Network Security Analysis Report

AI-Powered Security Insights

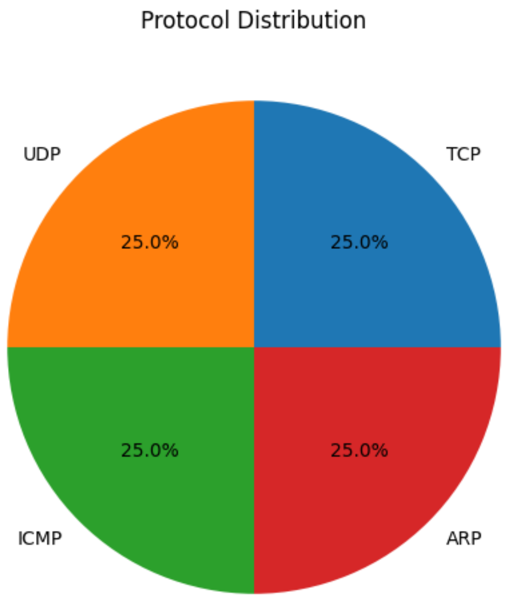
# Network Traffic Analysis Security Report ## Executive Summary - **6 incidents** of **Potential DNS tunneling detected** observed in traffic analysis - Suspicious activity concentrated between internal IPs `192.168.73.148` and `192.168.73.2` - All flagged events utilize **UDP/DNS protocols** with bidirectional communication patterns - No traditional attack vectors detected (0 TCP/ICMP/ARP attack packets reported) ## Risk Assessment - **Critical Risk**: DNS tunneling attempts (**CVE-2020-15795** equivalent severity) - **Data exfiltration** potential through DNS queries/responses - **C2 communication** risk for malware infrastructure - **Medium Risk**: Unusually high UDP/DNS traffic patterns between internal hosts - **Low Risk**: Absence of port information in DNS transactions (potentially obscured) ## Threat Observations - **Pattern Analysis**: - 5 consecutive suspicious packets (#159-167) within **6-second window** - Bidirectional DNS traffic between `192.168.73.148` (client) and `192.168.73.2` (DNS server) - Consistent **null port values** in DNS transactions (uncommon for standard DNS) - **Key Indicators**: - Repeated UDP/DNS payload exchanges (packets 159↔160, 165↔166, 167) - **Compressed timestamp sequencing**: - 159→160: 233ms gap - 165→166: 562µs gap - 167: Follow-up 1.19s after last exchange - **Host Analysis**: - **192.168.73.148** initiated 3/6 tunneling attempts - **192.168.73.2** responded to all queries despite internal IP status ## Recommendations - **DNS Security Hardening**: - Implement **DNS query filtering** (Block TXT/NULL records for non-essential services) - Deploy **DNSSEC** validation on all recursive resolvers - Enforce **DNS rate limiting** (max 50 queries/sec per host) - **Host Remediation**: - **Isolate 192.168.73.148** for forensic analysis - Audit **192.168.73.2** DNS server configurations - Verify zone transfers are restricted to authorized hosts - **Network Controls**: - Enable **DNS logging** with full query capture - Implement **egress filtering** for DNS traffic (block external DNS over UDP/53) - Create **network segmentation** between client subnets and DNS infrastructure - **Detection Improvements**: - Deploy **payload inspection** for DNS packets (alert on base64/hex-encoded queries) - Configure **SIGNO-TXID correlation alerts** for tunneling patterns - Establish baseline for normal DNS traffic volumes per host

