Network Traffic Security Analysis Report

Overall Threat Assessment

Threat Level: 10/10

Table of Contents

Executive Summary

``markdown
Executive Summary

129 instances of TCP connect scans detected originating from internal IP 192.168.153.154 targeting multiple external IP addresses (e.g., Microsoft-owned 204.79.197.203, 204.79.197.200, CDN/cloud IPs).
Activity occurred within a **1-minute window** (2017-10-18 05:28), indicating a rapid reconnaissance campaign.
Zero direct attack packets observed (TCP/UDP/ICMP/ARP), suggesting this was a preliminary network probing phase.
Risk Assessment

Critical Risk:

Mass TCP SYN scans indicate active network mapping for vulnerability discovery. Window size >1024 suggests potential **evasion of legacy IDS systems** that flag default window sizes.
Internal IP (192.168.153.154) as source implies **compromised device or insider threat**.

High Risk:

Targeting of Microsoft and CDN infrastructure (151.101.121.108, 213.139.38.16) suggests intent to probe cloud services or exploit known vulnerabilities.

Threat Observations

Scan Pattern:

5 distinct outbound connections in 1 minute, all with SYN flags and abnormal window sizes (>1024).
Consistent absence of src_port/dst_port in logs indicates potential **obfuscation of scan targets**.

Source Behavior:

Single internal host (192.168.153.154) scanning geographically diverse external IPs, consistent with automated tools like Nmap (-sS scan).

Protocol Focus:

100% TCP-based activity; no UDP/ICMP/ARP anomalies detected.

Recommendations

Immediate Actions:

Quarantine source IP 192.168.153.154 for forensic analysis (check for malware, unauthorized accounts, or lateral movement).
Update firewall rules to **block outbound SYN packets with window size >1024** to disrupt this scan pattern.

Network Hardening:

Deploy IDS/IPS signatures targeting TCP Window Size Anomalies (e.g., Suricata rule window_size:>1024;).
Implement **egress filtering** to restrict internal devices from initiating unsanctioned outbound SYN floods.

Threat Hunting:

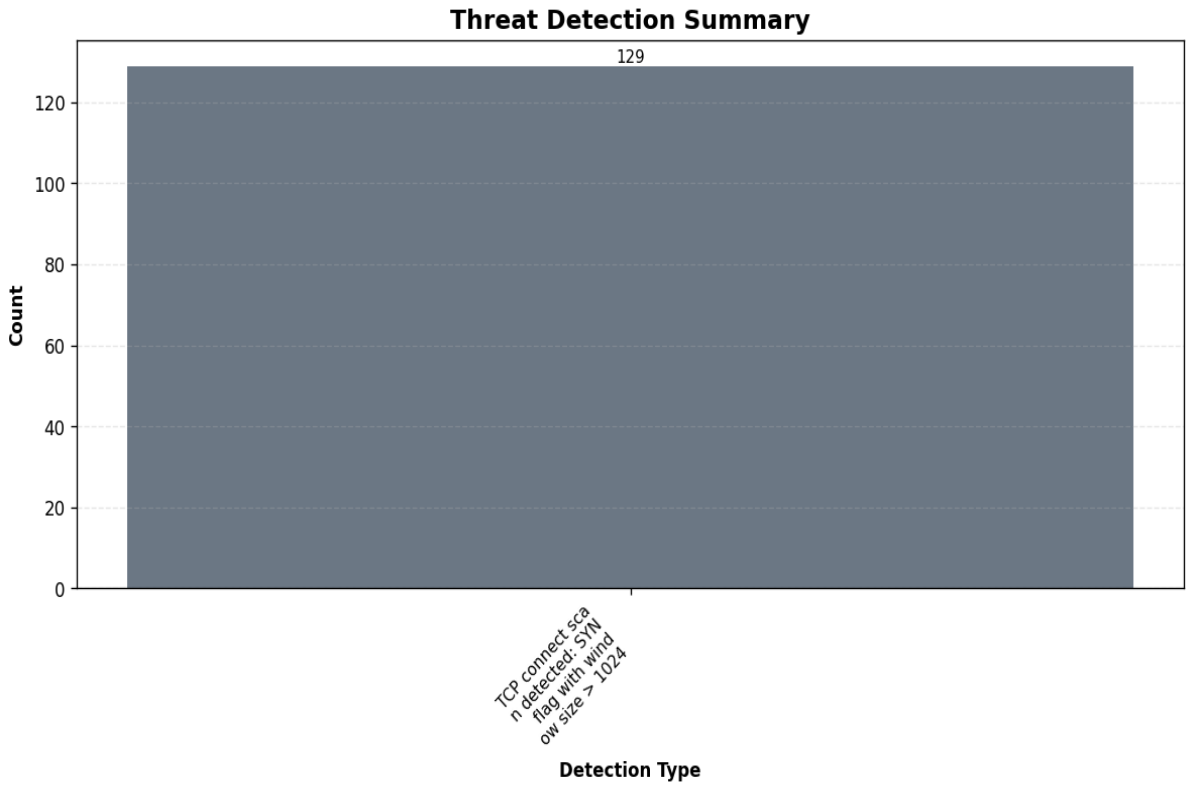
Review historical traffic from 192.168.153.154 for prior scan activity or C2 communications.
Analyze targeted external IPs (204.79.197.200, 213.139.38.16, etc.) to identify if they host sensitive services.

