Global Cyber Security Incidents - Q4 2022

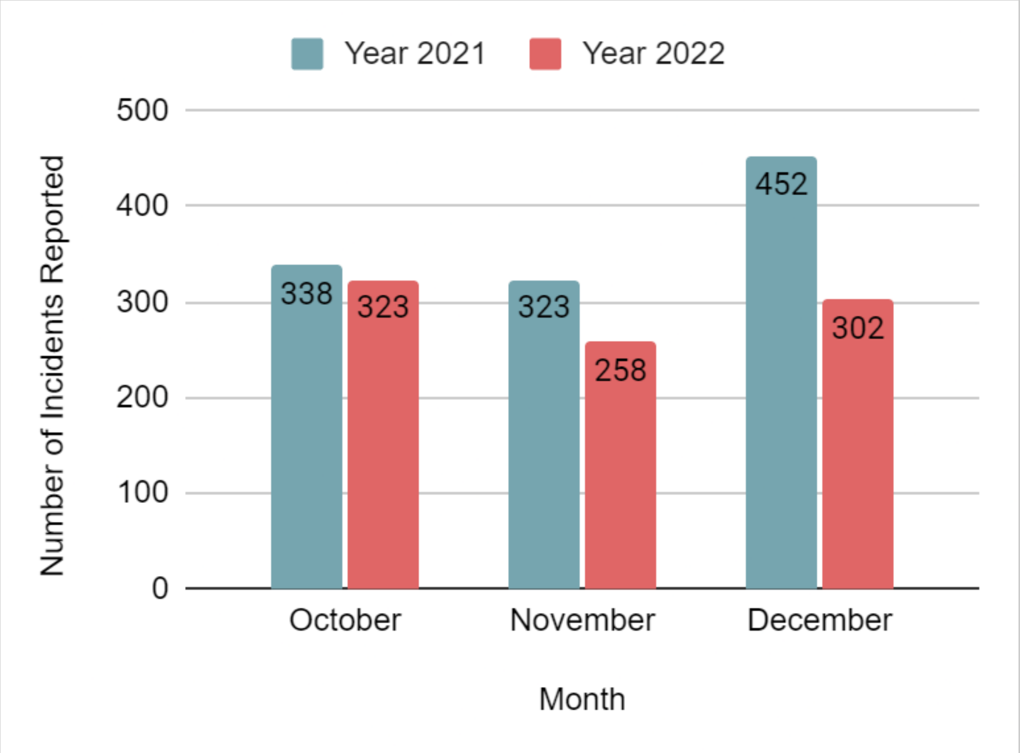
CloudSEK TRIAD Team

Overview

Data gathered from XVigil indicates a decline in cyber incidents in the last quarter of 2022 accounting for 17% of the total recorded incidents. Overall this quarter received fewer incidents than in 2021 with a sharp drop observed especially in the month of December.

A deeper analysis of data revealed the following two prominent changes in the types of attacks recorded:

- A significant increase was observed in Ransomware activity, which accounted for 18% of the TTPs employed by adversaries.
- The government sector saw an increase in cyber-attacks and emerged as the most targeted industry.



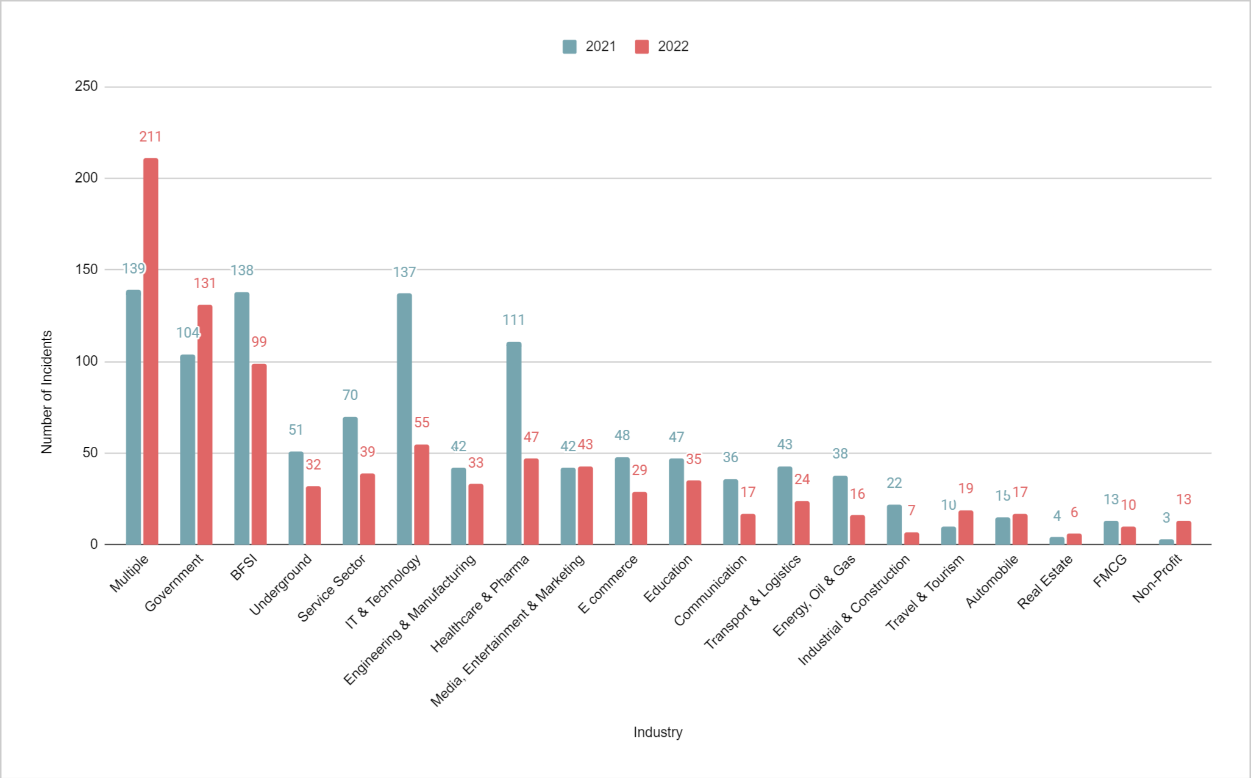
Number of incidents recorded in the last quarter of 2021 and 2022

In this report, we have provided an overview of the major trends* observed in the global threat landscape in the last quarter of 2022 and their correspondence with the trends in 2021.

***Note: The insights and distribution of threats by region are contingent on the presence of our clients in those regions.**

Most Targeted Industries

- Majority of incidents reported in the last quarter of 2022 impacted more than one industry, hence, Multiple emerged as the most targeted sector accounting for a 52% increase in recorded cyber incidents from 2021.
- Attacks of the Government sector increased significantly and it emerged as the second most targeted sector.
- While BFSI, IT & Technology, and Healthcare & Pharma; the three most targeted sectors of 2021; all witnessed a gradual decline in the number of targeted incidents, yet managed to stay in the top 10 targeted industries in 2022.
- Entities belonging to the Travel & Tourism and Non-Profit sectors also experienced an overall increase in the number of targeted cyber incidents in the last quarter of 2022.

