Raccolta dei registri ProcMon per la risoluzione dei problemi AMP all'avvio

Sommario

Introduzione

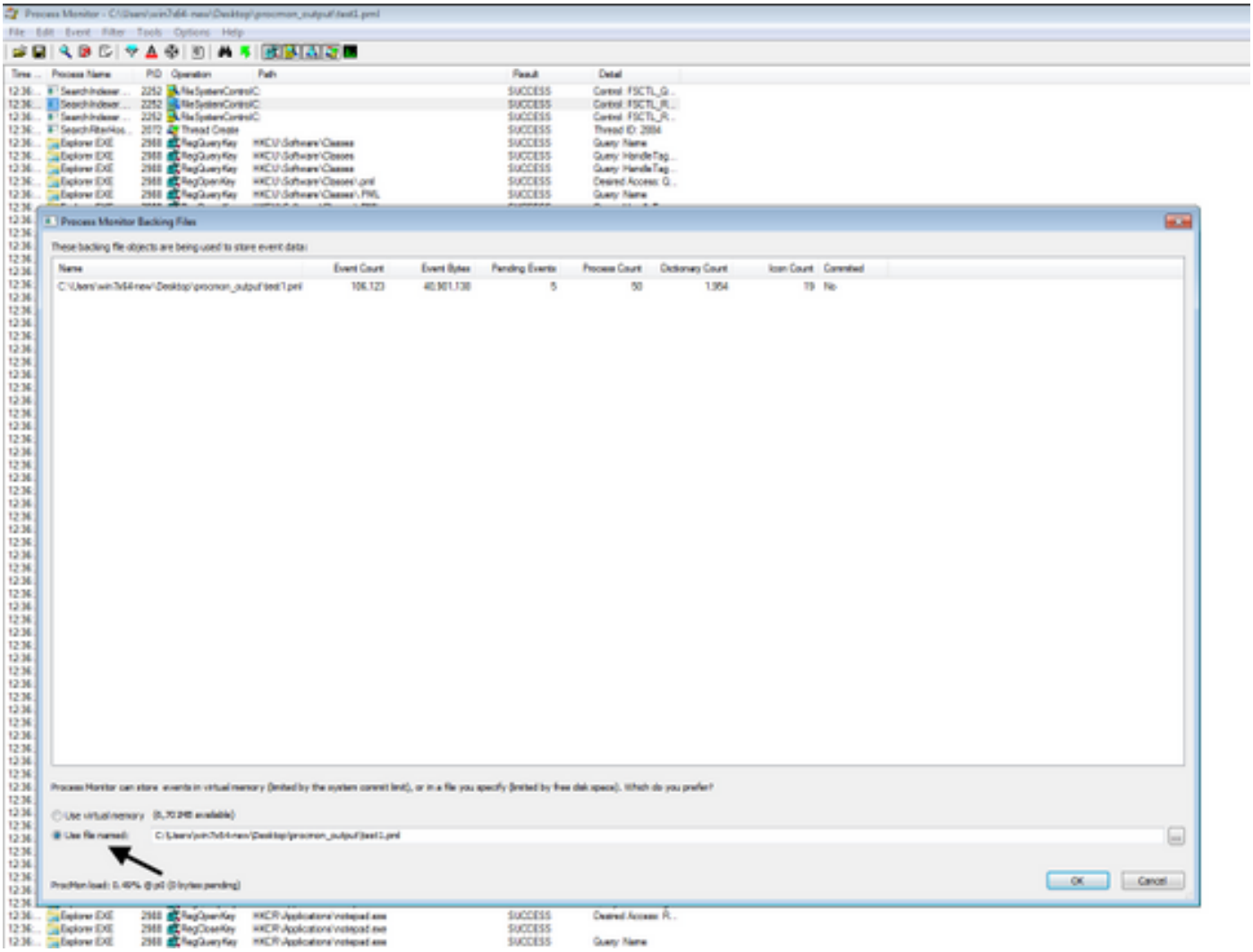
In qualità di amministratore di sistema, è possibile ottenere registri dettagliati utilizzando Process Monitor (procmon.exe) per determinare se il connettore FireAMP si blocca durante il processo di avvio del computer. Questi registri verranno richiesti anche da Cisco TAC per risolvere i problemi. Process Monitor è un'utilità gratuita che può aiutarci in questa fase. Il file può essere scaricato gratuitamente dal sito https://docs.microsoft.com/en-us/sysinternals/downloads/procmon

