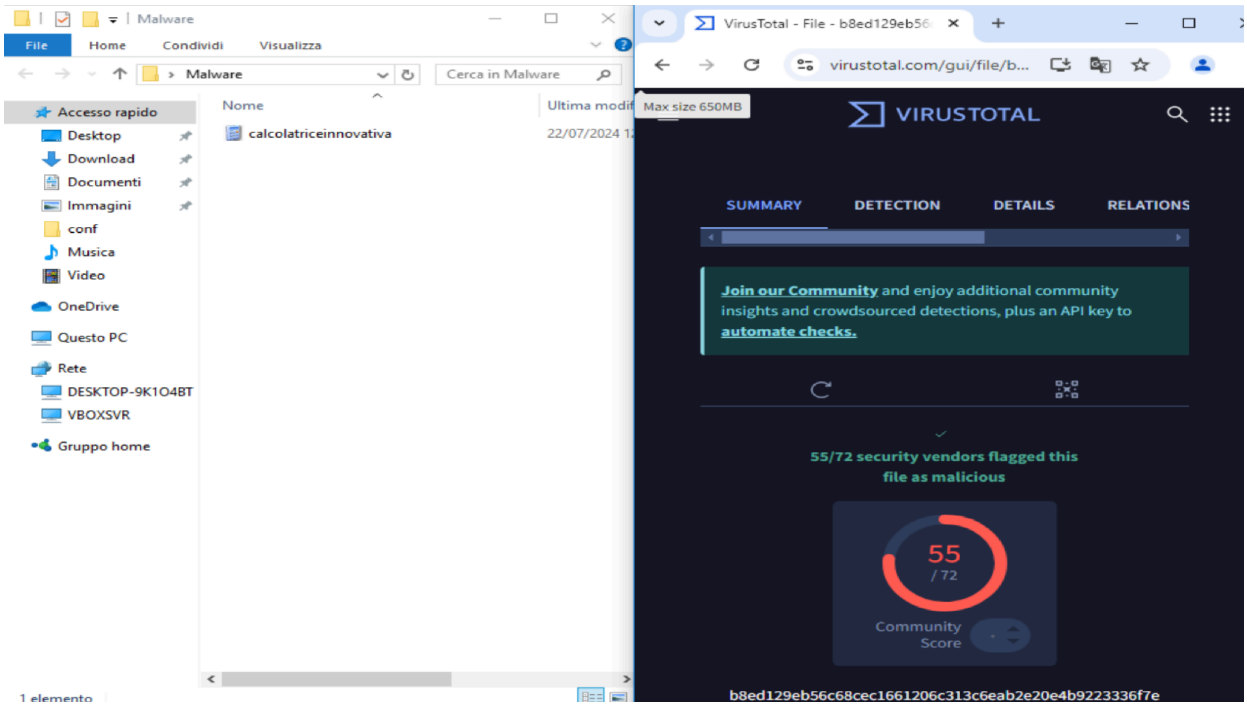
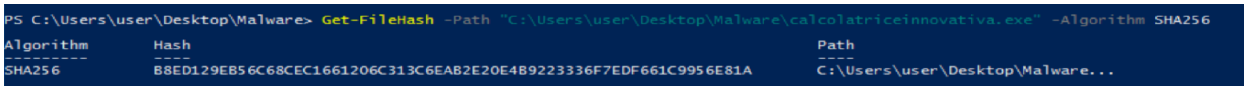
Oggi abbiamo provato una scansione di un Malware attraverso 4 metodi statici e uno dinamico.

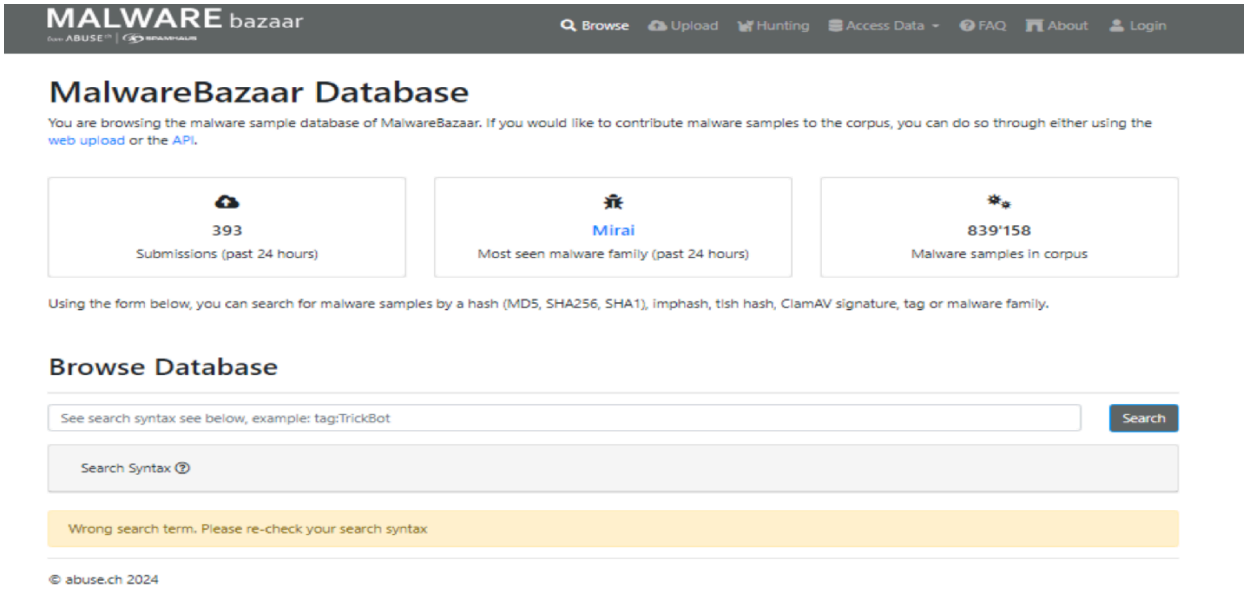
1. virustotal
   Incollando il file sospetto in questo sito web sono state riscontrate 55 intenzioni malevoli nel file, il che dimostra che è un malware, ma per conferma passeremo questo file al setaccio anche tramite altre applicazioni.



Stavolta avremo bisogno del codice hash del file quindi (essendo su windows) avviamo il comando per ricavare il codice hash dal file:
Get-FileHash -Path “path\del\file” -Algorithm SHA256

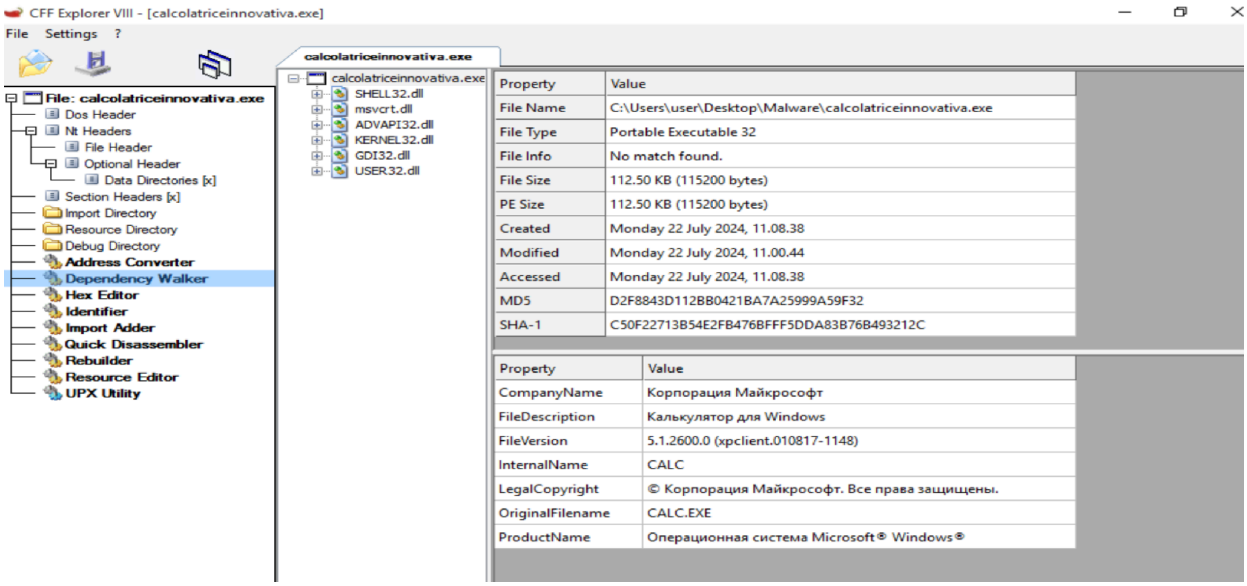


una volta ottenuto l’hash nel formato SHA256 che è il formato letto da Malware Bazaar, proviamo a cercare il codice Hash li.

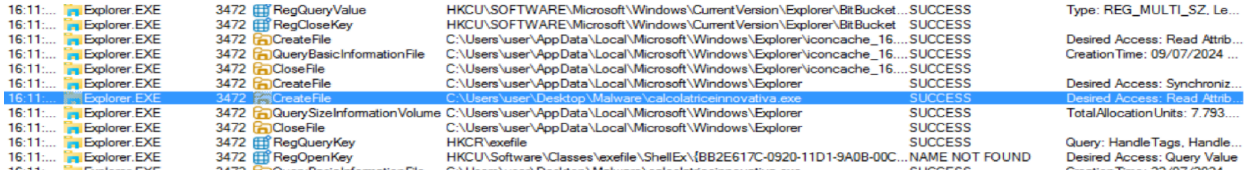


Probabilmente non ci da errori perchè in questo caso il codice non è così aggressivo.

