1. Nome del Processo e Origine Sospetta

- Il processo `calcolatricinnovativa.exe` viene eseguito dal percorso **C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe**, indicando chiaramente che è un file identificato o sospettato come dannoso.
- Il nome stesso, unito al fatto che si trovi in una cartella denominata "Malware", suggerisce che questo file sia malevolo o faccia parte di un test di sicurezza per analizzare malware.

2. Accessi Estesi al Registro di Sistema

- Il processo effettua numerosi **accessi al registro di sistema** e letture delle chiavi relative a configurazioni critiche, tra cui:
    - **Image File Execution Options**: Queste chiavi vengono spesso manipolate da malware per alterare il comportamento di file eseguibili, bloccare strumenti di sicurezza o antivirus, o per garantire che il malware venga eseguito automaticamente.
    - **Session Manager**: Queste chiavi sono collegate alla gestione delle sessioni di sistema e possono essere modificate per consentire l'esecuzione del malware ad ogni avvio del sistema.
    - **WinSock2**: Letture estese delle chiavi relative a WinSock, il componente di Windows che gestisce le comunicazioni di rete. Un malware che accede a queste chiavi potrebbe cercare di manipolare o intercettare il traffico di rete, reindirizzare le connessioni o alterare le configurazioni DNS.

3. Caricamento di DLL di Sistema

- Il processo **carica un gran numero di librerie di sistema (DLL)**, come:
    - **ntdll.dll**, **kernel32.dll**, **user32.dll**, che sono essenziali per la gestione dei processi e dell'interfaccia di sistema.
    - **ws2_32.dll**, **rasadhlp.dll**, che sono legate alla gestione delle connessioni di rete, suggerendo che il malware potrebbe avere intenzioni legate alla manipolazione o all'intercettazione di dati di rete.
- Il caricamento di queste DLL avviene senza errori (risultato **SUCCESS** per ogni operazione), consentendo al processo di eseguire potenzialmente operazioni malevole senza impedimenti da parte del sistema operativo.

4. Operazioni sui Thread e Creazione di Processi

- Il processo crea più **thread** per eseguire varie operazioni, un comportamento comune nei malware per gestire simultaneamente diverse attività (come raccolta di dati, manipolazioni di rete, o esecuzione di payload dannosi).

- Questi thread vengono creati con successo e terminano senza errori, suggerendo che il processo potrebbe aver eseguito tutte le sue operazioni con successo.

5. Process Exit e Durata Breve

- Alla fine del tracciamento, il processo si conclude con **"Process Exit"** e un **Exit Status di 0**, il che indica che il processo si è chiuso correttamente dal punto di vista del sistema operativo. Tuttavia, il fatto che si sia chiuso senza errori non significa che non abbia eseguito operazioni dannose.

6. Possibili Intenzioni Malevole

- L'accesso alle chiavi di registro legate alle configurazioni di esecuzione, insieme al caricamento di DLL di rete e di sistema critiche, suggerisce che il processo potrebbe:
    - **Manipolare o intercettare il traffico di rete**, sfruttando le configurazioni di **WinSock2** e altre librerie legate alla gestione delle connessioni.
    - **Bloccare o aggirare gli strumenti di sicurezza** modificando chiavi come **Image File Execution Options**, impedendo l'esecuzione di antivirus o software di rilevamento.
    - **Garantire la persistenza nel sistema** alterando chiavi di esecuzione automatica, assicurandosi di essere eseguito ad ogni avvio del computer.

7. Risultati dei Tracciamenti

- Ogni operazione che il processo tenta di eseguire (lettura di registro, caricamento di DLL, creazione di thread) risulta **"SUCCESS"**, indicando che il processo ha avuto pieno accesso alle risorse di sistema necessarie. Non ci sono segnali di errori o blocchi, il che potrebbe significare che il malware è stato in grado di operare senza restrizioni.

Conclusioni:

Il processo `calcolatricinnovativa.exe` mostra molti comportamenti che sono tipici di malware:

- **Accessi al registro di sistema** su chiavi critiche.
- **Caricamento di DLL di sistema**, soprattutto relative alla rete e alla gestione dei processi.
- **Operazioni di creazione di thread**, che possono essere utilizzate per gestire simultaneamente attività malevole.
- **Manipolazioni delle configurazioni di rete**, come indicato dagli accessi alle chiavi di WinSock2.

Questi elementi combinati indicano che il processo ha una **forte probabilità di essere malevolo**, con potenziali intenzioni di manipolare il traffico di rete, mantenere la persistenza nel sistema e ostacolare i meccanismi di sicurezza.

Raccomandazioni:

1. **Eliminazione del file**: Se non è già stato fatto, rimuovi il file `calcolatricinnovativa.exe` dal sistema.
2. **Scansione approfondita**: Utilizza un antivirus aggiornato o uno strumento anti-malware per eseguire una scansione completa del sistema e rilevare eventuali altri componenti dannosi.
3. **Verifica delle impostazioni di rete**: Controlla le configurazioni DNS e delle connessioni di rete per assicurarti che non siano state alterate dal malware.
4. **Monitoraggio delle connessioni di rete**: Usa strumenti come **`netstat`** o firewall per monitorare eventuali connessioni sospette verso server remoti che potrebbero essere stati stabiliti dal malware.