Analisi Malware 2

Comportamento generale del Malware:

Il task registrato nel JSON fornito è un albero di processi che descrive l'esecuzione del browser Google Chrome. Include informazioni sulla riga di comando utilizzata per avviare il browser, nonché gli ID dei processi e gli ID dei processi genitori.

I programmi legittimi, come i browser web, spesso utilizzano alberi di processi per organizzare e gestire la loro esecuzione. In questo caso, l'albero di processi mostra che Google Chrome è stato avviato con specifici argomenti della riga di comando e che ha creato un processo **GPU** e un processo di **utilità**. Questi processi sono comunemente utilizzati dai browser web per gestire diverse attività e ottimizzare le prestazioni.

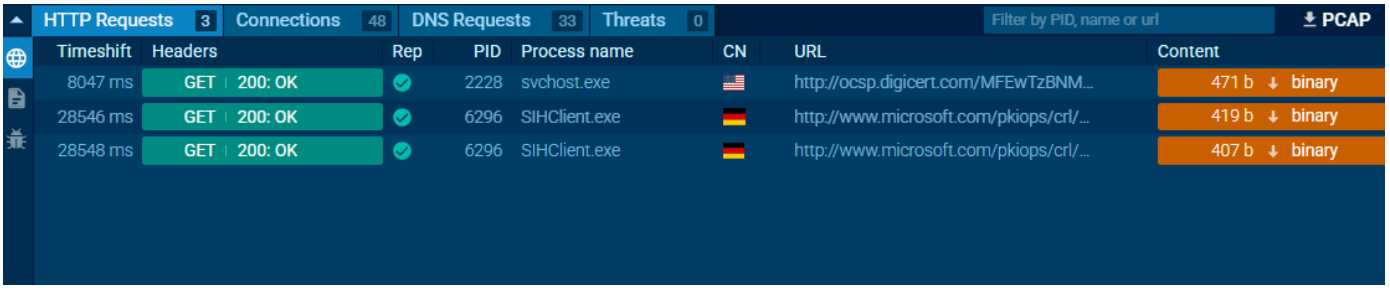
Anche i programmi malevoli possono utilizzare alberi di processi per nascondere le proprie attività o per eseguire codice dannoso. Avviando un browser web e creando processi aggiuntivi, il malware può offuscare la propria presenza e rendere più difficile il rilevamento. Tuttavia, senza ulteriore contesto o analisi, non è possibile determinare se l'albero di processi in questo caso sia utilizzato in modo malevolo.

Dettagli

- OS: Windows 10-64
- Orario e data di avvio del Malware: 25/08/2024, 22:44.
- Tempo in esecuzione: 47s
- PID minaccia: 6584
- URL: https://click.convertkit-mail2.com/wvuqovqrrwagh50ndddc7hnxdlxxxu8/48hvhehr87opx8ux/d3d3Lmluc3RhZ3JhbS5jb20vYXVzc2llbnVyc2VyZWNydWl0ZXJz
- Processi totali: 139
- Processi monitorati: 10
- Topologia dei processi:

Analisi mirata

Come da immagine possiamo iniziare a dire che il Malware in questione effettua 3 richieste HTTP con 2 processi diversi.



Spieghiamo cosa e chi sono questi processi:

- Svchost.exe: Svchost.exe è un processo di sistema che può ospitare uno o più servizi del sistema operativo Windows. Tali processi sono essenziali nell'implementazione e per il corretto funzionamento di alcuni servizi condivisi, in cui un numero di servizi può condividere un processo al fine di ridurre il consumo di risorse.
- SIHClient.exe: SIHClient.exe è un file eseguibile che è un componente di Windows 10 sistema operativo ed è sviluppato da Microsoft Corporation. La versione Windows di questo software è 10.0.10240.16384 .

