Detection Strategy for Hijack Execution Flow through the KernelCallbackTable on Windows., Detection Strategy DET0577

Archived: 2026-04-02 11:44:40 UTC

AN1593

Unexpected modification of the KernelCallbackTable in a process's PEB followed by invocation of modified callback functions (e.g., fnCOPYDATA) through Windows messages. Defender observes suspicious API call chains such as NtQueryInformationProcess → WriteProcessMemory → abnormal GUI callback execution, often correlating to anomalous process behavior such as network activity or code injection.

Log Sources

Mutable Elements

Field	Description
MonitoredProcesses	GUI applications (e.g., explorer.exe, notepad.exe) where KernelCallbackTable abuse is more likely.
CallbackFunctions	Specific callback functions (e.g., fnCOPYDATA, fnDWORD) expected to remain stable.
TimeWindow	Correlation interval between WriteProcessMemory calls and execution of modified callback functions.
AccessMaskThresholds	Access rights values that should be flagged when targeting GUI processes.