Esercitazione S9/L2

In questa esercitazione ho svolto l'analisi di un malware svolgendo prima una scansione statica poi una dinamica.

Dispositivi / Software utilizzati:

- Windows 10
- CFF Explorer
- VirusTotal
- Cuckoo
- MalwareBazaar

Scansione statica:

Si tratta dell'analisi del malware senza eseguirlo.
Grazie a diversi tool si potrà analizzare il programma (struttura, pattern, hash, metadati ecc.) cercando di comprendere la funzionalità e l'eventuale pericolosità in caso di malware.
Si andranno ad utilizzare diversi software per avere un confronto e approfondire la ricerca.
La scansione statica è parte fondamentale del malware analysis poiché si può analizzare il contenuto del programma, dalle librerie coinvolte al codice dello stesso.
Possono esserci anche dei casi in cui il malware in questione si comporti diversamente in ambienti diversi (in fase di scansione dinamica), con la scansione statica si può ovviare a questo problema.
I software che ho utilizzato per la scansione statica sono: **CFF Explorer, VirusTotal e MalwareBazaar**

Scansione dinamica:

Si tratta dell'analisi del malware eseguendolo in ambiente sicuro (sendbox).
Grazie ad alcuni tool si potrà analizzare il comportamento del malware in esecuzione.
Si può effettuare la scansione dinamica con o senza l'accesso a internet e si andrà a verificare se il programma effettuerà azioni sospette (creazioni di backdoor, esfiltrazione di dati, tentativi di connessione con server esterni ecc.). Dal comportamento del programma si potrà dedurre se si tratta di un malware e di quale tipo si tratta.
In questo caso ho usato **cuckoo** per la scansione dinamica.

La concatenazione delle due scansioni (statica e dinamica) porterà una comprensione più approfondita del malware.

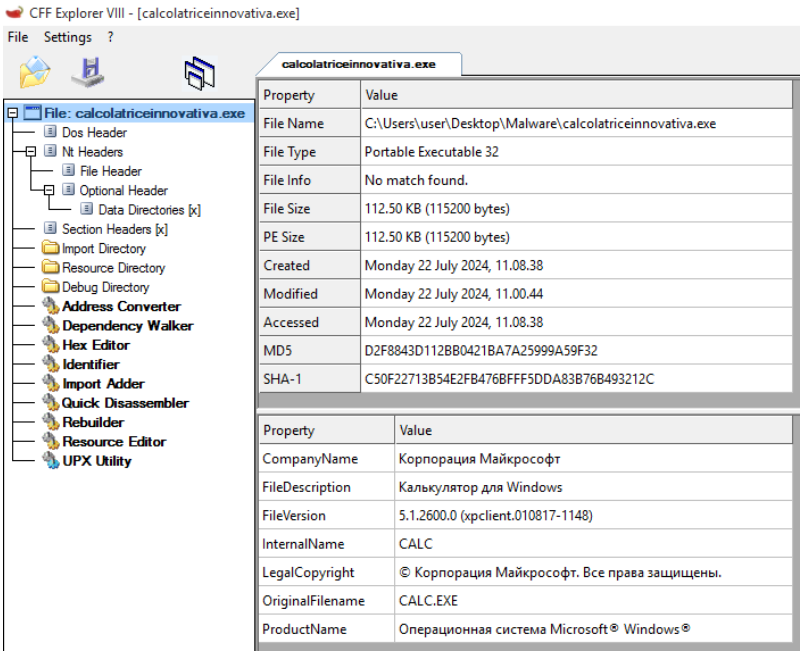
Procedimento:

Per iniziare la procedura di scansione del programma come prima cosa mi sono assicurato di creare un ambiente sicuro e isolato per poter svolgere tutte le attività senza ripercussioni.
Ho quindi clonato una VM di Windows 10 con all'interno i vari tool e il malware da scansionare. Il programma da scansionare si chiama **calcolatriceinnovativa.exe**.

