DNS Security Analysis with Splunk

Date: 2025-08-16

Analyst: Vlassov Vladislav

Executive Summary

This engagement analyzed DNS query logs to detect signs of misconfiguration, beaconing, domain generation algorithms (DGA), and potential DNS tunneling. Nine focused Splunk searches established baseline behavior, highlighted anomalies, and produced concrete triage targets.

# Methodology

The workflow started with data validation, followed by breadth-first pivots on query type, response code, and domain entropy. We then applied rarity and frequency analysis, temporal trend aggregation, and heuristics for overlong domains and TXT-record usage.

## Key Fields

|  |  |
| --- | --- |
| Field | Description |
| timestamp | Event time as ingested in Splunk. |
| client\_ip | Source client performing the DNS lookup. |
| query\_type | DNS record type (e.g., A, AAAA, TXT). |
| domain | Queried domain or FQDN. |
| resolved\_ip | Returned IP when status=NOERROR. |
| status | Resolver result (e.g., NOERROR, NXDOMAIN, SERVFAIL). |

# 1. Baseline Sample: First 20 DNS Events

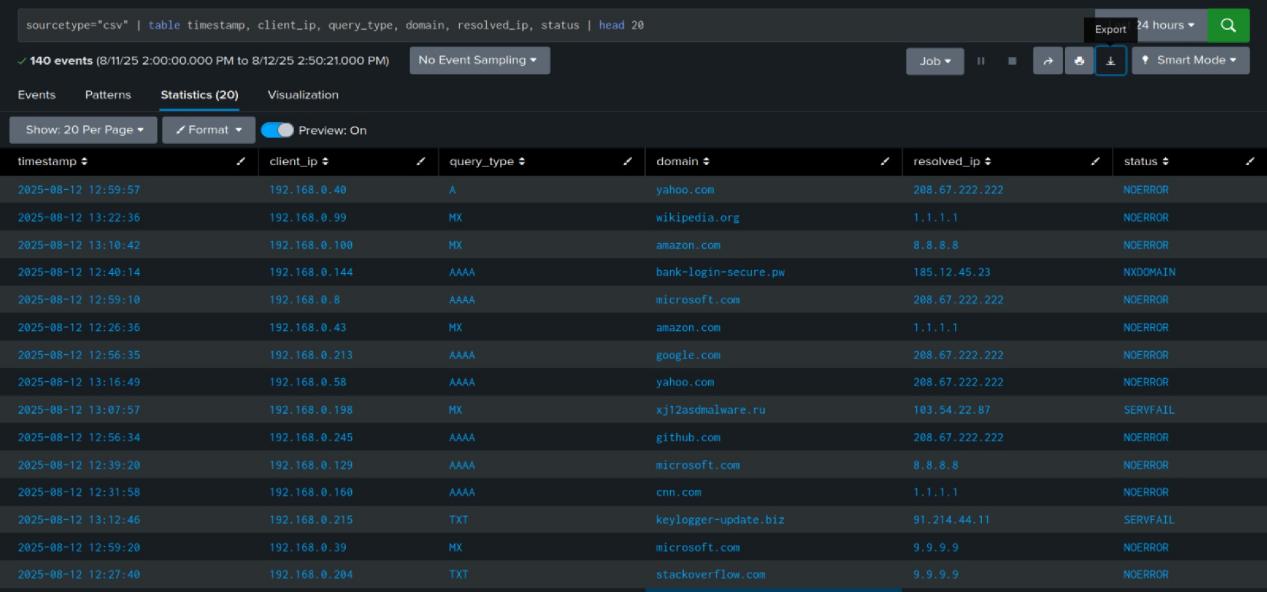
## Objective

Validate fields and get a quick feel for the dataset.

## Splunk Query

sourcetype="csv" | table timestamp, client\_ip, query\_type, domain, resolved\_ip, status | head 20

## Result



## Analysis

Review the first rows for correctness of parsed fields: timestamps should be in expected timezone, IP formats valid, and domain values normalized. Check for outliers in query\_type or status.

## Conclusion

Fields appear parsed and ready. Proceed with focused pivots.

