Malware analysis

La **malware analysis** è un processo fondamentale nel campo della cybersecurity che consiste nell'**analizzare a fondo software dannosi** (malware) per comprenderne il funzionamento, l'obiettivo e le modalità di diffusione.

Perché è importante?

- **Prevenzione:** Capendo come agisce un malware, è possibile sviluppare difese più efficaci e prevenire future infezioni.
- **Rimozione:** L'analisi permette di identificare e rimuovere il malware in modo sicuro ed efficace.
- **Indagini:** Aiuta a risalire all'origine dell'attacco e a identificare i responsabili.
- **Miglioramento dei sistemi di sicurezza:** I dati raccolti durante l'analisi contribuiscono a migliorare i software antivirus e i sistemi di rilevamento delle intrusioni.

Analisi statica

L'analisi statica è una tecnica fondamentale nella sicurezza informatica che permette di esaminare un file sospetto (come un eseguibile, un documento o uno script) senza effettivamente eseguirlo. Questo approccio offre diversi vantaggi, tra cui:

- **Sicurezza:** Evita di attivare il malware, riducendo il rischio di infezione del sistema.
- **Rapidità:** Molte analisi possono essere automatizzate, consentendo di esaminare un gran numero di file in poco tempo.

L'analisi statica si basa sull'esame del codice binario o del codice sorgente (se disponibile) del file. Le tecniche utilizzate includono:

- **Ispezione visiva:** Un analista esperto può individuare pattern sospetti, stringhe indicative di malware (come URL malevoli, nomi di file comuni ai malware) o strutture di codice tipiche delle minacce.
- **Disassemblaggio:** Il codice macchina viene convertito in un formato più leggibile (assembly) per facilitarne l'analisi.
- **Decompilazione:** In alcuni casi, è possibile ricostruire parzialmente il codice sorgente originale da un eseguibile compilato.
- **Analisi delle stringhe:** Vengono estratte tutte le stringhe di testo presenti nel file, che possono rivelare informazioni importanti sulle sue funzionalità.

- **Analisi dell'impronta digitale:** Si calcolano hash (come MD5, SHA-1, SHA-256) del file per confrontarlo con database di malware noti.
- **Analisi dell'entropia:** Misura la complessità del file e può aiutare a identificare file compressi, offuscati o crittografati.

Analisi dinamica

L'**analisi dinamica** è una tecnica fondamentale nella cibersicurezza che permette di studiare il comportamento di un software o di un sistema informatico mentre è in esecuzione. In altre parole, è come mettere un programma sotto una lente d'ingrandimento e osservarlo mentre svolge le sue funzioni, per capire esattamente cosa fa e come lo fa.

Perché è importante nell'ambito della cybersicurezza?

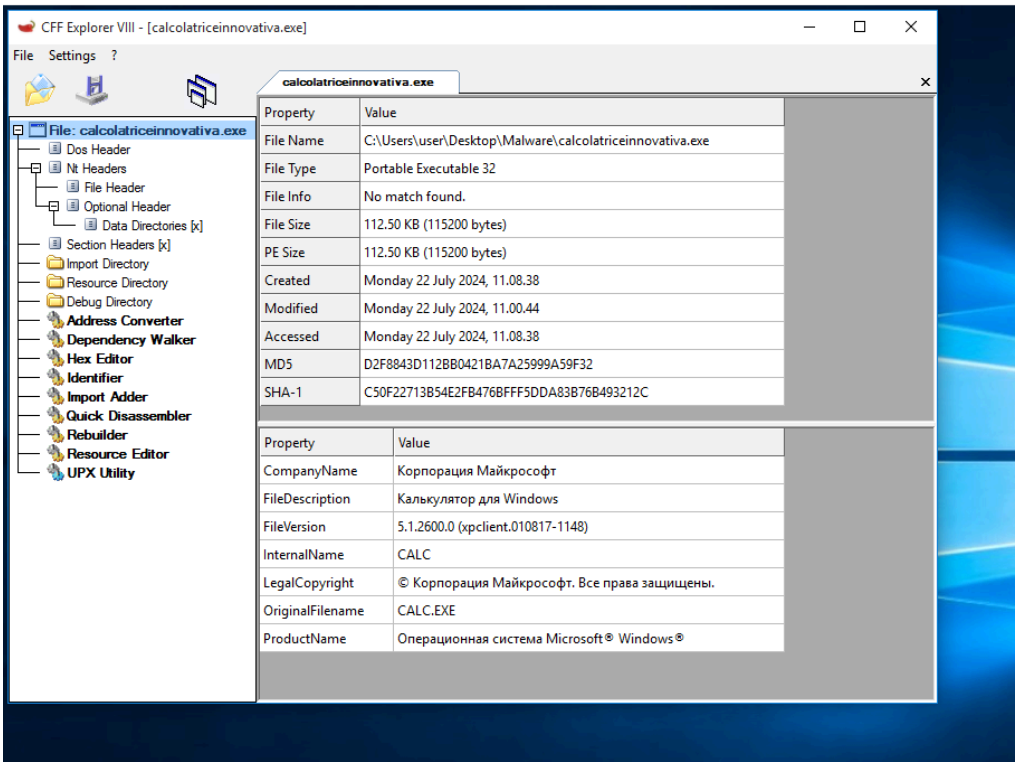
Identificazione di malware: Permette di individuare comportamenti sospetti e dannosi tipici dei malware, come la comunicazione con server esterni, la modifica di file di sistema o l'esecuzione di comandi sospetti.

