Detection Strategy for Hijack Execution Flow using Path Interception by Search Order Hijacking, Detection Strategy DET0564

Archived: 2026-04-05 18:31:20 UTC

AN1560

Processes executing binaries named after legitimate system utilities (e.g., net.exe, findstr.exe, python.exe) from non-standard or application-specific directories, combined with file creation or modification events for such binaries. Defender correlates file writes in vulnerable directories, process execution paths inconsistent with baseline system paths, and abnormal parent-child relationships in process lineage.

Log Sources

Mutable Elements

Field	Description
SuspiciousBinaryList	Common system utilities often hijacked (e.g., net.exe, cmd.exe, powershell.exe, python.exe).
MonitoredDirectories	Directories where executables should not normally be written (e.g., application folders, user profile subdirs).
TimeWindow	Correlation window between file creation and subsequent process execution.
ParentProcessBaseline	Expected parent processes for critical system binaries, deviations may indicate hijacking.
