Create or Modify System Process, Technique T1543 - Enterprise

Archived: 2026-04-02 10:44:52 UTC

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services.[1] On macOS, launchd processes known as Launch Daemon and Launch Agent are run to finish system initialization and load user specific parameters.[2]

Adversaries may install new services, daemons, or agents that can be configured to execute at startup or a repeatable interval in order to establish persistence. Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect.

Services, daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges. Adversaries may leverage this functionality to create or modify system processes in order to escalate privileges.[3]
