Detection of Scripting, Detection Strategy DET0735

Archived: 2026-04-05 16:42:40 UTC

AN1868

Monitor command-line arguments for script execution and subsequent behavior. Actions may be related to network and system information Discovery, Collection, or other scriptable post-compromise behaviors and could be used as indicators of detection leading back to the source script. Scripts are likely to perform actions with various effects on a system that may generate events, depending on the types of monitoring used.
Monitor log files for process execution through command-line and scripting activities. This information can be useful in gaining additional insight to adversaries' actions through how they use native processes or custom tools. Also monitor for loading of modules associated with specific languages.
Monitor contextual data about a running process, which may include information such as environment variables, image name, user/owner, or other information that may reveal abuse of system features.
Monitor for events associated with scripting execution, such as the loading of modules associated with scripting languages (e.g., JScript.dll, vbscript.dll).
Monitor for any attempts to enable scripts running on a system would be considered suspicious. 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.

Log Sources
