Detect Bidirectional Web Service C2 Channels via Process & Network Correlation, Detection Strategy DET0035

Archived: 2026-04-05 16:52:03 UTC

AN0100

Suspicious processes initiating encrypted HTTPS connections to common web service domains, followed by abnormal data upload behavior or automated posting behavior indicative of C2 bidirectional traffic.

Log Sources

Mutable Elements

Field	Description
TimeWindow	Timeframe for evaluating multiple network connections tied to the same process
DomainPattern	Regex or string patterns used to identify common Web service infrastructure (e.g., *.googleapis.com)
PayloadSizeThreshold	Minimum data upload size before flagging anomaly
ProcessNameExclusionList	Known benign updaters or service processes to reduce false positives

AN0101

Non-interactive system processes making encrypted HTTPS connections to well-known web services followed by high outbound traffic volume or scripted upload patterns.

Log Sources

Mutable Elements

Field	Description
UploadDirectionality	Bias detection toward sessions with larger upload vs download volume
HostnameRegexList	List of known public Web services used for dead drops or C2 (e.g., GitHub, Twitter)
ScriptParentName	Shell interpreter or automated job parent used for filtering (e.g., /usr/bin/python)

AN0102

Scripting engines (e.g., osascript, Python) initiating HTTPS requests to social media or content-sharing platforms, paired with automated response handling indicative of two-way communication.

Log Sources

Mutable Elements

Field	Description
ScriptEngineList	Scripting interpreters to monitor for unusual HTTP traffic (e.g., osascript, ruby, bash)
SocialMediaDomainPatterns	Patterns or domains used for C2 dead drops and responses (e.g., pastebin.com, twitter.com)
BurstConnectionRate	Threshold for number of short-lived HTTPS connections in a short window

---