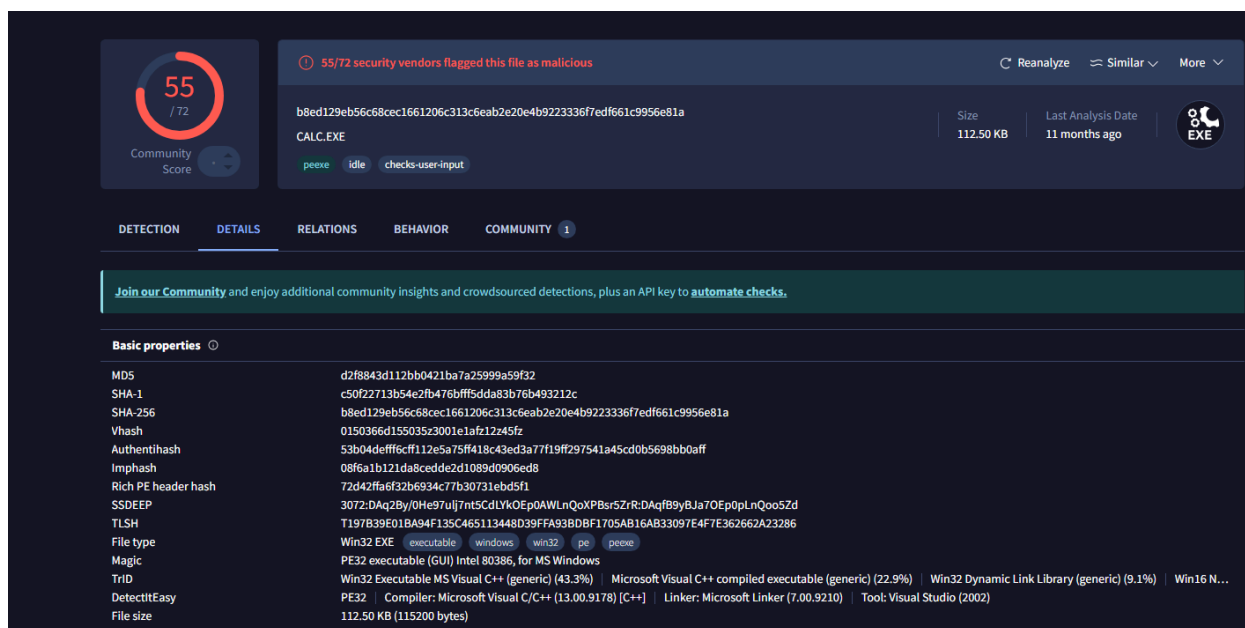


## ANALISI MALWARE

In questo scenario andremo ad analizzare un malware presente sulla macchina WIN 10 Pro, in particolar modo andremo ad effettuare l'**analisi statica** tramite *Virus Total*, *Malware Bazaar* e per avere maggiori dettagli utilizzeremo *CFF EXPLORER*, per quanto riguarda invece l'**analisi dinamica** andremo ad utilizzare *Cuckoo Sandbox* (<https://cuckoo.cert.ee/>) per eseguire il malware e vederne il comportamento.

### FASE 1 - Analisi con Virus Total

In questa fase facciamo un'analisi generale con Virus Total importando il nostro .exe sospetto, Virus Total ci darà delle informazioni generiche che ci possono aiutare a capire in quale categoria appartiene il malware, l'hash con diversi algoritmi (MD5, SHA) e altre informazioni generiche oltre a darci un indicatore di 55 su 72 relativo al fatto che viene riconosciuto come malware da diverse aziende.



55/72 security vendors flagged this file as malicious

Community Score: 55 / 72

Reanalyze Similar More

b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a

Size: 112.50 KB

Last Analysis Date: 11 months ago

CALC.EXE

peexe idle checks-user-input

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 1

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	d2f8843d112bb0421ba7a25999a59f32
SHA-1	c50f22713b54e2fb476bfff5dda83b76b493212c
SHA-256	b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a
Vhash	0150366d155035x3001e1af21245fz
Authentihash	53b04deff6cf112e5a75ff418c43ed3a77f19ff297541a45cd0b5698bb0aff
Imphash	08f6a1b121da8cedde2d1089d0906ed8
Rich PE header hash	72d42fa6f32b6934c77b30731ebd5f1
SSDEEP	3072:DAq2By/0He97ulj7nt5CdLYkOEp0AWLnQoXPBsr5ZrR:DAqfB9yBJa7OE0pLnQoo5Zd
TLSH	T197B39E01BA94F135C465113448D39FFA93BDBF1705AB16AB33097E4F7E362662A23286
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (43.3%)   Microsoft Visual C++ compiled executable (generic) (22.9%)   Win32 Dynamic Link Library (generic) (9.1%)   Win16 N...
DetectItEasy	PE32   Compiler: Microsoft Visual C/C++ (13.00.9178) [C++]   Linker: Microsoft Linker (7.00.9210)   Tool: Visual Studio (2002)
File size	112.50 KB (115200 bytes)



