



# launchctl

Created by Josh Carullo

## Description

launchctl can be used to load, start, stop, and unload macOS services. It is a command-line frontend to launchd.

Created	Tactics	Tags
2023-05-27	<div>ExecutionPersistence</div>	<div>bashzshoneliner</div>

## Paths

- /bin/launchctl

## Use Cases

### Use launchctl to execute an application

A oneliner that will load a plist as a LaunchAgent or LaunchDaemon, achieving persistence on a target machine. This command requires root privileges.

```
sudo launchctl load /Library/LaunchAgent/com.apple.installer
```

## Persistent launch agent

Creation of a persistent launch agent called with  
\$HOME/Library/LaunchAgents/com.apple.updates.plist

```
launchctl load -w ~/Library/LaunchAgents/com.apple.updates.plist
```

## Detections

- LaunchAgents and LaunchDaemons must have a plist file on disk in the root, system, or user Library directory. Monitoring for plist's with executables located in /tmp or /Shared could identify suspicious applications.
- Jamf Protect: Detect launchctl activity that unloads or bootsout specific service

## Resources

- 20 Common Tools & Techniques used by macOS threat Actors & Malware
- Mitre Attack Technique: launchctl T1569
- MITRE ATT&CK T1543.001 Create or Modify System Process: Launch Agent
- Komplex OS X Trojan (Sofacy)