Detection of Remote Data Staging Prior to Exfiltration, Detection Strategy DET0071

Archived: 2026-04-05 14:46:43 UTC

AN0194

Detects file transfers or mounting operations from remote hosts followed by write actions into a local staging directory, often using SMB or remote shell activity.

Log Sources

Mutable Elements

Field	Description
StagingDirectory	Common directories such as C:\Temp, Downloads, or hidden folders used for remote staging
RemotePathPatterns	UNC paths like \\10.* or \\domain\share indicating lateral data staging
CopyToolPatterns	Usage of robocopy, xcopy, copy-item, or scheduled tasks performing cross-host copies

AN0195

Detects inbound SCP, rsync, or NFS mounts from remote systems followed by aggregation of files into known staging paths like /mnt/staging or /var/tmp.

Log Sources

Mutable Elements

Field	Description
RemoteHosts	Expected inbound transfer hosts to filter normal activity from staging behavior
MountTargets	Directory destinations used as centralized locations
TransferVolumeThreshold	Threshold of transferred files or data volume over time

AN0196

Detects rsync or scp inbound from other hosts that then aggregate content into /Users/Shared or /private/tmp, often involving compressed files or scripts.

Log Sources

Mutable Elements

Field	Description
StagingPaths	Monitored remote-to-local write destinations such as /Users/Shared
CompressionIndicators	Presence of .zip, .7z, or tar.gz indicating consolidation
TimeWindow	Temporal correlation of transfer and staging write operations

AN0197

Detects remote writes or snapshots mounted from other systems into a central ESXi VMFS path or NFS store used for remote staging of files before exfiltration.

Log Sources

Mutable Elements

Field	Description
SnapshotFrequency	How often snapshots are mounted or restored from peer nodes
RemoteWriteVolume	Threshold for staging behavior vs. backup/operational activity
StorageMountPaths	Common local destinations for incoming data

AN0198

Detects remote write activity across cloud VMs or object storage buckets within the same region/account that correlate with data aggregation across hosts.

Log Sources

Mutable Elements

Field	Description
BucketNamePatterns	Destination naming convention used for staging (e.g., temp-store)
IAMContext	IAM role or user performing multi-host write ops
TransferWindow	Burst of high-volume inter-VM transfers indicating staging

---

Source: https://attack.mitre.org/detectionstrategies/DET0071#AN0197