Detection Strategy for SVG Smuggling with Script Execution and Delivery Behavior, Detection Strategy DET0510

Archived: 2026-04-05 17:57:01 UTC

AN1407

Detects suspicious SVG file creation or download events followed by script engine execution (e.g., wscript.exe, mshta.exe, rundll32.exe), network callbacks, or browser-based credential collection.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Threshold between SVG file write and script execution (e.g., < 60s)
ParentProcessWhitelist	Allowlisted script engines that may invoke browsers or JS in benign cases
FileExtensionPattern	Regex or string match for .svg, .svgz, or embedded .svg inside HTML or PDF

AN1408

Detects downloaded SVG files followed by execution of browser processes or tools like xdg-open, and rapid follow-on network connections or process spawns to interpreters like python or bash.

Log Sources

Mutable Elements

Field	Description
TargetPaths	Suspicious write locations such as /tmp/, ~/Downloads/
ExecutionContext	Processes spawned by browsers or svg-viewing apps that invoke interpreters
NetworkDestinations	URLs/IPs contacted post-SVG access – may reflect initial C2

AN1409

Detects SVGs downloaded via browser that invoke AppleScript, osascript, or JavaScriptCore processes, followed by network egress or file drop to LaunchAgents or ~/Library.

Log Sources

Mutable Elements

Field	Description
ScriptEngines	Scriptable binaries such as osascript, jsc, JavaScriptCore – may vary by OS version
UserContext	Restrict to non-system users or only specific login sessions
EmbeddedContentIndicators	SVGs embedded inside PDFs or HTML with script-based triggers

---