CFF Explorer:

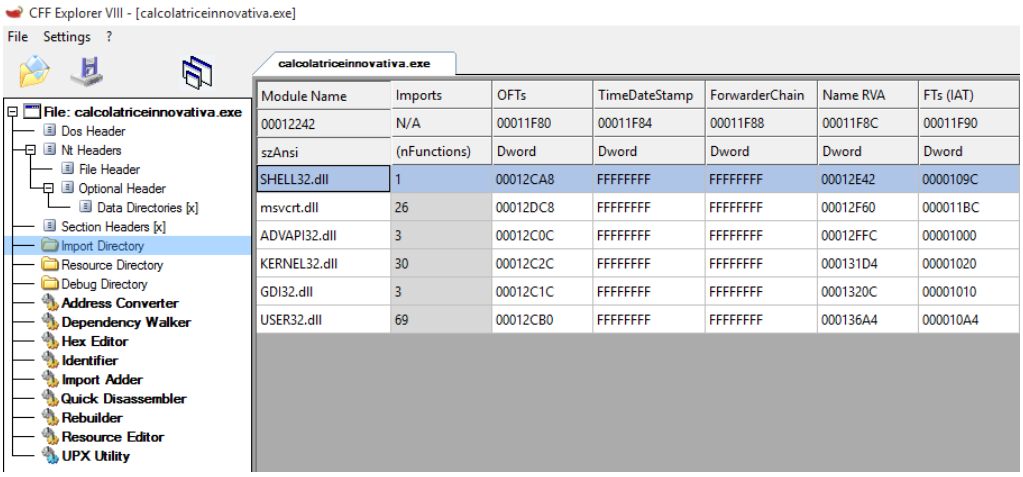
Ho utilizzato CFF Explorer come primo approccio per una scansione statica.

Si può notare dalla foto che questo programma ci restituisce una panoramica del file analizzato, dal percorso del file a una conoscenza del produttore.
Inoltre ci restituisce due codici HASH che permettono il riconoscimento univoco del file. Si può cercare inoltre riscontro sui vari motori di ricerca online per vedere se ci sono ulteriori informazioni in internet.



CFF Explorer, inoltre, ci offre la possibilità di esplorare il file analizzandolo dettagliatamente.
Si possono infatti andare a vedere le sezioni principali del file (dove si trovano il codice eseguibile, dati, configurazioni memorizzate e eventualmente payload), moduli importati, funzioni, librerie e tutto ciò che compone il file.

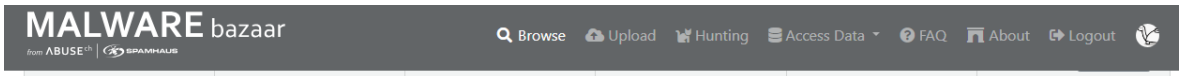
In “Import Directory” si potranno infatti vedere i moduli importati e le funzioni richiamate da quei moduli (oltre ad altre diciture della tabella).
Questo ci permette, conoscendo la funzionalità dei moduli, di capire il funzionamento del programma.



Si tratta di un’importante strumento poiché la conoscenza delle funzioni dei moduli ci potrà suggerire che tipo di azioni andrà a fare il programma eseguendolo.
In questo caso, essendo il programma una calcolatrice, se si troveranno parti che richiamano una connessione ad internet si può dedurre un comportamento anomalo del programma.
Bisogna, infatti, ragionare anche in base a che tipo di programma si sta analizzando per dedurre se si tratti di un malware o meno.

MalwareBazaar:

Ho utilizzato questo sito per avere una più amplia panoramica del file analizzato.
Si tratta di un sito contenente informazioni su malware noti. Si può effettuare sia una ricerca tramite codice HASH sia caricando direttamente il file.
Effettuando l'upload del file mi ha restituito una corrispondenza con un malware già presente nel database e mi ha dato una panoramica sul malware trovato.



