Detection of Automated Collection, Detection Strategy DET0734

Archived: 2026-04-05 16:43:30 UTC

AN1867

Monitor for any suspicious attempts to enable script execution on a system. If scripts are not commonly used on a system, but enabled, scripts running out of cycle from patching or other administrator functions are suspicious.
Scripts should be captured from the file system when possible, to determine their actions and intent.
Monitor executed commands and arguments for actions that could be taken to collect internal data.
Monitor for unexpected files (e.g., .pdf, .docx, .jpg) viewed for collecting internal data.
Monitor for information collection on assets that may indicate deviations from standard operational tools. Examples include unexpected industrial automation protocol functions, new high volume communication sessions, or broad collection across many hosts within the network.

Log Sources
