Beyond the good ol' LaunchAgents - 27 - Dock shortcuts

theevilbit.github.io/beyond/beyond_0027

February 8, 2022

> This is part 27 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.

macOS Dock stores shortcuts for applications, that we would like to access through the, well... Dock. It stores all settings in `~/Library/Preferences/com.apple.dock.plist`. Although we can edit this PLIST directly, we can also use the `defaults` utility to change it. For example adding a new entry:

```
defaults write com.apple.dock persistent-apps -array-add '<dict><key>tile-data</key>
<dict><key>file-data</key><dict><key>_CFURLString</key>
<string>/System/Applications/Books.app</string><key>_CFURLStringType</key>
<integer>0</integer></dict></dict></dict>'

killall Dock
```

> This is part 27 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.

Note that we don't need to add the `bundle-identifier` or the `book` tags, what is also detailed in Leo's presentation.

At the end we need to restart Dock, so the new icon shows up. Of course we could also change items. The problem it creates is that `defaults` uses the `cfprefsd` daemon to change the file, which is the one that normally changes this file anyway, so this can break detection. Below is the `fs_usage` file system log showing this change.

```
14:51:53  openat            [3]/com.apple.dock.plist
0.000017   cfprefsd
14:51:53  openat            [3]/com.apple.dock.plist
0.000010   cfprefsd
14:51:53  openat            [3]/com.apple.dock.plist
0.000008   cfprefsd
14:51:53    RdData[A]       com.apple.dock.plist
0.000822 W cfprefsd
14:51:53  openat            [3]/com.apple.dock.plist
0.000012   cfprefsd
14:51:53  fstatat64         [3]/com.apple.dock.plist
0.000006   cfprefsd
14:51:53  openat            [3]/com.apple.dock.plist
0.000012   cfprefsd
14:51:53  access            /Users/csaby/Library/Preferences/com.apple.dock.plist
0.000011   cfprefsd
14:51:53  openat
/_hwnkhn904xg_pwlhb83_k040000gn/T/TemporaryItems/com.apple.dock.plist.I5zYdrH
0.000127   cfprefsd
14:51:53    WrData[A]
/_hwnkhn904xg_pwlhb83_k040000gn/T/TemporaryItems/com.apple.dock.plist.I5zYdrH
0.000154 W cfprefsd
```

The other thing we can do, if we don't want to rely on `defaults`, is calling the Preferences API directly to change the file, or even `cfprefsd`'s XPC service. Thus as an attacker we can mask the change of this file to appear as legitimate. I leave this as an exercise to the reader how to do these.

macOS admins work a lot with Dock preferences, so you can find other tricks in their blogposts, here are a few for example:

Adding Objects To The Dock - krypted Terminal Tricks: Mastering the Iconic macOS Dock, Part 3 GitHub - kcrawford/dockutil: command line tool for managing dock items