

Detect Archiving and Encryption of Collected Data (T1560), Detection Strategy DET0526

Archived: 2026-04-05 16:30:56 UTC

AN1458

Detects adversarial archiving of files prior to exfiltration by correlating execution of compression/encryption utilities (e.g., makecab.exe, rar.exe, 7z.exe, powershell Compress-Archive) with subsequent creation of large compressed or encrypted files. Identifies abnormal process lineage involving crypt32.dll usage, command-line arguments invoking compression switches, and file write operations to temporary or staging directories.

Log Sources

Mutable Elements

| Field | Description |
|---------------------|---|
| ArchiveExtensions | List of file extensions treated as suspicious when created outside of expected paths. |
| ProcessAllowlist | Known business processes permitted to use compression/encryption utilities. |
| FileSizeThresholdMB | Minimum file size for flagging archive creation to reduce noise from benign small compressions. |

AN1459

Detects adversarial archiving activity through invocation of utilities like tar, gzip, bzip2, or openssl used in non-administrative or unusual contexts. Correlates command execution patterns with file creation of compressed/encrypted outputs in staging directories (e.g., /tmp, /var/tmp).

Log Sources

| Data Component | Name | Channel |
|--|----------------|---|
| Command Execution (DC0064) | auditd:SYSCALL | execve: Execution of tar, gzip, bzip2, or openssl with output redirection |
| File Creation (DC0039) | auditd:FILE | create: Creation of files ending in .tar, .gz, .bz2, .zip in /tmp or /var/tmp |

Mutable Elements

| Field | Description |
|-----------------------|---|
| ArchiveCommands | List of archiving/encryption utilities considered sensitive in the monitored environment. |
| SuspiciousDirectories | Paths where archive creation is suspicious (e.g., /tmp, user home directories). |
| TimeWindow | Temporal window to correlate command execution with file creation events. |

AN1460

Detects use of macOS-native archiving or encryption tools (zip, ditto, hdiutil) for staging collected data. Identifies unexpected invocation of archive utilities by Office apps, browsers, or background daemons. Correlates file creation of .zip/.dmg containers with process lineage anomalies.

Log Sources

| Data Component | Name | Channel |
|---|------------------|---|
| Process Creation (DC0032) | macos:unifiedlog | Execution of zip, ditto, hdiutil, or openssl by non-terminal parent processes |
| File Creation (DC0039) | macos:unifiedlog | Creation of .zip or .dmg files in user-accessible or temporary directories |

Mutable Elements

| Field | Description |
|-------------------------|--|
| AllowedArchiveUtilities | Business-approved applications (e.g., Time Machine, backup agents) that generate archives. |
| UserContext | Threshold for flagging archive creation under privileged or service accounts. |
| PayloadEntropyThreshold | Entropy threshold for detecting encrypted archives versus standard compressed files. |

Source: <https://attack.mitre.org/detectionstrategies/DET0526#AN1460>