Detection Strategy for Hijack Execution Flow for DLLs, Detection Strategy DET0201

Archived: 2026-04-05 17:33:18 UTC

AN0577

DLL hijacking behaviors including unexpected DLL loads from non-standard directories, replacement of DLLs, phantom DLL insertion, redirection file creation, and substitution of legitimate DLLs. Defender correlates file system modifications, registry changes, and module load telemetry to detect abnormal DLL behavior in trusted processes.

Log Sources

Mutable Elements

Field	Description
AllowedDllPaths	Known safe DLL directories to suppress false positives (e.g., C:\Windows\System32).
ProcessAllowList	Applications expected to load DLLs from non-standard locations (e.g., development tools).
TimeWindow	Correlation interval between DLL file creation, registry changes, and module load.
HashBaseline	Baseline hashes for legitimate DLLs used to detect substitution.
