Detecting Steganographic Command and Control via File + Network Correlation, Detection Strategy DET0235

Archived: 2026-04-05 15:31:41 UTC

AN0651

Detect the creation or modification of common media file formats (e.g., .jpg, .png, .wav) following suspicious process activity like compression or encryption, especially when paired with lateral movement or exfiltration behavior.

Log Sources

Mutable Elements

Field	Description
FileExtensionFilter	Allows tuning of monitored file types (e.g., .jpg, .png, .docx).
PayloadEntropyThreshold	Threshold for flagging potential hidden data in outbound payloads.
ExecutionToExfilTimeWindow	Time window between media creation and network transmission.

AN0652

Unusual use of steganographic or media processing binaries (e.g., `steghide`, `ffmpeg`, `imagemagick`) followed by outbound communication to external IPs with high data output and media MIME types.

Log Sources

Mutable Elements

Field	Description
ToolNameMatch	Specify which binaries to monitor (e.g., steghide, outguess).
OutboundTrafficPattern	Adjust based on known normal file upload services.

AN0653

Abnormal usage of Preview, ImageMagick, or binary editors to alter images/documents, followed by exfiltration or outbound connections with mismatched file MIME types or payload structure.

Log Sources

Mutable Elements

Field	Description
ParentProcessBaseline	Allow tuning based on expected apps calling image-editing tools.
TimeDelta	Gap between file manipulation and outbound connection.

AN0654

Suspicious modification of file artifacts (e.g., logs, ISO templates) on ESXi datastores, followed by beaconing or POST operations to external IPs potentially hiding payloads in file-like traffic.

Log Sources

Mutable Elements

Field	Description
FilenamePattern	Tune for likely stego file names (e.g., wallpaper.jpg, template.iso).
UnusualDestinationIP	Destination outside vCenter management subnet.
