Cyber Attack Analysis

Project Report

Table of Index

Project Summary

This project involves a comprehensive analysis of cyber attacks on a multinational organization with offices in various countries. The primary objective is to understand the nature of the attacks, identify vulnerable areas, and provide actionable insights to enhance the organization's security posture. The analysis is based on data captured from the organization's security devices, focusing on both system and mobile device attacks.

Problem Statement

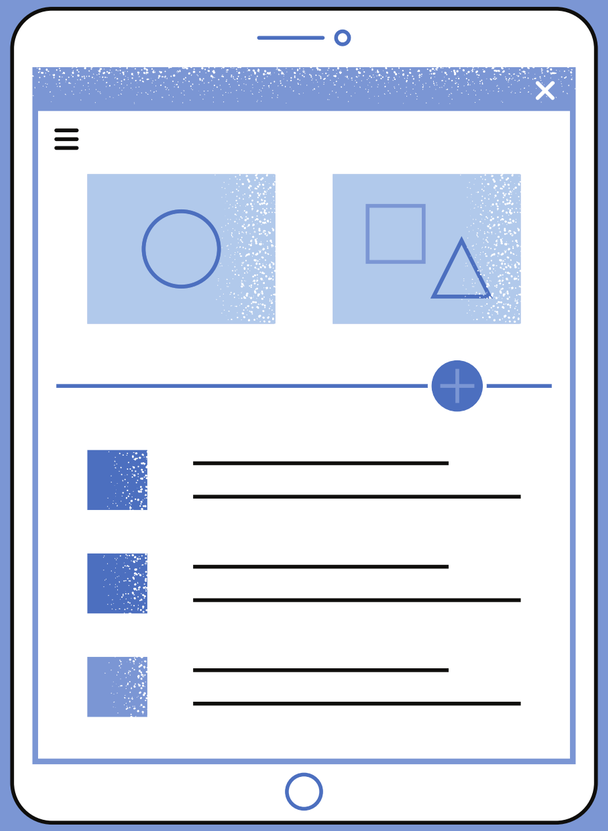
The multinational organization is experiencing a high frequency of cyber attacks targeting employees in crucial job roles across various departments and countries.

Despite having security devices in place, the organization struggles to understand the patterns, severity, and impact of these attacks, as well as the vulnerabilities in their systems and devices.

There is an urgent need to analyze the captured attack data to identify trends, prioritize response efforts, and implement effective security measures to protect the organization's assets and maintain client trust.

CYBER ATTACK ANALYSIS

OBJECTIVES



01 Objective

To analyze cyber attacks on a multinational organization, understand attack patterns, identify vulnerabilities, and provide actionable insights to enhance the organization's security measures and safeguard its assets and client trust.

02 Goal

To develop a comprehensive understanding of the cyber attack landscape faced by the organization and to equip the organization with data-driven recommendations for improving security protocols, employee awareness, and response strategies.

03 Outcome

The analysis identified key attack patterns and trends using PowerBI and SQL Server, revealing significant adware and DDoS attack percentages. Over 50% of employees were affected by cyber attacks, with detailed insights into system and device attack distributions. This led to actionable recommendations for improved cybersecurity practices, security device configurations, and employee awareness programs.

MISSION

STATEMENT

Our mission is to enhance the cybersecurity posture of the organization by thoroughly analyzing attack data, identifying vulnerabilities, and providing actionable insights and recommendations, thereby protecting organizational assets and maintaining client trust.

ABOUT
THE DATA

This project utilizes comprehensive datasets capturing various aspects of cyber attacks on a multinational organization's systems and devices. The data provides crucial insights into attack patterns, severity, vulnerabilities, and affected departments across different countries. The datasets are meticulously compiled to facilitate in-depth analysis and derive actionable security recommendations.

System Attacks: This dataset contains records of cyber attacks on employee systems, including source and destination IPs, date and time, ports, device status, protocols, packet flow information, traffic types, malware indicators, anomaly scores, alerts, severity levels, attack types, actions taken, device and browser information, operating systems, network segments, and log sources.

Device Attacks: This dataset records cyber attacks on employee mobile devices, capturing source and destination IPs, ports, protocols, device status, date and time, packet details, FLAG counts, segment and header sizes, and attack labels (adware, scareware, SMS malware, benign).

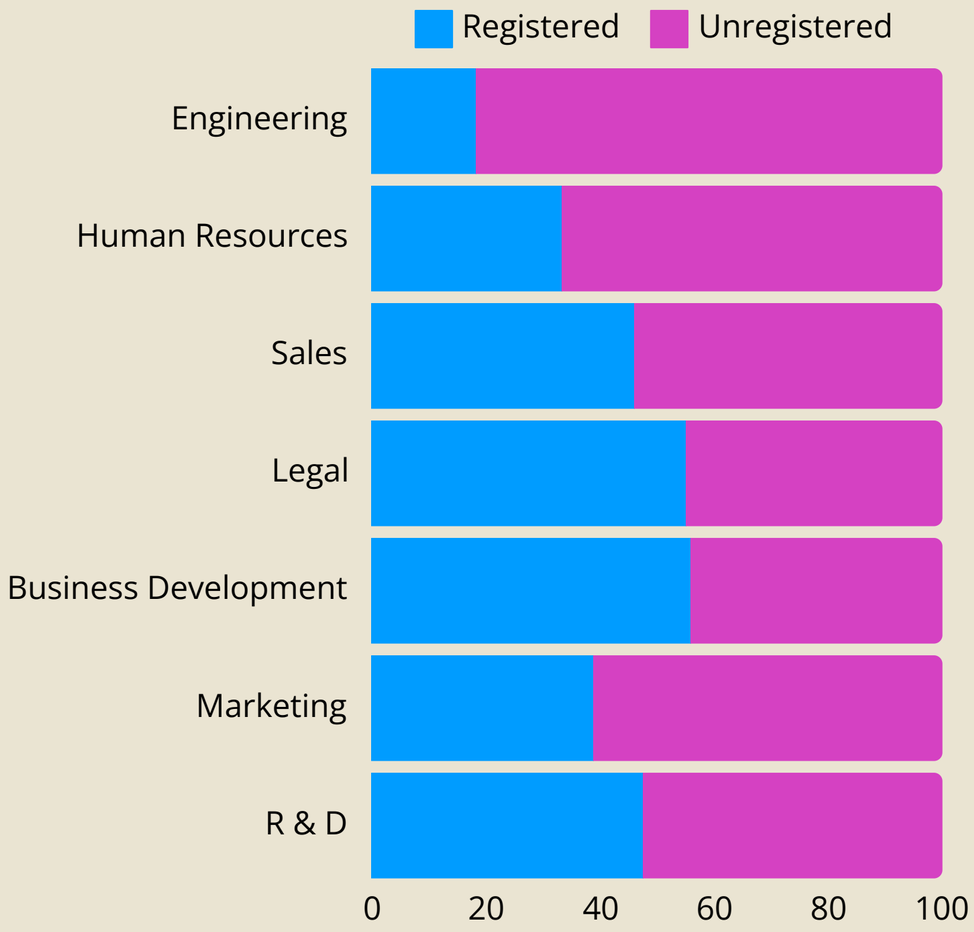
Dept. Info: This dataset contains information about employee IP addresses categorized by departments and countries, mapping IPs to specific departments to show which areas are affected by attacks.

