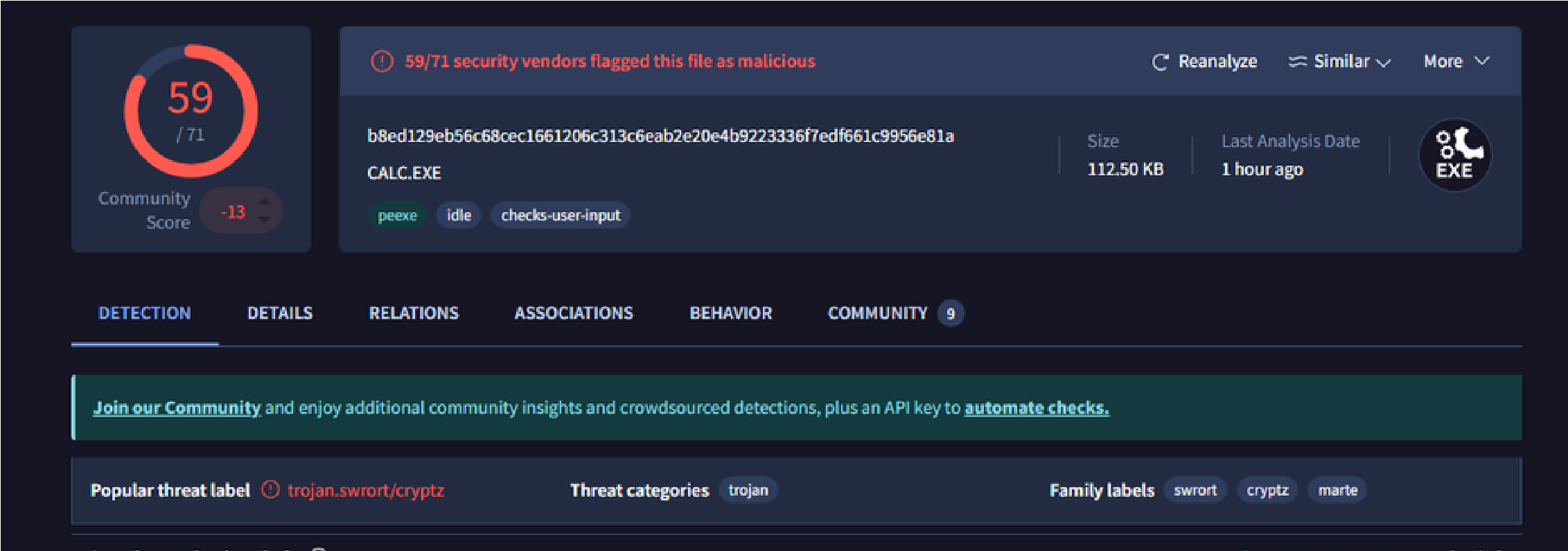
**Analisi Malware**

# Analisi statica



VirusTotal è un servizio online gratuito che consente

di analizzare file e URL sospetti per determinare se

contengono malware o altre minacce. Utilizza una

serie di motori antivirus e strumenti di analisi per

eseguire

scansioni

multiple,

offrendo

un

report

dettagliato sulla sicurezza di un file o di un link.

Abbiamo caricato il malware su VirusTotal e abbiamo riscontrato che 59 motori antivirus lo considerano un malware.

CFF Explorer è uno strumento di analisi e modifica di file PE (Portable Executable), utilizzato principalmente

