Beyond the good ol' LaunchAgents - 8 - Hammerspoon

theevilbit.github.io/beyond/beyond_0008

March 23, 2021

> This is part 8 in the series of “Beyond the good ol' LaunchAgents”, where I try to collect various persistence techniques for macOS. For more background check the introduction.

This idea came from my colleague @dejandayoff. It’s another application specific persistence option, related to Hammerspoon. The app is an automation tool, that allows macOS scripting through LUA scripting language. We can even embed full AppleScript code as well as run shell scripts.

The app looks for a single file, `~/.hammerspoon/init.lua`, and when started the script will be executed. They have plenty of examples on their Getting Started page, and an extensive API documentation.

I tried the following simple script.

```
hs.execute("id > ~/hs.txt")
```

It runs `id` and redirects its output to a file. Indeed, when the app is started, this file is created with the expected output.

```
csaby@bigsur ~ % open /Applications/Hammerspoon.app
csaby@bigsur ~ % cat hs.txt
uid=501(csaby) gid=20(staff)
groups=20(staff),12(everyone),61(localaccounts),79(_appserverusr),80(admin),81(_appser

csaby@bigsur ~ % cat ~/.hammerspoon/init.lua
hs.execute("id > ~/hs.txt")
```

Beyond that Hammerspoon has some really nice entitlements, so we get access to these privacy resources as well if it was ever approved for the app.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>com.apple.security.automation.apple-events</key>
        <true/>
        <key>com.apple.security.cs.allow-jit</key>
        <true/>
        <key>com.apple.security.cs.allow-unsigned-executable-memory</key>
        <true/>
        <key>com.apple.security.cs.disable-executable-page-protection</key>
        <true/>
        <key>com.apple.security.cs.disable-library-validation</key>
        <true/>
        <key>com.apple.security.device.audio-input</key>
        <true/>
        <key>com.apple.security.device.camera</key>
        <true/>
        <key>com.apple.security.personal-information.addressbook</key>
        <true/>
        <key>com.apple.security.personal-information.calendars</key>
        <true/>
        <key>com.apple.security.personal-information.location</key>
        <true/>
        <key>com.apple.security.personal-information.photos-library</key>
        <true/>
</dict>
</plist>
```