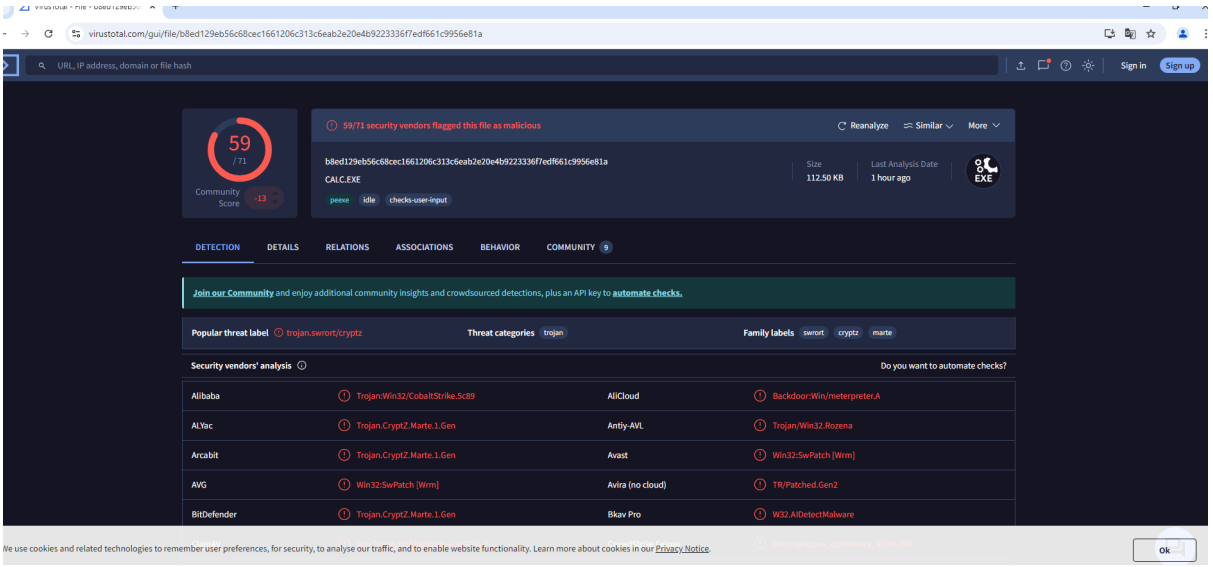
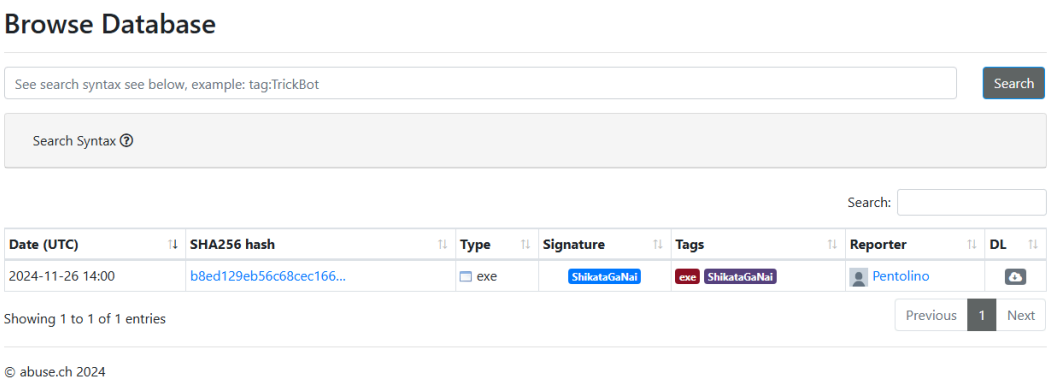
## S9L2 - Malware Analysis su calcolatriceinnovativa.exe

In questo esercizio, abbiamo analizzato il file **"calcolatriceinnovativa.exe"**, segnalato come sospetto da diversi strumenti di sicurezza. Lo scopo dell'analisi era comprendere il comportamento del malware e identificare le sue minacce potenziali.

