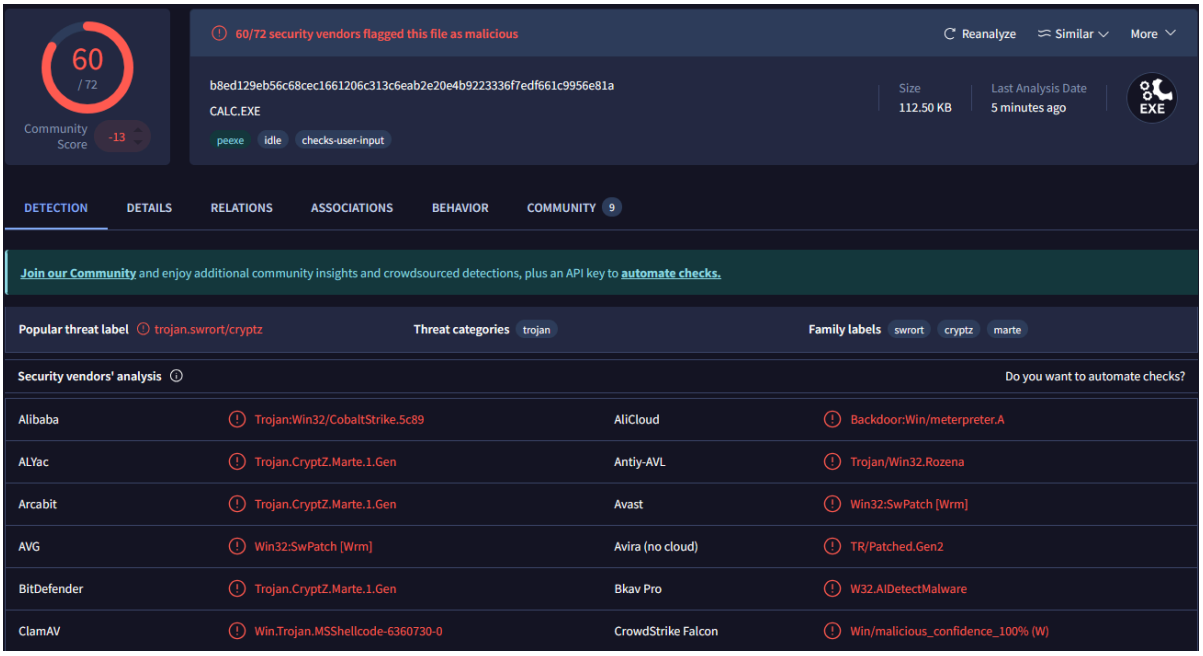
Analisi malware calcolatriceinnovativa.exe

Ricerca online

Virustotal

Questo malware è già riconosciuto dalla maggior parte degli antivirus e viene spesso categorizzato come Trojan.



MalwareBazaar

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

Link alla scansione:
https://bazaar.abuse.ch/sample/b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a/

Problemi di sicurezza:

1. **CHECK_AUTHENTICODE (high)**: Il file manca di un certificato digitale di autenticazione (Authenticode). Questo è un avviso importante, poiché l'assenza di un certificato potrebbe indicare che il file non è stato firmato da un produttore verificato, un potenziale segno di malware o software sospetto.
2. **CHECK_DLL_CHARACTERISTICS (high)**: Il file manca di caratteristiche di sicurezza per i DLL, come un livello di entropia elevato nel loro indirizzamento virtuale. La mancanza di protezione di questo tipo rende più facile che il file venga manipolato o modificato durante l'esecuzione.
3. **CHECK_NX (critical)**: Manca la protezione **Non-Executable (NX)** della memoria. Questo è un problema critico in quanto permette l'esecuzione di codice arbitrario da aree di memoria che dovrebbero essere protette (come lo stack o l'heap). L'assenza di questa protezione rende il file vulnerabile a exploit.
4. **CHECK_PIE (high)**: Manca la protezione **Position-Independent Executable (PIE)**. Senza PIE, la memoria del programma non è randomizzata, il che rende il programma più facilmente attaccabile (ad esempio, con exploit di tipo buffer overflow).

Capacità e comportamenti:

- **WIN32_PROCESS_API**: Il file è in grado di **creare processi e thread**, come evidenziato dalle chiamate alle funzioni `CloseHandle`, `CreateThread` di

`KERNEL32.dll`. Questo è tipico per i malware che devono eseguire codice in parallelo o manipolare altre istanze di programmi.

