Detection Strategy for Hijack Execution Flow through Path Interception by Unquoted Path, Detection Strategy DET0064

Archived: 2026-04-05 14:17:34 UTC

Analytics

- Windows

AN0176

Unquoted service or shortcut paths that contain spaces and allow path interception by higher-level executables. Defender observes registry service configurations with unquoted paths, file creation of executables in parent directories of unquoted paths, and subsequent process execution from unexpected locations.

Log Sources

Mutable Elements

Field	Description
MonitoredServices	List of critical services to check for unquoted paths in ImagePath registry keys.
SuspiciousBinaryList	Executables with names matching potential interception targets (e.g., program.exe, net.exe).
TimeWindow	Correlation interval between file creation in parent directories and execution of unquoted path process.
BaselineServiceConfig	Known good service paths for comparison against modified or unquoted values.
