S9/L2 Mattia Montis

Attività di Analisi del Malware

Di seguito è riportata una relazione completa basata sui dati raccolti dalle schermate fornite.

1. Panoramica del Malware

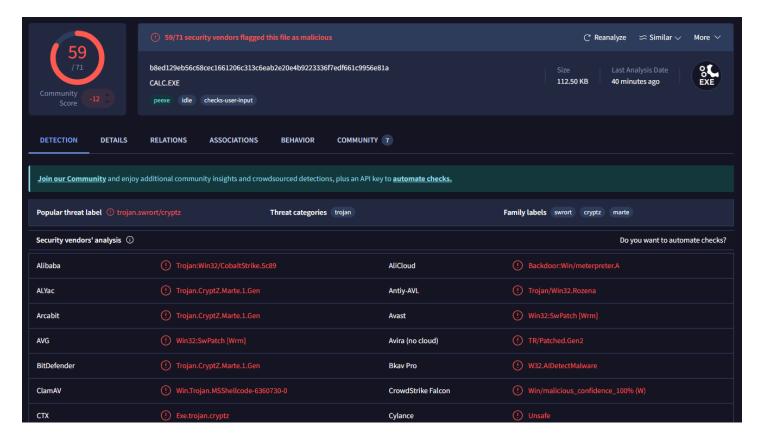
- Nome del file: calc.exe (alias calcolatriceinnovativa.exe)
- Dimensione: 112.50 KB (Malware Bazaar conferma 115.200 bytes)
- Hash SHA256:
 - b8ed129eb56c68cec1661206c313c6eab2e20e4b92233367fedf661c9956e81a
- Classificazione Generale: Trojan (etichettato con "trojan.swrort/cryptz")
- Comportamento principale: Likely backdoor e/o dropper.
- Rilevazioni dai Vendor (VirusTotal): 59/71 soluzioni antivirus hanno identificato il file come dannoso.

2. Analisi Statica

2.1. Risultati da VirusTotal

• Minacce associate:

- Trojan generici (es: Trojan.CryptZ.Marte.1.Gen, Win32/MShellcode, Backdoor:Win/meterpreter.A)
- Cobalt Strike, una piattaforma comunemente utilizzata per penetration testing, ma sfruttata anche da attori malevoli.
- Firma predominante: ShikataGaNai (un crypter/metamorphic encoder per nascondere il codice malevolo).



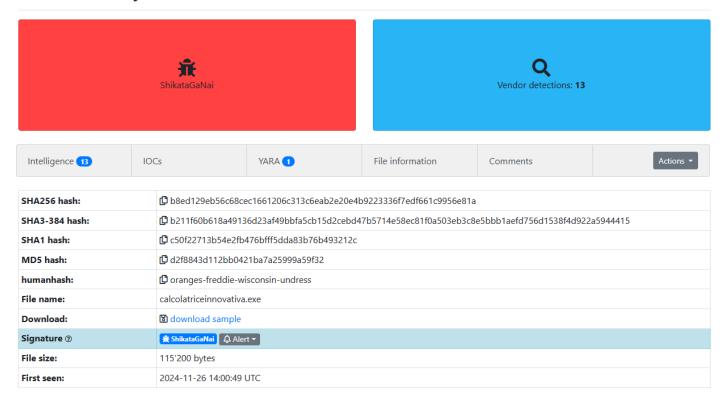
2.2. MalwareBazaar

- Firma ShikataGaNai: conferma che il codice è stato offuscato usando un encoder avanzato, noto per mutare il suo payload per evitare rilevamenti.
- Altri indicatori (IOC):
 - Hash multipli confermano unicità.
 - Nessuna descrizione completa del payload è fornita, il che suggerisce necessità di analisi dinamica per approfondire.

MalwareBazaar Database

You are currently viewing the MalwareBazaar entry for SHA256 b8ed129eb56c68cec1661206c313c6eab2e20e4b9223336f7edf661c9956e81a. While MalwareBazaar tries to identify whether the sample provided is malicious or not, there is no guarantee that a sample in MalwareBazaar is malicious.

