

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

What is normal?

wininit.exe (496) Properties

General

Statistics

Performance

Threads

Token

Modules

Memory

Environment

Handles

GPU

Disk and Network

Comment

File

Windows Start-Up Application
[\(Verified\) Microsoft Windows Publisher](#)
Version: 10.0.17763.1
Image file name:
C:\Windows\System32\wininit.exe

Process

Command line:
wininit.exe
Current directory:
C:\Windows\system32\
Started:
a week ago (9:33:49 AM 12/29/2020)
PEB address:
0xacda0ad000
Image type: 64-bit
Parent:
Non-existent process (384)
Mitigation policies:
DEP (permanent); ASLR (high entropy); Strict handle checks; CF Guard; Signatures restricted (Microsoft only)
Protection: Light (WinTcb)

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