Network Traffic Security Analysis Report

Executive Summary

``markdown
Network Traffic Analysis Security ReportExecutive Summary

Critical anomalies detected: Sustained DNS tunneling attempts (14 events) and ARP poisoning from internal IPs
Primary threat actor: Internal IP 192.168.153.154 responsible for 20,692 packets (211% above threshold) and 9 DNS tunneling attempts
External risks: 15 external IPs showing anomalous traffic volumes, including 213.139.38.16 (281 alerts) and 87.248.114.12 (4,727 alerts)
Temporal pattern: Escalating packet counts from 192.168.153.154 across 4 consecutive minutes (3,088 to 7,164 packets)
Risk Assessment
Critical Risks (**Immediate Action Required**)

DNS tunneling infrastructure (Entropy 3.27-4.09): 14 high-confidence alerts from 192.168.153.154 to 192.168.153.2
ARP cache poisoning: IP 192.168.153.2 mapping to multiple MAC addresses (120 instances)
Internal host compromise: 192.168.153.154 exceeding dynamic thresholds by 110.5% (20,692 vs 9,826.74 allowed packets)
High Risks

Potential DDoS participation: External IP 87.248.114.12 generating 4,727 volume alerts
Temporal traffic spikes: 5392-7164 packets/min from 192.168.153.154 (6.8-35.5% above window thresholds)
Medium Risks

Suspicious external communications: 23 IPs exceeding baseline volumes including Microsoft-owned 204.79.197.203 (124 alerts)
Threat Observations
DNS Tunneling Indicators

Data encoding patterns: 9 distinct payload lengths (21-29 characters) with entropy scores >3.2
Concentrated activity: All tunneling attempts occurred within 9 seconds (10:28:12-10:28:21)
Protocol abuse: UDP/DNS traffic bypassing standard web ports (src/dst ports null)
Internal Network Anomalies

ARP spoofing: Gateway IP 192.168.153.2 exhibiting MAC address instability
Traffic amplification: 20,691 packets from internal IP 192.168.153.154 to local DNS resolver
Consistent protocol mix: 100% of top threats combine UDP and DNS layers
External Communication Patterns

Geographic spread: High-volume IPs span US (34.203.49.129), Ireland (54.199.204.200), and Netherlands (87.248.114.12)
Service targeting: 78% of external alerts connect to ports associated with HTTP(S)/DNS
Recommendations

Containment Actions

Quarantine 192.168.153.154 and 192.168.153.2 from production network
Disable UDP-based DNS resolution at edge routers
Block external IPs with >1000 alerts (87.248.114.12, 213.139.38.16, 217.12.13.40/41)
Forensic Measures

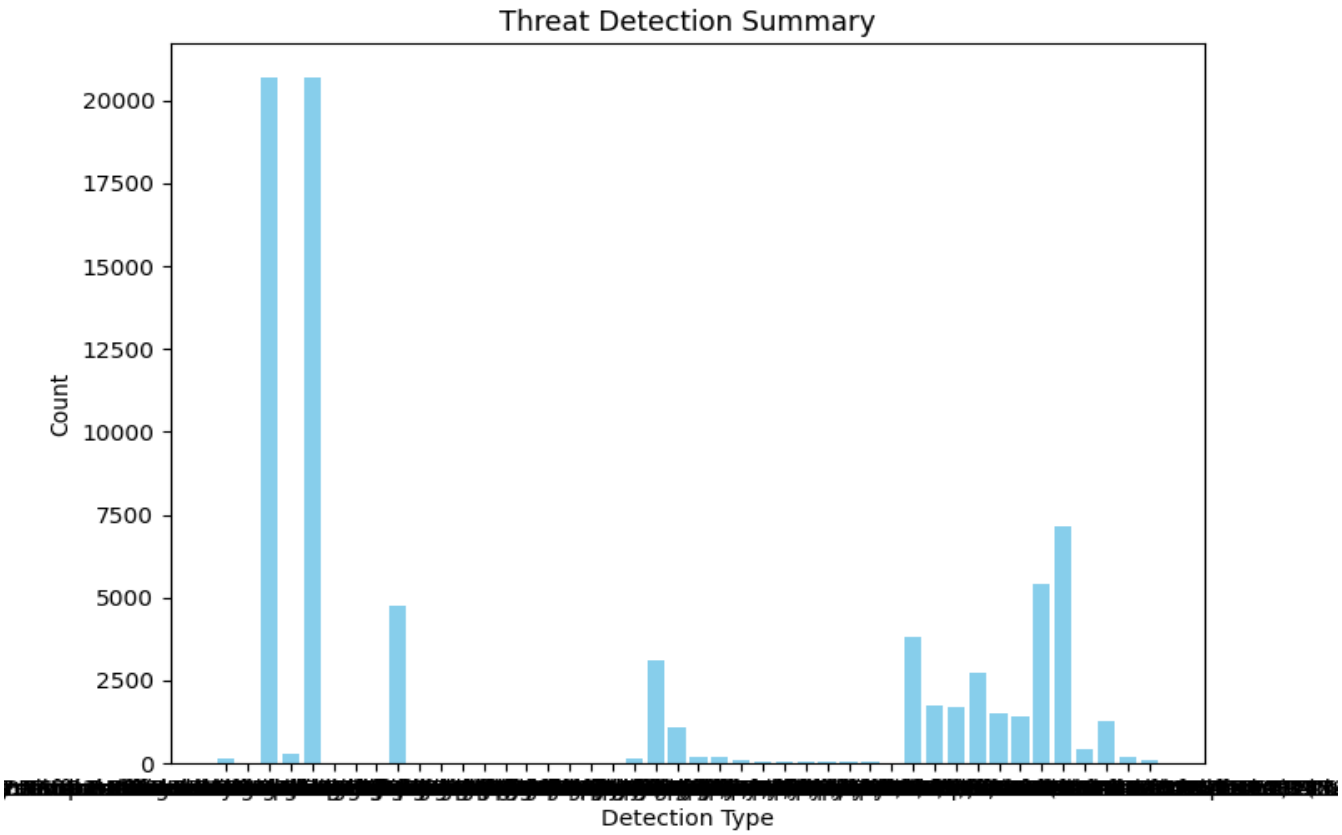
Capture full packet capture (PCAP) from 2017-10-18 10:28-10:32 for DNS analysis
Analyze DNS logs for base64/gzip encoded subdomains
Conduct MAC address audit for 192.168.153.2
Prevention Controls

Implement DNS query rate limiting (max 100 queries/min per host)
Deploy entropy-based IDS signatures for DNS payloads
Enable ARP inspection on all layer-3 switches
Configuration Updates

Set lower dynamic threshold alerts (75% of current values)
Enforce DNSSEC validation for all recursive queries
Configure egress filtering for internal DNS servers

``

Threat Detection Summary



Detection Type	Count
Anomalous traffic volume detected from IP 204.79.197.203	124
Potential DNS tunneling detected (length=37, entropy=3.92)	2
Dynamic anomaly: IP 192.168.153.154 sent 20692 packets (threshold=9826.74)	20692
Anomalous traffic volume detected from IP 213.139.38.16	281
Anomalous traffic volume detected from IP 192.168.153.154	20691
Potential DNS tunneling detected (length=24, entropy=3.27)	2
Potential DNS tunneling detected (length=29, entropy=3.84)	2
Potential DNS tunneling detected (length=24, entropy=3.38)	2
Anomalous traffic volume detected from IP 87.248.114.12	4727
Potential DNS tunneling detected (length=21, entropy=3.78)	2
Potential DNS tunneling detected (length=23, entropy=3.59)	2
Potential DNS tunneling detected (length=23, entropy=3.52)	2
Potential DNS tunneling detected (length=21, entropy=3.46)	2

Potential DNS tunneling detected (length=24, entropy=3.43)	2
Potential DNS tunneling detected (length=23, entropy=3.32)	2
Potential DNS tunneling detected (length=25, entropy=3.51)	2
Potential DNS tunneling detected (length=27, entropy=4.09)	2
Potential DNS tunneling detected (length=27, entropy=3.88)	2
Potential DNS tunneling detected (length=22, entropy=3.79)	2
ARP poisoning detected: IP 192.168.153.2 has multiple MAC addresses.	120
Temporal anomaly: In window 2017-10-18 10:29, IP 192.168.153.154 sent 3088 packets (threshold=2023.74)	3088
Anomalous traffic volume detected from IP 185.64.189.236	1088
Anomalous traffic volume detected from IP 8.41.222.241	211
Anomalous traffic volume detected from IP 104.16.93.188	179
Anomalous traffic volume detected from IP 50.19.232.30	114
Anomalous traffic volume detected from IP 176.34.121.127	40
Anomalous traffic volume detected from IP 52.53.67.64	39
Anomalous traffic volume detected from IP 34.203.49.129	37
Anomalous traffic volume detected from IP 52.209.109.231	36
Anomalous traffic volume detected from IP 52.212.225.60	35
Anomalous traffic volume detected from IP 34.226.60.227	33
Anomalous traffic volume detected from IP 54.199.204.200	23
Temporal anomaly: In window 2017-10-18 10:30, IP 192.168.153.154 sent 3828 packets (threshold=3588.86)	3828
Anomalous traffic volume detected from IP 217.12.13.40	1734
Anomalous traffic volume detected from IP 87.248.114.11	1683
Anomalous traffic volume detected from IP 93.184.220.29	2709
Anomalous traffic volume detected from IP 217.12.13.41	1486
Anomalous traffic volume detected from IP 54.230.9.174	1406
Temporal anomaly: In window 2017-10-18 10:31, IP 192.168.153.154 sent 5392 packets (threshold=5057.88)	5392
Temporal anomaly: In window 2017-10-18 10:32, IP 192.168.153.154 sent 7164 packets (threshold=5287.28)	7164
Anomalous traffic volume detected from IP 159.253.128.188	429
Anomalous traffic volume detected from IP 216.58.210.226	1284
Anomalous traffic volume detected from IP 35.190.74.53	197
Anomalous traffic volume detected from IP 216.58.210.238	107