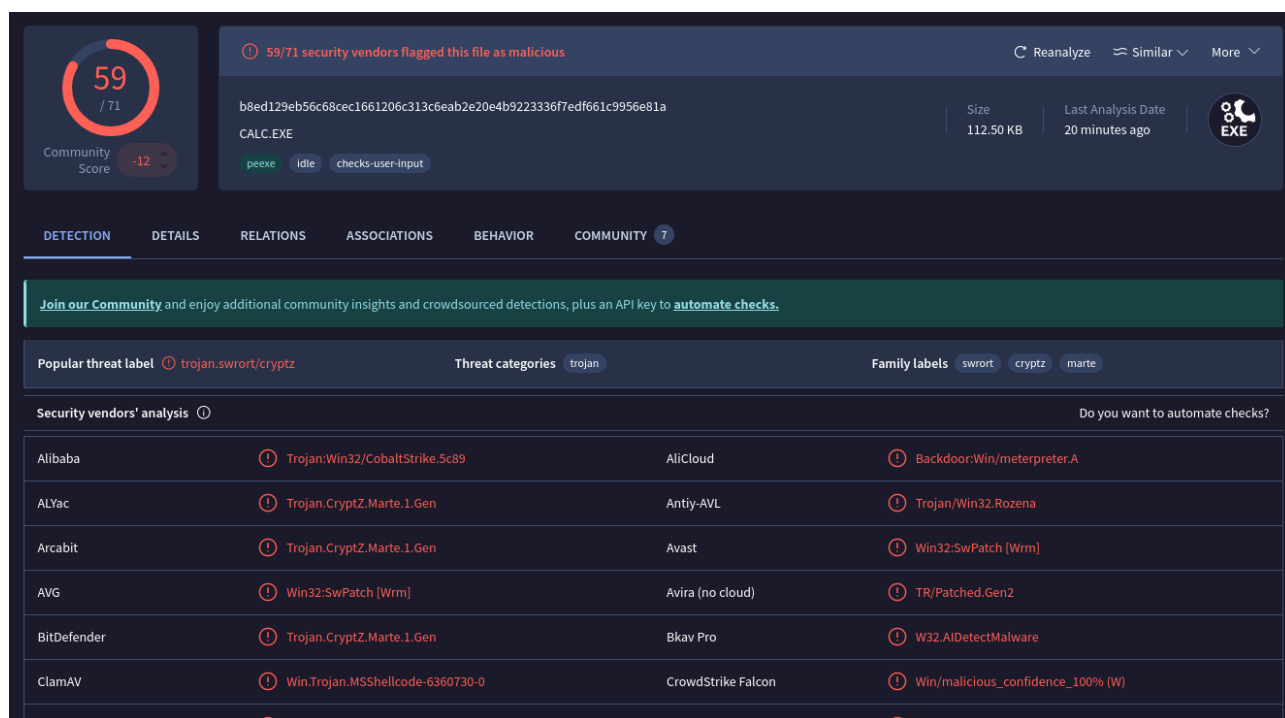


VirusTotal



Informazioni rilevanti

- File analizzato: CALC.EXE
- Hash: b8ed129eb5... (parziale).
- Rilevazioni: 59/71 motori antivirus identificano il file come malevolo.
- Minacce comuni identificate:
 - Trojan.CryptZ.Marte.1.Gen (varie denominazioni da più motori antivirus).
 - Backdoor (Meterpreter).
 - CobaltStrike (strumento spesso utilizzato per exploit e movimento laterale).

Interpretazione

1. Famiglia malware:

- Etichettato come trojan.swrort/cryptz e trojan.cryptz.marte. Il malware sembra appartenere a una categoria Trojan con capacità di crittografia/offuscamento.
- Meterpreter e CobaltStrike indicano che il malware potrebbe essere una backdoor, progettata per consentire il controllo remoto del sistema infetto.

2. Minacce principali:

- Capacità di controllo remoto (Meterpreter).
- Possibile offuscamento o packing (CobaltStrike potrebbe essere usato per nascondere il payload).
- Potenziale utilizzo di server Command & Control (C2) per esfiltrare dati o eseguire comandi.

3. Comunità:

- Il punteggio di comunità è -12, suggerendo un file ampiamente sospetto e pericoloso.

CFF Explorer

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	TimeStamp	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
0001305C	77E79A45	0238	LocalFree
00013028	77E79881	0234	LocalAlloc
00013036	77E67FD7	0198	GetProfileStringW
00013118	77E7166F	01E2	GlobalLock
0001300A	77E7C9DB	00FE	GetCommandLineW
0001301C	77E73679	0399	lstrcpyW
0001304A	77E641D5	0194	GetProfileIntW

Informazioni estratte

• Import Directory:

◦ Moduli importati: SHELL32.dll, msvcrt.dll, ADVAPI32.dll, KERNEL32.dll, GDI32.dll, USER32.dll.

◦ Funzioni particolari:

▪ GetCommandLineW: Recupera la riga di comando del processo (potenziale controllo del comportamento del malware in esecuzione).

▪ GlobalLock, LocalAlloc, GlobalFree: Tipiche di gestione della memoria (potenziale segnale di operazioni sullo heap).

▪ GetProfileStringW: Recupera informazioni da file di configurazione, spesso per determinare configurazioni del sistema target.

Interpretazione

1. Uso di API sospette:

◦ GetCommandLineW:

▪ Il malware potrebbe leggere la propria riga di comando per analizzare parametri forniti al momento dell'esecuzione.

- GetProfileStringW:

- Può essere usata per leggere informazioni di configurazione, a volte per determinare istruzioni di connessione a un server C2.

- LocalAlloc e GlobalLock:

- Utili per allocare memoria dinamica, spesso segnale di attività di offuscamento o decrittazione di payload runtime.

2. Analisi dei moduli importati:

- KERNEL32.dll:

- API fondamentali come gestione di file, memoria, e processi.

- ADVAPI32.dll:

- Utile per manipolazioni del Registro di sistema o per interazioni con la sicurezza locale.

- USER32.dll:

- Implicazioni grafiche o di input (es. keylogger?).

- GDI32.dll:

- Uso meno comune, potrebbe implicare manipolazioni grafiche specifiche.

3. Header e timestamp:

- Il timestamp falso o anomalo nell'intestazione PE è spesso usato dai malware per nascondere la data di creazione originale.

Analisi Statica:

- Dall'import directory del file emerge un potenziale uso delle funzioni di memoria e API critiche (es. GetCommandLineW) che supporta la teoria del trojan/backdoor identificato in VirusTotal.

- Le funzioni importate suggeriscono che il malware ha capacità di interagire con il sistema operativo per manipolare file, registro e connessioni.

[MalwareBazaar | SHA256](#)

[b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a \(ShikataGaNai\)](#)

si possono ottenere maggiori informazioni da Malware Bazaar