In questo documento viene descritto come raccogliere i log di ProcMon e i dump della memoria se il problema si verifica durante un processo di avvio del sistema (ovvero se sta generando BSOD all'avvio). Questi registri sono necessari per acquisire gli eventi di sistema che si verificano durante l'avvio.

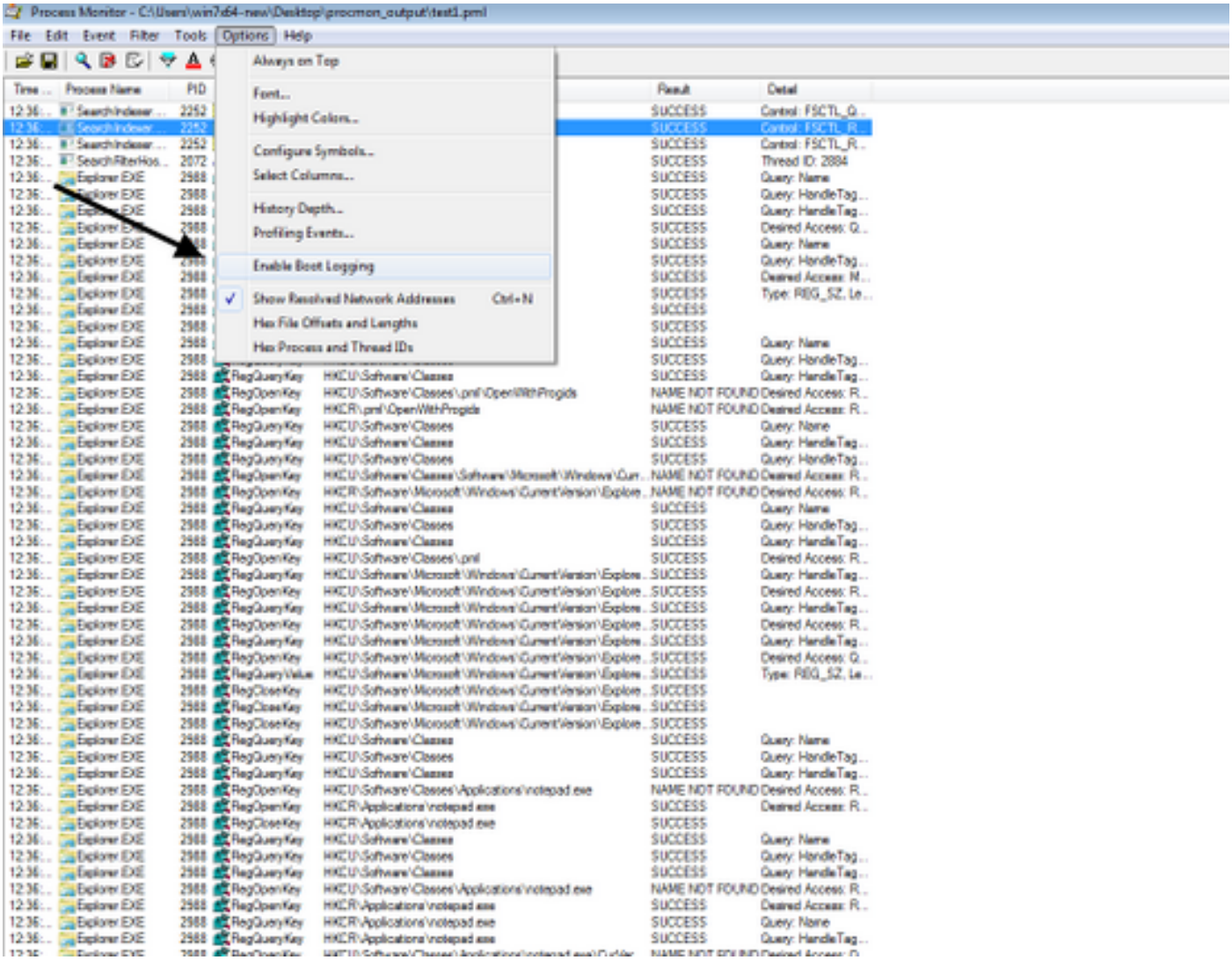
Procedura:

1. Impostare le macchine di prova in modo che il problema possa essere facilmente riprodotto.

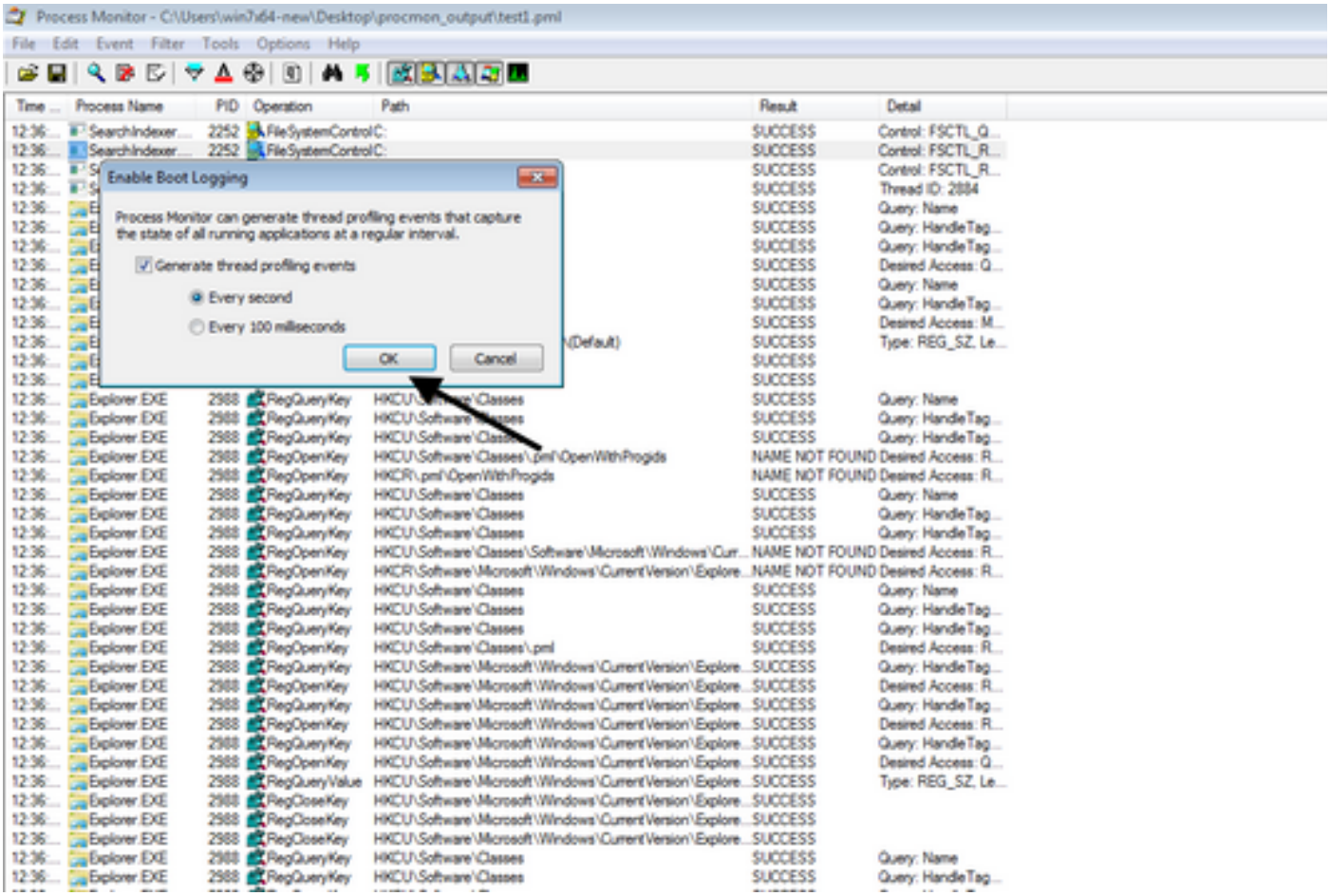
2. Scaricare ed eseguire lo strumento ProcMon come amministratore. Andare su **File -> Process Monitor Backing Files** e selezionare un **Percorso**.



