Peirates, Software S0683 | MITRE ATT&CK®

Archived: 2026-04-05 13:28:24 UTC

Domain	ID	Name	Use
Enterprise	T1619	Cloud Storage Object Discovery	Peirates can list AWS S3 buckets.[1]
Enterprise	T1609	Container Administration Command	Peirates can use `kubectl` or the Kubernetes API to run commands.[1]
Enterprise	T1613	Container and Resource Discovery	Peirates can enumerate Kubernetes pods in a given namespace.[1]
Enterprise	T1530	Data from Cloud Storage	Peirates can dump the contents of AWS S3 buckets. It can also retrieve service account tokens from kOps buckets in Google Cloud Storage or S3.[1]
Enterprise	T1610	Deploy Container	Peirates can deploy a pod that mounts its node's root file system, then execute a command to create a reverse shell on the node.[1]
Enterprise	T1611	Escape to Host	Peirates can gain a reverse shell on a host node by mounting the Kubernetes hostPath.[1]
Enterprise	T1046	Network Service Discovery	Peirates can initiate a port scan against a given IP address.[1]
Enterprise	T1528	Steal Application Access Token	Peirates gathers Kubernetes service account tokens using a variety of techniques.[1]

Domain	ID		Name	Use
Enterprise	T1552	.005	Unsecured Credentials: Cloud Instance Metadata API	Peirates can query the query AWS and GCP metadata APIs for secrets.[1]
		.007	Unsecured Credentials: Container API	Peirates can query the Kubernetes API for secrets.[1]
Enterprise	T1550	.001	Use Alternate Authentication Material: Application Access Token	Peirates can use stolen service account tokens to perform its operations. It also enables adversaries to switch between valid service accounts.[1]
Enterprise	T1078	.004	Valid Accounts: Cloud Accounts	Peirates can use stolen service account tokens to perform its operations.[1]

Source: https://attack.mitre.org/software/S0683