Detection of Web Protocol-Based C2 Over HTTP, HTTPS, or WebSockets, Detection Strategy DET0027

Archived: 2026-04-05 13:00:05 UTC

AN0075

Detects unexpected or high-volume HTTP/S/WebSocket communication from suspicious processes (e.g., PowerShell, rundll32) using uncommon user agents or mimicking browser traffic to unusual domains or IPs.

Log Sources

Mutable Elements

Field	Description
ProcessNameExclusions	Filter out legitimate browser/network utilities
UserAgentAnomalies	Detect non-browser user-agents or spoofed headers
OutboundByteRatioThreshold	Flag when outbound > inbound volume by 90%+

AN0076

Detects curl, wget, Python requests, or custom HTTP clients communicating over non-standard ports, with repetitive or beacon-like patterns or POST-heavy behavior to rare domains.

Log Sources

Mutable Elements

Field	Description
CommandLinePatternMatch	curl or wget in scripts with suspicious domains or silent flags
BeaconIntervalWindow	Fixed-timed HTTP callbacks with 60±5s jitter

AN0077

Detects applications such as Automator, AppleScript, or LaunchDaemons invoking HTTP/S traffic to non-standard domains or using suspicious headers (e.g., Base64 in URIs or cookie fields).

Log Sources

Mutable Elements

Field	Description
SuspiciousParentProcess	Non-browser parent of web traffic (e.g., AppleScript, bash)
URIEntropyThreshold	Unusually encoded data in GET/POST URIs

AN0078

Detects HTTP or HTTPS communication initiated by shell-based scripts or management daemons, especially those reaching public IPs over ports 80/443 using embedded curl or wget.

Log Sources

Mutable Elements

Field	Description
ShellScriptMatch	Match on commands like `wget https://*`, `curl -s`
ExternalConnectionFilter	Public IPs or external DNS hostnames

AN0079

Detects Web protocol misuse such as encoded HTTP headers, WebSocket upgrade requests with abnormal payloads, or TLS handshake anomalies suggesting embedded C2 channels.

Log Sources

Mutable Elements

Field	Description
HeaderEncodingPattern	Base64, hex, or UTF-16 encoding in URI, cookie, or host
TLSFingerprintMismatch	JA3 hash deviation from known clients
