

Analisi del file

"calcolatriceinnovativa.exe"

Librerie Importate

calcolatriceinnovativa.exe

calcolatriceinnovativa.exe

SHELL32.dll

msvcrt.dll

ADVAPI32.dll

KERNEL32.dll

GDI32.dll

USER32.dll

Property	Value
File Name	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe
File Type	Portable Executable 32
File Info	No match found.
File Size	112.50 KB (115200 bytes)
PE Size	112.50 KB (115200 bytes)
Created	Monday 22 July 2024, 12.08.38
Modified	Monday 22 July 2024, 12.00.44
Accessed	Monday 22 July 2024, 12.08.38
MD5	D2F8843D112BB0421BA7A25999A59F32
SHA-1	C50F22713B54E2FB476BFF5DDA83B76B493212C

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

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





Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ .0...0...yy..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	F0	00	00	000.....
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	0 00...i...l...l...Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program cannot
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	be run in DOS.
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode...\$.....
00000080	87	45	16	64	C3	24	78	37	C3	24	78	37	C3	24	78	37	!E0dA\$7A\$7A\$7
00000090	39	07	38	37	C6	24	78	37	19	07	64	37	C8	24	78	37	9087A\$700d7E\$7
000000A0	C3	24	78	37	C2	24	78	37	C3	24	79	37	44	24	78	37	A\$7A\$7A\$7yD\$7
000000B0	39	07	61	37	CE	24	78	37	54	07	3D	37	C2	24	78	37	90a7I\$770=7A\$7
000000C0	19	07	65	37	DF	24	78	37	39	07	45	37	C2	24	78	37	00e7B\$790E7A\$7
000000D0	52	69	63	68	C3	24	78	37	00	00	00	00	00	00	00	00	RichA\$7.....
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000F0	50	45	00	00	4C	01	03	00	A1	0E	CA	3A	00	00	00	00	PE...I00...0E...
00000100	00	00	00	00	E0	00	0F	01	0B	01	07	00	00	28	01	00	...a.00000...(0
00000110	00	96	00	00	00	00	00	00	B2	1F	01	00	00	10	00	00	!.....^0...0...

- 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: 0x0000011C
- Virtual 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: 0x00008A70
- Virtual 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.