MALWARE ANALYSIS

Traccia: Oggetto: Sarà condiviso un malware relativamente innocuo.
Compiti:

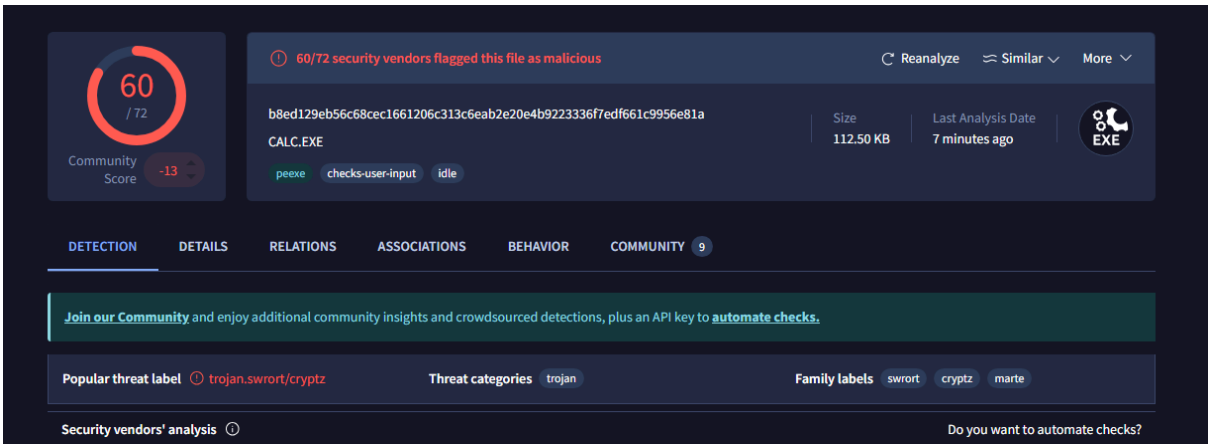
1. Analisi Statica: Esaminare il codice del malware senza eseguirlo, al fine di comprendere la sua struttura e le sue funzionalità.
2. Analisi Dinamica: Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

Svolgimento:
Si chiede di effettuare una Malware Analysis su un Malware su macchina virtuale Windows 10.
L'esercizio si dividerà in 2 fasi:

- Analisi Statica;
- Analisi Dinamica.

Entrambe le fasi sono fondamentali per comprendere le azioni che il malware compie e come riuscire a contrastarle di conseguenza.

Analisi Statica
Quando si effettua una Malware Analysis si comincia dall'analisi statica, ovvero l'analisi del codice del malware senza eseguirlo.
Per fare ciò esistono diversi strumenti utili, primo tra tutti VirusTotal, un servizio online gratuito che permette di analizzare file sospetti per rilevare malware, virus e altre minacce informatiche. Li analizza utilizzando motori antivirus e strumenti di sicurezza per eseguire la scansione di file o collegamenti, fornendo un rapporto dettagliato riguardo ad eventuali rilevamenti.
Il risultato ottenuto dalla scansione tramite **VirusTotal** sarà il seguente:



La rilevabilità di questo malware è molto alta, con un risultato di 60/72.

Il secondi strumento che si andrà ad utilizzare sarà **CFF Explorer**, ovvero un software che si utilizza per l'analisi e la modifica dei file su Windows.
Ciò che può essere analizzato tramite tramite CFF Explorer sono elementi come:

- Dos Header (contiene le firme MZ che lo rendono eseguibile);
- Import Directory (librerie importate);
- Resource Directory (risorse incorporate nel file);
- Hex Dump (rappresentazione esadecimale dei dati binari del file);
- Dependency Walker (librerie indispensabili per il corretto funzionamento del file);
- Resource Editor (per modificare le risorse incorporate nel file).

