Detection of Adversarial Process Discovery Behavior, Detection Strategy DET0034

Archived: 2026-04-05 17:49:44 UTC

AN0095

Identifies adversary behavior that launches commands or invokes APIs to enumerate active processes (e.g., tasklist.exe, Get-Process, or CreateToolhelp32Snapshot). Detects execution combined with parent process lineage, network session context, or remote origin.

Log Sources

Mutable Elements

Field	Description
ParentProcessName	Used to scope suspicious discovery from non-interactive or non-standard parent processes like Office macros, WMI, or script engines
CommandLinePattern	Adversaries may obfuscate or vary process discovery commands (e.g., aliases, PowerShell variants)
TimeWindow	Helps detect bursty discovery behavior within a short timeframe

AN0096

Detects execution of common process enumeration utilities (e.g., ps, top, htop) or access to /proc with suspicious ancestry. Correlates command usage with interactive shell context and user role.

Log Sources

Mutable Elements

Field	Description
AccessedPath	Filter based on suspicious /proc directory enumeration or high-volume ls/readlink usage
UserContext	Helps tune for root vs. low-priv users during interactive vs. scripted activity

AN0097

Monitors execution of ps, top, or launchctl with unusual parent processes or from terminal scripts. Also detects AppleScript-based process listing or `system_profiler SPApplicationsDataType` misuse.

Log Sources

Mutable Elements

Field	Description
ParentApp	Tunable to detect discovery from non-UI tools or script-based execution (osascript, zsh, cron)

AN0098

Detects process enumeration using `esxcli system process list` or `ps` on ESXi shell or via unauthorized SSH sessions. Correlates with interactive sessions and abnormal user roles.

Log Sources

Mutable Elements

Field	Description
User	Admins are expected to run these commands—flag if non-admin or unknown users do

AN0099

Monitors CLI-based execution of `show process` or equivalent on routers/switches. Correlates unusual device access, unauthorized roles, or config mode changes.

Log Sources

Mutable Elements

Field	Description
Username	Tunable based on authorized operators for network infrastructure
CommandString	Pattern match or regex scope for discovery commands

---