Rilevamento di vulnerabilità: Simulando attacchi reali, si possono scoprire vulnerabilità nel software che potrebbero essere sfruttate da hacker.

Analisi di rootkit: I rootkit sono malware che si nascondono nel sistema operativo per evitare di essere rilevati. L'analisi dinamica permette di individuare le loro tracce e capire come operano.

Valutazione delle contromisure: Si possono testare l'efficacia di firewall, antivirus e altri strumenti di sicurezza, verificando se riescono a bloccare attacchi e malware.

Analisi con **Eff Explorer**



Analizziamo i dati più importanti presenti nell'immagine:

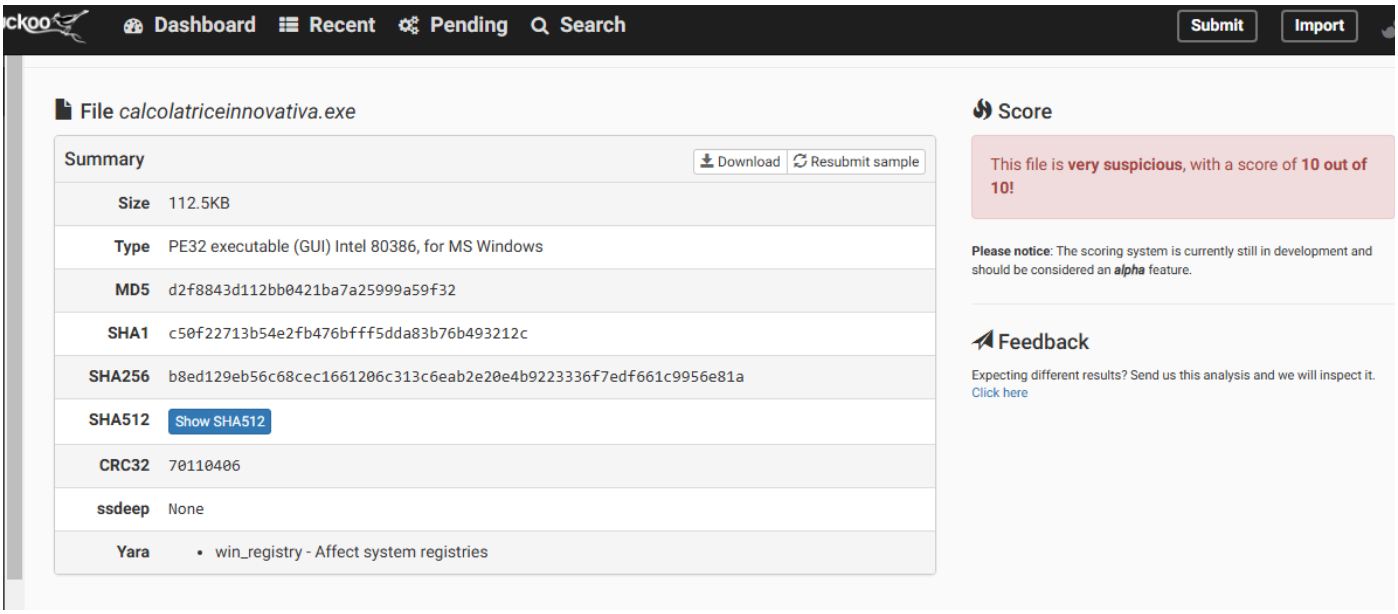
- **Nome file:** "calcolatriceinnovativa.exe". Questo è il nome assegnato al file.
- **Percorso:** "C:\Users\User\Desktop\Malware\calcolatriceinnovativa.exe". Indica la posizione del file sul disco rigido.
- **Tipo di file:** "Portable Executable 32". Questo indica che si tratta di un programma eseguibile a 32 bit per sistemi Windows.
- **Dimensioni del file:** 112.50 KB. Indica la dimensione totale del file in kilobyte.
- **Data di creazione, modifica e accesso:** Mostrano rispettivamente quando il file è stato creato, modificato e l'ultima volta che è stato aperto.
- **Hash MD5 e SHA-1:** Sono delle "impronte digitali" uniche del file. Se il file viene modificato, anche questi valori cambieranno.
- **Informazioni sulla società:** "Корпорация Майкрософт" (in italiano: "Corporazione Microsoft"). Indica che il file è stato creato da Microsoft però in lingua russa.
- **Descrizione del file:** "Калькулятор для Windows" (in italiano: "Calcolatrice per Windows"). Descrive la funzione del programma.
- **Versione del file:** "5.1.2600.0". Indica la versione del software.
- **Nome interno:** "CALC". È il nome interno del programma, spesso utilizzato nei sistemi operativi.

