CYBER THREAT ANALYSIS 2015-2024

OVERVIEW

The past decade has witnessed tremendous technological advancement especially in the artificial intelligence landscape.This has been accompanied by both benefits and challanges.Several tools have been developed to detect and prevent attacks but the attackers are also striking back harder and smarter with sophisticated tools.In this analysis we will unpack the nature of these attacks,assess their financial impact and pinpoint the most effective protection mechanisms.

OBJECTIVES

- To acccess the threat evolution for the past 9 years.
- To identify key vulnerabilities in the most prone attacked sectors
- To access the financial losses caused by different vulnerabilities and attacks.
- To determine the best protection mechanism against an attack.

BUSINESS UNDERSTANDING

- Cyber security is no longer just an IT issue but a business imperative. Over the years ,cyber attacks have surged evolving from isolated incidents to sophisticated ,AI driven attacks targetting different sectors. These attacks pose business risks as they may lead to financial losses and erode customers trust as a result of theft of personal information.

- Global cybercrime costs are projected to hit $10.5 trillion annually by 2025 necessitating the need to invest in proactive defense. This analysis strive to equip businesses, corporates and governments with the insights to understand the threats, financial impact and the appropriate defense mechanisms for defense against attacks.

Dataset link :https://www.kaggle.com/datasets/atharvasoundankar/global-cybersecurity-threats-2015-2024

DATA UNDERSTANDING

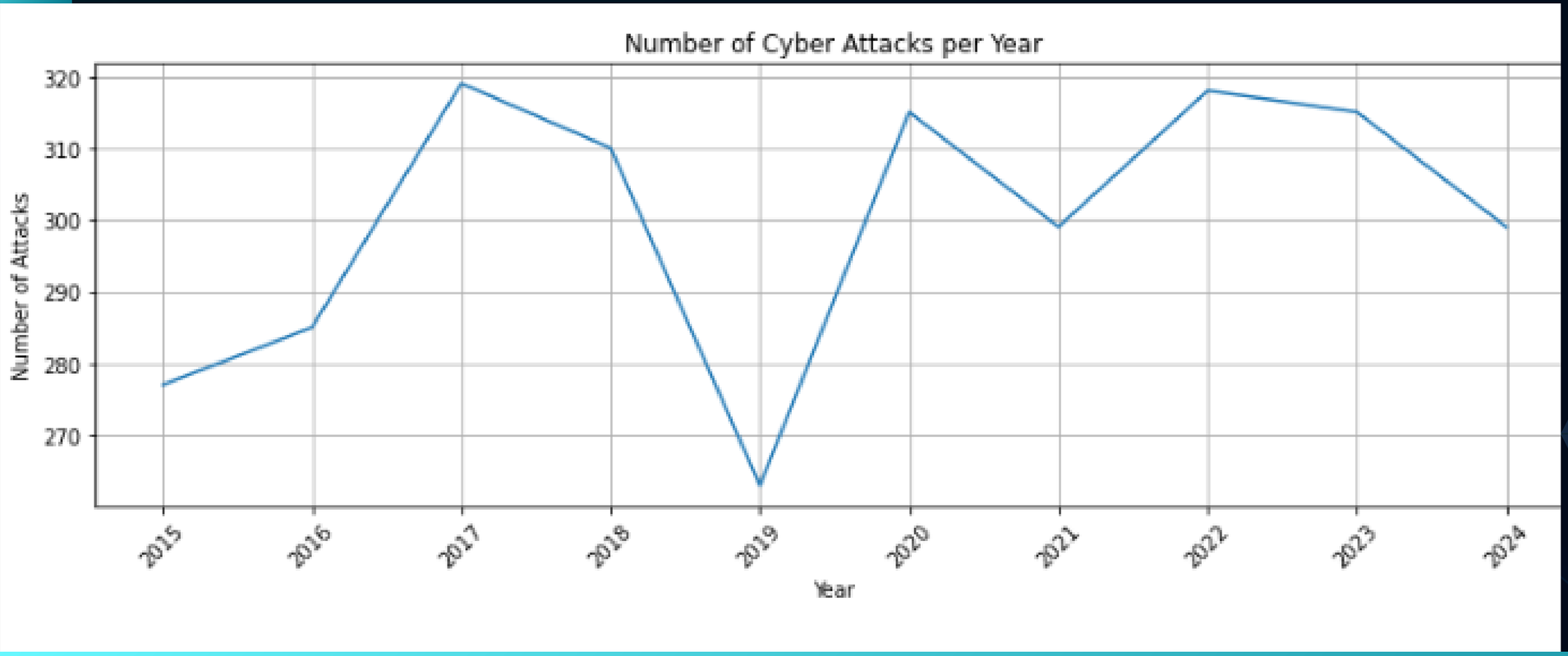
The data for this analysis was obtained from kaggle, with a total of 3000 observations across 10 columns.There were no missing values in the dataset,no outliers and no duplicated values.On further analysis,most of the columns data were uniformly distributed with a few skewedly distributed.The observed columns were:

Columns

- Country
- Year
- Target Industry
- Financial Loss
- Attack Source
- Number of Affected Users
- Defense Mechanism Used
- Attack Type
- Incident Resolution Time
- Security Vulnerability Type

DATA ANALYSIS AND VISUALIZATION

01 Trend Analysis of cyber attacks from the year 2015-2024

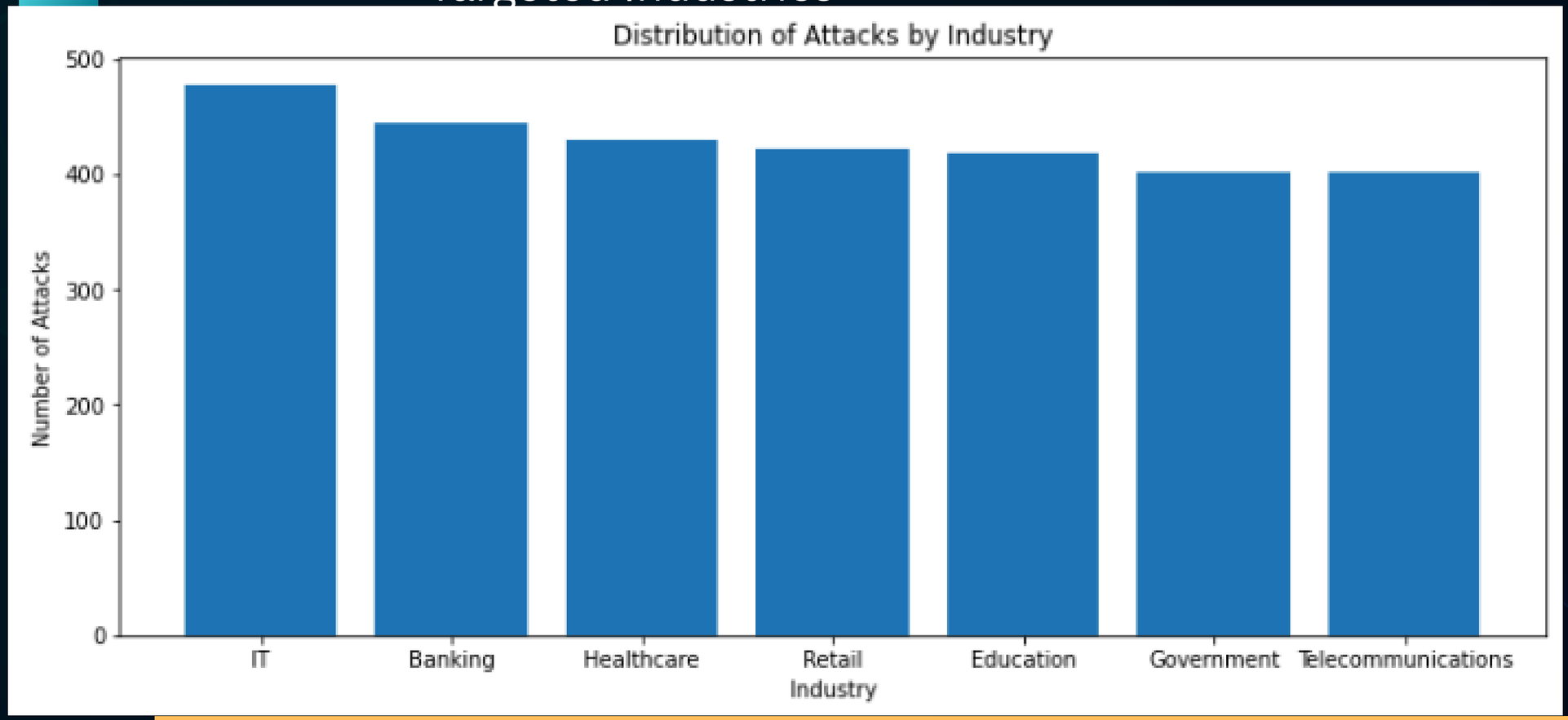


The number of cyber attacks increased steadily from the year 2015 peaking in the year 2017.Thereafter,a sharp decline in the year 2019 to a lowest of less than 270.This can be attributed to the covid 19 pandemic which saw business close down and movement restricted. There was a rapid increase in the number of attacks in the year 2020,and a decline in 2021.The graph shows that a decline is followed by a rise in attacks with attacks expected to increase in the year 2025.

