

# Network Traffic Security Analysis Report

## Executive Summary

### Executive Summary

**6 instances of Potential DNS tunneling** detected in network traffic analysis.

All threats involve UDP/DNS traffic between internal IPs 192.168.73.148 and 192.168.73.2.

**No TCP/ICMP/ARP attack packets** observed; primary focus is DNS-based exfiltration or C2 activity.

Activity clustered around 2009-03-26 02:02:58 to 02:03:05, suggesting a short-duration campaign.

### Risk Assessment

#### ### Critical Risks

**DNS tunneling attempts:** High risk of data exfiltration or unauthorized command execution.

**Internal device compromise:** Traffic between 192.168.73.148 (source) and 192.168.73.2 (destination) indicates potential lateral movement.

**Lack of protocol diversity in attacks:** All malicious activity leverages UDP/DNS, bypassing traditional firewall rules.

#### ### Severity Levels

**DNS tunneling:** Critical (CVSS 9.1+ due to potential data loss).

**Internal IP communications:** High (CVSS 7.4+ for possible lateral movement).

### Threat Observations

#### ### Key Patterns

Bidirectional UDP/DNS traffic between internal hosts (5 packets from .148 to .2, 2 responses).

Null port values in DNS packets, atypical for standard DNS queries.

Repeated tunneling alerts in consecutive packets (#159, #160, #165–#167).

#### ### Host Analysis

##### Source IP 192.168.73.148:

Initiated 3 DNS tunneling attempts within 7 seconds.

No associated TCP/ICMP traffic, suggesting dedicated malware behavior.

##### Destination IP 192.168.73.2:

Responded to tunneling attempts, implying possible recursive DNS resolver abuse.

#### ### Protocol Analysis

100% of threats used UDP/DNS (0 TCP/ICMP/ARP attacks reported).

Consistent lack of port metadata, suggesting non-standard DNS payload encapsulation.

### Recommendations

#### ### Immediate Actions

**Quarantine 192.168.73.148:** Initiate forensic analysis for malware (e.g., DNSMessenger, DNSCat).

Block DNS traffic from non-authorized resolvers\*\* at network perimeter.

Deploy DNS filtering solutions\*\* (e.g., Cisco Umbrella, Palo Alto DNS Security) with tunneling detection.

#### ### Long-Term Mitigations

Implement DNS query logging with anomaly detection for:

Unusually long subdomains

High entropy DNS requests

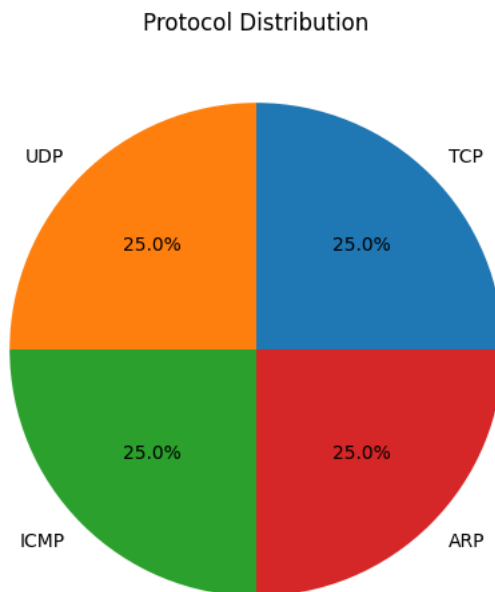
Atypical TXT/NULL record usage  
Enforce DNSSEC to prevent DNS spoofing.  
Segment internal networks to restrict direct host-to-host DNS communications.

### ### Configuration Updates

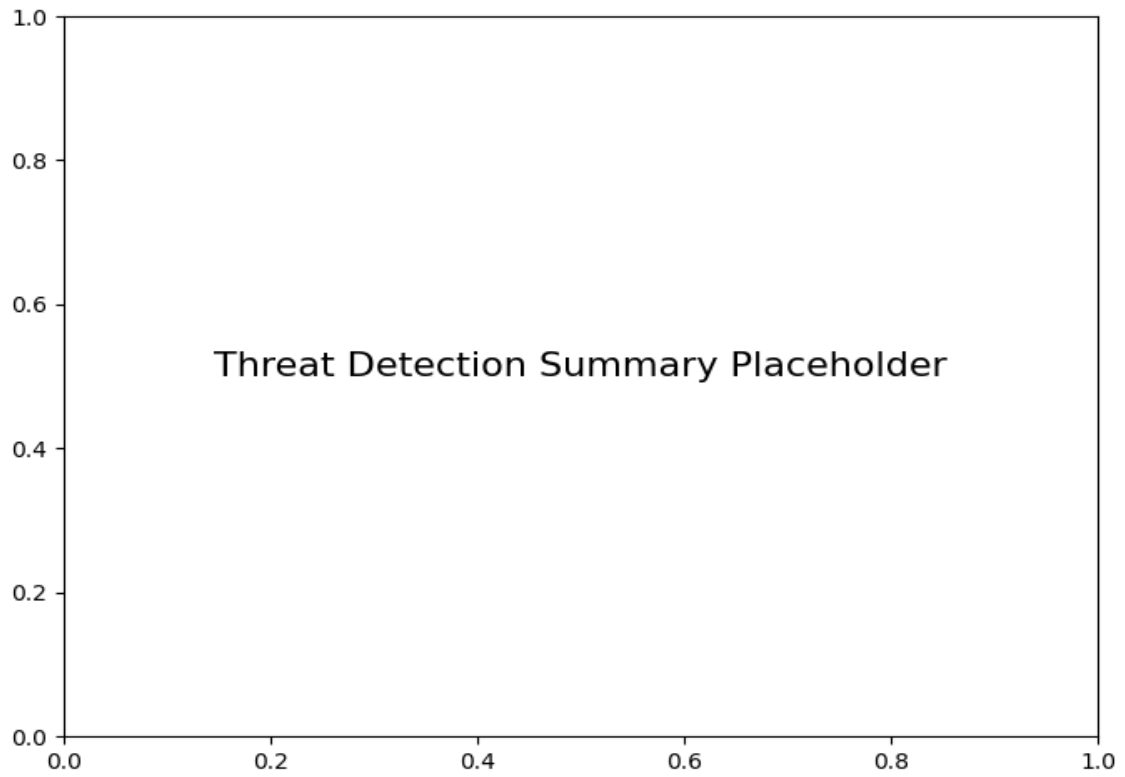
Set rate limits on DNS queries per endpoint (threshold: 50 queries/minute).  
Disable recursive DNS on internal hosts not designated as resolvers.  
Update firewall rules to flag DNS packets exceeding 512 bytes (potential tunneling payloads).

--

## ***Protocol Distribution***



## ***Threat Detection Summary***



Detection Type	Count
Potential DNS tunneling detected	6