- **WIN_BASE_API**: Usa l'API di base di Windows, in particolare funzioni come `LoadLibraryA`, `GetStartupInfoA`, e `GetCommandLineA`, che sono utilizzate per caricare librerie, ottenere informazioni sul sistema e ottenere i parametri di esecuzione del programma. Questo comportamento è comune in vari tipi di software, inclusi i malware, che possono caricare librerie esterne o ottenere dettagli sul sistema.
- **WIN_REG_API**: Il file è capace di **manipolare il registro di Windows**, utilizzando funzioni come `RegOpenKeyExA` e `RegQueryValueExA`. La modifica del registro è una caratteristica tipica dei malware che cercano di persistere nel sistema e mantenere la loro esecuzione anche dopo un riavvio.
- **WIN_USER_API**: Il file può **interagire con l'interfaccia grafica di Windows**. Le funzioni come `OpenClipboard` e `CreateWindowExW` suggeriscono che il programma può interagire con la GUI (interfaccia utente grafica), probabilmente per mostrare finestre o raccogliere informazioni da clipboard, un comportamento comune in malware che si travestono da applicazioni legittime.

La scansione BLint eseguita da MalwareBazaar ci permette fin da subito di comprendere la natura del malware.

- Il file analizzato presenta numerosi rischi di sicurezza (soprattutto con il **NX** e **PIE** mancanti), il che suggerisce che potrebbe essere vulnerabile a **sfruttamenti tramite exploit**.
- L'uso di funzioni per la manipolazione di processi, la gestione del registro e l'interazione con la GUI suggerisce che questo file potrebbe tentare di **eseguire azioni dannose sul sistema**, come la persistenza, l'acquisizione di informazioni sensibili o l'esecuzione di codice in background.
- La mancanza di un certificato di autenticazione e le caratteristiche di DLL non sicure fanno pensare che questo file potrebbe **non essere legittimo**, ma piuttosto un malware camuffato da applicazione innocua.

Analisi statica con CFF Explorer

Dos Header

Il **DOS Header** è la prima parte di un file eseguibile in formato **PE (Portable Executable)**.

Contiene informazioni critiche, tra cui la firma "MZ", che consente al sistema operativo di identificare il file come un eseguibile valido.

Durante l'**analisi di malware**, il DOS Header può rivelare eventuali manipolazioni o anomalie, aiutando a valutare l'integrità del file.

L'intestazione "MZ" e il DOS Header vengono spesso analizzati per rilevare:

- **Anomalie** nel formato, che possono indicare la presenza di un malware.
- **Punti di ingresso** non standard, che possono suggerire codice malevolo.
- **Sezioni nascoste** o contraffatte, utilizzate dai malware per eludere il rilevamento.

Questi sono i valori del Dos header del malware preso in analisi:

- **e_magic**: Questo è il *magic number* che identifica il file come eseguibile PE (Portable Executable). Valore: `5A4D` (equivalente a "MZ" in ASCII).
- **e_cblp**: Indica la dimensione dell'ultima pagina del file in byte. Valore: `0090` (144 byte in decimale).
- **e_cs**: Rappresenta il numero di blocchi a 16-bit (*paragraphs*) nell'intestazione del file. Valore: `0003`.
- **e_lfanew**: Specifica l'offset in cui inizia l'intestazione PE. Valore: `0040` (64 byte in decimale).
- **e_cparhdr**: Indica la dimensione in blocchi a 16-bit dell'intestazione aggiuntiva. Valore: `0004`.
- **e_sp**: Contiene il valore iniziale dello stack pointer. Valore: `0088` (136 in decimale).

La struttura del Dos Header è conforme al formato standard PE (Portable Executable), il che conferma che il file è un eseguibile Windows legittimo dal punto di vista strutturale.

Il file appare legittimo nella sua struttura superficiale, ma ciò non esclude la presenza di codice malevolo.

Section Headers

Qui troviamo le sezioni principali del programma.

calcolatriceinnovativa.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	000126B0	00001000	00012800	00000400	00000000	00000000	0000	0000	60000020
.data	0000101C	00014000	00000A00	00012C00	00000000	00000000	0000	0000	C0000040
.rsrc	00008A70	00016000	00008C00	00013600	00000000	00000000	0000	0000	40000040

Il programma presenta le seguenti sezioni principali:

1. **.text**: Contiene il codice eseguibile. Potrebbe contenere istruzioni malevoli o offuscate e quindi le funzioni principali del malware, come la registrazione delle battiture (keylogging) e il furto di informazioni.
2. **.data**: Include dati statici usati dal programma, come ad esempio le variabili.
3. **.rsrc**: Conserva risorse incorporate, come immagini o icone. Qui ad esempio troviamo l'icona della calcolatrice. Possono essere nascoste configurazioni e payload malevoli.

