



Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing


🔍


Sign in

Sign up


 redcanaryco / atomic-red-team Public


 Notifications


 Fork 2.8k


 Star 9.7k


<> Code


 Issues 6


 Pull requests 5


 Actions


 Wiki


 Security


 Insights


 Files


 f339e7d





 Go to file


>  .github


>  atomic\_red\_team


>  atomics


>  Indexes


>  T1003.001


>  T1003.002


>  T1003.003


>  T1003.004


>  T1003.005


>  T1003.006


>  T1003.007


>  T1003.008


>  T1003


>  T1006


>  T1007


>  T1010


>  T1012


>  T1014


>  T1016


>  T1018


>  T1020


>  T1021.001


>  T1021.002


>  T1021.003


>  T1021.006


>  T1027.001


>  T1027.002


>  T1027.004


>  T1027


>  T1030


>  T1033


>  T1036.003



>  T1036.004

>  T1036.005

>  T1036.006

>  T1036

atomic-red-team / atomics / T1037.005 / T1037.005.md 

 Atomic Red Team doc generat... Generated docs from job=generate-d... 819934c · 2 years ago 


Preview


Code


Blame

47 lines (22 loc) · 1.88 KB

Raw







# 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This is technically a deprecated technology (superseded by [Launch Daemon](#)), and thus the appropriate folder, `/Library/StartupItems` isn't guaranteed to exist on the system by default, but does appear to exist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 Startupltems directory to register their own persistence mechanism.(Citation: Methods of Mac Malware Persistence) Additionally, since Startupltems 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 Startupltems](#)

## Atomic Test #1 - Add file to Local Library Startupltems

Modify or create an file in /Library/Startupltems

[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
```

Page 1 of 2

- >  T1037.001
- >  T1037.002
- >  T1037.004
- ▼  T1037.005
  -  T1037.005.md
  -  T1037.005.yaml

