

# Detection of Credential Dumping from LSASS Memory via Access and Dump Sequence, Detection Strategy DET0363

Archived: 2026-04-05 15:27:16 UTC

## Analytics

- [Windows](#)

### AN1030

A non-privileged or abnormal process attempts to open a handle with full access (0x1F0FFF) to lsass.exe and subsequently invokes memory dump, file creation, or registry modification indicative of credential scraping. This behavior chain reflects staged credential theft activity.

### Log Sources

### Mutable Elements

Field	Description
AccessMask	Set to 0x1F0FFF to detect full memory access attempts; can be scoped down to reduce noise.
TimeWindow	Defines time between LSASS access and dump file creation or registry modification (e.g., 5 minutes).
ParentProcessName	Allowlist known legitimate tools (e.g., AV/EDR) accessing lsass.exe.
DumpFilePath	Paths where memory dumps are written, e.g., %TEMP%, C:\Windows\Temp.
CommandLinePattern	Common dumping syntax like rundll32, procdump, comsvcs.dll, Invoke-Mimikatz.

---

Source: <https://attack.mitre.org/detectionstrategies/DET0363#AN1030>