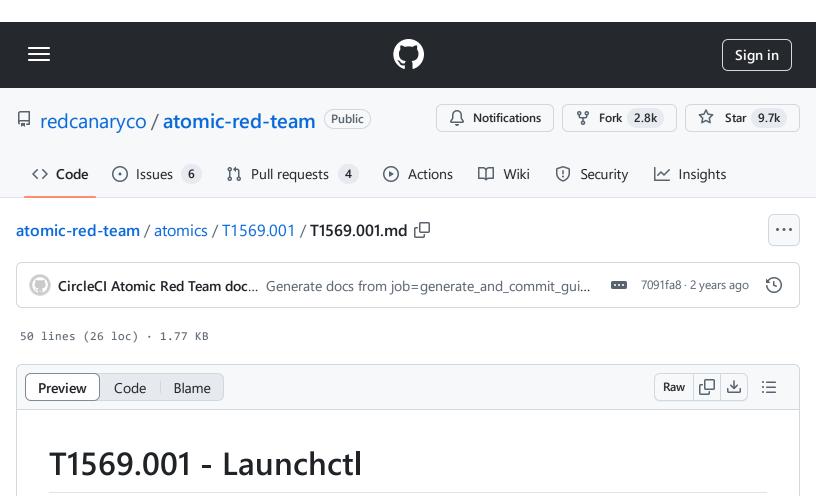
atomic-red-team/atomics/T1569.001/T1569.001.md at f339e7da7d05f6057fdfcdd3742bfcf365fee2a9 · redcanaryco/atomic-red-team · GitHub - 31/10/2024 15:12 https://github.com/redcanaryco/atomic-red-team/blob/f339e7da7d05f6057fdfcdd3742bfcf365fee2a9/atomics/T1569.001/T1569.001.md



# Description from ATT&CK

Adversaries may abuse launched to execute commands or programs. Launched interfaces with launched, the service management framework for macOS. Launched supports taking subcommands on the command-line, interactively, or even redirected from standard input. (Citation: Launched 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	Туре	Default Value
executable_path	Path of the executable to run.	Path	/System/Applications/Calculator.app/Contents/MacOS/G
label_name	Path of the executable to run.	String	evil

#### Attack Commands: Run with bash!

launchctl submit -1 #{label\_name} -- #{executable\_path}

ŗĊ

#### **Cleanup Commands:**

launchctl remove #{label\_name}

ي