

Analisi del Malware

Attività di Analisi del Malware

Oggetto: Sarà condiviso un malware relativamente innocuo.

Compiti:

Analisi Statica: Esaminare il codice del malware senza eseguirlo, al fine di comprendere la sua struttura e le sue funzionalità.

Analisi Dinamica: Eseguire il malware in un ambiente controllato per osservare il suo comportamento e identificare le sue azioni in tempo reale.

Cff Explorer + ProcMon

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

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, 11.08.38 |
| Modified | Monday 22 July 2024, 11.00.44 |
| Accessed | Monday 22 July 2024, 11.08.38 |
| 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® |

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

| Time ... | Process Name | PID | Operation | Path | Result | Detail |
|-----------|---------------------|------|------------------|---|----------------|-----------------------|
| 17:10:... | calcolatriceinno... | 2732 | Thread Exit | | SUCCESS | Thread ID: 5236, ... |
| 17:10:... | calcolatriceinno... | 2732 | Thread Exit | | SUCCESS | Thread ID: 2432, ... |
| 17:10:... | calcolatriceinno... | 2732 | Thread Exit | | SUCCESS | Thread ID: 32, Use... |
| 17:10:... | calcolatriceinno... | 2732 | TCP Reconnect | DESKTOP-9K104BT.wind3.hub.49603 ... | SUCCESS | Length: 0, sequen... |
| 17:10:... | calcolatriceinno... | 1796 | TCP Reconnect | DESKTOP-9K104BT.wind3.hub.49602 ... | SUCCESS | Length: 0, sequen... |
| 17:10:... | calcolatriceinno... | 2732 | TCP Reconnect | DESKTOP-9K104BT.wind3.hub.49603 ... | SUCCESS | Length: 0, sequen... |
| 17:10:... | calcolatriceinno... | 3304 | Process Start | | SUCCESS | Parent PID: 3668, ... |
| 17:10:... | calcolatriceinno... | 3304 | Thread Create | | SUCCESS | Thread ID: 2920 |
| 17:10:... | calcolatriceinno... | 3304 | Load Image | C:\Users\user\Desktop\Malware\calcol... | SUCCESS | Image Base: 0x100... |
| 17:10:... | calcolatriceinno... | 3304 | Load Image | C:\Windows\System32\ntdll.dll | SUCCESS | Image Base: 0x7fff... |
| 17:10:... | calcolatriceinno... | 3304 | Load Image | C:\Windows\SysWOW64\ntdll.dll | SUCCESS | Image Base: 0x7773... |
| 17:10:... | calcolatriceinno... | 3304 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Con... | REPARSE | Desired Access: Q... |
| 17:10:... | calcolatriceinno... | 3304 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Desired Access: Q... |
| 17:10:... | calcolatriceinno... | 3304 | CreateFile | C:\Windows | SUCCESS | Desired Access: E... |
| 17:10:... | calcolatriceinno... | 3304 | Load Image | C:\Windows\System32\wow64.dll | SUCCESS | Image Base: 0x590... |
| 17:10:... | calcolatriceinno... | 3304 | Load Image | C:\Windows\System32\wow64win.dll | SUCCESS | Image Base: 0x58f... |
| 17:10:... | calcolatriceinno... | 3304 | RegOpenKey | HKLM\SOFTWARE\Microsoft\WOW64 | SUCCESS | Desired Access: Q... |
| 17:10:... | calcolatriceinno... | 3304 | RegOpenKey | HKLM\Software\Microsoft\Windows N... | SUCCESS | Desired Access: Q... |
| 17:10:... | calcolatriceinno... | 3304 | RegOpenKey | HKLM\SOFTWARE\MICROSOFT\WIN... | NAME NOT FOUND | Desired Access: Q... |
| 17:10:... | calcolatriceinno... | 3304 | RegQueryValue | HKLM\SOFTWARE\MICROSOFT\WO... | NAME NOT FOUND | Length: 532 |
| 17:10:... | calcolatriceinno... | 3304 | RegCloseKey | HKLM\SOFTWARE\MICROSOFT\WO... | SUCCESS | |
| 17:10:... | calcolatriceinno... | 3304 | CreateFile | C:\Windows\System32\wow64log.dll | NAME NOT FOUND | Desired Access: R... |
| 17:10:... | calcolatriceinno... | 3304 | Load Image | C:\Windows\System32\kernel32.dll | SUCCESS | Image Base: 0x170... |
| 17:10:... | calcolatriceinno... | 3304 | Load Image | C:\Windows\SysWOW64\kernel32.dll | SUCCESS | Image Base: 0x771... |
| 17:10:... | calcolatriceinno... | 3304 | Load Image | C:\Windows\System32\kernel32.dll | SUCCESS | Image Base: 0x170... |
| 17:10:... | calcolatriceinno... | 3304 | Load Image | C:\Windows\System32\user32.dll | SUCCESS | Image Base: 0x170... |
| 17:10:... | calcolatriceinno... | 3304 | CreateFile | C:\Windows | SUCCESS | Desired Access: R... |
| 17:10:... | calcolatriceinno... | 3304 | QueryNameInfo... | C:\Windows | SUCCESS | Name: \Windows |
| 17:10:... | calcolatriceinno... | 3304 | CloseFile | C:\Windows | SUCCESS | |
| 17:10:... | calcolatriceinno... | 3304 | RegOpenKey | HKLM\Software\Microsoft\Wow64\86 | SUCCESS | Desired Access: R... |
| 17:10:... | calcolatriceinno... | 3304 | RegQueryValue | HKLM\SOFTWARE\MICROSOFT\WO... | NAME NOT FOUND | Length: 520 |
| 17:10:... | calcolatriceinno... | 3304 | RegQueryValue | HKLM\SOFTWARE\MICROSOFT\WO... | SUCCESS | Type: REG_SZ, Le... |
| 17:10:... | calcolatriceinno... | 3304 | RegCloseKey | HKLM\SOFTWARE\MICROSOFT\WO... | SUCCESS | |
| 17:10:... | calcolatriceinno... | 3304 | Load Image | C:\Windows\System32\wow64cpu.dll | SUCCESS | Image Base: 0x58f... |
| 17:10:... | calcolatriceinno... | 3304 | RegOpenKey | HKLM\SYSTEM\CurrentControlSet\Con... | REPARSE | Desired Access: Q... |
| 17:10:... | calcolatriceinno... | 3304 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | NAME NOT FOUND | Desired Access: Q... |
| 17:10:... | calcolatriceinno... | 3304 | CreateFile | C:\Users\user\Desktop\Malware | SUCCESS | Desired Access: E... |
| 17:10:... | calcolatriceinno... | 3304 | Load Image | C:\Windows\SysWOW64\kernel32.dll | SUCCESS | Image Base: 0x771... |
| 17:10:... | calcolatriceinno... | 3304 | Load Image | C:\Windows\SysWOW64\kernelBase.dll | SUCCESS | Image Base: 0x74f... |
| 17:10:... | calcolatriceinno... | 3304 | RegOpenKey | HKLM\System\CurrentControlSet\Contr... | REPARSE | Desired Access: Q... |

