# TTP Detail – T1053.006

## TTP Information

Name: Systemd Timers

Description: Adversaries may abuse systemd timers to perform task scheduling for initial or recurring execution of malicious code. Systemd timers are unit files with file extension <code>.timer</code> that control services. Timers can be set to run on a calendar event or after a time span relative to a starting point. They can be used as an alternative to [Cron](https://attack.mitre.org/techniques/T1053/003) in Linux environments.(Citation: archlinux Systemd Timers Aug 2020) Systemd timers may be activated remotely via the <code>systemctl</code> command line utility, which operates over [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: Systemd Remote Control)

Each <code>.timer</code> file must have a corresponding <code>.service</code> file with the same name, e.g., <code>example.timer</code> and <code>example.service</code>. <code>.service</code> files are [Systemd Service](https://attack.mitre.org/techniques/T1543/002) unit files that are managed by the systemd system and service manager.(Citation: Linux man-pages: systemd January 2014) Privileged timers are written to <code>/etc/systemd/system/</code> and <code>/usr/lib/systemd/system</code> while user level are written to <code>~/.config/systemd/user/</code>.

An adversary may use systemd timers to execute malicious code at system startup or on a scheduled basis for persistence.(Citation: Arch Linux Package Systemd Compromise BleepingComputer 10JUL2018)(Citation: gist Arch package compromise 10JUL2018)(Citation: acroread package compromised Arch Linux Mail 8JUL2018) Timers installed using privileged paths may be used to maintain root level persistence. Adversaries may also install user level timers to achieve user level persistence.(Citation: Falcon Sandbox smp: 28553b3a9d)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

**•** mitre-attack: persistence

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