Analisi del Malware

Attività di Analisi del Malware

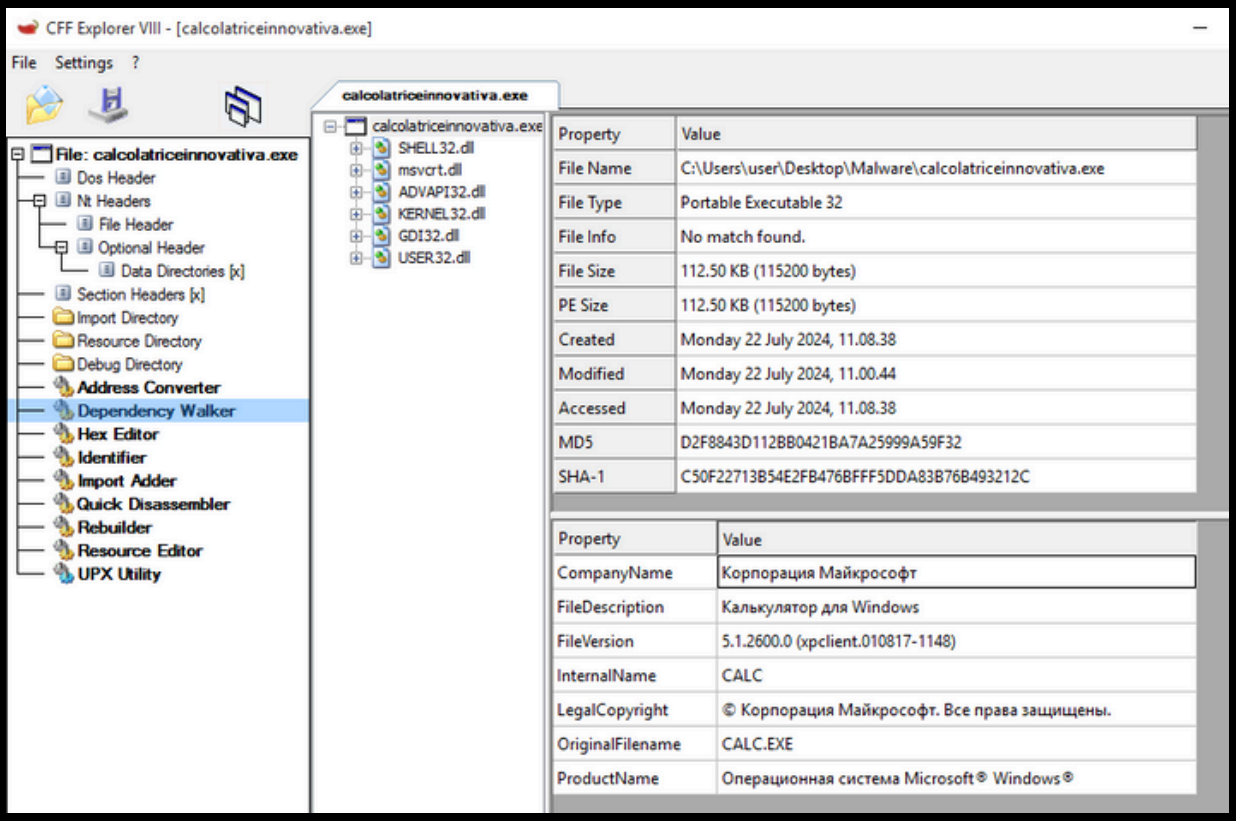
Oggetto: Sarà condiviso un malware relativamente innocuo.

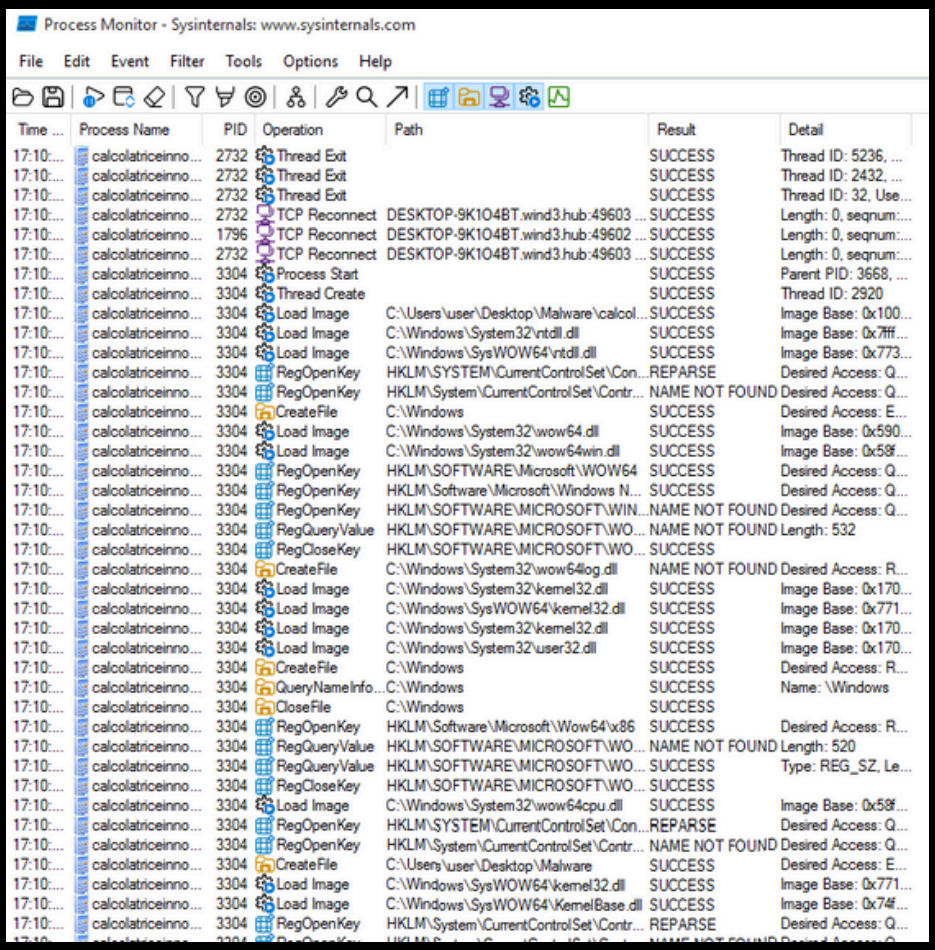
Compiti:

Analisi Statica: Esaminare il codice del malware senza eseguirlo, al fine di comprendere la sua struttura e le sue funzionalità.

