Detection Strategy for Process Hollowing on Windows, Detection Strategy DET0382

Archived: 2026-04-05 13:14:02 UTC

AN1076

Detects adversary use of suspended process creation, using the CREATE_SUSPENDED flag via CreateProcess, followed by unmapping the memory of the child process (NtUnmapViewOfSection) and replacing it with malicious code via VirtualAllocEx/WriteProcessMemory, then SetThreadContext and ResumeThread to begin execution within the hollowed process.

Log Sources

Mutable Elements

Field	Description
HollowedImageNamePattern	Regex to match common decoy executables used for hollowing (e.g., 'svchost.exe', 'notepad.exe')
TimeWindow_ProcessCreateToResume	Temporal threshold for unmap/write/execute sequence (e.g., within 5–10 seconds)
SuspendedProcessStartFlag	CreateProcess flag used to identify suspended thread creation
MemoryWriteSizeThreshold	Minimum byte size to flag suspicious memory overwrite in hollowed process