Ogni sezione ha una funzione specifica. La presenza di una sezione `.rsrc` suggerisce che il programma include risorse grafiche, il che è coerente con l'icona della calcolatrice utilizzata per camuffarsi.

Import Directory

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

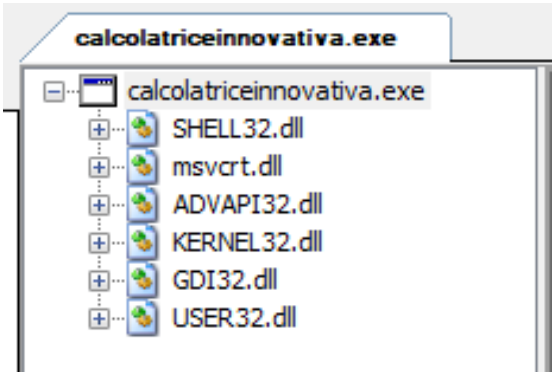
Il malware importa librerie standard di Windows, che potrebbero essere utilizzate sia per scopi legittimi che malevoli. Le librerie principali sono:

- **SHELL32.dll**: Consente l'esecuzione di comandi di sistema e interazioni con la shell di Windows.
- **USER32.dll**: Permette di interagire con l'interfaccia utente, come finestre, popup e input da mouse e tastiera. Potrebbe essere sfruttata per spiare l'interfaccia utente (ad esempio, keylogging o controllo del mouse).
- **GDI32.dll**: Gestisce risorse grafiche per il disegno di testo e grafica.
- **KERNEL32.dll**: Offre funzioni di basso livello per la gestione della memoria, dei processi, dei file e altre funzionalità di sistema.
- **ADVAPI32.dll**: Contiene funzioni avanzate per la gestione della sicurezza, il registro di sistema e i servizi di Windows.
- **MSVCRT.dll**: Consente di eseguire operazioni matematiche.

La combinazione di queste librerie potrebbe indicare funzionalità pericolose, come l'esecuzione di comandi di sistema tramite shell, la manipolazione del registro, lo spionaggio dell'utente o la manipolazione grafica per ingannare l'utente.

Dependency Walker

Il Dependency Walker elenca tutte le librerie DLL dalle quali il file eseguibile dipende, cioè le librerie che deve caricare per funzionare correttamente.

