Detect Time-Based Evasion via Sleep, Timer Loops, and Delayed Execution, Detection Strategy DET0141

Archived: 2026-04-05 17:54:23 UTC

AN0396

Process creation involving suspicious delays (e.g., Sleep, ping -n loops, WaitForSingleObject), followed by sensitive system access or lateral movement behaviors.

Log Sources

Mutable Elements

Field	Description
SleepDurationThreshold	Defines maximum allowable sleep duration in milliseconds before triggering anomaly detection.
TimeBetweenExecutionAndNextStage	Temporal window between initial process and next stage (e.g., lateral movement or persistence), used to correlate dormant activity.
UserContext	Whether the activity occurs in SYSTEM or user context may affect legitimacy scoring.

AN0397

Script-based execution of sleep loops or time delay commands (e.g., sleep, ping delay, while-loops) followed by file creation or network connections.

Log Sources

Mutable Elements

Field	Description
SleepLoopCount	Defines how many loop iterations or sleep cycles are considered anomalous in the monitored environment.
ExecutionScriptType	Identifies which scripting interpreter is used (e.g., bash, python, perl) to adjust detection logic.

AN0398

Use of `usleep`, `nanosleep`, or `NSTimer` calls in executables or binaries with no GUI interaction, especially followed by disk/network activity.

Log Sources

Mutable Elements

Field	Description
AppBundleIdentifier	Correlate with known/expected signed apps vs. unsigned binaries to reduce noise.
TimeToNextEvent	Minimum time expected between process start and observable I/O for normal apps.

Source: https://attack.mitre.org/detectionstrategies/DET0141#AN0396