Detection Strategy for Masquerading via File Type Modification, Detection Strategy DET0226

Archived: 2026-04-05 17:39:38 UTC

AN0630

Detects behavior where files with non-executable or misleading extensions (e.g., .jpg, .txt) are created or modified but subsequently executed as binaries based on internal file headers or abnormal parent process lineage. This includes identifying polyglot files or malformed magic bytes indicative of masquerading attempts.

Log Sources

Mutable Elements

Field	Description
benign_extensions	List of non-executable file types commonly used to mask payloads (.jpg, .txt, .gif)
monitored_directories	Targeted directories for initial access and downloads (e.g., %TEMP%, Downloads, AppData)
MagicByteMismatchThreshold	Detection tolerance for mismatches between extension and file signature (magic bytes)
TimeWindow	Time range between file creation and first execution
ParentProcessAnomalyScore	Anomaly score threshold for suspicious parent-child process combinations

AN0631

Detects when a script or binary is named with misleading or benign-looking extensions (.jpg, .doc) and is then executed via command line or a scheduled task. Includes ELF header mismatches and content-type inconsistencies on disk.

Log Sources

Mutable Elements

Field	Description
benign_extensions	Linux-targeted masquerade extensions (.jpg, .pdf, .png)

Field	Description
HeaderInspectionEnabled	Whether to parse file signatures or MIME types from file headers
ExecPathScope	Monitored directory scope for adversarial execution (e.g., /tmp/, /home/username/Downloads)

AN0632

Detects binaries disguised as media or document types through extension-only masquerading or by modifying the file signature. Observes execution of files whose extension is not typically executable (.jpg, .txt), yet have valid Mach-O headers or execute via Terminal or launch services.

Log Sources

Mutable Elements

Field	Description
LaunchAgentScope	Scope of services monitored for unusual launches (e.g., Finder, Terminal, Preview)
SignatureEnforcementLevel	How strictly the detection checks header validity vs. file extension
TimeWindow	Time range for linking file modification and execution events

---