Esercizio S9 L2 del 26/11/24 ***Daniele Paolone***

Malware Analysis

La malware analysis è il processo di esaminare e comprendere il comportamento, le funzionalità e gli obiettivi di un malware. Questo processo può essere suddiviso in due fasi principali:

- Analisi statica: esamina il malware senza eseguirlo, analizzando il codice sorgente per identificare firme, istruzioni o modelli di comportamento.

- Analisi dinamica: osserva il comportamento del malware in un ambiente controllato, come una sandbox.

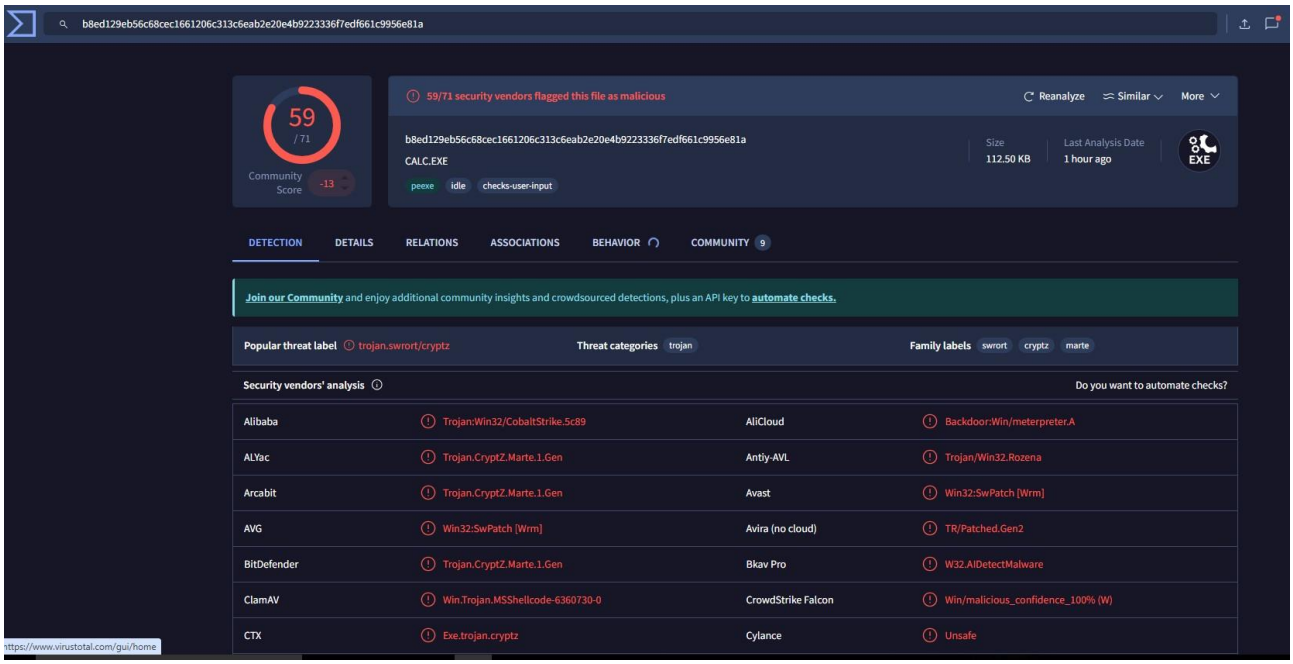
Per la prima fase, cioè quella statica, per l' esercizio da svolgere, sono stati utilizzati:

- virustotal.com
- malware baazar
- cff explorer

Virus total

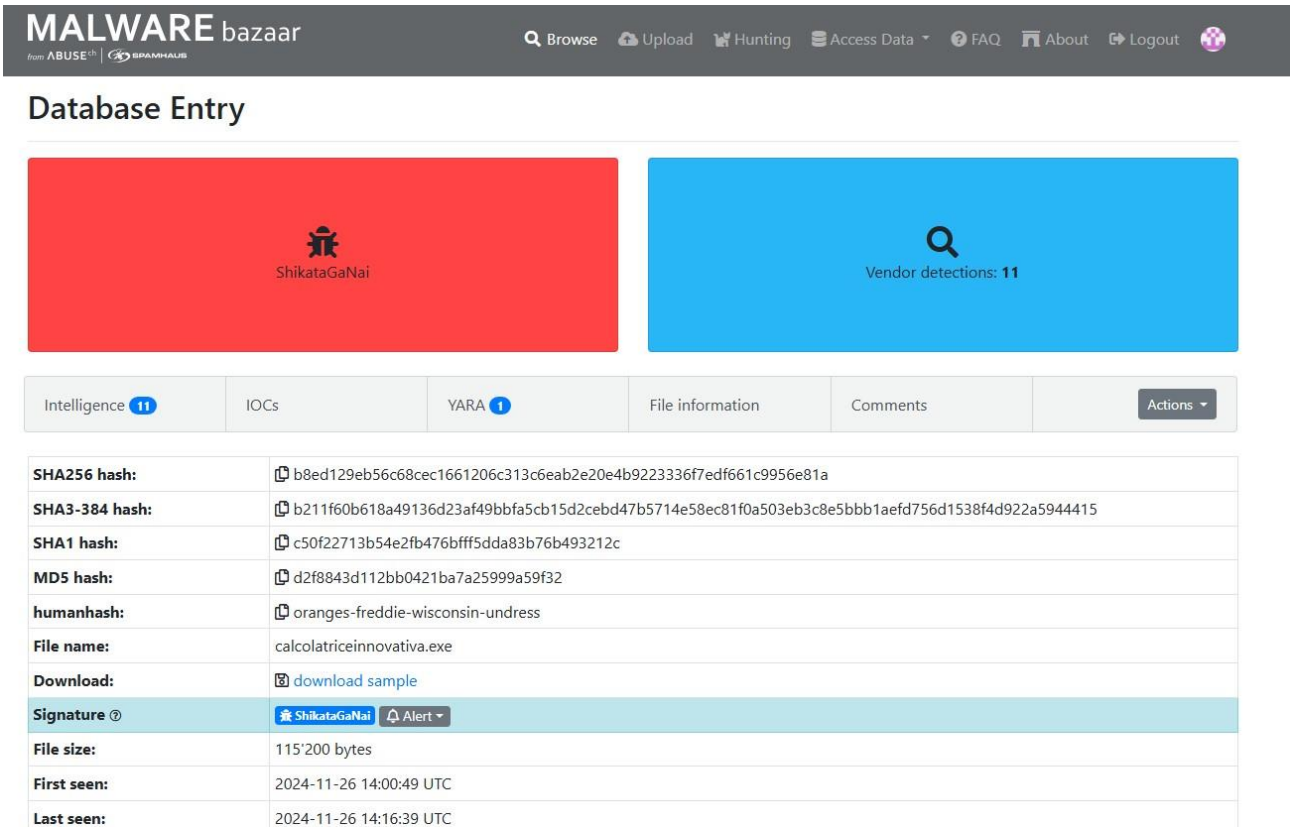
Dopo aver caricato il file malevolo sul sito, già dalla prima analisi rilasciata si può evincere:

- il suo punteggio evidenziato in rosso, che sta a significare che la maggior parte delle aziende che si occupano di sicurezza informatica, lo hanno riconosciuto come un trojan, nello specifico installa una backdoor sulla macchina della vittima.