DATA ANALYSIS AND VISUALIZATION

02

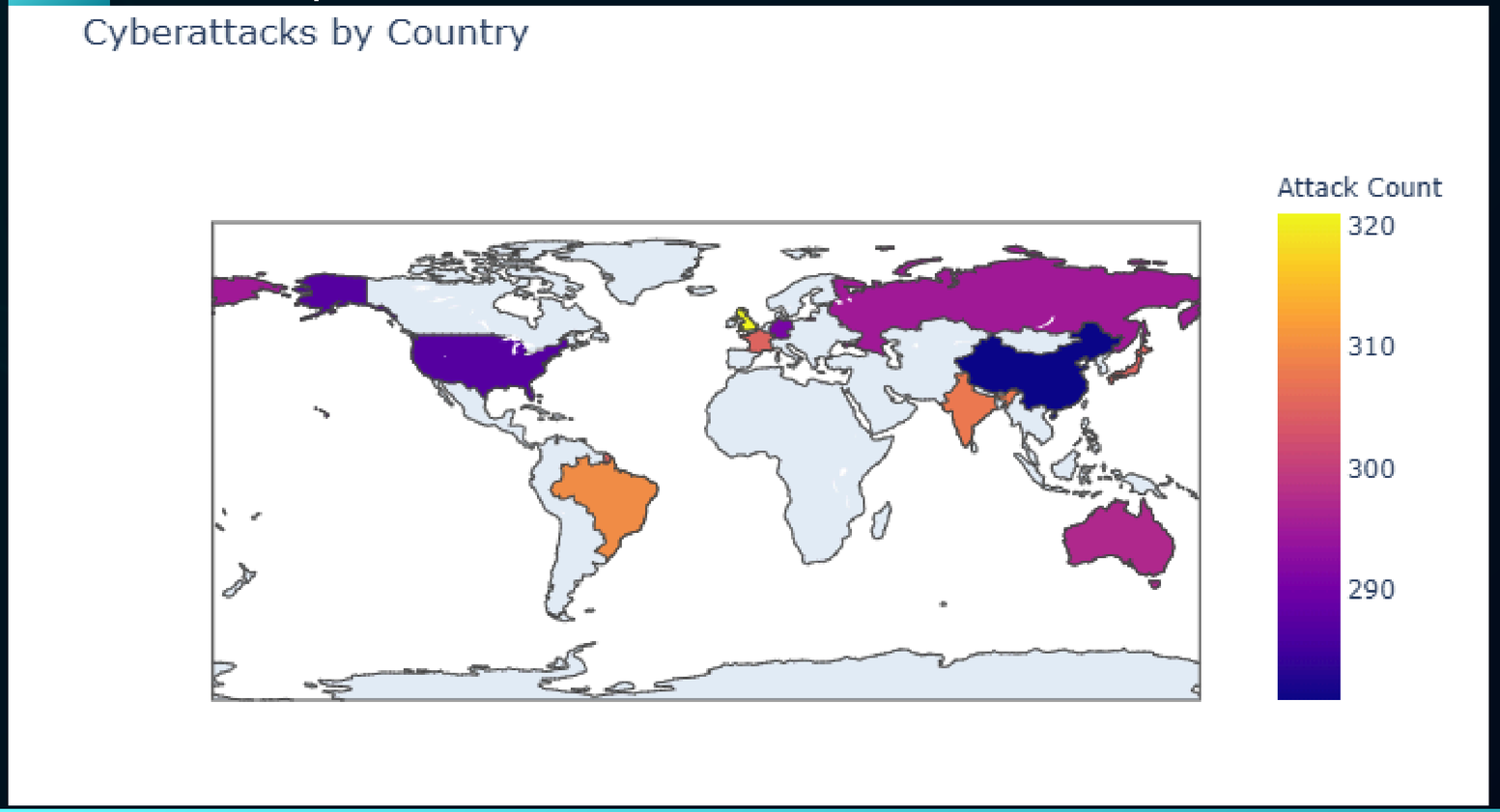
Targeted Industries



The IT industry is the most affected with a total of 478 attacks followed closely by the banking industry and health.The high numbers can be attributed to the huge amount of data as well as the financial gain in these sectors.Government and telecommunication were the lowest attacked at 403 each.The uniform distribution however, shows that all the industries are almost equally targeted thus all require robust defense mechanisms.

