INTRODUCTION

Following a request from TechSecure Inc., our team at OSPenTek Solutions conducted a detailed analysis of the corporate network traffic using Wireshark. The objective was to identify potential anomalies or signs of malicious activity that could indicate intrusion attempts or security compromises.

This work is part of our ongoing collaboration with TechSecure Inc. to ensure the highest efficiency and security of their IT systems.

Identification of Indicators of Compromise (IOCs)

a)

High volume of TCP SYN and DST flagged packets:
These often indicate port scanning attempts or Denial of Service (DoS) attacks, which aim to exploit vulnerabilities or overload systems

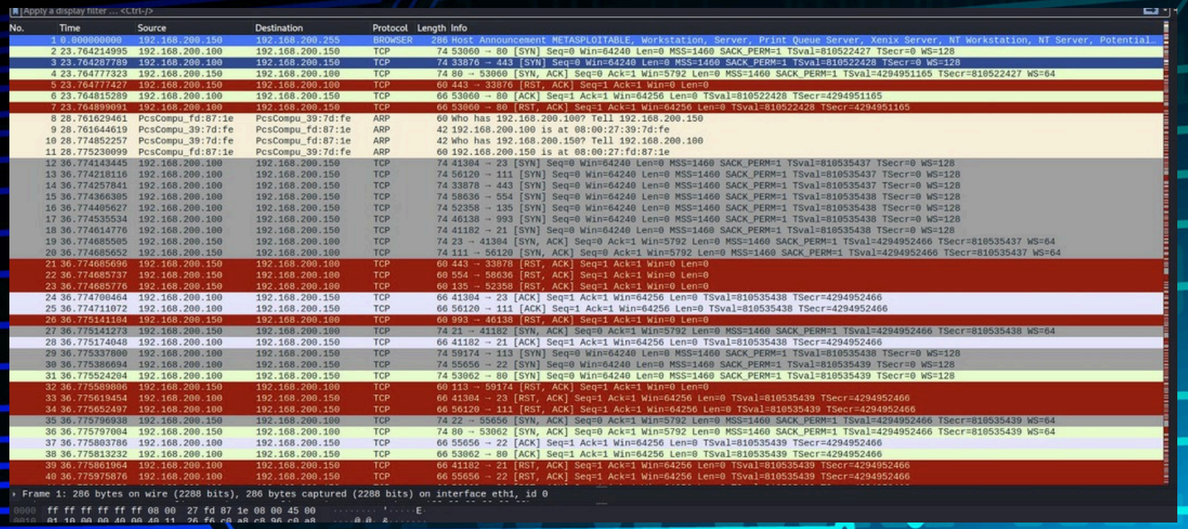
b)

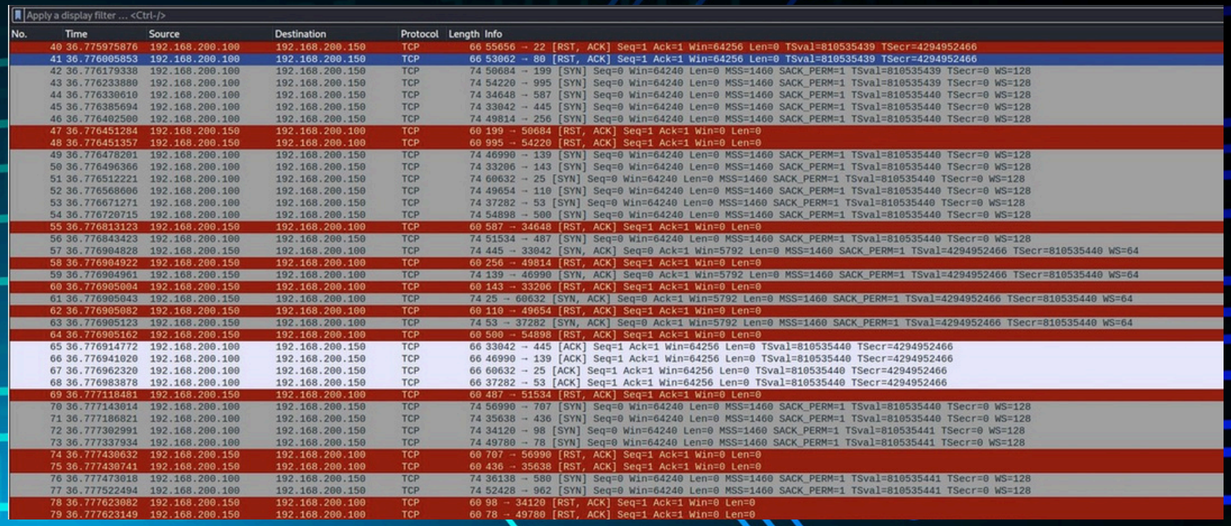
Intensive communication between few IP addresses:
A limited number of IP addresses were involved in significant traffic volume, potentially suggesting a compromised host or command-and-control server communications.