Andando a verificare le librerie importate, è possibile rilevarne alcune che, pur non essendo sospette, possono essere problematiche:

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
SHELL32.dll	1	00012CA8	FFFFFFFF	FFFFFFFF	00012E42	0000109C
msvcrt.dll	26	00012DC8	FFFFFFFF	FFFFFFFF	00012F60	000011BC
ADVAPI32.dll	3	00012C0C	FFFFFFFF	FFFFFFFF	00012FFC	00001000
KERNEL32.dll	30	00012C2C	FFFFFFFF	FFFFFFFF	000131D4	00001020
GDI32.dll	3	00012C1C	FFFFFFFF	FFFFFFFF	0001320C	00001010
USER32.dll	69	00012CB0	FFFFFFFF	FFFFFFFF	000136A4	000010A4

SHELL32.dll è una libreria che potrebbe insinuarsi nell'interfaccia utente, ADVAPI32.dll potrebbe alterare i registri, USER32.dll e KERNEL32.dll possono consentire di infiltrarsi nei permessi di root, msvcrt.dll è potenzialmente pericoloso (andrebbe analizzato il percorso su cui è presente questa libreria per verificarne la legittimità) e si tratta della libreria standard del linguaggio C.
Questo è solo uno dei diversi aspetti che si può analizzare per partire con una analisi statica.

L'altro strumento utile per l'analisi statica è **Procmon**, abbreviazione per Process Monitor, si utilizza per il monitoraggio del sistema sviluppato da Microsoft, controlla in tempo reale le attività di file system, registro di sistema, processi e thread e rete, è un grande aiuto nell'individuazione di malware.
Gli aspetti più importanti da analizzare saranno:

- verifica di modifiche sospette al registro di sistema per ottenere persistenza;
- attività di rete inaspettate;
- creazione o modifica di file di sistema;
- creazione di nuovi processi o iniezione di codice in altri processi;
- modifiche alle impostazioni di sicurezza.

Inoltre può essere utile una ricerca del malware effettuata su chat GPT che mi fornirà alcune informazioni sul malware. La risposta che mi è stata fornita è la seguente:

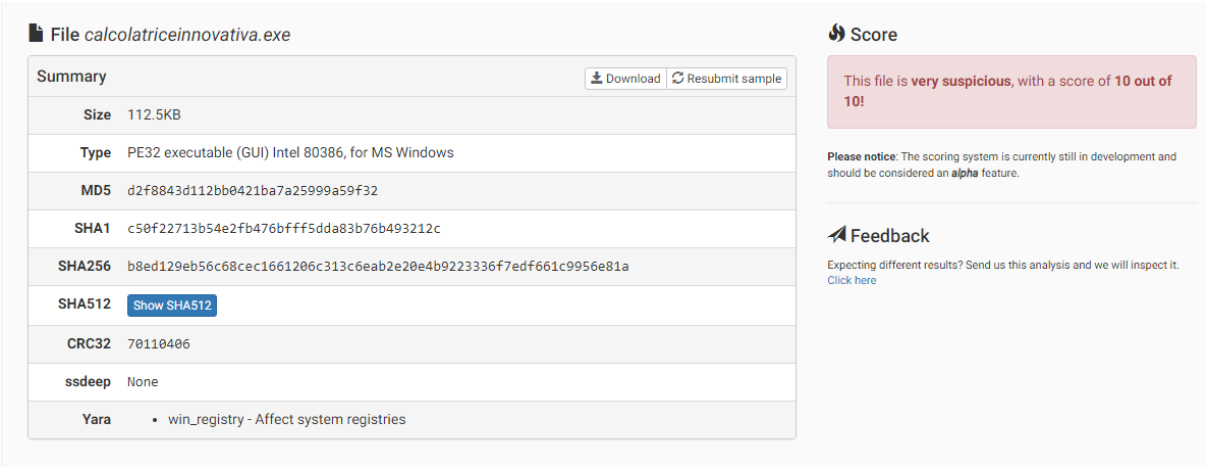
> Se il file sospetto è **calcolatriceinnovativa.xls**, si tratta di un file Excel, non di un eseguibile. Tuttavia, anche i file Excel possono contenere malware, in particolare attraverso **macro** o **codice VBA (Visual Basic for Applications)**, che possono essere utilizzati per eseguire codice malevolo quando il file viene aperto.