SHA256 hash:	b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a
SHA3-384 hash:	b211f60b618a49136d23af49bbfa5cb15d2cebd47b5714e58ec81f0a503eb3c8e5bbb1aefd756d1538f4d922a5944415
SHA1 hash:	c50f22713b54e2fb476bfff5dda83b76b493212c
MD5 hash:	d2f8843d112bb0421ba7a25999a59f32
humanhash:	oranges-freddie-wisconsin-undress
File name:	calcolatriceinnovativa.exe
Download:	download sample
File size:	115'200 bytes
First seen:	2024-11-26 14:00:49 UTC
Last seen:	2024-11-26 14:01:08 UTC
File type:	exe
MIME type:	application/x-dosexec
imphash	08f6a1b121da8cedde2d1089d0906ed8
ssdeep	3072:DAq2By/0He97ulj7nt5CdLYkOEp0AWLnQoXPBsr5ZrR:DAqfB9yBJa7OEp0pLnQoo5Zd
TLSH	T197B39E01BA94F135C465113448D39FFA93BDBF1705AB16AB33097E4F7E362662A23286
TrID	43.3% (.EXE) Win32 Executable MS Visual C++ (generic) (31206/45/13) 22.9% (.EXE) Microsoft Visual C++ compiled executable (generic) (16529/12/5) 9.1% (.DLL) Win32 Dynamic Link Library (generic) (6578/25/2) 7.0% (.EXE) Win16 NE executable (generic) (5038/12/1) 6.2% (.EXE) Win32 Executable (generic) (4504/4/1)
Magika	pebin
dhash icon	0082b4b2cad2ab00 (2 x Kutaki)
Reporter	Pentolino
Tags:	exe

Si può notare i vari codici HASH che mi ha riportato insieme ad un elenco di pericolosità trovate.

Findings

ID	Title	Severity
CHECK_AUTHENTICODE	Missing Authenticode	high
CHECK_DLL_CHARACTERISTICS	Missing dll Security Characteristics (HIGH_ENTROPY_VA)	high
CHECK_NX	Missing Non-Executable Memory Protection	critical
CHECK_PIE	Missing Position-Independent Executable (PIE) Protection	high

