S9L2

Analisi Malware

Oggi procederò con l'analisi di un programma potenzialmente malevolo, utilizzando un approccio strutturato che include due fasi fondamentali dell'analisi dei malware. Questo software prende le sembianze di una calcolatrice e si chiama **calcolatriceinnovativa.exe**:

1. Analisi Statica

L'analisi statica consiste nell'esaminare il codice del programma senza eseguirlo. L'obiettivo è identificare potenziali indicatori di compromissione, come istruzioni sospette, pattern di codice che sfruttano vulnerabilità, o comportamenti anomali.

2. Analisi Dinamica

L'analisi dinamica implica l'esecuzione controllata del programma malevolo in un ambiente isolato e sicuro, come una sandbox o una macchina virtuale appositamente configurata. Questa fase consente di osservare il comportamento effettivo del malware, come la creazione di file, modifiche al registro di sistema, connessioni di rete o altri tipi di attività dannose. L'analisi dinamica permette di ottenere informazioni utili per comprendere gli obiettivi e le tecniche del malware. Seguendo questo approccio combinato, sarà possibile raccogliere dati dettagliati sul programma malevolo, permettendo di valutarne le caratteristiche e l'impatto potenziale in modo più efficace.

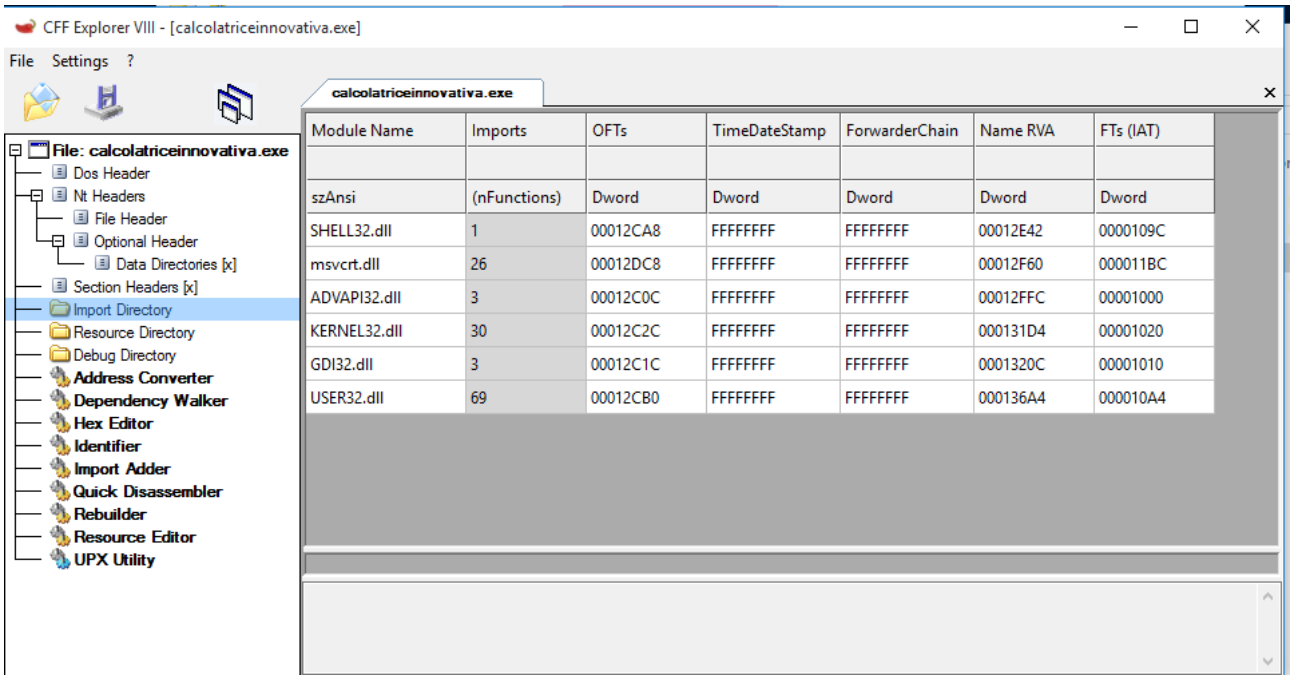
Entrambe le analisi sono divise in due categorie ovvero tra Base e Avanzata. La differenza di tale divisione è che nella statica basica si va ad analizzare ogni pattern all'interno del codice malevolo e nella dinamica avanzata si prova a vedere come reagisce il malware connesso alla connessione internet.

