

## Report Analisi Malware: CalcolatriceInnovativa.exe

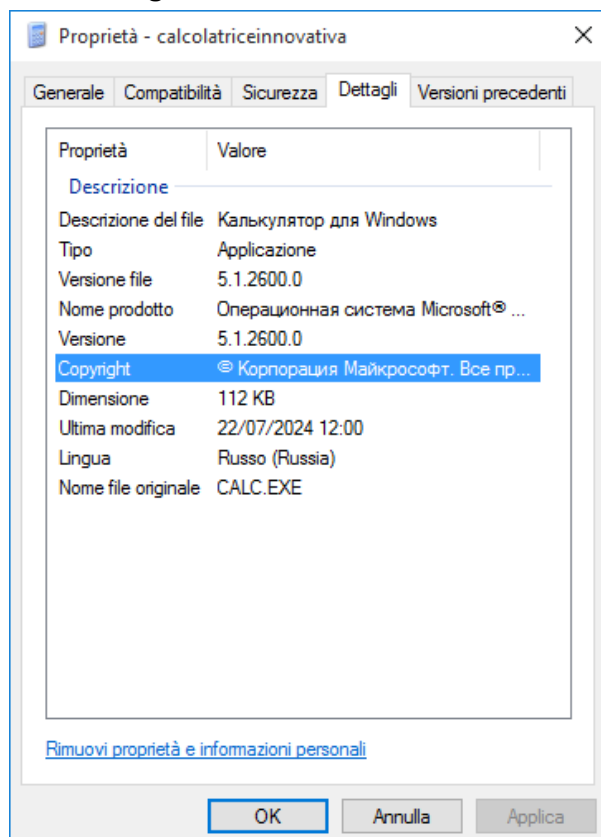
### Che cos'è questo file?

Il file analizzato si chiama **CalcolatriceInnovativa.exe**. A prima vista, sembra essere un'applicazione legittima, ma è risultato essere un **malware**, ovvero un programma dannoso. Questo file è progettato per fare cose che possono compromettere la sicurezza del tuo computer, come accedere ai tuoi dati, modificare impostazioni o lasciare una backdoor per altri attacchi.

### 1. Problemi di sicurezza nel file

Quando si analizza un programma, ci sono delle regole di sicurezza che deve seguire. Questo file non segue alcune di queste regole fondamentali:

- **Firmato digitalmente in maniera truffaldina.**



L'applicazione ha una firma digitale in Cirillico il che è molto sospetto, essendo in Europa un utente si aspetterebbe di avere un'applicazione con una firma digitale Europea.

## 2. Cosa fa di sospetto?

Durante l'analisi, abbiamo scoperto che il malware compie delle azioni molto insolite e dannose. Ecco alcune delle cose principali che potrebbe fare:

### A) Modifica i registri di sistema

I registri di sistema sono come il "cervello" di Windows: contengono tutte le informazioni sulle impostazioni del tuo computer. Questo malware può cambiarli per:

- **Attivarsi automaticamente:** Si imposta per partire ogni volta che accendi il PC, anche senza che tu lo avvii manualmente.
- **Nascondersi:** Potrebbe cambiare impostazioni per evitare che venga rilevato.

### B) Usa memoria per eseguire codice nascosto

Il programma è progettato per caricare ed eseguire codice malevolo direttamente nella memoria del computer. È come un ladro che entra in casa tua e agisce senza lasciare tracce evidenti.

### C) Comunicazione remota

È stato rilevato che potrebbe contenere strumenti per:

- **Controllo a distanza:** Qualcuno può entrare nel tuo PC e fare quello che vuole.
- **Furto di informazioni:** Può raccogliere dati sensibili, come password, file o informazioni bancarie per esempio .

### 3. Come lo sappiamo?

Abbiamo usato tre strumenti principali per analizzarlo:

## Analisi Statica

### A) VirusTotal

Un sito che permette di verificare i file con diversi antivirus contemporaneamente. Questo file è stato segnalato come **malevolo da 60 antivirus su 72**. Alcuni di questi lo hanno identificato come:

- **Trojan**: Un tipo di virus che nasconde altri programmi dannosi.
- **Meterpreter**: Strumento usato dai criminali informatici per controllare i computer delle vittime.

