# TTP Detail – T1543.001

## TTP Information

Name: Launch Agent

Description: 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 <code>/System/Library/LaunchAgents</code>, <code>/Library/LaunchAgents</code>, and <code>~/Library/LaunchAgents</code>.(Citation: AppleDocs Launch Agent Daemons)(Citation: OSX Keydnap malware) (Citation: Antiquated Mac Malware) Property list files use the <code>Label</code>, <code>ProgramArguments </code>, and <code>RunAtLoad</code> keys to identify the Launch Agent's name, executable location, and execution time.(Citation: OSX.Dok Malware) 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](https://attack.mitre.org/techniques/T1569/001) command.

Adversaries may install a new Launch Agent that executes at login by placing a .plist file into the appropriate folders with the <code>RunAtLoad</code> or <code>KeepAlive</code> keys set to <code>true</code>.(Citation: Sofacy Komplex Trojan)(Citation: Methods of Mac Malware Persistence) 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.(Citation: OSX Malware Detection)(Citation: OceanLotus for OS X)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

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

## Malware

* Bundlore
* Calisto
* CoinTicker
* CookieMiner
* CrossRAT
* Cuckoo Stealer
* Dacls
* Dok
* FruitFly
* Green Lambert
* Keydnap
* Komplex
* MacMa
* MacSpy
* NETWIRE
* OSX\_OCEANLOTUS.D
* Proton
* ThiefQuest
* macOS.OSAMiner