# Detection Strategy for Compressed Payload Creation and Execution, Detection Strategy DET0281

Archived: 2026-04-05 17:39:18 UTC

### AN0782

Monitors for compression tool usage (e.g., 7zip, WinRAR, MakeCab) that follows or precedes file modification, suspicious file types (e.g., .exe, .dll) being compressed, or dropped from self-extracting archives followed by immediate execution.

#### Log Sources

#### Mutable Elements

| Field | Description |
|---|---|
| CompressedFileType | Zip, .rar, .cab, .gz – tune based on expected legitimate use of compression in environment |
| SFXExecutionDelay | Expected time between archive unpacking and first execution – short delays are suspicious |
| UserContext | Restrict detection to non-admin or interactive users if excessive FPs from sys admin activity |

### AN0783

Detects sequential command-line compression utilities (e.g., gzip, tar, zip, 7z) followed by execution of unpacked files, especially in temp directories or under non-standard locations like /dev/shm or /tmp with ELF binaries.

#### Log Sources

#### Mutable Elements

| Field | Description |
|---|---|
| PathRegex | Flag compressed archives extracted to /tmp, /dev/shm, or user’s home dir |
| CompressionToolPatterns | gzip, tar, bzip2, xz, 7z – tune to suppress admin packaging workflows |
| ExecutionAfterUnpackWindow | How soon a new file is executed after it’s unpacked |

### AN0784

Identifies archive utilities (e.g., ditto, unzip, xar, pkgutil) used to extract payloads to non-standard paths, then correlates with execution or file permission changes (e.g., `chmod +x`) and process spawns from decompressed location.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| DecompressionPathMatch | Target unusual extraction paths (~/Library/, /tmp/, /private/tmp/) |
| ToolBinaryNames | List of decompression utilities used in the environment |
| FollowOnExecutionDelta | Time between decompression and first binary execution |

---