External Proxy Behavior via Outbound Relay to Intermediate Infrastructure, Detection Strategy DET0325

Archived: 2026-04-02 12:07:33 UTC

AN0922

Unusual process (e.g., `rundll32`, `mshta`, `wscript`, or custom payloads) initiates network connection to external IPs/domains that proxy C2 traffic, often over uncommon ports or high entropy HTTP/S connections.

Log Sources

Mutable Elements

Field	Description
DestinationASN	Adjust for known benign but high-risk infrastructure (e.g., hosting providers like DigitalOcean, OVH, etc.).
ParentProcess	Detect suspicious lineage—proxy tools launched from script interpreters or LOLBins.
EntropyThreshold	Tune based on expected randomness in outbound request payloads.

AN0923

`curl`, `wget`, `ncat`, `socat`, or custom binaries initiate outbound traffic to Internet-based proxies (e.g., via VPS or CDN). Behavior may include reverse shell constructs or persistent outbound beacons.

Log Sources

Mutable Elements

Field	Description
CommandLinePattern	Regex or command substring matches indicative of dynamic proxy setup.
ExternalIPList	Tunable list of IPs or ASNs related to known proxy/VPS abuse.
UserContext	Unexpected users running networking tools (e.g., www-data, apache).

AN0924

AppleScript or terminal sessions launch tools (`curl`, `nc`, `ssh`) to external IPs not commonly accessed. Outbound connections are made by LaunchAgents/LaunchDaemons, often masquerading as system services.

Log Sources

Mutable Elements

Field	Description
LaunchAgentPath	Detect persistence used to restart proxy after reboot.
ExternalPort	Often high or non-standard ports, configurable for outbound proxy detection.
ProcessReputation	Flag unsigned or anomalous binaries making external connections.

AN0925

ESXi shell or guest VM tools initiate external connections via scripted traffic forwarding to Internet-based proxies. Detected by firewall or shell audit logs showing outbound connection spikes from hypervisor or guest VM to remote proxy nodes.

Log Sources

Mutable Elements

Field	Description
VMOutboundPatterns	Detect when VMs communicate with Internet IPs not in workload profiles.
ProxyHostPattern	Regex for proxy-related tools/scripts executed on the host.
ConnectionDirectionality	Outbound only connections from ESXi to new IPs.

AN0926

Changes to NAT/firewall policies enabling outbound port forwarding from internal IPs to Internet-based proxy endpoints. Log spikes in outbound flows to CDN, VPS, or anomalous ASNs with few return packets.

Log Sources

Mutable Elements

Field	Description
FlowThreshold	Number of flows or bytes transferred per minute—flag surges to unrecognized ASNs.
DestinationIPCategory	Proxy destination categories: CDN, TOR exit node, anonymous hosting.
ConfigChangeUser	Track if unexpected user or automation changed NAT/forwarding rules.

Source: https://attack.mitre.org/detectionstrategies/DET0325#AN0926