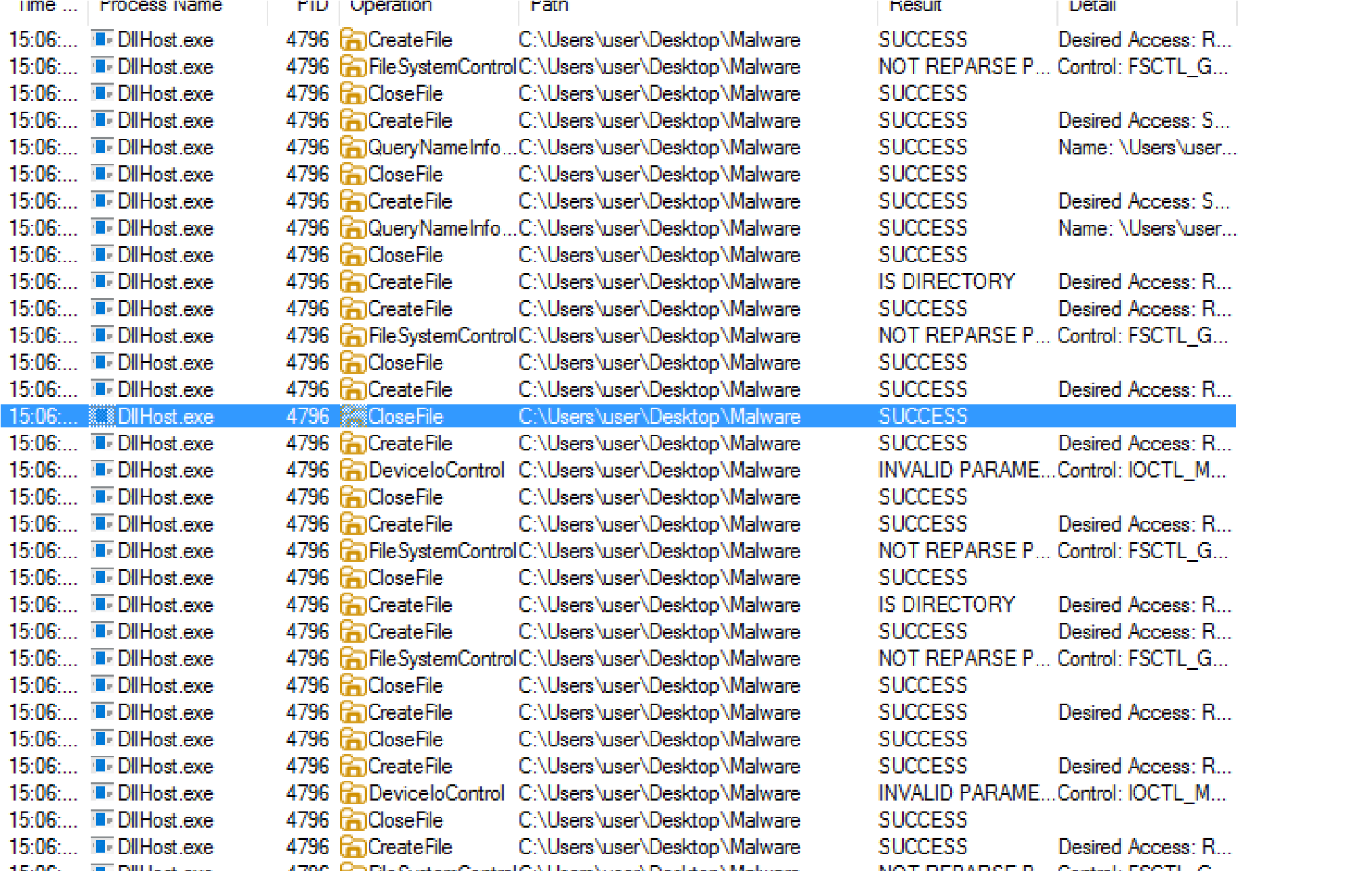
per l'ingegneria inversa e l'analisi di malware. È molto utile per gli sviluppatori e gli analisti di sicurezza per

esaminare i file eseguibili Windows (come .exe, .dll,.sys), permettendo di visualizzare e modificare le

varie sezioni interne dei file.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | |  | | --- | | Il messaggio "Bound Import Directory RVA Invalid" è un errore che può verificarsi durante l'analisi di un file PE (Portable Executable) come un .exe o .dll, e si riferisce a un problema con la Bound Import Table del file. Potrebbe essere un campanello di allarme malware. | |
|  | |  | | --- | | Il messaggio "Program cannot run in DOS" che appare in CFF Explorer si riferisce a un'indicazione che il file che stai cercando di analizzare è un programma Windows e non può essere eseguito in un ambiente DOS (Disk Operating System). Questo messaggio è legato alla struttura del file  PE (Portable Executable) e alla compatibilità del programma.  Potrebbe anche indicare che il file è stato modificato (da malware o altro software) per sembrare che sia stato progettato per DOS quando, in realtà, è un programma Windows. | | |

