Behavioral Detection of Thread Execution Hijacking via Thread Suspension and Context Switching, Detection Strategy DET0295

Archived: 2026-04-05 12:51:58 UTC

Analytics

- Windows

AN0822

Detects hijacking of an existing thread (OpenThread) through a behavioral chain involving thread suspension (SuspendThread), memory modification (VirtualAllocEx + WriteProcessMemory), context manipulation (SetThreadContext), and thread resumption—all within another live process's address space (ResumeThread).

Log Sources

Mutable Elements

Field	Description
TargetProcessList	Sensitive processes that should never be targeted for thread hijack attempts
TimeWindow	Expected delay between SuspendThread and ResumeThread events; tight thresholds reduce evasion
SuspiciousThreadContextRegions	Memory regions or offsets that should not be targeted for SetThreadContext
ParentProcessAnomalyThreshold	Score deviation of the parent/child relationship in a thread injection chain

---