Detection Strategy for Exfiltration to Cloud Storage, Detection Strategy DET0570

Archived: 2026-04-05 14:59:15 UTC

AN1571

Unusual processes (e.g., powershell.exe, excel.exe) accessing large local files and subsequently initiating HTTPS POST requests to domains associated with cloud storage services (e.g., dropbox.com, drive.google.com, box.com). Defender perspective: correlation between file reads in sensitive directories and high outbound traffic volume to known storage APIs.

Log Sources

Mutable Elements

Field	Description
CloudStorageDomains	List of monitored domains for cloud services (dropbox.com, drive.google.com, onedrive.live.com).
ExfilVolumeThreshold	Data volume threshold (e.g., >10MB in single session) used to flag abnormal transfers.
UserContext	User accounts permitted to use sanctioned cloud services versus unexpected accounts.

AN1572

Processes such as curl, wget, rclone, or custom scripts executing uploads to cloud storage endpoints. Defender perspective: detect chained events where tar/gzip is executed to compress files followed by HTTPS PUT/POST requests to known storage services.

Log Sources

Mutable Elements

Field	Description
AllowedTools	Known tools used legitimately for backups (rclone, gsutil). Deviations raise suspicion.
WorkHours	Baseline normal data transfer hours to reduce false positives.

AN1573

Applications or scripts invoking cloud storage APIs (Dropbox sync, iCloud, Google Drive client) in unexpected contexts. Defender perspective: detect sensitive file reads by non-standard applications followed by unusual encrypted uploads to external cloud storage domains.

Log Sources

Mutable Elements

Field	Description
WatchedApps	Track processes that normally should not upload data (e.g., Preview, Calculator).
EntropyThreshold	High-entropy file uploads may indicate encrypted payloads designed for exfiltration.

AN1574

Unusual ESXi processes (vmx, hostd) reading datastore files and generating outbound HTTPS traffic toward external cloud storage endpoints. Defender perspective: anomalous datastore activity followed by network transfers to Dropbox, AWS S3, or other storage services.

Log Sources

Mutable Elements

Field	Description
DatastoreTransferThreshold	Threshold for outbound data exfiltration from ESXi datastore files.
ApprovedStorageServices	Whitelist of sanctioned storage providers used by admins for backup operations.
