# TTP Detail – T1546.006

## TTP Information

Name: LC\_LOAD\_DYLIB Addition

Description: Adversaries may establish persistence by executing malicious content triggered by the execution of tainted binaries. Mach-O binaries have a series of headers that are used to perform certain operations when a binary is loaded. The LC\_LOAD\_DYLIB header in a Mach-O binary tells macOS and OS X which dynamic libraries (dylibs) to load during execution time. These can be added ad-hoc to the compiled binary as long as adjustments are made to the rest of the fields and dependencies.(Citation: Writing Bad Malware for OSX) There are tools available to perform these changes.

Adversaries may modify Mach-O binary headers to load and execute malicious dylibs every time the binary is executed. Although any changes will invalidate digital signatures on binaries because the binary is being modified, this can be remediated by simply removing the LC\_CODE\_SIGNATURE command from the binary so that the signature isn’t checked at load time.(Citation: Malware Persistence on OS X)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

**•** mitre-attack: persistence