Analisi file data.pdf

1. **Introduzione**

Il presente report descrive l'analisi di un file PDF sospetto che sembra contenere un link malevolo. L'obiettivo è identificare il tipo di malware coinvolto e il comportamento del sistema quando il PDF viene aperto.

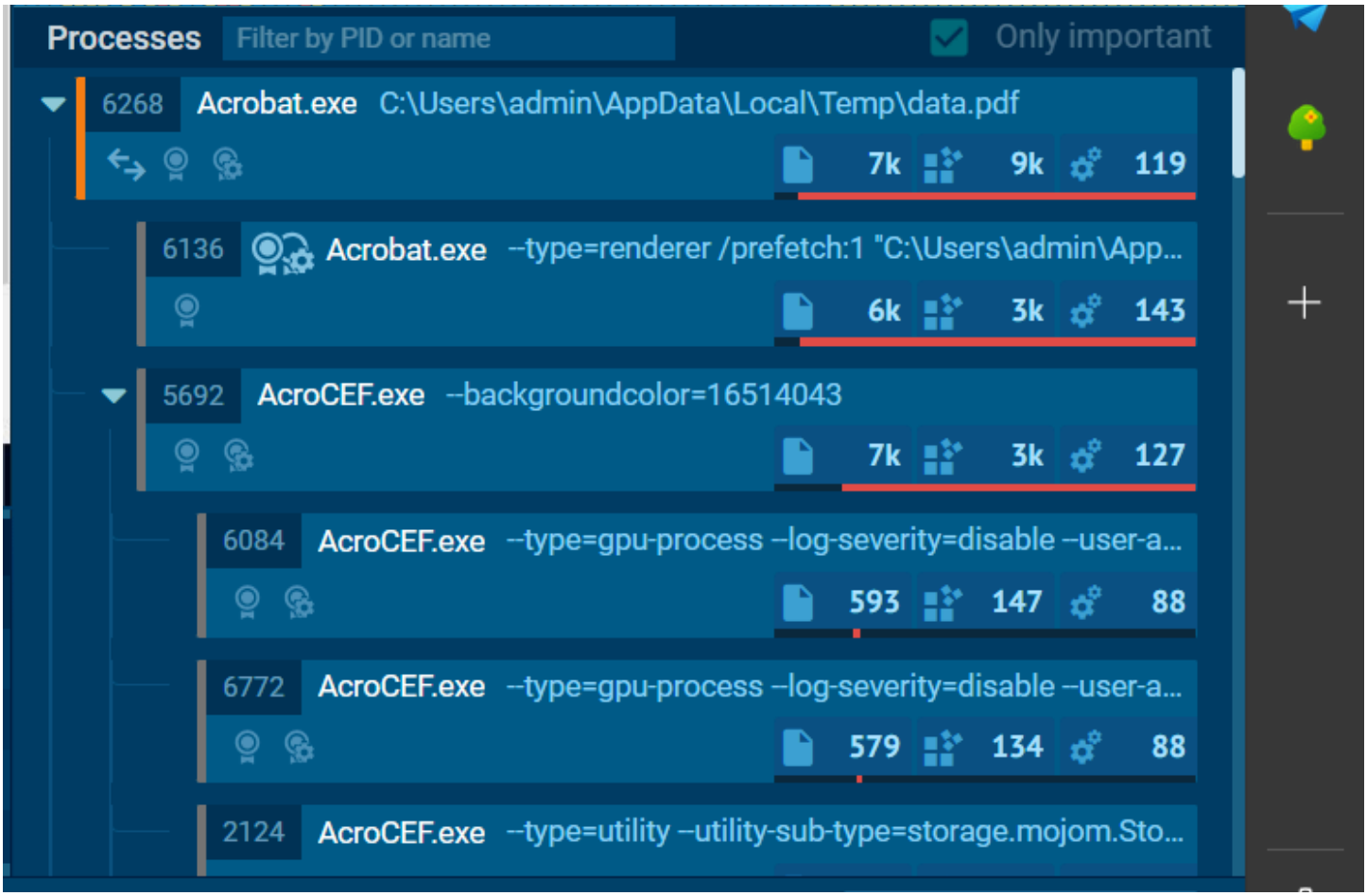
2. **Descrizione del PDF**

- Nome del file: data.pdf
- Hash MD5: 0D06D5045BC3830C9E90E1D046EF01

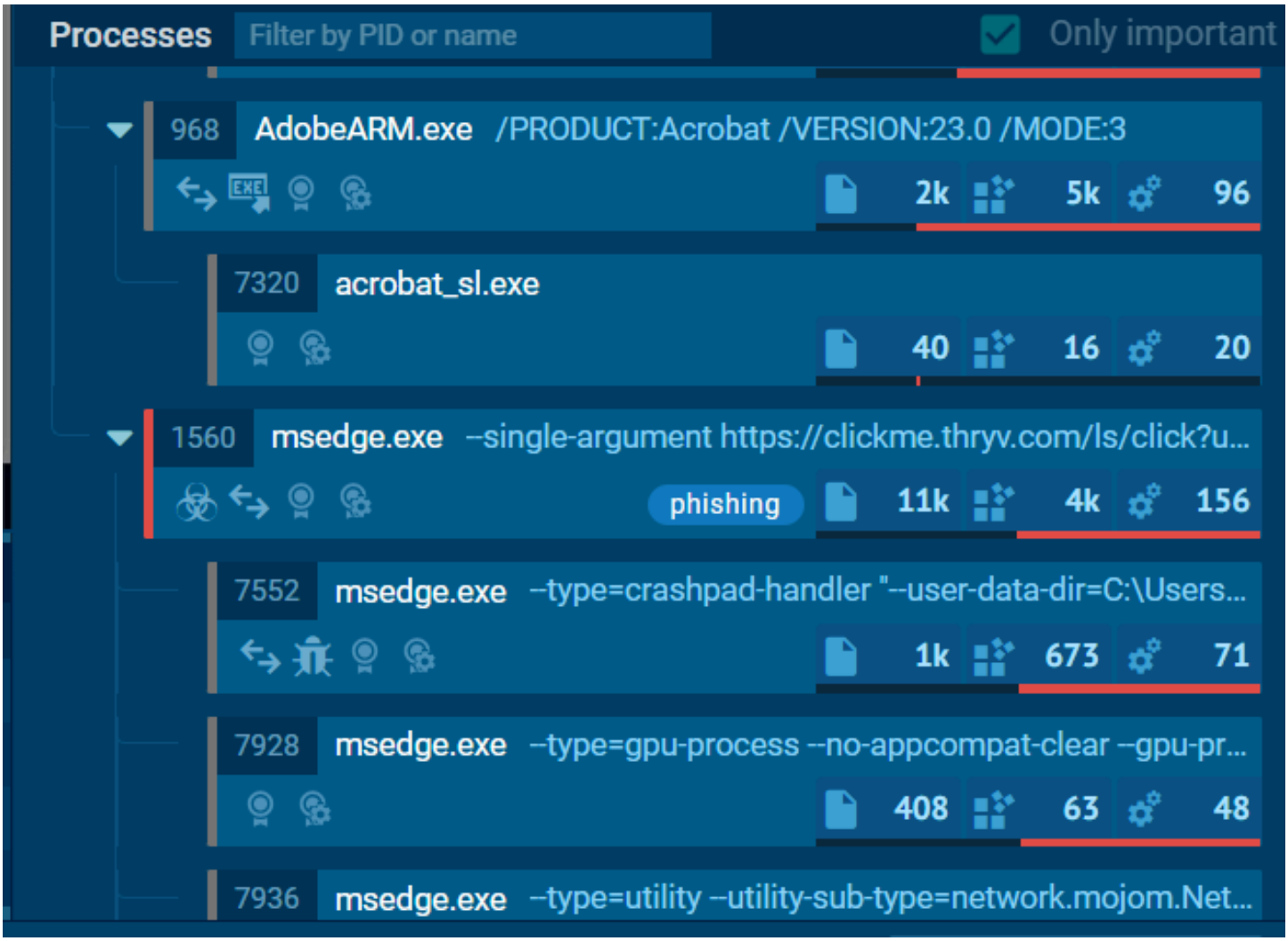
3. **Comportamento Osservato**

Quando il PDF viene aperto con Adobe Acrobat, si puo' notare che vengono avviati dei processi sospetti:

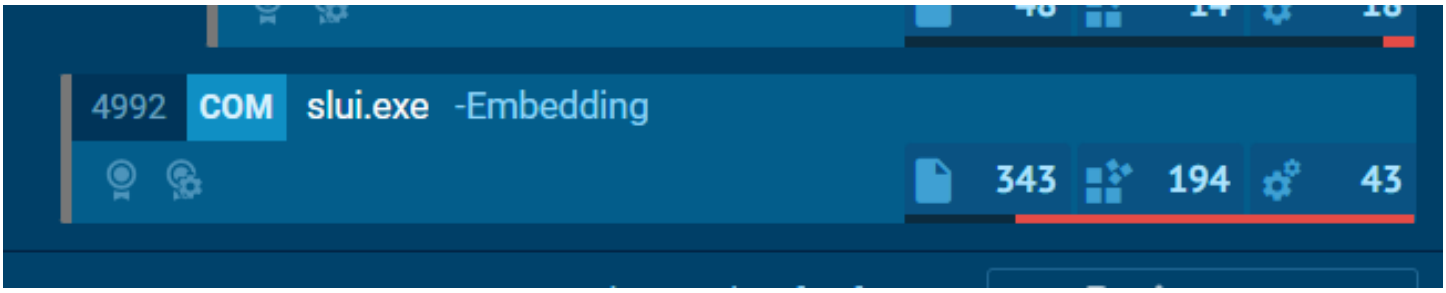
- Processo Acrobat.exe:



    - Un processo denominato AcroCEF.exe viene avviato, che potrebbe essere responsabile della gestione dei contenuti web all'interno del PDF.
