# TTP Detail – T1552.007

## TTP Information

Name: Container API

Description: Adversaries may gather credentials via APIs within a containers environment. APIs in these environments, such as the Docker API and Kubernetes APIs, allow a user to remotely manage their container resources and cluster components.(Citation: Docker API)(Citation: Kubernetes API)

An adversary may access the Docker API to collect logs that contain credentials to cloud, container, and various other resources in the environment.(Citation: Unit 42 Unsecured Docker Daemons) An adversary with sufficient permissions, such as via a pod's service account, may also use the Kubernetes API to retrieve credentials from the Kubernetes API server. These credentials may include those needed for Docker API authentication or secrets from Kubernetes cluster components.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Tools

* Peirates