Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

6 instances of potential DNS tunneling detected in network traffic
Activity observed between internal IPs 192.168.73.148 ↔ 192.168.73.2
No traditional attack patterns detected (0 TCP/UDP/ICMP/ARP attack packets)
Primary risk: Covert data exfiltration/command-and-control via DNS protocol abuse
Risk Assessment
Critical Vulnerabilities

DNS tunneling attempts (Severity: High)
Entropy value 3.52 suggests possible encoded payloads
Repeated 24-byte payloads indicate potential beaconing behavior
Internal host compromise risk (Severity: Medium-High)
Bidirectional malicious DNS traffic between internal hosts suggests lateral movement
Security Posture Indicators

100% of detected threats involved DNS protocol abuse
0 packets flagged in traditional attack categories (TCP/UDP/ICMP/ARP)
Threat Observations
DNS Tunneling Patterns

Consistent payload characteristics across all detections:
Fixed payload length: 24 bytes
Uniform entropy measurement: 3.52
UDP/DNS protocol combination in 100% of cases
Suspicious traffic flow between:
Source: 192.168.73.148 (endpoint device)
Destination: 192.168.73.2 (internal infrastructure)
Temporal Analysis

Burst activity detected within 7-second window (02:02:58 - 02:03:05)
Repeating request-response pattern between same endpoints
Recommendations
Immediate Actions

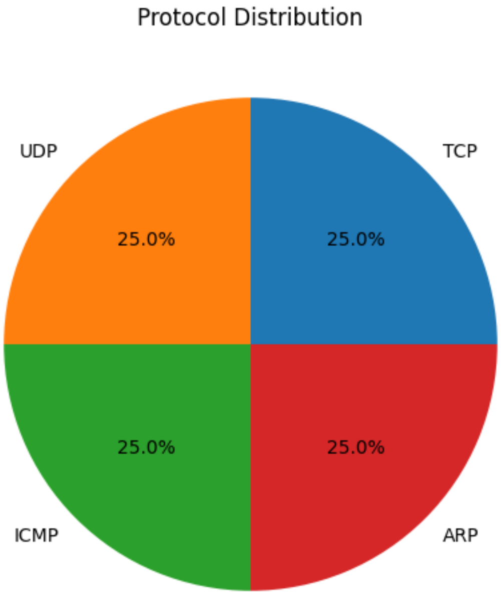
Isolate host 192.168.73.148 for forensic investigation
Implement DNS query logging for both affected IP addresses
Deploy DNS tunneling detection tools (e.g., DNSCat2 detection scripts)
Technical Controls

Enforce DNS policy controls:
Block non-standard DNS query types (TXT, NULL, AXFR)
Implement DNS query length restrictions (< 24 bytes)
Configure network segmentation between client devices and internal DNS servers
Monitoring Enhancements

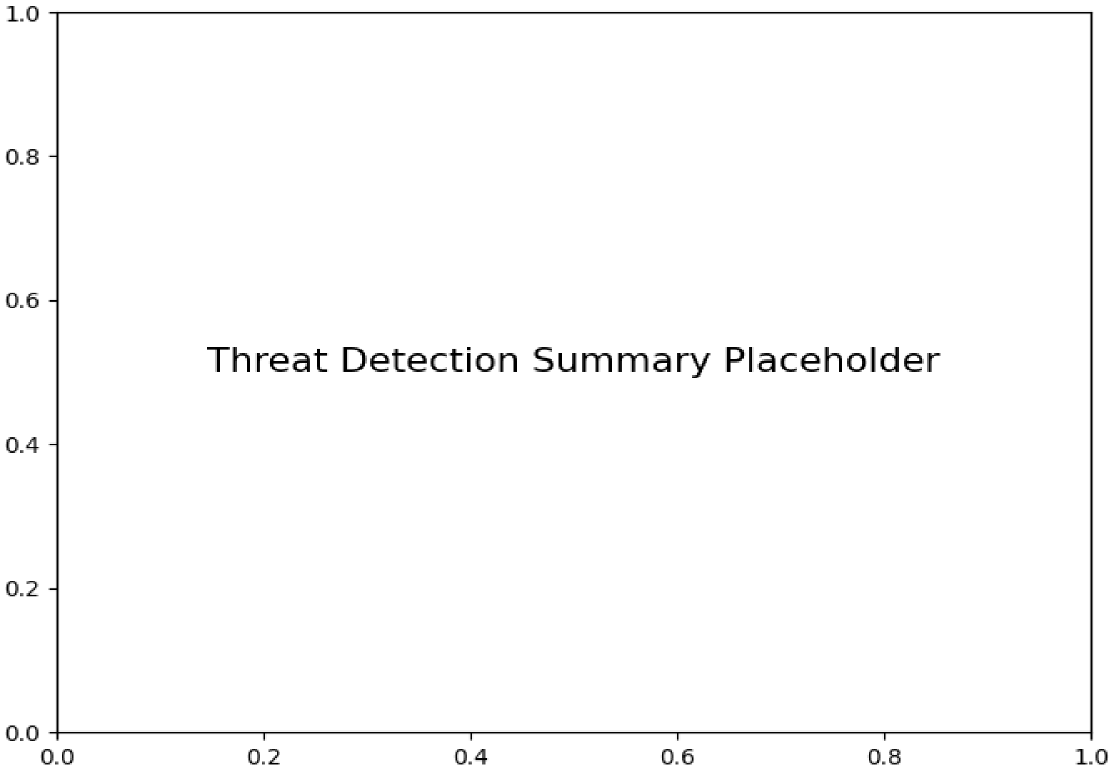
Create IDS/IPS rules targeting:
Repeated DNS queries with identical payload sizes
UDP traffic with entropy thresholds between 3.0-4.0
Implement behavioral baselining for internal DNS traffic patterns
Organizational Measures

Conduct endpoint malware scan on all devices in 192.168.73.0/24 subnet
Review DNS server (192.168.73.2) configuration for cache poisoning vulnerabilities
Initiate user awareness training focused on phishing prevention (common DNS tunneling entry vector)

Protocol Distribution



Threat Detection Summary



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