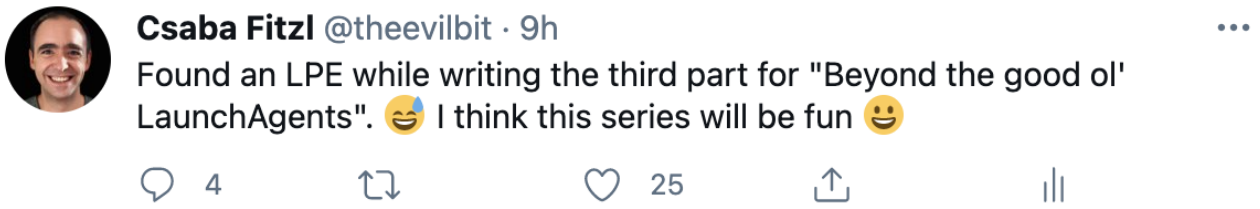
Beyond the good ol' LaunchAgents - 3 - Login Items

theevilbit.github.io/beyond/beyond_0003

March 17, 2021

> This is part 3 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.

To clear up some expectations. The below tweet is not about this method, that is deferred for now. :)

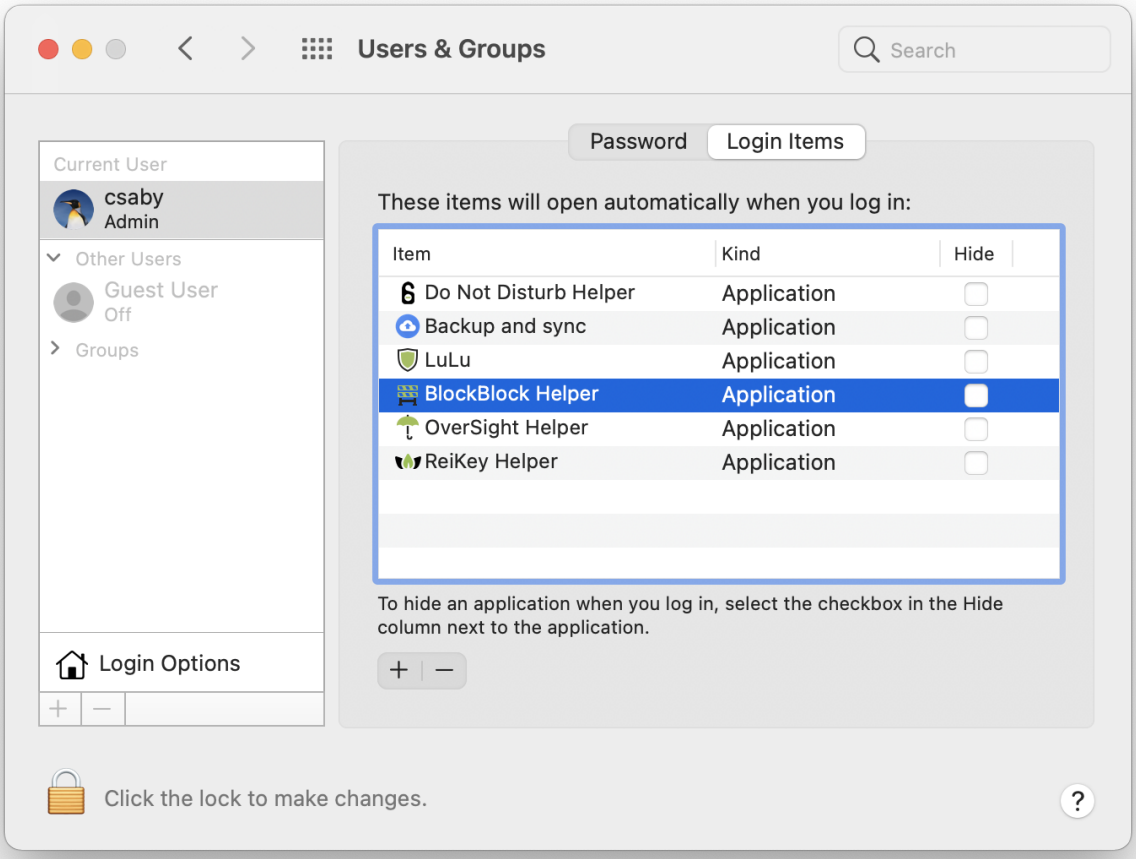


Login items are probably one of the most well documented methods to persist on macOS. It's widely used by various application to launch themselves upon user login. These applications show up in the menubar most of the time.

There are two ways of setting up Login Items.

Launch Services Framework

The first method is using the **Launch Services Framework**, to which the API reference can be found here. There was a great document, which details how to use the API. Luckily it's still available through arhive.org: Adding a preference to launch app on login using the Shared File List API – Rhult's Blog



Login Items installed via the LS framework typically show up under *System Preferences -> Users & Groups -> Login Items*. We can use this menu to either add or remove something from the list.

