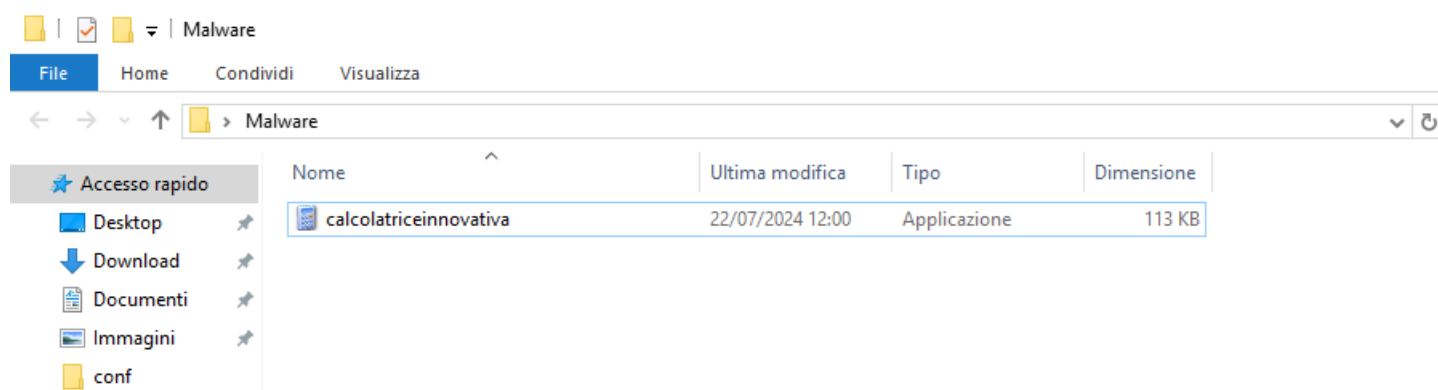


Introduzione:

Il compito di oggi era svolgere un'analisi sia **statica** ma anche **dinamica**, del **malware** presente all'interno della macchina exploitabile Windows 10. Ovvero **calcolatriceinnovativa**:



1) Che cos'è l'analisi statica?

L'analisi statica è una tecnica di analisi del malware che consiste nell'esaminare il codice di un programma senza eseguirlo.

Punti a favore sono:

Sicurezza, Completezza, Velocità, Individuazione di vulnerabilità;

Punti a sfavore invece sono:

Limitazioni nell'interpretazione, Offuscamento del codice, Tempo e risorse, Conoscenza tecnica, Falsi positivi;

2) Che cos'è l'analisi dinamica?

A differenza dell'analisi statica che esamina il codice senza eseguirlo, l'analisi dinamica coinvolge l'esecuzione controllata del malware in un ambiente **isolato e sicuro**.

Punti a favore:

Osservazione diretta del comportamento, rilevamento di tecniche evasive, raccolta di indicatori di compromissione;

Punti a sfavore:

Necessità di un ambiente controllato, possibile mancato rilevamento.

Pratica:

Prima di tutto ho fatto analizzare al software **VirusTotal** (analizza file, URL, domini e indirizzi IP sospetti per rilevare malware e altri tipi di minacce) l'applicazione per determinare se fosse o meno un **malware**, e la risposta è **chiaramente positiva**:

59/71 security vendors flagged this file as malicious

Reanalyze Similar More

b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a

Size: 112.50 KB | Last Analysis Date: 57 minutes ago

CALC.EXE

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.

Popular threat label: trojan.swort/cryptz | Threat categories: trojan | Family labels: swort cryptz marte

Security vendors' analysis

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

Successivamente tramite un **motore di ricerca** ho cercato il **malware** per vedere se ci fossero notizie a riguardo e se potessi trovare informazioni importanti riguardo quest'ultimo:

Google

calcolatrice innovativa malware

Tutti Video Immagini Notizie Web Libri Finanza Altro Strumenti

Red Hot Cyber
https://www.redhotcyber.com › post › moses-staff-utiliz...
Moses Staff utilizza un RAT che si maschera da ...
6 feb 2022 — La società di sicurezza Cybereason ha scoperto un nuovo Trojan di accesso remoto (RAT) chiamato StrifeWater, associato agli hacker del ...

Cliccando sul primo risultato si apre una pagina che parla di questo malware in particolare:

Moses Staff utilizza un RAT che si maschera da calcolatrice di Windows per avviare l'attacco.

Redazione RHC : 6 Febbraio 2022 07:54

La società di sicurezza Cybereason [ha scoperto un nuovo Trojan di accesso remoto \(RAT\) chiamato StrifeWater](#), associato agli hacker del gruppo di hacktivisti Moses Staff. Sui sistemi vittime, il malware si maschera da calcolatore di Windows.

Il gruppo Moses Staff è stato segnalato per la prima volta dai ricercatori di Check Point nel 2021, il quale ha attaccato le organizzazioni israeliane, ha violato le loro reti, crittografato i dati e poi si è rifiutato di negoziare un riscatto.

Infatti, i ricercatori di [sicurezza informatica](#) hanno riportato che si trattava di **attacchi politicamente motivati e deliberatamente distruttivi**. Ma ad oggi, molte aziende al di fuori di Israele sono diventate vittime di questo gruppo di criminali informatici.

- Innovazione tecnologica
- Intelligenza artificiale
- Interviste
- News
- Post sponsorizzati
- Psicologia e tecnologia
- Risk Management
- Social Network
- Storia dell'informatica

Vuoi diventare un Ethical Hacker?

Iscriviti ora al corso in partenza e approfitta dell'imperdibile promozione.

Utilizzando il codice RHC
Il 5% verrà devoluto alla nostra community.