**Procmon** Process Monitor (ProcMon) è uno strumento di monitoraggio avanzato per sistemi Windows, sviluppato da Sysinternals (Microsoft), che permette di registrare e analizzare in tempo reale tutte le attività di sistema, come operazioni di file system, modifiche al registro di sistema e attività di processo. Viene utilizzato principalmente per l'analisi delle prestazioni, la risoluzione di problemi e l'investigazione di malware.



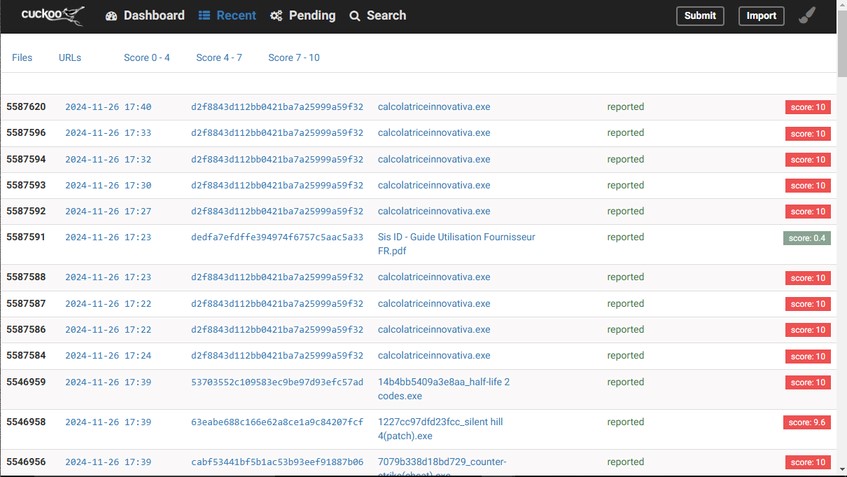
La maggior parte dei risultati è **SUCCESS**, indicando che le operazioni (es. apertura o chiusura del file/directory) hanno avuto esito positivo.

Ci sono alcune voci con esito **NOT REPARSE POINT** e **INVALID PARAMETER**. Questi risultati non rappresentano errori critici ma potrebbero indicare:

Tentativi di manipolazione o accesso avanzato (ad esempio, malware che cerca punti di reindirizzamento o esegue operazioni anomale).

# Analisi dinamica

Cuckoo Sandbox è una piattaforma di analisi automatica di malware, progettata per eseguire e monitorare comportamenti sospetti in un ambiente virtuale isolato. Utilizzato principalmente in contesti di sicurezza informatica, Cuckoo permette di analizzare file eseguibili, documenti e URL per scoprire se contengono codice dannoso, senza rischiare danni al sistema operativo host.



Quando si trova un file con "10 su 10", si sta riferendo a una valutazione che indica che tutti i 10 motori antivirus (o strumenti di rilevamento) integrati nel sistema di analisi di Cuckoo hanno identificato il file come dannoso. Questo significa che il file è stato riconosciuto da ogni motore di rilevamento come una minaccia, suggerendo con alta probabilità che si tratti di malware.

**Conclusioni sull'analisi del malware:**

L'analisi del malware è un processo fondamentale per comprendere la natura di una minaccia informatica, le sue modalità di azione e il suo impatto potenziale su un sistema o una rete.

Attraverso l'uso di strumenti come Cuckoo Sandbox, VirusTotal, e altri software di analisi, è possibile ottenere un quadro completo del comportamento di un file sospetto, aiutando a prevenire danni e a sviluppare soluzioni per contrastarlo.