3. In Procmon Tool, selezionare **Options -> Enable Boot Logging** (Opzioni > Abilita registrazione avvio).



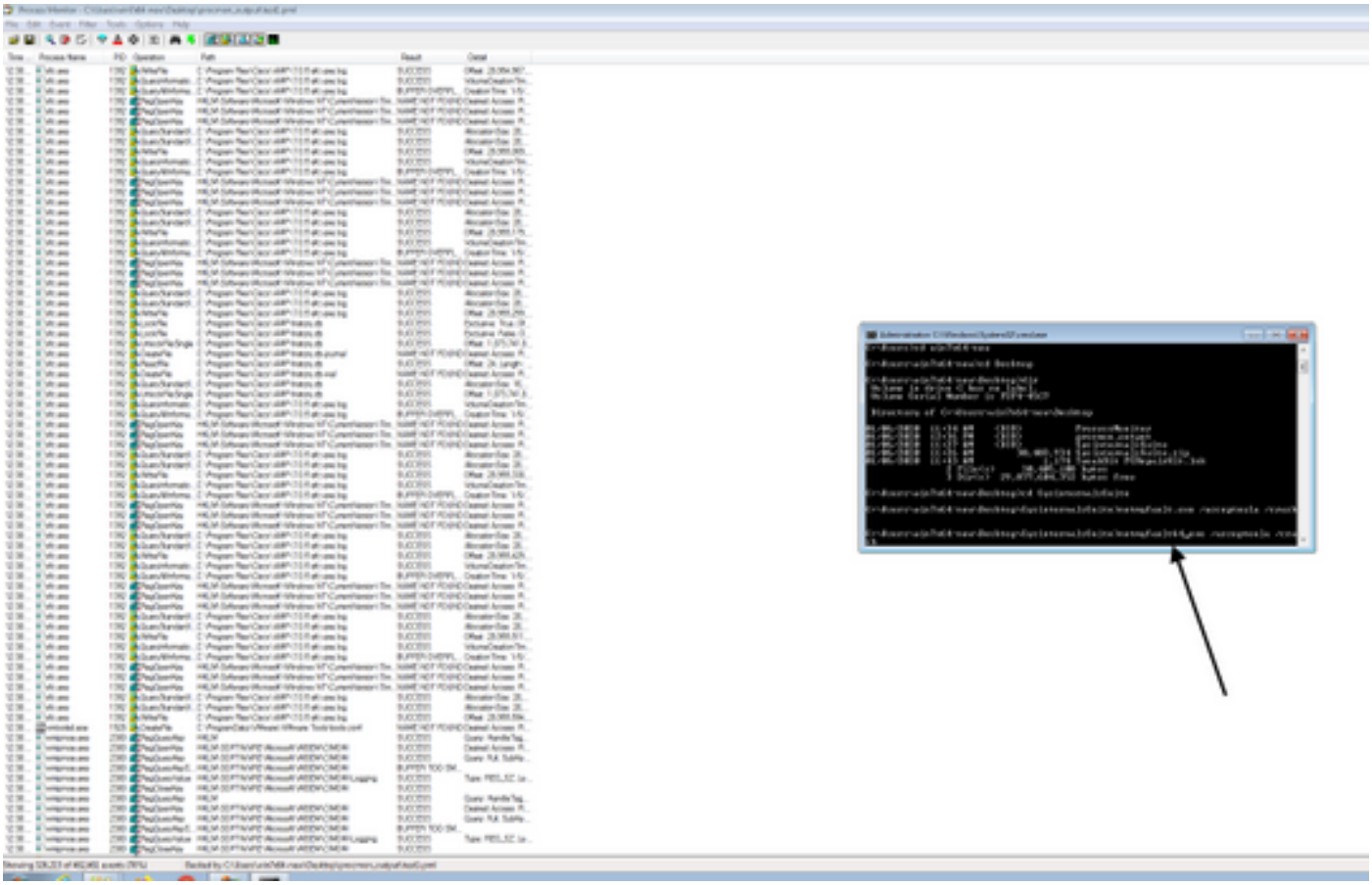
4. Selezionare **Genera eventi profiling minaccia** e **Ogni secondo.**