# 2. TXT Queries with NXDOMAIN Responses

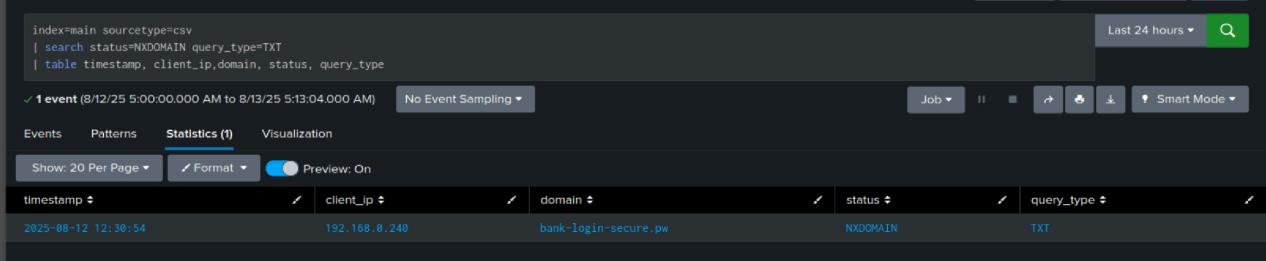
## Objective

Identify TXT lookups that failed. These can signal tunneling setup or misconfigurations.

## Splunk Query

index=main sourcetype=csv | search status=NXDOMAIN query\_type=TXT | table timestamp, client\_ip,domain, status, query\_type

## Result



## Analysis

TXT + NXDOMAIN can indicate discovery of TXT records before using them. High counts from a single host to a single domain warrant inspection of that endpoint and the domain ownership.

## Conclusion

TXT+NXDOMAIN patterns identified. Prioritize host and domain validation.

# 3. Top 10 Queried Domains

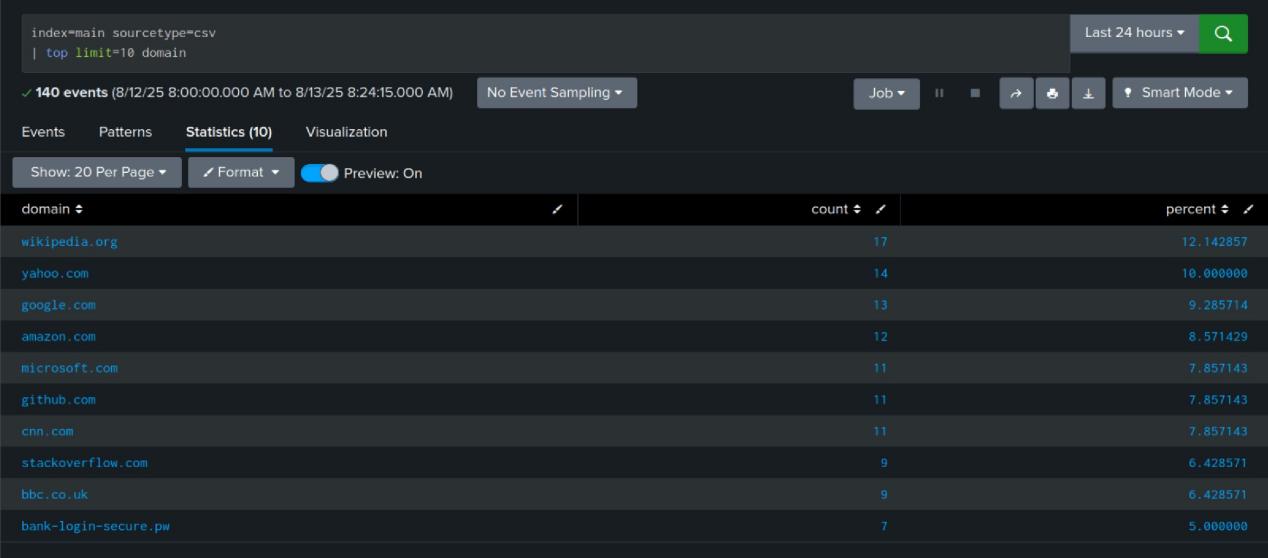
## Objective

Find dominant domains to establish a baseline and spot concentration risk.