Notiamo che il Malware inoltre ha effettuato ben 48 connessioni con TCP e UDP in vari indirizzi Ip di paesi diversi tra:

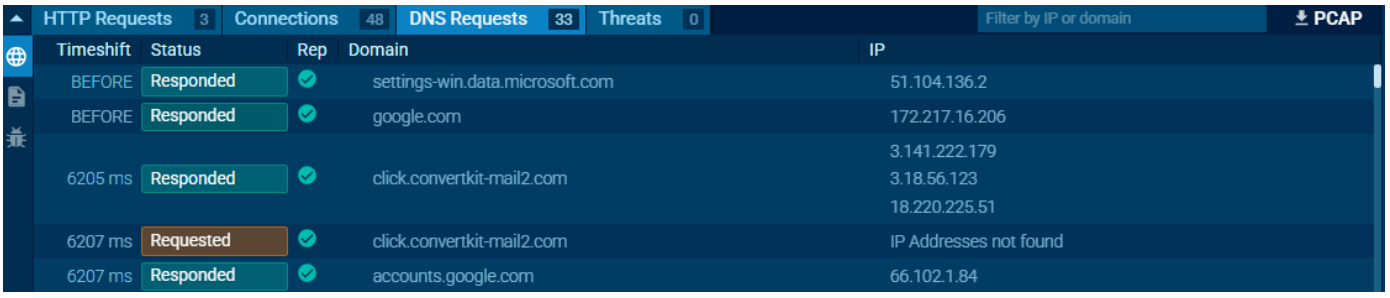
- Irlanda
- Usa
- Olanda
- Germania

E lo ha fatto con i seguenti processi:

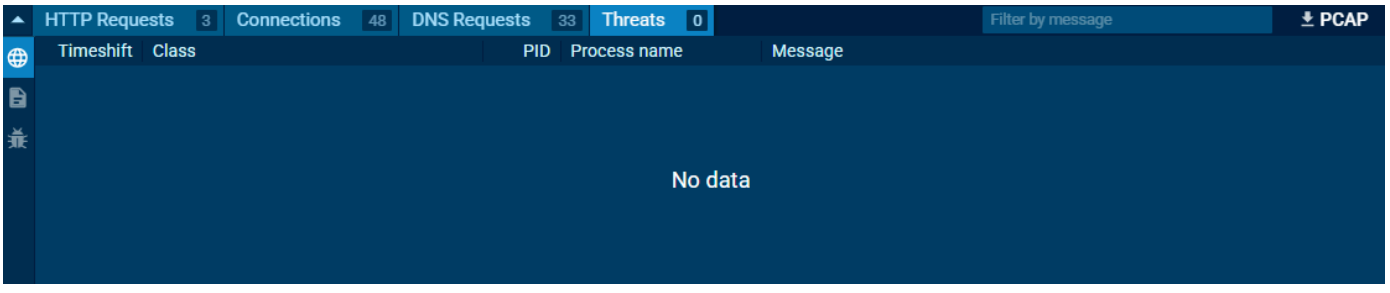
- System
- svchost.exe
- RUXIMICS.exe
- MoUsoCoreWorker.exe
- chrome.exe
- SIHClient.exe

Mostro a livello visivo quanto riportato qui sopra:

Successivamente notiamo anche le 33 richieste ai vari DNS.



Un dato molto interessante è che non abbiamo rilevato azioni malevole con questa analisi.



Comportamento di Google Chrome e Possibili Implicazioni di Sicurezza.

Questa relazione analizza una serie di evidenze relative all’esecuzione del browser Google Chrome, con particolare attenzione ai seguenti aspetti:

- Struttura dell'albero dei processi (Process Tree).
- Utilizzo dei Mutex.
- Riga di comando e parametri di esecuzione.

L’obiettivo è determinare se le attività osservate possano avere implicazioni di sicurezza, ovvero se siano indicative di un comportamento legittimo del browser o possano essere sfruttate da malware per occultare operazioni malevole.

Process tree.

L’analisi del process tree mostra l’esecuzione di Google Chrome con specifici argomenti della riga di comando, oltre alla creazione di processi aggiuntivi, tra cui:

