2 - System > smms.exe

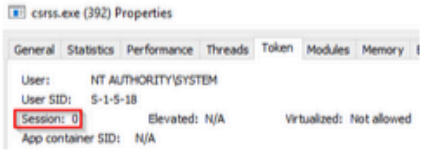
Task 4 System > smss.exe

The next process is **smss.exe** (**Session Manager Subsystem**). This process, also known as the **Windows Session Manager**, is responsible for creating new sessions. It is the first user-mode process started by the kernel.

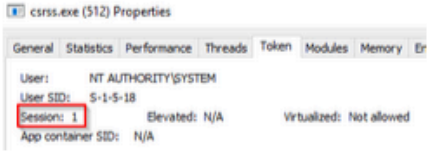
This process starts the kernel and user modes of the Windows subsystem (you can read more about the NT Architecture here). This subsystem includes win32k.sys (kernel mode), winsrv.dll (user mode), and csrss.exe (user mode).

Smss.exe starts csrss.exe (Windows subsystem) and wininit.exe in Session 0, an isolated Windows session for the operating system, and csrss.exe and winlogon.exe for Session 1, which is the user session. The first child instance creates child instances in new sessions, done by smss.exe copying itself into the new session and self-terminating. You can read more about this process here.

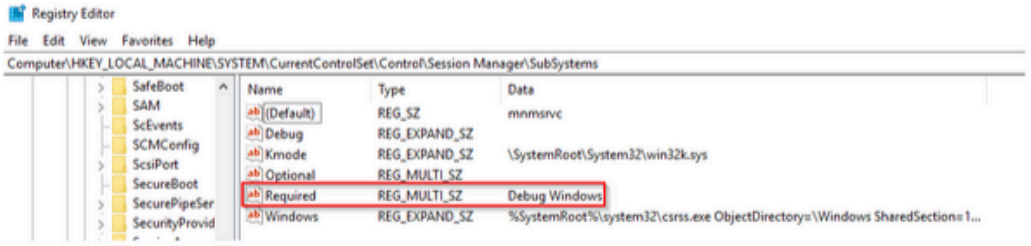
Session 0 (csrss.exe & wininit.exe)



Session 1 (csrss.exe & winlogon.exe)



Any other subsystem listed in the `Required` value of `HKLM\System\CurrentControlSet\Control\Session Manager\Subsystems` is also launched.



SMSS is also responsible for creating environment variables, virtual memory paging files and starts winlogon.exe (the Windows Logon Manager).

What is normal?

What is normal?

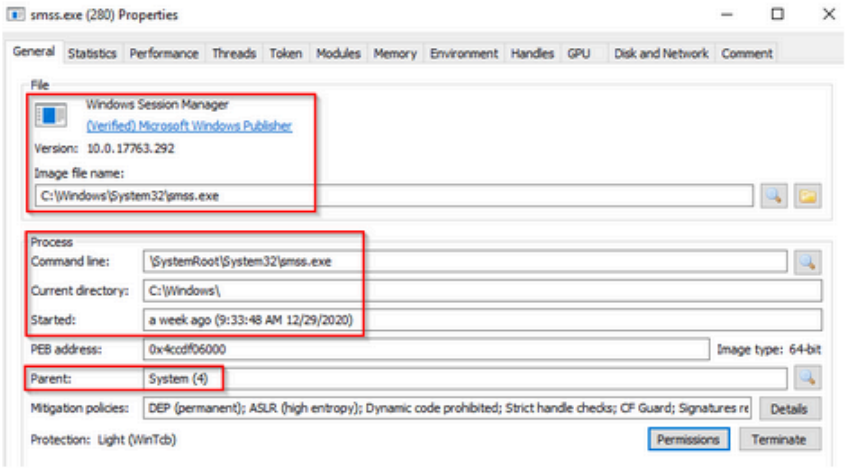


Image Path: %SystemRoot%\System32\smss.exe
Parent Process: System
Number of Instances: One master instance and child instance per session. The child instance exits after creating the session.
User Account: Local System
Start Time: Within seconds of boot time for the master instance

What is unusual?

- A different parent process other than System (4)
- The image path is different from C:\Windows\System32
- More than one running process. (children self-terminate and exit after each new session)
- The running User is not the SYSTEM user
- Unexpected registry entries for Subsystem

Answer the questions below

Aside from csrss.exe, what process does smss.exe spawn in Session 1?

winlogon.exe ✓ Correct Answer Hint