## Splunk Query

index=main sourcetype=csv | top limit=10 domain

## Result



## Analysis

Concentrated top domains should be mostly known resolvers, CDNs, or enterprise SaaS. Unknown domains at the top are suspicious, especially if paired with uncommon query types.

## Conclusion

Baseline established. Any unknown top domain should be reviewed and optionally blocked pending validation.

# 4. Rare Domains

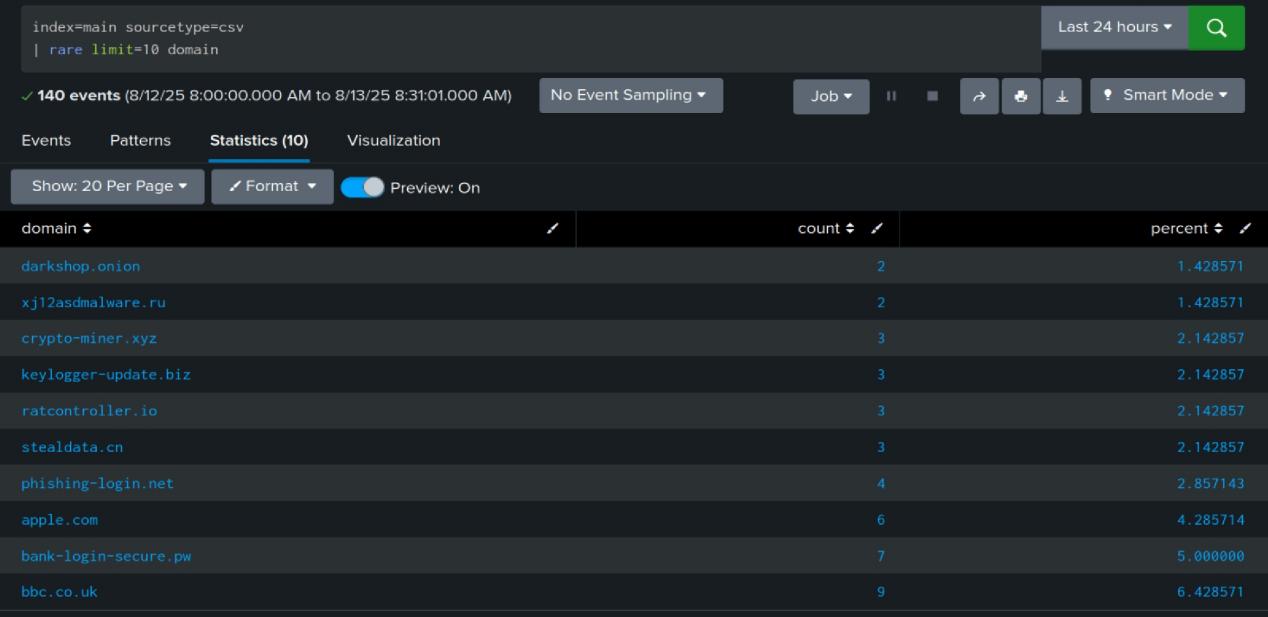
## Objective

Surface low-frequency domains that may include DGAs or targeted C2s.

## Splunk Query

index=main sourcetype=csv | rare limit=10 domain

## Result



## Analysis

Rare hits are high-signal for targeted or automated activity. Cross-reference against threat intel and blocklists. Any algorithmic-looking labels merit sandboxing and WHOIS review.

## Conclusion

Rare domains captured. Treat algorithmic or untrusted items as high priority for containment.