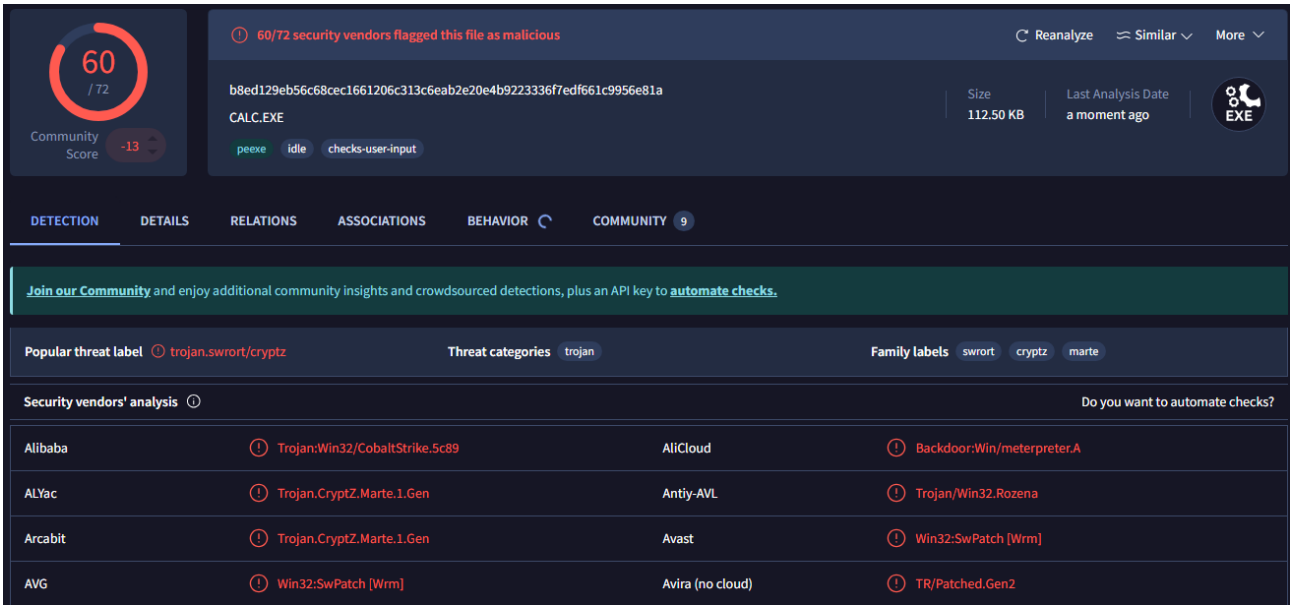
Reviews

ID	Capabilities	Evidence
WIN32_PROCESS_API	Can Create Process and Threads	KERNEL32.dll::CloseHandle KERNEL32.dll::CreateThread
WIN_BASE_API	Uses Win Base API	KERNEL32.dll::LoadLibraryA KERNEL32.dll::GetStartupInfoA KERNEL32.dll::GetCommandLineW
WIN_REG_API	Can Manipulate Windows Registry	ADVAPI32.dll::RegOpenKeyExA ADVAPI32.dll::RegQueryValueExA
WIN_USER_API	Performs GUI Actions	USER32.dll::OpenClipboard USER32.dll::CreateWindowExW

Mi ha inoltre trovato una corrispondenza con shikata ga nai, un encoder per offuscare i malware cercando di renderli meno visibili ai sistemi di sicurezza.

VirusTotal:

Si tratta di un servizio online che permette di analizzare file, URL, domini e indirizzi IP per rilevare malware, URL dannosi e altre attività sospette. Per fare ciò Virustotal utilizza decine di antivirus e strumenti di rilevamento di malware per scansionare il contenuto. Ogni strumento risponde all'analisi richiesta dall'utente e restituirà eventuali rilevamenti trovati.



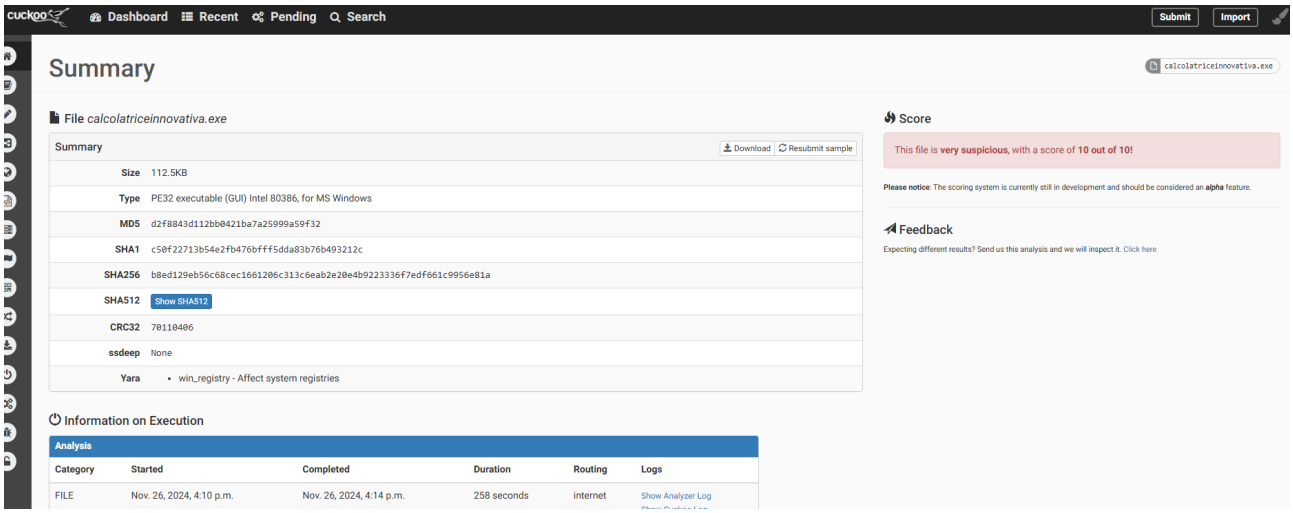
Come si può notare dalla foto il programma analizzato è risultato essere un malware in 60/72 casi. Viene riportato inoltre cosa risulta essere in base alle analisi degli antivirus, la maggior parte riporta la possibilità di un trojan o di una backdoor.

Ci si può anche spostare in altre sezioni per ricevere dettagli più approfonditi eventuali associazioni, e descrizione del malware.

