# TTP Detail – T1204.003

## TTP Information

Name: Malicious Image

Description: Adversaries may rely on a user running a malicious image to facilitate execution. Amazon Web Services (AWS) Amazon Machine Images (AMIs), Google Cloud Platform (GCP) Images, and Azure Images as well as popular container runtimes such as Docker can be backdoored. Backdoored images may be uploaded to a public repository via [Upload Malware](https://attack.mitre.org/techniques/T1608/001), and users may then download and deploy an instance or container from the image without realizing the image is malicious, thus bypassing techniques that specifically achieve Initial Access. This can lead to the execution of malicious code, such as code that executes cryptocurrency mining, in the instance or container.(Citation: Summit Route Malicious AMIs)

Adversaries may also name images a certain way to increase the chance of users mistakenly deploying an instance or container from the image (ex: [Match Legitimate Resource Name or Location](https://attack.mitre.org/techniques/T1036/005)).(Citation: Aqua Security Cloud Native Threat Report June 2021)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: execution

## APTs (Intrusion Sets)

* TeamTNT