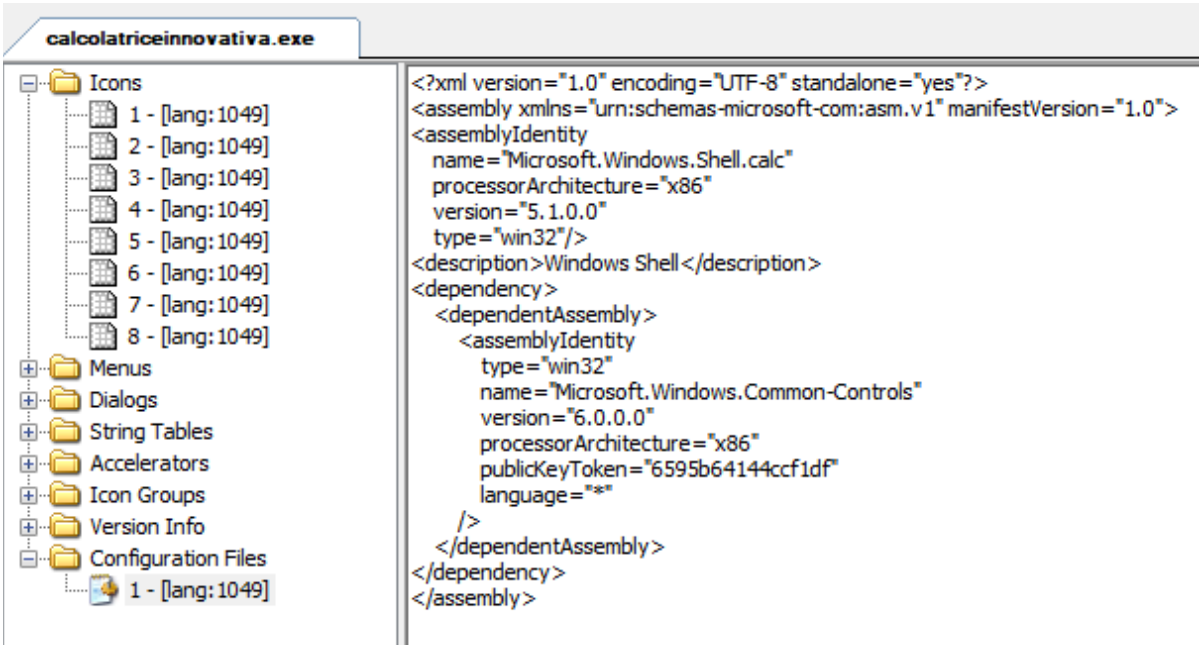


Property	Value
CompanyName	Корпорация Майкрософт
FileDescription	Калькулятор для Windows
FileVersion	5.1.2600.0 (xpclient.010817-1148)
InternalName	CALC
LegalCopyright	© Корпорация Майкрософт. Все права защищены.
OriginalFilename	CALC.EXE
ProductName	Операционная система Microsoft® Windows®

Questa sezione rivela che il file presenta una provenienza dubbia. Questo aspetto richiede particolare attenzione, soprattutto considerando le funzioni e le librerie coinvolte.

Resource Editor

Questa sezione elenca le risorse incorporate nel file eseguibile, organizzate in categorie come icone, dialoghi, gruppi di icone e file di configurazione.



L'analisi delle risorse del file ha evidenziato due punti rilevanti:

Icona del programma: Il file utilizza l'icona di una calcolatrice per sembrare un'applicazione legittima.

Configuration Files: Il programma viene descritto internamente come una *shell di Windows*, il che suggerisce potenziali funzionalità pericolose, come l'esecuzione di comandi arbitrari.

Analisi dinamica con Cuckoo

https://cuckoo.ee/analysis/5587621/summary/

Grazie a questa analisi dinamica tramite Cuckoo otteniamo altri dati utili che ci suggeriscono il comportamento del malware.

Yara rule

Lo **Yara rule** identifica che il malware interagisce con il **registro di sistema**, il che potrebbe indicare che tenta di alterare configurazioni di sistema, stabilire persistenza, o eseguire altre attività malevole.

Allocazione di Memoria Read-Write-Execute

- **API utilizzata**: `NtAllocateVirtualMemory`.
- **Dettagli dell'allocazione**:
    - **Protection**: `PAGE_EXECUTE_READWRITE` indica che l'area di memoria allocata può essere letta, scritta e anche eseguita. Questo è sospetto perché spesso indica che il malware potrebbe:
        - Decodificare o decomprimere il proprio codice in memoria.
        - Caricare un payload secondario in memoria.
        - Eseguire codice shell (come un exploit).
    - **Region size**: 4096 byte (4 KB) sono stati allocati, che è una dimensione tipica per caricare o eseguire porzioni di codice.
    - **Base address**: 0x00280000, l'indirizzo virtuale in cui è stata allocata la memoria.

Il comportamento è altamente sospetto e indica che il file potrebbe essere "packed" (impacchettato), ossia utilizza tecniche per nascondere il codice malevolo e caricarlo in esecuzione.

