Detection Strategy for Stripped Payloads Across Platforms, Detection Strategy DET0019

Archived: 2026-04-05 13:10:23 UTC

AN0055

Executable or script payloads lacking symbol information and readable strings that are created or dropped by unusual or short-lived processes.

Log Sources

Mutable Elements

Field	Description
EntropyThreshold	Payloads with extremely low string entropy may indicate stripped or obfuscated binaries
ParentProcessName	Used to scope or whitelist common system builders, compilers, or admin tools
TimeWindow	Correlates file creation and process spawning within a short timeframe

AN0056

Executable or binary files created without symbol tables or with stripped sections, especially by non-user shell processes or compilers invoked outside standard dev paths.

Log Sources

Mutable Elements

Field	Description
StripFlags	Flag combinations in compiled binaries indicating symbol table removal
DirectoryScope	Whitelist compiler output directories to reduce false positives
FileSizeRange	Heuristic boundaries for abnormal small or overly large stripped binaries

AN0057

Creation of run-only AppleScripts or Mach-O binaries lacking symbol table and string references, especially when dropped by user space scripting engines or staging apps.

Log Sources

Mutable Elements

Field	Description
RunOnlyFlag	AppleScript flag to disable reverse engineering (run-only compiled scripts)
ParentProcess	Filter to isolate staging or suspicious scripting engines
SignedStatus	Tuning based on unsigned vs. developer-signed payloads

AN0058

Inbound binary payloads transferred over HTTP/S with compressed or encoded headers, lacking signature markers or metadata indicative of compiler/toolchain.

Log Sources

Mutable Elements

Field	Description
MIMEType	Tune for octet-stream or mismatched Content-Type headers
PayloadSize	Payload threshold for executable-sized artifacts
TransferEncoding	Suspicious base64 or chunked encoding not matching normal app behavior

---