We can also use some scripting to get the same information.

```
csaby@mac ~ % osascript -e 'tell application "System Events" to get count of login
items'
6
csaby@mac ~ % osascript -e 'tell application "System Events" to get the name of every
login item'
Do Not Disturb Helper, Backup and sync from Google, LuLu, BlockBlock Helper,
OverSight Helper, ReiKey Helper
```

However as noted, this is not the complete picture. For example my Shield.app doesn't show up in the list. We have another framework to interact with Login Items.

Service Management Framework

The other is called the the **Service Management Framework**, and there is great documentation from Apple about how to use it. The document can be found here. If the application is sandboxed, this is the only option to install a login item, the other method won't work.

Adding and removing items can be done via a single API call, SMLoginItemSetEnabled. This is what I use for Shield at the time of this writing.

The Apple developer guide says:

> Login items installed using the Service Management framework are not visible in System Preferences and can only be removed by the application that installed them.

This confirms why Shield is not visible. This is also interesting, especially for an attacker or malware, as it doesn't leave an obvious visual trace. But we can still find these login items.

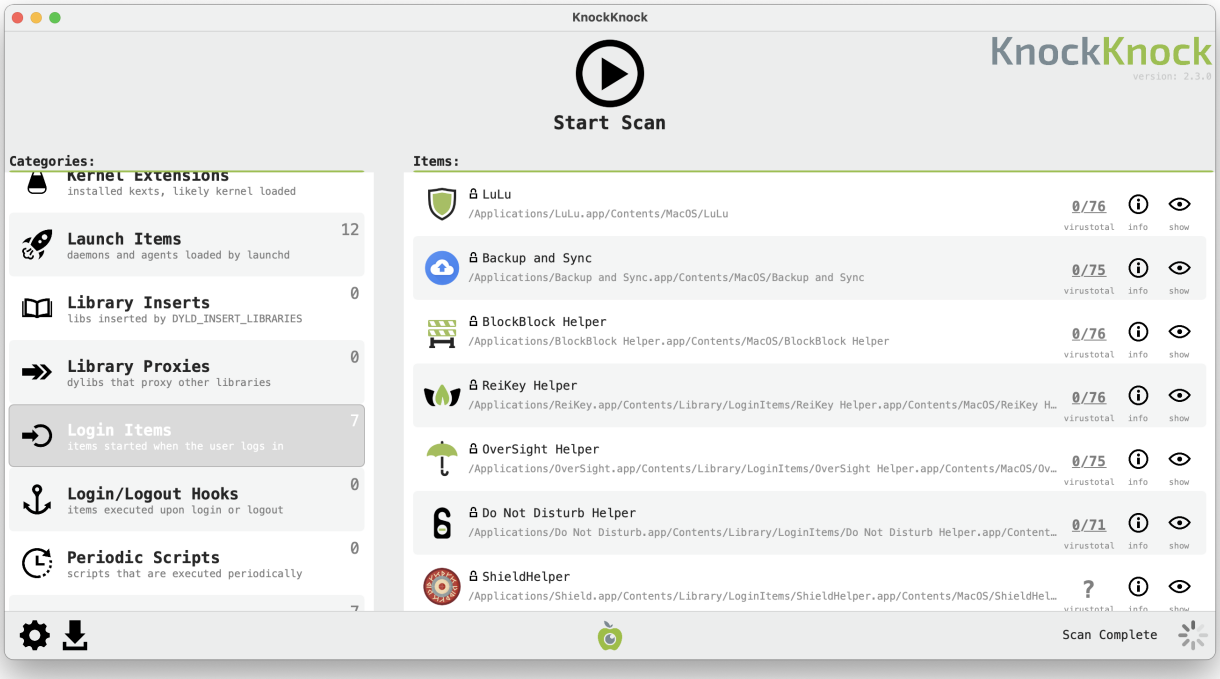
```
csaby@mac ~ % ls -l /var/db/com.apple.xpc.launchd
total 32
drwxr-xr-x  2 root  wheel   64 Jan  1  2020 config
-rw-r--r--  1 root  wheel  181 Apr 20  2020 disabled.248.plist
-rw-r--r--  1 root  wheel  907 Mar 17 06:27 disabled.501.plist
-rw-r--r--@ 1 root  wheel    0 Oct 11  2019 disabled.migrated
-rw-r--r--@ 1 root  wheel  730 Mar 17 05:59 disabled.plist
-rw-r--r--  1 root  wheel  561 Dec 16 21:39 loginitems.501.plist
```

These items will be available under `/var/db/com.apple.xpc.launchd` in the `loginitems.[userid].plist` files. Let's open `loginitems.501.plist`.

```
<?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>version.com.csaba.fitzl.shield.ShieldHelper</key>
        <string>1</string>
        <key>com.csaba.fitzl.shield.ShieldHelper</key>
        <string>com.csaba.fitzl.shield</string>
</dict>
</plist>
```

We can note, that Shield is indeed listed there.

We can also find Login Items installed via the SM framework using Objective-See's KnockKnock.



As we can see it does find all Login Items, not just those visible at *System Preferences*. Its source code is open, so you can check how it does it: KnockKnock/LoginItems.m