BROWSE

All LOOBins 53

TACTICS

Collection 11
Command and Control 4
Credential Access 6
Defense Evasion 22
Discovery 27
Execution 9
Exfiltration 3
Impact 3
Lateral Movement 2
Persistence 5
Privilege Escalation 1
Reconnaissance 4
Resource Development 1

TAGS

bash 22
clipboard 3
compress 2
configuration 6
dylib 2
files 2
gatekeeper 2
groups 2
network 5
oneliner 13
osascript 3
pbpaste 2
users 3
XCSSET 2
zsh 13

launchctl

Created by Josh Carullo

Description

launchctl can be used to load, start, stop, and unload macOS services. It is a command-line frontend to launchd.

Created	Tactics	Tags
2023-05-27	Execution Persistence	bash zsh oneliner

Paths

- `/bin/launchctl`

Use Cases

Use launchctl to execute an application

A oneliner that will load a plist as a LaunchAgent or LaunchDaemon, achieving persistence on a target machine. This command requires root privileges.

```
sudo launchctl load /Library/LaunchAgent/com.apple.installer
```

Persistent launch agent

Creation of a persistent launch agent called with $HOME/Library/LaunchAgents/com.apple.updates.plist

```
launchctl load -w ~/Library/LaunchAgents/com.apple.updates.plist
```

Detections

- LaunchAgents and LaunchDaemons must have a plist file on disk in the root, system, or user Library directory. Monitoring for plist's with executables located in /tmp or /Shared could identify suspicious applications.
- Jamf Protect: Detect launchctl activity that unloads or bootsout specific service

Resources

- 20 Common Tools & Techniques used by macOS threat Actors & Malware

- Mitre Attack Technique: launchctl T1569
- MITRE ATT&CK T1543.001 Create or Modify System Process: Launch Agent
- Komplex OS X Trojan (Sofacy)