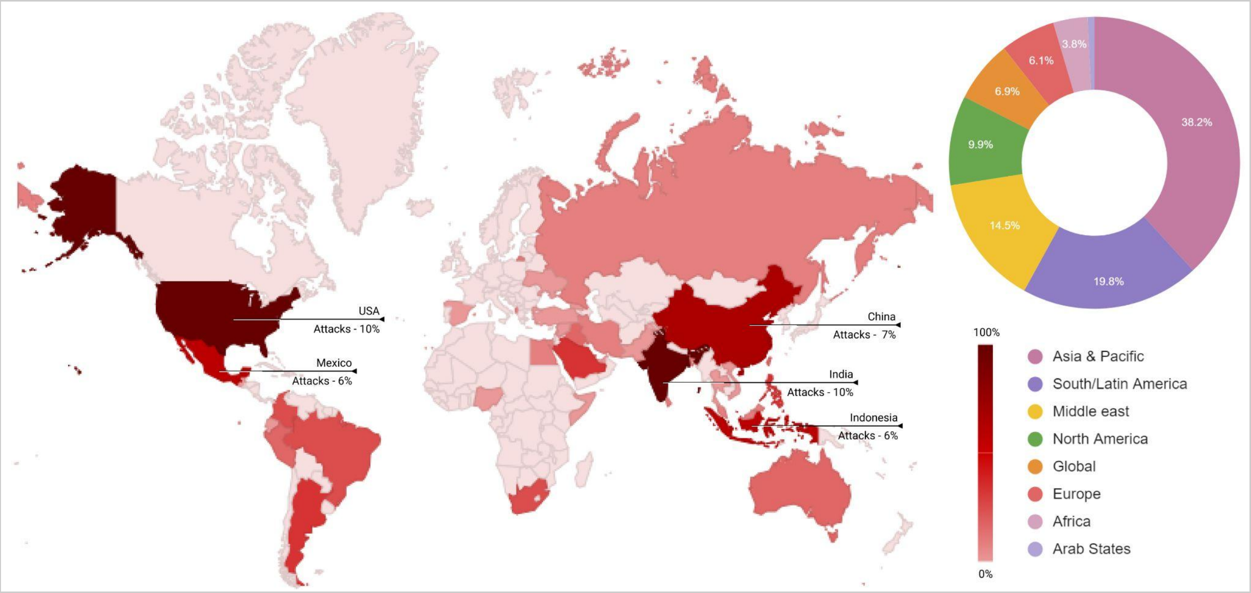


Trends observed in the most targeted industries in the last quarter of 2021 & 2022

Industry in Spotlight - Government

- As government-centric attacks increased in Q4 of 2022, Asia & Pacific became the most affected region in this sector, with the maximum percentage of incidents reported from India (10%), China (7%) and Indonesia (6%).
- Even though the USA (along with India) loomed as the most targeted country in this sector, North America collectively landed on the fourth position in the list of most affected regions (in the government sector).

- Mexico alongside Indonesia, ranked third in the most impacted country in this category; thereby making South/Latin America the second most affected region in this industry.
- Surprisingly enough, the Middle East region emerged as the third most targeted region in this sector, in the last quarter of 2022.

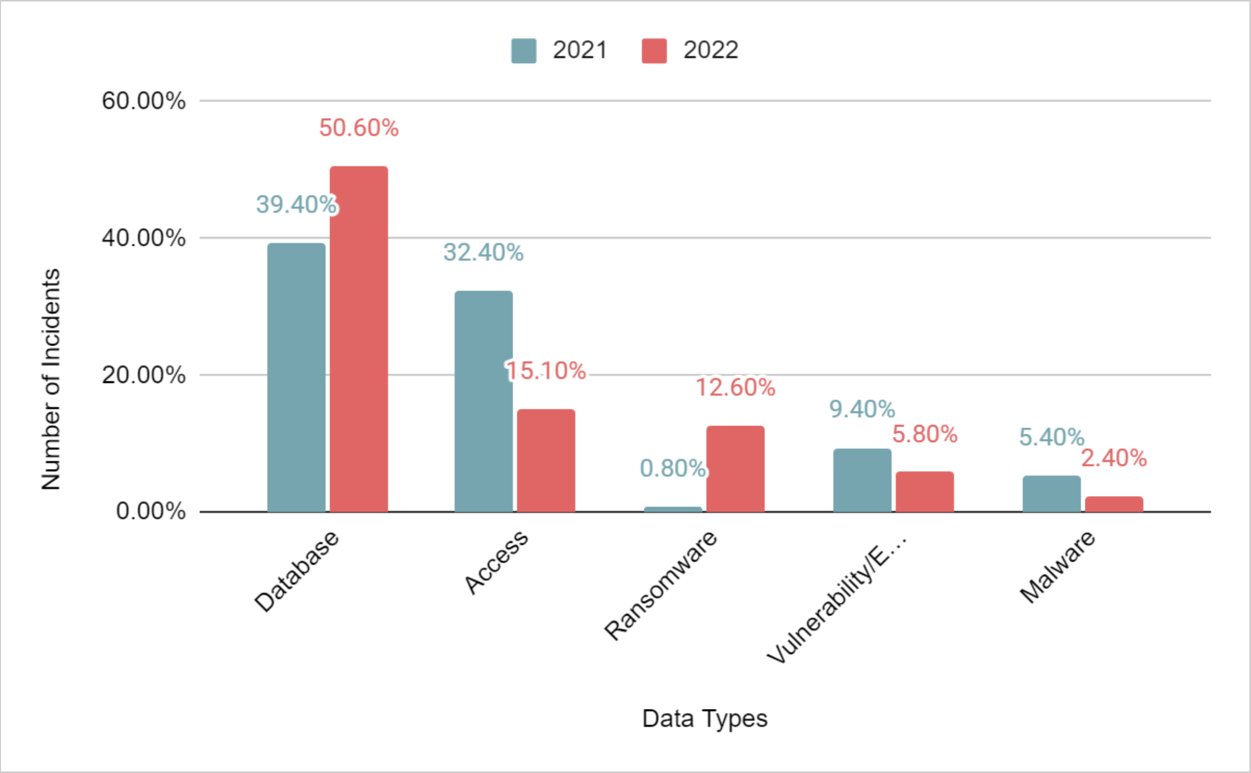


Region-wise distribution of government-related cyber incidents reported in the last quarter of 2022

Most Exploited Data Types

Database and access (primarily initial access) remained the most exploited data types in the last quarter of both the years 2021 and 2022. However, the ratios of their contribution varied, where access was more readily exploited in 2021, than in 2022. This could possibly be due to the hike observed in the number of initial access brokers (IABs) during 2021.