Analisi statica

Come primo passaggio utilizzerò **CFF Explorer**

CFF Explorer è uno strumento utile per analizzare file binari, in particolare eseguibili Windows in formato PE (Portable Executable) come .exe e .dll. Consente di esplorare la struttura interna del file, mostrando dettagli come intestazioni, sezioni, tabelle di importazione (funzioni e librerie usate) e di esportazione (funzioni rese disponibili). Può anche rivelare risorse incorporate come icone, stringhe o immagini.
Include un editor esadecimale per modifiche a basso livello e strumenti per esaminare anomalie strutturali o offuscamenti nel file, utili per identificare comportamenti sospetti. Permette di controllare certificati digitali e debug information per capire l'origine del file. Grazie a queste funzionalità, è prezioso per l'analisi di malware, aiutando a individuare dipendenze sospette o comportamenti potenzialmente dannosi, il tutto senza eseguire il programma.

In questo caso utilizzerò CFF explorer per visionare le librerie che utilizzerà la nostra calcolatrice.

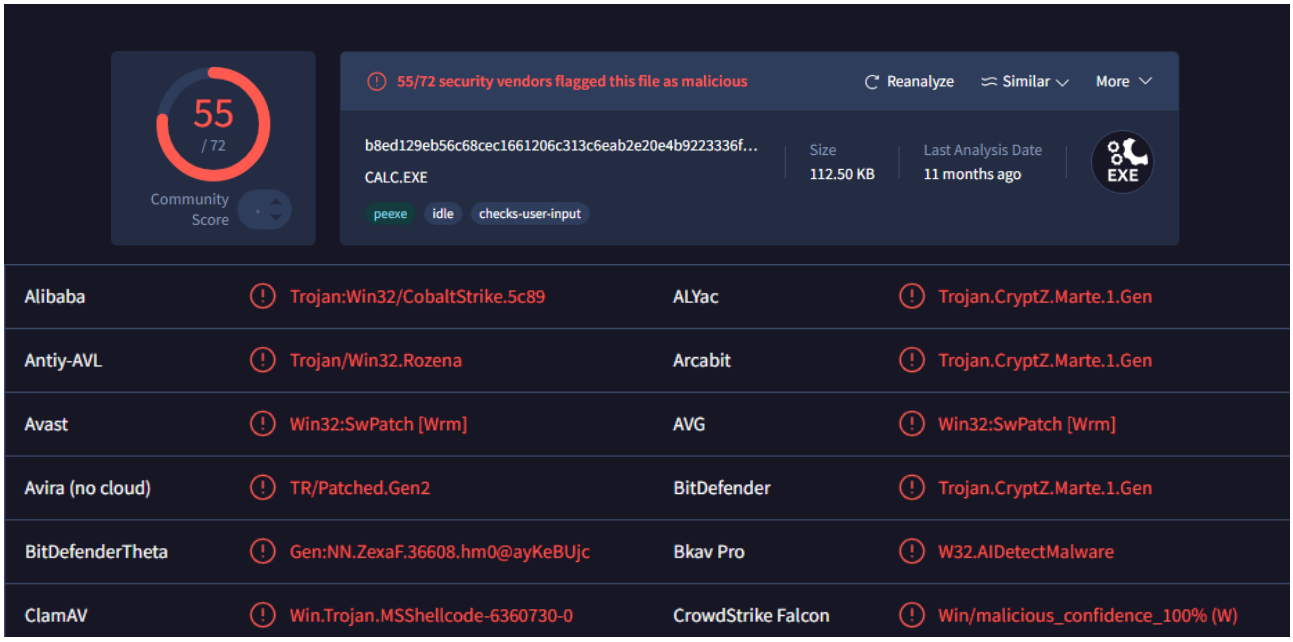


Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
SHELL32.dll	1	00012CA8	FFFFFFFF	FFFFFFFF	00012E42	0000109C
msvcrt.dll	26	00012DC8	FFFFFFFF	FFFFFFFF	00012F60	000011BC
ADVAPI32.dll	3	00012C0C	FFFFFFFF	FFFFFFFF	00012FFC	00001000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

Già dalla schermata iniziale di CFF Explorer ho ottenuto un primo indizio significativo: perché un programma apparentemente innocuo, come una calcolatrice, dovrebbe utilizzare librerie che permettono di modificare o creare chiavi di registro, oppure di creare o alterare file? Questo comportamento è sospetto, poiché una calcolatrice dovrebbe limitarsi a operazioni matematiche e non necessitare di accesso a risorse critiche del sistema. La presenza di tali librerie potrebbe indicare funzionalità nascoste o comportamenti malevoli progettati per compromettere il sistema.

Come secondo passaggio, calcolerò il codice hash del programma e lo analizzerò utilizzando VirusTotal. Questo servizio confronterà l'hash del file sospetto con i database dei principali software anti-malware. Se l'hash corrisponde a quello di un file precedentemente identificato come malevolo, VirusTotal segnalerà la minaccia. Questo metodo consente di verificare rapidamente se il file è stato già classificato come pericoloso, facilitando l'identificazione di malware senza richiedere un'analisi dettagliata iniziale.

