Event Triggered Execution: Emond, Sub-technique T1546.014 - Enterprise

Archived: 2026-04-05 17:57:32 UTC

Adversaries may gain persistence and elevate privileges by executing malicious content triggered by the Event Monitor Daemon (emond). Emond is a Launch Daemon 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`.[1][2][3]

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.[1][2][3] 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.

Source: https://attack.mitre.org/techniques/T1546/014