Implant Internal Image, Technique T1525 - Enterprise

Archived: 2026-04-05 14:49:03 UTC

Adversaries may implant cloud or container images with malicious code to establish persistence after gaining access to an environment. 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 implanted or backdoored. Unlike Upload Malware, this technique focuses on adversaries implanting an image in a registry within a victim's environment. Depending on how the infrastructure is provisioned, this could provide persistent access if the infrastructure provisioning tool is instructed to always use the latest image.[1]

A tool has been developed to facilitate planting backdoors in cloud container images.[2] If an adversary has access to a compromised AWS instance, and permissions to list the available container images, they may implant a backdoor such as a Web Shell.[1]
