Pod or container name similarity

Pods that are created by controllers such as Deployment or DaemonSet have random suffix in their names. Attackers can use this fact and name their backdoor pods as they were created by the existing controllers. For example, an attacker could create a malicious pod named coredns-{random suffix} which would look related to the CoreDNS Deployment.

Info

ID: MS-TA9023
Tactic: Defense Evasion
MITRE technique: T1036.005

Also, attackers can deploy their containers in the kube-system namespace where the administrative containers reside.

Mitigations

ID	Mitigation	Description
MS-M9005.003	Gate images deployed to Kubernetes cluster	Restrict deployment of new containers from trusted supply chain