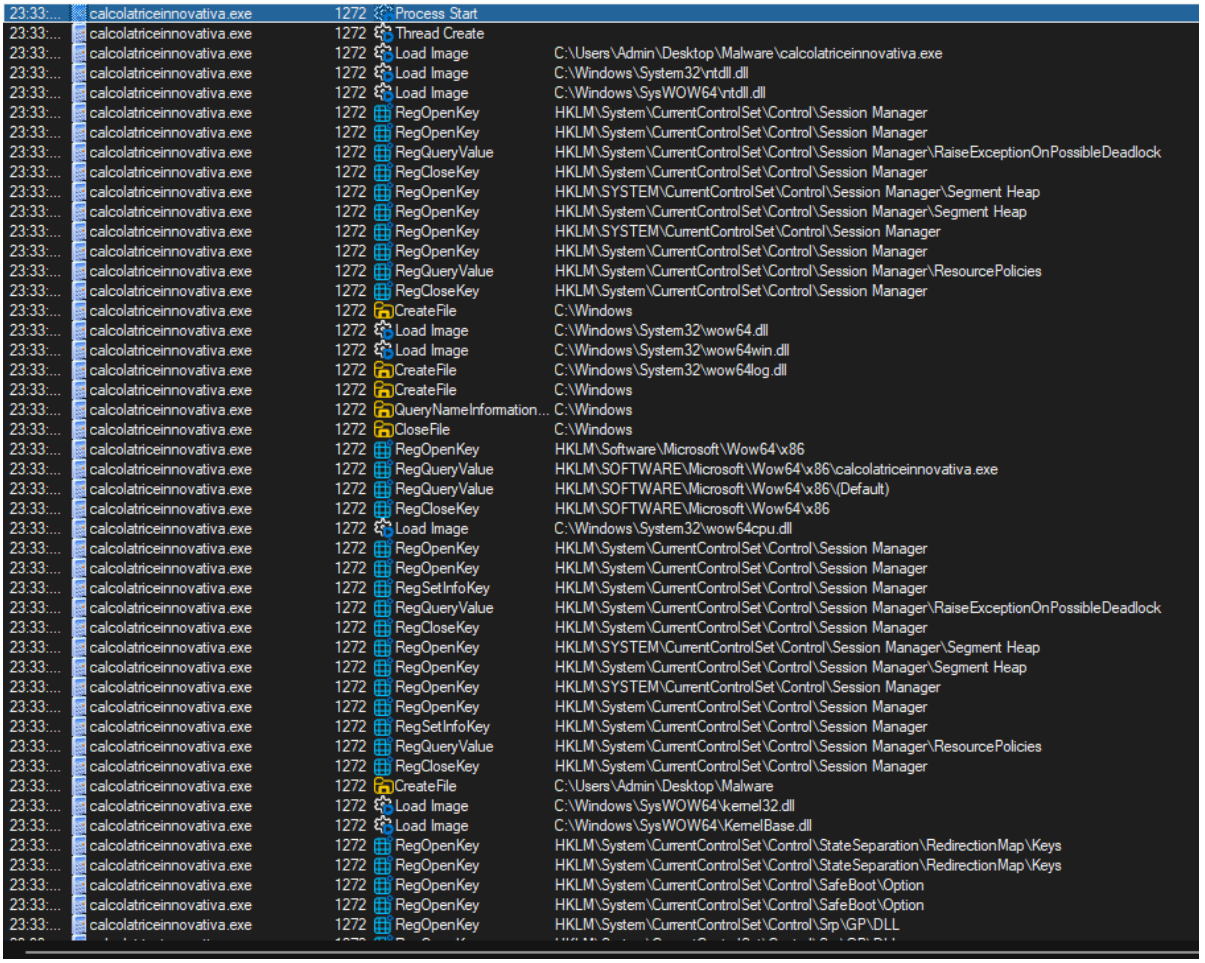
Entropia del file binario

Entropy: L'entropia della sezione `.text` è **6.86**, che è considerata alta.