Innanzitutto, il file è stato caricato su **VirusTotal**, dove ha ottenuto un punteggio di **59/71**. Questo indica che molti antivirus lo hanno identificato come **Trojan** o malware pericoloso. Questi risultati hanno confermato che il file è potenzialmente dannoso e che l'analisi approfondita era necessaria.




Successivamente, il file è stato esaminato su **MalwareBazaar**, dove è stato segnalato da un utente con caratteristiche significative, come la mancanza di protezioni di sicurezza. In particolare, mancavano protezioni come **NX (No Execute)** e **PIE (Position Independent Executable)**. L'assenza di queste protezioni rende più facile per il malware eseguire codice arbitrario nella memoria, poiché il sistema operativo non ha le difese necessarie per bloccare la sovrascrittura di memoria e l'esecuzione di codice dannoso.



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

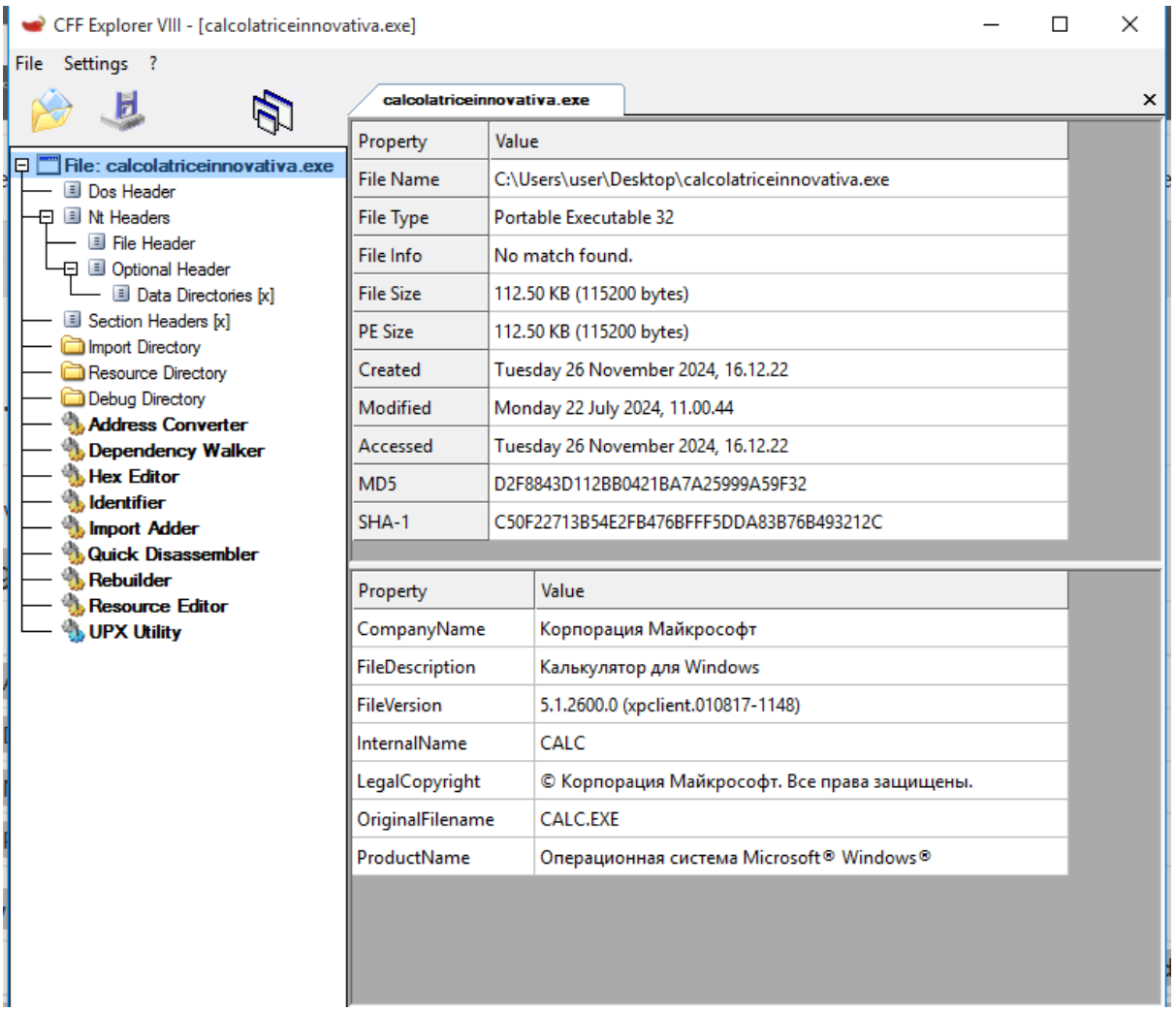
| ID | Title | Severity |
|---|---|---|
| CHECK_AUTHENTICODE | Missing Authenticode | high |
| CHECK_DLL_CHARACTERISTICS | Missing dll Security Characteristics (HIGH_ENTROPY_VA) | high |
| CHECK_NX | Missing Non-Executable Memory Protection | critical |
| CHECK_PIE | Missing Position-Independent Executable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

