Analisi Malware

Dato un file eseguibile di nome **calcolatriceinnovativa.exe** lo andremo ad analizzare seguendo 3 step principali: analisi preliminare, analisi statica, analisi dinamica.

Analisi preliminare

Per analisi preliminare si intende confrontare il codice hash del file su siti come Virus Total, Malware Bazaar, il primo basato su motori antivirus e analisi comportamentale, mentre Malware Bazaar è un archivio di malware utile per ricerche approfondite e sviluppo di strumenti di rilevamento.

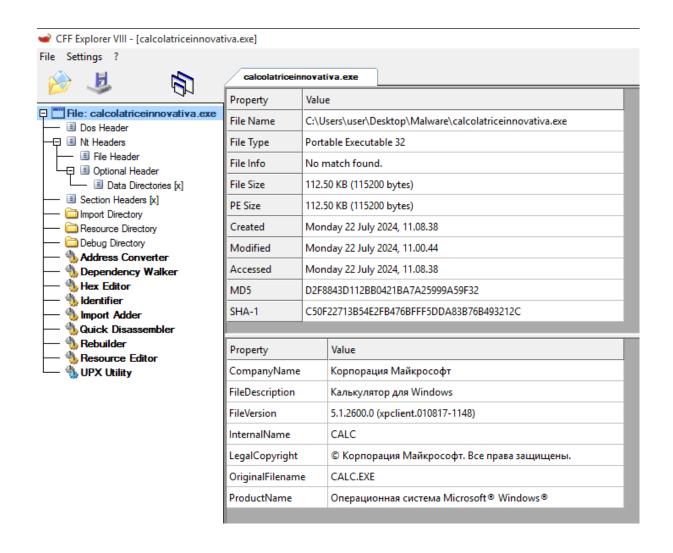
Analisi statica/ dinamica

L'analisi statica e l'analisi dinamica sono due modi diversi di studiare un malware ma si completano a vicenda.

L'analisi statica(CFF Explorer, ProcMon) consiste nell'esaminare il malware **senza eseguirlo**. Si analizza il file binario o il codice sorgente (se disponibile) per raccogliere informazioni.

L'analisi dinamica prevede invece l'esecuzione del malware in un ambiente controllato (sandbox) per osservare il suo comportamento in tempo reale.

Per iniziare bisognerebbe innanzitutto contestualizzare quello che dovrebbe effettivamente andare a fare il file una volta eseguito, come nel nostro caso se vediamo che calcolatriceinnovativa.exe dovrebbe essere una calcolatrice ma con un'analisi dettagliata vedo che accede ai registri di windows per modificare dei parametri sospetti,già li si accende un campanello di allarme.



Con strumenti come **CFF Explorer** puoi esplorare il cuore del file, scoprendo le **sezioni** che contengono codice, dati o risorse. Se trovi sezioni con nomi strani o dimensioni sospette, potrebbe essere un ulteriore segnale di allarme.

L'analisi statica è sicura perché non esegue nulla, ma ha dei limiti: se il malware usa tecniche di offuscamento o crittografia per nascondere le sue funzioni, potresti non riuscire a capirne il comportamento.

Da qui infatti per completare tutto il quadro di analisi entra in gioco l'analisi dinamica (Cuckoo) durante l'esecuzione, osservi cosa fa il malware in tempo reale. Ad esempio, controlli se crea nuovi file, modifica chiavi di registro, avvia processi sospetti o cerca di connettersi a indirizzi IP o domini. È qui che il malware "mostra le sue carte", rivelando come agisce per infettare un sistema o rubare dati. Questo ti permette di capire l'impatto che avrebbe su un sistema reale. L'analisi dinamica è molto utile, ma non è priva di sfide. Alcuni malware sono progettati per rilevare quando sono in una sandbox e nascondere il loro comportamento per non essere scoperti.

| | | | | , |
|---|--|--|--|--|
| Affect system registries | | rule | win_registry | |
| unpack itself) (1 event) | | | | , |
| Arguments | | Status | Retu | urn Repeated |
| process_identifier: 230 rstpot_alize 4099 stank_cfep_typass; 0 heap_den_bypass; 0 heap_den_bypass; 0 protection: e4_fORGE_EXECUTE_READWRITE) base_address_track_come allocation_type_4096_(MEM_COMMIT) process_handle: 0xffffffff | | 1 | θ | 0 |
| sed data indicative of a packer (2 events) | | | | ` |
| ddress': u'0x00001000', u'entropy': 6.863688338632866, u'name': u'.text', u'virtual_size': u'0x000126b0') | entropy | 6.86368833863 | description | A section with a high entropy has been found |
| | description | Overall entropy of this PE file is high | | |
| | unpack itself) (1 event) Arguments process_identifier_220 region_size_4896 stack_dep_Uppass_0 stack_dep_Uppass_0 teack_pivoted_0 heap_dep_Uppass_0 protection_of_(PAGE_EXECUTE_READWRITE) base_address_toxeo_20080e0 allocation_type_4866 (MEM_COMMIT) | Arguments process_identifier: 228 region_size. 4996 stack_dep_bypass: 0 stack_protest heap_ct_bypass: 0 heap_ct_bypass: | Arguments Status Process_identifier; 228 region_size. 4996 statek_dep_Lypass: 0 statek_pivotes: 0 hesp_dep_Lypass: 0 statek_pivotes: 0 hesp_dep_Lypass: 0 statek_dep_Lypass: 0 statek_pivotes: 0 hesp_dep_Lypass: 0 h | Arguments Status Ret process_identifier;228 region_size: 4996 statck_dep_typass: 0 statck_protes: 0 heap_tep_typass: 0 statck_protes: 0 lines: 0 l |

Conclusione

in conclusione possiamo dire che l'analisi statica ti dà una prima idea di come il malware è costruito e cosa potrebbe fare, mentre l'analisi dinamica ti mostra cosa fa davvero quando viene eseguito. Entrambe sono fondamentali per capire e contrastare le minacce informatiche.