SCOPRI DI PIÙ



Che successivamente mi rimanda a questo link:

BLOG

StrifeWater RAT: Iranian APT Moses Staff Adds New Trojan to Ransomware Operations



cybereason®

Dove troviamo informazioni importantissime riguardo il malware:

Nuovo Remote Access Trojan (RAT): Un RAT recentemente non documentato chiamato StrifeWater è stato valutato come parte dell'arsenale utilizzato dal gruppo APT iraniano Moses Staff. Si ritiene che il RAT venga impiegato specificamente nella fase iniziale dell'infezione e successivamente sostituito con altri strumenti.

Varie funzionalità: Il RAT StrifeWater offre diverse capacità, tra cui: elencare i file di sistema, eseguire comandi di sistema, acquisire schermate, creare persistenza e scaricare aggiornamenti e moduli ausiliari.

Sotto il radar: Il RAT StrifeWater sembra essere rimosso dall'ambiente infetto prima del dispiegamento del ransomware. Questa potrebbe essere la ragione per cui il RAT non è stato rilevato in precedenza.

Ransomware sponsorizzato dallo stato: Moses Staff impiega il ransomware post-esfiltrazione non per ottenere guadagni finanziari, ma per interrompere le operazioni, oscurare l'attività di spionaggio e infliggere danni ai sistemi per avanzare gli obiettivi geopolitici dell'Iran.

Vittime in tutto il mondo: La lista delle vittime di Moses Staff include numerosi paesi e regioni, tra cui: Israele, Italia, India, Germania, Cile, Turchia, Emirati Arabi Uniti e Stati Uniti.

CFF Explorer:

Successivamente con **CFF Explorer** uno strumento avanzato che permette di analizzare i file **PE** (Portable Executable, .exe, .dll), ho ispezionato il file:



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

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	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®

Controllando il **TimeDateStamp** non risulta nulla di strano, dato che la data risulta essere **19 aprile 2001, 11:47:13 (UTC)**:

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

Member	Offset	Size	Value	Meaning
Machine	000000F4	Word	014C	Intel 386
NumberOfSections	000000F6	Word	0003	
TimeDateStamp	000000F8	Dword	3ACA0EA1	
PointerToSymbolTa...	000000FC	Dword	00000000	
NumberOfSymbols	00000100	Dword	00000000	
SizeOfOptionalHea...	00000104	Word	00E0	
Characteristics	00000106	Word	010F	Click here

La presenza di questo flag in un file non progettato per ambienti Terminal Server potrebbe destare sospetti. Potrebbe essere un tentativo di **eludere controlli** in sessioni remote.

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

Member	Offset	Size	Value	Meaning
Magic	00000108	Word	010B	PE32
MajorLinkerVersion	0000010A	Byte	07	
MinorLinkerVersion	0000010B	Byte	00	
SizeOfCode	0000010C	Dword	00012800	
SizeOfInitializedData	00000110	Dword	00009600	
SizeOfUninitializedData	00000114	Dword	00000000	
AddressOfEntryPoint	00000118	Dword	00011FB2	.text
BaseOfCode	0000011C	Dword	00001000	
BaseOfData				
ImageBase				
SectionAlignmer				
FileAlignment				
MajorOperatingS				
MinorOperatingS				
MajorImageVersi				
MinorImageVersi				
MajorSubsystem				
MinorSubsystem				
Win32VersionVal				
SizeOfImage				
SizeOfHeaders				
Checksum	00000148	Dword	00000000	
Subsystem	0000014C	Word	0002	Windows GUI
DllCharacteristics	0000014E	Word	8000	Click here

DllCharacteristics

- ☐ DLL can move
- ☐ Code Integrity Image
- ☐ Image is NX compatible
- ☐ Image understands isolation and doesn't want it
- ☐ Image does not use SEH
- ☐ Do not bind this image
- ☐ Driver uses WDM model
- ☒ Terminal Server Aware

OK Cancel

In **USER32.dll** fornisce funzioni per l'interazione con l'interfaccia utente (messaggi, finestre, dialoghi). In un contesto sospetto potrebbe essere utilizzata per keylogging o per imitare finestre legittime.

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

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
00012AA4	N/A	00011FE4	00011FE8	00011FEC	00011FF0	00011FF4
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
000133DA	77D33DC5	00A2	DispatchMessageW
000133EE	77D33DD3	02AA	TranslateMessage
00013402	77D34024	02A8	TranslateAcceleratorW
0001341A	77D378FF	019E	IsChild
00013424	77D38518	01A2	IsDialogMessageW
00013438	77D340BF	013E	GetMessageW
00013446	77D40D40	01B4	LoadAcceleratorsW
0001345A	77D3AE4C	0061	CreateWindowExW
0001346C	77D68839	01E3	MessageBoxW
0001347A	77D3718C	01C9	LoadStringW
00013488	77D7E3E6	0267	SetProcessDefaultLayout
000134A2	77D5EEA0	0147	GetProcessDefaultLayout

Dall'elenco delle funzioni associate a questa libreria possiamo fare alcune considerazioni:

MessageBoxW: Potrebbe essere usata dal malware per visualizzare messaggi all'utente (es. richieste di riscatto nei ransomware).

CreateWindowExW: Utilizzata per creare finestre. Potenzialmente usata per imitare interfacce utente legittime.

DispatchMessageW, TranslateMessage: Usate per gestire eventi nell'interfaccia utente. Anche queste sono normali, ma se combinate con altre azioni sospette (es. keylogging), potrebbero essere rilevanti.

SetProcessDefaultLayout: È piuttosto insolita e potrebbe indicare manipolazioni più specifiche, anche se da sola non è immediatamente sospetta.

GetMessageW: Permette di ricevere messaggi dalla coda. In combinazione con funzioni che monitorano eventi, potrebbe essere usata per intercettare input dell'utente.