Traccia:

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.

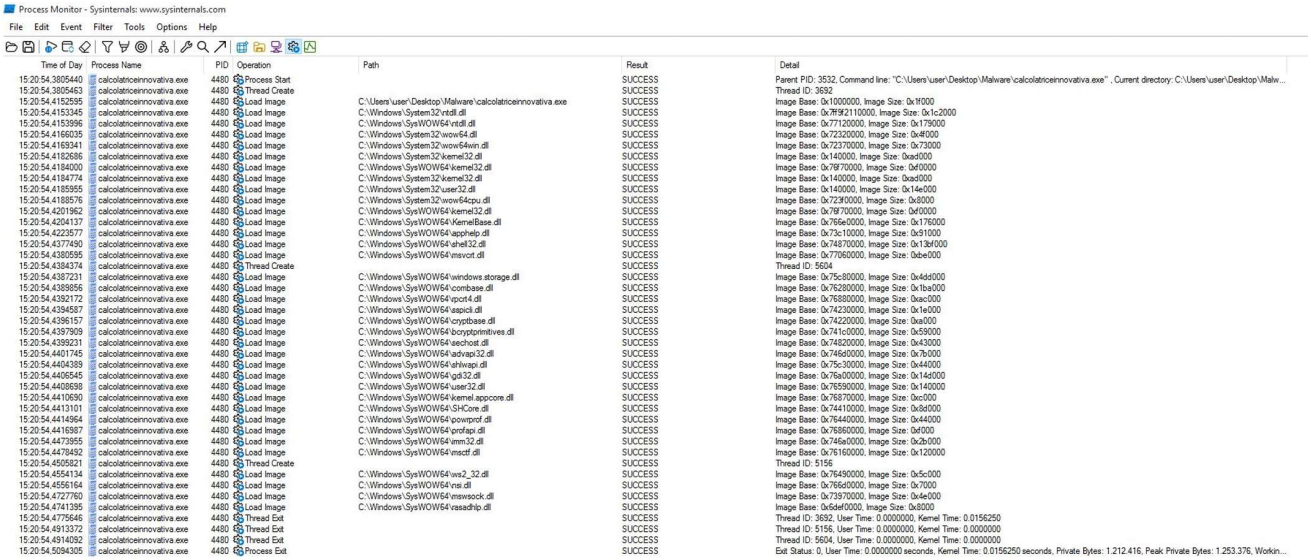
Suggerimento: ChatGPT (o altri LLM) possono ricevere in input degli screenshot da analizzare.

Dalle attività processi e thread si può osservare:

- Il processo inizia caricando numerose librerie di sistema Windows (DLL).
- Carica file da diverse cartelle di sistema, in particolare da C:\Windows \System32 e C:\Windows\SysWOW64.
- Crea diversi thread durante l'esecuzione.
- Tutte le operazioni mostrate risultano in "SUCCESS", indicando che il malware è riuscito a eseguire le sue azioni senza errori.
- Il processo termina dopo aver compiuto numerose operazioni di caricamento e creazione di thread.

Questo comportamento è tipico di un malware che cerca di:

- Nascondersi come un'applicazione legittima (in questo caso, una calcolatrice)
- Caricare componenti di sistema per mascherare la sua attività o sfruttare vulnerabilità
- Creare thread multipli per eseguire diverse azioni contemporaneamente
- Potenzialmente stabilire persistenza nel sistema o eseguire altre attività malevole



Dalle attività sul file system si può osservare:

1. **Esecuzione e caricamento:**
   - Il malware viene eseguito dalla cartella "**C:\Users\user\Desktop\Malware**".
   - Tenta di accedere a vari file di sistema e DLL, probabilmente per caricarli in memoria.

2. **Accesso a file di sistema:**
   - Accede a numerose DLL di sistema in **C:\Windows\SysWOW64**, incluse **apphelp.dll, kernel32.dll, user32.dll, ws2_32.dll** (per funzionalità di rete) e altre.
   - Questo potrebbe essere per nascondere la sua attività o per utilizzare funzioni di sistema legittime.

