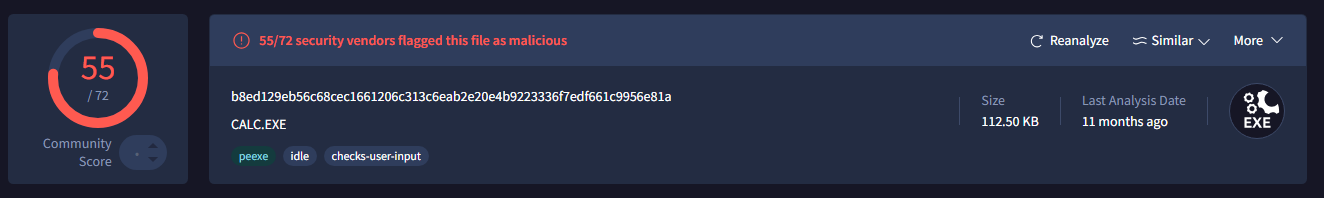
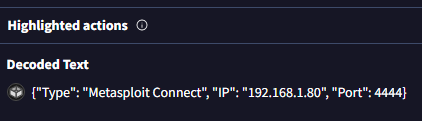
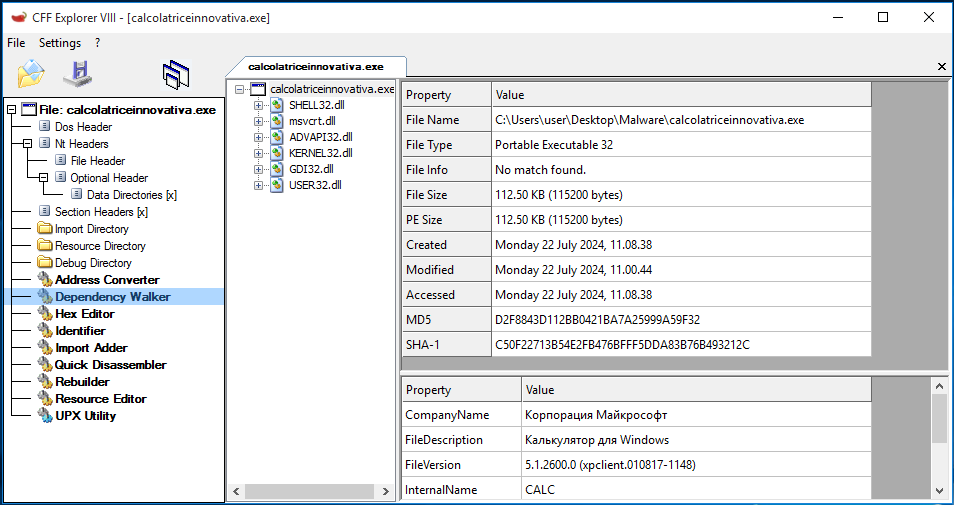
**S9/L2**

**Malware Analysis**

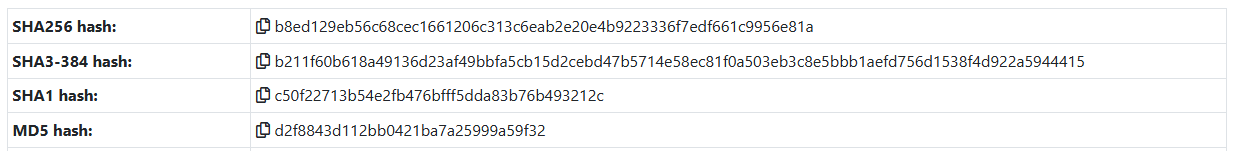
L’obiettivo di oggi è analizzare il malware **calcolatriceinnovativa.exe** tramite analisi statica di base e analisi dinamica di base per notare le differenze tra le due tipologie di scansione.   
  
**SCANSIONE STATICA DI BASE**  
  
Si inizia la scansione caricando il file su **Virus Total**, il risultato sarà il seguente:   
  
  
Controllando i vendor, si può evincere la tipologia di malware:  
  
  
Si capisce che si ha a che fare con una backdoor. Si possono raccogliere più informazioni nella sezione Behaviour, dove l’ipotesi viene ulteriormente confermata:  


Tramite **il Decoded Text** si vedrà lo scopo del malware che tenterà di mettere in connessione, tramite backdoor, il dispositivo della vittima all’indirizzo IP 192.168.1.80 tramite la porta 4444.

