Analisi del Malware

Oggi si analizzerà un Malware chiamato **calcolatrice innovativa.exe.**
Per prima cosa creiamo un ambiente sicuro dove inserire l'eseguibile ritenuto malevolo, utilizzeremo una macchina virtuale Windows 10.
Questo ci permette di creare un posto dove mettere e testare file sospetti senza infettare altri dispositivi.

Eseguiremo dei passaggi fondamentali per capire se contiene codice malevolo
Dopo una ricerca su internet

STEP 1 - Analisi Statica di base: esame del codice senza eseguirlo (metadati, struttura del file, stringhe, chiamate sospette)

STEP 2 - Analisi Dinamica di base: si esegue il malware per monitorare le azioni che compie senza connessione a internet

STEP 3 - Analisi Statica avanzata: Decompilazione del codice, analisi pattern (modo in cui ragiona, come si muove, il suo scopo etc)

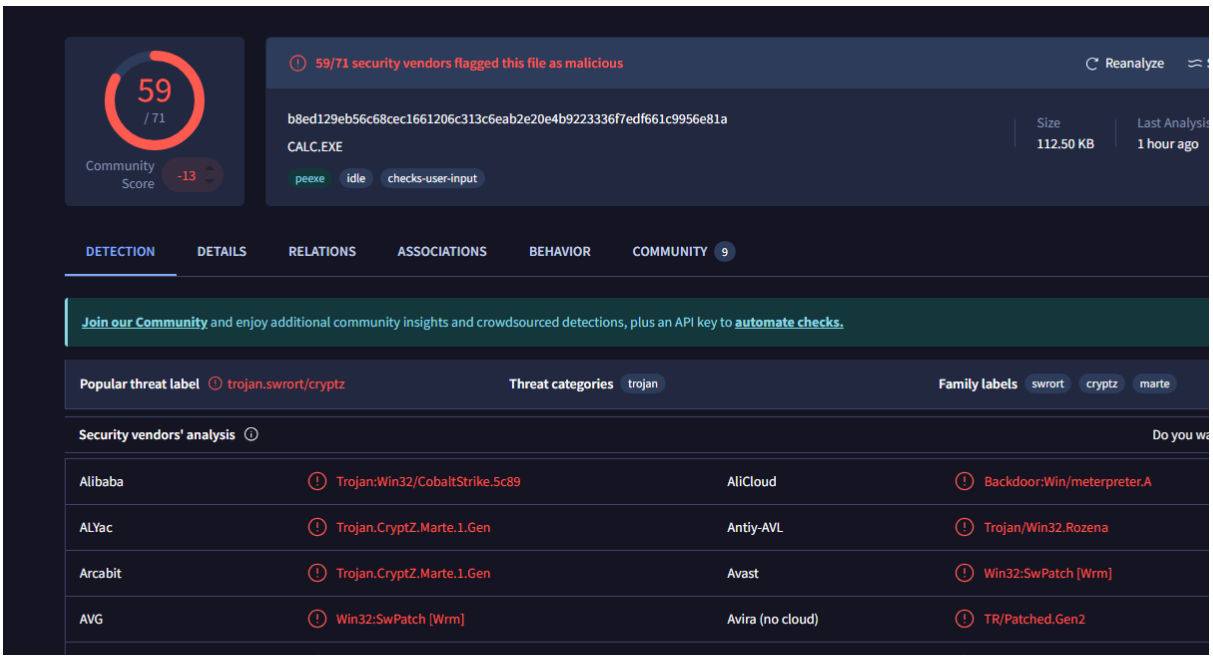
STEP 4 - Analisi Dinamica avanzata: viene eseguito ma con connessione a internet, rileva le capacità avanzate di eseguire operazioni remote o comunicazione con altri nodi della rete

Si utilizzano i seguenti siti web per verificare la presenza di una componente malevola **(STEP 1)**

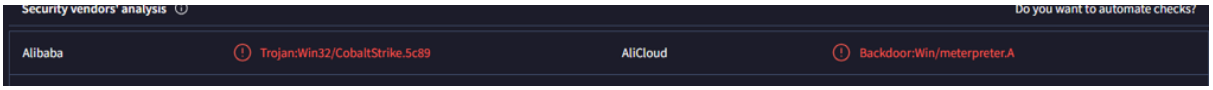
VirusTotal: E' una piattaforma online che permette di analizzare file sospetti confrontando il codice hash (MD5, SHA-1, SHA-256) con i database di numerosi antivirus e antimalware tra i più popolari. Questo processo aiuta a individuare eventuali minacce alla sicurezza, come malware, virus o altri file dannosi.

CFF EXPLORER: Uno strumento avanzato per analizzare file eseguibili e verificare eventuali interazioni sospette con il sistema operativo, inclusi i registri di Windows. Ideale per esperti di sicurezza informatica e analisti di malware, consente di ispezionare la struttura interna dei file PE (Portable Executable), visualizzare e modificare sezioni del file, controllare le dipendenze e individuare potenziali manipolazioni o accessi non autorizzati ai registri di sistema.

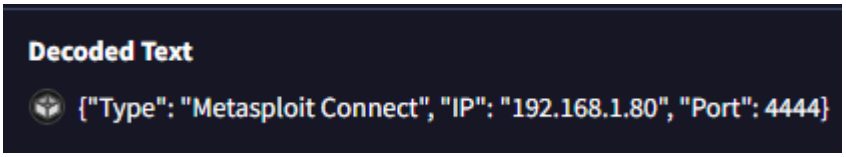
Ecco una immagine di VirusTotal dopo la scansione



Il sito ha trovato 59 compatibilità su 71, questo significa che questo eseguibile è maligno.
Se notiamo il prima riga, quella di Alibaba possiamo notare che il file malevolo potrebbe essere una **BACKDOOR**

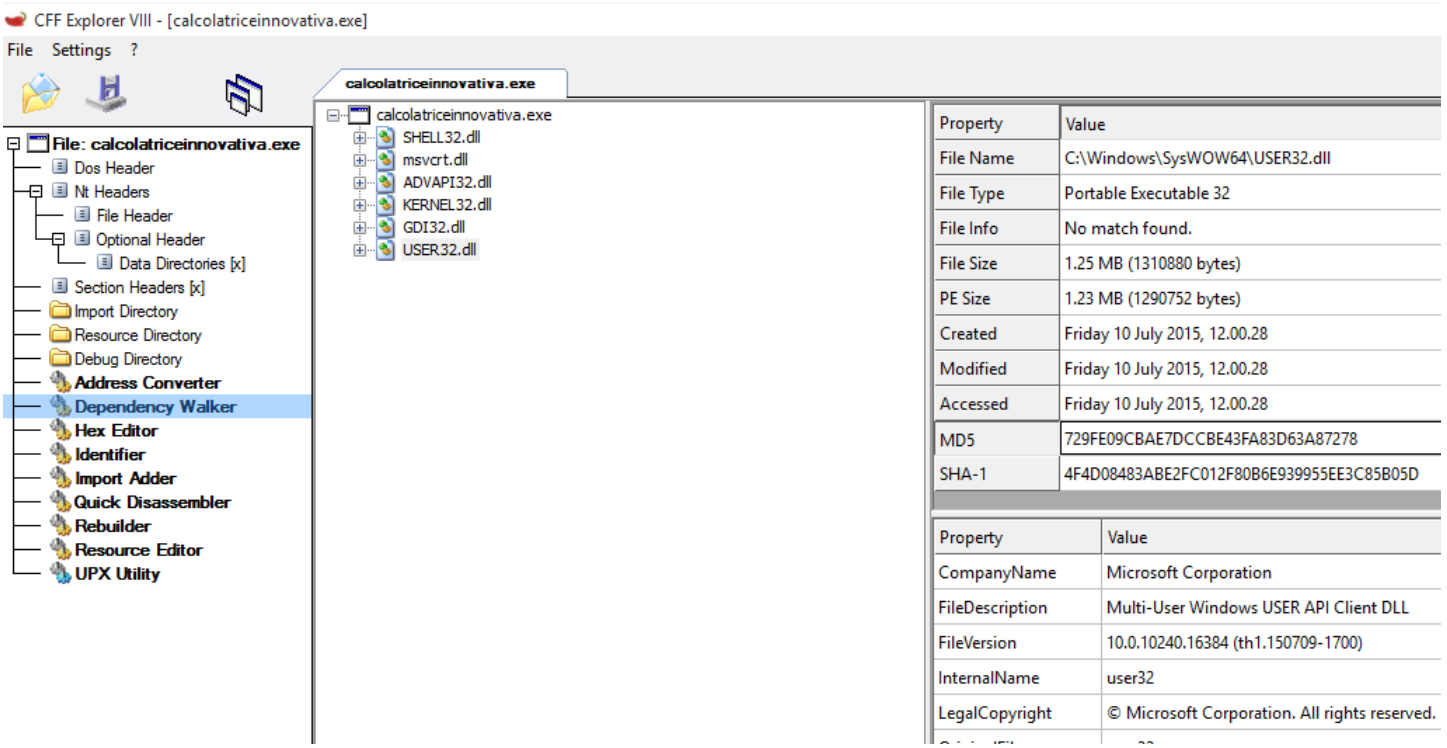


Virus total ci dà un'informazione in più: ci dice cosa potrebbe fare questo Malware