Virustotal / Hash

VirusTotal - File - b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a

virustotal.com/gui/file/b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a/details

b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a

59 / 71
Community Score -13

59/71 security vendors flagged this file as malicious

Reanalyze Similar

b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a
CALC.EXE
Size 112.50 KB
Last Analysis Date 46 minutes ago

peexe idle checks-user-input

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.

Basic properties

| | |
|---------------------|--|
| MD5 | d2f8843d112bb0421ba7a25999a59f32 |
| SHA-1 | c50f22713b54e2fb476bfff5dda83b76b493212c |
| SHA-256 | b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a |
| Vhash | 0150366d155035z3001e1afz12z45fz |
| Authentihash | 53b04defff6cff112e5a75ff418c43ed3a77f19ff297541a45cd0b5698bb0aff |
| Imphash | 08f6a1b121da8cedde2d1089d0906ed8 |
| Rich PE header hash | 72d42ffa6f32b6934c77b30731ebd5f1 |
| SSDEEP | 3072:DAq2By/0He97ulj7nt5CdLYkOE0pAWLnQoXPBsr5ZrR:DAqfB9yBJa70Ep0pLnQoo5Zd |
| TLSH | T197B39E01BA94F135C465113448D39FFA93BDBF1705AB16AB33097E4F7E362662A23286 |
| File type | Win32 EXE executable windows win32 pe peexe |
| Magic | PE32 executable (GUI) Intel 80386, for MS Windows |
| TrID | Win32 Executable MS Visual C++ (generic) (43.3%) Microsoft Visual C++ compiled executable (generic) (22.9%) Win32 Dynamic |
| DetectItEasy | PE32 Compiler: Microsoft Visual C/C++ (13.00.9178) [C++] Linker: Microsoft Linker (7.00.9210) Tool: Visual Studio (2002) |
| Magika | PEBIN |
| File size | 112.50 KB (115200 bytes) |

