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}
```

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

Cleanup Commands:

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