32.dll per attività di basso livello come l'allocazione della memoria e la lettura/scrittura di file.

GDI32.dll: gestisce le funzioni grafiche, come il disegno di forme e la gestione delle immagini all'interno di Windows.

In genere, se usata in un malware, potrebbe servire per la manipolazione grafica di interfacce o per creare finestre maliziose che imitano quelle legittime.

USER32.dll: contiene funzioni per la gestione dell'interfaccia utente di Windows, come la gestione di finestre, caselle di dialogo e input da tastiera e mouse.

Il malware potrebbe usare questa libreria per creare o manipolare finestre per ingannare l'utente o per raccogliere input dall'utente.

Inoltre, il malware è composto da diverse sezioni che definiscono come il codice e i dati vengono caricati nella memoria.

.text: contiene il codice eseguibile del malware. Questa è la sezione dove risiede il codice vero e proprio che il malware eseguirà quando viene avviato. Questo è il cuore operativo del malware, dove si trovano le istruzioni dannose.

.data: questa sezione contiene i dati globali e statici utilizzati dal malware. Include variabili e strutture di dati che il codice eseguibile usa durante l'esecuzione.

Questa sezione potrebbe memorizzare informazioni critiche per l'esecuzione del malware, come configurazioni o dati raccolti.

.rsrc: la sezione delle risorse contiene dati come icone, immagini, messaggi di dialogo o altre risorse utilizzate dal malware.

Potrebbe essere utilizzata per visualizzare elementi dell'interfaccia o messaggi ingannevoli per convincere l'utente sulla bontà del file.

FACOLTATIVO

Mascheramento:

Il malware si presenta come una "calcolatrice innovativa", un chiaro tentativo di ingannare l'utente facendogli credere che si tratti di un software legittimo e innocuo, così da indurlo a eseguirlo senza sospetti.

Tecniche di evasione:

- **Offuscamento**: Il codice sembra essere compresso o crittografato, suggerendo tecniche di offuscamento per nascondere le vere intenzioni del malware. Questo è indicato dalla sezione `.text` eseguibile, che potrebbe contenere codice compresso (con un rapporto di compressione zlib inferiore a 0.3).
- **Bassa attività iniziale**: Quando eseguito, il malware mostra poca attività, il che potrebbe essere una tecnica per evitare il rilevamento da parte di sistemi di analisi automatizzati o antivirus. Questo comportamento è comune nei malware progettati per passare inosservati.
- **Rilevamento di ambienti virtuali**: È possibile che il malware tenti di identificare se viene eseguito all'interno di una macchina virtuale. Questo serve a ostacolare l'analisi, poiché spesso i

ricercatori utilizzano VM per studiare il comportamento del malware.

Funzionalità di accesso remoto:

Il malware sembra includere funzionalità di accesso remoto. Ciò potrebbe indicare che l'eseguibile è progettato per consentire agli attaccanti di stabilire una connessione con la macchina infetta e controllarla da remoto, una caratteristica comune nei Trojan o nelle backdoor.

Cattura di input:

L'eseguibile crea un oggetto **DirectInput**, che viene comunemente utilizzato per intercettare l'input da tastiera. Questa tecnica potrebbe essere utilizzata per catturare le credenziali dell'utente o altri dati sensibili, come password e informazioni personali.

Attività di rete:

Il malware comunica con l'indirizzo IP 192.168.1.80, che è stato segnalato come malevolo. Questa attività di rete potrebbe indicare che il malware invia dati rubati a un server di controllo o riceve comandi da esso per ulteriori azioni sul sistema infetto.

Tecniche MITRE ATT&CK:

- **T1027.002 e T1027**: Il malware utilizza offuscamento di file o informazioni, incluso il packing del software, per nascondere il suo codice e sfuggire all'analisi.
- **T1056**: Cattura di input, una tecnica utilizzata per rubare informazioni sensibili dall'utente.
- **T1518.001**: Potenziale rilevamento di software di sicurezza. Il malware potrebbe verificare la presenza di antivirus o altri software di sicurezza, modificando il suo comportamento per evitarne la rilevazione.
- **T1082**: Raccolta di informazioni sul sistema. Il malware potrebbe raccogliere dettagli sul sistema, come la configurazione di rete o il

tipo di hardware, per adattarsi all'ambiente e prepararsi a ulteriori attacchi.

Conclusione:

In base a queste osservazioni, il malware **calcolatriceinnovativa.exe** sembra essere progettato per stabilire un accesso remoto al sistema infetto, catturare input dell'utente (probabilmente per rubare credenziali) e raccogliere informazioni sul sistema. Utilizza una serie di tecniche di evasione per evitare il rilevamento, tra cui l'offuscamento del codice e un comportamento passivo iniziale. La connessione a un indirizzo IP segnalato come malevolo suggerisce che il malware potrebbe far parte di una campagna più ampia di compromissioni, forse utilizzato come punto di ingresso per ulteriori attacchi o movimenti laterali all'interno della rete.