Detect Archiving via Library (T1560.002), Detection Strategy DET0268

Archived: 2026-04-05 14:33:25 UTC

AN0747

Detects adversarial archiving using libraries (zlib, zip APIs) invoked by scripts or binaries. Correlates process executions of Python, PowerShell, or custom .NET binaries with DLL/module loads linked to compression libraries, followed by archive file creation.

Log Sources

Mutable Elements

Field	Description
LibraryAllowlist	Known business applications using compression libraries.
SuspiciousExtensions	Archive extensions considered sensitive in monitored environments.
TimeWindow	Correlation window between script/library invocation and file creation.

AN0748

Detects adversarial archiving by scripts or binaries calling compression libraries (libzip, zlib, bzip2). Correlates execution of Python, Perl, or compiled binaries with dynamic linking to archiving libraries and creation of compressed files in /tmp or user directories.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	auditd:SYSCALL	execve: Execution of python, perl, or custom binaries invoking compression libraries
Module Load (DC0016)	auditd:MMAP	load: Loading of libzip.so, libz.so, or libbz2.so by processes not normally associated with archiving
File Creation (DC0039)	auditd:FILE	create: Creation of .zip, .gz, .bz2 files in /tmp, /var/tmp, or /home directories

Mutable Elements

Field	Description
MonitoredLibraries	List of shared objects linked to compression/encryption.
ArchivePaths	Directories where archive creation is flagged as anomalous.
EntropyThreshold	Entropy level used to distinguish encryption from normal compression.

AN0749

Detects malicious archiving via system or third-party libraries (libz, libarchive) invoked by Python, Swift, or Objective-C binaries. Correlates unified logs of library loads with creation of compressed or encrypted archives (.zip, .gz, .bz2, .dmg).

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	Execution of Python, Swift, or other binaries invoking archiving libraries
Module Load (DC0016)	macos:unifiedlog	Loading of libz.dylib, libarchive.dylib by non-standard applications
File Creation (DC0039)	macos:unifiedlog	Creation of .zip, .gz, .dmg archives in /Users, /tmp, or application directories

Mutable Elements

Field	Description
AllowedProcesses	Applications allowed to load compression libraries (e.g., backup agents).
UserContext	Flag archiving under privileged or system accounts as suspicious.
FileExtensionFilter	Targeted monitoring of sensitive file formats or compressed containers.
