Behavioral Detection of PE Injection via Remote Memory Mapping, Detection Strategy DET0106

Archived: 2026-04-05 14:43:19 UTC

AN0297

Detects PE injection through a behavioral sequence where one process opens (OpenProcess) a handle to another, allocates remote memory (VirtualAllocEx), writes a PE header (MZ) or shellcode (WriteProcessMemory), then initiates a new thread (CreateRemoteThread or NtCreateThreadEx) in that process—executing injected code in memory without touching disk. Optional: injects a trampoline or shellcode that unpacks/reflectively maps the payload.

Log Sources

Mutable Elements

Field	Description
PayloadEntropyThreshold	Controls for detecting high-entropy memory writes indicating shellcode or encrypted PE
TargetProcessList	High-value or sensitive processes that should never have remote threads injected
TimeWindow	Max allowed delay between memory write and thread execution
ParentProcessAnomalyThreshold	Used to filter legitimate process hierarchies vs anomalous injection sources

---