Boot or Logon Autostart Execution: Login Items, Sub-technique T1547.015 - Enterprise

Archived: 2026-04-05 14:31:18 UTC

Adversaries may add login items to execute upon user login to gain persistence or escalate privileges. Login items are applications, documents, folders, or server connections that are automatically launched when a user logs in.[1] Login items can be added via a shared file list or Service Management Framework.[2] Shared file list login items can be set using scripting languages such as AppleScript, whereas the Service Management Framework uses the API call `SMLoginItemSetEnabled`.

Login items installed using the Service Management Framework leverage `launchd`, are not visible in the System Preferences, and can only be removed by the application that created them.[2][3] Login items created using a shared file list are visible in System Preferences, can hide the application when it launches, and are executed through LaunchServices, not launchd, to open applications, documents, or URLs without using Finder.[4] Users and applications use login items to configure their user environment to launch commonly used services or applications, such as email, chat, and music applications.

Adversaries can utilize AppleScript and Native API calls to create a login item to spawn malicious executables.[5] Prior to version 10.5 on macOS, adversaries can add login items by using AppleScript to send an Apple events to the "System Events" process, which has an AppleScript dictionary for manipulating login items.[6] Adversaries can use a command such as `tell application "System Events" to make login item at end with properties /path/to/executable`.[7][8][9] This command adds the path of the malicious executable to the login item file list located in `~/Library/Application Support/com.apple.backgroundtaskmanagementagent/backgrounditems.btm`.[7] Adversaries can also use login items to launch executables that can be used to control the victim system remotely or as a means to gain privilege escalation by prompting for user credentials.[10][11][12]

Source: https://attack.mitre.org/techniques/T1547/015