3. **Operazioni di lettura e mapping:**
   - Esegue operazioni di lettura su alcune DLL, come **apphelp.dll e ws2_32.dll.**
   - Crea file mapping per diverse DLL, il che potrebbe indicare tentativi di iniezione di codice o manipolazione della memoria.

4. **Interrogazioni di sicurezza:**
   - Esegue molte query di sicurezza sui file, che potrebbero essere tentativi di identificare le impostazioni di sicurezza del sistema o di cercare vulnerabilità.

5. **Attività di rete:**
   - Il caricamento di **ws2_32.dll** e **mswsock.dll** suggerisce che il malware potrebbe tentare di stabilire connessioni di rete.

6. **Persistenza e nascondimento**:
   - Non ci sono chiari segni di tentativi di persistenza nel sistema dai log forniti, ma potrebbe essere una fase successiva non catturata in questo log.

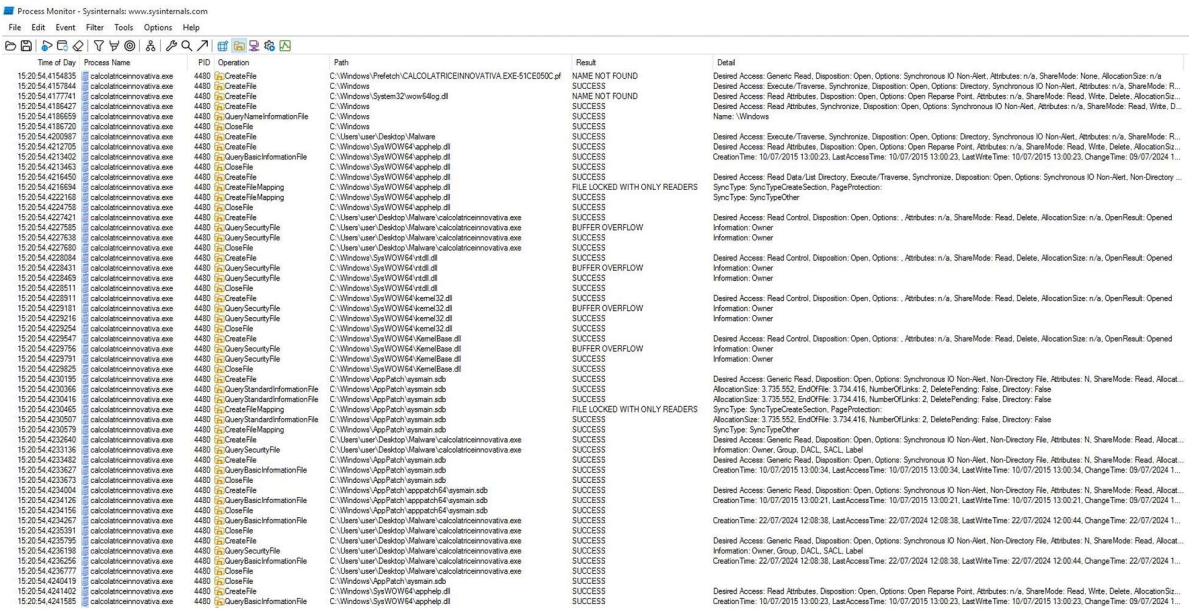
7. **Potenziale keylogging o cattura di input:**
   - Il caricamento di **imm32.dl**l e **user32.dll** potrebbe indicare tentativi di intercettare l'input dell'utente.

8. **Esplorazione del sistema:**
   - Le numerose query sui file di sistema potrebbero indicare che il malware sta

raccogliendo informazioni sul sistema host.

9. **Possibile offuscamento:**
- L'accesso a molte DLL di sistema potrebbe essere un tentativo di mascherare la sua vera natura mescolando la sua attività con operazioni di sistema normali.

