Detection of Tainted Content Written to Shared Storage, Detection Strategy DET0471

Archived: 2026-04-02 11:21:35 UTC

AN1298

Detects adversary tampering of shared directories via file drops (e.g., malicious LNK, EXE, VBS) followed by user execution or suspicious network activity.

Log Sources

Mutable Elements

Field	Description
SharedPathPrefix	Defines monitored shared directories (e.g., \\server\HR\).
ExecutableExtensions	Monitored file types dropped in shared paths (e.g., .lnk, .exe, .vbs).

AN1299

Detects script or binary modification within shared NFS/SMB directories followed by process execution from those paths.

Log Sources

Mutable Elements

Field	Description
MountPath	Mount path of monitored shared volumes (e.g., /mnt/shared).
FilenamePattern	Pattern matching of abnormal or disguised filenames.

AN1300

Detects modification of shared network folders via .app bundles or scripting files with hidden extensions (e.g., double extensions like docx.app).

Log Sources

Mutable Elements

Field	Description
FileExtensionDeception	Monitors use of hidden extensions or double extensions.
TargetSharedFolder	Defines sensitive shared folders (e.g., /Users/Shared/HR).

AN1301

Detects upload of malicious or unusual file types into cloud-shared folders, followed by user downloads or interactions.

Log Sources

Mutable Elements

Field	Description
UserUploadRateThreshold	Abnormal upload patterns into shared drives.
MaliciousFileIndicator	File hash or known-bad filename pattern matching.

AN1302

Detects embedded macros or scripts added to shared documents or use of external references to execute code.

Log Sources

Mutable Elements

Field	Description
MacroExecutionPolicy	Controls macro execution based on user or group policy.
SuspiciousKeywordMatch	Regex match on suspicious VBA function names or calls.
