Detection Strategy for NTFS File Attribute Abuse (ADS/EAs), Detection Strategy DET0432

Archived: 2026-04-05 13:45:54 UTC

AN1206

Suspicious use of NTFS file attributes such as Alternate Data Streams (ADS) or Extended Attributes (EA) to hide data. Defender perspective: anomalous file creations or modifications containing colon syntax (file.ext:ads), API calls like ZwSetEaFile/ZwQueryEaFile, or PowerShell/Windows utilities interacting with -stream parameters. Correlation across file metadata anomalies, process lineage, and command execution provides context.

Log Sources

Mutable Elements

Field	Description
ADSPathWhitelist	Exclude legitimate ADS usage by system or AV tools.
ProcessScope	Restrict monitoring to suspicious parent processes (e.g., powershell.exe, cmd.exe, wscript.exe).
TimeWindow	Correlate ADS creation with subsequent process execution to strengthen malicious context.

Source: https://attack.mitre.org/detectionstrategies/DET0432#AN1206