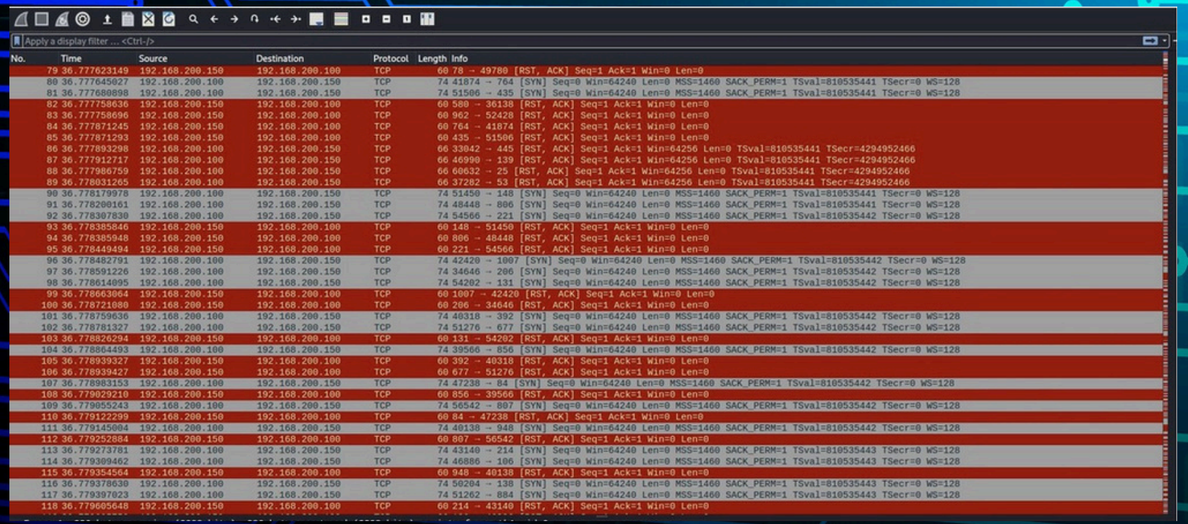
c)

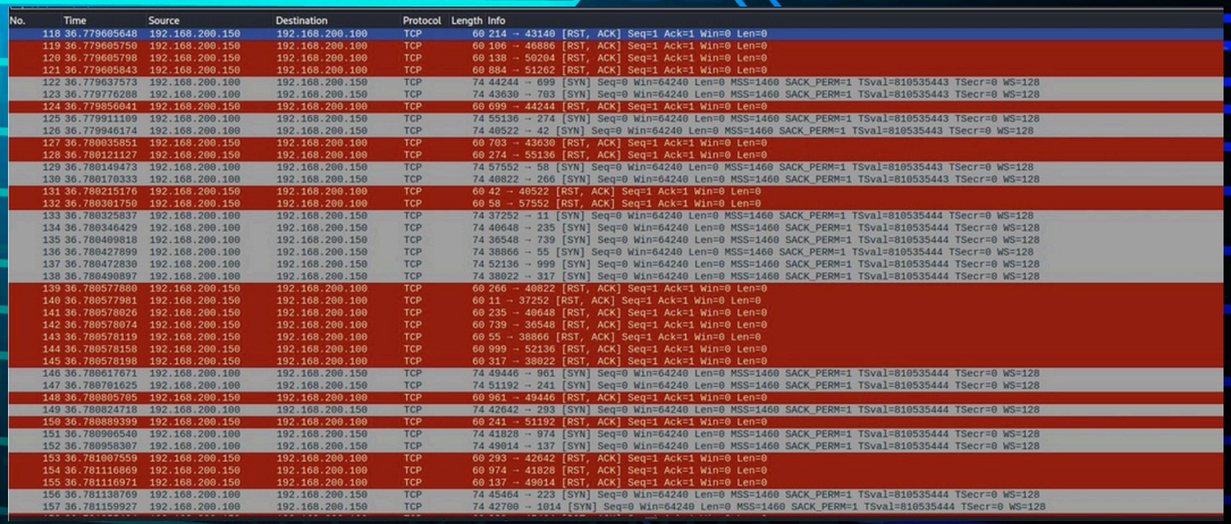
Red-flagged packets:
These indicate TCP communication interruptions or anomalies, suggesting potential transmission errors or abnormally terminated connections.

Packet Analysis









Attack Vector Hypotheses

a)

Port Scanning and DoS Attacks:
Attackers may have used scanning techniques to identify vulnerable services or launched DoS attacks to disrupt business operations.

b)

TCP Session Hijacking:
Alterations in sequence and ACK numbers suggest attempts to intercept or manipulate TCP sessions - a common tactic in session hijacking attacks.

Recommendations

a) IDS/IPS Implementation:
Deploy intrusion detection and prevention systems to monitor and intercept suspicious activity in real-time.

b) Access Control & Traffic Limitation:
Implement strict network access controls and traffic shaping measures to mitigate DoS attack impacts

c) Regular Updates & Patching:
Maintain all devices and software with current updates to reduce exposed vulnerabilities

d) Ongoing Security Awareness Training:
Conduct continuous staff education on potential risks and security best practices to prevent incidents

Conclusion

Our analysis has revealed concerning indicators that require immediate attention to prevent potential damage. By implementing the proposed recommendations, TechSecure Inc. can significantly enhance the security and resilience of its network infrastructure.

OSPenTek Solutions remains committed to supporting TechSecure Inc. in implementing these measures and in the ongoing monitoring of their systems' security.