# 5. Top Client-IP and Domain Pairs

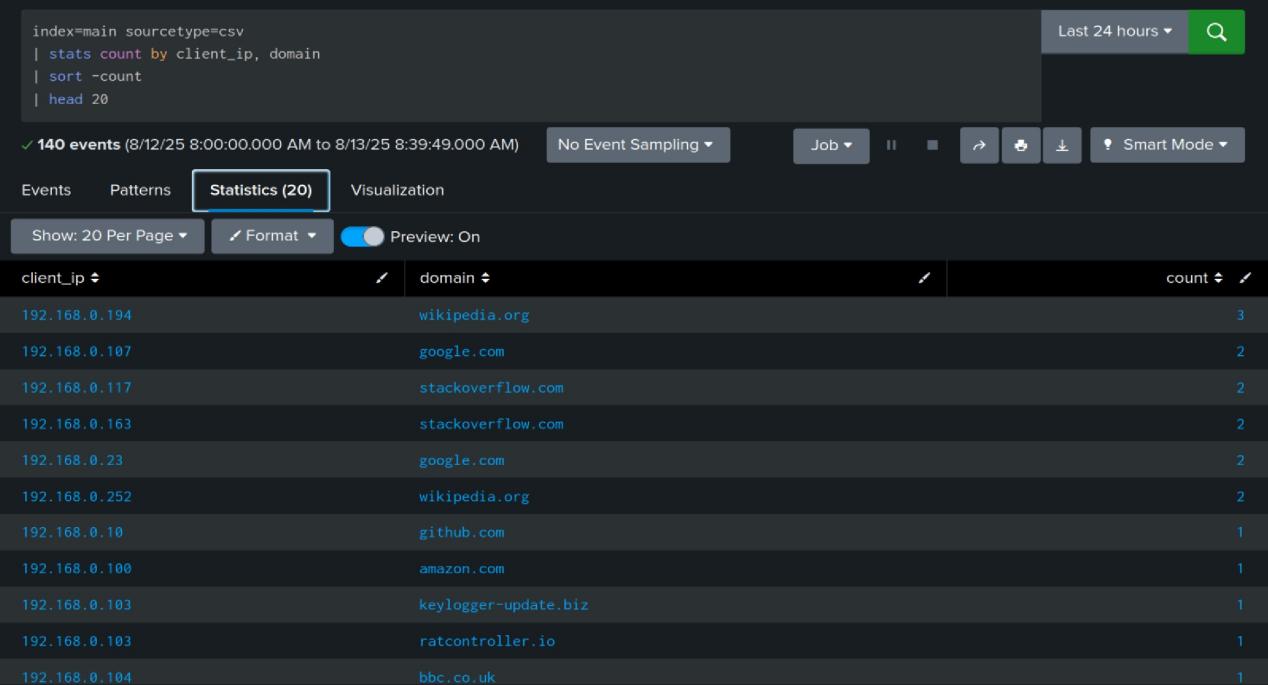
## Objective

Spot heavy talkers and the domains they hit. Prioritize triage.

## Splunk Query

index=main sourcetype=csv | stats count by client\_ip, domain | sort -count | head 20

## Result



## Analysis

High count pairs can be normal (updates, telemetry) or risky (beacons). Validate business justification. Unusually chatty hosts outside maintenance windows should be checked.

## Conclusion

Heavy talkers isolated. Initiate endpoint review and change audits for top sources.