Office Country: This dataset includes data on office locations, office codes by country, and the number of employees in each office, helping to understand the geographical distribution and scale of cyber attacks across regions.

% OF EMPLOYEES FACED ATTACK

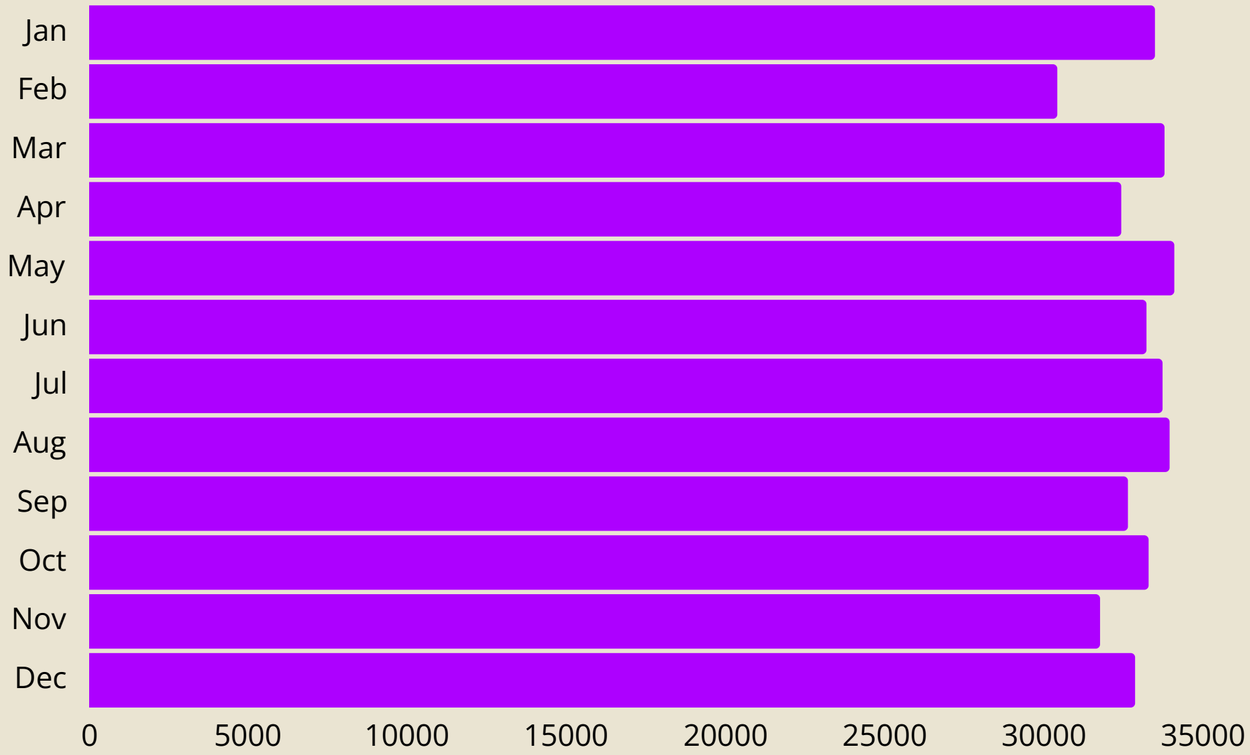
- **Overall:** Out of 74,879 employees, 44,742 (59.75%) have faced cyber attacks. Among these, 36.37% were registered attacks while a significantly higher 63.63% were on unregistered devices.
- **System Attacks:** Out of the total employee base, 39,999 employees (53.42%) have faced system attacks. Of these attacks, 49.93% were on registered devices, whereas 50.07% were on unregistered devices, showing a nearly equal distribution between registered and unregistered systems.
- **Device Attacks:** A smaller portion of the workforce, 4,743 employees (6.33%), have experienced device attacks. Among these, 34.84% were on registered devices, while 65.16% were on unregistered devices, indicating that unregistered devices are more vulnerable to attacks.

