Detection Strategy for T1528 - Steal Application Access Token, Detection Strategy DET0515

Archived: 2026-04-05 12:50:44 UTC

AN1423

Access and retrieval of container service account tokens followed by unauthorized API requests using those tokens to interact with the Kubernetes API server or internal services.

Log Sources

Data Component	Name	Channel
File Access (DC0055)	kubernetes:audit	GET or LIST requests to /var/run/secrets/kubernetes.io/serviceaccount/ followed by access to the Kubernetes API server

Mutable Elements

Field	Description
TimeWindow	Adjust based on how quickly tokens are expected to be used post-access
UserContext	Tuning for known service accounts that legitimately access the API

AN1424

Token retrieval from instance metadata endpoints such as AWS IMDS or Azure IMDS, followed by API usage using the obtained token from non-standard applications.

Log Sources

Mutable Elements

Field	Description
UserAgent	May need tuning for known automation tools versus unexpected curl usage
TimeWindow	Correlate retrieval and use of token within expected timeout window

AN1425

Unusual OAuth app registration followed by user-granted OAuth tokens and subsequent high-privilege resource access via those tokens.

Log Sources

Mutable Elements

Field	Description
ConsentScope	Tunable based on risky or privileged scopes in the environment
AppUserRatio	Threshold of how many users have authorized a given app

AN1426

Use of OAuth tokens by third-party apps to access user mail, calendar, or SharePoint resources where the token was granted recently or via spearphishing.

Log Sources

Data Component	Name	Channel
Cloud Storage Access (DC0025)	m365:unified	App-only or delegated access patterns where client_id != known enterprise apps

Mutable Elements

Field	Description
ClientAppIDAllowList	Defenders may allow known app IDs, flag unknowns
AccessVolumeThreshold	Rate of resource access by a newly consented app

AN1427

Programmatic access to user content via stolen access tokens in platforms like Slack, GitHub, Google Workspace — especially from new IPs, apps, or excessive resource access.

Log Sources

Mutable Elements

Field	Description
GeoVelocity	Flag when token use appears across geographically distant logins

Field	Description
OAuthScopeSensitivity	Weight certain scopes (admin, file.read) as higher risk

---

Source: https://attack.mitre.org/detectionstrategies/DET0515#AN1426