Create or Modify System Process: Container Service, Sub-technique T1543.005 - Enterprise

Archived: 2026-04-05 15:18:39 UTC

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.[1] A user with access to the (rootful) docker command may also be able to escalate their privileges on the host.[2]

In Kubernetes environments, DaemonSets allow an adversary to persistently Deploy Containers on all nodes, including ones added later to the cluster.[3][4] Pods can also be deployed to specific nodes using the `nodeSelector` or `nodeName` fields in the pod spec.[5][6]

Note that containers can also be configured to run as Systemd Services.[7][8]

Source: https://attack.mitre.org/techniques/T1543/005