DEPARTMENT-WISE CYBER ATTACKS BY DEVICE AND SYSTEM STATUS



- System and total device attacks are positively correlated, indicating that as the number of system attacks increases, device attacks also tend to rise. This correlation suggests that attackers often target both systems and devices within the organization simultaneously.
- Unregistered devices faced significantly more attacks, totaling 251,741, compared to 143,885 attacks on registered devices. This highlights a critical vulnerability, as unregistered devices are more susceptible to cyber threats, potentially due to weaker security measures.
- In the Engineering department, unregistered devices accounted for 25.83% of total attacks, making it a major target within the organization. Additionally, the average total attacks were higher for unregistered devices, with an average of 35,963 attacks, compared to 20,555 attacks on registered devices.
- Monthly total attacks ranged from 30,416 to 34,092, showing consistent attack activity throughout the year. DDoS attacks were particularly prevalent, accounting for 33.57% of system attacks across different countries. The Engineering department saw the most significant divergence between device and system attacks, with device attacks exceeding system attacks by 113,458.

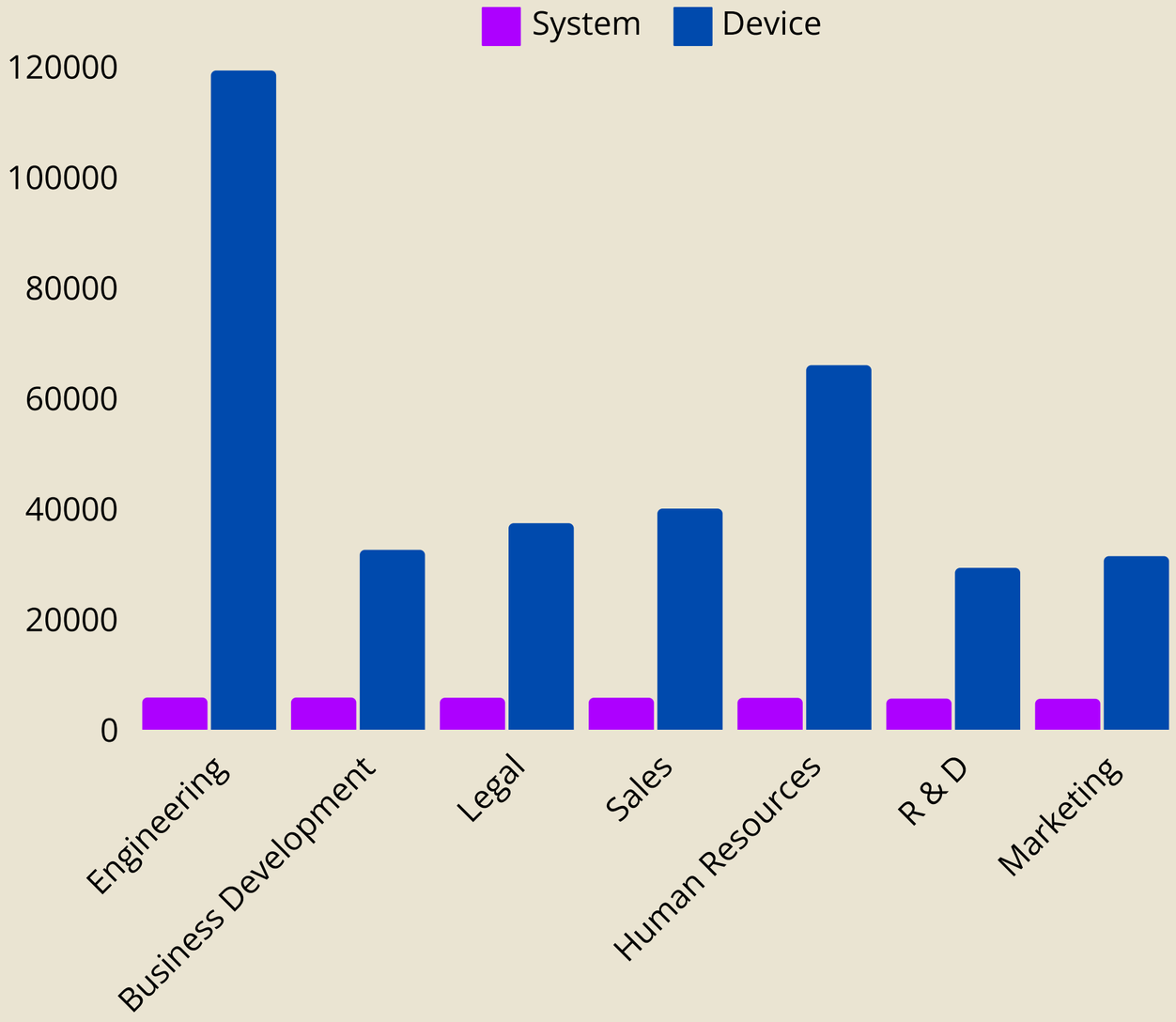
MONTH WISE ATTACKS



In May, the organization experienced the highest number of total attacks at 34,092, which was 12.09% higher than the lowest month, February, with 30,416 attacks.

