# TTP Detail – T1501

## TTP Information

Name: Systemd Service

Description: Systemd services can be used to establish persistence on a Linux system. The systemd service manager is commonly used for managing background daemon processes (also known as services) and other system resources.(Citation: Linux man-pages: systemd January 2014)(Citation: Freedesktop.org Linux systemd 29SEP2018) Systemd is the default initialization (init) system on many Linux distributions starting with Debian 8, Ubuntu 15.04, CentOS 7, RHEL 7, Fedora 15, and replaces legacy init systems including SysVinit and Upstart while remaining backwards compatible with the aforementioned init systems.

Systemd utilizes configuration files known as service units to control how services boot and under what conditions. By default, these unit files are stored in the <code>/etc/systemd/system</code> and <code>/usr/lib/systemd/system</code> directories and have the file extension <code>.service</code>. Each service unit file may contain numerous directives that can execute system commands.

\* ExecStart, ExecStartPre, and ExecStartPost directives cover execution of commands when a services is started manually by 'systemctl' or on system start if the service is set to automatically start.
\* ExecReload directive covers when a service restarts.
\* ExecStop and ExecStopPost directives cover when a service is stopped or manually by 'systemctl'.

Adversaries have used systemd functionality to establish persistent access to victim systems by creating and/or modifying service unit files that cause systemd to execute malicious commands at recurring intervals, such as at system boot.(Citation: Anomali Rocke March 2019)(Citation: gist Arch package compromise 10JUL2018)(Citation: Arch Linux Package Systemd Compromise BleepingComputer 10JUL2018)(Citation: acroread package compromised Arch Linux Mail 8JUL2018)

While adversaries typically require root privileges to create/modify service unit files in the <code>/etc/systemd/system</code> and <code>/usr/lib/systemd/system</code> directories, low privilege users can create/modify service unit files in directories such as <code>~/.config/systemd/user/</code> to achieve user-level persistence.(Citation: Rapid7 Service Persistence 22JUNE2016)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence