Detection of Proxy Infrastructure Setup and Traffic Bridging, Detection Strategy DET0445

Archived: 2026-04-05 13:31:20 UTC

AN1229

Suspicious process spawning (e.g., `rundll32`, `svchost`, `powershell`, or `netsh`) followed by network connection creation to internal hosts or uncommon external endpoints on high or non-standard ports.

Log Sources

Mutable Elements

Field	Description
ParentProcessName	Legitimate system processes that may rarely spawn network-capable child processes (e.g., `rundll32`, `svchost`).
DestinationPort	Watch for high-numbered ports or well-known proxy ports like 1080, 8080, 4444.
TimeWindow	Capture unusual spikes in outbound connections over a short period.

AN1230

User-space tools (e.g., `socat`, `ncat`, `iptables`, `ssh`) used in non-standard ways to establish reverse shells, port-forwarding, or inter-host connections. Often chained with uncommon outbound destinations or SSH tunnels.

Log Sources

Mutable Elements

Field	Description
CommandLinePattern	Shell piping into tools like `socat`, `ncat`, or `openssl` for tunnel creation.
OutboundPortRange	Flag connections made from internal systems to uncommon high ports externally.
ProcessUserContext	Capture low-privilege or unexpected users executing system-level network tools.

AN1231

AppleScript, LaunchAgents, or remote login services (`ssh`, `networksetup`) establishing proxy tunnels or dynamic port forwards to external IPs or alternate local hosts.

Log Sources

Mutable Elements

Field	Description
TargetDomain	Identify suspicious domains often associated with CDN-routed or anonymized endpoints (e.g., Cloudflare, Fastly).
AppleScriptUsage	Alert when AppleScript or Automator tools are used for network tunneling tasks.
LaunchAgentSource	Monitor for LaunchAgents executing proxy tools or dynamic ports.

AN1232

Direct use of `nc`, `socat`, or reverse tunnel scripts initiated by abnormal user contexts or unauthorized VIBs initiating connections from hypervisor to external systems.

Log Sources

Mutable Elements

Field	Description
CLICommand	Custom proxy or port forwarding scripts executed from ESXi shell.
DestinationIP	Unusual outbound connections from ESXi host, particularly to internet.
UserContext	Root or elevated users initiating unexpected tunnels.

AN1233

Dynamic or static port forwarding rules added to route traffic through an internal host, or configuration changes to proxy firewall rules not aligned with baselined policy.

Log Sources

Mutable Elements

Field	Description
RuleType	Focus on new allow/permit rules with dynamic NAT or port forwarders.
ChangeUser	Flag any non-admins initiating proxy config changes.
FlowVolumeDelta	Detect sharp changes in bi-directional traffic patterns.

Source: https://attack.mitre.org/detectionstrategies/DET0445#AN1233