Nell'immagine precedente, che mostra il monitoraggio di *Process Monitor* (ProcMon) per il file `calcolatriceinnovativa.exe`, non sembra esserci alcuna attività esplicita relativa alla gestione di processi o thread del sistema da parte del malware. Tutte le azioni visibili riguardano principalmente interazioni con il file system e il registro di sistema.

Tuttavia, ecco un'analisi di come potrebbe essere il comportamento del malware in termini di gestione dei processi e dei thread se tali operazioni fossero presenti:

1. **Creazione di Processi (CreateProcess)**:
    - Se il malware fosse progettato per avviare altri processi, si vedrebbe una serie di operazioni `CreateProcess`, in cui `calcolatriceinnovativa.exe` esegue nuovi eseguibili o script come parte delle sue operazioni malevole. Potrebbe anche usare questo meccanismo per scaricare ed eseguire payload aggiuntivi.
2. **Iniezione di Codice nei Processi**:
    - Un comportamento comune nei malware è l'iniezione di codice in processi legittimi (come `explorer.exe` o `svchost.exe`). Se presente, apparirebbero chiamate API come `OpenProcess`, `VirtualAllocEx`, `WriteProcessMemory` e `CreateRemoteThread`. Questo comportamento serve a nascondere l'attività del malware all'interno di processi fidati del sistema, rendendolo più difficile da rilevare.
3. **Creazione e Gestione di Thread**:
    - Il malware potrebbe anche creare propri thread interni per eseguire attività parallele, come comunicazioni di rete o crittografia di file. Questo comporterebbe chiamate a `CreateThread`, `SuspendThread`, o `ResumeThread`. Questi thread potrebbero rimanere in background per monitorare il sistema o eseguire payload a intervalli regolari.
4. **Escalation dei Privilegi**:
    - In alcuni casi, i malware tentano di ottenere privilegi elevati per poter controllare meglio il sistema. In Process Monitor, questo potrebbe apparire come chiamate per manipolare token di sicurezza, ad esempio `OpenProcessToken` o `AdjustTokenPrivileges`.

Analisi di Azioni sui Processi/Thread nell'Immagine

Dall'immagine, sembra che le uniche interazioni di `calcolatriceinnovativa.exe` siano con il proprio file e il registro di sistema. Non ci sono chiamate API visibili per manipolare altri processi o per eseguire codice in thread esterni. Questo suggerisce che il malware, almeno nel contesto mostrato, si limita a leggere e monitorare risorse locali piuttosto che interagire attivamente con altri processi del sistema operativo.

Se necessario, un'analisi più dettagliata potrebbe essere effettuata utilizzando strumenti di monitoraggio specifici per le operazioni di processo e thread, come strumenti di debug (ad esempio, OllyDbg o x64dbg) o tramite monitoraggio avanzato delle API di Windows.