Detection Strategy for Embedded Payloads, Detection Strategy DET0214

Archived: 2026-04-05 13:32:47 UTC

AN0599

Detection of executables or scripts containing hidden embedded resources or secondary payloads, often with anomalies in file size vs. functionality or dropped child binaries.

Log Sources

Mutable Elements

Field	Description
OverlaySizeThreshold	Threshold in bytes where appended sections to binaries are considered suspicious
ProcessTreeDepth	Controls how far child process lineage is analyzed for dropped embedded payloads
TimeWindow	Defines correlation interval between file write and process execution

AN0600

Detection of shell scripts, ELF binaries, or archives containing embedded secondary payloads, self-extracting components, or unusual compression behavior during runtime.

Log Sources

Mutable Elements

Field	Description
FileSectionCount	Tuning value for ELF binaries with appended sections or resources
ScriptLength	Threshold for long shell scripts with base64-encoded binary content
ExtractedFileCount	Number of files written from a single script execution

AN0601

Detection of Mach-O binaries or AppleScripts that contain nested, encoded, or run-only embedded payloads dropped at runtime.

Log Sources

Mutable Elements

Field	Description
ScriptFormatType	Run-only AppleScripts or signed scripting payloads may require scoped detection
DroppedBinaryCount	Threshold on number of binaries created by the parent payload
ParentProcessName	Allows focusing on suspicious interpreter or staging tools

---