Cross-Platform Detection of JavaScript Execution Abuse, Detection Strategy DET0264

Archived: 2026-04-05 15:36:30 UTC

AN0733

Detects JavaScript execution through WSH (wscript.exe, cscript.exe) or HTA (mshta.exe), particularly when spawned from Office macros, web browsers, or abnormal user paths. Correlates script execution with outbound network activity or system modification.

Log Sources

Mutable Elements

Field	Description
ParentProcess	Execution of wscript.exe, cscript.exe, or mshta.exe from suspicious parent like Excel or Outlook.
ScriptPath	Script loaded from %TEMP%, user download folder, or via UNC/web path.
TimeWindow	Execution of JavaScript during non-business or patch windows.
UserContext	Execution by accounts not typically authorized for scripting (e.g., non-admin users).
EntropyScore	Obfuscated JS with high entropy detected by AMSI or ScriptBlock logging.

AN0734

Detects JavaScript for Automation (JXA) via osascript or compiled scripts using OSAKit APIs. Flags execution involving system modification, inter-process scripting, or browser abuse.

Log Sources

Mutable Elements

Field	Description
ScriptLocation	Execution of JXA from user-controlled paths like ~/Downloads or /Volumes.
ParentProcess	osascript invoked by third-party apps (VSCode, browsers, etc.).
APIInvocation	Use of OSAKit API by apps not typically scripting-enabled.

AN0735

Detects Node.js or JavaScript interpreter execution from web shells, cron jobs, or local users. Correlates execution with reverse shell behavior, file modifications, or abnormal outbound connections.

Log Sources

Mutable Elements

Field	Description
ScriptPath	Script launched from /tmp, /var/tmp, or hidden dot directories.
BinaryName	Custom compiled JS binaries like node_shell or interpreter disguises.
UserExecutionContext	Execution by service accounts or low-privilege users running cron scripts.
NetworkFollowUp	Connection attempts to C2 post-node.js execution.
