Detect Abuse of Component Object Model (T1559.001), Detection Strategy DET0224

Archived: 2026-04-05 14:52:05 UTC

AN0628

Detects anomalous use of COM objects for execution, such as Office applications spawning scripting engines, enumeration of COM interfaces via registry queries, or processes loading atypical DLLs through COM activation. Correlates process creation, module loads, and registry queries to flag suspicious COM-based code execution or persistence.

Log Sources

Mutable Elements

Field	Description
COMObjectAllowList	Legitimate COM CLSIDs and ProgIDs used by enterprise applications, to reduce false positives.
ParentProcessExclusions	Expected parent-child process relationships (e.g., explorer.exe spawning dllhost.exe).
TimeWindow	Threshold for correlating COM object execution with subsequent process creation or DLL load.