5. Assicurarsi che tutti i filtri pertinenti siano selezionati in Procmon e che i dati siano stati raccolti.

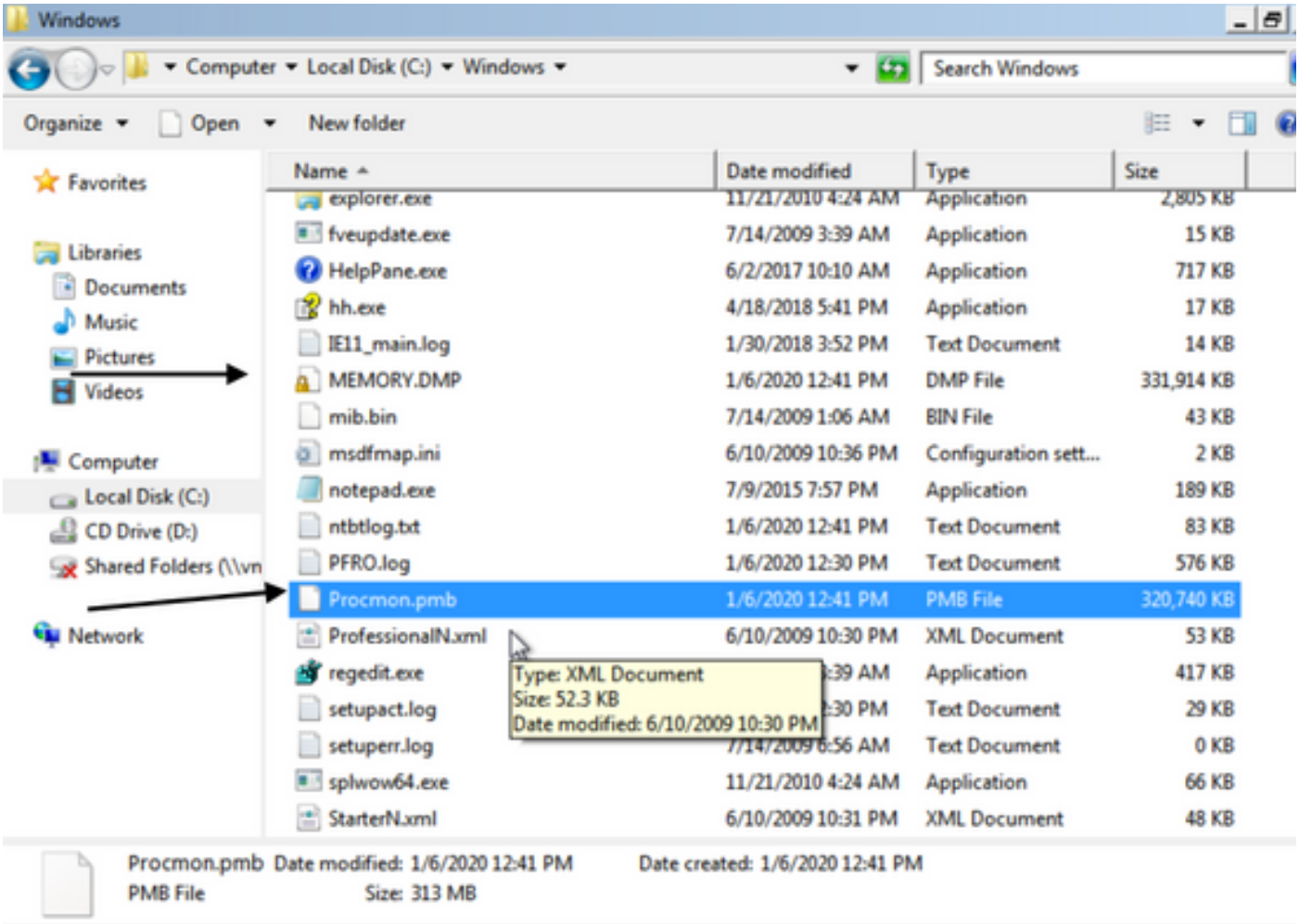
6. Se non si è in grado di replicare l'arresto anomalo, è possibile forzare l'arresto anomalo di Windows utilizzando l'utility NotMyFault64.exe, che è possibile ottenere da https://live.sysinternals.com/files/