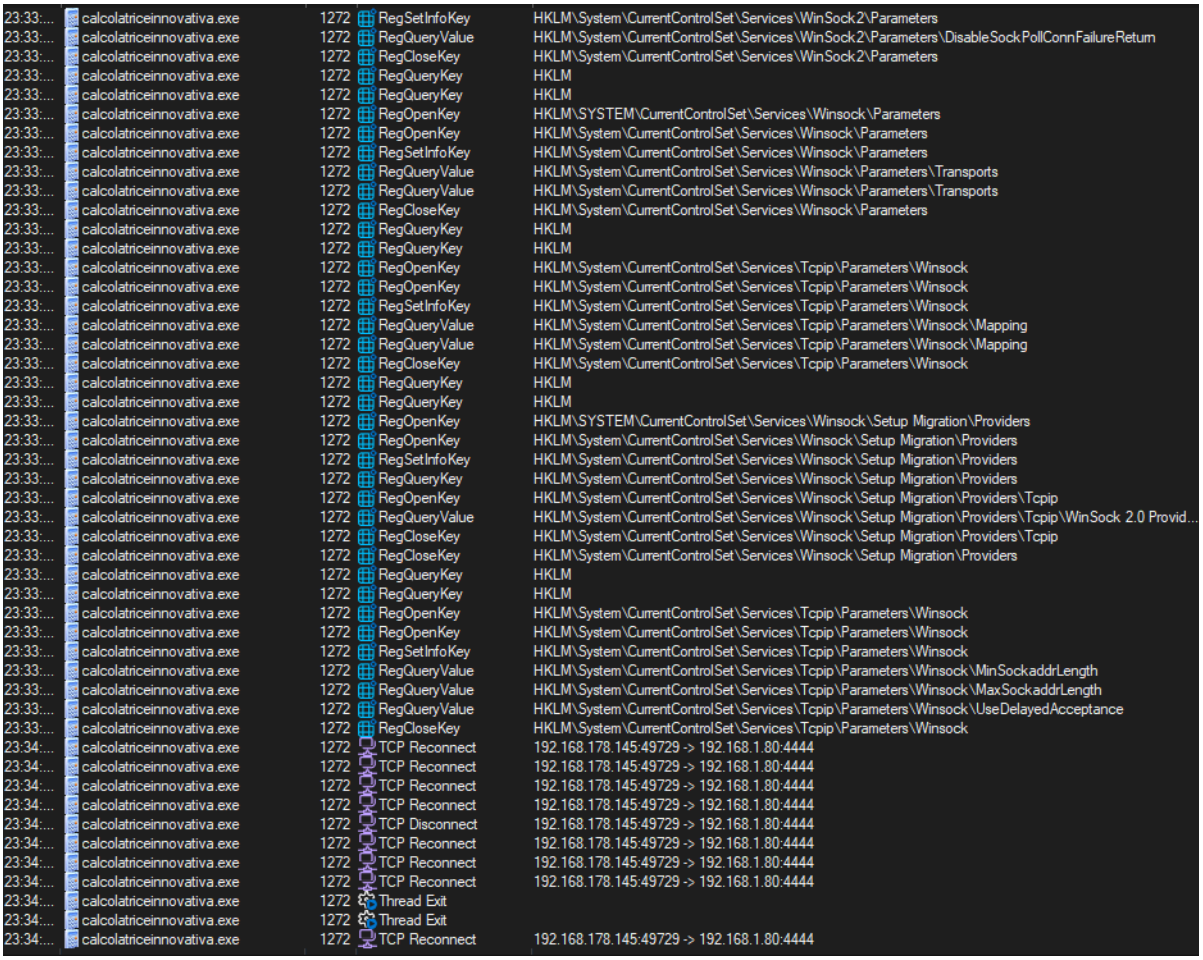
- L'entropia elevata è un indicatore comune di compressione o crittografia del codice all'interno del file binario.
- **Virtual Size**: La dimensione virtuale della sezione `.text` è superiore rispetto alla dimensione dei dati (`0x00012800` vs `0x00001000`), suggerendo un possibile unpacking dinamico.

L'entropia elevata e la discrepanza nella dimensione indicano che il file potrebbe essere stato compresso o crittografato da un packer, che il malware utilizza per evitare l'analisi statica.

Analisi dinamica con Process Monitor



23:33:...	calcolatriceinnovativa.exe	1272	Process Start	
23:33:...	calcolatriceinnovativa.exe	1272	Thread Create	
23:33:...	calcolatriceinnovativa.exe	1272	Load Image	C:\Users\Admin\Desktop\Malware\calcolatriceinnovativa.exe
23:33:...	calcolatriceinnovativa.exe	1272	Load Image	C:\Windows\System32\ntdll.dll
23:33:...	calcolatriceinnovativa.exe	1272	Load Image	C:\Windows\SysWOW64\ntdll.dll
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock
23:33:...	calcolatriceinnovativa.exe	1272	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies
23:33:...	calcolatriceinnovativa.exe	1272	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	CreateFile	C:\Windows
23:33:...	calcolatriceinnovativa.exe	1272	Load Image	C:\Windows\System32\wow64.dll
23:33:...	calcolatriceinnovativa.exe	1272	Load Image	C:\Windows\System32\wow64win.dll
23:33:...	calcolatriceinnovativa.exe	1272	CreateFile	C:\Windows\System32\wow64log.dll
23:33:...	calcolatriceinnovativa.exe	1272	CreateFile	C:\Windows
23:33:...	calcolatriceinnovativa.exe	1272	QueryNameInformation...	C:\Windows
23:33:...	calcolatriceinnovativa.exe	1272	CloseFile	C:\Windows
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\Software\Microsoft\Wow64\x86
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\x86\calcolatriceinnovativa.exe
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\x86\(Default)
23:33:...	calcolatriceinnovativa.exe	1272	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\x86
23:33:...	calcolatriceinnovativa.exe	1272	Load Image	C:\Windows\System32\wow64cpu.dll
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock
23:33:...	calcolatriceinnovativa.exe	1272	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies
23:33:...	calcolatriceinnovativa.exe	1272	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager
23:33:...	calcolatriceinnovativa.exe	1272	CreateFile	C:\Users\Admin\Desktop\Malware
23:33:...	calcolatriceinnovativa.exe	1272	Load Image	C:\Windows\SysWOW64\kernel32.dll
23:33:...	calcolatriceinnovativa.exe	1272	Load Image	C:\Windows\SysWOW64\KernelBase.dll
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\StateSeparation\RedirectionMap\Keys
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\StateSeparation\RedirectionMap\Keys
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL



23:33:...	calcolatriceinnovativa.exe	1272	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters\DisableSockPollConnFailureReturn
23:33:...	calcolatriceinnovativa.exe	1272	RegCloseKey	HKLM\System\CurrentControlSet\Services\WinSock2\Parameters
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryKey	HKLM
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryKey	HKLM
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Parameters
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Services\Winsock\Parameters
23:33:...	calcolatriceinnovativa.exe	1272	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Winsock\Parameters
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Services\Winsock\Parameters\Transports
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Services\Winsock\Parameters\Transports
23:33:...	calcolatriceinnovativa.exe	1272	RegCloseKey	HKLM\System\CurrentControlSet\Services\Winsock\Parameters
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryKey	HKLM
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryKey	HKLM
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock
23:33:...	calcolatriceinnovativa.exe	1272	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\Mapping
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\Mapping
23:33:...	calcolatriceinnovativa.exe	1272	RegCloseKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryKey	HKLM
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryKey	HKLM
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Winsock\Setup Migration\Providers
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers
23:33:...	calcolatriceinnovativa.exe	1272	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers\Tcpip
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers\Tcpip\WinSock 2.0 Provid...
23:33:...	calcolatriceinnovativa.exe	1272	RegCloseKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers\Tcpip
23:33:...	calcolatriceinnovativa.exe	1272	RegCloseKey	HKLM\System\CurrentControlSet\Services\Winsock\Setup Migration\Providers
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryKey	HKLM
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryKey	HKLM
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock
23:33:...	calcolatriceinnovativa.exe	1272	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock
23:33:...	calcolatriceinnovativa.exe	1272	RegSetInfoKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\MinSockaddrLength
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\MaxSockaddrLength
23:33:...	calcolatriceinnovativa.exe	1272	RegQueryValue	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock\UseDelayedAcceptance
23:33:...	calcolatriceinnovativa.exe	1272	RegCloseKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Winsock
23:34:...	calcolatriceinnovativa.exe	1272	TCP Reconnect	192.168.178.145:49729 -> 192.168.1.80:4444
23:34:...	calcolatriceinnovativa.exe	1272	TCP Reconnect	192.168.178.145:49729 -> 192.168.1.80:4444
23:34:...	calcolatriceinnovativa.exe	1272	TCP Reconnect	192.168.178.145:49729 -> 192.168.1.80:4444
23:34:...	calcolatriceinnovativa.exe	1272	TCP Reconnect	192.168.178.145:49729 -> 192.168.1.80:4444
23:34:...	calcolatriceinnovativa.exe	1272	TCP Disconnect	192.168.178.145:49729 -> 192.168.1.80:4444
23:34:...	calcolatriceinnovativa.exe	1272	TCP Reconnect	192.168.178.145:49729 -> 192.168.1.80:4444
23:34:...	calcolatriceinnovativa.exe	1272	TCP Reconnect	192.168.178.145:49729 -> 192.168.1.80:4444
23:34:...	calcolatriceinnovativa.exe	1272	TCP Reconnect	192.168.178.145:49729 -> 192.168.1.80:4444
23:34:...	calcolatriceinnovativa.exe	1272	Thread Exit	
23:34:...	calcolatriceinnovativa.exe	1272	Thread Exit	
23:34:...	calcolatriceinnovativa.exe	1272	TCP Reconnect	192.168.178.145:49729 -> 192.168.1.80:4444

Dal log mostrato nelle immagini, il malware ha eseguito una serie di attività sospette e potenzialmente dannose. Ecco un riassunto delle principali azioni svolte:

