Multi-Platform Software Discovery Behavior Chain, Detection Strategy DET0392

Archived: 2026-04-05 18:36:52 UTC

AN1100

Adversary spawns a process or script to enumerate installed software using WMI, registry, or PowerShell, potentially followed by additional discovery or evasion behavior.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Detection may be scoped to multiple discovery commands within a short timeframe.
ParentProcess	Tuning based on whether discovery activity stems from suspicious versus approved management tools.

AN1101

Adversary invokes 'dpkg -l', 'rpm -qa', or other package managers via shell or script to enumerate installed software.

Log Sources

Mutable Elements

Field	Description
ScriptName	Path to the wrapper script that invokes enumeration commands.
TTYContext	Scope detection to interactive vs. background shell contexts.

AN1102

Adversary runs 'system_profiler SPApplicationsDataType' or queries plist files to enumerate software via Terminal or scripts.

Log Sources

Mutable Elements

Field	Description
AppScope	Whether enumeration targets user apps or system apps.
ProcessGroup	Parent process or scripting environment (e.g., Python, osascript).

AN1103

Adversary uses cloud-native APIs or CLI (e.g., AWS Systems Manager, Azure Resource Graph) to list installed software on cloud workloads.

Log Sources

Mutable Elements

Field	Description
UserAgent	Differentiate access from automated scripts vs. authorized console.
InventoryType	May focus on Application or Platform inventory only.

AN1104

Adversary uses 'esxcli software vib list' to enumerate installed VIBs, drivers, and modules.

Log Sources

Mutable Elements

Field	Description
HostAccessMode	Detection may vary based on whether enumeration is local or remote.
ScriptChain	Presence of enumeration in broader scripted sequence.
