Analisi del file "calcolatriceinnovativa.exe" Librerie Importate

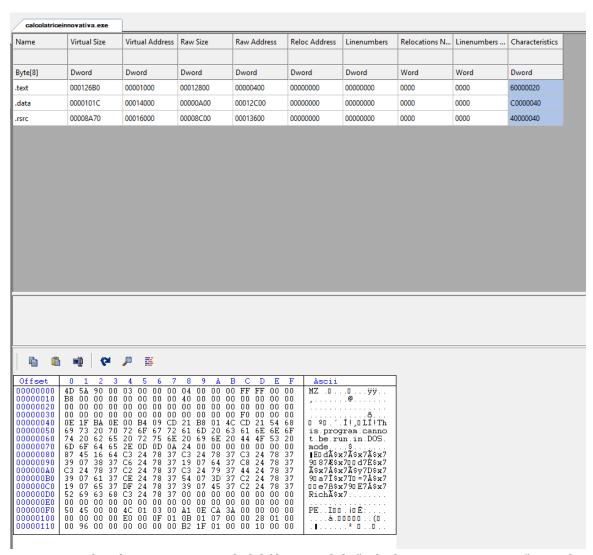
calcolatriceinnovativa.exe				
calcolatriceinnovativa.exe				
SHELL32.dll msvcrt.dll dr. ShELL32.dll dr. ShERNEL32.dll dr. ShERNEL32.dll dr. ShERNEL32.dll dr. ShERNEL32.dll dr. ShERNEL32.dll	Property	Value		
	File Name	C:\U	sers\user\Desktop\Malware\calcolatriceinnovativa.exe	
	File Type	Porta	able Executable 32	
	File Info	No n	natch found.	
	File Size	112.5	50 KB (115200 bytes)	
	PE Size	112.50 KB (115200 bytes)		
	Created	Mon	day 22 July 2024, 12.08.38	
	Modified	Mon	day 22 July 2024, 12.00.44	
	Accessed	Monday 22 July 2024, 12.08.38		
	MD5	D2F8	843D112BB0421BA7A25999A59F32	
	SHA-1	C50F22713B54E2FB476BFFF5DDA83B76B493212C		
	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®	

Il file eseguibile "calcolatriceinnovativa.exe" utilizza le seguenti librerie (DLL):

- SHELL32.dll: Fornisce funzioni utilizzate per l'interfaccia utente di Windows, tra cui la gestione di file e cartelle, oltre alle finestre di dialogo comuni.
- msvcrt.dll: Libreria C runtime di Microsoft, che fornisce funzioni standard del linguaggio C, come gestione di file, input/output, gestione della memoria e altre funzionalità di base.
- ADVAPI32.dll: Fornisce l'accesso a funzionalità avanzate del sistema operativo Windows, come la gestione del registro di sistema, servizi e sicurezza.
- KERNEL32.dll: Contiene le funzioni base del sistema operativo Windows, tra cui la gestione della memoria, input/output, e gestione di thread e processi.

- GDI32.dll: Utilizzata per la grafica e il rendering di testo e immagini, soprattutto per operazioni di disegno in applicazioni con interfaccia grafica.
- USER32.dll: Gestisce componenti dell'interfaccia utente, come finestre, controlli e messaggi.

Sezioni del Malware



Possiamo vedere le sezioni principali del file eseguibile "calcolatriceinnovativa.exe". Ecco le descrizioni di ciascuna sezione:

1..text:

- Virtual Size: 0x000126B0- Virtual Address: 0x00001000- Raw Size: 0x00012800

- Descrizione: Questa è la sezione del codice eseguibile. Contiene le istruzioni eseguibili dal processore. Il malware, se presente, esegue le sue operazioni dannose da questa sezione. È la parte fondamentale dove si trovano le funzionalità principali dell'applicazione o del malware.

2. .data:

Virtual Size: 0x0000011CVirtual Address: 0x00014000

- Raw Size: 0x00000A00

- Descrizione: Questa sezione contiene i dati inizializzati utilizzati dal programma. In un malware, questa sezione può essere utilizzata per mantenere variabili, dati statici o strutture necessarie per il funzionamento del codice in .text.

3. .rsrc:

Virtual Size: 0x00008A70Virtual Address: 0x00016000

- Raw Size: 0x0000C00

- Descrizione: Questa sezione contiene risorse del programma, come icone, immagini, file di dialogo o altri tipi di risorse. Nei malware, questa sezione può essere utilizzata per nascondere risorse dannose come payload, stringhe cifrate o altri componenti.

Considerazione Finale

In base alle informazioni raccolte, il file "calcolatriceinnovativa.exe" sembra essere un file eseguibile di piccole dimensioni che si presenta come una calcolatrice per Windows. Tuttavia, diversi indizi possono suggerire che questo file potrebbe essere di natura dannosa:

- Le librerie importate sono comuni e utilizzate da molti programmi legittimi, ma sono anche le stesse che spesso vengono usate da malware per interagire con il sistema operativo. Questi possono essere utilizzati per attività dannose.
- Le sezioni del file indicano che si tratta di un file PE (Portable Executable), che può eseguire codice. La sezione .rsrc potrebbe contenere risorse malevole nascoste.
- Gli hash MD5 e SHA-1 potrebbero essere confrontati con database di malware noti per identificare eventuali corrispondenze con minacce già rilevate.

Il fatto che il file sia descritto come una calcolatrice, ma risulti sospetto per via della lingua russa utilizzata nelle sue proprietà (possibilmente alterate), suggerisce che questo file potrebbe essere stato camuffato per apparire innocuo, mentre esegue attività potenzialmente dannose.