1. **Accesso a numerose chiavi di registro di sistema**:
    - Il malware ha aperto e chiuso numerose chiavi di registro, incluse le chiavi sotto `HKLM\System\CurrentControlSet\Services\` relative a `Winsock`, `Tcpip`, `WinSock2`, nonché le chiavi di configurazione di Windows come `HKLM\Software\Microsoft\Windows\CurrentVersion`.
    - Queste letture possono suggerire che il malware stia raccogliendo informazioni sul dispositivo vittima, per poi inviarle ad un server remoto e permettere all'attaccante di attaccare con precisione in un secondo momento.
2. Modifica di alcune chiavi di registro:
    - Il malware non si sta limitando a leggere, ma sta anche modificando alcune chiavi di registro tramite il comando `SetInfoRegKey`.

    - Dimostra quindi il tentativo da parte del programma di modificare le variabili e l'ambiente del dispositivo vittima.
3. **Caricamento di librerie di sistema**:
    - Il malware ha caricato file DLL di sistema come `ntdll.dll`, `kernel32.dll`, `wow64.dll`, e altri. Questo potrebbe essere un tentativo di utilizzare funzioni di sistema per eseguire operazioni come la gestione della memoria, l'esecuzione di comandi, e l'interazione con altre risorse di sistema.
4. **Operazioni su file**:
    - Il malware ha creato e aperto file in alcuni percorsi, tra cui di sistema come `C:\Windows\System32`.
5. **Connessioni di rete**:
    - Il malware ha tentato di stabilire connessioni TCP su indirizzi IP specifici (`192.168.178.14` e `192.168.1.80`) e ha eseguito operazioni di "Reconnect" e "Disconnect" su queste connessioni. Queste operazioni possono suggerire che il malware sta cercando di stabilire una connessione e di comunicare con un server remoto.
6. **Creazione e gestione di processi**:
    - Sono visibili operazioni come la creazione di thread e la gestione di processi.

In sintesi, il malware sembra essere impegnato in una serie di attività progettate per compromettere la sicurezza del sistema attraverso modifiche al registro, la raccolta delle informazioni, la creazione di connessioni remote e il caricamento di componenti di sistema.

Queste azioni potrebbero essere parte di un **tentativo di persistente compromissione** e **controllo del sistema infetto**.

Conclusioni

L'uso di funzioni per la manipolazione di processi, la gestione del registro e l'interazione con la rete, suggerisce che questo file potrebbe tentare di eseguire azioni dannose sul sistema, come la persistenza, l'acquisizione di informazioni sensibili o l'esecuzione di codice in background.

Già da questa prima analisi, dunque, anche se non abbiamo la certezza su quali sono tutte le attività che il malware può svolgere, possiamo confermare che questo eseguibile può essere molto pericoloso.

Bisogna sempre tenere in considerazione che il malware potrebbe non essere nel pieno del suo potenziale dato che si trova all'interno di una sandbox.

Inoltre, in questo esercizio, il malware è stato reso appositamente più innoquo rispetto alla sua reale natura, in quanto, per esempio, tenta di collegarsi a indirizzi IP privati e non a indirizzi IP pubblici (come accadrebbe invece con un malware realemente malevolo).

Raccomandazioni

Se il sistema è stato infettato da questo malware, consiglio di adottare le seguenti misure:

1. **Isolare il dispositivo:** Disconnettere il dispositivo dalla rete per impedire la diffusione del malware ad altri sistemi.
2. **Eseguire una scansione completa con un antivirus aggiornato:** Utilizzare un software antivirus affidabile per rilevare e rimuovere tutte le tracce del malware.
3. **Ripristinare il sistema da un backup pulito:** Se disponibile, ripristinare il sistema da un backup creato prima dell'infezione.
4. **Cambiare tutte le password:** Modificare le password di tutti gli account utilizzati sul dispositivo infetto.
5. **Installare patch di sicurezza:** Assicurarsi che il sistema operativo e tutte le applicazioni installate siano aggiornati con le ultime patch di sicurezza.

Prevenire le Infezioni

Per prevenire future infezioni, è consigliabile adottare le seguenti misure precauzionali:

- Installare un software antivirus affidabile e mantenerlo aggiornato.
- Evitare di aprire allegati e-mail sospetti o di cliccare su link non sicuri.
- Tenere aggiornato il sistema operativo e le applicazioni.
- Utilizzare un firewall.

- Creare regolarmente backup dei dati importanti.
- Essere cauti quando si scaricano e si installano software da fonti non affidabili.