

Network Traffic Security Analysis Report

Overall Threat Assessment



Table of Contents

Placeholder for table of contents	0
-----------------------------------	---

Executive Summary

Network Traffic Analysis Security ReportExecutive Summary

3 TCP connect scans detected from internal IP 192.168.73.148 to external Google IPs (64.233.169.104, 74.125.45.100).

6 DNS tunneling attempts observed between 192.168.73.148 and 192.168.73.2, indicating potential data exfiltration.

No direct attack packets (TCP/UDP/ICMP/ARP) observed, but reconnaissance and covert channel activities detected.

Risk Assessment

High Severity Risks

TCP SYN scans with abnormal window sizes (>1024): Suggests **network reconnaissance** or **port scanning** from an internal host (192.168.73.148).

DNS tunneling (entropy=3.52): Indicates **potential data exfiltration** or **command-and-control (C2) communication** via DNS queries.

Moderate Severity Risks

Repeated UDP/DNS traffic between internal hosts (192.168.73.148 ↔ 192.168.73.2) warrants investigation for **covert channels**.

Threat Observations

TCP Connect Scans

Source IP: 192.168.73.148 (internal)

Target IPs: 64.233.169.104 (Google), 74.125.45.100 (Google)

Technique: SYN packets with **abnormally large window sizes (>1024)**—common in **stealth scans** to bypass basic detection.

Timing: Scans occurred within a **30-second window** (02:02:13 to 02:02:41), suggesting automated probing.

DNS Tunneling Indicators

High entropy (3.52) in DNS packets, atypical for legitimate DNS traffic.

Bidirectional traffic between 192.168.73.148 and 192.168.73.2, indicating possible **data exchange**.

Length=24: Short but suspicious payloads, often used in **DNS tunneling tools** like DNSCat2.

Recommendations

Immediate Actions

Isolate 192.168.73.148: Investigate for **compromise** or **malicious insider activity**.

Block outbound DNS from unauthorized hosts: Restrict DNS queries to approved resolvers.

Deploy IDS/IPS rules to flag:

SYN scans with window size >1024.

High-entropy DNS packets (threshold: entropy >3.0).