Architecture Review:

Segment internal networks to limit single-devicegress capabilities.
Enable detailed logging of TCP window sizes and port metadata for future investigations.

``

Threat Detection Summary



Detection Details

Detection Type	Count
TCP connect scan detected: SYN flag with window size > 1024	129

Source/Destination Analysis

IP Address	As Source	As Destination	Total
192.168.153.154	5	0	5
204.79.197.203	0	1	1
204.79.197.200	0	1	1
213.139.38.16	0	2	2
151.101.121.108	0	1	1

Event Timeline

Time	Packet #	Protocol	Detection
05:28:08.813	33	TCP	TCP connect scan detected: SYN flag with window size > 1024
05:28:08.897	40	TCP	TCP connect scan detected: SYN flag with window size > 1024
05:28:09.336	298	TCP	TCP connect scan detected: SYN flag with window size > 1024
05:28:09.439	431	TCP	TCP connect scan detected: SYN flag with window size > 1024
05:28:09.635	754	TCP	TCP connect scan detected: SYN flag with window size > 1024

Appendix: Raw Traffic Analysis Data


```
{
  "detection_counts": {
    "TCP connect scan detected: SYN flag with window size > 1024": 129
  },
  "attack_stats": {
    "tcp_packets": 0,
    "udp_packets": 0,
    "icmp_packets": 0,
    "arp_packets": 0
  },
  "top_threats": [
    {
      "packet_number": 33,
      "timestamp": "2017-10-18T05:28:08.813858",
      "minute": "2017-10-18 05:28",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.153.154",
      "dst_ip": "204.79.197.203",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    },
    {
      "packet_number": 40,
      "timestamp": "2017-10-18T05:28:08.897855",
      "minute": "2017-10-18 05:28",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.153.154",
      "dst_ip": "204.79.197.200",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    },
    {
      "packet_number": 298,
      "timestamp": "2017-10-18T05:28:09.336478",
      "minute": "2017-10-18 05:28",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.153.154",
      "dst_ip": "213.139.38.16",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    },
    {
      "packet_number": 431,
      "timestamp": "2017-10-18T05:28:09.439889",
      "minute": "2017-10-18 05:28",
```

```
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.153.154",
      "dst_ip": "213.139.38.16",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    },
    {
      "packet_number": 754,
      "timestamp": "2017-10-18T05:28:09.635881",
      "minute": "2017-10-18 05:28",
      "protocols": [
        "TCP"
      ],
      "src_ip": "192.168.153.154",
      "dst_ip": "151.101.121.108",
      "src_port": null,
      "dst_port": null,
      "detection_details": [
        "TCP connect scan detected: SYN flag with window size > 1024"
      ]
    }
  ]
}
```