Detection Strategy for Hide Infrastructure, Detection Strategy DET0411

Archived: 2026-04-05 16:54:19 UTC

AN1148

Monitor DNS queries, proxy logs, and user-agent strings for anomalous patterns associated with adversary attempts to hide infrastructure. Defenders may observe DNS resolutions to short-lived domains, abnormal WHOIS registration data, or filtering of known defensive/responder IP addresses.

Log Sources

Mutable Elements

Field	Description
SuspiciousDomains	List of domains registered with privacy-protected or suspicious WHOIS metadata.
ResponderIPs	Known incident response or scanning infrastructure IP ranges.

AN1149

Detect adversaries filtering traffic or modifying server responses to evade scanning. Monitor iptables, nftables, or proxy configurations that deny or redirect requests from known scanning agents or defensive tools.

Log Sources

Data Component	Name	Channel
Process Creation (DC0032)	auditd:SYSCALL	execve: Execution of commands modifying iptables/nftables to block selective IPs
Response Metadata (DC0106)	NSM:Flow	Altered response metadata or blocked content based on user-agent or geolocation

Mutable Elements

Field	Description
BlockedAgents	User-agent strings or scanning tools to monitor for selective filtering.

AN1150

Monitor unified logs for manipulation of proxy configurations, DNS resolution, or filtering rules. Adversaries may redirect responses or use trusted domains that later resolve to malicious C2 infrastructure.

Log Sources

Mutable Elements

Field	Description
TrustedHostingProviders	Known hosting/CDN providers often abused to hide malicious C2 infrastructure.

AN1151

Inspect network telemetry for adversary attempts to blend malicious traffic with legitimate flows using VPNs, proxies, or geolocation spoofing. Defensive teams may observe anomalous tunnels, encrypted sessions to suspicious domains, or geo-mismatched IP activity.

Log Sources

Mutable Elements

Field	Description
GeoIPRanges	Regions to monitor for unexpected or mismatched geolocation activity.

AN1152

Monitor VM-level DNS and network traffic logs for adversary-controlled domains or selective response behavior (e.g., dropped requests from security scanners).

Log Sources

Mutable Elements

Field	Description
MonitoredVMs	Targeted virtual machines where adversaries may attempt to hide C2 traffic.