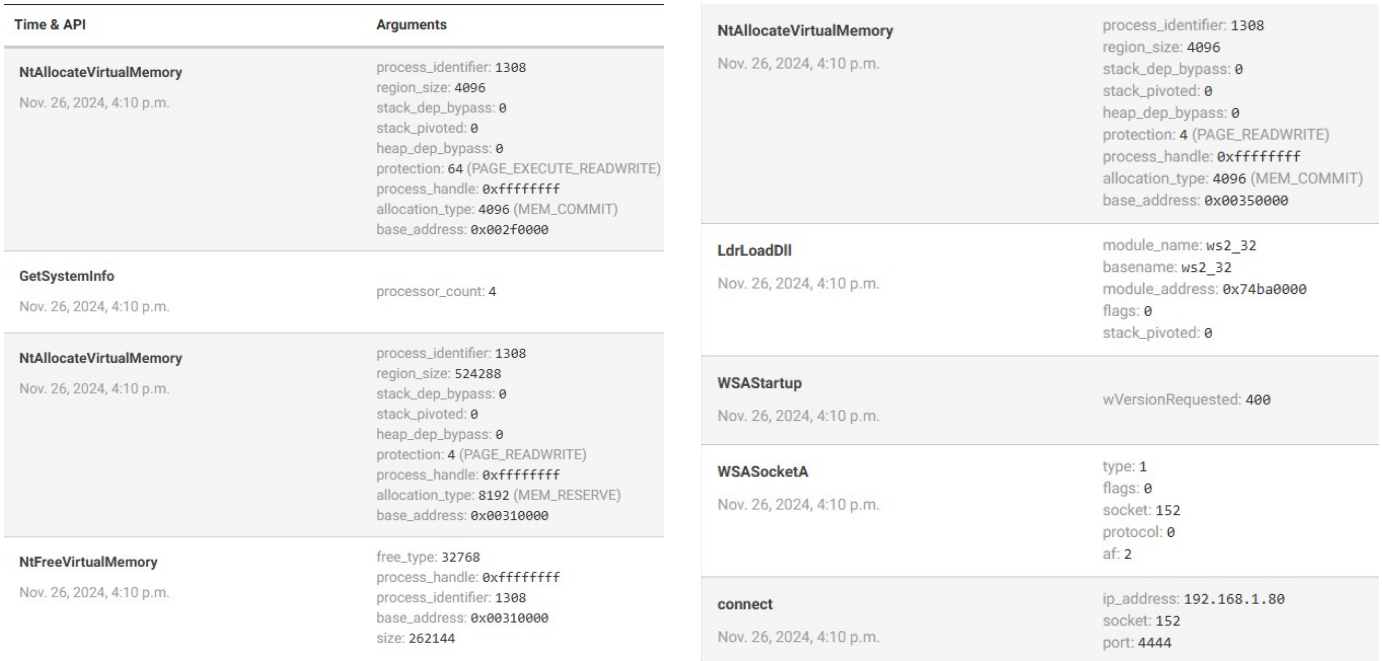
Dopo aver confrontato l'analisi dei 3 precedenti software, si può dedurre che si tratta di un malware, più in particolare una backdoor.
Per concludere la fase di malware analysis si procederà con l'analisi dinamica.

Cuckoo:

Per quest'ultima fase della malware analysis andrò ad utilizzare Cuckoo, un software che permette la scansione dinamica di un programma.
Questo software svolge l'analisi in una sua sandbox (una specie di mini macchina virtuale apposita e sicura) e riscontra i comportamenti del malware.



Ho usato la versione web in questo caso, non differisce comunque il funzionamento.
Si può notare dalla foto precedente che ci mostra (in alto a dx) un punteggio di pericolosità (in questo caso 10/10) oltre ai vari codici HASH,tipo e grandezza del file (al centro)



Ci sono molti dettagli che vengono riportati dal software, ho deciso di riportare questo esempio, si tratta del funzionamento specifico del programma.
Mostra infatti tutte le funzioni richiamate, allocazione di memoria, e infine una connessione con la funzione "connect" che stabilisce, o prova a farlo, una connessione ad un indirizzo specifico, in questo caso 192.168.1.80:4444.

Si può considerare la fase di malware analysis conclusa, e si può stabilire con certezza che si tratta di un malware.