Beyond the good ol' LaunchAgents - 21 - Re-opened Applications

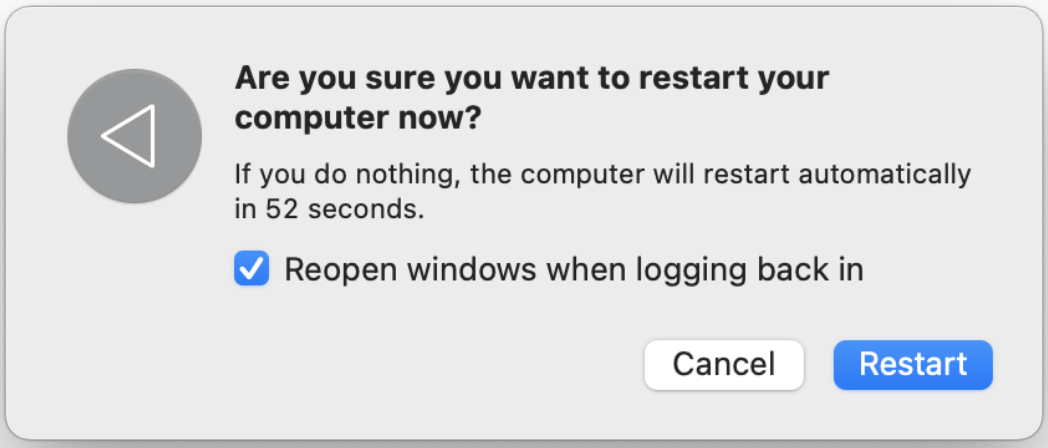
theevilbit.github.io/beyond/beyond_0021

October 12, 2021

> This is part 21 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 method was also documented by Patrick Wardle, in his original Methods of Malware Persistence white paper and also at MITRE ATT&CK®.

When we restart macOS, we are presented with the following window:



I guess, most users keep it selected, and then macOS will reopen all apps.

This information is stored in `~/Library/Preferences/ByHost/com.apple.loginwindow.<UUID>.plist`. The UUID is our Mac's UUID, which we can get by running the following command:

```
ioreg -rd1 -c IOPlatformExpertDevice | awk -F'"' '/IOPlatformUUID/{print $4}'
```

We can query the apps by either running the command:

```
defaults -currentHost read com.apple.loginwindow TALAppsToRelaunchAtLogin
(
        {
        BackgroundState = 2;
        BundleID = "com.apple.terminal";
        Hide = 0;
        Path = "/System/Applications/Utilities/Terminal.app";
    },
        {
        BackgroundState = 2;
        BundleID = "com.apple.finder";
        Hide = 0;
        Path = "/System/Library/CoreServices/Finder.app";
    },
...
```

or:

```
plutil -p ~/Library/Preferences/ByHost/com.apple.loginwindow.<UUID>.plist
{
  "TALAppsToRelaunchAtLogin" => [
    0 => {
      "BackgroundState" => 2
      "BundleID" => "com.apple.terminal"
      "Hide" => 0
      "Path" => "/System/Applications/Utilities/Terminal.app"
    }
    1 => {
      "BackgroundState" => 2
      "BundleID" => "com.apple.finder"
      "Hide" => 0
      "Path" => "/System/Library/CoreServices/Finder.app"
    }
...
```

The only thing attackers need to do is add their app to this list.