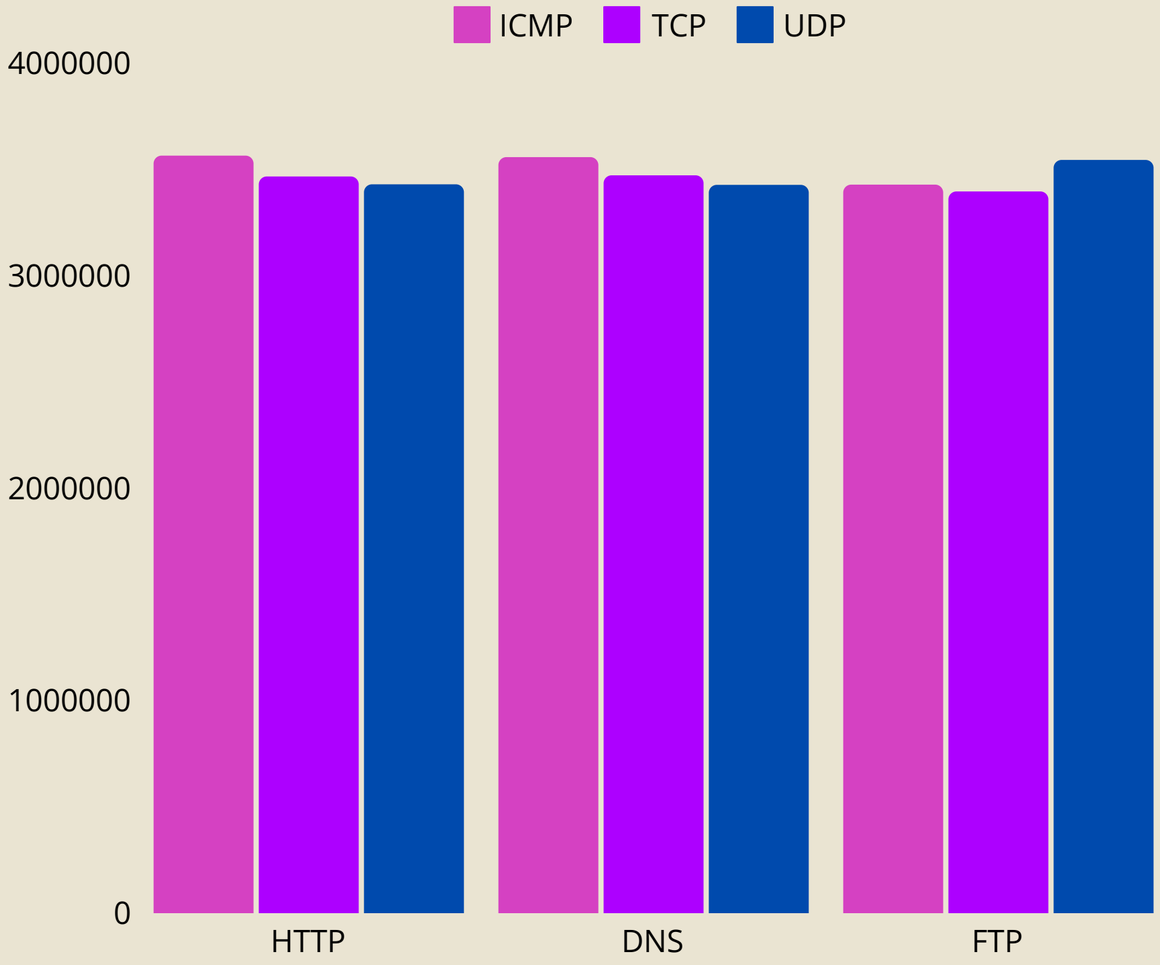
Across all 12 months, the total attacks varied within this range, consistently indicating a persistent threat level throughout the year.

DEPARTMENT-WISE SYSTEM AND DEVICE ATTACKS



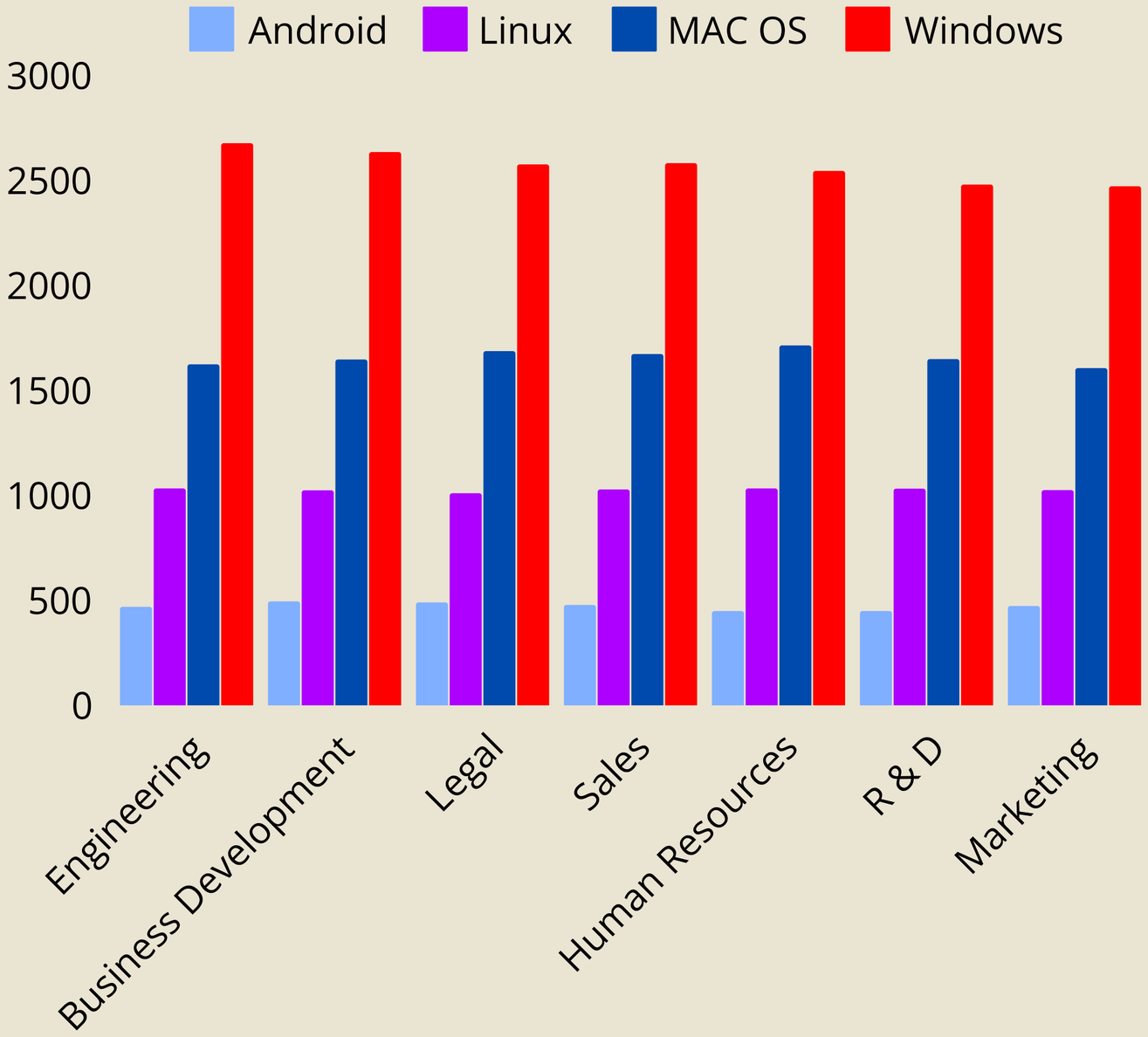
- **Highest System Attacks:** Engineering had the highest number of system attacks at 5,795, which was 4.08% higher than Marketing, which had the lowest at 5,568.
- **Percentage of Total System Attacks:** Engineering accounted for 14.49% of all system attacks.
- **Divergence in Attacks:** The largest divergence between device and system attacks was in the Engineering department, with device attacks being 113,458 higher than system attacks.

