Detection Strategy for Device Driver Discovery, Detection Strategy DET0579

Archived: 2026-04-05 13:33:34 UTC

AN1595

Monitor for suspicious usage of driver enumeration utilities (driverquery.exe) or API calls such as EnumDeviceDrivers(). Registry queries against HKLM\SYSTEM\CurrentControlSet\Services and HardwareProfiles that are abnormal may also indicate attempts to discover installed drivers and services. Correlate command execution, process creation, and registry access to build a behavioral chain of driver discovery.

Log Sources

Mutable Elements

Field	Description
AllowedUtilities	Whitelist expected administrative usage of driverquery.exe or other enumeration utilities.
TimeWindow	Correlation window between process creation and registry queries to identify suspicious chaining of events.

AN1596

Detect attempts to enumerate kernel modules through lsmod, modinfo, or inspection of /proc/modules and /dev entries. Focus on unusual execution contexts such as unprivileged users or processes outside expected administrative workflows.

Log Sources

Mutable Elements

Field	Description
KnownAdminUsers	Limit detection noise by filtering expected kernel module inspection by root or system maintenance scripts.

AN1597

Detect loading or inspection of kernel extensions (kextstat, kextfind) and file access to /System/Library/Extensions/. Monitor unexpected usage of these utilities by non-administrative users or scripts.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	macos:unifiedlog	exec: Execution of kextstat, kextfind, or ioreg targeting driver information
File Access (DC0055)	macos:unifiedlog	read: File access to /System/Library/Extensions/ or related kernel extension paths

Mutable Elements

Field	Description
AllowedMaintenanceTasks	Tune detection by excluding expected system diagnostic or patch-related invocations of kext utilities.