IABs are threat actors who facilitate cyber-attacks, APT groups, and ransomware campaigns. Their increasing numbers in 2021 and the subsequent increase in ransomware activity in 2022 is suggestive of the fact that the IAB market has been proliferating over the past two years.

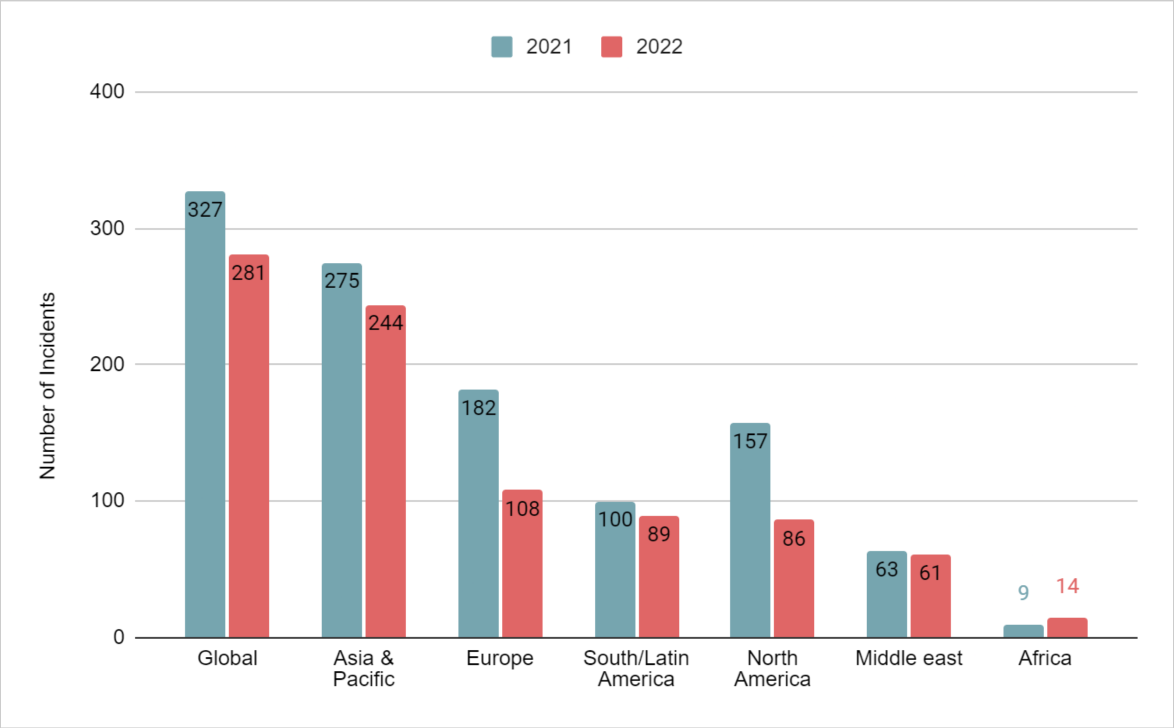


Most exploited data types in the last quarter of 2021 & 2022

While the overall exploitation of malware and vulnerability data types decreased in this quarter, the rise in ransomware exploitation is significant. LockBIT, RansomHouse, Everest, BlackCat, etc. were some prominent ransomware operators observed active in Q4 OF 2022. The ransomware attack on AIIMS, India was one of the notable incidents of this period.

