4 - Wininit.exe

Task 6 wininit.exe

The **Windows Initialization Process**, **wininit.exe**, is responsible for launching services.exe (Service Control Manager), lsass.exe (Local Security Authority), and lsaiso.exe within Session 0. It is another critical Windows process that runs in the background, along with its child processes.

wininit.exe	496	NT AUTHORITY\SYSTEM	Windows Start-Up Application	C:\Windows\System32\wininit.exe
services.exe	632	NT AUTHORITY\SYSTEM	Services and Controller app	C:\Windows\System32\services.exe
lsass.exe	640	NT AUTHORITY\SYSTEM	Local Security Authority Process	C:\Windows\System32\lsass.exe

Note: lsaiso.exe is a process associated with **Credential Guard and KeyGuard**. You will only see this process if Credential Guard is enabled.

What is normal?

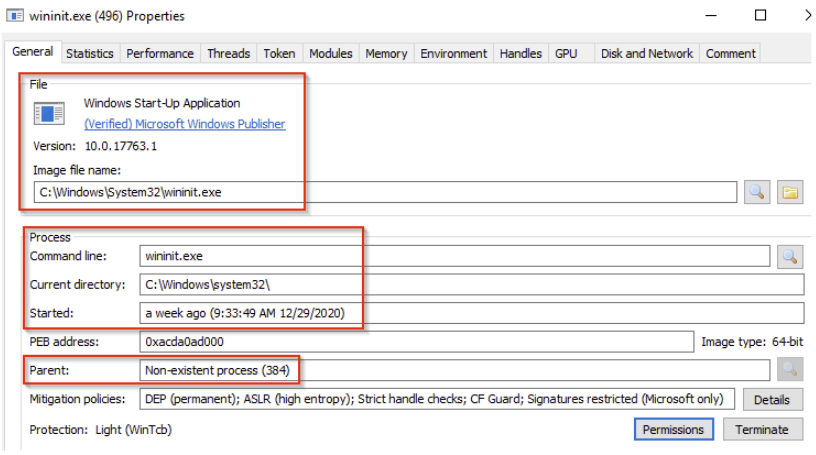

Image Path: %SystemRoot%\System32\wininit.exe
Parent Process: Created by an instance of smss.exe
Number of Instances: One
User Account: Local System
Start Time: Within seconds of boot time

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 in plain sight
- Multiple running instances
- Not running as SYSTEM