# TTP Detail – T1610

## TTP Information

Name: Deploy Container

Description: Adversaries may deploy a container into an environment to facilitate execution or evade defenses. In some cases, adversaries may deploy a new container to execute processes associated with a particular image or deployment, such as processes that execute or download malware. In others, an adversary may deploy a new container configured without network rules, user limitations, etc. to bypass existing defenses within the environment. In Kubernetes environments, an adversary may attempt to deploy a privileged or vulnerable container into a specific node in order to [Escape to Host](https://attack.mitre.org/techniques/T1611) and access other containers running on the node. (Citation: AppSecco Kubernetes Namespace Breakout 2020)

Containers can be deployed by various means, such as via Docker's <code>create</code> and <code>start</code> APIs or via a web application such as the Kubernetes dashboard or Kubeflow. (Citation: Docker Containers API)(Citation: Kubernetes Dashboard)(Citation: Kubeflow Pipelines) In Kubernetes environments, containers may be deployed through workloads such as ReplicaSets or DaemonSets, which can allow containers to be deployed across multiple nodes.(Citation: Kubernetes Workload Management) Adversaries may deploy containers based on retrieved or built malicious images or from benign images that download and execute malicious payloads at runtime.(Citation: Aqua Build Images on Hosts)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: execution

## Malware

* Doki
* Kinsing

## Tools

* Peirates

## APTs (Intrusion Sets)

* TeamTNT