History

| | |
|------------------|-------------------------|
| Creation Time | 2001-04-03 17:55:45 UTC |
| First Submission | 2023-12-11 16:06:21 UTC |

Microsoft Bing

b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a

CERCA COPILOT IMMAGINI VIDEO MAPPE NOTIZIE SHOPPING ESPANDI

Informazioni sui risultati di 16.000.000

MalwareBazaar
https://bazaar.abuse.ch/sample/...
MalwareBazaar | SHA256 ...
MalwareBazaar Database. You are currently viewing the MalwareBazaar entry for SHA256

cuckoo.ee/analysis/5587624/summary/

Summary

File *calcatriceinnovativa.exe*

| Summary | | Download | Resubmit sample |
|---------|--|----------|-----------------|
| Size | 112.5KB | | |
| Type | PE32 executable (GUI) Intel 80386, for MS Windows | | |
| MDS | d2f8843d112bb0421ba7a25999a59f32 | | |
| SHA1 | c50f22713b54e2fb476bff5dda83b76b493212c | | |
| SHA256 | b0ed129eb56c68cec1661206c313c6aab2e20e4b9223336f7edf661c9956e81a | | |
| SHA512 | Show SHA512 | | |
| CRC32 | 70110406 | | |
| ssdeep | None | | |
| Yara | • win_registry - Affect system registries | | |

Score

This file is **very suspicious**, with a score of 10 out of 10!

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

Feedback

Expecting different results? Send us this analysis and we will inspect it.
[Click here](#)

Information on Execution

| Analysis | | | | | |
|----------|--------------------------|--------------------------|-------------|----------|--|
| Category | Started | Completed | Duration | Routing | Logs |
| FILE | Nov. 26, 2024, 5:53 p.m. | Nov. 26, 2024, 5:57 p.m. | 266 seconds | internet | Show Analyzer Log Show Cuckoo Log |

Relazione

Per analizzare il malware, ho utilizzato cinque strumenti principali: CFF Explorer, ProcMon, VirusTotal, Malware Bazaar e Cuckoo. Questi strumenti mi hanno aiutato a capire meglio cosa fa il malware sia guardando il suo codice senza eseguirlo (analisi statica), sia osservando come si comporta mentre viene eseguito (analisi dinamica).

Analisi Statica:

Per l'analisi statica, ho usato CFF Explorer per esaminare il file del malware. Questo programma mi ha permesso di vedere la struttura del file, come le librerie che usa e le sezioni che contiene. Senza eseguire il malware, ho potuto identificare alcune informazioni importanti, come le funzioni che potrebbero essere utilizzate per scopi malevoli.

Poi, ho caricato il file su VirusTotal. Questo strumento mi ha aiutato a vedere se altri antivirus avevano già riconosciuto il file come dannoso. Con VirusTotal, è facile capire se il malware è già conosciuto da altri esperti di sicurezza. Infine, ho cercato il malware su Malware Bazaar, tramite l'hash trovato su VirusTotal, la ricerca l'ho fatto su Edge, in quanto Chrome, in qualche modo filtra le ricerche per proteggere l'utente.

Malware Bazaar è un archivio di campioni di malware dove puoi trovare informazioni su file simili e scoprire se il malware che sto analizzando ha delle varianti note o è stato già analizzato.

Analisi Dinamica:

Per l'analisi dinamica, ho utilizzato Cuckoo tramite il servizio online cuckoo.ee per caricare il file del malware e analizzarlo in un ambiente sicuro. Cuckoo ha generato un report dopo aver analizzato il file.

Per monitorare ulteriormente il comportamento del malware, ho usato ProcMon. Questo strumento mi ha consentito di vedere tutte le operazioni che il malware stava cercando di eseguire, come la creazione o la modifica del file e le modifiche al registro del sistema.

In questo modo, con l'analisi statica ho ottenuto una comprensione iniziale del file senza eseguirlo, mentre con l'analisi dinamica ho potuto osservare direttamente il suo comportamento per capire meglio come agisce quando viene eseguito.