Detection Strategy for Hijack Execution Flow across OS platforms., Detection Strategy DET0218

Archived: 2026-04-05 14:45:37 UTC

AN0609

Unusual modifications to service binary paths, registry keys, or DLL load paths resulting in alternate execution flow. Defender observes registry key modifications, suspicious file writes into system directories, and processes loading libraries from abnormal paths.

Log Sources

Mutable Elements

Field	Description
ServiceBaseline	Expected registry keys and service paths for comparison.
AllowedDllPaths	Directories considered valid for DLL loading.
TimeWindow	Correlation interval between registry/file modification and process execution.

AN0610

Adversary manipulation of shared library paths, environment variables, or replacement of service binaries. Defender observes suspicious modifications in /etc/ld.so.preload, service config changes, or file writes replacing existing executables.

Log Sources

Mutable Elements

Field	Description
MonitoredDirectories	Directories where binary replacement should trigger alerts.
EnvVarMonitors	Environment variables like LD_PRELOAD or PATH to monitor.

AN0611

Abuse of DYLD_INSERT_LIBRARIES or hijacking framework paths for malicious libraries. Defender observes processes invoking abnormal dylibs, modified plist files, or persistence entries pointing to altered binaries.

Log Sources

Mutable Elements

Field	Description
AllowedDylibPaths	Baseline directories for dylib loading.
PlistMonitors	Specific plist files used for persistence monitoring.

Source: https://attack.mitre.org/detectionstrategies/DET0218#AN0609