# TTP Detail – T1569.001

## TTP Information

Name: Launchctl

Description: Adversaries may abuse launchctl to execute commands or programs. Launchctl interfaces with launchd, the service management framework for macOS. Launchctl supports taking subcommands on the command-line, interactively, or even redirected from standard input.(Citation: Launchctl Man)

Adversaries use launchctl to execute commands and programs as [Launch Agent](https://attack.mitre.org/techniques/T1543/001)s or [Launch Daemon](https://attack.mitre.org/techniques/T1543/004)s. Common subcommands include: <code>launchctl load</code>,<code>launchctl unload</code>, and <code>launchctl start</code>. Adversaries can use scripts or manually run the commands <code>launchctl load -w "%s/Library/LaunchAgents/%s"</code> or <code>/bin/launchctl load</code> to execute [Launch Agent](https://attack.mitre.org/techniques/T1543/001)s or [Launch Daemon](https://attack.mitre.org/techniques/T1543/004)s.(Citation: Sofacy Komplex Trojan)(Citation: 20 macOS Common Tools and Techniques)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* AppleJeus
* Calisto
* Cuckoo Stealer
* LoudMiner
* XCSSET
* macOS.OSAMiner