PACKETS LENGTH BY PACKET TYPE AND PROTOCOL



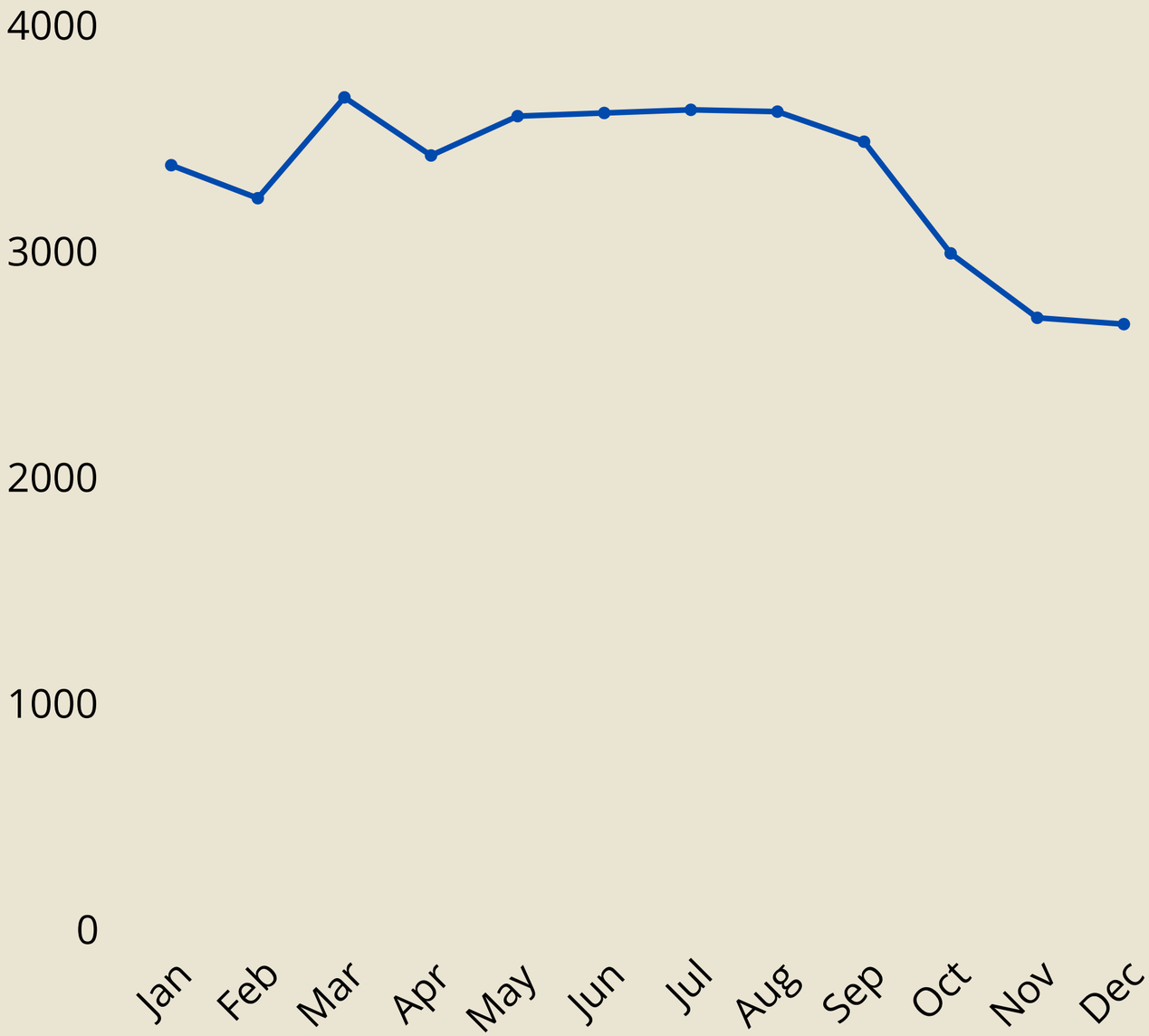
- **Highest Total Packet Length:** ICMP had the highest total packet length at 10,540,891, followed by UDP at 10,391,591 and TCP at 10,324,452.
- **HTTP in ICMP:** HTTP within the ICMP protocol accounted for 11.39% of the total packet length.
- **Highest Average Packet Length:** ICMP had the highest average packet length at 3,513,630.33, followed by UDP at 3,463,863.67 and TCP at 3,441,484.

