

# Analisi dinamica basica

## Sommario

Traccia esercizio principale .....	2
Traccia esercizio facoltativo .....	2
Requisiti.....	2
Svolgimento esercizio principale .....	3
Svolgimento esercizio facoltativo .....	6

## Traccia esercizio principale

Rispondere ai seguenti quesiti, con riferimento al file eseguibile:

**C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe**

- Identificare eventuali azioni del malware sul **file system** utilizzando Process Monitor, fornendo una **descrizione** tramite AI;
- Identificare eventuali azioni del malware su **processi e thread** utilizzando Process Monitor, fornendo una **descrizione** tramite AI.

Suggerimento: ChatGPT (o altri LLM) possono ricevere in input degli screenshot da analizzare.

## Traccia esercizio facoltativo

- Aggiungere una considerazione finale sul malware in analisi in base alle informazioni raccolte ed elaborate con AI.

## Requisiti

Vedi report M6\W21\D5

# Svolgimento esercizio principale

Avviare “calcolatriceinnovativa.exe” e avviare procmon (Process Monitor)

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
15:20:54.2805440	calcolatriceinnovativa.exe	4480	Process Start		SUCCESS	Parent PID: 3532, Command Line: "C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe", Current directory: C:\Users\user\Desktop\Malw...
15:20:54.2805463	calcolatriceinnovativa.exe	4480	Thread Create		SUCCESS	Thread ID: 3692
15:20:54.4152595	calcolatriceinnovativa.exe	4480	Load Image	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Image Base: 0x1000000, Image Size: 0x1000
15:20:54.4153345	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\System32\ntldr.dll	SUCCESS	Image Base: 0x7f9211000, Image Size: 0x1c2000
15:20:54.4153396	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\ntldr.dll	SUCCESS	Image Base: 0x77120000, Image Size: 0x170000
15:20:54.4156035	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x72200000, Image Size: 0x4f000
15:20:54.4163341	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x72370000, Image Size: 0x72000
15:20:54.4163698	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x1400000, Image Size: 0x4d000
15:20:54.4184000	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x7f970000, Image Size: 0x4f000
15:20:54.4185955	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x1400000, Image Size: 0x4d000
15:20:54.4185776	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x72300000, Image Size: 0x6000
15:20:54.4201982	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Image Base: 0x7f970000, Image Size: 0x4f000
15:20:54.4204137	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Image Base: 0x77120000, Image Size: 0x170000
15:20:54.4223577	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Image Base: 0x73c10000, Image Size: 0x31000
15:20:54.4237740	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\shel32.dll	SUCCESS	Image Base: 0x74070000, Image Size: 0x130000
15:20:54.4265096	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\ole32.dll	SUCCESS	Image Base: 0x77060000, Image Size: 0x4e000
15:20:54.4384374	calcolatriceinnovativa.exe	4480	Thread Create		SUCCESS	Thread ID: 5604
15:20:54.4387231	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\windows.storage.dll	SUCCESS	Image Base: 0x7c5b0000, Image Size: 0x4d5000
15:20:54.4388096	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\combase.dll	SUCCESS	Image Base: 0x7c5b0000, Image Size: 0x7ba000
15:20:54.4392172	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\vcrt4.dll	SUCCESS	Image Base: 0x76880000, Image Size: 0x6c000
15:20:54.4394587	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\api-ms.dll	SUCCESS	Image Base: 0x74200000, Image Size: 0x1e000
15:20:54.4396157	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\cryptbase.dll	SUCCESS	Image Base: 0x74200000, Image Size: 0x4d000
15:20:54.4397909	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\bcryptprimitives.dll	SUCCESS	Image Base: 0x741c0000, Image Size: 0x59000
15:20:54.4399231	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Image Base: 0x74200000, Image Size: 0x43000
15:20:54.4401745	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\advapi32.dll	SUCCESS	Image Base: 0x74600000, Image Size: 0x30000
15:20:54.4404389	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\shlwapi.dll	SUCCESS	Image Base: 0x75c30000, Image Size: 0x44000
15:20:54.4405445	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\gdi32.dll	SUCCESS	Image Base: 0x76000000, Image Size: 0x14d000
15:20:54.4406808	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\SHELL32.dll	SUCCESS	Image Base: 0x76500000, Image Size: 0x14c000
15:20:54.4410690	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\kernel.appcore.dll	SUCCESS	Image Base: 0x76870000, Image Size: 0xc000
15:20:54.4413101	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\SHCore.dll	SUCCESS	Image Base: 0x74140000, Image Size: 0x6a000
15:20:54.4414964	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\powrtr.dll	SUCCESS	Image Base: 0x76440000, Image Size: 0x44000
15:20:54.4416987	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\profapi.dll	SUCCESS	Image Base: 0x76800000, Image Size: 0x4000
15:20:54.4422595	calcolatriceinnovativa.exe	4480	Thread Exit		SUCCESS	Thread ID: 5604, User Time: 0.000000, Kernel Time: 0.000000
15:20:54.4476892	calcolatriceinnovativa.exe	4480	Thread Create		SUCCESS	Thread ID: 5156
15:20:54.4495621	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	Image Base: 0x76490000, Image Size: 0x5c000
15:20:54.4554134	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\rsa.dll	SUCCESS	Image Base: 0x765d0000, Image Size: 0x7000
15:20:54.4727760	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\mssocket.dll	SUCCESS	Image Base: 0x73970000, Image Size: 0x4e000
15:20:54.4741395	calcolatriceinnovativa.exe	4480	Load Image	C:\Windows\SysWOW64\iaship.dll	SUCCESS	Image Base: 0x6d400000, Image Size: 0x3d000
15:20:54.4775646	calcolatriceinnovativa.exe	4480	Thread Exit		SUCCESS	Thread ID: 3692, User Time: 0.000000, Kernel Time: 0.0156250
15:20:54.4913372	calcolatriceinnovativa.exe	4480	Thread Exit		SUCCESS	Thread ID: 5156, User Time: 0.000000, Kernel Time: 0.000000
15:20:54.4914092	calcolatriceinnovativa.exe	4480	Thread Exit		SUCCESS	Thread ID: 5604, User Time: 0.000000, Kernel Time: 0.000000
15:20:54.5094305	calcolatriceinnovativa.exe	4480	Process Exit		SUCCESS	Exit Status: 0, User Time: 0.000000seconds, Kernel Time: 0.0155250seconds, Private Bytes: 1,212,416, Peak Private Bytes: 1,253,376, Workin...

