Detection Strategy for Junk Code Obfuscation with Suspicious Execution Patterns, Detection Strategy DET0322

Archived: 2026-04-02 10:53:21 UTC

AN0913

Detects the presence of executables with high NOP padding, unusually large binary size for their function, and follow-on execution or memory injection from such files, especially when originating from temp or user-space paths.

Log Sources

Mutable Elements

Field	Description
NOPThreshold	High proportion of 0x90 opcodes indicating junk code – tune to suppress noise from some packing tools
ExecutableSizeThreshold	Size range for abnormally large binaries relative to their runtime behavior
TimeWindow	Window between file creation and execution – short intervals may indicate staged payload execution

AN0914

Detects ELF binaries written to disk that demonstrate anomalous file size or entropy, quickly followed by execution or memory region writes into remote processes (e.g., using ptrace).

Log Sources

Mutable Elements

Field	Description
BinarySizeThreshold	Used to flag binaries much larger than typical shell utilities or payloads
MemoryWriteTargets	Which processes are allowed ptrace/mprotect – can limit to suspicious child-to-parent targeting
ExecutionAfterWriteWindow	Temporal threshold for file write to execution

AN0915

Identifies Mach-O binaries dropped into temporary directories with abnormally high binary size or padding patterns, followed by privilege escalation, `exec`, or memory mapping of other processes.

Log Sources

Mutable Elements

Field	Description
TempFilePaths	Track dropped executables in ~/Library/, /tmp/, or /private/tmp/
MachOPaddingThreshold	Define padding size or section entropy anomalies in Mach-O file format
FollowOnPrivilegeEscalation	Detects whether the binary attempts privilege escalation within short execution window

---