# TTP Detail – T1053.004

## TTP Information

Name: Launchd

Description: This technique is deprecated due to the inaccurate usage. The report cited did not provide technical detail as to how the malware interacted directly with launchd rather than going through known services. Other system services are used to interact with launchd rather than launchd being used by itself.

Adversaries may abuse the <code>Launchd</code> daemon to perform task scheduling for initial or recurring execution of malicious code. The <code>launchd</code> daemon, native to macOS, is responsible for loading and maintaining services within the operating system. This process loads the parameters for each launch-on-demand system-level daemon from the property list (plist) files found in <code>/System/Library/LaunchDaemons</code> and <code>/Library/LaunchDaemons</code> (Citation: AppleDocs Launch Agent Daemons). These LaunchDaemons have property list files which point to the executables that will be launched (Citation: Methods of Mac Malware Persistence).

An adversary may use the <code>launchd</code> daemon in macOS environments to schedule new executables to run at system startup or on a scheduled basis for persistence. <code>launchd</code> can also be abused to run a process under the context of a specified account. Daemons, such as <code>launchd</code>, run with the permissions of the root user account, and will operate regardless of which user account is logged in.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

**•** mitre-attack: persistence

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