# TTP Detail – T1543.005

## TTP Information

Name: Container Service

Description: Adversaries may create or modify container or container cluster management tools that run as daemons, agents, or services on individual hosts. These include software for creating and managing individual containers, such as Docker and Podman, as well as container cluster node-level agents such as kubelet. By modifying these services, an adversary may be able to achieve persistence or escalate their privileges on a host.

For example, by using the `docker run` or `podman run` command with the `restart=always` directive, a container can be configured to persistently restart on the host.(Citation: AquaSec TeamTNT 2023) A user with access to the (rootful) docker command may also be able to escalate their privileges on the host.(Citation: GTFOBins Docker)

In Kubernetes environments, DaemonSets allow an adversary to persistently [Deploy Container](https://attack.mitre.org/techniques/T1610)s on all nodes, including ones added later to the cluster.(Citation: Aquasec Kubernetes Attack 2023)(Citation: Kubernetes DaemonSet) Pods can also be deployed to specific nodes using the `nodeSelector` or `nodeName` fields in the pod spec.(Citation: Kubernetes Assigning Pods to Nodes)(Citation: AppSecco Kubernetes Namespace Breakout 2020)

Note that containers can also be configured to run as [Systemd Service](https://attack.mitre.org/techniques/T1543/002)s.(Citation: Podman Systemd)(Citation: Docker Systemd)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

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