Detection Strategy for Steganographic Abuse in File & Script Execution, Detection Strategy DET0119

Archived: 2026-04-02 11:11:22 UTC

AN0331

Detects execution of image viewers or PowerShell scripts accessing or decoding files with mismatched MIME headers or embedded script-like byte patterns; often correlated with suspicious parent-child process lineage and outbound connections.

Log Sources

Mutable Elements

Field	Description
ParentProcessImage	Tune to identify image editors/viewers invoking script interpreters (e.g., `mspaint.exe` > `powershell.exe`)
MimeHeaderMismatchTolerance	Adjust tolerance for image file headers that do not match file extensions or content structure
TimeWindow	Define the temporal range to correlate decoding → execution → network beaconing

AN0332

Detects access to media files followed by execution of scripts (bash, Python, etc.) referencing those same files, or outbound traffic triggered shortly after file read. Correlates unusual use of tools like `steghide`, `exiftool`, or image libraries.

Log Sources

Mutable Elements

Field	Description
MonitoredToolsList	Define the list of steganographic or image-parsing tools to alert on (e.g., `steghide`, `imagemagick`)
ScriptInterpreterMatch	Tune to detect script engines accessing media files (e.g., `python script.py image.png`)

AN0333

Detects manipulation of PNG, JPG, or GIF files by user-initiated scripts followed by script execution or exfiltration behavior, especially from `osascript`, `python`, or `bash`, in combination with LaunchAgent persistence or curl activity.

Log Sources

Mutable Elements

Field	Description
StegoToolNamePatterns	Adapt to known or emerging tools using stego methods on macOS (e.g., `Invoke-PSImage`, `stegsolve`)
ParentScriptSources	Update list of trusted versus unknown scripting hosts launching activity tied to image handling

---