Detection Strategy for Exfiltration Over Web Service, Detection Strategy DET0548

Archived: 2026-04-05 13:34:21 UTC

AN1511

Processes that normally do not initiate network communications suddenly making outbound HTTPS connections with high outbound-to-inbound data ratios. Defender view: correlation between process creation logs (e.g., Word, Excel, PowerShell) and subsequent anomalous network traffic volumes toward common web services (Dropbox, Google Drive, OneDrive).

Log Sources

Mutable Elements

Field	Description
MonitoredServices	List of legitimate web services to baseline (Dropbox, OneDrive, Google Drive).
ExfilVolumeThreshold	Outbound data threshold for flagging unusual activity, tunable by environment.
TimeWindow	Aggregation period to calculate anomalies in outbound data volume.

AN1512

Processes (tar, curl, python scripts) accessing large file sets and initiating outbound HTTPS POST requests with payload sizes inconsistent with baseline activity. Defender perspective: detect abnormal sequence of file archival followed by encrypted uploads to external web services.

Log Sources

Mutable Elements

Field	Description
MonitoredTools	Suspicious command-line utilities used for exfiltration (curl, wget, python).
DataVolumeThreshold	Bytes transferred threshold per session to flag unusual uploads.

AN1513

Office apps or scripts writing files followed by xattr manipulation (to evade quarantine) and subsequent HTTPS uploads. Defender perspective: anomalous file modification + outbound TLS traffic originating from non-networking apps (Word, Excel, Preview).

Log Sources

Mutable Elements

Field	Description
WatchedApplications	Applications not expected to perform bulk data transfers (Office apps, Preview).

AN1514

Abnormal API calls from user accounts invoking file upload endpoints outside normal baselines (M365, Google Drive, Box). Defender perspective: monitor unified audit logs for elevated frequency of Upload, Create, or Copy operations from compromised accounts.

Log Sources

Mutable Elements

Field	Description
APICallThreshold	Maximum number of API calls per user/session before triggering alert.
UserBaselineProfiles	Baseline normal data transfer patterns by user/role.

AN1515

ESXi guest OS or management interface processes establishing unexpected external HTTPS connections. Defender perspective: monitor vmx or hostd processes making outbound web requests with significant data transfer.

Log Sources

Mutable Elements

Field	Description
DatastoreTransferThreshold	Threshold for outbound transfers from ESXi datastores.
