What is Kubernetes secrets enumeration?

Kubernetes secrets enumeration is listing and reading Secret objects to harvest credentials. Secrets are base64-encoded, not encrypted by default, so read access, gained through a stolen token or node identity, exposes database passwords, VPN keys, and cloud credentials that fuel lateral movement. Defend with least-privilege RBAC on secrets, encryption at rest, and external secret stores.

HOW IT WORKS

01 How it works and example

With a stolen service-account token or an impersonated node identity, the attacker lists secrets across namespaces and reads them, collecting database passwords, mesh VPN auth keys, registry credentials, and cloud keys. Each harvested secret opens another system, which is how a single foothold becomes cluster-wide and then network-wide access, as seen in recent intrusions.

SOURCES

[1] MITRE ATT&CK Cloud Matrix

[2] HuggingFace, Agent intrusion technical timeline

[3] Kubernetes: encrypting secret data at rest

Find the cloud and Kubernetes attack paths before someone else does.

securelayer7.net/learn/cloud-security/kubernetes-secrets-enumeration

Open online