Di seguito sono riportate le istruzioni per l'esecuzione. https://docs.microsoft.com/en-us/windows/client-management/generate-kernel-or-complete-crash-dump

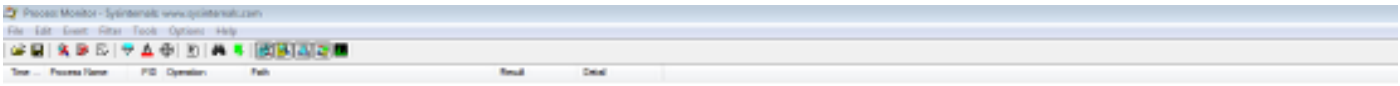


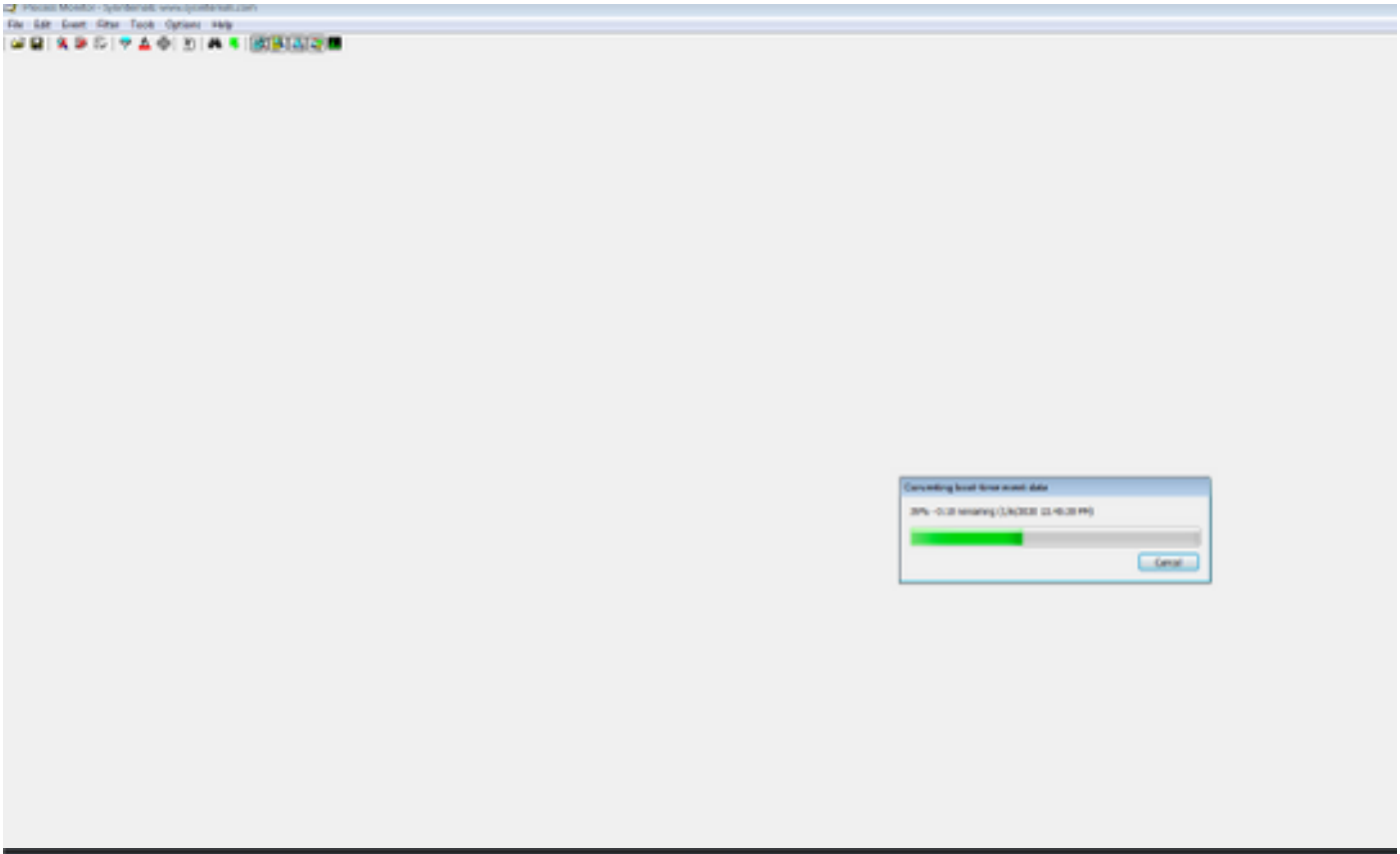
7. Bloccare la macchina.