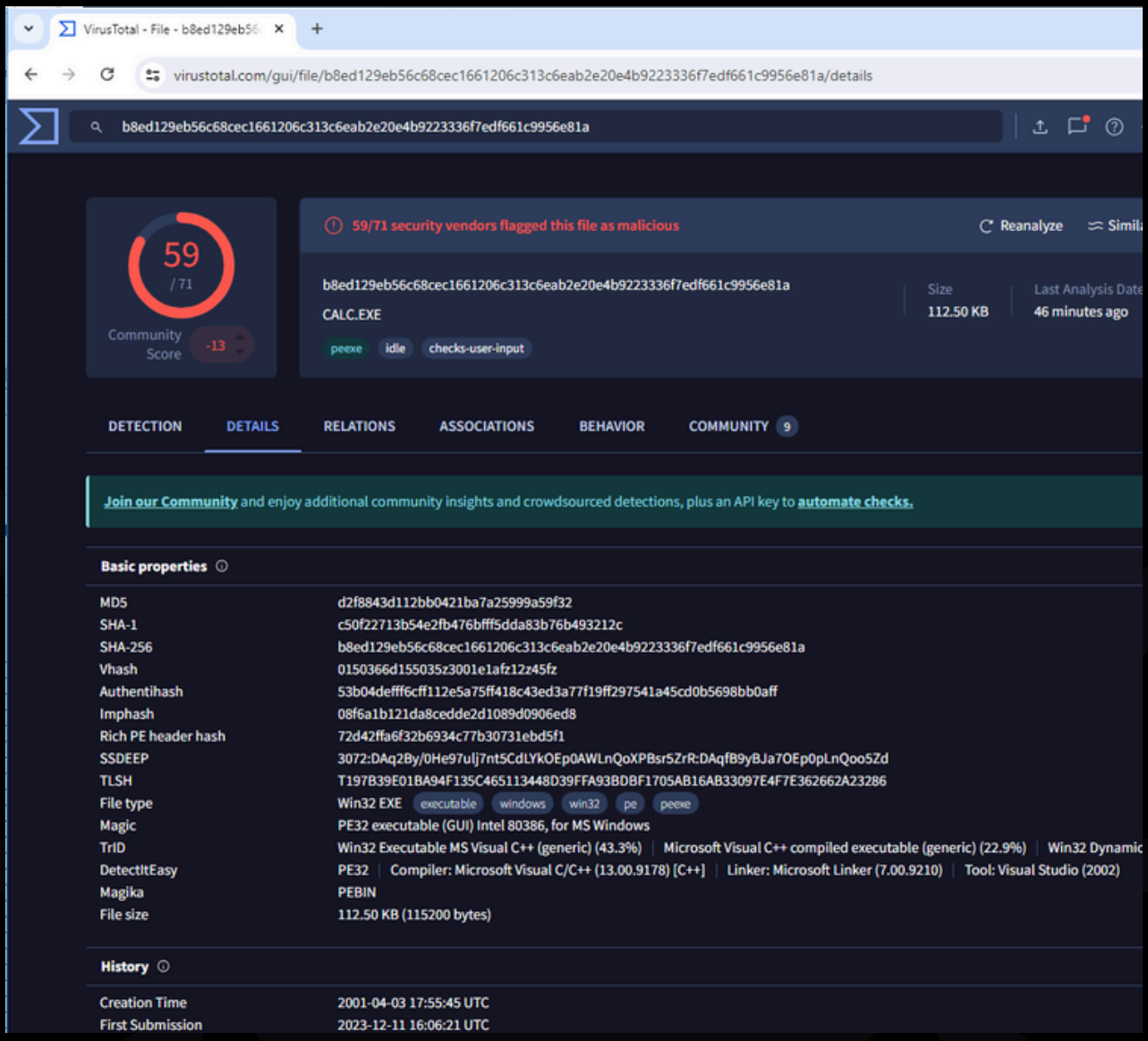
Analisi Dinamica: Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

