Security Software Discovery Across Platforms, Detection Strategy DET0016

Archived: 2026-04-05 13:13:35 UTC

AN0048

Adversary executes commands to enumerate installed antivirus, EDR, or firewall agents using WMI, registry queries, and built-in tools (e.g., tasklist, netsh, sc query). Correlated with elevated process privileges or scripting engine usage.

Log Sources

Mutable Elements

Field	Description
ParentProcess	Defenders can tune based on trusted or known-good parent process relationships
ImagePathContains	Regex match on adversary tool or enumeration script used

AN0049

Adversary runs discovery commands such as `ps aux`, `systemctl status`, or `cat /etc/init.d/` to enumerate security software or services. Often occurs alongside privilege escalation or bash script execution.

Log Sources

Mutable Elements

Field	Description
ExecutableName	Adjust for custom script names or wrappers used in the environment
TimeWindow	Tuning threshold for multiple enumeration commands within short duration

AN0050

Adversary attempts to detect monitoring agents such as Little Snitch, KnockKnock, or other system daemons via process listing (`ps -e`), application folder checks, and system extension listing.

Log Sources

Mutable Elements

Field	Description
ToolNameMatch	Adversary may search for specific software names; defenders can tune based on local deployments

---

Source: https://attack.mitre.org/detectionstrategies/DET0016#AN0049