PACKETS LENGTH BY PACKET TYPE AND PROTOCOL



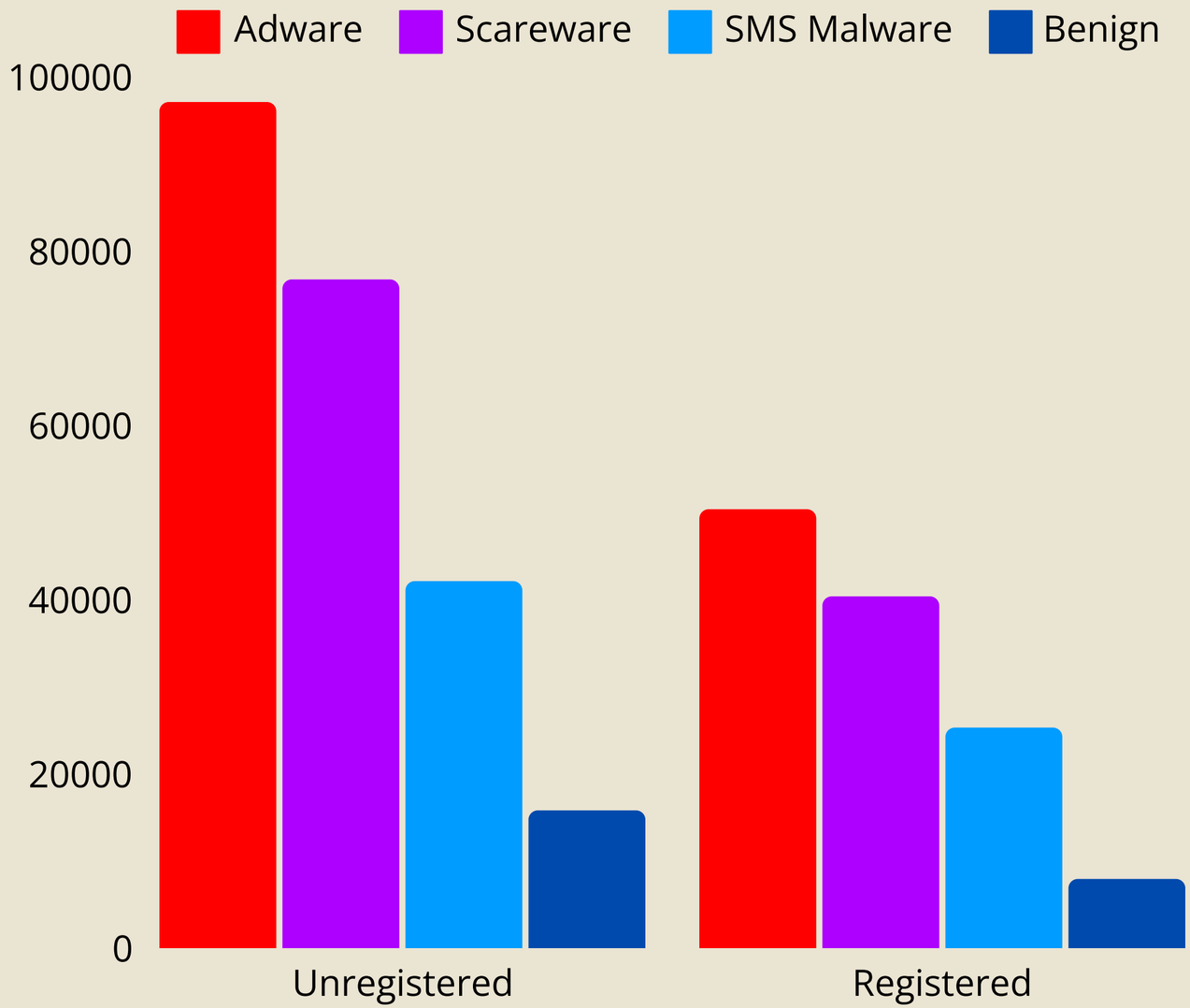
- **Highest Total System Attacks:** Windows had the highest total system attacks at 17,953, followed by macOS, Linux, and Android VM.
- **Engineering in Windows:** Engineering on Windows accounted for 6.69% of all system attacks.
- **Highest Average System Attacks:** Windows had the highest average system attacks at 2,564.71, followed by macOS, Linux, and Android VM.