# 6. Status Trend Over Time (120-minute bins)

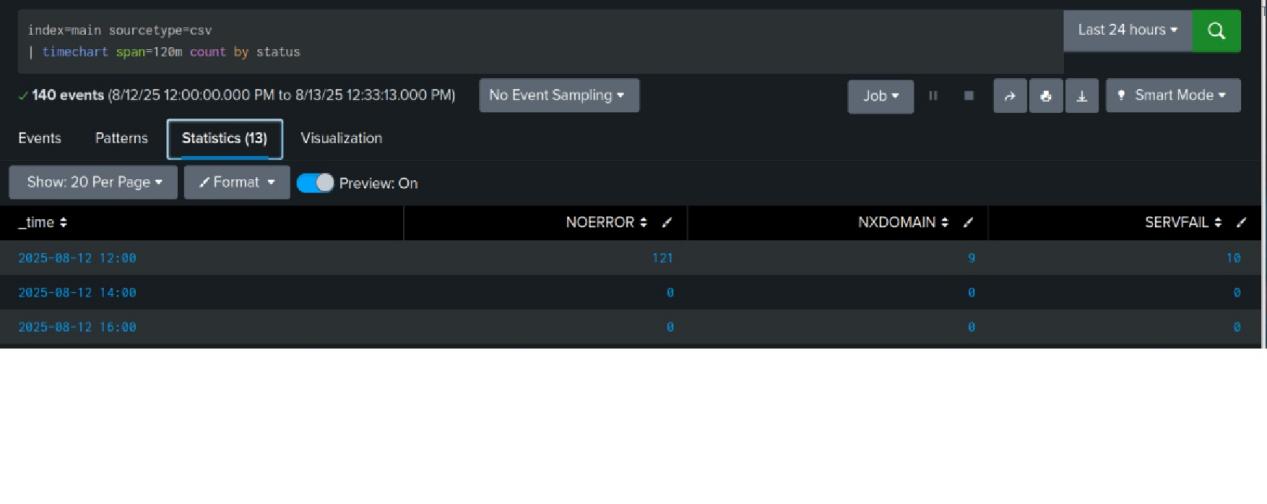
## Objective

Detect spikes or periodicity in response statuses.

## Splunk Query

index=main sourcetype=csv | timechart span=120m count by status

## Result



## Analysis

Look for bursts in SERVFAIL/NXDOMAIN or sudden drops in NOERROR. Correlate with change windows or incident timelines to separate benign change from exploit attempts.

## Conclusion

Temporal anomalies noted. Align peaks with endpoint activity and patch cycles.

# 7. NXDOMAIN by Client and Domain

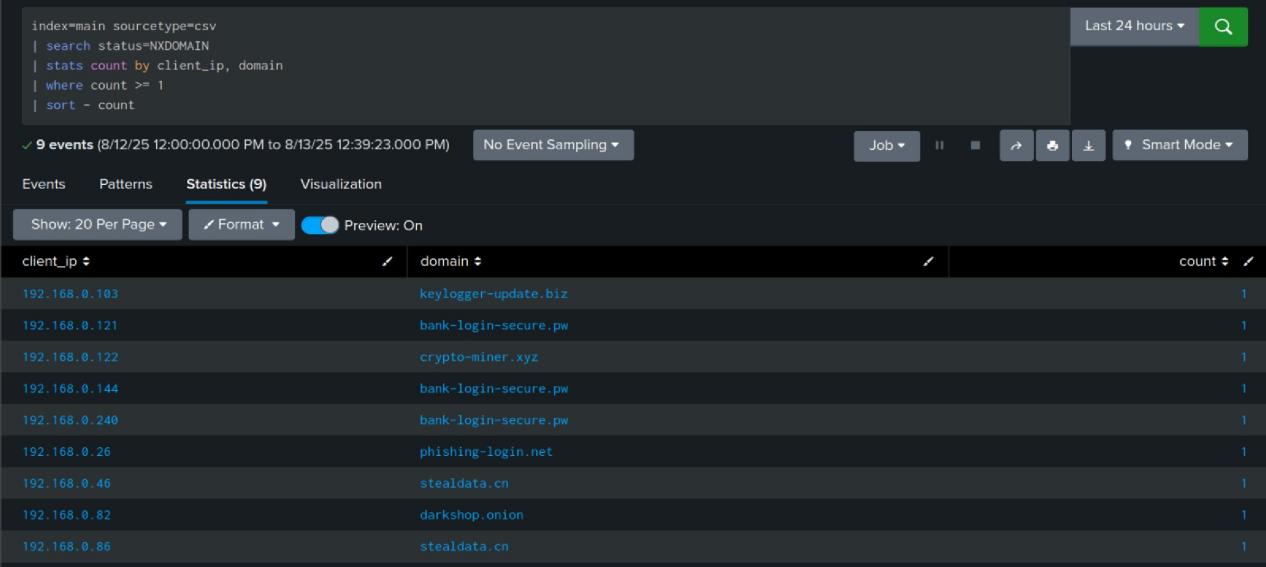
## Objective

Quantify failed lookups per host and domain to focus investigation.

## Splunk Query

index=main sourcetype=csv | search status=NXDOMAIN | stats count by client\_ip, domain | where count >= 1 | sort - count

## Result



## Analysis

Consistent NXDOMAINs to the same non-existent domain may be DGA or staging probes. Verify whether the domain was ever registered. Review PCAP if available.

