Detection Strategy for Polymorphic Code Mutation and Execution, Detection Strategy DET0324

Archived: 2026-04-05 13:14:12 UTC

AN0919

Identifies self-modifying executables that exhibit changes in binary hash, entropy, or memory sections during or between executions—often tied to dynamic unpacking or decryption behaviors.

Log Sources

Mutable Elements

Field	Description
EntropyThreshold	Tune based on expected baseline entropy for executables; higher values may indicate polymorphic packing.
TimeWindow	Correlate rapid process spawn + image load activity suggesting mutation engine usage.
ParentProcessPatterns	Define expected or suspicious parent-child chains (e.g., script runner -> encoded PE)

AN0920

Detects files or processes where execution results in frequent re-creation or modification of ELF binaries or interpreter scripts, often using chmod + execve with abnormal entropy.

Log Sources

Mutable Elements

Field	Description
WriteExecThreshold	Tune to alert on write followed by chmod + exec in quick succession.
FileEntropyDeviation	Detect high deviation from average entropy score of baseline ELF/script files.
ExecutionFrequency	Abnormal burst executions of file with identical functionality but varying hash.

AN0921

Tracks modification of executables or interpreter payloads (e.g., Mach-O, dylib) that mutate across runs—using scripting engines, JIT compilers, or side-loaded plugins.

Log Sources

Mutable Elements

Field	Description
ScriptEnginePatterns	Detection may vary based on whether Python/Swift/AppleScript is used to mutate payloads.
MachOEntropyThreshold	Entropy tuning based on expected baseline for system vs user binaries.
SignedBinaryChangeRate	Helps flag apps that change but maintain signed status across invocations.

Source: https://attack.mitre.org/detectionstrategies/DET0324#AN0921