# TTP Detail – T1647

## TTP Information

Name: Plist File Modification

Description: Adversaries may modify property list files (plist files) to enable other malicious activity, while also potentially evading and bypassing system defenses. macOS applications use plist files, such as the <code>info.plist</code> file, to store properties and configuration settings that inform the operating system how to handle the application at runtime. Plist files are structured metadata in key-value pairs formatted in XML based on Apple's Core Foundation DTD. Plist files can be saved in text or binary format.(Citation: fileinfo plist file description)

Adversaries can modify key-value pairs in plist files to influence system behaviors, such as hiding the execution of an application (i.e. [Hidden Window](https://attack.mitre.org/techniques/T1564/003)) or running additional commands for persistence (ex: [Launch Agent](https://attack.mitre.org/techniques/T1543/001)/[Launch Daemon](https://attack.mitre.org/techniques/T1543/004) or [Re-opened Applications](https://attack.mitre.org/techniques/T1547/007)).

For example, adversaries can add a malicious application path to the `~/Library/Preferences/com.apple.dock.plist` file, which controls apps that appear in the Dock. Adversaries can also modify the <code>LSUIElement</code> key in an application’s <code>info.plist</code> file to run the app in the background. Adversaries can also insert key-value pairs to insert environment variables, such as <code>LSEnvironment</code>, to enable persistence via [Dynamic Linker Hijacking](https://attack.mitre.org/techniques/T1574/006).(Citation: wardle chp2 persistence)(Citation: eset\_osx\_flashback)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Cuckoo Stealer
* XCSSET