Detection Strategy for Dynamic Resolution using Fast Flux DNS, Detection Strategy DET0485

Archived: 2026-04-05 15:11:14 UTC

AN1331

Identify repeated DNS resolutions where the same domain name returns multiple IPs in short succession, combined with low TTL values and high query volume from unusual processes. Correlate with process lineage (e.g., Office apps spawning abnormal DNS lookups).

Log Sources

Mutable Elements

Field	Description
DNSQueryBurstThreshold	Number of unique IPs returned per domain in a short window
TimeWindow	Adjust correlation timeframe for fast flux detection (e.g., 5–10 minutes)

AN1332

Monitor resolver logs and auditd events for domains resolving to a rotating set of IPs within very short TTL intervals. Correlate high query rates from non-browser applications (e.g., python, curl).

Log Sources

Mutable Elements

Field	Description
TTLThreshold	Minimum TTL value considered suspicious (e.g., < 60 seconds)
DomainReputationFeed	External TI feed to exclude benign CDN or load balancer behavior

AN1333

Use unified logs to identify processes issuing repeated DNS queries where the resolved IP addresses change frequently within very short TTL values. Correlate with outbound network traffic to validate C2-like patterns.

Log Sources

Mutable Elements

Field	Description
DNSRotationRate	Rate of IP churn per domain to trigger detection
NewDomainThreshold	Flag if domain was registered recently (e.g., < 30 days)

AN1334

Monitor ESXi syslog and esxcli outputs for abnormal DNS resolver behavior, such as frequent domain-to-IP changes or unauthorized modifications of DNS settings used by management agents. Correlate domain lookups with short TTL values.

Log Sources

Mutable Elements

Field	Description
ResolverConfigPaths	Whitelist of expected DNS resolvers configured on ESXi
ExternalDomainWhitelist	Known trusted external domains for hypervisor services

---

Source: https://attack.mitre.org/detectionstrategies/DET0485#AN1334