Behavioral Detection of DLL Injection via Windows API, Detection Strategy DET0389

Archived: 2026-04-05 18:03:32 UTC

Analytics

- Windows

AN1095

Detects DLL injection through correlation of memory allocation and writing to remote process memory (e.g., VirtualAllocEx, WriteProcessMemory), followed by remote thread creation (e.g., CreateRemoteThread) that loads a suspicious or unsigned DLL using LoadLibrary or reflective loading.

Log Sources

Mutable Elements

Field	Description
InjectedDLLSignatureStatus	Whether the DLL is unsigned, untrusted, or loaded from a non-standard path
TimeWindow	Temporal correlation threshold between memory operations and thread creation
TargetProcessList	List of sensitive or high-value processes targeted for injection (e.g., explorer.exe, winlogon.exe)
ParentProcessAnomalyThreshold	Degree of deviation from expected parent-child lineage

---