Behavior-chain, platform-aware detection strategy for T1124 System Time Discovery, Detection Strategy DET0151

Archived: 2026-04-05 13:26:45 UTC

AN0430

Untrusted or unusual process/script (cmd.exe, powershell.exe, w32tm.exe, net.exe, custom binaries) queries system time/timezone (e.g., w32tm /tz, net time \host, Get-TimeZone, GetTickCount API) and (optionally) is followed within a short window by time-based scheduling or conditional execution (e.g., schtasks /create, at.exe, PowerShell Start-Sleep with large values).

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation window (e.g., 5–15 minutes) between time discovery and follow-on scheduling/conditional actions.
AllowedParents	Legitimate parent processes (e.g., corporate scripts, management agents) that frequently call time APIs.
CommandlineKeywordList	Extend/restrict keyword list for time queries (e.g., custom PS functions, .NET calls).
UserContextScope	Restrict to non-service, non-administrative, or newly created/rare users.
ProcessPrevalenceThreshold	Frequency threshold to exclude common estate-wide benign usage.

AN0431

A process (often spawned by a shell, interpreter, or malware implant) executes time discovery via commands (date, timedatectl, hwclock, cat /etc/timezone, /proc/uptime) or direct syscalls (time(), clock_gettime) and is (optionally) followed by scheduled task creation/modification (crontab, at) or conditional sleep logic.

Log Sources

Mutable Elements

Field	Description
AuditRulesSyscalls	Scope of syscalls (time, clock_gettime, gettimeofday) monitored; may be performance-sensitive.
AllowedBinaries	List of legitimate automation/orchestration tools frequently querying time.
TimeWindow	Correlation window (e.g., 5–20 minutes) to link time discovery to follow-on cron/at changes.
UserContextScope	Ignore root-owned maintenance agents if desired; focus on interactive or newly created users.

AN0432

Process/script execution of systemsetup -gettimezone, date, ioreg, or API usage (timeIntervalSinceNow, gettimeofday) followed by time-based scheduling (launchd plist modification) or sleep-based execution.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	process exec events of systemsetup, date, ioreg with command_line parameters indicating time discovery
Scheduled Job Metadata (DC0005)	macos:unifiedlog	New/modified launchd plist (persistence/scheduling) within TimeWindow after time query

Mutable Elements

Field	Description
LaunchdPaths	Organization-specific list of allowed launchd write locations to filter benign agents.
TimeWindow	Correlation window to link time discovery to launchd persistence/scheduling.
AllowedCallers	Known management agents (e.g., JAMF) that legitimately call systemsetup/date.

AN0433

Interactive or remote shell/API invocation of esxcli system clock get or querying time parameters via hostd/vpxa shortly followed by time/ntp configuration checks or scheduled task creation, executed by non-standard accounts or outside maintenance windows.

Log Sources

Mutable Elements

Field	Description
MaintenanceWindow	Only alert if outside approved ops windows.
PrivilegedAccountsAllowList	Suppress alerts for known service accounts.
RemoteIPAllowList	Whitelist management station IPs.
TimeWindow	Correlation between esxcli time query and subsequent hostd/vpxa config calls.

AN0434

Non-standard or rare users/locations issue CLI commands like "show clock detail" or "show timezone"; optionally followed by configuration of time/timezone or NTP sources. AAA/TACACS+ accounting and syslog correlate execution to identity, source IP, and privilege level.

Log Sources

Data Component	Name	Channel
Command Execution (DC0064)	networkdevice:syslog	command-exec: CLI commands containing "show clock", "show clock detail", "show timezone" executed by suspicious user/source
File Modification (DC0061)	networkdevice:config	config-change: timezone or ntp server configuration change after a time query command

Mutable Elements

Field	Description
AllowedAdminSubnets	Only alert on access from outside the NOC/management subnets.
KnownMaintenanceUsers	Whitelist known automation/orchestration accounts.
TimeWindow	Correlation window between time query and config change.

Source: https://attack.mitre.org/detectionstrategies/DET0151#AN0431