**60 / 72**  
Community Score -13

60/72 security vendors flagged this file as malicious

Reanalyze Similar More

b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a  
CALC.EXE  
Size: 112.50 KB  
Last Analysis Date: 49 minutes ago

peexe checks-user-input idle

DETECTION DETAILS RELATIONS ASSOCIATIONS BEHAVIOR COMMUNITY 9

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

Popular threat label trojan.swrort/cryptz Threat categories trojan Family labels swrort cryptz marte

Security vendors' analysis Do you want to automate checks?

Alibaba	Trojan.Win32/CobaltStrike.5c89	AliCloud	Backdoor.Win/meterpreter.A
ALYac	Trojan.CryptZ.Marte.1.Gen	Antiy-AVL	Trojan/Win32.Rozena
Arcabit	Trojan.CryptZ.Marte.1.Gen	Avast	Win32:SwPatch (Wrm)
AVG	Win32:SwPatch (Wrm)	Avira (no cloud)	TR/Patched.Gen2
BitDefender	Trojan.CryptZ.Marte.1.Gen	Bkav Pro	W32.AIDetectMalware
ClamAV	Win.Trojan.MSShellcode-6360730-0	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.cryptz	Cylance	Unsafe
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
DrWeb	Trojan.Swrort.1	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.CryptZ.Marte.1.Gen (B)	eScan	Trojan.CryptZ.Marte.1.Gen
ESET-NOD32	A Variant Of Win32/Rozena.DT	Fortinet	W32/Swrort.Cltr
GData	Trojan.CryptZ.Marte.1.Gen	Google	Detected
Gridinsoft (no cloud)	Trojan.Win32.Generic.oats3	Huorong	VirTool/Meterpreter.a

## B) BLint (Binary Linter) tool presente su MalwareBazaar

Questo strumento controlla la struttura del file. Ha rilevato che:

- Non rispetta standard di sicurezza moderni.
- Può creare nuovi processi, modificare registri e interagire con l'utente senza permesso.

**MALWARE** bazaar  
from ABUSE<sup>th</sup> | by BURNMALIB

[Browse](#) [Upload](#) [Hunting](#) [Access Data](#) [FAQ](#) [About](#) [Login](#)

### BLint

The following table provides more information about this file using [BLint](#). BLint is a Binary Linter to check the security properties, and capabilities in executables.

#### Findings

ID	Title	Severity
CHECK_AUTHENTICODE	Missing Authenticode	high
CHECK_DLL_CHARACTERISTICS	Missing dll Security Characteristics (HIGH_ENTROPY_VA)	high
CHECK_NX	Missing Non-Executable Memory Protection	critical
CHECK_PIE	Missing Position-Independent Executable (PIE) Protection	high

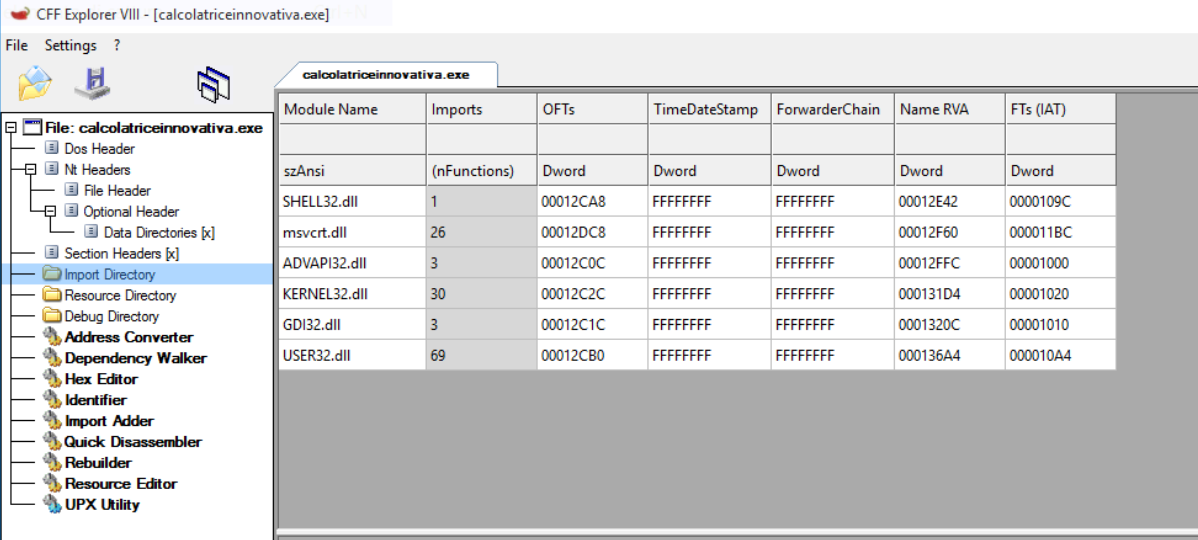
#### Reviews

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

## C) CFF Explorer

Questa applicazione offre agli utenti una serie di strumenti e funzionalità per esplorare ed analizzare file eseguibili in modo efficiente. Con CFF Explorer, gli utenti possono approfondire la struttura dei file eseguibili portabili, visualizzare informazioni dettagliate su intestazioni, sezioni, importazioni, esportazioni e molto altro. *9 Softonic International*

