# TTP Detail – T1177

## TTP Information

Name: LSASS Driver

Description: The Windows security subsystem is a set of components that manage and enforce the security policy for a computer or domain. The Local Security Authority (LSA) is the main component responsible for local security policy and user authentication. The LSA includes multiple dynamic link libraries (DLLs) associated with various other security functions, all of which run in the context of the LSA Subsystem Service (LSASS) lsass.exe process. (Citation: Microsoft Security Subsystem)

Adversaries may target lsass.exe drivers to obtain execution and/or persistence. By either replacing or adding illegitimate drivers (e.g., [DLL Side-Loading](https://attack.mitre.org/techniques/T1073) or [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1038)), an adversary can achieve arbitrary code execution triggered by continuous LSA operations.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: execution

**•** mitre-attack: persistence