Detection of Credential Harvesting via API Hooking, Detection Strategy DET0139

Archived: 2026-04-05 16:21:37 UTC

AN0389

Detects credential harvesting via userland API hooking (e.g., SetWindowsHookEx, IAT, or inline patching) by correlating memory modifications with hook installation functions and suspicious module loads in credential-sensitive processes like lsass.exe, explorer.exe, or winlogon.exe.

Log Sources

Mutable Elements

Field	Description
TargetProcess	Credential-sensitive targets (e.g., explorer.exe, winlogon.exe) may vary by environment
AccessMask	Tuning for access rights like 0x1FFFFF for full access vs. thread injection
TimeWindow	Correlate memory access and hook setup in short windows (5–10 seconds)

AN0390

Detects credential interception via malicious LD_PRELOAD-based shared libraries loaded into ssh, sudo, or scp processes. Correlates environment variable injection, unexpected library loads, and memory patching behavior.

Log Sources

Mutable Elements

Field	Description
InjectedLibraryName	Watch for user-defined suspicious .so files (e.g., libhook.so, libshadow.so)
TargetProcessName	Hooked binaries vary by use case (e.g., ssh, login, gdm)

AN0391

Detects DYLD_INSERT_LIBRARIES abuse to hook credential-sensitive applications by correlating process spawns with unauthorized library injection and monitoring changes to the __TEXT segment (code) of credential handling binaries.

Log Sources

Mutable Elements

Field	Description
DYLDInjectedPath	Tunable based on naming patterns or location of malicious dylibs
ParentProcessName	Hooking attempts may stem from terminal.app, bash, or AppleScript-based launchers

---