Detection of Local Data Staging Prior to Exfiltration, Detection Strategy DET0261

Archived: 2026-04-05 17:33:04 UTC

AN0724

Detects file reads across locations followed by writes to temp or staging directories, often compressed or encrypted, indicating local staging behavior.

Log Sources

Mutable Elements

Field	Description
StagingDirList	Paths such as C:\Temp, C:\Windows\Tasks, etc.
ArchivingToolPatterns	Matches to 7z.exe, rar.exe, zip.exe, or custom scripts.
TimeWindow	How long to correlate file reads followed by compression.

AN0725

Detects aggregation of files from different directories into /tmp, /mnt, or user-specified directories with archiving tools like tar or gzip.

Log Sources

Mutable Elements

Field	Description
StagingDirs	e.g., /tmp, /var/tmp, custom user dirs
ArchiveUtilities	tar, gzip, zip, 7z
UserThreshold	Number of files or size written in short time

AN0726

Detects staged data aggregated in /Users/Shared, /private/tmp with compression tools like ditto or zip, initiated via Terminal or AppleScript.

Log Sources

Mutable Elements

Field	Description
StagingTargets	Shared dirs commonly abused for local collection
CompressionBinaries	zip, tar, ditto
TimeWindow	Seconds/minutes between source file read and output staging write

AN0727

Detects local staging behavior via snapshot creation or files written into VMFS partitions by scripts or unauthorized shell access.

Log Sources

Mutable Elements

Field	Description
SnapshotThreshold	Rapid creation or deletion of snapshots
CLIInvoker	Unexpected CLI/script invocation outside maintenance windows
VMFSWriteRate	Volume of data written locally in short time
