# TTP Detail – T1612

## TTP Information

Name: Build Image on Host

Description: Adversaries may build a container image directly on a host to bypass defenses that monitor for the retrieval of malicious images from a public registry. A remote <code>build</code> request may be sent to the Docker API that includes a Dockerfile that pulls a vanilla base image, such as alpine, from a public or local registry and then builds a custom image upon it.(Citation: Docker Build Image)

An adversary may take advantage of that <code>build</code> API to build a custom image on the host that includes malware downloaded from their C2 server, and then they may utilize [Deploy Container](https://attack.mitre.org/techniques/T1610) using that custom image.(Citation: Aqua Build Images on Hosts)(Citation: Aqua Security Cloud Native Threat Report June 2021) If the base image is pulled from a public registry, defenses will likely not detect the image as malicious since it’s a vanilla image. If the base image already resides in a local registry, the pull may be considered even less suspicious since the image is already in the environment.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion