Network Traffic Security Analysis Report

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

6 instances of potential DNS tunneling detected in traffic analysis
Bidirectional suspicious DNS traffic observed between internal hosts 192.168.73.148 ↔ 192.168.73.2
Zero malicious TCP/ICMP/ARP packets detected across analyzed traffic
Risk Assessment
Critical Risks

DNS tunneling attempts (Severity: High)
Entropy value 3.52 with consistent payload length (24 bytes) suggests possible data exfiltration/command channel
Recurring pattern across 5 consecutive packets indicates sustained malicious activity
Network Protocol Risks

UDP/DNS abuse confirmed as primary attack vector
No observed traditional attack traffic (TCP floods, ARP spoofing, or ICMP anomalies)
Threat Observations
DNS Tunneling Patterns

Consistent characteristics across all detections:
Payload length: 24 bytes
Entropy: 3.52 (suspicious for DNS TXT/Null records)
UDP protocol exploitation
Host Communication Analysis

Primary suspect: 192.168.168.73.148
Initiated 3 outbound DNS requests within 7-second window
Received 2 DNS responses from 192.168.73.2
Temporal Pattern

Burst activity between 02:02:58 and 02:03:05 UTC
Average 2.3 seconds between request/response sequences
Recommendations
Immediate Actions

Quarantine host 192.168.73.148 for forensic analysis
Implement DNS query filtering policies:
Block non-standard DNS record types (TXT, NULL) at network perimeter
Set rate limits for DNS requests per endpoint (max 5 queries/minute)
Technical Controls

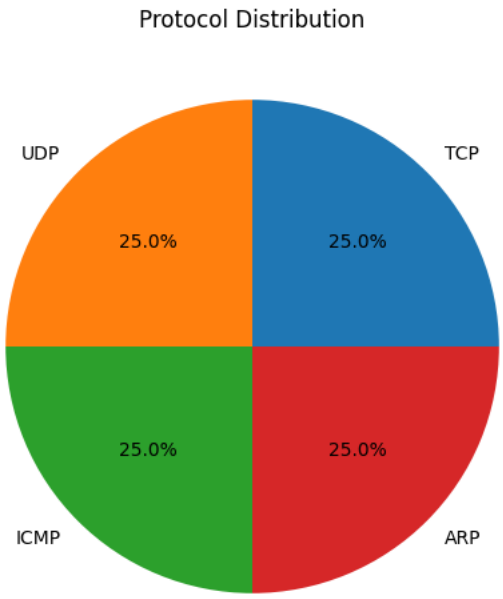
Deploy DNS monitoring solution with:
Entropy-based anomaly detection (threshold >3.0)
Payload length analysis (flag >20 byte DNS payloads)
Enable DNS logging with full query capture

Network Hardening

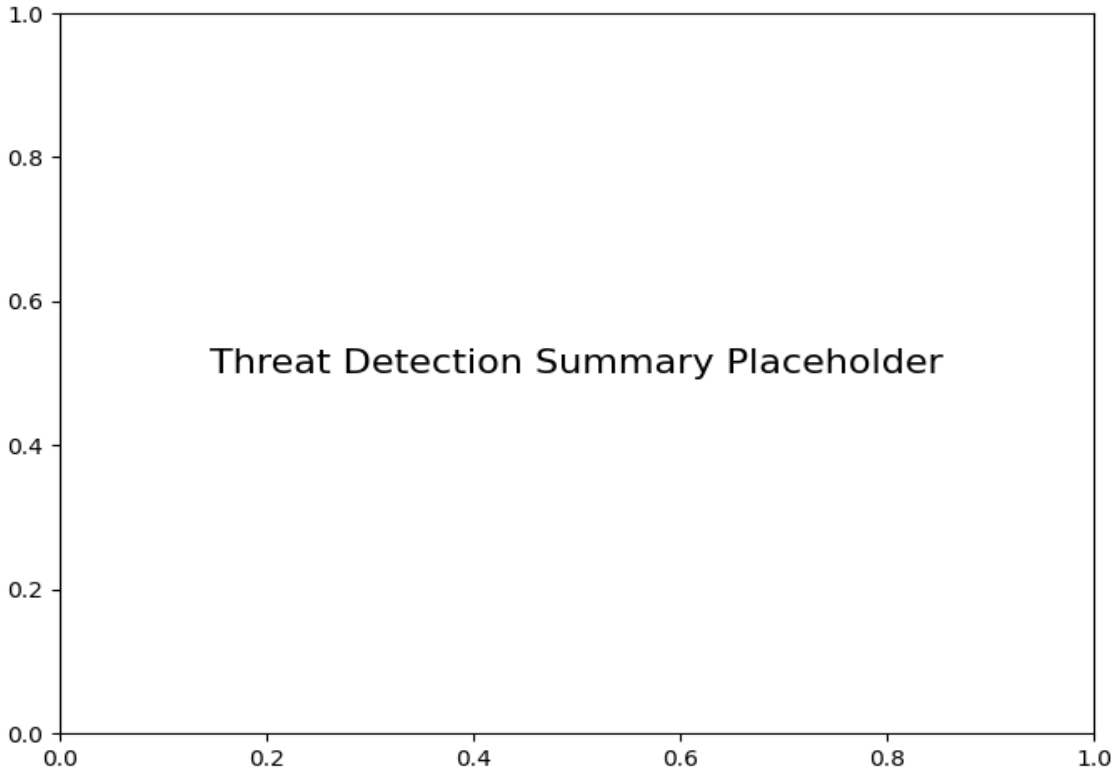
Create firewall rule to block internal DNS traffic between non-authorized servers
Implement DNSSEC validation for all recursive resolvers
Restrict DNS zone transfers to authorized nameservers only
Threat Hunting

Search historical logs for previous activity from 192.168.73.148 to:
Unknown external domains
Dynamic DNS providers
Algorithmically-generated domain names
Conduct endpoint memory analysis on 192.168.73.148 for DNS tunneling tools (dnscat2, iodine, etc.)

Protocol Distribution



Threat Detection Summary



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