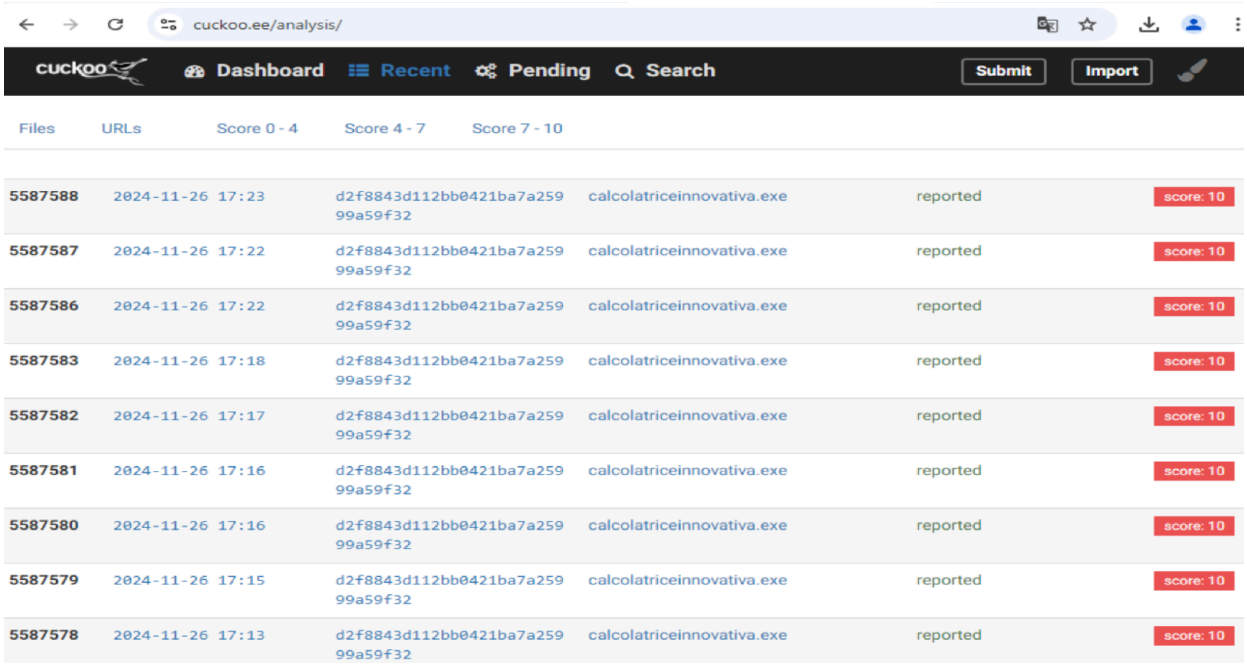
Facciamo una prova anche tramite CFF Explorer dove possiamo vedere molti dati del file utili.



e per finire proviamo anche Procmon.



Dinamica: Cuckoo


cuckoo.ee/analysis/
cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
Files
URLs
Score 0 - 4
Score 4 - 7
Score 7 - 10
5587588 2024-11-26 17:23 d2f8843d112bb0421ba7a25999a59f32 calcolatriceinnovativa.exe reported score: 10
5587587 2024-11-26 17:22 d2f8843d112bb0421ba7a25999a59f32 calcolatriceinnovativa.exe reported score: 10
5587586 2024-11-26 17:22 d2f8843d112bb0421ba7a25999a59f32 calcolatriceinnovativa.exe reported score: 10
5587583 2024-11-26 17:18 d2f8843d112bb0421ba7a25999a59f32 calcolatriceinnovativa.exe reported score: 10
5587582 2024-11-26 17:17 d2f8843d112bb0421ba7a25999a59f32 calcolatriceinnovativa.exe reported score: 10
5587581 2024-11-26 17:16 d2f8843d112bb0421ba7a25999a59f32 calcolatriceinnovativa.exe reported score: 10
5587580 2024-11-26 17:16 d2f8843d112bb0421ba7a25999a59f32 calcolatriceinnovativa.exe reported score: 10
5587579 2024-11-26 17:15 d2f8843d112bb0421ba7a25999a59f32 calcolatriceinnovativa.exe reported score: 10
5587578 2024-11-26 17:13 d2f8843d112bb0421ba7a25999a59f32 calcolatriceinnovativa.exe reported score: 10