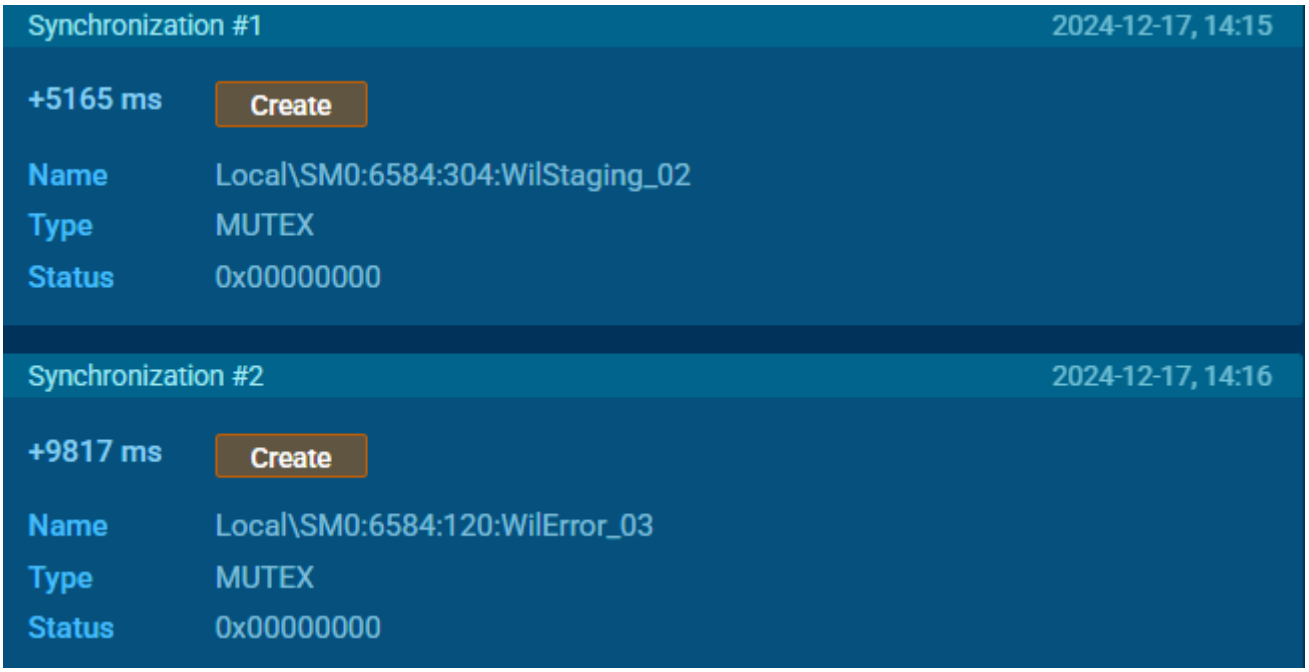
- Un processo GPU: utilizzato per l’accelerazione grafica.
- Un processo di utilità: gestisce funzioni aggiuntive del browser.

Sebbene sia normale che un browser crei processi secondari per ottimizzare le prestazioni, i malware possono sfruttare questo comportamento per:

- Nascondere codice malevolo all'interno di processi legittimi, come quelli di Chrome.
- Eseguire codice dannoso sotto il contesto di un browser, rendendo più difficile l'individuazione da parte degli strumenti di sicurezza.

Mutex.

Sono stati identificati due mutex



con i seguenti nomi:

- "Local\SM0:6584:304:WilStaging_02"
- "Local\SM0:6584:120:WilError_03"

I mutex vengono utilizzati da Chrome per gestire l'accesso a risorse condivise ed evitare che più istanze del browser entrino in conflitto tra loro.

