Detect Network Provider DLL Registration and Credential Capture, Detection Strategy DET0580

Archived: 2026-04-05 14:14:20 UTC

Analytics

- Windows

AN1598

Detects registration of new or modified network provider DLLs via registry changes, anomalous file creation of DLLs in system directories, and suspicious process activity (mpnotify.exe interacting with non-standard DLLs). Multi-event correlation ties registry modification events to subsequent DLL loads during user logon activity.

Log Sources

Mutable Elements

Field	Description
MonitoredRegistryKeys	Specific registry keys to monitor for DLL registration (e.g., NetworkProvider Order).
SuspiciousDLLPaths	Directories or file name patterns outside of normal system DLL locations.
TimeWindow	Window correlating registry modification, DLL creation, and subsequent logon activity.
