Detection Strategy for Hijack Execution Flow: Dynamic Linker Hijacking, Detection Strategy DET0435

Archived: 2026-04-05 12:38:25 UTC

AN1209

Detection focuses on identifying abuse of LD_PRELOAD and related linker variables. Defender perspective: monitor unexpected setting or modification of LD_PRELOAD in shell initialization scripts or environment exports, file creation of suspicious shared libraries, and correlation of these modifications with anomalous process execution. Key signals include execve events with LD_PRELOAD defined, newly created .so files in user directories, and processes hooking libc functions exhibiting abnormal behavior.

Log Sources

Mutable Elements

Field	Description
WatchedEnvVars	Environment variables like LD_PRELOAD, LD_LIBRARY_PATH. Defenders can tune based on development vs. production systems.
MonitoredDirectories	Non-standard library paths (e.g., /tmp, user home dirs). May be tuned to reduce false positives from benign development activity.
CorrelationWindow	Timeframe to correlate suspicious library creation with process execution that loads it.

AN1210

Detection centers on DYLD_INSERT_LIBRARIES and DYLD_LIBRARY_PATH abuse. Defender perspective: monitor for modification of these environment variables in shell or plist files, file creation of dylibs in user-controlled paths, and correlation of environment variable usage with unexpected module loads by user applications. Suspicious indicators include processes with DYLD_INSERT_LIBRARIES set, execution of applications loading untrusted dylibs, and anomalies in module load history.

Log Sources

Mutable Elements

Field	Description
WatchedEnvVars	macOS linker variables like DYLD_INSERT_LIBRARIES. Tunable to development environments where use may be expected.
BaselineDylibs	Known dylibs typically loaded by apps. Deviations highlight potential hijacking.
MonitoredDirectories	Locations where dylibs are monitored for tampering (e.g., /Applications, /System/Library, /tmp).