PACKETS LENGTH BY PACKET TYPE AND PROTOCOL



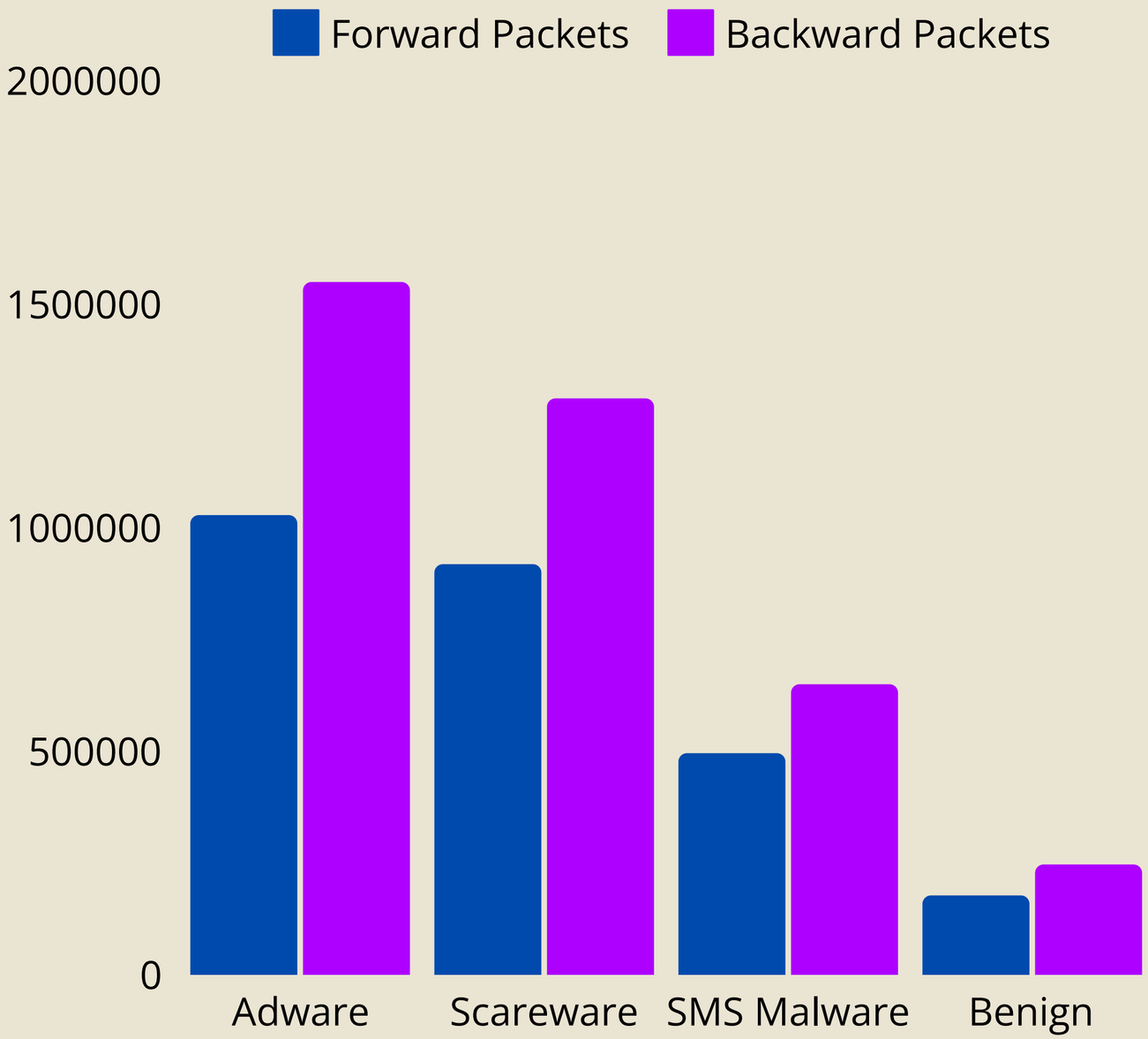
- **Highest System Attacks:** March had the highest number of system attacks at 3,678, which was 37.50% higher than December, the month with the lowest number of system attacks at 2,675.
- **March's Share of Attacks:** March accounted for 9.20% of all system attacks.
- **Monthly Range:** Throughout the year, system attacks ranged from 2,675 to 3,678.

PACKETS LENGTH BY PACKET TYPE AND PROTOCOL



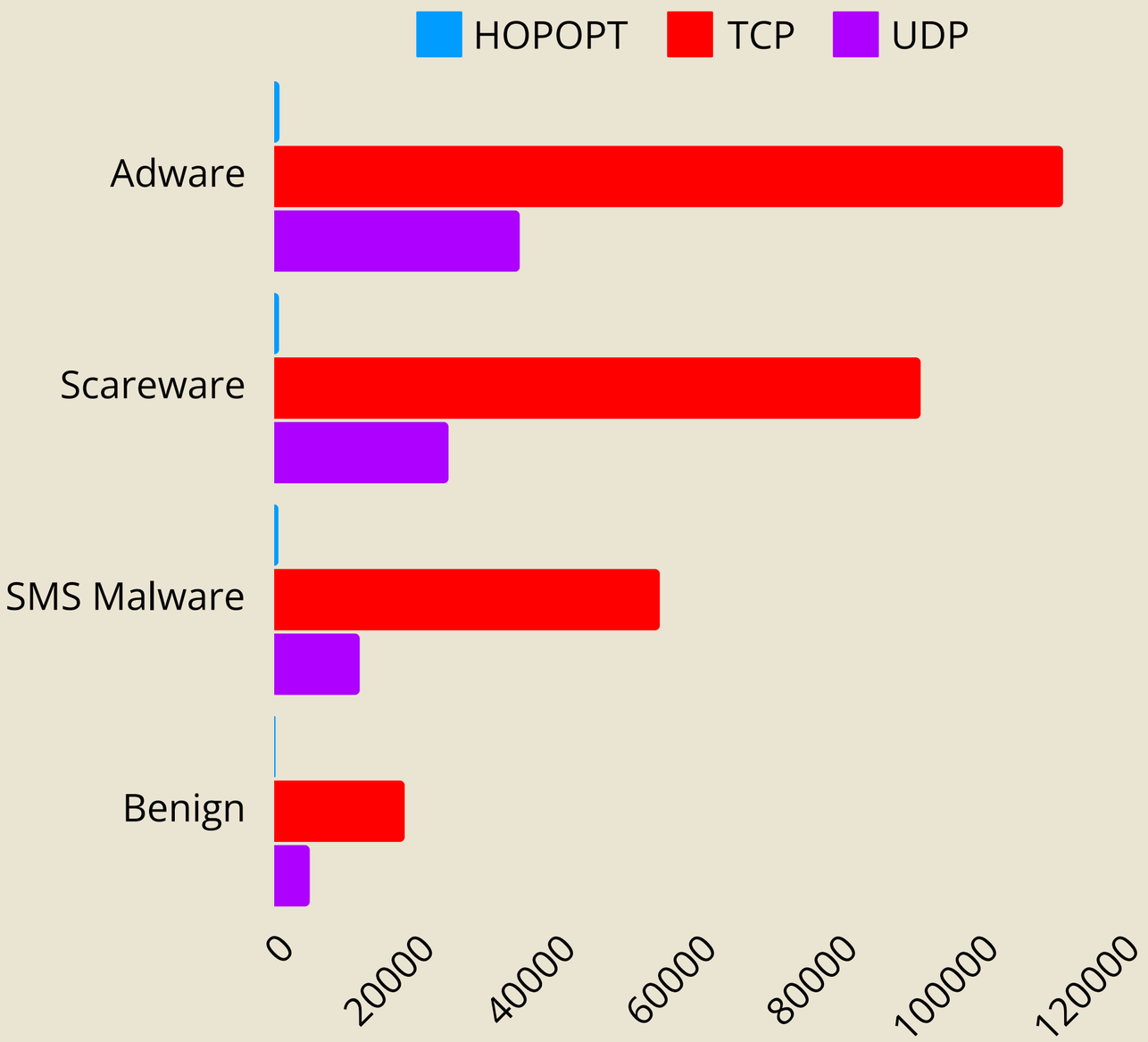
- **Adware in Unregistered Devices:** Adware attacks accounted for 27.30% of all device attacks on unregistered devices.
- **Highest Average Device Attacks by Label:** Adware had the highest average device attacks at 73,721.50, followed by Scareware, SMS Malware, and Benign.

