Detection Strategy for Fileless Storage via Registry, WMI, and Shared Memory, Detection Strategy DET0344

Archived: 2026-04-05 14:30:37 UTC

AN0973

Detects abuse of fileless storage mechanisms such as Registry keys, WMI classes, and Event Logs used to stage payloads, scripts, or encoded content outside traditional files.

Log Sources

Mutable Elements

Field	Description
RegistryPathFilter	Scoped to suspicious or abused paths like HKCU\Software\Classes\ or HKLM\SYSTEM\CurrentControlSet\Services\
PayloadEntropyThreshold	Minimum entropy level to flag suspicious registry or WMI content as encoded payloads
TimeWindow	Temporal window for correlating WMI/registry modifications with process creation or network usage

AN0974

Detects usage of shared memory directories (/dev/shm, /run/shm) for temporary storage of obfuscated, encoded, or executable data without persistence to disk.

Log Sources

Mutable Elements

Field	Description
PathPrefix	Shared memory mount path used (e.g., /dev/shm/ or /run/shm/)
FilenameRegex	Regex to match non-standard, suspicious, or encoded filenames
ExecCorrelationWindow	Time window to correlate process execution from shared memory directories

Source: https://attack.mitre.org/detectionstrategies/DET0344#AN0974