# DNS Log Analysis/Research/Questions

By: Ryan Stewart

## DNS query logs include:

- Date-Time
- Querying IP, Port
- Query type
- The requested domain

In DNS log analysis, focus on the requested domain and its reputation/category. Analyzing DNS logs could have detected domains used in the "SolarWinds SUNBURST" attack. Investigate:

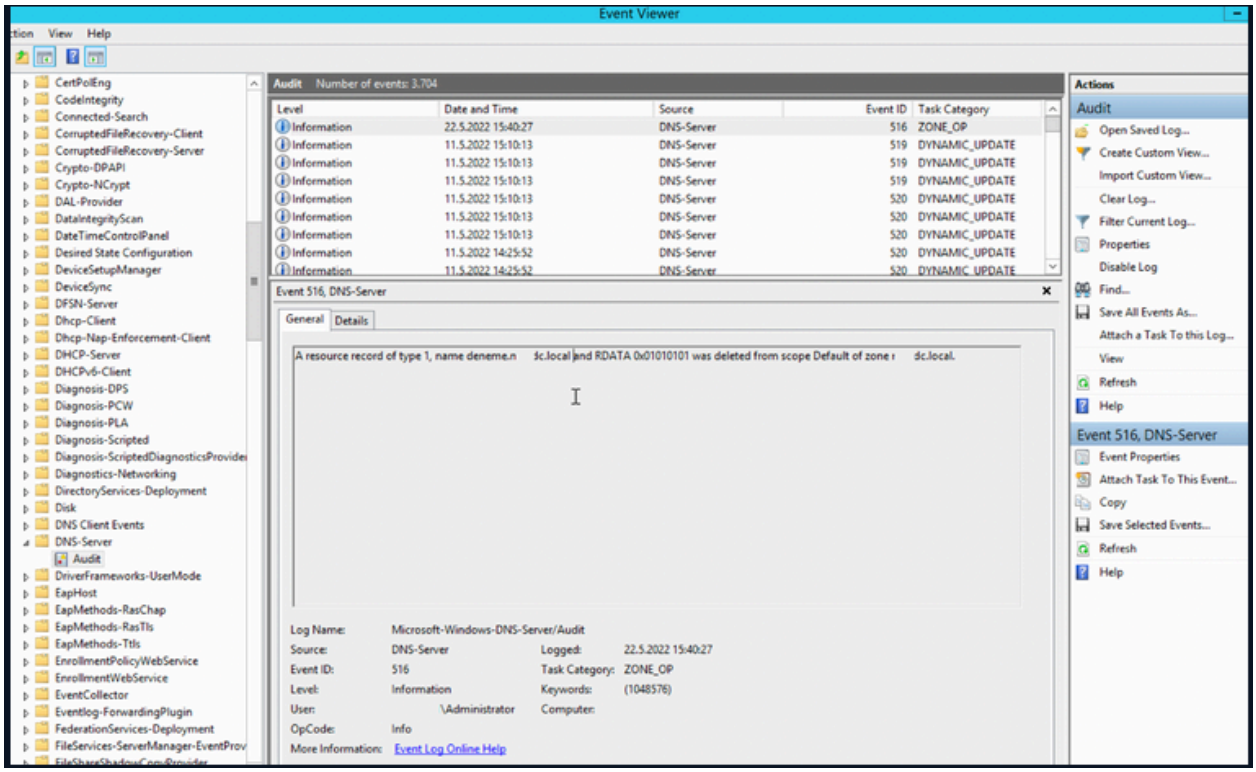
- First-time visited domains
- Domains or subdomains over a certain character size
- Detection of NX returning domains
- Domain IOC controls
- Detection of DNS over TLS, DNS over HTTPS accesses

```
Feb  5 09:13:11 ns1 named[80090]: client 192.168.10.12#3534: query: 4gjygvd3Sg13f77paxsNk7d36ta.tun.mydomain.com IN A
Feb  5 09:13:13 ns1 named[80090]: client 192.168.10.12#3533: query: 3SSc78Hlz454gjygvd5f7l5f7g13f77paxsNk7d36ta.tun.mydomain.com IN A
Feb  5 09:13:17 ns1 named[80090]: client 192.168.10.12#2537: query: zgjyg78Hl5f7g13f77paxsNk7d36ta.tun.mydomain.com IN A
Feb  5 09:13:18 ns1 named[80090]: client 192.168.10.12#2558: query: z454gjygv8Hl5f7g13f77paxsNk7d36ta.tun.mydomain.com IN A
Feb  5 09:13:21 ns1 named[80090]: client 192.168.10.12#3534: query: 7paxsNz454gjygvd3SSc78f7g13f7k7d36ta.tun.mydomain.com IN A
Feb  5 09:13:28 ns1 named[80090]: client 192.168.10.12#2522: query: ygvd3z454gjSSc78Hl5f7g13f77paxsNk7d36ta.tun.mydomain.com IN A
Feb  5 09:13:36 ns1 named[80090]: client 192.168.10.12#3536: query: jygvd3SSz454gc78Hl5f7g13f77paxsNk7d36ta.tun.mydomain.com IN A
Feb  5 09:13:40 ns1 named[80090]: client 192.168.10.12#4536: query: zl5f7g13f77pa7d36ta.tun.mydomain.com IN A
Feb  5 09:13:43 ns1 named[80090]: client 192.168.10.12#2136: query: d36taz454gjygvd3SSc78H3f77paxsNk7.tun.mydomain.com IN A
Feb  5 09:13:48 ns1 named[80090]: client 192.168.10.12#4336: query: Nk7d36tz454gjygvd3SSc78H3f77paxsa.tun.mydomain.com IN A
```

## Example DNS Logs Analysis:

1. Suspicious DNS Tunneling Activity:
    - DNS requests towards randomly created subdomains from IP 192.168.10.12 in 1 minute.
2. Suspicious Oracle Server Activity:
    - DNS queries from Oracle Database server (192.168.10.3) to Microsoft services domains.

DNS log analysis is a valuable tool for detecting potential threats and understanding network activities.




**Quiz Questions:**

**Question 1:** Given DNS Log Entry: Mar 5 19:12:11 ns1 named[80090]: client 172.16.11.34#3261: query: am4wuz3zifexz5u.onion IN A

**Quiz Questions:**

**What could the suspicious activity be at the DNS log above**

A) DNS Proxy

B) DNS Tunnel

C) DNS over HTTPS

D) Access to the TOR network.

**Question 2:** Which of the following is not a DNS record type?

A) MX

B) NS

C) A

D) IP

**Question 3:**

**DNS log;**

*Feb 5 09:12:11 ns1 named[80090]: client 192.168.10.3#3261: query: dns.google IN A*

**Firewall log;**

*date=2022-05-21 time=09:12:13 type="traffic" subtype="forward" srcip=192.168.10.3 srcport=50495 srcintfrole="lan" dstip=8.8.4.4 dstport=853 dstintfrole="wan" proto=6 action="accept"*

**What could the suspicious activity be at the DNS and firewall logs above?**

A) DNS Flood

B) DNS Tunnel

C) DNS over HTTPS

D) DNS Hijacking

*The log entry shows a DNS-over-TLS (DoT) communication from a local device (192.168.10.3) to a Google DNS server (8.8.4.4) on **port 853**. The firewall accepted the traffic. While the activity is generally secure, consider monitoring for deviations from typical DNS patterns, checking the reputation of the destination IP, and ensuring the source IP and port are legitimate. Regularly compare such activities against your network's baseline to detect any anomalies.