# TTP Detail – T1547.015

## TTP Information

Name: Login Items

Description: Adversaries may add login items to execute upon user login to gain persistence or escalate privileges. Login items are applications, documents, folders, or server connections that are automatically launched when a user logs in.(Citation: Open Login Items Apple) Login items can be added via a shared file list or Service Management Framework.(Citation: Adding Login Items) Shared file list login items can be set using scripting languages such as [AppleScript](https://attack.mitre.org/techniques/T1059/002), whereas the Service Management Framework uses the API call <code>SMLoginItemSetEnabled</code>.

Login items installed using the Service Management Framework leverage <code>launchd</code>, are not visible in the System Preferences, and can only be removed by the application that created them.(Citation: Adding Login Items)(Citation: SMLoginItemSetEnabled Schroeder 2013) Login items created using a shared file list are visible in System Preferences, can hide the application when it launches, and are executed through LaunchServices, not launchd, to open applications, documents, or URLs without using Finder.(Citation: Launch Services Apple Developer) Users and applications use login items to configure their user environment to launch commonly used services or applications, such as email, chat, and music applications.

Adversaries can utilize [AppleScript](https://attack.mitre.org/techniques/T1059/002) and [Native API](https://attack.mitre.org/techniques/T1106) calls to create a login item to spawn malicious executables.(Citation: ELC Running at startup) Prior to version 10.5 on macOS, adversaries can add login items by using [AppleScript](https://attack.mitre.org/techniques/T1059/002) to send an Apple events to the “System Events” process, which has an AppleScript dictionary for manipulating login items.(Citation: Login Items AE) Adversaries can use a command such as <code>tell application “System Events” to make login item at end with properties /path/to/executable</code>.(Citation: Startup Items Eclectic)(Citation: hexed osx.dok analysis 2019)(Citation: Add List Remove Login Items Apple Script) This command adds the path of the malicious executable to the login item file list located in <code>~/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm</code>.(Citation: Startup Items Eclectic) Adversaries can also use login items to launch executables that can be used to control the victim system remotely or as a means to gain privilege escalation by prompting for user credentials.(Citation: objsee mac malware 2017)(Citation: CheckPoint Dok)(Citation: objsee netwire backdoor 2019)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

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

## Malware

* Dok
* Green Lambert
* NETWIRE