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
15:20:54.4154835	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\Prefetch\CALCOLATRICEINNOVATIVA.EXE-5ICE59C.pf	NAME NOT FOUND	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: None, AllocationSize: n/a
15:20:54.4157844	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows	SUCCESS	Desired Access: Execute/Traverse, Synchronization: Disposition: Open, Options: Non-Alert, Attributes: n/a, ShareMode: R, AllocationSize: n/a
15:20:54.4177651	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a
15:20:54.4186427	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows	SUCCESS	Desired Access: Read Attributes, Synchronization: Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, D...
15:20:54.4186720	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows	SUCCESS	Name: Windows
15:20:54.4200587	calcolatriceinnovativa.exe	4480	CreateFile	C:\Users\user\Desktop\Malware	SUCCESS	Desired Access: Execute/Traverse, Synchronization: Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: R...
15:20:54.4212705	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a
15:20:54.4213402	calcolatriceinnovativa.exe	4480	QueryBasicInformationFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Creation Time: 10/07/2015 13:00:23, LastAccess Time: 10/07/2015 13:00:23, LastWrite Time: 10/07/2015 13:00:23, Change Time: 09/07/2024 1...
15:20:54.4213463	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
15:20:54.4216450	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Data/Full Control, Execute/Traverse, Synchronization: Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory ...
15:20:54.4216894	calcolatriceinnovativa.exe	4480	CreateFile Mapping	C:\Windows\SysWOW64\apphelp.dll	FILE LOCKED WITH ONLY READERS	Succ Type: SyncTypeCreateSection, PageProtection: SyncType: SyncTypeOther
15:20:54.4222168	calcolatriceinnovativa.exe	4480	CreateFile Mapping	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
15:20:54.4224758	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	
15:20:54.4227421	calcolatriceinnovativa.exe	4480	CreateFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, OpenResult: Opened
15:20:54.4227585	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	BUFFER OVERFLOW	Information: Owner
15:20:54.4227880	calcolatriceinnovativa.exe	4480	CloseFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Information: Owner
15:20:54.4228084	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\SysWOW64\ntldr.dll	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, OpenResult: Opened
15:20:54.4228493	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Windows\SysWOW64\ntldr.dll	BUFFER OVERFLOW	Information: Owner
15:20:54.4228511	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\SysWOW64\ntldr.dll	SUCCESS	Information: Owner
15:20:54.4228911	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, OpenResult: Opened
15:20:54.4229101	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	BUFFER OVERFLOW	Information: Owner
15:20:54.4229216	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	Information: Owner
15:20:54.4229254	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\SysWOW64\kernel32.dll	SUCCESS	
15:20:54.4229547	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, OpenResult: Opened
15:20:54.4229756	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Windows\SysWOW64\KernelBase.dll	BUFFER OVERFLOW	Information: Owner
15:20:54.4229791	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	Information: Owner
15:20:54.4229825	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	
15:20:54.4230195	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\AppPatch\iasymian.sdb	SUCCESS	