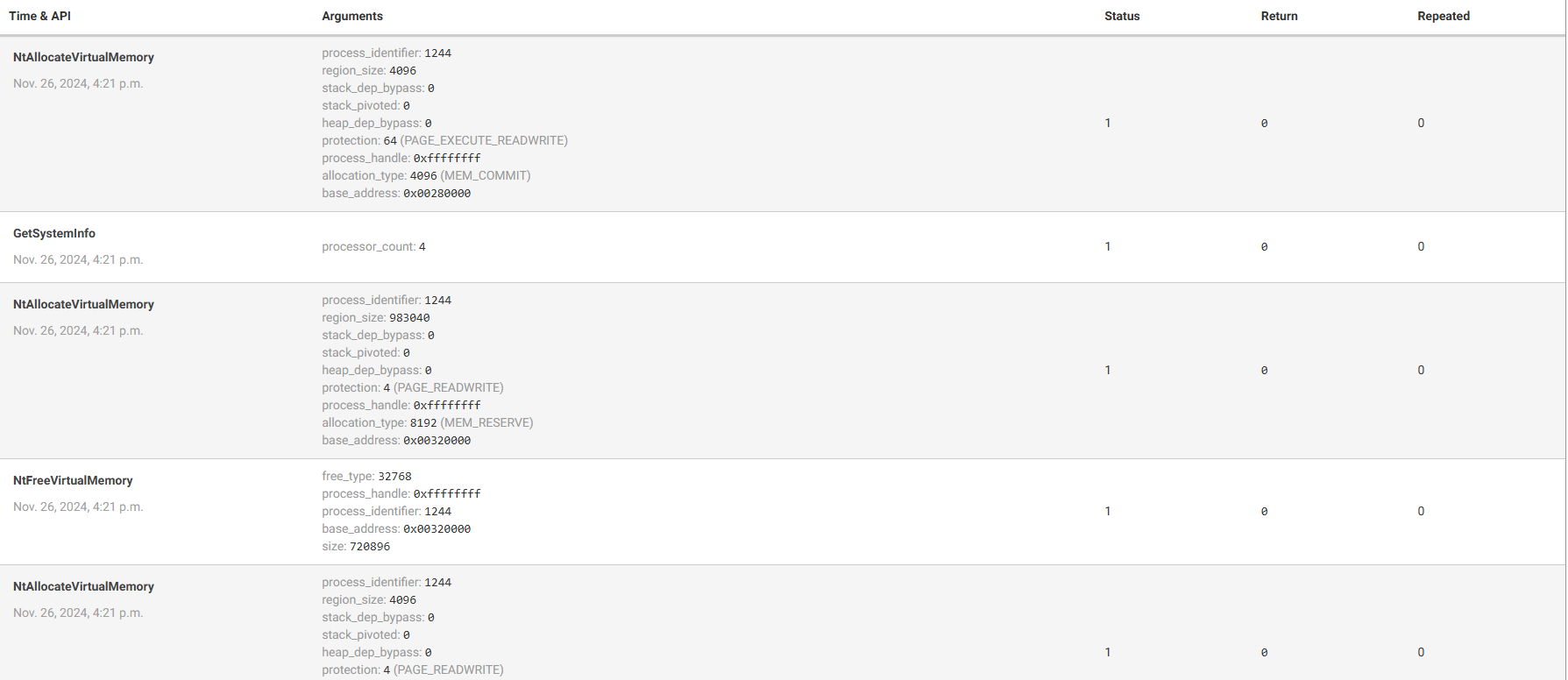
Approfondendo la ricerca tramite **CFF Explorer**, si può analizzare in modo più approfondito il malware. Nello specifico, si può controllare da quali file il malware dipende, impedendogli il giusto funzionamento se dovessero mancare:



Vedendo le librerie importate, si possono notare quali sono le azioni che il malware può effettuare:  
  
Tramite **KERNEL32** e **USER32** si può evincere che il malware ha accesso a funzioni di sistema.  
Tramite **ADVAPI32** il malware potrebbe interagire con il registro di sistema Windows  
Tramite **SHELL32** il malware suggerisce che potrebbe componenti GUI.

Continuando la scansione statica possiamo utilizzare Malware Bazaar, dove troveremo anche i file hash del malware:  


**SCANSIONE DINAMICA DI BASE**

Una volta approfondita la scansione statica, si può passare a quella dinamica utilizzato il software **Cuckoo**. Grazie alla scansione dinamica si effettuerà una simulazione di utilizzo del malware in ambiente protetto, dove si potrà analizzare nel dettaglio il comportamento del malware. Di seguito il risultato:  
  
  
Dal Behaviour Analysis si possono notare nel dettaglio i vari step che il malware tenterà di eseguire per connettere la macchina vittima all’IP dell’attaccante.   
 **In conclusione**, si può confermare con totale sicurezza che il file .exe calcolatriceinnovativa è una backdoor che lascia libero accesso all’attaccante di accedere al dispositivo della vittima.