Detection of Script-Based Proxy Execution via Signed Microsoft Utilities, Detection Strategy DET0466

Archived: 2026-04-05 16:31:36 UTC

AN1288

Execution of Microsoft-signed scripts (e.g., pubprn.vbs, installutil.exe, wscript.exe, cscript.exe) used to proxy execution of untrusted or external binaries. Behavior is detected through command-line process lineage, child process spawning, and unsigned payload execution from signed parent.

Log Sources

Mutable Elements

Field	Description
ParentProcessName	Environment-specific paths to script interpreters like wscript.exe, cscript.exe, pubprn.vbs, or installutil.exe.
TimeWindow	Time delta between signed script execution and suspicious child process creation.
ChildCommandLineRegex	Regex pattern used to detect malicious payload execution (e.g., download cradle, PowerShell decode).
SignedToUnsignedTransition	Indicates whether the parent is signed by Microsoft but child is unsigned or unknown.