

# Network Traffic Security Analysis Report

## Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

**Primary threats detected:** DNS tunneling (10 instances) and ICMP tunneling (14 instances)

**Key concerns:** Multiple high-entropy payloads indicative of potential data exfiltration/covert channels

**Critical internal IPs involved:** 172.20.10.9 (source/destination), 172.20.10.1, 172.20.10.2

**Timeframe:** Concentrated activity between 12:14-12:17 on 2025-03-14

Risk Assessment

**DNS Tunneling (Severity: Critical)**

**2x high-risk patterns:**

Recurring bidirectional traffic between 172.20.10.9 ↔ 172.20.10.1

Multiple query lengths (25-32 bytes) with elevated entropy (3.53-4.00)

**ICMP Tunneling (Severity: Critical)**

**14 identical payload structures:**

Fixed 128-byte payloads with extreme entropy (6.43-6.58)

Originating from 172.20.10.2 to 172.20.10.9

Threat Observations

DNS Anomalies

**Suspicious query characteristics:**

6 distinct detection patterns across 10 events

Packet #226-227 (12:14) and #236-237 (12:15) show request/response tunneling patterns

Unusually long subdomains (25-32 characters) for TXT/Null records

ICMP Anomalies

**Tunneling indicators:**

128-byte payloads exceed normal ICMP error message sizes

Shannon entropy values (6.43-6.58) suggest encrypted/compressed content

Sustained traffic from 172.20.10.2 (Packet #254 and 13 similar events)

Protocol Analysis

**0 TCP/UDP/ARP packets** in attack stats suggest:

Exclusive use of "allowed" protocols (DNS/ICMP) for evasion

Potential encrypted payloads bypassing traditional packet inspection

Recommendations

**1. Immediate Containment:**

Quarantine 172.20.10.2 and 172.20.10.9 for forensic investigation

Block ICMP payloads >64 bytes at network perimeter

**2. DNS Hardening:**

Implement DNS query length restrictions (max 20 characters)

Deploy anomaly detection for high-entropy DNS queries (threshold: entropy >3.2)

**3. ICMP Mitigation:**

Enable ICMP type/code whitelisting (allow only echo request/reply)  
Deploy payload entropy analysis for ICMP traffic

4. **Network Segmentation:**

Restrict internal device communication via firewall policies  
Implement east-west traffic monitoring for lateral movement

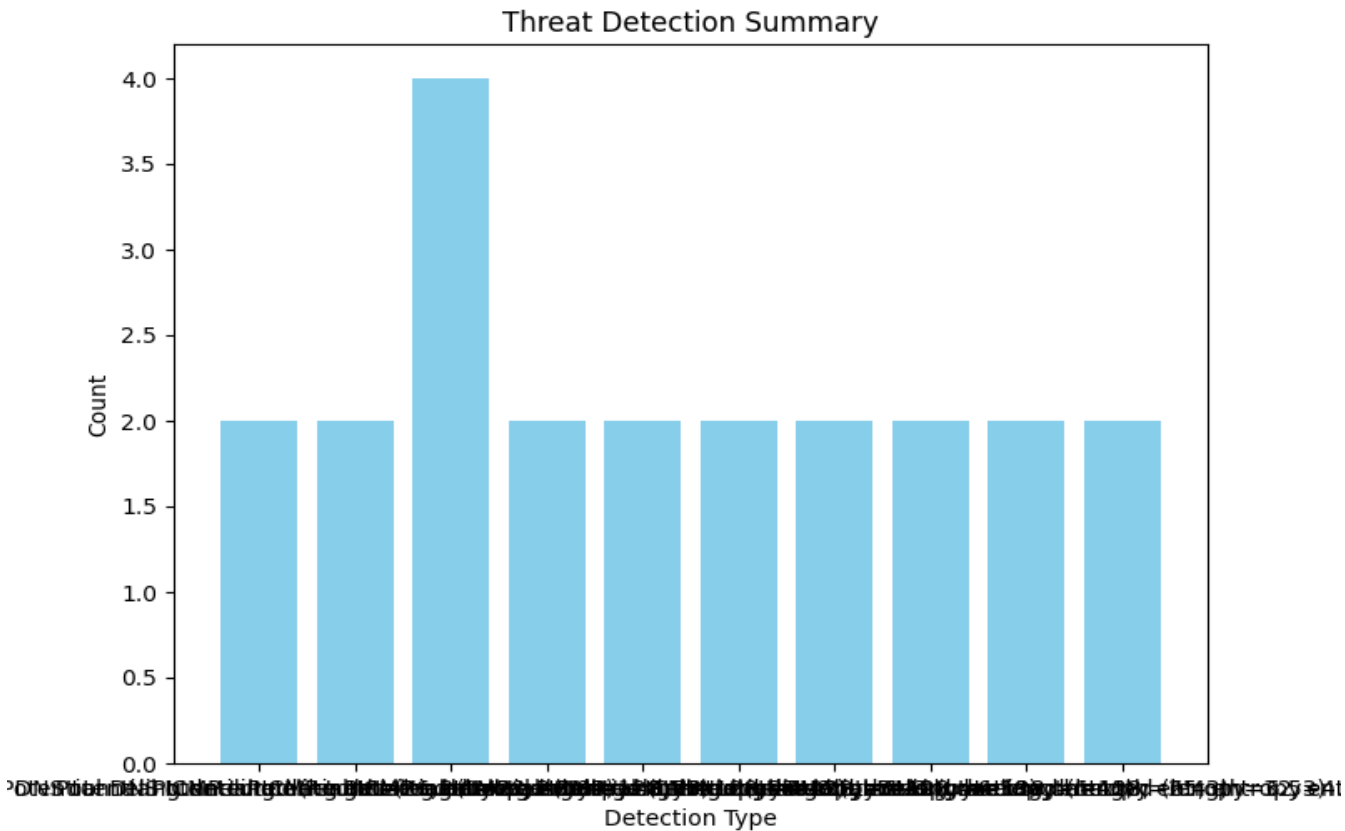
5. **Threat Hunting:**

Review historical DNS logs from 172.20.10.1 (potential recursive resolver abuse)  
Analyze 172.20.10.2 for process-level ICMP tunnel artifacts (ping -d anomalies)

6. **IDS/IPS Updates:**

Create signatures for repeated ICMP payloads with entropy >6.0  
Enable DNS tunneling detection rules (e.g., domain generation algorithm patterns)

**Threat Detection Summary**



Detection Type	Count
Potential DNS tunneling detected (length=26, entropy=3.84)	2
Potential DNS tunneling detected (length=28, entropy=3.53)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.48)	4
Potential ICMP tunneling detected (byte length=128, entropy=6.49)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.58)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.46)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.43)	2
Potential ICMP tunneling detected (byte length=128, entropy=6.53)	2
Potential DNS tunneling detected (length=25, entropy=4.00)	2
Potential DNS tunneling detected (length=32, entropy=3.80)	2