15:20:54.4230366	calcolatriceinnovativa.exe	4480	QueryStandardInformationFile	C:\Windows\AppPatch\iasymian.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, Allocat...
15:20:54.4230416	calcolatriceinnovativa.exe	4480	QueryStandardInformationFile	C:\Windows\AppPatch\iasymian.sdb	SUCCESS	AllocationSize: 3,735,552, EndOfFile: 3,734,416, NumberOfLinks: 2, DeletePending: False, Directory: False
15:20:54.4230465	calcolatriceinnovativa.exe	4480	CreateFile Mapping	C:\Windows\AppPatch\iasymian.sdb	FILE LOCKED WITH ONLY READERS	Succ Type: SyncTypeCreateSection, PageProtection: SyncType: SyncTypeOther
15:20:54.4230507	calcolatriceinnovativa.exe	4480	QueryStandardInformationFile	C:\Windows\AppPatch\iasymian.sdb	SUCCESS	AllocationSize: 3,735,552, EndOfFile: 3,734,416, NumberOfLinks: 2, DeletePending: False, Directory: False
15:20:54.4230579	calcolatriceinnovativa.exe	4480	QueryStandardInformationFile	C:\Windows\AppPatch\iasymian.sdb	SUCCESS	AllocationSize: 3,735,552, EndOfFile: 3,734,416, NumberOfLinks: 2, DeletePending: False, Directory: False
15:20:54.4232640	calcolatriceinnovativa.exe	4480	CreateFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, Allocat...
15:20:54.4232811	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Information: Owner, Group, DACL, SACL, Label
15:20:54.4232842	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, Allocat...
15:20:54.4232827	calcolatriceinnovativa.exe	4480	QueryBasicInformationFile	C:\Windows\AppPatch\iasymian.sdb	SUCCESS	Creation Time: 10/07/2015 13:00:34, LastAccess Time: 10/07/2015 13:00:34, LastWrite Time: 10/07/2015 13:00:34, Change Time: 09/07/2024 1...
15:20:54.4233673	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\AppPatch\iasymian.sdb	SUCCESS	
15:20:54.4234404	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\AppPatch\apppatch64\iasymian.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, Allocat...
15:20:54.4234126	calcolatriceinnovativa.exe	4480	QueryBasicInformationFile	C:\Windows\AppPatch\apppatch64\iasymian.sdb	SUCCESS	Creation Time: 10/07/2015 13:00:21, LastAccess Time: 10/07/2015 13:00:21, LastWrite Time: 10/07/2015 13:00:21, Change Time: 09/07/2024 1...
15:20:54.4234156	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\AppPatch\apppatch64\iasymian.sdb	SUCCESS	
15:20:54.4234267	calcolatriceinnovativa.exe	4480	QueryBasicInformationFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Creation Time: 22/07/2024 12:08:38, LastAccess Time: 22/07/2024 12:08:38, LastWrite Time: 22/07/2024 12:00:44, Change Time: 22/07/2024 1...
15:20:54.4235391	calcolatriceinnovativa.exe	4480	CreateFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	
15:20:54.4235795	calcolatriceinnovativa.exe	4480	CreateFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, Allocat...
15:20:54.4235188	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Information: Owner, Group, DACL, SACL, Label
15:20:54.4235256	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Creation Time: 22/07/2024 12:08:38, LastAccess Time: 22/07/2024 12:08:38, LastWrite Time: 22/07/2024 12:00:44, Change Time: 22/07/2024 1...
15:20:54.4235777	calcolatriceinnovativa.exe	4480	CloseFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	
15:20:54.4240415	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\AppPatch\iasymian.sdb	SUCCESS	
15:20:54.4241402	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a
15:20:54.4241585	calcolatriceinnovativa.exe	4480	QueryBasicInformationFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	Creation Time: 10/07/2015 13:00:23, LastAccess Time: 10/07/2015 13:00:23, LastWrite Time: 10/07/2015 13:00:23, Change Time: 09/07/2024 1...