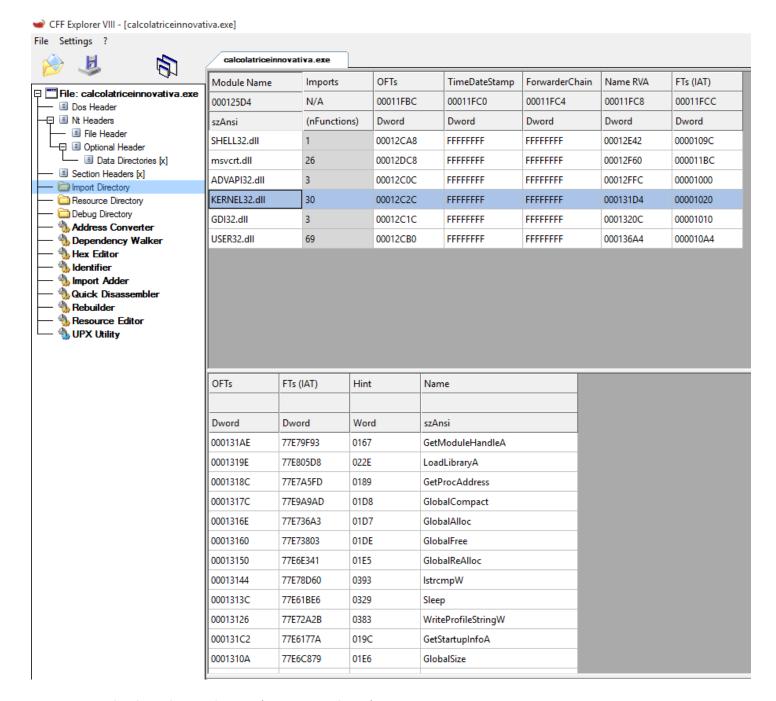
Database Entry



2.3. Analisi con CFF Explorer

L'analisi statica della struttura binaria mostra:

- Dipendenze Importate: Librerie critiche del sistema operativo Windows:
 - **KERNEL32.dll**: include funzioni come GetModuleHandleA, LoadLibraryA, e gestione della memoria (GlobalAlloc, GlobalFree).
 - SHELL32.dll e altre librerie usate per interazioni con il sistema operativo.
- Funzioni sospette identificate:
 - Sleep: potrebbe simulare inattività per evitare sandbox.
 - LoadLibraryA e GetProcAddress: spesso utilizzate per caricare funzioni a runtime, un comportamento caratteristico del codice offuscato o dinamico.
 - WriteProfileStringW: potrebbe modificare configurazioni o registri di sistema.



3. Analisi Dinamica (suggerita)

Per completare l'analisi, il file dovrà essere eseguito in un **sandbox sicuro**, come Cuckoo Sandbox o Any.Run, per osservare il comportamento runtime:

3.1. Aspettative

- Persistenza: Creazione di chiavi di registro o modifiche di configurazioni.
- Comunicazioni di rete: Tentativi di contattare un server C2 (Command and Control).
- Azioni ostili: Potenziale rilascio di payload aggiuntivi (es: ransomware, keylogger).

3.2. Cosa monitorare

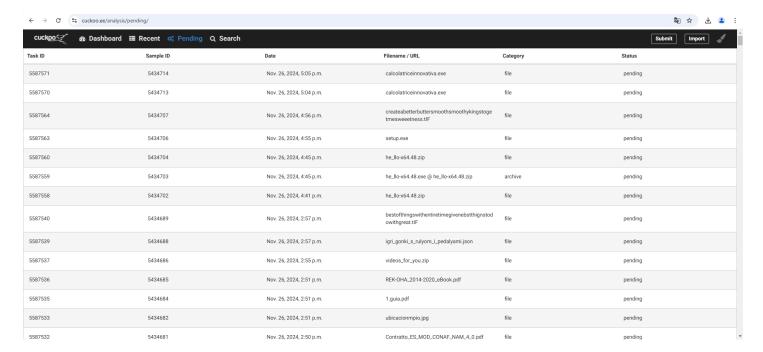
- File Dropped: Se il malware scrive altri file su disco.
- Connessioni di rete: IP/DNS sospetti, protocolli usati.
- Processi anomali: Creazione di processi figli o iniezioni in altri processi.

4. Raccomandazioni

- 1. **Isolamento:** Non eseguire il file al di fuori di un ambiente virtualizzato (VM o sandbox).
- 2. Segnalazione: Hash e IOC dovrebbero essere condivisi con il team di sicurezza informatica per avvisare altri sistemi.

3. Protezione futura:

- Rafforzare le soluzioni AV con regole YARA che rilevano signature come ShikataGaNai.
- Monitorare log per tracciare modifiche di registro o rete.



Conclusione:

Basandosi sull'analisi statica, il file calc.exe è altamente sospetto e rappresenta una potenziale minaccia. L'offuscamento tramite ShikataGaNai, le funzioni importate e le classificazioni antivirus suggeriscono che il malware abbia capacità di evasione e funzioni avanzate come la comunicazione con un server remoto o l'iniezione di codice.

Un'analisi dinamica sarà essenziale per confermare il comportamento e i target precisi.