
malware analysis

Nel compito di oggi abbiamo fatto due analisi del malware presente nella nostra macchina virtuale di windows 10 pro, nello specifico abbiamo fatto un'analisi statica per capire che tipo di malware era e successivamente un'analisi dinamica per vedere il comportamento di questo malware.

ANALISI STATICA:

Per fare la nostra analisi statica abbiamo utilizzato diversi tool come virus total, cff explorer e chat gpt per capire appunto quale fosse la rilevabilità del virus, il tipo e altre informazioni che abbiamo estrapolato come vediamo nelle immagini:

ANALISI CON VIRUS TOTAL:

59
/71

Community Score

-11

59/71 security vendors flagged this file as malicious

Reanalyze Similar More

b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a

Size
112.50 KB

Last Analysis Date
1 minute ago

EXE

peexe

idle

checks-user-input

DETECTION

DETAILS

RELATIONS

ASSOCIATIONS

BEHAVIOR

COMMUNITY 4

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

☒ Display grouped sandbox reports

C2AE

1

0

0

0

0

0

Microsoft Sysinternals

0

0

0

0

26

3

Zenbox

2

4

0

0

0

0

Activity Summary

Download Artifacts Full Reports Help

2 Detections

2 MALWARE 1 TROJAN

Mitre Signatures

7 INFO

IDS Rules

NOT FOUND

Sigma Rules

NOT FOUND

Dropped Files

26 OTHER

Zenbox

Network comms

3 IP

Behavior Tags

ANALISI CON CFF EXPLORER:

Windows 10 pro - Metasploitable [In esecuzione] - Oracle VirtualBox

CFF Explorer VIII - [calcolatriceinnovativa.exe]

File Settings ?

ExplorerSuite.exe 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 Addr
- Quick Disassembler
- Rebuilder
- Resource Editor
- UPX Utility

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®

3. Analisi dei Metadati

I dettagli riportano informazioni relative a un'applicazione apparentemente legittima:

- Il file si presenta come una copia della calcolatrice di Windows (calc.exe) di un sistema operativo Windows XP.
- I metadati indicano che il produttore è "Microsoft Corporation", ma potrebbero essere stati modificati per mascherare un file malevolo.

4. Considerazioni Sospette

1. Dimensione inconsueta:
Il file ha una dimensione di 112 KB, mentre l'applicazione calc.exe originale di Windows XP è generalmente più piccola. Questo potrebbe indicare la presenza di codice aggiunto (es. malware).
2. Hash del file:
Gli hash MD5 e SHA-1 devono essere confrontati con le versioni ufficiali di calc.exe. Qualsiasi discrepanza confermerebbe la modifica del file.
3. Metadati anomali:
I dettagli sembrano legittimi, ma i malware spesso falsificano i metadati per imitare applicazioni conosciute e ridurre i sospetti.

Conclusione

Il file `calcolatricinnovativa.exe` potrebbe sembrare legittimo, ma la sua dimensione anomala, l'uso di metadati standard e la posizione in una cartella chiamata "Malware" suggeriscono un file compromesso o malevolo. Un'analisi più approfondita (statica e dinamica) è necessaria per confermare la natura del file.

ANALISI DINAMICA:

Per fare l'analisi dinamica ci siamo serviti del tool cuckoo per vedere il comportamento effettivo del malware in questione.

Come possiamo vedere nelle seguenti immagini, caricando il malware nel sito possiamo vedere molte informazioni riguardo quello che è il reale scopo del malware:

Il file *calcolatriceinnovativa.exe*

Riepilogo

Scaricamento Reinvia il campione

Misurare 112,5 KB

Tipo Esecuibile PE32 (GUI) Intel 80386, per MS Windows

MD5 d2f8843d112bb0421ba7a25999a59f32

SHA1 c50f22713b54e2fb476bfff5dda83b76b493212c

SHA256 b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a

SHA512 [Mostra SHA512](#)

CRC32 70110406

profondo Nessuno

lara

- win_registry - Influenza i registri di sistema

Informazioni sull'esecuzione


Analisi					
Categoria	Iniziato	Completato	Durata	Instradamento	Registri
FILE	26 novembre 2024, 16:58	26 novembre 2024, 17:02	233 secondi	Internet	Mostra registro analizzatore Mostra registro cuculo


Analisi

Categoria	Iniziato	Completato	Durata	Instradamento	Registri
FILE	26 novembre 2024, 16:58	26 novembre 2024, 17:02	233 secondi	Internet	Mostra registro analizzatore Mostra registro cuculo

Firme

 Regola Yara rilevata per il file (1 evento)

 Assegna memoria di lettura-scrittura-esecuzione (solitamente per decomprimere se stesso) (1 evento)

 Il binario probabilmente contiene dati criptati o compressi indicativi di un packer (2 eventi)

 Il file è stato identificato da 16 motori AntiVirus su IRMA come dannoso (16 eventi)

 Il file è stato identificato da 59 motori AntiVirus su VirusTotal come dannoso (50 su 59 eventi)

Regola Yara rilevata per il file (1 evento)

descrizione	Influenzare i registri di sistema	regola	registro_vittoria
-------------	-----------------------------------	--------	-------------------

Assegna memoria di lettura-scrittura-esecuzione (solitamente per decomprimere se stesso) (1 evento)

Tempo e API	Argomenti	Stato	Ritorno	Ripetuto
NtAllocateVirtualMemory 26 novembre 2024, 16:58	process_idenfier: 220 region_size: 4096 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x00200000 allocation_type: 4096 (MEM_COMMIT) process_handle: 0xffffffff	1	0	0

