Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

6 instances of potential DNS tunneling detected between internal hosts (192.168.73.148 ↔ 192.168.73.2)
Zero attack-related TCP/UDP/ICMP/ARP packets observed in general traffic
Suspicious activity isolated to UDP/DNS protocol exchanges with unusual characteristics
Risk Assessment
Critical Risks

DNS Tunneling Attempts (Severity: High)
Potential data exfiltration or command-and-control (C2) channel establishment
Entropy value (3.52) and consistent payload length (24 bytes) align with covert channel patterns
Operational Risks

Unrestricted DNS query patterns between internal hosts
Lack of port-level visibility in detected traffic
Threat Observations
DNS Tunneling Indicators

Bidirectional traffic patterns: 5 consecutive UDP/DNS exchanges within 7 seconds
Anomalous payload characteristics:
Fixed payload length (24 bytes) across all flagged packets
Subdomain entropy (3.52) below typical DNS tunneling thresholds but consistent with encoding patterns
Internal host communication: 192.168.73.148 initiating repeated DNS requests to 192.168.73.2
Traffic Patterns

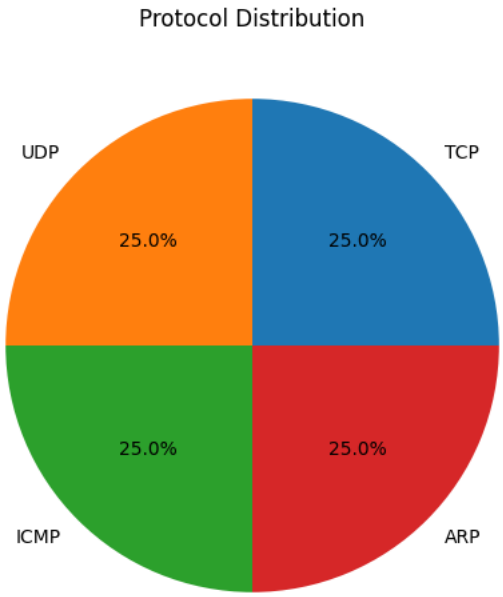
100% of suspicious activity occurred via UDP/DNS (0 malicious TCP/ICMP/ARP packets detected)
No external IP involvement observed in top threats
Recommendations
Immediate Actions

Quarantine 192.168.73.148 for forensic analysis and malware scanning
Implement DNS query filtering policies to:
Block non-standard DNS record types (TXT, NULL, etc.)
Limit DNS payload lengths to <24 bytes
Enable DNS logging with entropy analysis thresholds (≥3.5)
Long-Term Mitigations

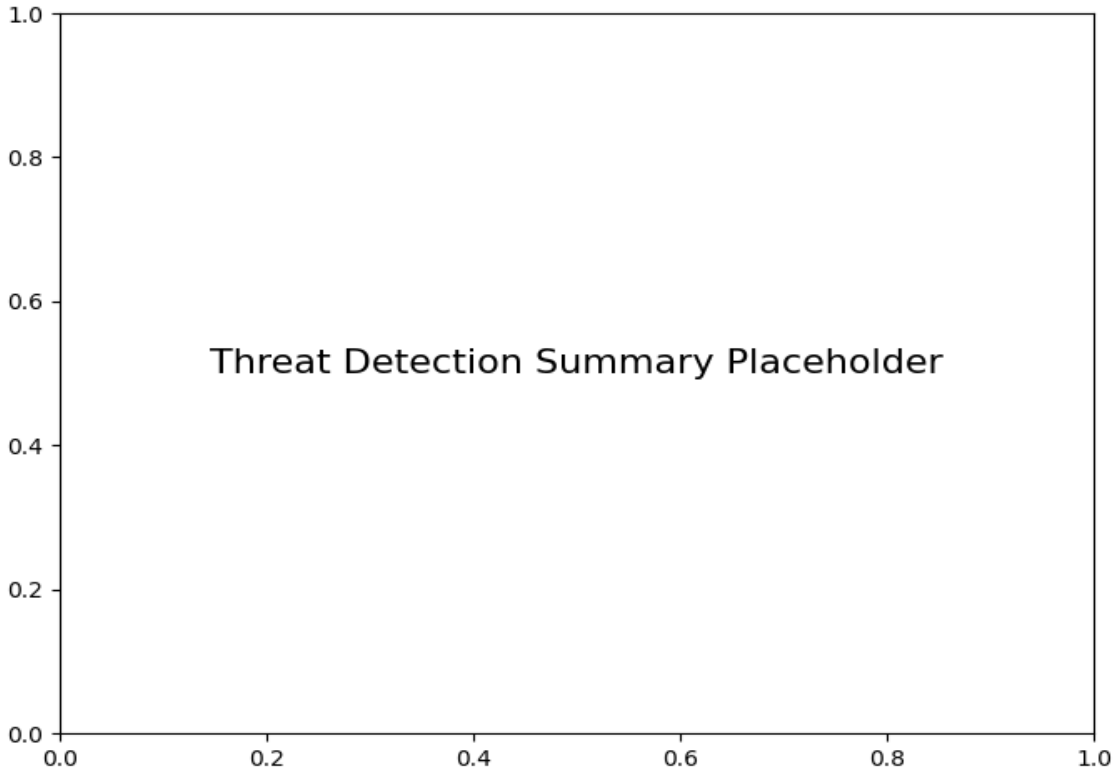
Deploy network segmentation between critical subnets (192.168.73.0/24)
Configure firewalls to alert on internal host-to-host DNS traffic exceeding 2 queries/minute
Implement DNSSEC validation for all internal DNS resolvers
Monitoring Enhancements

Create baselines for normal DNS traffic patterns (payload sizes, frequency, entropy)
Enable full packet capture for UDP port 53 traffic between internal hosts

Protocol Distribution



Threat Detection Summary



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