
Cyber Attack
Analysis
Go to Report

CYBER ATTACK ANALYSIS | PROJECT INFORMATION

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.

About Data:

The analysis is supported by four key datasets:

System Attacks: Records of attacks on employee systems. The key attributes are: Source and destination IPs, date and time of attack, ports, device status, protocols, packet flow, traffic type, malware indicators, anomaly scores, alerts, severity levels, attack types, actions taken, device/browser information, operating systems, network segments, log sources.

Device Attacks: Records of attacks on employee mobile devices. The key attributes are: Source and destination IPs, ports, protocols, device status, date and time, packet details, FLAG counts, segment and header sizes, attack labels (adware, scareware, SMS malware, benign).

Dept. Info: IP addresses of employees categorized by departments and countries.

Office Country: Data on office locations, country-wise office codes, and the number of employees per office.

Analysis Conducted:

Attack Patterns and Trends: Identifying peak periods for cyber attacks by analyzing date and time data, examining which country offices and departments experience the highest frequency of attacks, understanding the most common protocols and ports targeted by attackers.

Severity and Impact Assessment: Categorizing attacks based on severity to prioritize response efforts, analyzing anomaly scores and alerts to gauge the impact of detected threats.

Attack Types and Malware Indicators: Identifying common attack signatures and types, such as adware, scareware, and SMS malware, examining the presence of malware indicators to understand the types of malicious software used.

Employee and Device Vulnerability: Differentiating between attacks on registered vs. unregistered devices, identifying which operating systems and browsers are most frequently targeted.

Network and Segment Analysis: Analyzing which network segments are most vulnerable, identifying the primary sources of logs to understand where most attacks are detected.

Overview | System Attacks | Device Attacks

CYBER ATTACK | OVERVIEW

Russia 1

Affected Employees

44742 | 59.75%

74879

Total Employees

Registered

36.37%

Unregistered

63.63%

395626

Total Attacks

Top Attack or Label

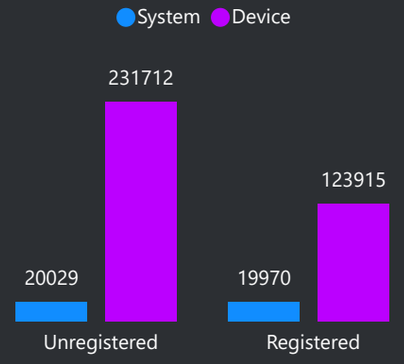
Adware | 147443

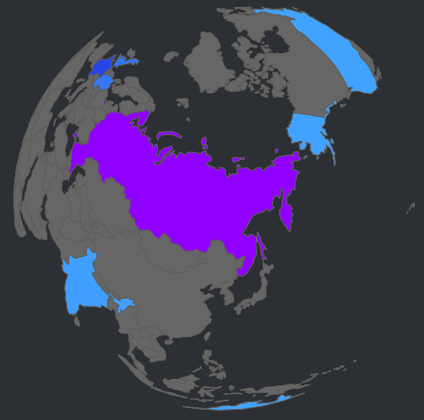
395626

Total Attacks

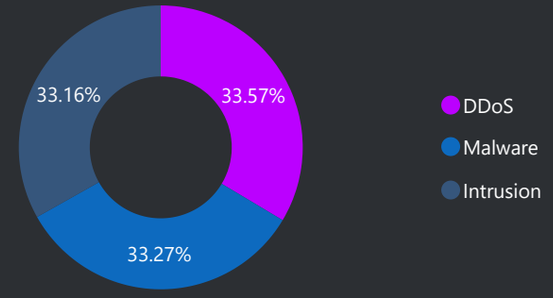
37.27%

Status wise Device and System Attacks

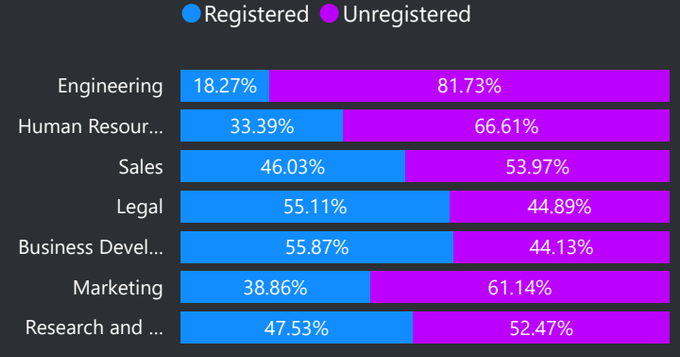




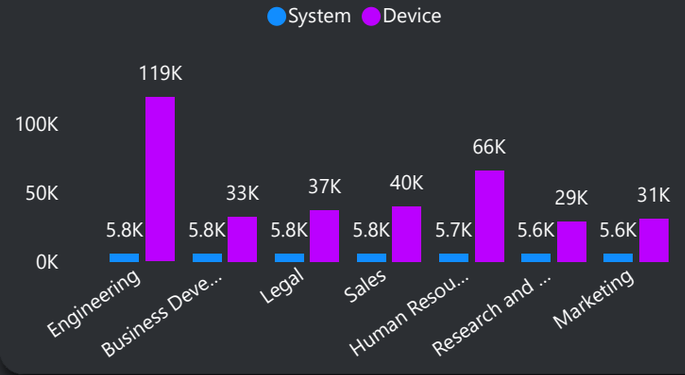
System Attacks by Attack Type



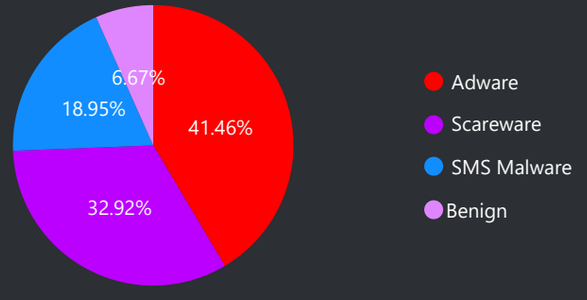
Dept. wise Attacks by Device Status



Dept. wise System and Device Attacks



Device Attacks by Attack Label



SYSTEM ATTACKS | DASHBOARD

United Sta

Affected Employees

39999 | 53.42%

74879

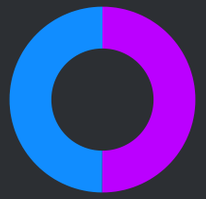
Total Employees

Registered

49.93%

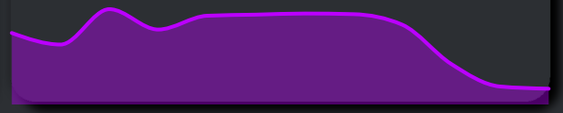
Unregistered

50.07%



Total Attacks

39999



Top Attack Type

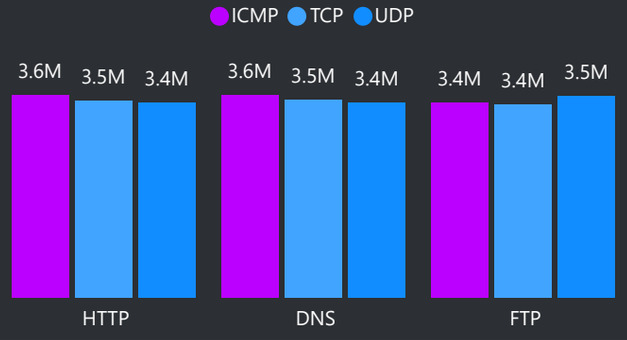
DDoS | 13428

39999

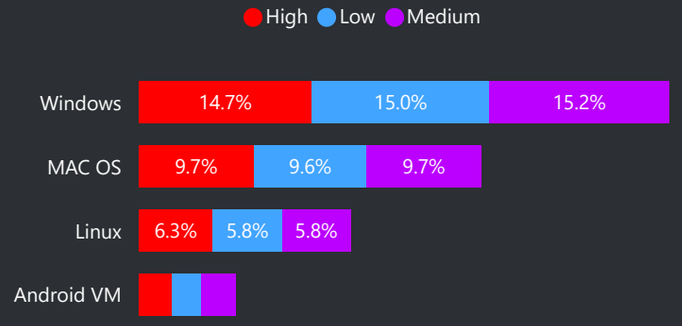
Total System Attacks

33.57%

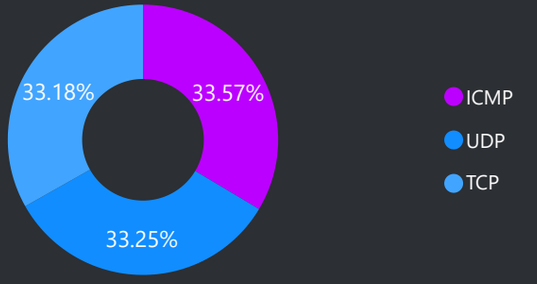
Packets Legth by Packet Type and Protocol



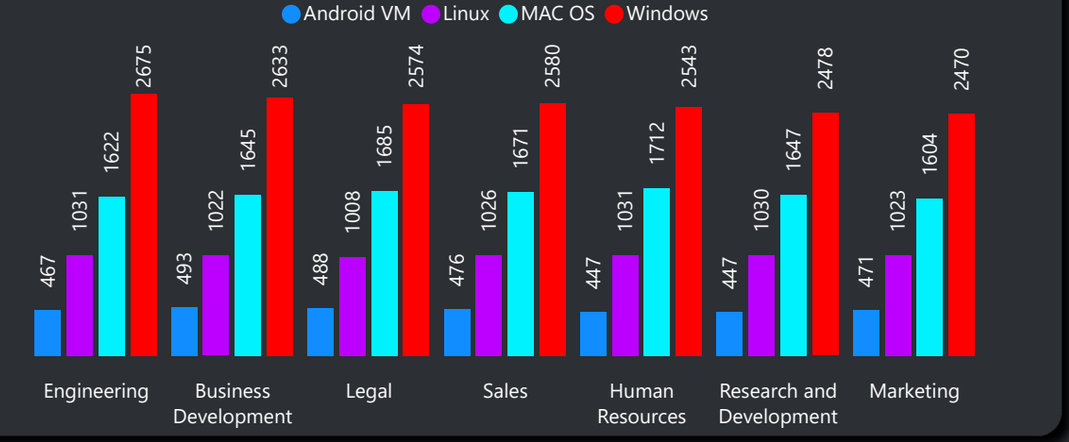
Attacks by OS & Severity Level



Attacks by Protocols



Attacks by OS



Target IP	Device Status	Protocol	Flow Duration(ms)	Network Segment	Traffic T
1.1.189.171	Unregistered	ICMP	4461618	Segment B	HTTP
1.100.166.191	Registered	UDP	102053041	Segment A	DNS
1.100.73.63	Registered	UDP	94814905	Segment B	HTTP
1.101.117.52	Unregistered	UDP	78652389	Segment B	HTTP
1.101.24.101	Registered	ICMP	109695281	Segment B	HTTP
1.102.176.87	Unregistered	UDP	33404816	Segment A	HTTP
1.103.183.132	Registered	UDP	97503886	Segment C	FTP
1.105.159.177	Registered	TCP	4031258	Segment A	DNS
1.105.2.246	Unregistered	ICMP	16925080	Segment A	FTP
1.107.48.44	Unregistered	ICMP	115210170	Segment C	HTTP