Come evidenziato nella schermata sottostante, il software è stato identificato come malevolo, in particolare un **trojan**. Un trojan, abbreviazione di *Trojan horse* (cavallo di Troia), è un tipo di malware che si maschera da programma legittimo o utile per indurre l'utente a eseguirlo. Una volta attivato, il trojan può svolgere attività dannose, come rubare dati sensibili, consentire accesso remoto al sistema o scaricare altri tipi di malware. Questo comportamento rende i trojan particolarmente insidiosi, poiché spesso passano inosservati fino a quando non hanno già causato danni.



Approfondendo le informazioni fornite da VirusTotal, emerge che questo trojan è in realtà una **backdoor**. Una backdoor è una tipologia di malware progettata per fornire accesso remoto non autorizzato al sistema infetto, aggirando le normali misure di sicurezza. Una volta attivato, il software malevolo permette a un attaccante di controllare il dispositivo, potenzialmente eseguendo comandi, rubando dati o installando ulteriori malware, rendendo il sistema altamente vulnerabile.

Analisi Dinamica

Il primo passaggio dell'analisi dinamica sarà l'utilizzo di un software come **Cuckoo**, che offre una sandbox sicura per testare il malware. In questa sandbox, il programma sospetto potrà essere eseguito senza rischiare di compromettere il sistema reale. Al termine del test, Cuckoo genererà un report dettagliato sul comportamento del malware, evidenziando attività come modifiche al file system, chiavi di registro alterate, connessioni di rete e altri comportamenti potenzialmente dannosi. Questo approccio permette di analizzare in sicurezza gli effetti del malware.

Nella schermata sottostante si può osservare che il programma della calcolatrice esegue una serie di operazioni sospette. In primo luogo, alloca memoria e utilizza il comando **GetSystemInfo** per raccogliere informazioni sul sistema su cui è in esecuzione. Successivamente, richiama la libreria **LdrLoadDll**, seguita dai comandi **WSAStartup**, **WSASocketA** e **connect.** Questi ultimi vengono utilizzati per stabilire una connessione con l'indirizzo IP 192.168.1.80/24, sulla porta 4444. Questo comportamento è tipico di malware che stabiliscono comunicazioni non autorizzate per trasferire dati o ricevere comandi da un attaccante remoto.

Time & API	Arguments	Status	Return	Repeated
NtAllocateVirtualMemory Nov. 26, 2024, 4:09 p.m.	process_identifier: 2836 region_size: 4096 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 protection: 64 (PAGE_EXECUTE_READWRITE) process_handle: 0xffffffff allocation_type: 4096 (MEM_COMMIT) base_address: 0x003f0000	1	0	0
GetSystemInfo Nov. 26, 2024, 4:09 p.m.	processor_count: 4	1	0	0
NtAllocateVirtualMemory Nov. 26, 2024, 4:09 p.m.	process_identifier: 2836 region_size: 1048576 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 protection: 4 (PAGE_READWRITE) process_handle: 0xffffffff allocation_type: 8192 (MEM_RESERVE) base_address: 0x007a0000	1	0	0
NtFreeVirtualMemory Nov. 26, 2024, 4:09 p.m.	free_type: 32768 process_handle: 0xffffffff process_identifier: 2836 base_address: 0x007a0000 size: 786432	1	0	0
LdrLoadDll Nov. 26, 2024, 4:09 p.m.	module_name: ws2_32 basename: ws2_32 module_address: 0x75890000 flags: 0 stack_pivoted: 0	1	0	0
WSAStartup Nov. 26, 2024, 4:09 p.m.	wVersionRequested: 400	1	0	0
WSASocketA Nov. 26, 2024, 4:09 p.m.	type: 1 flags: 0 socket: 152 protocol: 0 af: 2	1	152	0
connect Nov. 26, 2024, 4:09 p.m.	ip_address: 192.168.1.80 socket: 152 port: 4444		4294967295	0

Considerazioni finali

Dopo l'analisi dinamica, si può affermare che il programma **calcolatriceinnovativa.exe** è effettivamente un malware contenente un **trojan**, progettato per stabilire una comunicazione con una macchina esterna. Tuttavia, come si evince dall'indirizzo IP utilizzato, la comunicazione non è diretta verso l'esterno della rete, ma verso l'interno. Infatti, nell'ultima fase del test, ho configurato la macchina **Kali Linux** con l'indirizzo IP **192.168.1.80/24** e l'ho messa in ascolto utilizzando un exploit tramite **msfconsole**. Questo exploit ha attivato una **shell Meterpreter**, che, sfruttando il trojan, mi ha permesso di eseguire comandi sulla macchina target in remoto. Questo comportamento conferma la natura malevola del software, in grado di compromettere e controllare la macchina infetta.