# TTP Detail – T1546.017

## TTP Information

Name: Udev Rules

Description: Adversaries may maintain persistence through executing malicious content triggered using udev rules. Udev is the Linux kernel device manager that dynamically manages device nodes, handles access to pseudo-device files in the `/dev` directory, and responds to hardware events, such as when external devices like hard drives or keyboards are plugged in or removed. Udev uses rule files with `match keys` to specify the conditions a hardware event must meet and `action keys` to define the actions that should follow. Root permissions are required to create, modify, or delete rule files located in `/etc/udev/rules.d/`, `/run/udev/rules.d/`, `/usr/lib/udev/rules.d/`, `/usr/local/lib/udev/rules.d/`, and `/lib/udev/rules.d/`. Rule priority is determined by both directory and by the digit prefix in the rule filename.(Citation: Ignacio Udev research 2024)(Citation: Elastic Linux Persistence 2024)

Adversaries may abuse the udev subsystem by adding or modifying rules in udev rule files to execute malicious content. For example, an adversary may configure a rule to execute their binary each time the pseudo-device file, such as `/dev/random`, is accessed by an application. Although udev is limited to running short tasks and is restricted by systemd-udevd's sandbox (blocking network and filesystem access), attackers may use scripting commands under the action key `RUN+=` to detach and run the malicious content’s process in the background to bypass these controls.(Citation: Reichert aon sedexp 2024)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

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