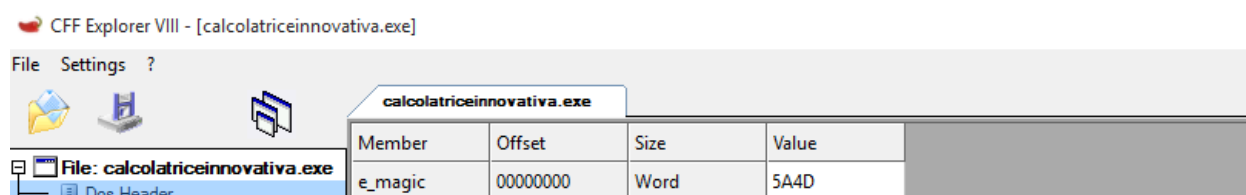
Imports

- + GDI32.dll
- + SHELL32.dll
- + KERNEL32.dll
- + msvcrt.dll
- + ADVAPI32.dll
- + USER32.dll

## FASE 1 - CFF Explorer

Con questo tool andremo ad analizzare a fondo tutte le informazioni riguardanti il nostro file sospetto.

Come prima cosa all'interno del Dos Header possiamo vedere subito la firma del file, in questo caso all'interno del campo **e\_magic** viene riportato il valore esadecimale 5A4D che se convertito in ascii risulta MZ che è la firma necessaria a far sì che il programma sia eseguibile su sistemi Windows.



Di seguito invece spostandosi all'interno dell'**Import Directory** e **Dependencies Walker** possiamo vedere quali sono le librerie e le relative funzioni che il programma importa e che sono necessarie al suo funzionamento. In questo caso dobbiamo contestualizzare quello che il software dovrebbe fare e confrontarlo con le funzioni importate delle varie librerie. Nel nostro esempio abbiamo una calcolatrice e analizzando le varie funzioni possiamo vedere che ne importa alcune necessarie per il collegamento a internet, le analizzeremo successivamente con l'analisi dinamica per trarne delle conclusioni.

calcolatriceinnovativa.exe						
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

## FASE 2 - Analisi Dinamica con Cuckoo Sandbox e Procmon

Tramite *Cuckoo Sandbox* andiamo ad effettuare un'analisi approfondita eseguendo il file e analizzandone il comportamento. Una volta lanciato il programma **Cuckoo** risalta subito all'occhio che il software utilizza una DLL windows dedicata alle funzioni che vediamo di seguito. Nello specifico la calcolatrice inizializza la libreria tramite **WSAStartup**, crea il socket per il collegamento di rete con **WSASocketA** e infine si connette ad un server remoto nel nostro caso indicato con l'IP 192.168.1.80, come abbiamo detto precedentemente tramite l'analisi delle funzioni contestualizzate allo scopo di utilizzo del software possiamo determinare che risulta sospettoso ed "impossibile" che una calcolatrice tenta una connessione con un server remoto. Lo stesso risultato l'abbiamo ottenuto analizzando l'esecuzione con il software **Procmon** e vedendo che viene avviato un processo di connessione **TCP** all'indirizzo IP citato sopra.

Time & API	Arguments
<b>WSAStartup</b> Nov. 26, 2024, 4:11 p.m.	wVersionRequested: 400
<b>WSASocketA</b> Nov. 26, 2024, 4:11 p.m.	type: 1 flags: 0 socket: 152 protocol: 0 af: 2
<b>connect</b> Nov. 26, 2024, 4:11 p.m.	ip_address: 192.168.1.80 socket: 152 port: 4444

## CONCLUSIONI

Dalle supposizioni fatte precedentemente possiamo quindi determinare che *calcolatriceinnovativa.exe* è a tutti gli effetti un Trojan che tenta l'installazione di una **backdoor** per aprire una sessione di reverse shell al server remoto con indirizzo ip 192.168.1.80 sulla porta 4444 attraverso le funzioni della libreria **ws2\_32.dll**