

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 / T1569.001 / T1569.001.md

CircleCI Atomic Red Team doc... Generate docs from job=genera... 7091fa8 · 2 years ago

History

Preview

Code

Blame

50 lines (26 loc) · 1.77 KB

Raw

T1569.001 - Launchctl

Description from ATT&CK

Adversaries may abuse launchctl to execute commands or programs. Launchctl interfaces with launchd, the service management framework for macOS. Launchctl supports taking subcommands on the command-line, interactively, or even redirected from standard input.(Citation: Launchctl Man)

Adversaries use launchctl to execute commands and programs as [Launch Agents](#) or [Launch Daemons](#). Common subcommands include: `launchctl load`, `launchctl unload`, and `launchctl start`. Adversaries can use scripts or manually run the commands `launchctl load -w "%s/Library/LaunchAgents/%s"` or `/bin/launchctl load` to execute [Launch Agents](#) or [Launch Daemons](#).(Citation: Sofacy Komplex Trojan)(Citation: 20 macOS Common Tools and Techniques)

Atomic Tests

- [Atomic Test #1 - Launchctl](#)

Atomic Test #1 - Launchctl

Utilize launchctl

Supported Platforms: macOS

auto_generated_guid: 6fb61988-724e-4755-a595-07743749d4e2







Inputs:

Name	Description	Type	Default Value
executable_path	Path of the executable to run.	Path	/System/Applications/Calculator.app/Conter
label_name	Path of the executable to run.	String	evil

Attack Commands: Run with `bash` !

```
launchctl submit -l #{label_name} -- #{executable_path}
```

Page 1 of 2

- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005
- >  T1039
- >  T1040

Cleanup Commands:

```
launchctl remove #{label_name}
```

