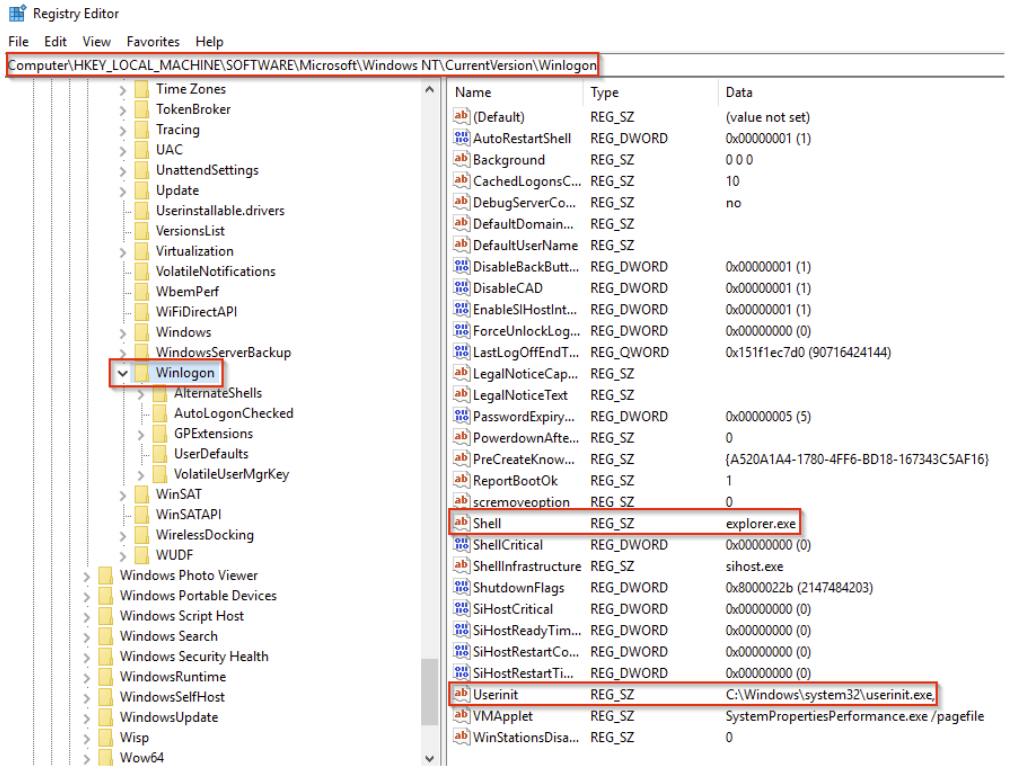
8 - winlogon.exe

Task 10 winlogon.exe

The **Windows Logon**, **winlogon.exe**, is responsible for handling the **Secure Attention Sequence** (SAS). It is the ALT+CTRL+DELETE key combination users press to enter their username & password.

This process is also responsible for loading the user profile. It loads the user's NTUSER.DAT into HKCU, and userinit.exe loads the user's shell. Read more about this process here.



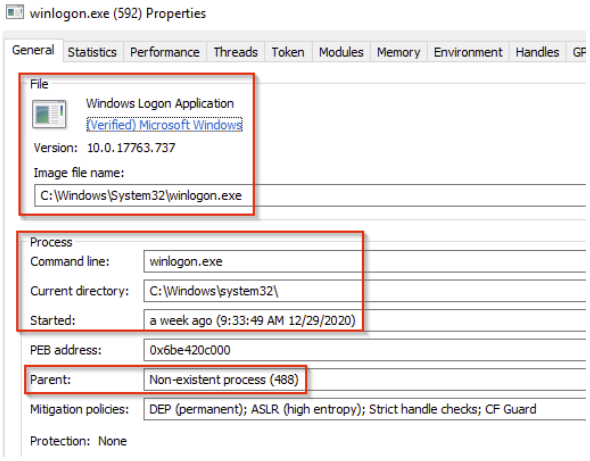
It is also responsible for locking the screen and running the user's screensaver, among other functions. You can read more about this process here.

Remember from earlier sections, smss.exe launches this process along with a copy of csrss.exe within Session 1.

winlogon.exe	592	NT AUTHORITY\SYSTEM	Windows Logon Application	C:\Windows\System32\winlogon.exe	winlogon.exe
fontdrvhost.exe	764	Font Driver Host\UMFD-1	Usermode Font Driver Host	C:\Windows\System32\fontdrvhost.exe	"fontdrvhost.exe"
dwm.exe	952	Window Manager\DWM-1	Desktop Window Manager	C:\Windows\System32\dwm.exe	"dwm.exe"

What is normal?

What is normal?



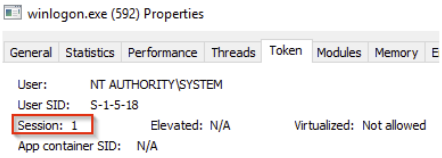


Image Path: %SystemRoot%\System32\winlogon.exe
Parent Process: Created by an instance of smss.exe that exits, so analysis tools usually do not provide the parent process name.
Number of Instances: One or more
User Account: Local System
Start Time: Within seconds of boot time for the first instance (for Session 1). Additional instances occur as new sessions are created, typically through Remote Desktop or Fast User Switching logons.

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
- Not running as SYSTEM
- Shell value in the registry other than explorer.exe

Answer the questions below

What is the non-existent parent process for winlogon.exe?

smss.exe

✓ Correct Answer