# TTP Detail – T1547.007

## TTP Information

Name: Re-opened Applications

Description: Adversaries may modify plist files to automatically run an application when a user logs in. When a user logs out or restarts via the macOS Graphical User Interface (GUI), a prompt is provided to the user with a checkbox to "Reopen windows when logging back in".(Citation: Re-Open windows on Mac) When selected, all applications currently open are added to a property list file named <code>com.apple.loginwindow.[UUID].plist</code> within the <code>~/Library/Preferences/ByHost</code> directory.(Citation: Methods of Mac Malware Persistence)(Citation: Wardle Persistence Chapter) Applications listed in this file are automatically reopened upon the user’s next logon.

Adversaries can establish [Persistence](https://attack.mitre.org/tactics/TA0003) by adding a malicious application path to the <code>com.apple.loginwindow.[UUID].plist</code> file to execute payloads when a user logs in.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

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