# TTP Detail – T1547.008

## TTP Information

Name: LSASS Driver

Description: Adversaries may modify or add LSASS drivers to obtain persistence on compromised systems. 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 drivers to obtain persistence. By either replacing or adding illegitimate drivers (e.g., [Hijack Execution Flow](https://attack.mitre.org/techniques/T1574)), an adversary can use LSA operations to continuously execute malicious payloads.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation

## Malware

* Pasam
* Wingbird