Boot or Logon Initialization Scripts: Login Hook, Sub-technique T1037.002 - Enterprise

Archived: 2026-04-05 16:18:12 UTC

Adversaries may use a Login Hook to establish persistence executed upon user logon. A login hook is a plist file that points to a specific script to execute with root privileges upon user logon. The plist file is located in the `/Library/Preferences/com.apple.loginwindow.plist` file and can be modified using the `defaults` command-line utility. This behavior is the same for logout hooks where a script can be executed upon user logout. All hooks require administrator permissions to modify or create hooks.[1][2]

Adversaries can add or insert a path to a malicious script in the `com.apple.loginwindow.plist` file, using the `LoginHook` or `LogoutHook` key-value pair. The malicious script is executed upon the next user login. If a login hook already exists, adversaries can add additional commands to an existing login hook. There can be only one login and logout hook on a system at a time.[3][4]

Note: Login hooks were deprecated in 10.11 version of macOS in favor of Launch Daemon and Launch Agent

---

Source: https://attack.mitre.org/techniques/T1037/002