## 1. Esecuzione e caricamento:

- Il file è stato eseguito dalla directory **C:\Users\user\Desktop\Malware**.
- Durante l'esecuzione, ha tentato di accedere a numerosi file di sistema e librerie **DLL** per caricarli in memoria.
- Il comportamento osservato include il caricamento di DLL standard di Windows da directory come:
  - C:\Windows\System32
  - C:\Windows\SysWOW64
- Tra le DLL caricate si trovano:
  - apphelp.dll, kernel32.dll, user32.dll, ws2\_32.dll, mswsock.dll, imm32.dll.

---

## 2. Accesso a file di sistema e librerie:

- L'accesso a queste DLL potrebbe essere riconducibile a:
  - Mascheramento di attività malevole utilizzando funzioni di sistema legittime.
  - Utilizzo di funzionalità di rete avanzate o vulnerabilità di sistema.
- Sono state eseguite operazioni di lettura e mapping di memoria sulle DLL, come su `ws2_32.dll` e `apphelp.dll`, indicando possibili tentativi di:
  - Iniezione di codice.
  - Manipolazione della memoria.

---

## 3. Operazioni su thread e processi:

- Il processo ha creato diversi thread durante l'esecuzione, probabilmente per eseguire operazioni parallele.
- Non ci sono segni di persistenza, ma è possibile che il malware stia preparando fasi successive non catturate nei log.

---

## 4. Attività di rete:

- Il caricamento di librerie di rete, come `ws2_32.dll` e `mswsock.dll`, indica che il file potrebbe tentare di stabilire connessioni di rete.
- Questo potrebbe essere preparatorio per attività di comunicazione remota o per contattare server di comando e controllo (C2).

---

## 5. Interrogazioni di sicurezza:

- Numerose query di sicurezza sui file di sistema sono state osservate. Queste potrebbero essere tentativi di:
  - Identificare le impostazioni di sicurezza.
  - Cercare file o configurazioni vulnerabili per sfruttarle.

---

## 6. Possibili funzionalità malevole:

- **Persistenza e nascondimento:**
  - Non ci sono chiari segni di tentativi di persistenza nei log analizzati, ma il malware potrebbe mirare a stabilire una presenza nel sistema in fasi successive.
- **Keylogging o intercettazione di input:**
  - Il caricamento di `imm32.dll` e `user32.dll` potrebbe indicare tentativi di intercettare l'input dell'utente.

- **Esplorazione del sistema:**

- Le numerose interrogazioni e accessi ai file di sistema suggeriscono che il malware stia raccogliendo informazioni sull'ambiente host.

- **Offuscamento:**

- L'accesso a molte DLL di sistema può essere un tentativo di confondere un'analisi manuale, mescolando attività malevole con operazioni legittime.

---

### Conclusione combinata:

Le attività osservate indicano che `calcolatriceinnovativa.exe` è potenzialmente un **malware in fase iniziale di esecuzione**, con l'obiettivo di:

1. Caricare librerie di sistema e manipolare la memoria.
2. Prepararsi per attività malevole, come:
  - Connessioni di rete.
  - Raccolta di input o dati sensibili (potenziale keylogging).
  - Esplorazione del sistema per trovare vulnerabilità o configurazioni sfruttabili.
3. Mascherare la sua vera natura utilizzando funzioni di sistema legittime.

---

### Azioni consigliate:

1. **Eseguire un'analisi statica:**
  - Utilizzare strumenti come **PEStudio** o **IDA Pro** per analizzare eventuali funzioni sospette o codice incorporato.
2. **Monitorare l'attività di rete:**
  - Utilizzare **Wireshark** per rilevare connessioni sospette e analizzare il traffico.
3. **Eseguire il file in un ambiente sandbox:**
  - Testare il comportamento del file in una sandbox come **Cuckoo Sandbox** per osservare eventuali azioni non visibili nei log.
4. **Isolamento preventivo:**
  - Isolare l'host compromesso per evitare ulteriori danni o propagazioni.
5. **Analizzare le connessioni dei server:**
  - Se rilevati contatti con server esterni, verificare gli indirizzi IP e i domini per identificare eventuali server di comando e controllo.
6. **Rimuovere il file:**
  - Se confermata la natura malevola, eliminare il file e ripristinare il sistema a uno stato precedente sicuro.

Questo comportamento, associato alle informazioni osservate nei log, indica che il malware è progettato per stabilire una presenza iniziale e successivamente attivare payload più dannosi.

## Svolgimento esercizio facoltativo

### Considerazione finale sul malware in analisi

Sulla base delle informazioni raccolte ed elaborate, il malware analizzato sembra essere progettato per raccogliere informazioni preliminari sul sistema senza compiere azioni distruttive immediate. Il comportamento osservato, come il caricamento di librerie di rete (**ws2\_32.dll**, **mswsock.dll**) e numerose query al registro di sistema, suggerisce un possibile **malware di ricognizione**. Questo tipo di malware è comunemente utilizzato per identificare vulnerabilità o configurazioni utili a fasi successive di un attacco, come il download di payload aggiuntivi o l'ottenimento di accesso remoto.

La breve durata di esecuzione e l'assenza di attività manifestamente malevole nei log potrebbero indicare che il file è stato progettato per operare in modo furtivo, evitando di generare anomalie evidenti. Tuttavia, non si può escludere che il malware abbia eseguito azioni dannose non catturate nei log forniti.

In conclusione, l'analisi suggerisce che il malware rappresenti una **minaccia potenziale**, con un comportamento iniziale focalizzato sulla raccolta di informazioni e sul mascheramento della propria attività. Si consiglia un'ulteriore analisi in un ambiente controllato per verificare eventuali comportamenti non rilevati in questa fase.