DATA ANALYSIS AND VISUALIZATION

03 Geospatial Attack Distribution



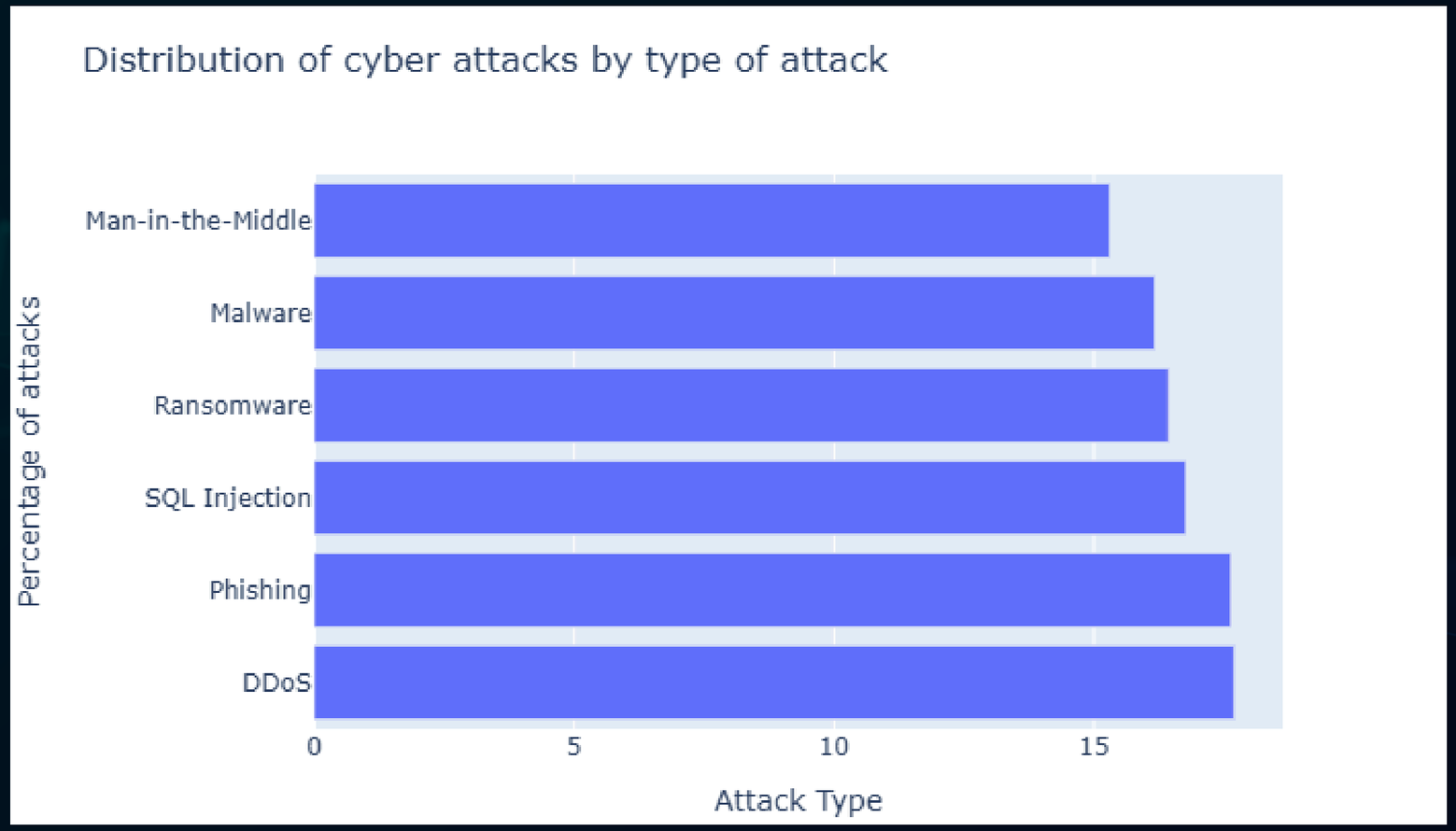
UK	321
Brazil	310
India	308
France	305
Japan	305
Australia	297
Russia	295
Germany	291
USA	287
China	281

United Kingdom witnessed the highest number of attacks followed by Brazil and India respectively.London is a global financial hub leading to the high numbers.Brazil has recently seen the digitazation of its banking sector and developmnet of FinTech. This creates an avenue for cyber attacks.China and USA being the worlds top economies have greatly invested in their security infrastructure thus the low number of attacks.