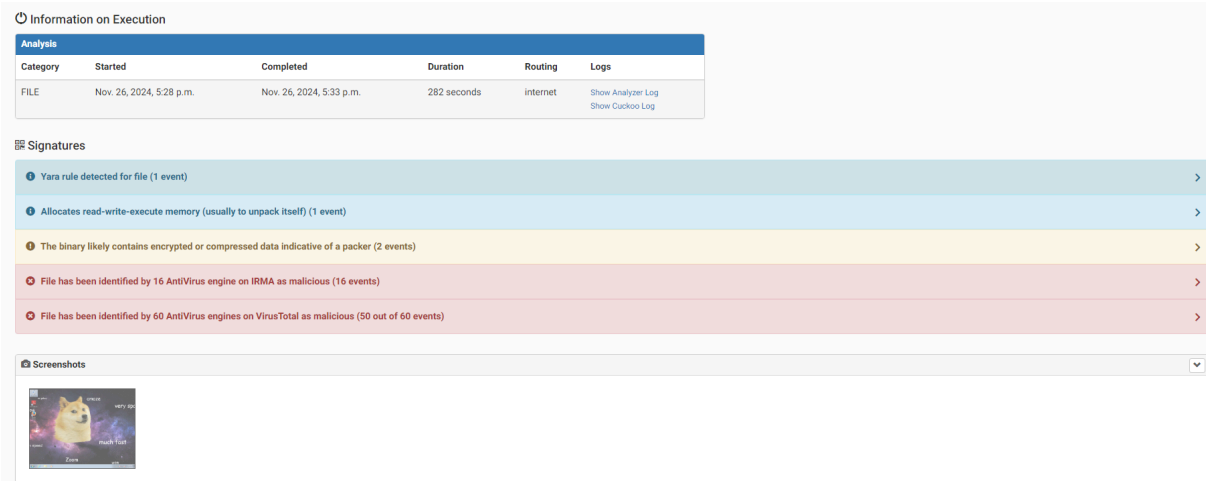
Analisi Dinamica

Per analisi dinamica si intende l'analisi del malware tramite esecuzione in un ambiente sicuro ed isolato.

Per eseguirla è stato utilizzato lo strumento **Cuckoo**, si tratta di una sandbox open source, ovvero crea un ambiente protetto per l'esecuzione di un malware per monitorarne il comportamento, determinare se si tratta di un malware e soprattutto quali azioni esegue sul sistema.

Tramite l'esecuzione su Cuckoo possiamo rilevare un numero molto alto di attività malevole. Di seguito un esempio tra quelle rilevate:





Conclusioni

La Malware Analysis è una disciplina fondamentale nel campo della sicurezza informatica, si concentra sull'identificazione, comprensione e gestione delle minacce informatiche. Il processo si divide fondamentalmente in due tipologie di analisi: statica e dinamica.

L'analisi statica implica l'ispezione del codice del malware senza eseguirlo. Vengono utilizzati strumenti come disassemblatori e decompilatori per esaminare il comportamento del malware a livello di codice, alla ricerca di pattern, funzioni sospette o exploit conosciuti.

L'analisi dinamica, invece, comporta l'esecuzione del malware in un ambiente controllato, come una sandbox, per osservare il suo comportamento durante l'esecuzione, monitorando interazioni con il file system, il registro di sistema, la rete e i processi. Strumenti come Cuckoo Sandbox sono essenziali per raccogliere informazioni e tracciare attività sospette.

In conclusione, la malware analysis è una parte essenziale della difesa informatica moderna. Consente non solo di rilevare e rimuovere minacce esistenti, ma anche di migliorare le difese proattive contro attacchi futuri, fornendo preziose informazioni su come i malware agiscono e come possono essere prevenuti. L'approccio combinato tra analisi statica e dinamica, supportato da strumenti avanzati, è fondamentale per garantire una risposta efficace contro le minacce informatiche in continua evoluzione.

Progetto a cura di
Sonia Laterza