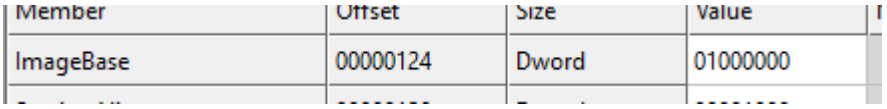
Reviews

| ID | Capabilities | Evidence |
|---|---|---|
| WIN32_PROCESS_API | Can Create Process and Threads | KERNEL32.dll::CloseHandle<br>KERNEL32.dll::CreateThread |
| WIN_BASE_API | Uses Win Base API | KERNEL32.dll::LoadLibraryA<br>KERNEL32.dll::GetStartupInfoA<br>KERNEL32.dll::GetCommandLineW |
| WIN_REG_API | Can Manipulate Windows Registry | ADVAPI32.dll::RegOpenKeyExA<br>ADVAPI32.dll::RegQueryValueExA |
| WIN_USER_API | Performs GUI Actions | USER32.dll::OpenClipboard<br>USER32.dll::CreateWindowExW |

Con **CFFExplorer**, abbiamo rilevato che il file aveva una **ImageBase statica**, indicando che il malware non cambia la posizione della memoria in cui il codice viene caricato in modo dinamico. Questo può facilitare l'esecuzione del codice dannoso e aggirare sistemi di protezione come la **Random Address Space Layout Randomization (ASLR)**. Abbiamo anche notato dipendenze da **kernel32.dll**, **advapi32.dll** e **user32.dll**:

- **kernel32.dll**: include funzioni come CreateEventW, CreateThreadW e ResetEvent. Queste API permettono al malware di gestire processi e thread nel sistema, manipolare la memoria e creare attività dannose.
- **advapi32.dll**: include funzioni come RegOpenKeyExA e RegQueryValueExA. Queste API consentono al malware di modificare il registro di sistema, dove i dati di configurazione possono essere manipolati per mantenere persistente il malware o per eseguire azioni dannose durante la riavvio del sistema.
- **user32.dll**: include funzioni come CreateWindowExW, utilizzate dal malware per interagire con l'interfaccia utente grafica. Queste API consentono al malware di visualizzare finestre di dialogo, sovrascrivere la finestra del desktop e manipolare la vista dell'utente per distrarlo o renderlo incapace di rilevare attività dannose.


CFF Explorer VIII - [calcolatriceinnovativa.exe]
File Settings ?
calcolatriceinnovativa.exe
File: calcolatriceinnovativa.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Resource Directory
Debug Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Property Value
File Name C:\Users\user\Desktop\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 Tuesday 26 November 2024, 16.12.22
Modified Monday 22 July 2024, 11.00.44
Accessed Tuesday 26 November 2024, 16.12.22
MD5 D2F8843D112BB0421BA7A25999A59F32
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®


Member Offset Size Value
ImageBase 00000124 Dword 01000000

calcolatriceinnovativa.exe

| Module Name | Imports | OFTs | TimeDateStamp | ForwarderChain | Name RVA | FTs (IAT) |
|---|---|---|---|---|---|---|
| 000125D4 | N/A | 00011FBC | 00011FC0 | 00011FC4 | 00011FC8 | 00011FCC |
| 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 |

| OFTs | FTs (IAT) | Hint | Name |
|---|---|---|---|
| | | | |
| Dword | Dword | Word | szAnsi |
| 000130FA | 77E71B14 | 01E9 | GlobalUnlock |
| 000130EA | 77E730C1 | 0047 | CreateEventW |
| 000130DA | 77E7AC37 | 0065 | CreateThread |
| 000130CC | 77E74A69 | 02A9 | ResetEvent |
| 000130C0 | 77E6F65E | 039C | lstrcpynW |
| 000130B4 | 77E74A3B | 02EC | SetEvent |
| 0001309E | 77E79D5B | 0365 | WaitForSingleObject |

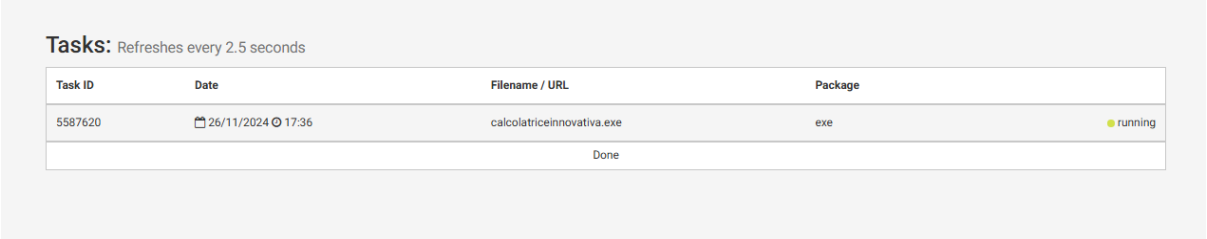
| msvcrt.dll | 26 | 00012DC8 | FFFFFFFF | FFFFFFFF | 00012F60 | 000011BC |
|---|---|---|---|---|---|---|
| ADVAPI32.dll | 3 | 00012C0C | FFFFFFFF | FFFFFFFF | 00012FFC | 00001000 |
| KERNEL32.dll | 30 | 00012C2C | FFFFFFFF | FFFFFFFF | 000131D4 | 00001020 |
| GDI32.dll | 3 | 00012C1C | FFFFFFFF | FFFFFFFF | 0001320C | 00001010 |
| USER32.dll | 69 | 00012CB0 | FFFFFFFF | FFFFFFFF | 000136A4 | 000010A4 |

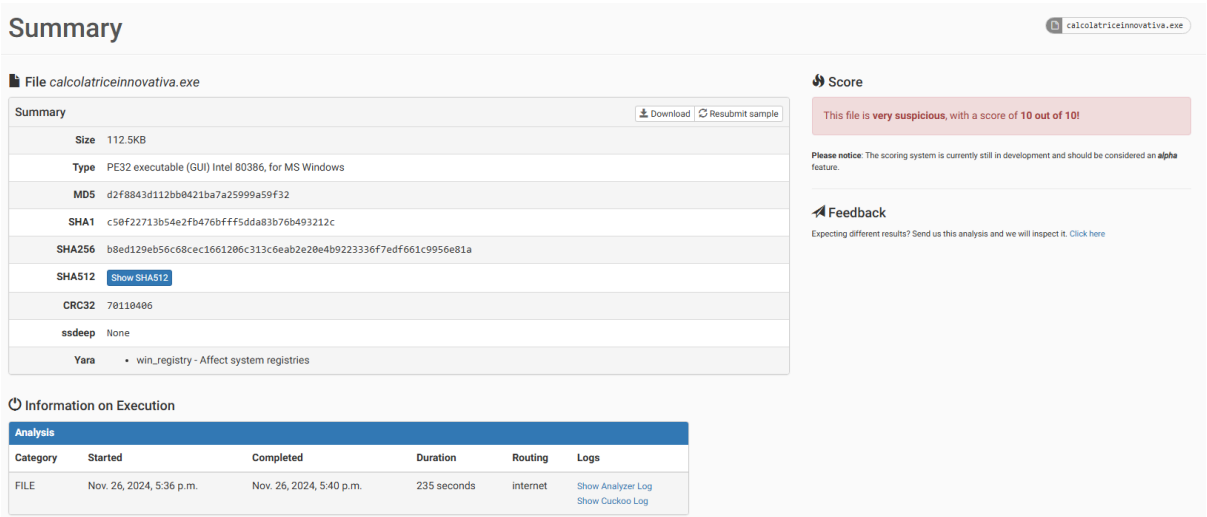
| OFTs | FTs (IAT) | Hint | Name |
|---|---|---|---|
| | | | |
| Dword | Dword | Word | szAnsi |
| 00012FEC | 77DC22EA | 01E1 | RegOpenKeyExA |
| 00012FD8 | 77DC23D7 | 01EB | RegQueryValueExA |
| 00012FCA | 77DC189A | 01C8 | RegCloseKey |

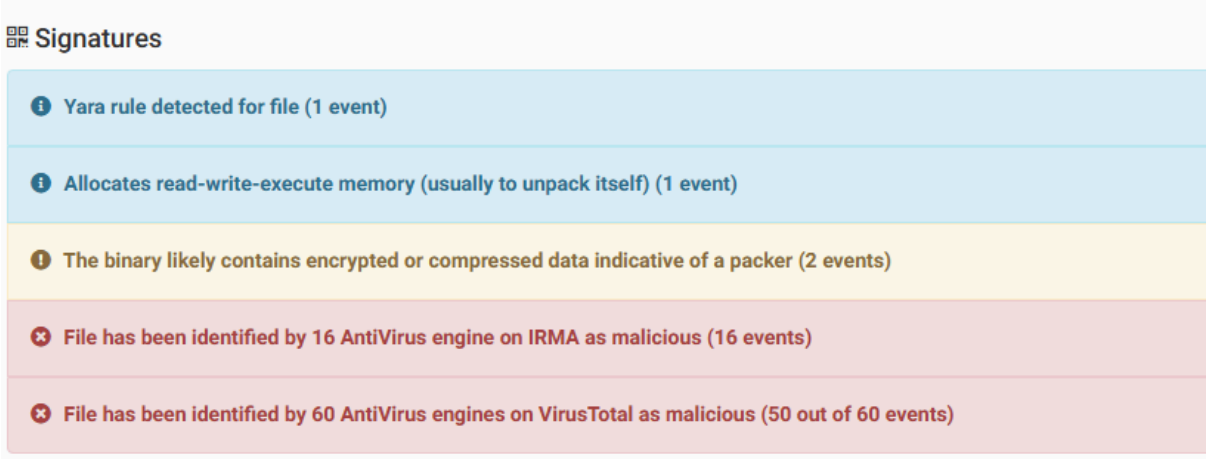
| GDI32.dll | 3 | 00012C1C | FFFFFFFF | FFFFFFFF | 0001320C | 00001010 |
|---|---|---|---|---|---|---|
| USER32.dll | 69 | 00012CB0 | FFFFFFFF | FFFFFFFF | 000136A4 | 000010A4 |

| OFTs | FTs (IAT) | Hint | Name |
|---|---|---|---|
| | | | |
| Dword | Dword | Word | szAnsi |
| 00013438 | 77D340BF | 013E | GetMessageW |
| 00013446 | 77D40D40 | 01B4 | LoadAcceleratorsW |
| 0001345A | 77D3AE4C | 0061 | CreateWindowExW |
| 0001346C | 77D68839 | 01E3 | MessageBoxW |

