# TTP Detail – T1609

## TTP Information

Name: Container Administration Command

Description: Adversaries may abuse a container administration service to execute commands within a container. A container administration service such as the Docker daemon, the Kubernetes API server, or the kubelet may allow remote management of containers within an environment.(Citation: Docker Daemon CLI)(Citation: Kubernetes API)(Citation: Kubernetes Kubelet)

In Docker, adversaries may specify an entrypoint during container deployment that executes a script or command, or they may use a command such as <code>docker exec</code> to execute a command within a running container.(Citation: Docker Entrypoint)(Citation: Docker Exec) In Kubernetes, if an adversary has sufficient permissions, they may gain remote execution in a container in the cluster via interaction with the Kubernetes API server, the kubelet, or by running a command such as <code>kubectl exec</code>.(Citation: Kubectl Exec Get Shell)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Hildegard
* Kinsing
* Siloscape

## Tools

* Peirates

## APTs (Intrusion Sets)

* TeamTNT