Behavioral Detection of Obfuscated Files or Information, Detection Strategy DET0378

Archived: 2026-04-05 16:33:15 UTC

AN1064

Correlates script execution or suspicious parent processes with creation or modification of encoded, compressed, or encrypted file formats (e.g., .zip, .7z, .enc) and abnormal command-line syntax or PowerShell obfuscation.

Log Sources

Mutable Elements

Field	Description
PayloadEntropyThreshold	Tune entropy threshold to distinguish obfuscation from legitimate compression
TimeWindow	Adjust correlation window between script execution and encoded file creation
SuspiciousParentProcessList	Customize based on environment to include LOLBins or admin tools misused for obfuscation

AN1065

Detects use of gzip, base64, tar, or openssl in scripts or commands that encode/encrypt files after file staging or system enumeration.

Log Sources

Mutable Elements

Field	Description
CommandRegex	Customize for tools seen in environment (e.g., gzip, bzip2, xz)
SensitivePathList	Specify file paths likely targeted for obfuscation (e.g., /etc/, /home/)

AN1066

Monitors use of archive or encryption tools (zip, openssl) tied to user-scripted activity or binaries writing encoded payloads under /Users or /Volumes.

Log Sources

Mutable Elements

Field	Description
FilenameExtensionList	Tunable to identify uncommon or encrypted file formats (e.g., .enc, .b64, .xz)
UserContext	Tune to prioritize unexpected file access by service accounts

AN1067

Identifies transfer of base64, uuencoded, or high-entropy files over HTTP, FTP, or custom protocols in lateral movement or exfiltration streams.

Log Sources

Mutable Elements

Field	Description
EntropyThreshold	Adjust threshold to reduce false positives in compressed but benign data
ProtocolScope	Refine by enabling inspection of specific exfil vectors (e.g., FTP, HTTP POST)

AN1068

Detects encoded PowerCLI or Base64-encoded payloads staged via datastore uploads or shell access (e.g., ESXi Shell or backdoored VIBs).

Log Sources

Mutable Elements

Field	Description
StagingLocation	Tune based on observed adversary paths (e.g., /vmfs/volumes/...)
EncodedLengthThreshold	Tune length of encoded payloads before triggering detection

---