Multi-Platform Detection Strategy for T1678 - Delay Execution, Detection Strategy DET0372

Archived: 2026-04-05 12:49:01 UTC

AN1048

Correlated use of sleep/delay mechanisms (e.g., kernel32!Sleep, NTDLL APIs) in short-lived processes, combined with parent processes invoking suspicious scripts (e.g., wscript, powershell) with minimal user interaction.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Delay duration that distinguishes benign scripts from evasive behavior.
ParentProcessName	Legitimate parent-child combinations may differ across environments.
SleepFunctionPattern	Different APIs may be used to invoke sleep (e.g., Sleep, NtDelayExecution).

AN1049

Shell scripts or binaries invoking repeated 'sleep', 'ping', or low-level syscalls (e.g., nanosleep) in short-lived execution chains with no user or system interaction. Frequently seen in malicious cron jobs or payload stagers.

Log Sources

Mutable Elements

Field	Description
CommandLineRegex	Environment-specific delay scripts may vary (sleep 300, ping -n 60, etc.).
TimeBetweenSyscalls	Threshold for determining if delay is artificially extended.
UserContext	Root vs. service user context alters risk profile.

AN1050

Execution of AppleScript, bash, or launchd jobs that invoke delay functions (e.g., sleep, delay in AppleScript) with limited parent interaction and staged follow-on commands.

Log Sources

Mutable Elements

Field	Description
ScriptPattern	AppleScript vs shell scripts differ per threat and org.
UserContext	Execution under user vs daemon context changes severity.
DelayDurationThreshold	Amount of delay that distinguishes benign usage vs evasion.