Il binario probabilmente contiene dati criptati o compressi indicativi di un packer (2 eventi)

sezione	{u'dimensione_dati': u'0x00012800', u'indirizzo_virtuale': u'0x00001000', u'entropia': 6,863688338632866, u'nome': u'.testo', u'dimensione_virtuale': u'0x000126b0'}	entropia	6,86368833863	descrizione	È stata trovata una sezione con un'entropia elevata
entropia	0,663677130045	descrizione	L'entropia complessiva di questo file PE è elevata		

❌ Il file è stato identificato da 16 motori AntiVirus su IRMA come dannoso (16 eventi)

Antivirus G Data (Windows)	Virus: Trojan.CryptZ.Marte.1.Gen (motore A)
Sicurezza di Avast Core (Linux)	Win32:SwPatch [Wrm]
C4S ClamAV (Linux)	Win.Trojan.MSShellcode-6360730-0
Antivirus F-Secure (Linux)	Trojan.TR/Patched.Gen2 [Acquario]
Protezione di Windows (Windows)	Trojan:Win32/Meterpreter.A
Forticlient (Linux)	W32/Swrort.C!tr
Antivirus Sophos (Linux)	Mal/EncPk-ACE
eScan Antivirus (Linux)	Trojan.CryptZ.Marte.1.Gen(DB)
Sicurezza ESET (Windows)	una variante del trojan Win32/Rozena.DT
Scanner CLI McAfee (Linux)	Trojan swrort.d
Antivirus DrWeb (Linux)	Trojan.Swrort.1
Trend Micro SProtect (Linux)	BKDR_SWRORT.SM
ClamAV (Linux)	Win.Trojan.MSShellcode-6360730-0
Antivirus Bitdefender (Linux)	Trojan.CryptZ.Marte.1.Gen
Kaspersky Standard (Windows)	HEUR:Trojan.Win32.Generic
Scanner della riga di comando Emsisoft (Windows)	Trojan.CryptZ.Marte.1.Gen (B)

Report Analisi Malware: calcolatricinnovativa.exe

1. Riepilogo del File

Dimensione: 112,5 KB.

Tipo: Eseguibile PE32 (GUI), architettura Intel 80386, per sistemi Microsoft Windows.

Hash:

MD5: d2f8843011b8234baf32999a59f3f532

SHA1: c50f22713b5e4b7f6bff5dda83b76492132c

SHA256: b8ed12eb56c8ce1661c26dc313c6aeb762336f7edf661c9956e81a

CRC32: 70118486

Regola YARA: Il file ha attivato una regola specifica associata alla modifica dei registri di sistema (win_registry), indicando un potenziale comportamento malevolo.

2. Informazioni sull'Esecuzione

Cronologia di Esecuzione

Inizio: 26 novembre 2024, 16:58.

Completamento: 26 novembre 2024, 17:02.

Durata: 233 secondi.

Rilevamento: Accesso a Internet (potenzialmente per comunicazione C2).

Registro: Mostra alterazioni o accessi ai registri di sistema.

Modifica di chiavi di registro per influenzare il comportamento del sistema.

3. Indicatori di Comportamento Sospetto

Entropia Elevata

Osservazioni: Il file presenta un'entropia molto elevata (6.86), indice di potenziale criptazione o offuscamento del codice.

Sezione PE sospetta:

Dimensione: 0x00001280.

Entropia della sezione: 6.86 (indicativa di compressione o dati criptati).

Conclusione: Il file potrebbe essere stato impacchettato o offuscato per nascondere il suo contenuto malevolo.

API Utilizzate

NtAllocateVirtualMemory: Allocazione dinamica di memoria con permessi PAGE_EXECUTE_READWRITE.

Utilizzato per caricare codice malevolo in memoria, solitamente indicativo di un loader o dropper

Argomenti principali:

Region_size: 4096.

Base_address: 0x00000000 (indirizzo allocato dinamicamente).

Potenziale obiettivo: Decodifica o caricamento di payload malevolo in memoria.

Regola YARA

La regola YARA ha identificato una firma specifica legata alla modifica dei registri di sistema, una tecnica comunemente utilizzata per:

Persistenza.

Disabilitare funzionalità di sicurezza.

Alterare il comportamento del sistema.

4. Identificazione dai Motori Antivirus

Il file è stato identificato come malevolo da 16 diversi motori antivirus. Dettagli delle rilevazioni:

Trojan: Varianti identificate includono Trojan.CryptZ, Win32.MSShellcode, e Trojan.SwPatch.

Specifiche: CryptZ: Famiglia di trojan noti per la crittografia o offuscamento.

Meterpreter.A: Modulo di Metasploit, spesso utilizzato per prendere il controllo remoto di un sistema.

Patched.Gen2: Eseguibili legittimi modificati con codice malevolo.

Packer Malevolo: Rilevato comportamento tipico di un packer offuscato (es. Mal/EncPk-ACE).

5. Valutazione del Rischio

Comportamento Potenziale

Persistenza: Probabile modifica di chiavi di registro per sopravvivere ai riavvii.

Esecuzione in Memoria: Il file potrebbe auto-decomprimersi e iniettare codice malevolo in un altro processo.

Crittografia: Offuscamento del payload per evitare rilevamenti.

Comunicazione di Rete: Presente attività Internet, potenzialmente per comunicazione con un server di comando e controllo (C2).

Classificazione Generale

Il file **calcolatricinnovativa.exe** si comporta come un trojan multiuso, con capacità di offuscamento, iniezione di codice e potenziale comunicazione remota.

Conclusione

Il file **calcolatricinnovativa.exe** è stato confermato malevolo, con comportamenti tipici di un trojan offuscato e capacità di modificare i registri e comunicare con server remoti. È consigliabile isolarlo e procedere con un'analisi approfondita in un ambiente controllato.