- Processo msedge.exe:



- Processo slui.exe:



4. Attività di Rete

- Richieste HTTP:
  - Diverse richieste HTTP GET verso l'URL acroipm2.adobe.com, molte delle quali restituiscono un codice di risposta 404 Not Found.

5.Indicazioni di Compromissione (IOC)

- Indicatori di Rete:
  - URL sospetti: http://acroipm2.adobe.com/assets/...
  - Richieste HTTP fallite con risposta 404 Not Found, indicando tentativi di connessione a risorse non esistenti o disattivate.

6. Potenziale Malware e Scopo

- Tipo di Malware: Trojan/Downloader
  - Il PDF contiene un link malevolo che, se cliccato, reindirizza a un sito che può ospitare ulteriori componenti malevoli o tentare di eseguire attacchi di phishing.
- Scopo:
  - Infezione del Sistema: Tentativo di scaricare ed eseguire malware aggiuntivo.
  - Furto di Informazioni: Raccolta di credenziali o altre informazioni sensibili.

7. Soluziuoni (Raccomandazioni)

- Non cliccare su link sospetti: Evitare di interagire con link all'interno di PDF non verificati.
- Mantenere Aggiornati i software e i SO
- Analisi Approfondita: Eseguire una scansione completa del sistema con un antivirus aggiornato e monitorare ulteriori attività sospette.

Conclusione:

L'analisi del PDF ha rivelato attività sospette legate a tentativi di connessione a risorse non disponibili e l'esecuzione di processi legati alla gestione dei contenuti web. È probabile che il PDF contenga un link malevolo con l'intento di compromettere il sistema dell'utente.