Potenziale uso malevolo

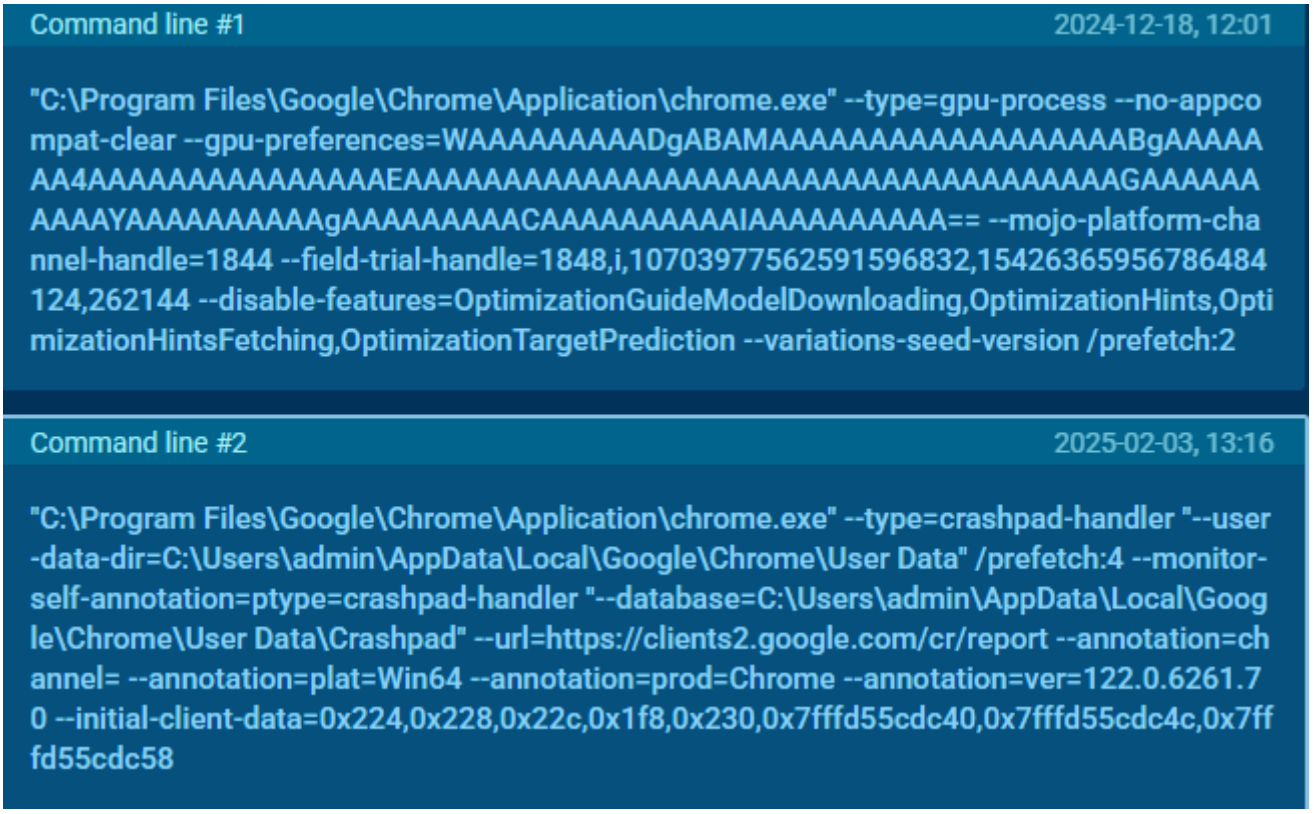
I malware possono abusare dei mutex per:

- Verificare se sono già in esecuzione, impedendo l'esecuzione di più istanze contemporaneamente.
- Nascondere la loro presenza, creando mutex con nomi simili a quelli di applicazioni legittime.

In questo caso, i mutex osservati sembrano legati a Chrome.

Analisi della Riga di Comando.

La riga di comando usata per avviare Chrome contiene parametri e flag specifici



tra cui:

- Definizione del tipo di processo.
- Disabilitazione di alcune funzionalità.
- Partecipazione a field trials (test sperimentali di Google).

Potenziale uso malevolo

Sebbene questa riga di comando sembri legittima, i malware possono:

- Eseguire codice malevolo mascherandolo come un'istanza di Chrome.
- Disabilitare funzionalità di sicurezza del browser modificando i flag.
- Creare processi simili per evitare il rilevamento.

Anche in questo caso, non ci sono evidenze dirette di un comportamento malevolo.

Raccomandazioni e consigli.

L’analisi mostra che il comportamento osservato potrebbe essere legittimo, ma i malware possono sfruttare meccanismi simili per nascondere la loro attività. Per determinare se ci siano anomalie, si consiglia di:

- Monitorare i processi associati a Chrome con strumenti avanzati (es. Process Explorer, Sysmon).
- Verificare le firme digitali dei processi per assicurarsi che siano effettivamente eseguibili legittimi di Google.
- Analizzare il traffico di rete generato dai processi sospetti per rilevare eventuali connessioni anomale.
- Confrontare i mutex identificati con quelli normalmente utilizzati da Chrome, per verificare se siano stati alterati.
- Verificare i flag della riga di comando per individuare eventuali parametri anomali o sospetti.

Solo un’analisi più approfondita può confermare se il comportamento osservato sia del tutto legittimo o se vi sia una minaccia in corso.