DATA ANALYSIS AND VISUALIZATION

04

Distribution of attacks based on the Attack Type

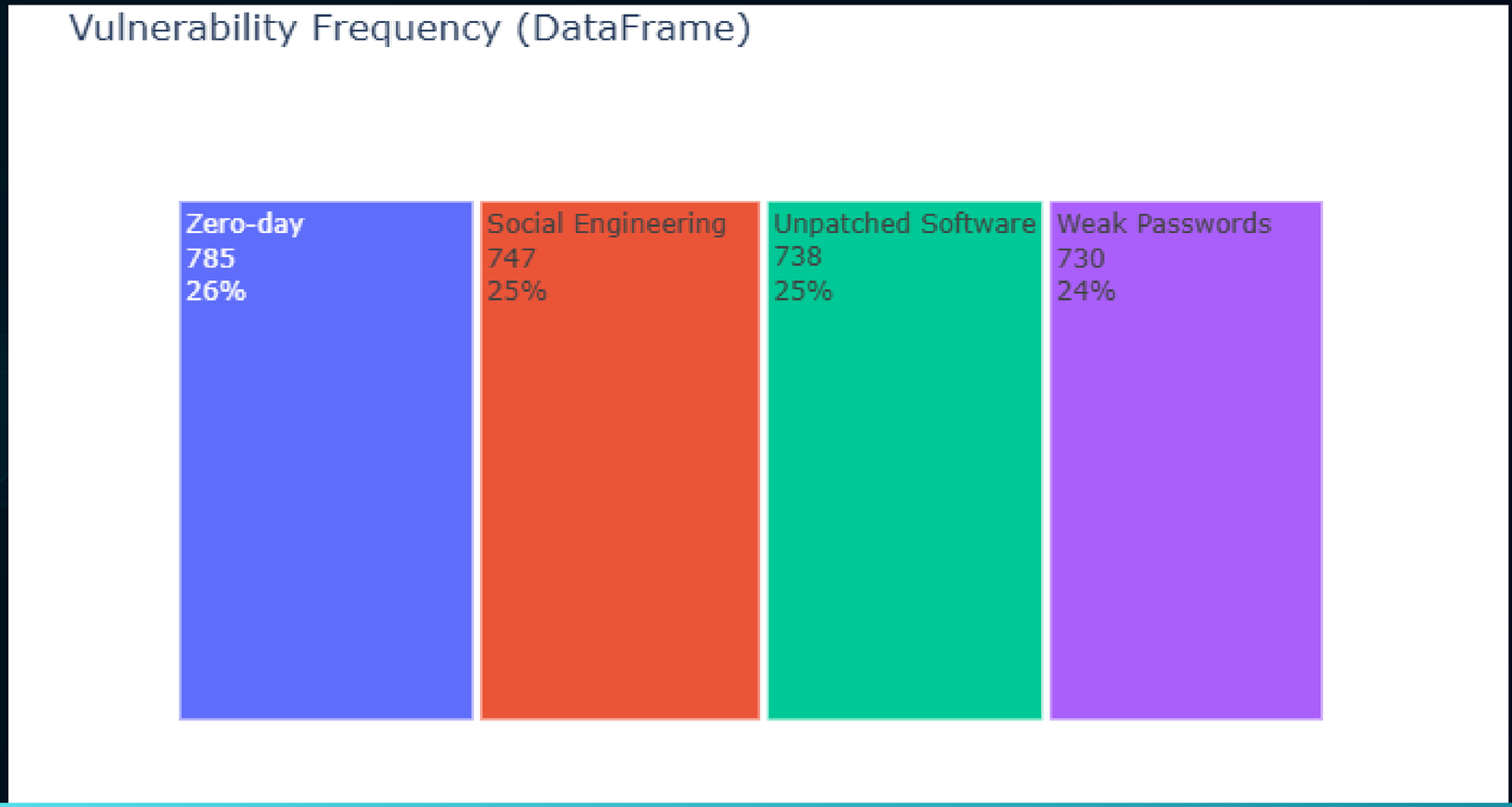


DDoS was the most prevalent attack type at 17.7%, followed closely by phishing at 17.6%.Man-in-the-middle contributed the least at 15.3%.The plot revealed that the attacks are nearly uniformly distributed with little variation in their frequencies.Phishing and DDoS are the most prevalent because they require less technical expertise,are easy to execute and are highly effective at disrupting operations and stealing sensitive data.Man-in-the-midle however,requires more technical experience and infrastructure.

