Removable Media Execution Chain Detection via File and Process Activity, Detection Strategy DET0301

Archived: 2026-04-05 12:59:41 UTC

Analytics

- Windows

AN0841

Execution of files originating from removable media after drive mount, with correlation to file write activity, autorun usage, or lateral spread via staged tools.

Log Sources

Mutable Elements

Field	Description
DriveLetterMatch	Detect activity on mounted drives typically used by USB (e.g., E:, F:, G:). Tune based on enterprise usage.
FileExecutionWindow	Set timing threshold for execution shortly after drive mount (e.g., < 5 minutes).
ParentProcess	Restrict detection to suspicious process lineage like explorer.exe, powershell.exe, or unsigned binaries.
FileEntropy	Use entropy thresholding to detect packed/obfuscated payloads dropped to removable media.
