

# Behavioral Detection of DNS Tunneling and Application Layer Abuse, Detection Strategy DET0400

Archived: 2026-04-05 17:02:43 UTC

## AN1121

Detects high-frequency or anomalous DNS queries initiated by non-browser, non-system processes (e.g., PowerShell, rundll32, python.exe) used to establish command and control via DNS tunneling.

### Log Sources

### Mutable Elements

Field	Description
QueryLengthThreshold	Subdomain length for detecting base32/base64-encoded payloads
ProcessImageFilter	Flag non-standard executables making DNS queries
TimeWindow	Rate of queries in short interval per process

## AN1122

Detects local daemons or scripts generating outbound DNS queries with long or frequent subdomains, indicative of DNS tunneling via tools like `iodine`, `dnscat2`, or `dig` from cronjobs or reverse shells.

### Log Sources

### Mutable Elements

Field	Description
SubdomainEntropyScore	Detects encoded payloads or randomness in DNS labels
DaemonAllowList	Allowlisted system daemons expected to perform frequent lookups

## AN1123

Detects scripting environments (AppleScript, osascript, curl) or non-native tools performing DNS queries with encoded subdomains, often used for data exfiltration or beaconing.

### Log Sources

**Mutable Elements**

Field	Description
EntropyThreshold	Tunable threshold for randomness in subdomain labels
UncommonProcessContext	Filters on user-launched or cron-based queries

**AN1124**

Detects clients issuing DNS queries with high volume, long subdomain lengths, encoded payload patterns, or to known malicious infrastructure; indicative of DNS-based C2 channels.

**Log Sources**

**Mutable Elements**

Field	Description
DomainReputationFeed	List of suspicious/malicious C2 domains
QueryRatePerClient	Tunable burst rate per IP per second

**AN1125**

Detects unusual outbound DNS traffic from ESXi hosts, often from shell scripts, custom daemons, or malicious VIBs interacting with external DNS infrastructure outside the management plane.

**Log Sources**

**Mutable Elements**

Field	Description
OutboundDNSVolume	Threshold for data volume and frequency from ESXi IPs
KnownGoodVIBs	Baseline known packages for allowlist comparison

---

Source: <https://attack.mitre.org/detectionstrategies/DET0400#AN1121>