CFF

Con questa immagine possiamo capire quali librerie del sistema operativo, in questo caso Windows, sono state richiamate per eseguire il Malware

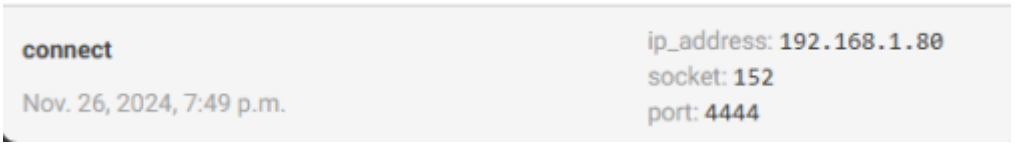


Dopo aver analizzato attentamente e creato un laboratorio sicuro si testa il programma.

PROCMON: Programma utilizzato per capire ed analizzare le interazioni che il malware ha con il sistema operativo in tempo reale.

Time ...	Process Name	PID	Operation	Path	Result	Detail
16:50:...	Explorer.EXE	3792	Thread Create		SUCCESS	Thread ID: 2720
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x71e...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x71e...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x110...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x772...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x110...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x230...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x71e...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x772...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x779...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\shell32.dll	SUCCESS	Image Base: 0x75d...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Image Base: 0x777...
16:50:...	calcolatriceinno...	5100	Thread Create		SUCCESS	Thread ID: 4036
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\windows.stor...	SUCCESS	Image Base: 0x759...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\combase.dll	SUCCESS	Image Base: 0x773...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\rpcrt4.dll	SUCCESS	Image Base: 0x756...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\sspicli.dll	SUCCESS	Image Base: 0x74c...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Image Base: 0x74c...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\bcryptprimitiv...	SUCCESS	Image Base: 0x74c...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x755...
16:50:...	calcolatriceinno...	5100	Thread Create		SUCCESS	Thread ID: 4552
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x77b...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x74c...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x74d...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\user32.dll	SUCCESS	Image Base: 0x752...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\kernel.appco...	SUCCESS	Image Base: 0x755...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\SHCore.dll	SUCCESS	Image Base: 0x758...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\powrprof.dll	SUCCESS	Image Base: 0x757...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\profapi.dll	SUCCESS	Image Base: 0x755...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\imm32.dll	SUCCESS	Image Base: 0x752...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\msctf.dll	SUCCESS	Image Base: 0x775...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	Image Base: 0x773...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\nsi.dll	SUCCESS	Image Base: 0x752...
16:50:...	calcolatriceinno...	5100	Load Image	C:\Windows\SysWOW64\mswsock.dll	SUCCESS	Image Base: 0x73d...

Quando avviamo il programma malevolo, senza interazioni con internet, si attiva, crea un socket e cerca di collegarsi con un indirizzo ip ed una porta designata



Un possibile attaccante rimane in ascolto e potrebbe ricevere informazioni o ancora peggio entrare nella macchina e prenderne il controllo.

Con l’utilizzo di una macchina Kali e di Metasploit si testa l'efficienza del malware.

Come si può notare la connessione è avvenuta con successo, da qui un possibile attaccante potrebbe fare la scalate di privilegi ed aggiungerci backdoor o prendere il controllo.

Considerazioni

I file sospetti devono essere analizzati e testati in ambienti sicuri per evitare un possibile attacco informatico, non bisogna scaricare file da siti non sicuri e prestare attenzione a possibili email di phishing.

Per analizzare un Malware ci vuole tempo ed esperienza, ci si deve far domande sul funzionamento del file come in questo caso, **la calcolatrice perché dovrebbe comunicare con l’esterno?, perchè ci sono poche librerie inerenti alla calcolatrice?, perchè un dipendente ha scaricato una calcolatrice invece di utilizzare quella già presente nel sistema?.**

Dopo questi procedimenti si lavora per non far causare di nuovo un possibile attacco mettendo delle restrizioni aggiungendo regole più severe sui Firewall e fare corsi sull’ingegneria sociale ai dipendenti.