TOTAL FORWARD AND BACKWARD PACKETS BY ATTACK LABELS



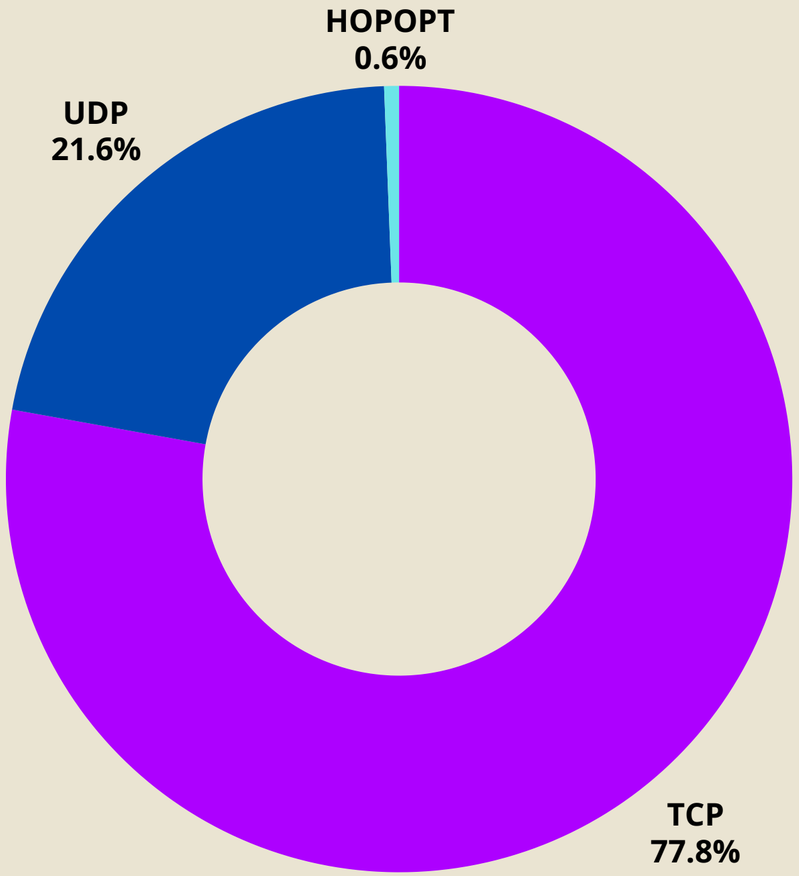
- **Highest Forward Packets:** Adware had the highest number of forward packets at 1,027,343, which was 481.41% higher than Benign, the label with the lowest forward packets at 176,700.
- **Positive Correlation:** Forward packets and total backward packets are positively correlated with each other.
- **Adware's Share of Forward Packets:** Adware accounted for 39.26% of all forward packets.
- **Divergence in Forward and Backward Packets:** The most significant difference between forward and backward packets occurred with the Adware label, where backward packets exceeded forward packets by 521,436.

DEVICE ATTACKS BY LABEL AND PROTOCOLS



- **Adware in TCP:** Adware attacks in the TCP protocol accounted for 31.46% of all device attacks.
- **Highest Average Device Attacks by Protocol:** TCP had the highest average device attacks at 69,191, followed by UDP at 19,171.75 and HOPOPT at 544.

ATTACKS BY PROTOCOLS



TCP had the highest device attacks at 276764, followed by UDP at 76687 and HOPOPT at 2176.

SUMMARY

OF THE ANALYSIS

01 Attack Trends and Vulnerabilities

The analysis revealed significant vulnerabilities in unregistered devices, which faced a higher percentage of attacks compared to registered devices. Notably, adware attacks in the TCP protocol were particularly prevalent, highlighting the need for enhanced security measures for unregistered devices and protocols commonly targeted by attackers.

02 Department and Operating System Insights

The Engineering department experienced the highest number of system and device attacks, particularly on Windows operating systems. This indicates a critical need for targeted security improvements and awareness programs in the Engineering department to mitigate the higher risk of attacks in this area.

03 Employee Impact and Recommendations

Over half of the employees (59.75%) faced attacks, mostly on unregistered devices. Recommendations include stricter security protocols for unregistered devices, regular security training, and improved monitoring for vulnerable departments and operating systems.

TIPS

TO IMPROVE SECURITY POSTURE

01 Enhance Security Protocols for Unregistered Devices

Implement stricter security measures for unregistered devices, including mandatory registration and regular security updates, to reduce their vulnerability to attacks.

02 Conduct Regular Security Training

Provide ongoing security awareness training for employees, particularly in departments like Engineering that are most affected, to educate them on recognizing and mitigating cyber threats.

03 Improve Monitoring and Defense Mechanisms

Upgrade security device configurations to better detect and block attacks, focusing on commonly targeted protocols and operating systems, and ensure continuous monitoring of network segments and traffic.