DATA ANALYSIS AND VISUALIZATION

05

vulnerabilities mostly exploited by attackers

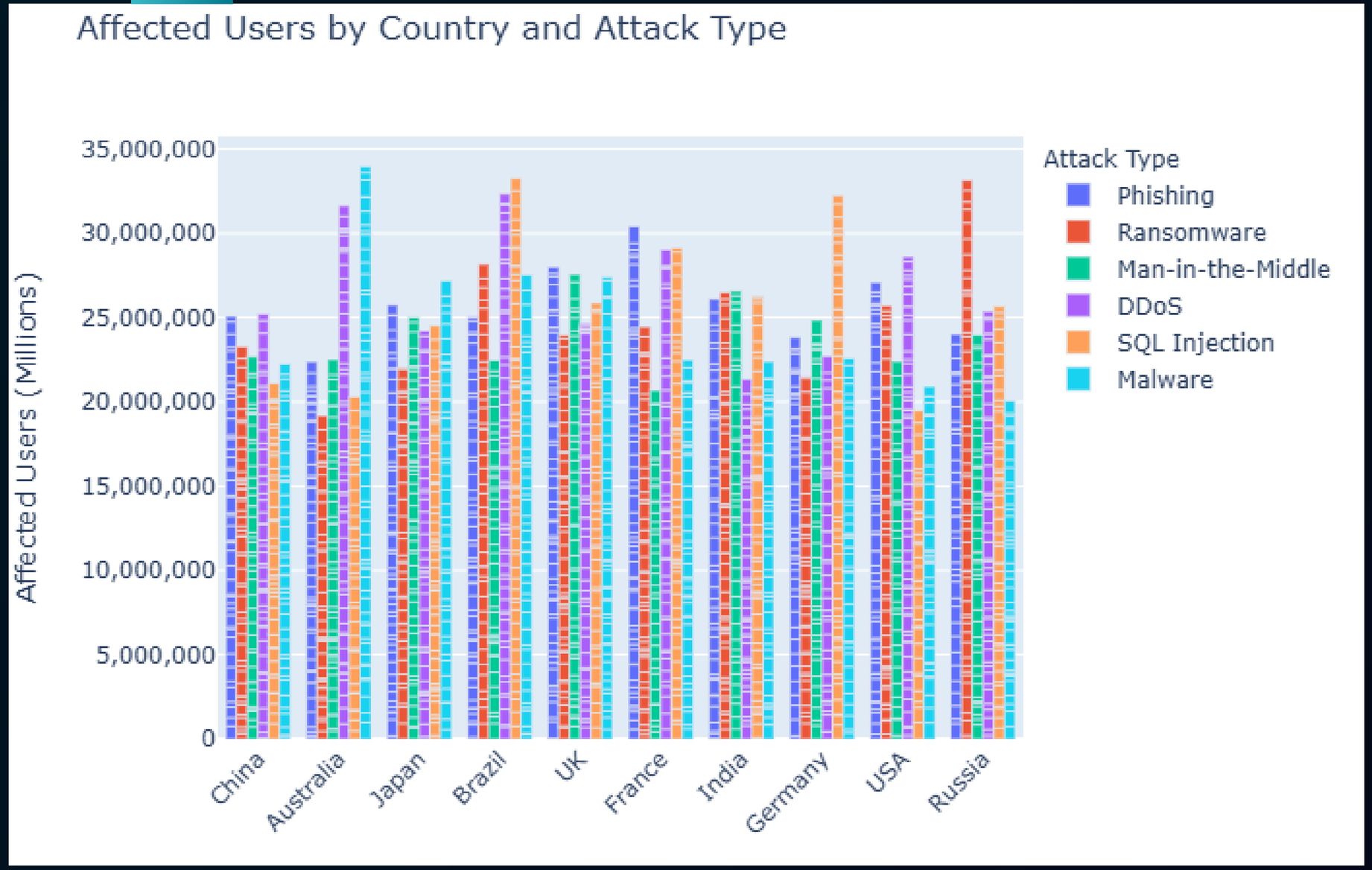


Zero-day vulnerabilities are the most common as attackers exploit them before patches exist, while social engineering, especially phishing, tricks users into giving up sensitive information. Unpatched software creates openings due to delayed updates, and weak or reused passwords make it easier for attackers to break in.