Questo malware sembra essere nella fase iniziale di esecuzione, caricando varie librerie di sistema e potenzialmente preparandosi per attività malevole come connessioni di rete, intercettazione di input e possibile manipolazione del sistema. Il suo comportamento suggerisce che potrebbe essere un trojan o un payload iniziale progettato per stabilire una presenza nel sistema prima di scaricare o attivare funzionalità più dannose



Time of Day	Process Name	PID	Operation	Path	Result	Detail
15:20:54.4154835	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\Prefetch\CALCOLATRICEINNOVATIVA.EXE-51CE050C.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, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Attributes: n/a, ShareMode: R...
15:20:54.4177741	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, AllocationSiz...
15:20:54.4186427	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: Read, Write, D...
15:20:54.4186659	calcolatriceinnovativa.exe	4480	QueryNameInformationFile	C:\Windows	SUCCESS	Name: \Windows
15:20:54.4186720	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows	SUCCESS	
15:20:54.4200987	calcolatriceinnovativa.exe	4480	CreateFile	C:\Users\user\Desktop\Malware	SUCCESS	Desired Access: Execute/Traverse, Synchronize, 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, AllocationSiz...
15:20:54.4213402	calcolatriceinnovativa.exe	4480	QueryBasicInformationFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	CreationTime: 10/07/2015 13:00:23, LastAccessTime: 10/07/2015 13:00:23, LastWriteTime: 10/07/2015 13:00:23, ChangeTime: 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/List Directory, Execute/Traverse, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory ...
15:20:54.4216894	calcolatriceinnovativa.exe	4480	CreateFileMapping	C:\Windows\SysWOW64\apphelp.dll	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection:
15:20:54.4222168	calcolatriceinnovativa.exe	4480	CreateFileMapping	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	SyncType: SyncTypeOther
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
15:20:54.4227638	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Information: Owner
15:20:54.4227680	calcolatriceinnovativa.exe	4480	CloseFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	
15:20:54.4228084	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: , Attributes: n/a, ShareMode: Read, Delete, AllocationSize: n/a, OpenResult: Opened
15:20:54.4228431	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Windows\SysWOW64\ntdll.dll	BUFFER OVERFLOW	Information: Owner
15:20:54.4228469	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Information: Owner
15:20:54.4228511	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	
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
15:20:54.4229181	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
15:20:54.4229826	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\SysWOW64\KernelBase.dll	SUCCESS	
15:20:54.4230195	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, Allocat...
15:20:54.4230366	calcolatriceinnovativa.exe	4480	QueryStandardInformationFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 3.735.552, EndOfFile: 3.734.416, NumberOfLinks: 2, DeletePending: False, Directory: False
15:20:54.4230416	calcolatriceinnovativa.exe	4480	QueryStandardInformationFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 3.735.552, EndOfFile: 3.734.416, NumberOfLinks: 2, DeletePending: False, Directory: False
15:20:54.4230465	calcolatriceinnovativa.exe	4480	CreateFileMapping	C:\Windows\AppPatch\sysmain.sdb	FILE LOCKED WITH ONLY READERS	SyncType: SyncTypeCreateSection, PageProtection:
15:20:54.4230507	calcolatriceinnovativa.exe	4480	QueryStandardInformationFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 3.735.552, EndOfFile: 3.734.416, NumberOfLinks: 2, DeletePending: False, Directory: False
15:20:54.4230579	calcolatriceinnovativa.exe	4480	CreateFileMapping	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	SyncType: SyncTypeOther
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...
15:20:54.4233136	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Information: Owner, Group, DACL, SACL, Label
15:20:54.4233482	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N, ShareMode: Read, Allocat...
15:20:54.4233627	calcolatriceinnovativa.exe	4480	QueryBasicInformationFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	CreationTime: 10/07/2015 13:00:34, LastAccessTime: 10/07/2015 13:00:34, LastWriteTime: 10/07/2015 13:00:34, ChangeTime: 09/07/2024 1...
15:20:54.4233673	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\AppPatch\sysmain.sdb	SUCCESS	
15:20:54.4234004	calcolatriceinnovativa.exe	4480	CreateFile	C:\Windows\AppPatch\apppatch64\sysmain.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\sysmain.sdb	SUCCESS	CreationTime: 10/07/2015 13:00:21, LastAccessTime: 10/07/2015 13:00:21, LastWriteTime: 10/07/2015 13:00:21, ChangeTime: 09/07/2024 1...
15:20:54.4234156	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\AppPatch\apppatch64\sysmain.sdb	SUCCESS	
15:20:54.4234267	calcolatriceinnovativa.exe	4480	QueryBasicInformationFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	CreationTime: 22/07/2024 12:08:38, LastAccessTime: 22/07/2024 12:08:38, LastWriteTime: 22/07/2024 12:00:44, ChangeTime: 22/07/2024 1...
15:20:54.4235391	calcolatriceinnovativa.exe	4480	CloseFile	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...
15:20:54.4236198	calcolatriceinnovativa.exe	4480	QuerySecurityFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	Information: Owner, Group, DACL, SACL, Label
15:20:54.4236256	calcolatriceinnovativa.exe	4480	QueryBasicInformationFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	CreationTime: 22/07/2024 12:08:38, LastAccessTime: 22/07/2024 12:08:38, LastWriteTime: 22/07/2024 12:00:44, ChangeTime: 22/07/2024 1...
15:20:54.4236777	calcolatriceinnovativa.exe	4480	CloseFile	C:\Users\user\Desktop\Malware\calcolatriceinnovativa.exe	SUCCESS	
15:20:54.4240419	calcolatriceinnovativa.exe	4480	CloseFile	C:\Windows\AppPatch\sysmain.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, AllocationSiz...
15:20:54.4241585	calcolatriceinnovativa.exe	4480	QueryBasicInformationFile	C:\Windows\SysWOW64\apphelp.dll	SUCCESS	CreationTime: 10/07/2015 13:00:23, LastAccessTime: 10/07/2015 13:00:23, LastWriteTime: 10/07/2015 13:00:23, ChangeTime: 09/07/2024 1...

Facoltativo:

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

Dall'analisi di tutte le attività, si rileva:

1. Avvio del processo: Il malware viene avviato dalla cartella "C:\Users\user\Desktop\Malware".

2. Caricamento di librerie di sistema: Il malware carica numerose librerie di sistema Windows (DLL) come **ntdll.dll, kernel32.dll, user32.dll, gdi32.dll**, ecc. Questo è un comportamento comune per molti eseguibili Windows, anche quelli legittimi.

3. Accesso al registro di sistema: Il malware effettua numerose query e operazioni sul registro di Windows, principalmente nelle chiavi relative a **WinSock** e configurazioni di rete. Questo potrebbe indicare che il malware sta cercando di raccogliere informazioni sulla configurazione di rete del sistema o sta tentando di modificare le impostazioni di rete.

4. Operazioni sui file: Il malware apre e legge vari file di sistema, principalmente DLL.

5. Creazione di thread: Il malware crea alcuni thread aggiuntivi, che potrebbero essere utilizzati per eseguire operazioni in parallelo.

6. Operazioni di rete: Il caricamento di librerie come **ws2_32.dll** e **mswsock.dl**l suggerisce che il malware potrebbe avere funzionalità di rete, anche se nel log non sono visibili connessioni di rete

effettive.

7. Breve durata di esecuzione: Il processo termina relativamente rapidamente con un codice di uscita 0, che normalmente indica una terminazione senza errori.

8. Nessuna attività manifestamente malevola: Nel log non sono visibili azioni chiaramente maligne come la creazione di file sospetti, l'avvio di altri processi o modifiche evidenti al sistema. Tuttavia, questo non esclude la possibilità che il malware abbia eseguito azioni dannose non catturate in questo log.

9. Possibile malware di ricognizione: Il comportamento osservato potrebbe essere coerente con un malware di ricognizione, progettato per raccogliere informazioni sul sistema infetto senza compiere azioni distruttive immediate.