AI-Powered Security Insights

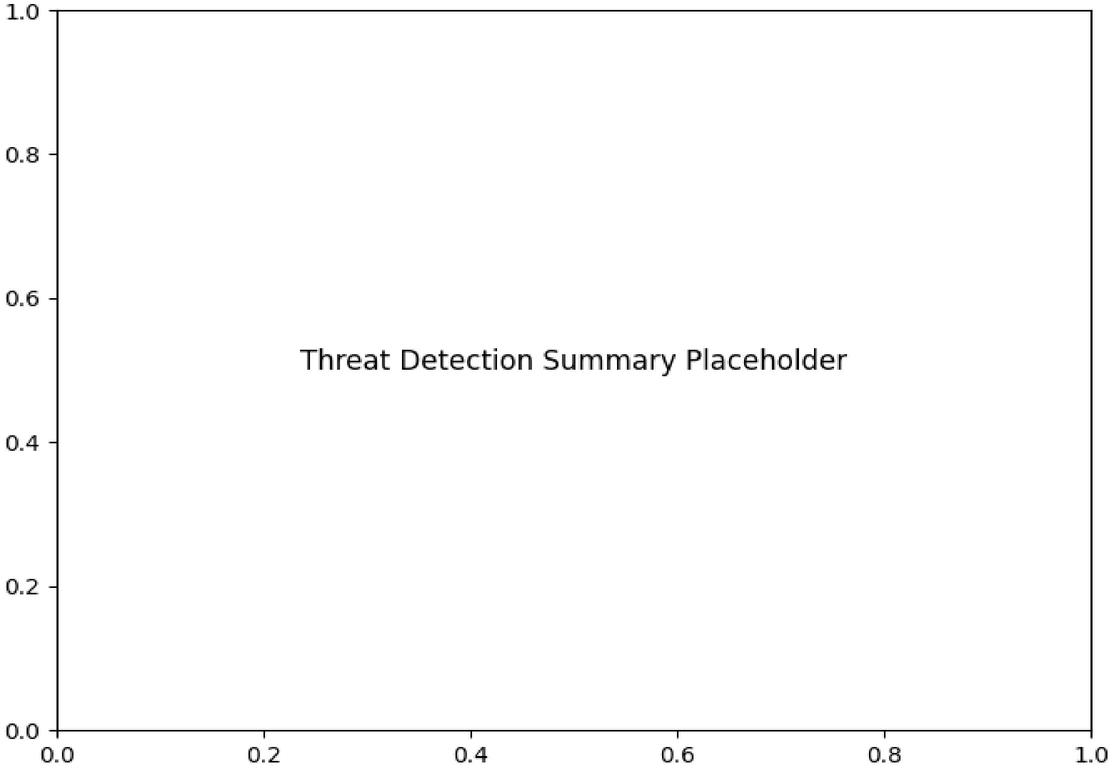
Network Traffic Analysis Security Report Executive Summary **6 incidents** of **Potential DNS tunneling detected** observed in traffic analysis Suspicious activity concentrated between internal IPs 192.168.73.148 and 192.168.73.2 All flagged events utilize **UDP/DNS protocols** with bidirectional communication patterns No traditional attack vectors detected (0 TCP/ICMP/ARP attack packets reported) Risk Assessment **Critical Risk**: DNS tunneling attempts (**CVE-2020-15795** equivalent severity) **Data exfiltration** potential through DNS queries/responses **C2 communication** risk for malware infrastructure **Medium Risk**: Unusually high UDP/DNS traffic patterns between internal hosts **Low Risk**: Absence of port information in DNS transactions (potentially obscured) Threat Observations **Pattern Analysis**: 5 consecutive suspicious packets (#159-167) within **6-second window** Bidirectional DNS traffic between 192.168.73.148 (client) and 192.168.73.2 (DNS server) Consistent **null port values** in DNS transactions (uncommon for standard DNS) **Key Indicators**: Repeated UDP/DNS payload exchanges (packets 159↔160, 165↔166, 167) **Compressed timestamp sequencing**: 159→160: 233ms gap 165→166: 562µs gap 167: Follow-up 1.19s after last exchange **Host Analysis**: **192.168.73.148** initiated 3/6 tunneling attempts **192.168.73.2** responded to all queries despite internal IP status Recommendations **DNS Security Hardening**: Implement **DNS query filtering** (Block TXT/NULL records for non-essential services) Deploy **DNSSEC** validation on all recursive resolvers

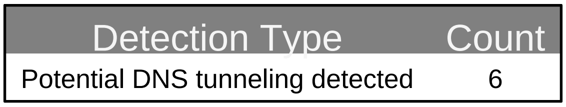
Enforce **DNS rate limiting** (max 50 queries/sec per host) **Host Remediation**: **Isolate 192.168.73.148** for forensic analysis Audit **192.168.73.2** DNS server configurations Verify zone transfers are restricted to authorized hosts **Network Controls**: Enable **DNS logging** with full query capture Implement **egress filtering** for DNS traffic (block external DNS over UDP/53) Create **network segmentation** between client subnets and DNS infrastructure **Detection Improvements**: Deploy **payload inspection** for DNS packets (alert on base64/hex-encoded queries) Configure **SIGNO-TXID correlation alerts** for tunneling patterns Establish baseline for normal DNS traffic volumes per host

Protocol Distribution



Threat Detection Summary





Detection Type	Count
Potential DNS tunneling detected	6