Data Obfuscation: Steganography, Sub-technique T1001.002 - Enterprise

Archived: 2026-04-05 13:19:01 UTC

ID	Name	Analytic ID	Analytic Description
DET0235	Detecting Steganographic Command and Control via File + Network Correlation	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.
		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.
		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.
		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.