# TTP Detail – T1519

## TTP Information

Name: Emond

Description: Adversaries may use Event Monitor Daemon (emond) to establish persistence by scheduling malicious commands to run on predictable event triggers. Emond is a [Launch Daemon](https://attack.mitre.org/techniques/T1160) that accepts events from various services, runs them through a simple rules engine, and takes action. The emond binary at <code>/sbin/emond</code> will load any rules from the <code>/etc/emond.d/rules/</code> 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 <code>/private/var/db/emondClients</code>, specified in the [Launch Daemon](https://attack.mitre.org/techniques/T1160) configuration file at<code>/System/Library/LaunchDaemons/com.apple.emond.plist</code>.(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](https://attack.mitre.org/techniques/T1160) service.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation