Behavior-chain, platform-aware detection strategy for T1129 Shared Modules, Detection Strategy DET0018

Archived: 2026-04-05 13:45:14 UTC

AN0052

A process (often LOLBin or user-launched program) loads a DLL from a user-writable/UNC/Temp path or unsigned/invalid signer. Within a short window the DLL is (a) newly written to disk, (b) spawned as follow-on execution (rundll32/regsvr32), or (c) establishes outbound C2.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Correlation window between file write → module load → network (e.g., 0–20 minutes).
SuspiciousPathRegex	Regex for user-writable/UNC/temp paths to flag (e.g., %TEMP%, %APPDATA%, *\share\).
UnsignedOnly	Alert only when SignatureStatus != Valid to reduce noise.
RareSignerThreshold	Frequency threshold for unseen/rare signers in last N days.
MinFileSizeKB	Ignore tiny DLL stubs to cut noise.

AN0053

A process loads a shared object (.so) via dlopen/LD_PRELOAD/open from non-standard or temporary locations (e.g., /tmp, /dev/shm), especially shortly after that .so is written or fetched, or linked via manipulated environment variables (LD_PRELOAD/LD_LIBRARY_PATH).

Log Sources

Mutable Elements

Field	Description
SuspiciousDirs	(/tmp, /dev/shm, /var/tmp, user home dirs) – adjust to your environment.
TimeWindow	Correlate write/fetch of .so to its load (e.g., 0–30 minutes).

Field	Description
EnvVarWatchlist	LD_PRELOAD, LD_LIBRARY_PATH, LD_AUDIT.
AllowedSigning/HashList	Known-good signed or hashed shared objects.

AN0054

A process loads a non-system .dylib/.so via dyld (dlopen/dlsym) from user-writable locations (~/Library, /tmp) or after the library was recently created/downloaded, often followed by network egress or persistence.

Log Sources

Data Component	Name	Channel
Module Load (DC0016)	macos:unifiedlog	dyld/unified log entries indicating image load from non-system paths
Process Creation (DC0032)	macos:endpointsecurity	exec: Process execution context for loaders calling dlopen/dlsym
File Access (DC0055)	macos:endpointsecurity	ES_EVENT_TYPE_NOTIFY_OPEN: Open of .dylib/.so in user-writable locations

Mutable Elements

Field	Description
SuspiciousDirs	~/Library, /tmp, /Users/*/.* (hidden dirs) – tune to enterprise layout.
UnsignedOnly	Alert only when code-signing is invalid or absent.
TimeWindow	Correlate write/open to module load within N minutes.
