T1546.014 - Emond

Description from ATT&CK

> Adversaries may gain persistence and elevate privileges by executing malicious content triggered by the Event Monitor Daemon (emond). Emond is a [Launch Daemon](https://attack.mitre.org/techniques/T1543/004) that accepts events from various services, runs them through a simple rules engine, and takes action. The emond binary at `/sbin/emond` will load any rules from the `/etc/emond.d/rules/` directory and take action once an explicitly defined event takes place.
> The rule files are in the plist format and define the name, event type, and action to take. Some examples of event types include system startup and user authentication. Examples of actions are to run a system command or send an email. The emond service will not launch if there is no file present in the QueueDirectories path `/private/var/db/emondClients`, specified in the Launch Daemon configuration file at `/System/Library/LaunchDaemons/com.apple.emond.plist`.(Citation: xorrior emond Jan 2018)(Citation: magnusviri emond Apr 2016)(Citation: sentinelone macos persist Jun 2019)
>
> Adversaries may abuse this service by writing a rule to execute commands when a defined event occurs, such as system start up or user authentication.(Citation: xorrior emond Jan 2018)(Citation: magnusviri emond Apr 2016)(Citation: sentinelone macos persist Jun 2019) Adversaries may also be able to escalate privileges from administrator to root as the emond service is executed with root privileges by the Launch Daemon service.

Atomic Tests

- Atomic Test #1 - Persistance with Event Monitor - emond

Atomic Test #1 - Persistance with Event Monitor - emond

Establish persistence via a rule run by OSX's emond (Event Monitor) daemon at startup, based on https://posts.specterops.io/leveraging-emond-on-macos-for-persistence-a040a2785124

Supported Platforms: macOS

auto_generated_guid: 23c9c127-322b-4c75-95ca-eff464906114

Inputs:

Name	Description	Type	Default Value

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

plist	Path to attacker emond plist file	Path	PathToAtomicsFolder/T1546.014/src/T1546.014_emon

Attack Commands: Run with `sh`! Elevation Required (e.g. root or admin)

```
sudo cp "#{plist}" /etc/emond.d/rules/T1546.014_emond.plist
sudo touch /private/var/db/emondClients/T1546.014
```

Cleanup Commands:

```
sudo rm /etc/emond.d/rules/T1546.014_emond.plist
sudo rm /private/var/db/emondClients/T1546.014
```