# Detection of System Binary Proxy Execution, Detection Strategy DET0793

Archived: 2026-04-05 15:23:52 UTC

**AN1925**

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 associated arguments for application programs which support executing custom code, scripts, commands, or executables.
Monitor for unusual processes execution, especially for processes that allow the proxy execution of malicious files.

**Log Sources**

---