DEVICE ATTACKS | DASHBOARD

Russia 1

Affected Employees

4743 | 6.33%

74879

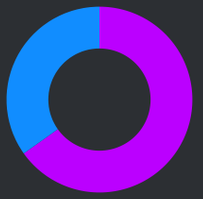
Total Employees

Registered

34.84%

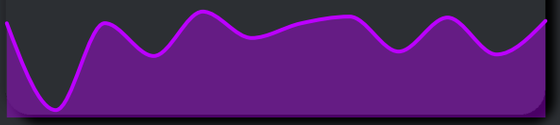
Unregistered

65.16%



Total Attacks

355627



Top Label

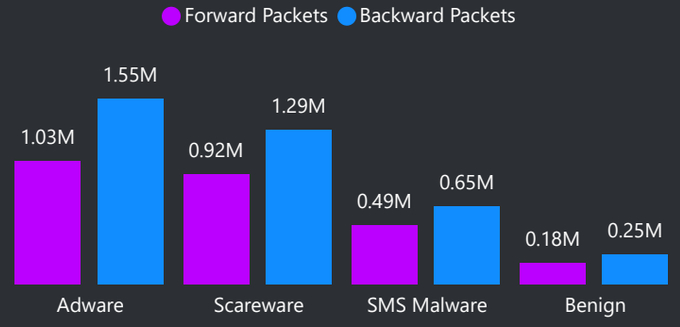
Adware | 147443

355627

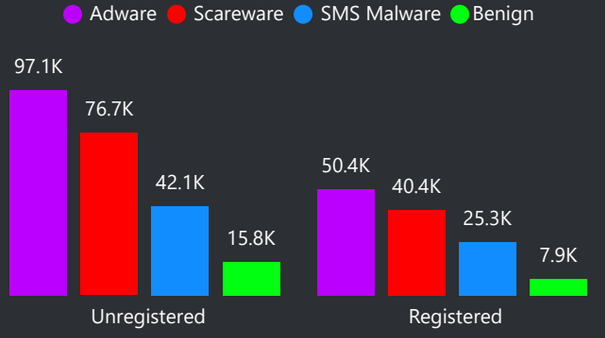
Total Device Attacks

41.46%

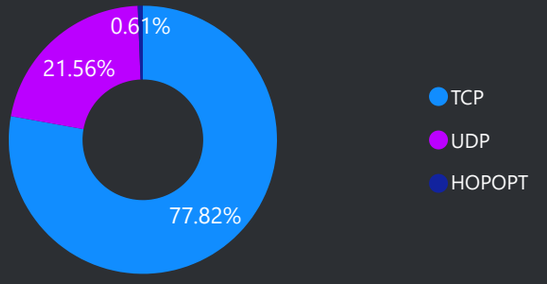
Total Forward & Backward Packets by Attack Labels



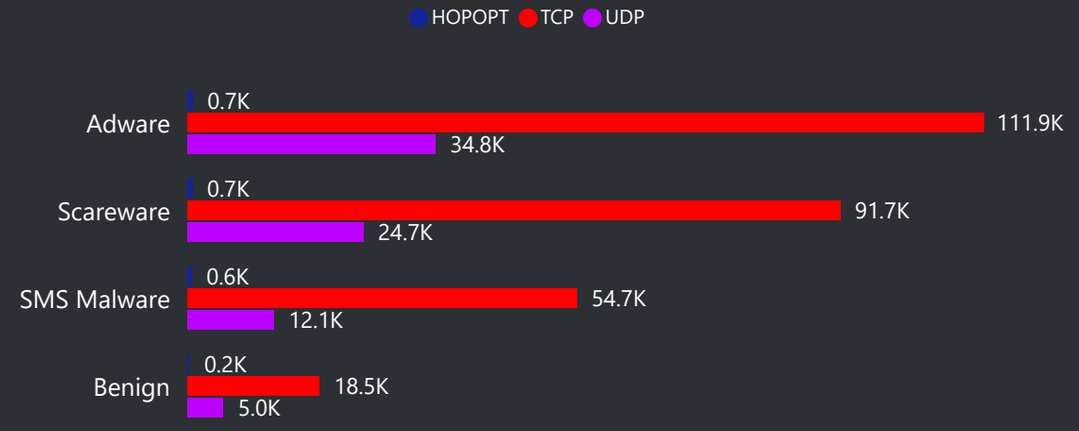
Device Status and Label wise Attacks



Attacks by Protocols



Attacks by Label and Protocol



Target IP	Label	Protocol	Flow Duration(ms)	Forward Packets	Backward Pa
0.117.2.1	Adware	HOPOPT	103006129	20	
0.117.2.1	Scareware	HOPOPT	78352307	16	
0.117.2.1	SMS Malware	HOPOPT	24401243	6	
0.143.2.19	Scareware	HOPOPT	2500607	4	
0.143.2.19	SMS Malware	HOPOPT	5001507	8	
0.199.2.19	SMS Malware	HOPOPT	5305617	2	
0.95.2.0	SMS Malware	HOPOPT	5305121	2	
0.95.2.3	Adware	HOPOPT	561942951	34	
0.95.2.3	Scareware	HOPOPT	847354795	44	
0.95.2.3	SMS Malware	HOPOPT	1035443005	31	
1.161.188.253	Adware	UDP	2634936	5	