T1037.005 - Startup Items

Description from ATT&CK

> Adversaries may use startup items automatically executed at boot initialization to establish persistence. Startup items execute during the final phase of the boot process and contain shell scripts or other executable files along with configuration information used by the system to determine the execution order for all startup items.(Citation: Startup Items)
> This is technically a deprecated technology (superseded by Launch Daemon), and thus the appropriate folder, `/Library/StartupItems` isn't guaranteed to exist on the system by default, but does appear to exist by default on macOS Sierra. A startup item is a directory whose executable and configuration property list (plist), `StartupParameters.plist`, reside in the top-level directory.
>
> An adversary can create the appropriate folders/files in the StartupItems directory to register their own persistence mechanism.(Citation: Methods of Mac Malware Persistence) Additionally, since StartupItems run during the bootup phase of macOS, they will run as the elevated root user.

Atomic Tests

Atomic Test #1 - Add file to Local Library StartupItems

Modify or create an file in /Library/StartupItems

Reference

Supported Platforms: macOS

auto_generated_guid: 134627c3-75db-410e-bff8-7a920075f198

Attack Commands: Run with `sh`! Elevation Required (e.g. root or admin)

```
sudo touch /Library/StartupItems/EvilStartup.plist
```

Cleanup Commands:

```
sudo rm /Library/StartupItems/EvilStartup.plist
```