Detect Archiving via Custom Method (T1560.003), Detection Strategy DET0438

Archived: 2026-04-02 11:40:17 UTC

AN1213

Detects suspicious custom compression/encryption routines through anomalous script or binary execution that produces high-entropy files without standard archiving utilities. Correlates script execution, memory API usage (bitwise ops, CryptoAPI calls), and creation of archive-like files with uncommon headers.

Log Sources

Mutable Elements

Field	Description
EntropyThreshold	Minimum entropy level that flags suspicious custom archives.
AllowedProcesses	Known business processes performing encryption or compression.
TimeWindow	Correlation timeframe between script execution and file creation.

AN1214

Detects custom archive routines by correlating script execution (Python, Perl, Bash) with creation of high-entropy files in temporary or user directories. Flags processes performing unusual bitwise operations or writing files without standard compression headers.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	auditd:SYSCALL	execve: Execution of interpreters creating archive-like outputs without calling tar/gzip
File Creation (DC0039)	auditd:FILE	create: Creation of files with anomalous headers and entropy levels in /tmp or user directories
Process Modification (DC0020)	linux:osquery	Detection of bitwise operations or custom encryption functions in memory traces

Mutable Elements

Field	Description
ArchivePaths	Directories monitored for anomalous archive creation (e.g., /tmp, /home).
EntropyThreshold	Entropy score to flag files lacking recognizable compression headers.
ScriptAllowlist	Scripts/processes known to use custom compression methods.

AN1215

Detects custom archiving by monitoring execution of Swift/Objective-C apps or scripts producing high-entropy files with non-standard headers. Correlates unified logs of abnormal NSFileHandle/NSData operations, memory use of XOR/bitwise operations, and file creation events.

Log Sources

Mutable Elements

Field	Description
UserContext	Flag if archiving occurs under privileged/system accounts.
EntropyThreshold	Entropy score cutoff for identifying custom compressed or encrypted files.
AllowedApps	Applications legitimately using custom archiving for business purposes.
