Detection of Data Staging Prior to Exfiltration, Detection Strategy DET0014

Archived: 2026-04-05 14:50:54 UTC

AN0040

Detects staging of sensitive files into temporary or public directories, compression with 7zip/WinRAR, or batch copy prior to exfiltration.

Log Sources

Mutable Elements

Field	Description
StagingDirectoryList	Temp folders or user profile staging directories
CompressionToolList	7z.exe, rar.exe, zip.exe paths
TimeWindow	Temporal bounds for detecting batch staging activities

AN0041

Detects script or user activity copying files to a central temp or /mnt directory followed by archive/compression utilities.

Log Sources

Mutable Elements

Field	Description
StagingDirectoryList	e.g., /tmp/, /var/tmp/, /mnt/
ArchivingCommandPatterns	grep for 'tar', 'zip', 'gzip', '7z'
UserContext	Interactive or elevated shells running archiving commands

AN0042

Detects files collected into user temp or shared directories followed by compression with ditto, zip, or custom scripts.

Log Sources

Mutable Elements

Field	Description
CompressionUtilityList	e.g., 'ditto', 'zip', 'tar'
SharedDirectoryIndicators	e.g., /Users/Shared/ or /private/tmp/
ScriptInvocationContext	osascript or Terminal automation by non-GUI processes

AN0043

Detects virtual disk expansion or file copy operations to cloud buckets or mounted volumes from isolated instances.

Log Sources

Mutable Elements

Field	Description
CloudBucketList	Staging bucket or mount point for data
InstanceTag	Behavior restricted to specific ephemeral instances
ObjectWriteThreshold	Volume or size of files pushed in burst

AN0044

Detects snapshots or data stored in VMFS volumes from root CLI or remote agents.

Log Sources

Mutable Elements

Field	Description
SnapshotFrequency	Number of snapshots in short time period
AccessUserList	Non-admins or automation accounts writing to datastores
CLIContext	Manual or unexpected API calls triggering snapshots

---