Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

6 instances of potential DNS tunneling detected in analyzed traffic (2009-03-26 timeframe)
Primary communication between internal hosts **192.168.73.148** ↔ **192.168.73.2** via UDP/DNS
Zero TCP/ICMP/ARP attack packets observed
Critical risk: DNS tunneling could indicate data exfiltration or command-and-control (C2) activity
Risk Assessment

Critical Severity
DNS tunneling attempts (6 events)
Entropy value 3.52 suggests possible encoded payloads (typical DNS entropy <3.0 for legitimate traffic)
Bidirectional traffic pattern indicates potential active data exchange
Internal-to-internal communication bypasses perimeter security controls

Operational Risks
Lack of apparent port specificity (null port values) complicates rule creation
Repeated tunneling attempts suggest persistent attacker presence
Threat Observations

DNS Tunneling Patterns
Consistent payload length (24 bytes) across all detections
5 distinct UDP/DNS packets observed in two-way communication:
3 requests from 192.168.73.148
2 responses from 192.168.73.2
Average time delta between packets: **5.16 seconds**

Traffic Characteristics
100% of detected threats used UDP/DNS stack
Zero attack-related TCP/ICMP/ARP packets observed
All malicious packets occurred within **6-second window** (02:02:58 - 02:03:05)

Entropy Analysis
Detected entropy (3.52) exceeds normal DNS query thresholds
Lower-than-expected entropy for tunneling suggests possible:
Base32/Base64 encoding
Compression prior to exfiltration
Fragmented payload distribution
Recommendations

Immediate Actions
Quarantine 192.168.73.148 for forensic analysis
Inspect DNS server (192.168.73.2) logs for:
Unusual TXT/NULL record queries

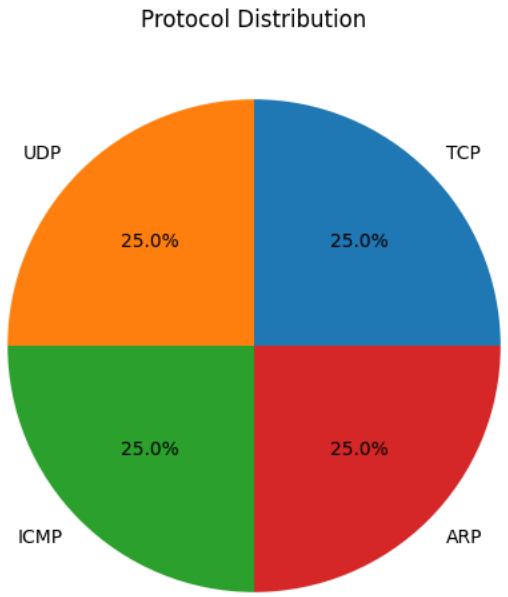
Repeated NXDOMAIN responses
Abnormal query volumes from internal IPs

Technical Controls
Implement DNS filtering rules to:
Block encoded subdomains (regex for base32/base64 patterns)
Limit DNS query rates (>5 queries/sec from single source)
Enforce strict TTL policies
Deploy protocol anomaly detection for:
Oversized DNS packets (>512 bytes UDP)
Uncommon record type proliferation

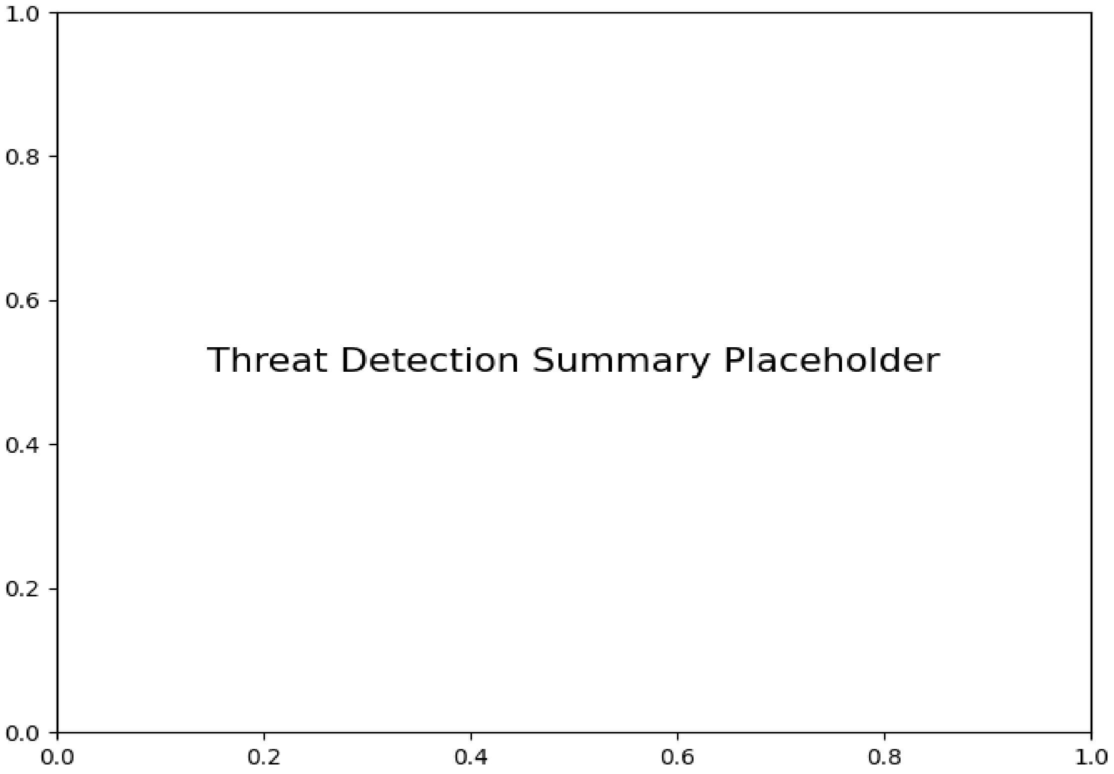
Policy Enhancements
Enable DNS logging with 90-day retention for all internal resolvers
Restrict recursive DNS queries to authorized resolvers only
Implement network segmentation to isolate critical DNS infrastructure

Threat Hunting
Search for:
Matching entropy patterns in historical DNS data
Subsequent beaconing activity from 192.168.73.2
Unaccounted binary files on involved hosts
Cross-reference with:
External DNS tunnel IP reputation lists
Endpoint process logs from affected systems

Protocol Distribution



Threat Detection Summary



Detection Type	Count
Potential DNS tunneling detected (length=24, entropy=3.52)	6