Plist File Modification, Technique T1647 - Enterprise

Archived: 2026-04-05 16:59:29 UTC

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 `info.plist` 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.[1]

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) or running additional commands for persistence (ex: Launch Agent/Launch Daemon or Re-opened Applications).

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 `LSUIElement` key in an application's `info.plist` file to run the app in the background. Adversaries can also insert key-value pairs to insert environment variables, such as `LSEnvironment`, to enable persistence via Dynamic Linker Hijacking.[2][3]

Source: https://attack.mitre.org/techniques/T1647