Detection Strategy for Command Obfuscation, Detection Strategy DET0505

Archived: 2026-04-05 15:00:50 UTC

AN1394

Detection of command-line activity exhibiting syntactic obfuscation patterns, such as excessive escape characters, base64 encoding, command concatenation, or outlier command length and entropy.

Log Sources

Mutable Elements

Field	Description
CommandLineEntropyThreshold	Used to flag base64 or token-heavy command-line strings
SuspiciousCharacterCount	Escape character and symbol frequency in command-line strings
TimeWindow	Window between command execution and follow-up child or file write behavior

AN1395

Detection of shell commands that leverage encoded execution, command chaining, excessive piping, or unusual token patterns indicative of obfuscation.

Log Sources

Mutable Elements

Field	Description
CommandLineTokenCount	Tuning value for token or argument count in shell invocations
EncodedExecRegex	Environment-specific regex patterns for encoded or eval'd command lines
GlobPatternAnomalies	Shell-specific globbing or directory traversal string detection

AN1396

Detection of obfuscated commands via shell, osascript, or AppleScript interpreters using unusual tokens, encoding, variable substitution, or runtime string reconstruction.

Log Sources

Mutable Elements

Field	Description
InterpreterParentFilter	Limits detection scope to shell or scripting interpreters like zsh, bash, osascript
ScriptEntropyThreshold	Minimum entropy required to consider the command or script obfuscated
ArgumentLengthDeviation	Deviation from baseline for long or highly nested arguments

---