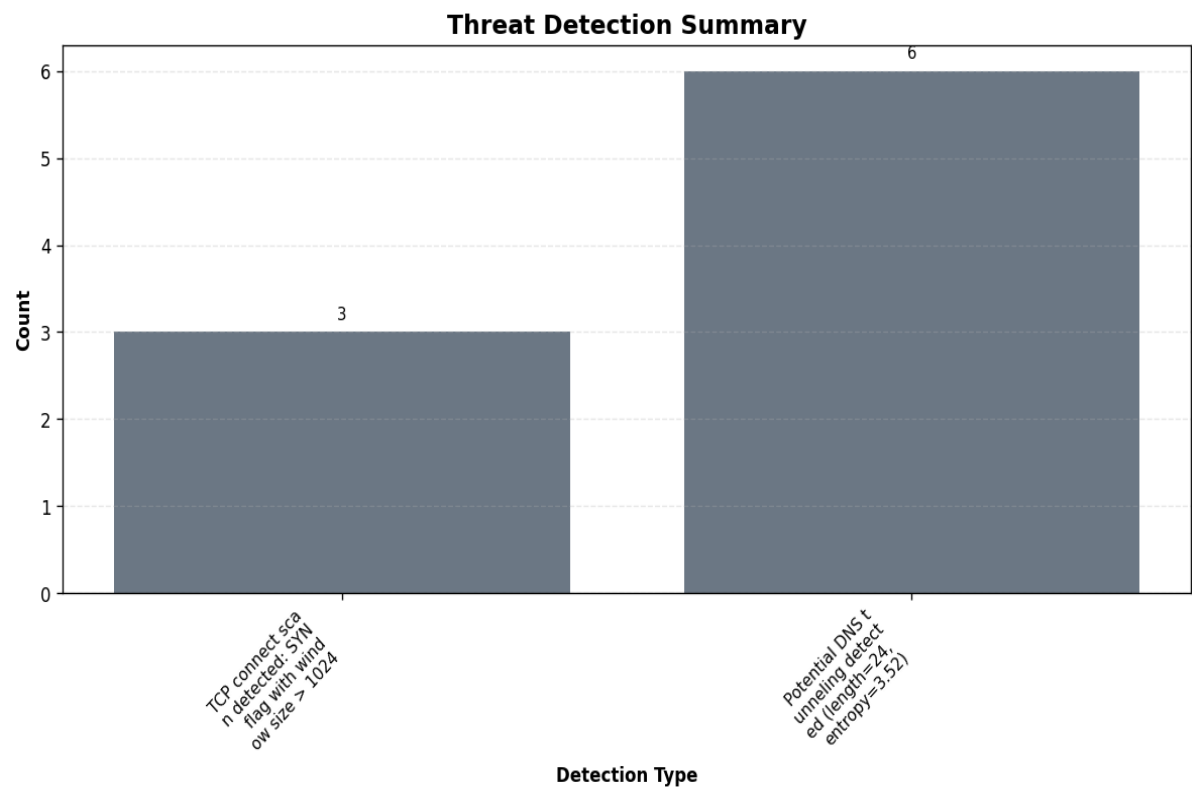
Long-Term Mitigations

Enable DNS logging: Monitor for **unusual query patterns** (e.g., long subdomains, TXT records).

Conduct endpoint forensics on 192.168.73.148 for malware (e.g., C2 beacons, tunneling tools).

Implement network segmentation: Limit internal host communication to reduce lateral movement risks.

Threat Detection Summary



Detection Details

Detection Type	Count
TCP connect scan detected: SYN flag with window size > 1024	3
Potential DNS tunneling detected (length=24, entropy=3.52)	6

Source/Destination Analysis

IP Address	As Source	As Destination	Total
192.168.73.148	4	1	5
64.233.169.104	0	2	2
74.125.45.100	0	1	1

192.168.73.2	1	1	2
--------------	---	---	---

Event Timeline

Time	Packet #	Protocol	Detection
02:02:13.074	1	TCP	TCP connect scan detected: SYN flag with window size > 1024
02:02:33.647	8	TCP	TCP connect scan detected: SYN flag with window size > 1024
02:02:41.721	55	TCP	TCP connect scan detected: SYN flag with window size > 1024
02:02:58.910	159	UDP, DNS	Potential DNS tunneling detect ed (length=24, entropy=3.52)
02:02:59.143	160	UDP, DNS	Potential DNS tunneling detect ed (length=24, entropy=3.52)

Appendix: Raw Traffic Analysis Data

```
{
  "detection_counts": {
    "TCP connect scan detected: SYN flag with window size > 1024": 3,
    "Potential DNS tunneling detected (length=24, entropy=3.52)": 6
  },
  "attack_stats": {
    "tcp_packets": 0,
    "udp_packets": 0,
    "icmp_packets": 0,
    "arp_packets": 0
  },
  "top_threats": [
    {
      "packet_number": 1,
      "timestamp": "2009-03-26T02:02:13.074226",
      "minute": "2009-03-26 02:02",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.73.148",
      "dst_ip": "64.233.169.104",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    },
    {
      "packet_number": 8,
      "timestamp": "2009-03-26T02:02:33.647367",
      "minute": "2009-03-26 02:02",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.73.148",
      "dst_ip": "64.233.169.104",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    },
    {
      "packet_number": 55,
      "timestamp": "2009-03-26T02:02:41.721536",
      "minute": "2009-03-26 02:02",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.73.148",
      "dst_ip": "74.125.45.100",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    },
    {
      "packet_number": 159,
      "timestamp": "2009-03-26T02:02:58.910572",
```

```
    "minute": "2009-03-26 02:02",
    "protocols": [
      "UDP",
      "DNS"
    ],
    "src_ip": "192.168.73.148",
    "dst_ip": "192.168.73.2",
    "src_port": null,
    "dst_port": null,
    "detection_details": [
      "Potential DNS tunneling detected (length=24, entropy=3.52)"
    ]
  },
  {
    "packet_number": 160,
    "timestamp": "2009-03-26T02:02:59.143110",
    "minute": "2009-03-26 02:02",
    "protocols": [
      "UDP",
      "DNS"
    ],
    "src_ip": "192.168.73.2",
    "dst_ip": "192.168.73.148",
    "src_port": null,
    "dst_port": null,
    "detection_details": [
      "Potential DNS tunneling detected (length=24, entropy=3.52)"
    ]
  }
]
```

This report was automatically generated by DeepSeek AI

Filename: security_report_20250422_002620.pdf

SHA-256 Hash: e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855

Generated on: 2025-04-22 00:26:55