# TTP Detail – T1543.004

## TTP Information

Name: Launch Daemon

Description: Adversaries may create or modify Launch Daemons to execute malicious payloads as part of persistence. Launch Daemons are plist files used to interact with Launchd, the service management framework used by macOS. Launch Daemons require elevated privileges to install, are executed for every user on a system prior to login, and run in the background without the need for user interaction. During the macOS initialization startup, the launchd process loads the parameters for launch-on-demand system-level daemons from plist files found in <code>/System/Library/LaunchDaemons/</code> and <code>/Library/LaunchDaemons/</code>. Required Launch Daemons parameters include a <code>Label</code> to identify the task, <code>Program</code> to provide a path to the executable, and <code>RunAtLoad</code> to specify when the task is run. Launch Daemons are often used to provide access to shared resources, updates to software, or conduct automation tasks.(Citation: AppleDocs Launch Agent Daemons)(Citation: Methods of Mac Malware Persistence)(Citation: launchd Keywords for plists)  
  
Adversaries may install a Launch Daemon configured to execute at startup by using the <code>RunAtLoad</code> parameter set to <code>true</code> and the <code>Program</code> parameter set to the malicious executable path. The daemon name may be disguised by using a name from a related operating system or benign software (i.e. [Masquerading](https://attack.mitre.org/techniques/T1036)). When the Launch Daemon is executed, the program inherits administrative permissions.(Citation: WireLurker)(Citation: OSX Malware Detection)  
  
Additionally, system configuration changes (such as the installation of third party package managing software) may cause folders such as <code>usr/local/bin</code> to become globally writeable. So, it is possible for poor configurations to allow an adversary to modify executables referenced by current Launch Daemon's plist files.(Citation: LaunchDaemon Hijacking)(Citation: sentinelone macos persist Jun 2019)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

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

## Malware

* AppleJeus
* Bundlore
* COATHANGER
* Dacls
* Green Lambert
* LoudMiner
* OSX\_OCEANLOTUS.D
* ThiefQuest
* XCSSET