DATA ANALYSIS AND VISUALIZATION

07

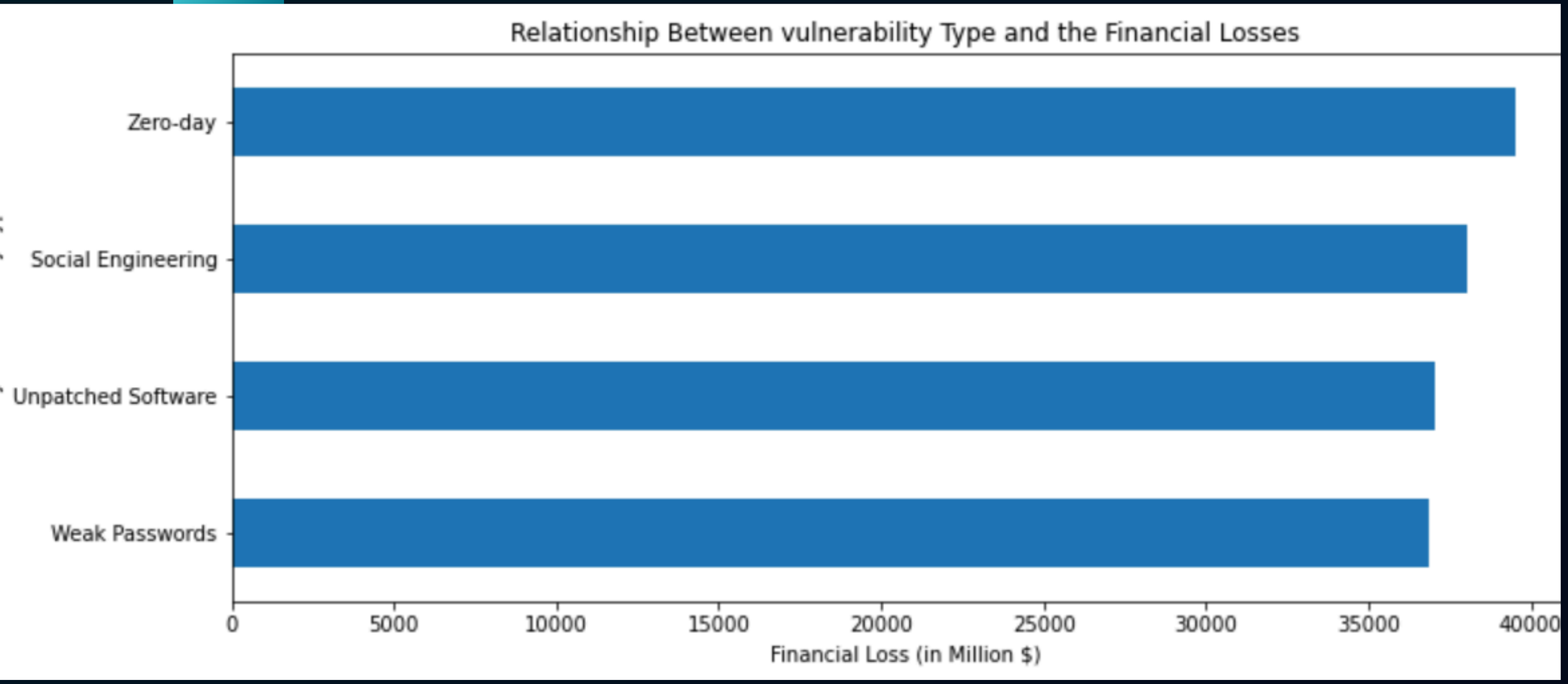
Number of Affected users by Attack Type



Australia had the highest number of people affected by malware and DDoS attack,Brazil SQL Injection and DDoS.Most peple in Germany also suffered SQL Injection attacks while Russia saw the highest number of ransomeware attacks.The other countries,China,Japan were fairly uniformly distributed.

