# TTP Detail – T1547.011

## TTP Information

Name: Plist Modification

Description: Adversaries can modify property list files (plist files) to execute their code as part of establishing persistence. Plist files are used by macOS applications to store properties and configuration settings for applications and services. Applications use information plist files, <code>Info.plist</code>, to tell the operating system how to handle the application at runtime using structured metadata in the form of keys and values. Plist files are formatted in XML and based on Apple's Core Foundation DTD and can be saved in text or binary format.(Citation: fileinfo plist file description)

Adversaries can modify paths to executed binaries, add command line arguments, and insert key/pair values to plist files in auto-run locations which execute upon user logon or system startup. Through modifying plist files in these locations, adversaries can also execute a malicious dynamic library (dylib) by adding a dictionary containing the <code>DYLD\_INSERT\_LIBRARIES</code> key combined with a path to a malicious dylib under the <code>EnvironmentVariables</code> key in a plist file. Upon user logon, the plist is called for execution and the malicious dylib is executed within the process space. Persistence can also be achieved by modifying the <code>LSEnvironment</code> key in the application's <code>Info.plist</code> file.(Citation: wardle artofmalware volume1)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

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