Malware Baazar

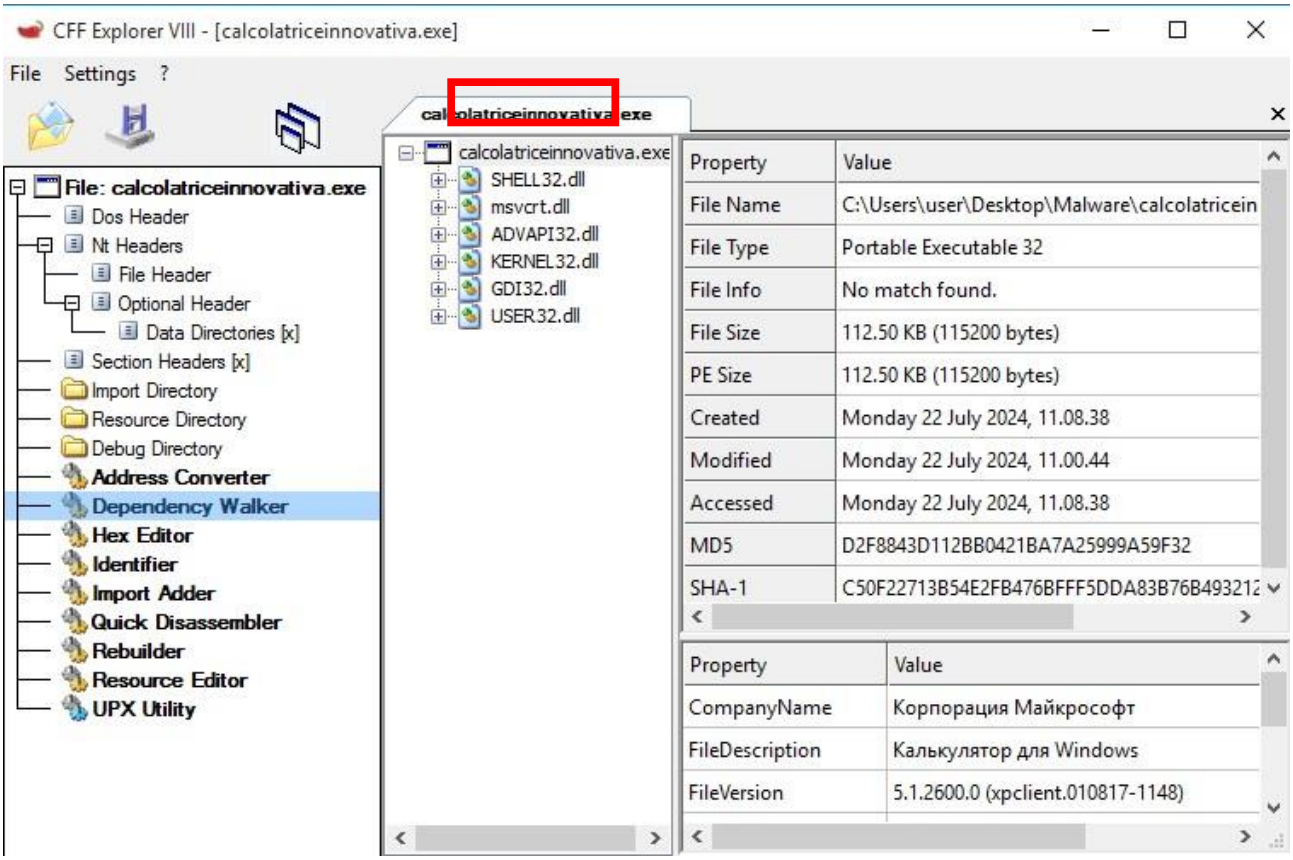
VirusTotal rilascia l' hashing del malware, cioè la sua impronta digitale, questo vuol dire che è stato fatto un report su di esso. In questo modo si può verificare se un file corrisponde al malware analizzato confrontandolo con l'hash. Inoltre Gli hash possono essere usati per aggiornare database di antimalware o strumenti di sicurezza per rilevare il malware.
Si inserisce l' hashing sul sito Malware Baazar per avere altre informazioni e ulteriore conferma.



Come si può notare dall' immagine, viene segnalato l' utilizzo nel codice, dell' encoder *shigata ga nai*. Viene utilizzato per offuscare il codice così da non essere riconosciuto dagli antimalware, in base al numero di iterazioni applicate.