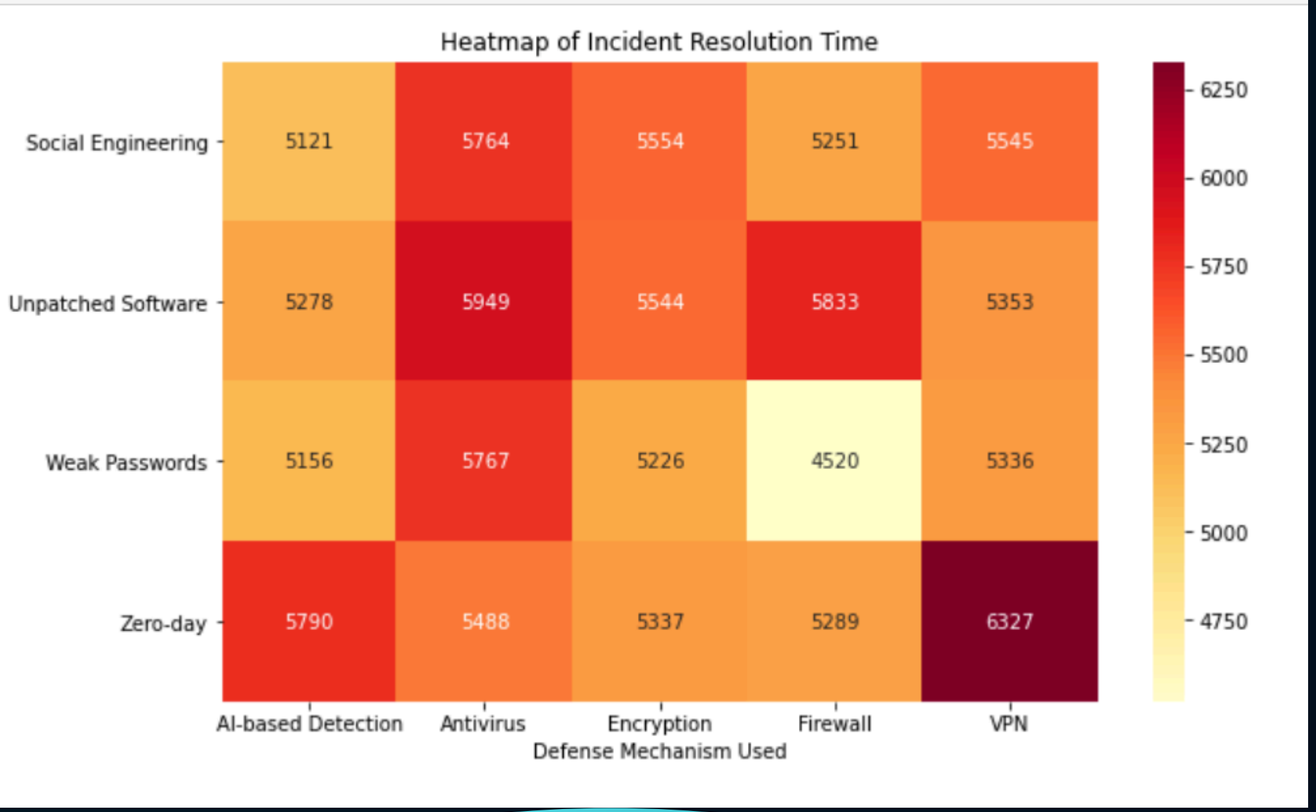
DATA ANALYSIS AND VISUALIZATION

06 Financial Impact of the different vulnerabilities



Zero day resulted in the greatest financial loss followed by Social Engineering,Unpatched Software and lastly weak passwords. Zero day result in higher losses because they are not easy to detect and prevent due to their exploitation of unknown vulnerabilities

Weak passwords bottomed,with about 37,000 million loss reported.This is because passwords may be coupled with other measures such as firewalls thus preventing further system intrusion.



Generally,firewall performed the best against weak passwords with a cumulative incident resolution time of 4520 hours.It also performed well at mitigating Zero Day attacks at 5289 hours.AI Based Detection performed well for Social Engineering and Unpatched Software.

Antivirus and VPN were the worst performers.Antivirus are least effective because they mainly rely on known threat signatures making them weak against new attacks.VPNs encrypt traffic and protect data in transit but does not detect malicious content.

Vulnerability Type	Best Mechanism	Worst Mechanism
Social Engineering	AI-based Detection	Antivirus
Unpatched Software	AI-based Detection	Antivirus
Weak Passwords	Firewall	Antivirus
Zero-day	Firewall	VPN

CONCLUSION

RECCOMMENDATION