Suspicious Database Access and Dump Activity Across Environments (T1213.006), Detection Strategy DET0242

Archived: 2026-04-05 13:33:50 UTC

AN0676

Unusual database command-line access (e.g., `psql`, `mysql`, `mongo`) from non-admin users, occurring outside typical automation windows or without known service context. Often followed by data dumps to .sql/.csv files or outbound data transfers. Defender sees CLI tools launched interactively or by unusual parent processes, file writes to dump-like filenames, and external connections shortly after.

Log Sources

Mutable Elements

Field	Description
AllowedDBClients	List of user or automation accounts expected to use database clients
DumpFilePattern	Filename patterns used to identify data dumps (e.g., *.sql, backup_*.csv)
TimeWindow	Time threshold for correlating execution, file write, and outbound transfer

AN0677

Database client execution (e.g., sqlcmd.exe, isql.exe) by users or from locations not tied to enterprise automation or backups. Often followed by creation of .sql/.bak/.csv files, registry artifacts for ODBC/JDBC drivers, or encrypted ZIPs. Defender sees SQL tools launched by explorer.exe, Powershell, or odd parent processes, plus file writes in user temp locations.

Log Sources

Mutable Elements

Field	Description
KnownDBToolPaths	Directories where legitimate database tools are installed
ExportExtensionPatterns	List of file extensions commonly used for DB exports
MaxTransferVolume	Threshold for outbound data volume that may suggest large DB dumps

AN0678

Execution of Java-based or CLI database tools (e.g., DBeaver, Beekeeper, mysql, psql) from user profiles not tied to dev/admin roles, especially when followed by file writes and cloud sync activity. Defender correlates GUI tool launches, file write events in ~/Downloads or ~/Documents, and outbound API calls to known cloud services.

Log Sources

Mutable Elements

Field	Description
CloudSyncDomainList	FQDNs of sync services used to detect likely outbound DB leakages
UserPrivilegeLevel	Whether to treat low-privilege users accessing DB tools as higher risk

AN0679

Database enumeration and export activity (e.g., `SELECT * FROM`, `SHOW DATABASES`) issued via ephemeral VMs, admin APIs, or cloud shell from non-monitoring accounts. Defender correlates audit logs (CloudTrail, GCP Admin, AzureDiagnostics), storage write ops, and cross-region transfers by identities not tied to DB operations.

Log Sources

Mutable Elements

Field	Description
IAMAccessPatterns	Define which IAM roles/accounts are allowed DB operations
S3ExportThreshold	Size threshold (MB) or file pattern for S3-based exfil monitoring
DBQueryVerbosityThreshold	Number of rows/columns or duration to flag long-running queries

AN0680

Unusual or excessive database/table exports from SaaS database platforms (e.g., Snowflake, Firebase, BigQuery, Airtable) by users or apps not in known analytics or dev groups. Defender observes access patterns outside baseline working hours or with new query templates, and correlates those with audit logs or file downloads.

Log Sources

Data Component	Name	Channel
Application Log Content (DC0038)	saas:Snowflake	QUERY: Large or repeated SELECT * queries to sensitive tables

Data Component	Name	Channel
File Access (DC0055)	m365:unified	Bulk downloads or API extractions from Microsoft-hosted data repositories (e.g., Dynamics 365)

Mutable Elements

Field	Description
BaselineQueryTemplates	Query hash or shape for common BI/ETL jobs to reduce false positives
OffHoursAccessWindow	Window to define after-hours activity thresholds for DB access

---