

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 VirusTotal, 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 lì si accende un campanello di allarme.

CFF Explorer VIII - [calcolatriceinnovativa.exe]

File Settings ?

calcolatriceinnovativa.exe

File: calcolatriceinnovativa.exe

- Dos Header
- Nt Headers
 - File Header
 - Optional Header
 - Data Directories [x]
 - Section Headers [x]
- Import Directory
- Resource Directory
- Debug Directory
- Address Converter
- Dependency Walker
- Hex Editor
- Identifier
- Import Adder
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

Property	Value
File Name	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	112.50 KB (115200 bytes)
PE Size	112.50 KB (115200 bytes)
Created	Monday 22 July 2024, 11.08.38
Modified	Monday 22 July 2024, 11.00.44
Accessed	Monday 22 July 2024, 11.08.38
MD5	D2F8843D112BB0421BA7A25999A59F32
SHA-1	C50F22713B54E2FB476BFFF5DDA83B76B493212C

Property	Value
CompanyName	Корпорация Майкрософт
FileDescription	Калькулятор для Windows
FileVersion	5.1.2600.0 (xpclient.010817-1148)
InternalName	CALC
LegalCopyright	© Корпорация Майкрософт. Все права защищены.
OriginalFilename	CALC.EXE
ProductName	Операционная система Microsoft® Windows®

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.

Signatures

1

Yara rule detected for file (1 event)

description

Affect system registries

rule

win_registry

1

Allocates read-write-execute memory (usually to unpack itself) (1 event)

Time & API

Arguments

Status

Return

Repeated

NTAllocateVirtualMemory

Nov 26, 2024, 4:58 p.m.

process_identifier: 228

region_size: 4896

stack_dep_bypass: 0

stack_pivoted: 0

heap_dep_bypass: 0

protection: 64 (PAGE_EXECUTE_READWRITE)

base_address: 0x00280000

allocation_type: 4096 (MEM_COMMIT)

process_handle: 0xffffffff

1

0

0

1

The binary likely contains encrypted or compressed data indicative of a packer (2 events)

section

{u'size_of_data': u'0x00012800', u'virtual_address': 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

entropy

0.663677130045

description

Overall entropy of this PE file is high

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.