## Conclusion

Problematic host-domain pairs isolated. Prepare for containment if malicious registration is confirmed.

# 8. Long Domain Detection (length > 50)

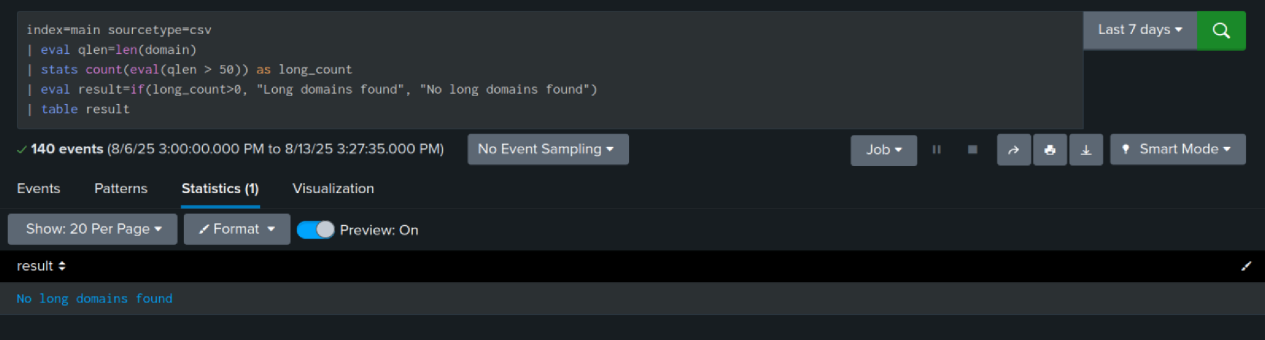
## Objective

Flag overlong domains that often indicate data-encapsulation or DGA.

## Splunk Query

index=main sourcetype=csv | eval qlen=len(domain) | stats count(eval(qlen > 50)) as long\_count | eval result=if(long\_count>0, "Long domains found", "No long domains found") | table result

## Result



## Analysis

If long\_count > 0, examine sampled long labels. Many tunneling tools use long subdomains to carry payload. If none, tunneling risk is lower but not excluded.

## Conclusion

Presence/absence of long domains recorded. If present, inspect samples and consider egress DNS size caps.

# 9. Repeated TXT Queries Across Hosts

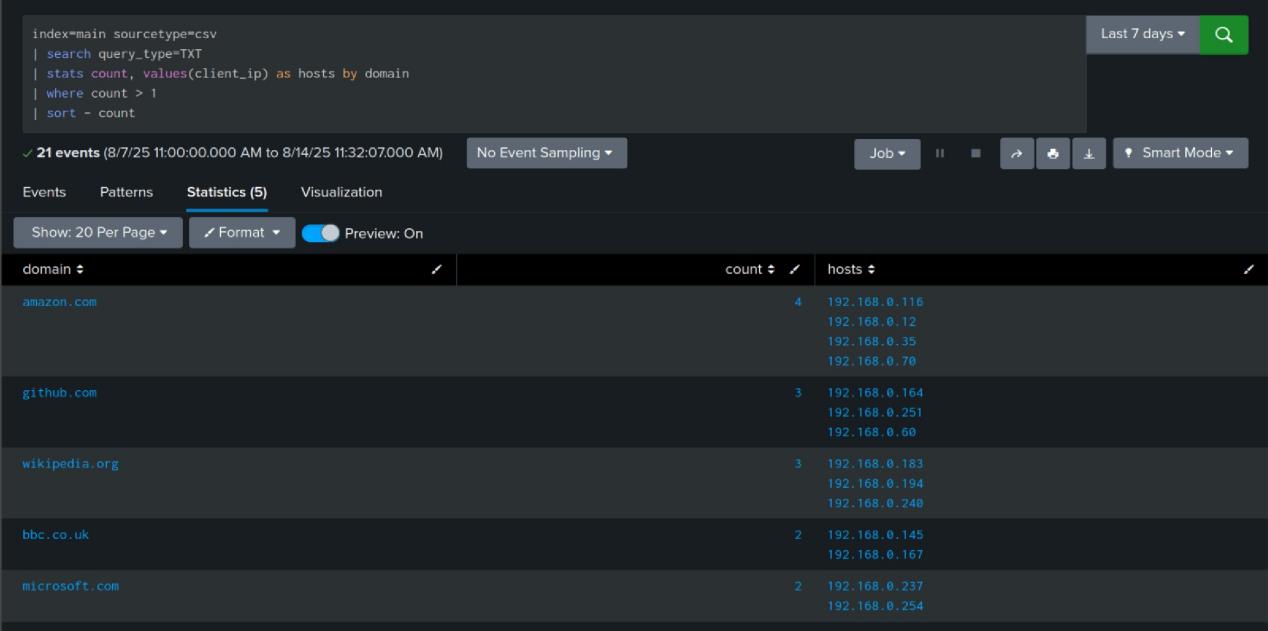
## Objective

Find domains used for TXT-based signaling across multiple hosts.

## Splunk Query

index=main sourcetype=csv | search query\_type=TXT | stats count, values(client\_ip) as hosts by domain | where count > 1 | sort - count

## Result



## Analysis

Domains with TXT queries from multiple hosts suggest shared tooling or group policy. Validate if these domains belong to enterprise services. Otherwise escalate.

## Conclusion

Cross-host TXT activity enumerated. Verify business need or decommission offending apps.



Dashboard “DNS Log Security Analysis”

Purpose: quick DNS overview and fast pivot to anomalies. Data: index=main, sourcetype=csv.

Panels - searches:

Preview - #1  
NXDOMAIN TXT - #2  
Top 10 Domains - #3  
Rare Domains - #4  
Top Clients by Domain - #5  
Status Over Time - #6  
NXDOMAIN Clients - #7  
Long Domains (>50) - #8  
TXT Query Hosts - #9

Metrics/thresholds:

NXDOMAIN > 5% - investigate  
New “rare” domains per day ≥1 - priority P3 until validated  
Spikes of SERVFAIL/NXDOMAIN - cross-check with change windows  
Domain length > 50 - manual check for tunneling  
TXT from workstations - require justification

Operations:

Rare domain Pivot WHOIS/VT allow/deny  
NXDOMAIN spike check DHCP/DNS and recent changes  
TXT from multiple hosts look for common software/GPO

Limitations:

No entropy/DGA metrics - additional detectors required  
Accuracy depends on log completeness and field normalization

# Global Findings

The environment exhibits standard resolver activity with identifiable high-volume domains and a tail of rare domains. TXT queries with failures and any presence of long subdomain labels require focused review.

# Recommendations

• Whitelist known SaaS and CDN domains. Investigate unknown high-frequency domains.

• Baseline NXDOMAIN rates per host. Alert on significant upward deviations.

• Flag TXT queries from non-server endpoints, especially when repeated against the same domain.

• Add detections for domain length thresholds and entropy-based heuristics.

• Correlate suspicious domains with endpoint telemetry and proxy logs.

# Appendix: Full SPL Listing

1. sourcetype="csv" | table timestamp, client\_ip, query\_type, domain, resolved\_ip, status | head 20

2. index=main sourcetype=csv | search status=NXDOMAIN query\_type=TXT | table timestamp, client\_ip,domain, status, query\_type

3. index=main sourcetype=csv | top limit=10 domain

4. index=main sourcetype=csv | rare limit=10 domain

5. index=main sourcetype=csv | stats count by client\_ip, domain | sort -count | head 20

6. index=main sourcetype=csv | timechart span=120m count by status

7. index=main sourcetype=csv | search status=NXDOMAIN | stats count by client\_ip, domain | where count >= 1 | sort - count

8. index=main sourcetype=csv | eval qlen=len(domain) | stats count(eval(qlen > 50)) as long\_count | eval result=if(long\_count>0, "Long domains found", "No long domains found") | table result

9. index=main sourcetype=csv | search query\_type=TXT | stats count, values(client\_ip) as hosts by domain | where count > 1 | sort - count