Detect Archiving via Utility (T1560.001), Detection Strategy DET0298

Archived: 2026-04-05 13:54:38 UTC

AN0831

Detects adversarial archiving using built-in or third-party utilities (makecab, diantz, xcopy, certutil, 7z, WinRAR, WinZip). Correlates suspicious process creation events with command-line arguments for compression/encoding, followed by creation of archive files (.cab, .zip, .7z, .rar). Identifies anomalous loading of crypt32.dll for encryption operations or execution of diantz.exe to compress remotely staged files.

Log Sources

Mutable Elements

Field	Description
SuspiciousExtensions	List of archive extensions considered high risk (.cab, .zip, .7z, .rar).
ProcessAllowlist	Known business utilities allowed to create archives without alerting.
FileSizeThresholdMB	Minimum archive size threshold to filter out benign small compressions.

AN0832

Detects execution of archiving utilities (tar, gzip, bzip2, xz, zip, openssl) followed by suspicious archive file creation. Correlates archive creation in temporary or staging directories with execution of commands involving compression or encryption options.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	auditd:SYSCALL	execve: Execution of tar, gzip, bzip2, xz, zip, or openssl with compression/encryption arguments
File Creation (DC0039)	auditd:FILE	create: Creation of archive files in /tmp, /var/tmp, or user home directories

Mutable Elements

Field	Description
ArchiveCommands	List of archiving utilities considered suspicious.
MonitoredDirectories	Paths where archive creation is flagged as unusual (e.g., /tmp, /var/tmp).
TimeWindow	Correlation window for linking utility execution with archive creation.

AN0833

Detects invocation of macOS-native archiving utilities (zip, ditto, hdiutil) or openssl used for encryption. Correlates execution with archive or encrypted file creation (.zip, .dmg, .tar.gz) in user or temporary directories. Identifies anomalous use of archiving commands by Office applications or daemons.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	Execution of zip, ditto, hdiutil, or openssl by processes not normally associated with archiving
File Creation (DC0039)	macos:unifiedlog	Creation of .zip, .dmg, .tar.gz files in /Users, /tmp, or application directories

Mutable Elements

Field	Description
AllowedArchivers	Business-approved applications permitted to create archives (e.g., backup agents).
UserContext	Flag archiving under privileged or service accounts as higher risk.
PayloadEntropyThreshold	Entropy threshold for detecting encrypted archives versus normal compression.
