3 - csrss.exe

Task 5 csrss.exe

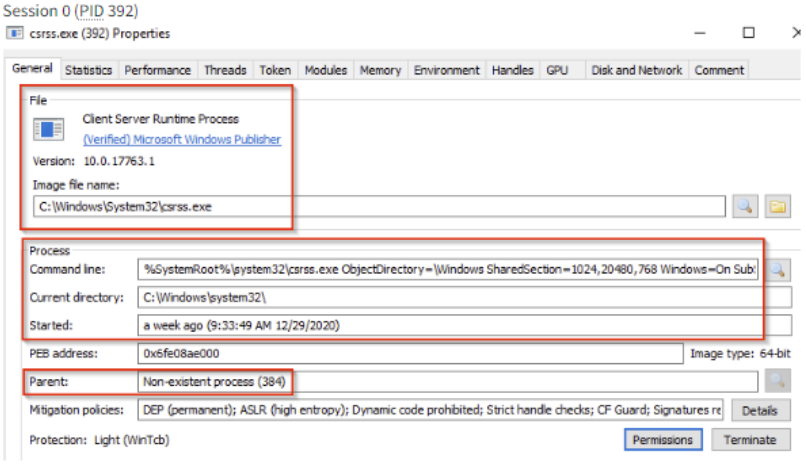
As mentioned in the previous section, **csrss.exe** (**Client Server Runtime Process**) is the user-mode side of the Windows subsystem. This process is always running and is critical to system operation. If this process is terminated by chance, it will result in system failure. This process is responsible for the Win32 console window and process thread creation and deletion. For each instance, csrsrv.dll, basesrv.dll, and winsrv.dll are loaded (along with others).

This process is also responsible for making the Windows API available to other processes, mapping drive letters, and handling the Windows shutdown process. You can read more about this process here.

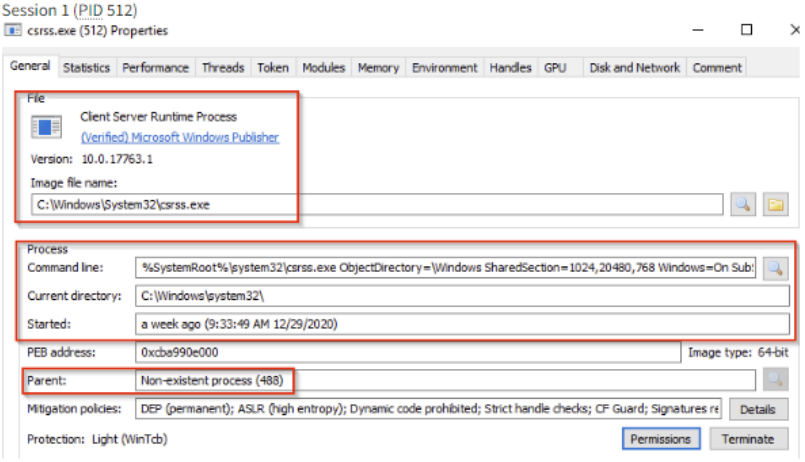
Note: Recall that csrss.exe and winlogon.exe are called from smss.exe at startup for Session 1.

What is normal?

Session 0 (PID 392)



Session 1 (PID 512)



Notice what is shown for the parent process for these two processes. Remember, these processes are spawned by smss.exe, which self-terminates itself.

Image Path: %SystemRoot%\System32\csrss.exe
Parent Process: Created by an instance of smss.exe
Number of Instances: Two or more
User Account: Local System
Start Time: Within seconds of boot time for the first two instances (for Session 0 and 1). Start times for additional instances occur as new sessions are created, although only Sessions 0 and 1 are often created.

What is unusual?

- An actual parent process. (smss.exe calls this process and self-terminates)
- Image file path other than C:\Windows\System32
- Subtle misspellings to hide rogue processes masquerading as csrss.exe in plain sight
- The user is not the SYSTEM user.