CFF Explorer

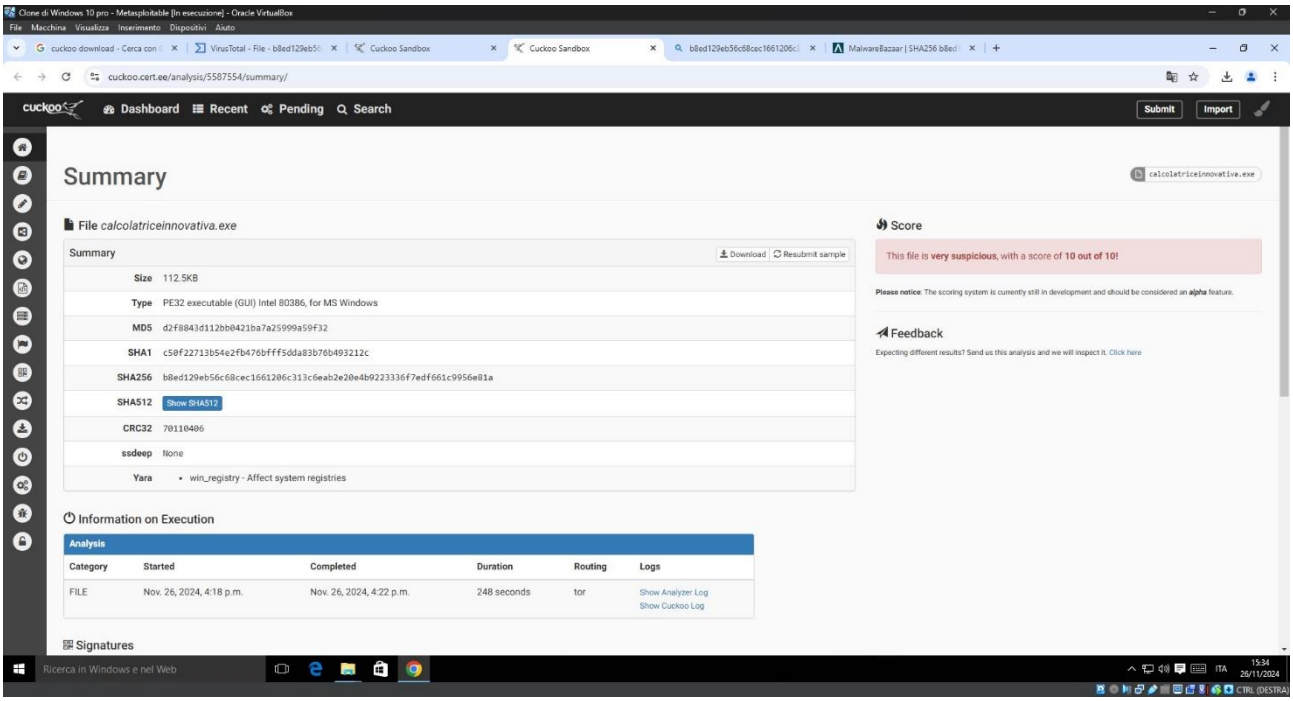
Con questo terzo tool, andiamo a verificare la voce "*dependency walker*". Questa sezione elenca tutte le librerie dalle quali il file eseguibile dipende, cioè le librerie che deve caricare per funzionare correttamente. Come rappresentato nell' immagine, il malware ha bisogno della libreria shell32.dll. Questo ci conferma quanto riscontrato da virustotal che lo segnala come backdoor. Perché tramite questa libreria, può creare una shell, cioè un collegamento tra l' attaccante e la vittima, con la quale può dare istruzione e muoversi liberamente nella macchina.



Per la seconda fase, cioè l' analisi dinamica, si utilizza il tool cuckoo.

Cuckoo

Esso consente di esaminare file sospetti e osservare il loro comportamento in un ambiente virtuale o isolato (sandbox).



Anche con questo tool, si ha la conferma che è un malware, dato che lo classifica con un punteggio di 10/10. Ma essendo un' analisi dinamica, si può capire anche come agisce. Infatti nella sezione behavioral analysis, si può notare, come cerchi di connettersi ed inviare dati ad una macchina esterna.