Verifichiamo quali librerie sono state importate :



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

**SHELL32.dll:** Usata per modificare file e cartelle, potrebbe nascondere il programma stesso.

**msvcrt.dll:** Aiuta a gestire la memoria, ma i malware la usano per fare operazioni complesse.

**ADVAPI32.dll:** Permette di modificare le impostazioni interne di Windows, come i registri. Questo è un segnale di rischio.

**KERNEL32.dll:** Aiuta il programma a gestire memoria e processi, ma può essere abusata per fare cose dannose.

**USER32.dll:** Contiene **tantissime funzioni sospette** (69 in totale), che il file potrebbe usare per mostrarti messaggi ingannevoli o finestre false.

**In poche parole:** Questo file usa trucchi per nascondersi e agire in modo pericoloso , inoltre potrebbe effettuare anche altre operazioni come cambiare impostazioni, mostrarti messaggi falsi e rubare dati.

# Analisi Dinamica

## B) Cuckoo Sandbox

Questo strumento ci permette di vedere come si comporta il file quando viene eseguito(il file viene eseguito su una VM creata appositamente è un sistema piu' sicuro di analizzare programmi di qui non si sa l'esistenza).

Abbiamo notato che:

- **Modifica i registri di Windows.**
- **Alloca memoria sospetta**, segno che potrebbe prepararsi per azioni dannose.
- **Presenta sezioni con dati criptati**, tipico nei malware che vogliono nascondere il loro funzionamento.

The screenshot displays the Cuckoo Sandbox web interface. The main panel shows a summary of the file analysis for 'calculatriceinnovativa.exe'. The file is identified as a PE32 executable (GUI) for Intel 80386, with a size of 112,500 bytes. The MD5 hash is 02f84321122042187a7239918f9f32, and the SHA1 hash is c5f822713054e2f047d0f7f5d0a3070d493212c. The SHA256 hash is b8e129e56c8cc166120c131c6eab2c8e4b9233367edf661c9956e1a. The SHA32 hash is 78181846. The CRC32 hash is 78181846. The file is identified as a 'win\_registry' type, which affects system registries. The 'Information on Execution' table shows a single analysis entry for the file, started on Nov 26, 2024, at 7:49 p.m., completed on Nov 26, 2024, at 7:54 p.m., with a duration of 293 seconds, routed to the Internet, and with logs available. The 'Signatures' section lists several events: 'Yara rule detected for file (1 event)', 'Allocates read-write-execute memory (usually to unpack itself) (1 event)', 'The binary likely contains encrypted or compressed data indicative of a packer (2 events)', 'File has been identified by 16 AntiVirus engines on IBM as malicious (16 events)', and 'File has been identified by 60 AntiVirus engines on VirusTotal as malicious (50 out of 60 events)'. The 'Score' section indicates that the file is very suspicious, with a score of 10 out of 10. A feedback message states: 'Please notice: The scoring system is currently still in development and should be considered an alpha feature.'

Category	Started	Completed	Duration	Routing	Logs
FILE	Nov 26, 2024, 7:49 p.m.	Nov 26, 2024, 7:54 p.m.	293 seconds	Internet	Show Analysis Log Show Cuckoo Log

Section	Entropy	Description
section	6.86368833863	A section with a high entropy has been found
entropy	0.663677130045	Overall entropy of this PE file is high

## 4. Quali sono i rischi per l'utente?

Se esegui questo file sul tuo computer, ecco cosa potrebbe succedere:

- **Perdita di dati:** Informazioni personali, come password o documenti, possono essere rubate.
- **Controllo remoto:** Un attaccante potrebbe usare il tuo computer per scopi illegali.
- **Compromissione del sistema:** Il malware potrebbe rallentare il computer o renderlo instabile.
- **Diffusione del malware:** Potrebbe utilizzare il tuo PC per infettare altri dispositivi nella rete.