8. Avviare il computer in modalità provvisoria e raccogliere manualmente **Procmon.pmb** e **MEMORY.DMP**, entrambi i file si trovano nella cartella C:\Windows. Questi file devono essere condivisi con Cisco TAC.



7. Se si è in grado di eseguire l'avvio in "modalità normale" se i file PMB vengono generati nella cartella C:\Windows, se si avvia nuovamente ProcMon verranno visualizzati i seguenti log. Da questo, è possibile salvare nuovamente gli eventi facendo clic sul pulsante Salva.





Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
12:41:...	smss.exe	292	Process Start		SUCCESS	Parent PID: 4, Com...
12:41:...	smss.exe	292	Thread Create		SUCCESS	Thread ID: 296
12:41:...	smss.exe	292	Load Image	C:\Windows\System32\smss.exe	SUCCESS	Image Base: 0x479...
12:41:...	smss.exe	292	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x779...
12:41:...	smss.exe	292	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Ima...	NAME NOT FOUND	Desired Access: Q...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: R...
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 1,024
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 1,024
12:41:...	smss.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41:...	smss.exe	292	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
12:41:...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 74,752, Len...
12:41:...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 1,024, Leng...
12:41:...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 107,008, Le...
12:41:...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 104,448, Le...
12:41:...	smss.exe	292	Thread Create		SUCCESS	Thread ID: 300
12:41:...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 104,448 Length: 2,560 I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O Priority: Normal
12:41:...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 107,008, Le...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\MiniNT	REPARSE	Desired Access: R...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\MiniNT	NAME NOT FOUND	Desired Access: R...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\...	REPARSE	Desired Access: All...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\...	SUCCESS	Desired Access: All...
12:41:...	smss.exe	292	RegDeleteValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	
12:41:...	smss.exe	292	RegSetValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_SZ, Le...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: R...
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_DWO...
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_DWO...
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Desired Access: M...
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41:...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41:...	smss.exe	292	RegDeleteValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41:...	smss.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Desired Access: M...
12:41:...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 0, Name: A...
12:41:...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 1, Name: M...
12:41:...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 2, Name: N...
12:41:...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 3, Name: PI...
12:41:...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 4, Name: P...
12:41:...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 5, Name: U...
12:41:...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NO MORE ENTRI...	Index: 6, Length: 4...
12:41:...	smss.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41:...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Desired Access: M...