Cosa ci dicono questi dati?

A prima vista, il file sembra essere una semplice calcolatrice per Windows creata da Microsoft. Tuttavia, ci sono alcuni elementi che potrebbero far sorgere dei dubbi:

- **Informazioni contraddittorie:** Una calcolatrice non dovrebbe andare su internet ne scaricare dati.
- **Nome del file:** il nome del file è calcolatrice Corporazione Microsoft, se era davvero di Microsoft non doveva essere scritta in russo.

Cuckoo sandbox



Spiegazione dettagliata dei dati presentati:

- **File calcolatriceinnovativa.exe:** Questo è il nome del file analizzato.
- **Score:** Il punteggio di questo file è di 10 su 10, il che indica un livello di sospetto molto alto. Un punteggio elevato suggerisce che il file potrebbe essere un malware (virus, trojan, ecc.).
- **Summary:**Questa sezione fornisce un riassunto delle caratteristiche principali del file.
  - **Size:** La dimensione del file è di 112,5 KB.
  - **Type:** Il tipo di file è un eseguibile PE32 (Portable Executable) per sistemi Windows a 32 bit.
  - **MD5, SHA1, SHA256, SHA512, CRC32, ssdeep:** Sono degli hash, ovvero delle impronte digitali uniche del file. Questi valori vengono utilizzati per identificare in modo univoco il file e per verificare se una copia del file è stata modificata.
  - **Yara:** Indica che il file ha attivato alcune regole Yara, che sono delle firme utilizzate per identificare malware. In questo caso, la regola attivata è "win_registry", che suggerisce che il file potrebbe interagire con il registro di sistema di Windows, un'azione tipica dei malware.

Cosa significano questi risultati?

In base all'analisi, il file "calcolatriceinnovativa.exe" presenta un rischio molto elevato di essere un malware. Il punteggio elevato, le caratteristiche del file e le regole Yara attivate supportano questa conclusione.

In conclusione

L'analisi del malware rivela un panorama minaccioso in continua evoluzione. I malware, sempre più sofisticati e adattativi, richiedono un approccio multidisciplinare e strumenti all'avanguardia per essere identificati e neutralizzati. L'analisi dinamica e statica, combinate con l'intelligenza artificiale, rappresentano strumenti indispensabili per affrontare questa sfida. Tuttavia, la corsa all'innovazione tra attaccanti e difensori è costante, rendendo fondamentale il continuo aggiornamento delle conoscenze e delle tecnologie.