Infine, il file è stato caricato su **Cuckoo Sandbox** per un'analisi dinamica, dove ha ottenuto un punteggio di **10/10** per la sua pericolosità. Questo ha confermato che il malware può allocare memoria in modo sospetto, creare processi e manipolare il registro di sistema. L'analisi ha anche mostrato come il malware cerchi di rimanere nascosto nel sistema, mantenendo un comportamento persistente e pericoloso.



| Time & API | Arguments |
| --- | --- |
| **NtAllocateVirtualMemory**<br>Nov. 26, 2024, 5:36 p.m. | process_identifier: 1100<br>region_size: 4096<br>stack_dep_bypass: 0<br>stack_pivoted: 0<br>heap_dep_bypass: 0<br>protection: 64 (PAGE_EXECUTE_READWRITE)<br>process_handle: 0xffffffff<br>allocation_type: 4096 (MEM_COMMIT)<br>base_address: 0x002f0000 |
| **NtAllocateVirtualMemory**<br>Nov. 26, 2024, 5:36 p.m. | process_identifier: 1100<br>region_size: 1179648<br>stack_dep_bypass: 0<br>stack_pivoted: 0<br>heap_dep_bypass: 0<br>protection: 4 (PAGE_READWRITE)<br>process_handle: 0xffffffff<br>allocation_type: 8192 (MEM_RESERVE)<br>base_address: 0x00430000 |
| **NtFreeVirtualMemory**<br>Nov. 26, 2024, 5:36 p.m. | free_type: 32768<br>process_handle: 0xffffffff<br>process_identifier: 1100<br>base_address: 0x00430000<br>size: 917504 |
| **NtAllocateVirtualMemory**<br>Nov. 26, 2024, 5:36 p.m. | process_identifier: 1100<br>region_size: 4096<br>stack_dep_bypass: 0<br>stack_pivoted: 0<br>heap_dep_bypass: 0<br>protection: 4 (PAGE_READWRITE)<br>process_handle: 0xffffffff<br>allocation_type: 4096 (MEM_COMMIT)<br>base_address: 0x00510000 |

| Time & API | Arguments | Status | Return | Repeated |
| --- | --- | --- | --- | --- |
| **WSAStartup**<br>Nov. 26, 2024, 5:36 p.m. | wVersionRequested: 400 | 1 | 0 | 0 |
| **WSASocketA**<br>Nov. 26, 2024, 5:36 p.m. | type: 1<br>flags: 0<br>socket: 152<br>protocol: 0<br>af: 2 | 1 | 152 | 0 |
| **connect**<br>Nov. 26, 2024, 5:37 p.m. | ip_address: 192.168.1.80<br>socket: 152<br>port: 4444 | | 4294967295 | 0 |

Questo malware è un **Trojan** perché cerca di nascondersi e compromettere il sistema senza che l'utente se ne accorga. La mancanza di protezioni come **NX** e **PIE** rende il malware particolarmente pericoloso, poiché gli permette di eseguire codice dannoso facilmente. Le sue capacità di manipolare il sistema e persistente nel tempo lo rendono un'infezione difficile da rimuovere.

In conclusione, il file **"calcolatriceinnovativa.exe"** è un malware avanzato che può compromettere un computer, manipolare le impostazioni del sistema operativo e nascondersi per continuare a danneggiarlo. Il file è stato progettato per eludere le difese di sicurezza e agire senza essere rilevato, il che lo rende molto pericoloso.