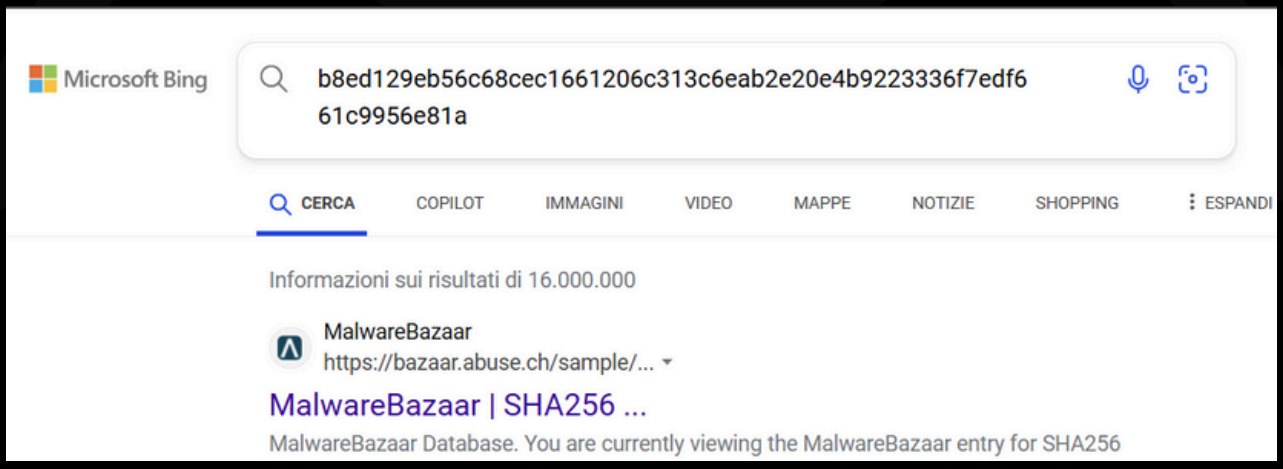
Cff Explorer + ProcMon



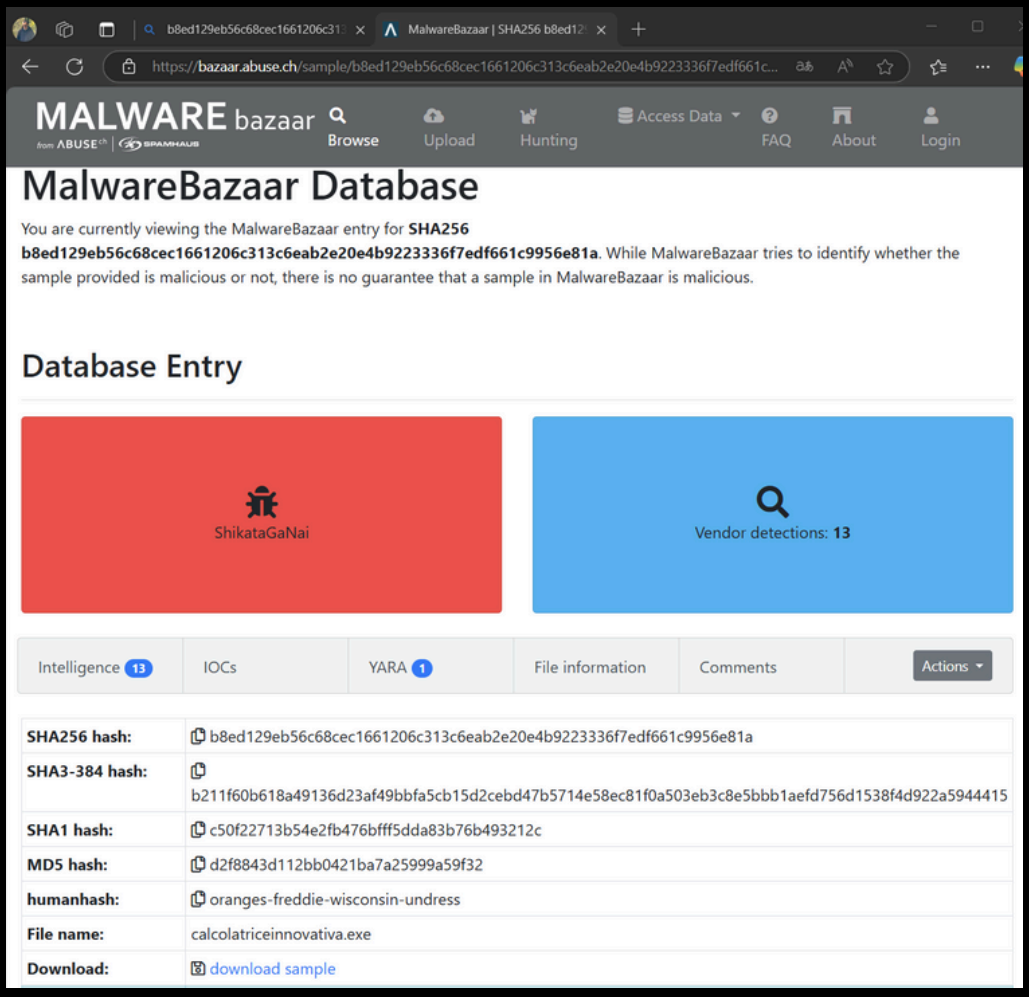


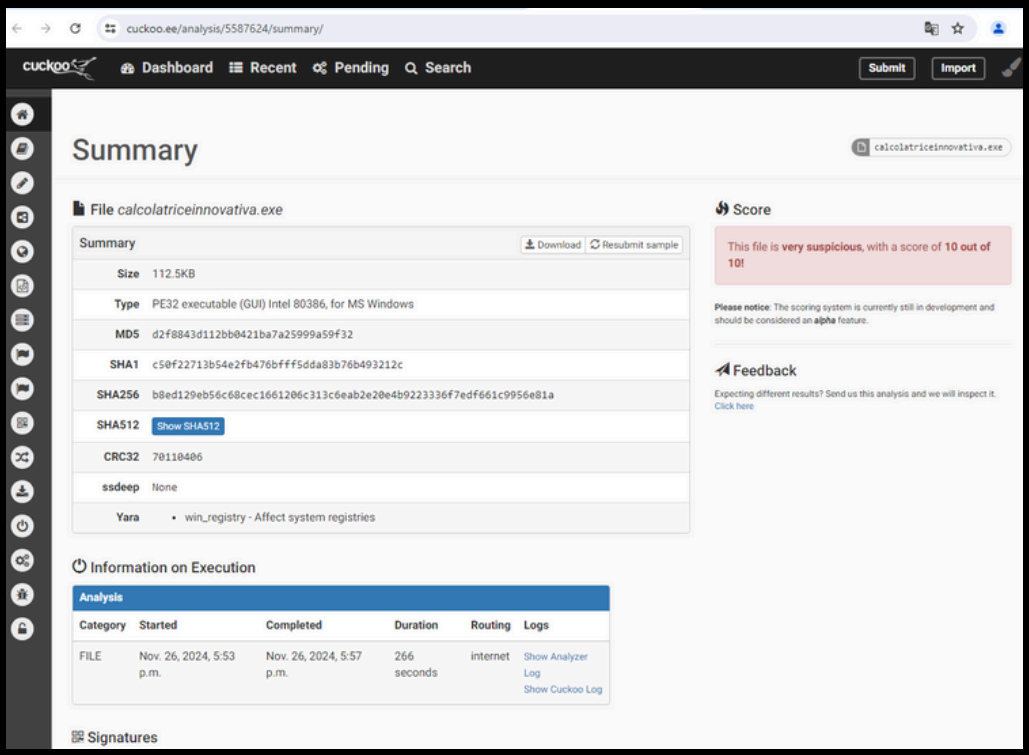
Virustotal / Hash





MBazaar / Cuckoo





Relazione

Per analizzare il malware, ho utilizzato cinque strumenti principali: CFF Explorer, ProcMon, VirusTotal, Malware Bazaar e Cuckoo. Questi strumenti mi hanno aiutato a capire meglio cosa fa il malware sia guardando il suo codice senza eseguirlo (analisi statica), sia osservando come si comporta mentre viene eseguito (analisi dinamica).

Analisi Statica:

Per l' analisi statica, ho usato CFF Explorer per esaminare il file del malware. Questo programma mi ha permesso di vedere la struttura del file, come le librerie che usa e le sezioni che contiene. Senza eseguire il malware, ho potuto identificare alcune informazioni importanti, come le funzioni che potrebbero essere utilizzate per scopi malevoli.
Poi, ho caricato il file su VirusTotal . Questo strumento mi ha aiutato a vedere se altri antivirus avevano già riconosciuto il file come dannoso. Con VirusTotal, è facile capire se il malware è già conosciuto da altri esperti di sicurezza. Infine, ho cercato il malware su Malware Bazaar, tramite l'hash trovato su VirusTotal, la ricerca l'ho fatto un Edge, in quanto Chrome, in qualche modo filtra le ricerche per protegere l'utente.
Malware Bazaar è un archivio di campioni di malware dove puoi trovare informazioni su file simili e scoprire se il malware che sto analizzando ha delle varianti note o è stato già analizzato.

Analisi Dinamica:

Per l'analisi dinamica, ho utilizzato Cuckoo tramite il servizio online cuckoo.ee per caricare il file del malware e analizzarlo in un ambiente sicuro. Cuckoo ha generato un report dopo aver analizzato il file.
Per monitorare ulteriormente il comportamento del malware, ho usato ProcMon. Questo strumento mi ha consentito di vedere tutte le operazioni che il malware stava cercando di eseguire, come la creazione o la modifica del file e le modifiche al registro del sistema.
In questo modo, con l'analisi statica ho ottenuto una comprensione iniziale del file senza eseguirlo, mentre con l'analisi dinamica ho potuto osservare direttamente il suo comportamento per capire meglio come agisce quando viene eseguito.