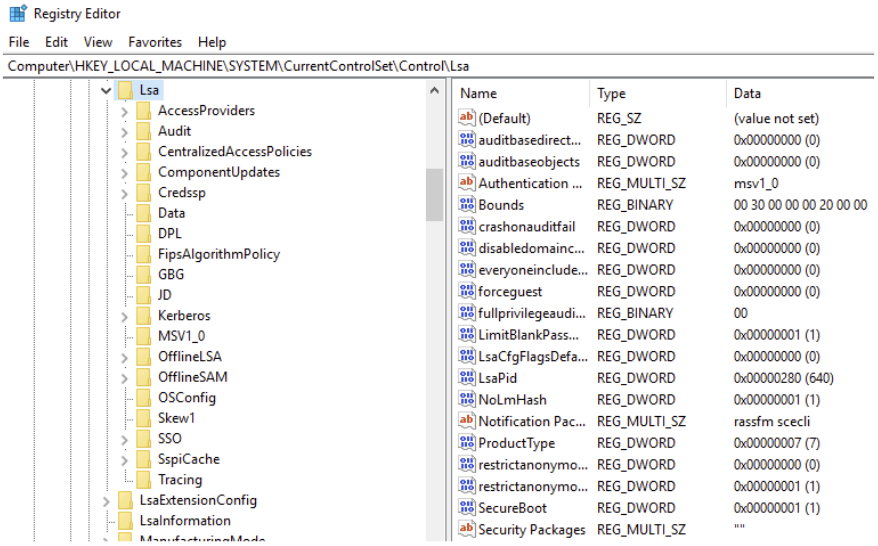
7 - lsass.exe

Task 9 lsass.exe

Per Wikipedia, "Local Security Authority Subsystem Service (**LSASS**) is a process in Microsoft Windows operating systems that is responsible for enforcing the security policy on the system. It verifies users logging on to a Windows computer or server, handles password changes, and creates access tokens. It also writes to the Windows Security Log."

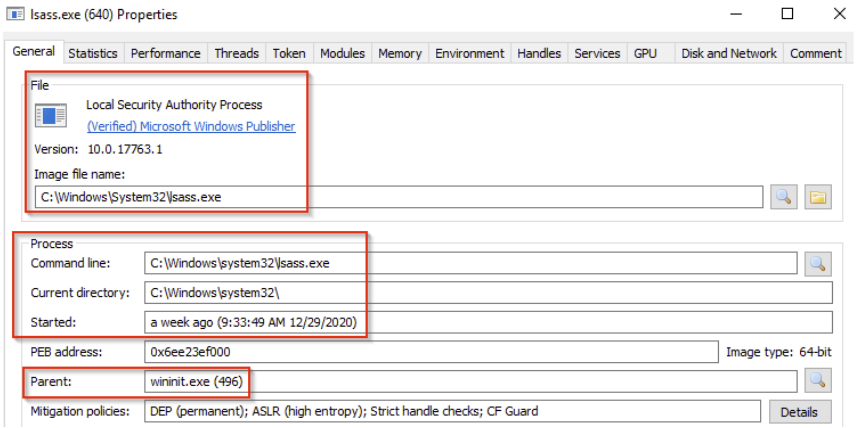
It creates security tokens for SAM (Security Account Manager), AD (Active Directory), and NETLOGON. It uses authentication packages specified in `HKLM\System\CurrentControlSet\Control\Lsa`.



Lsass.exe is another process adversaries target. Common tools such as **mimikatz** are used to dump credentials, or adversaries mimic this process to hide in plain sight. Again, they do this by either naming their malware by this process name or simply misspelling the malware slightly.

Extra reading: How LSASS is maliciously used and additional features that Microsoft has put into place to prevent these attacks.

What is normal?



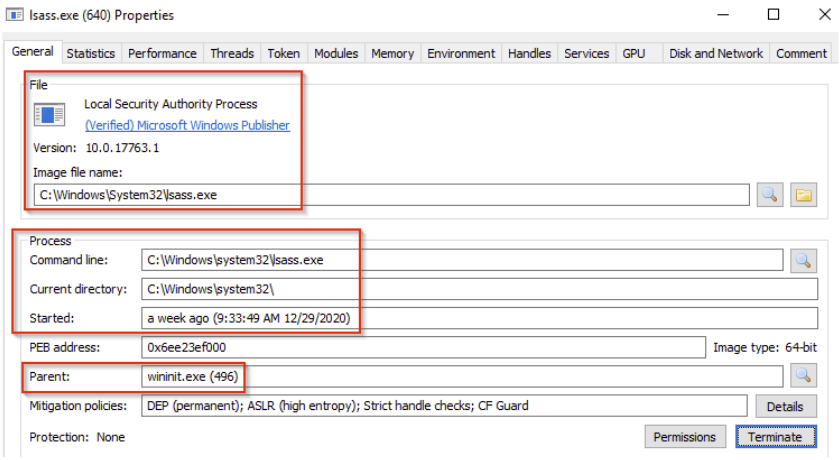


Image Path: %SystemRoot%\System32\lsass.exe
Parent Process: wininit.exe
Number of Instances: One
User Account: Local System
Start Time: Within seconds of boot time

What is unusual?

- A parent process other than wininit.exe
- Image file path other than C:\Windows\System32
- Subtle misspellings to hide rogue processes in plain sight
- Multiple running instances
- Not running as SYSTEM