

# Create or Modify System Process: Launch Agent, Sub-technique T1543.001 - Enterprise

Archived: 2026-04-05 16:59:42 UTC

Adversaries may create or modify launch agents to repeatedly execute malicious payloads as part of persistence. When a user logs in, a per-user launchd process is started which loads the parameters for each launch-on-demand user agent from the property list (.plist) file found in `/System/Library/LaunchAgents`, `/Library/LaunchAgents`, and `~/Library/LaunchAgents`.<sup>[1][2][3]</sup> Property list files use the `Label`, `ProgramArguments`, and `RunAtLoad` keys to identify the Launch Agent's name, executable location, and execution time.<sup>[4]</sup> Launch Agents are often installed to perform updates to programs, launch user specified programs at login, or to conduct other developer tasks.

Launch Agents can also be executed using the [Launchctl](#) command.

Adversaries may install a new Launch Agent that executes at login by placing a .plist file into the appropriate folders with the `RunAtLoad` or `KeepAlive` keys set to `true`.<sup>[5][6]</sup> The Launch Agent name may be disguised by using a name from the related operating system or benign software. Launch Agents are created with user level privileges and execute with user level permissions.<sup>[7][8]</sup>

---

Source: <https://attack.mitre.org/techniques/T1159>