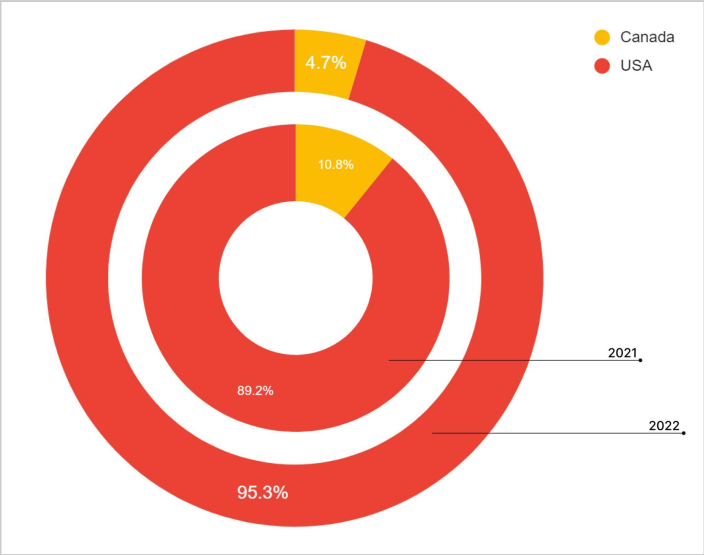
Most Impacted Regions

As usual, most of the reported incidents had a global impact which was closely followed by Asia & Pacific, Europe, the Middle East, and Africa. However, an interesting shift occurred in the position of North and South/Latin America. North America witnessed a drastic decrease in attacks in 2022, as compared to the number of attacks in 2021.



Number of incidents recorded in each region in the last quarter of 2021 and 2022

Region in Spotlight - North America

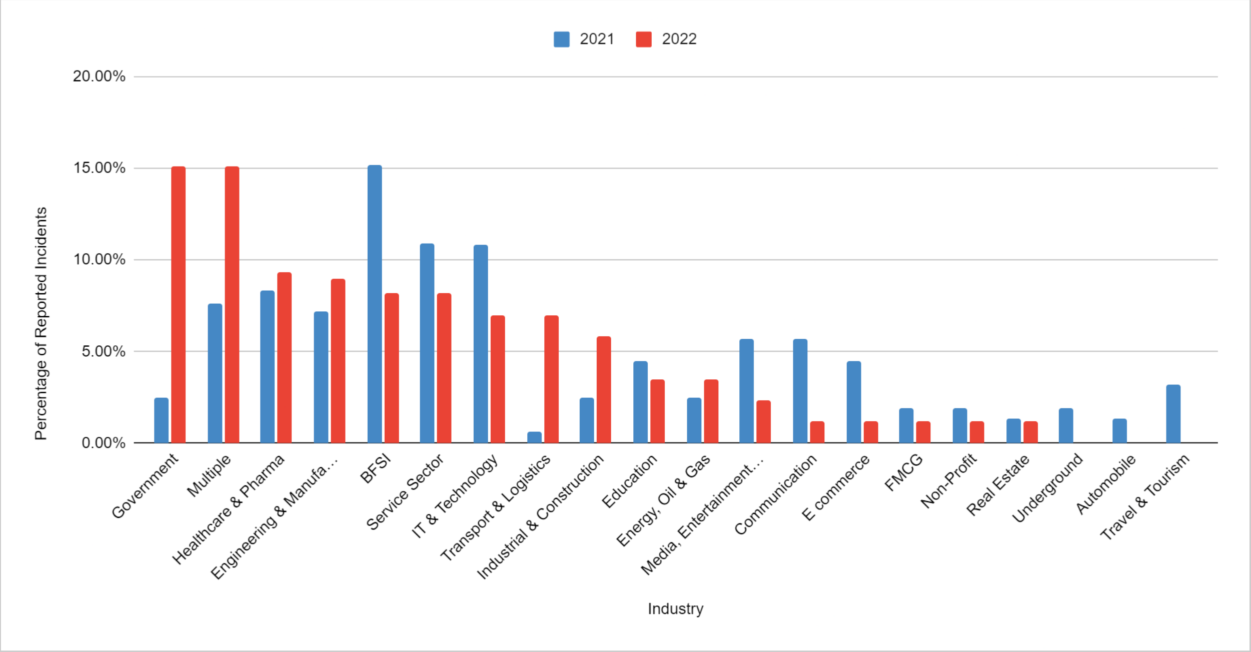


USA & Canada's contribution in the last quarter of 2021 & 2022

Due to the irregular and unusual decrease in the number of incidents reported, North America has become the region of the spotlight in this quarter. A majority of incidents reported in this region were from USA and Canada in both 2021 and 2022. Even though USA's contribution to this statistics increased by 6% in 2022, there was an overall decrease in the number of targeted attacks.

A significant paradigm shift was observed in the industries targeted in this region, from 2021 to 2022.

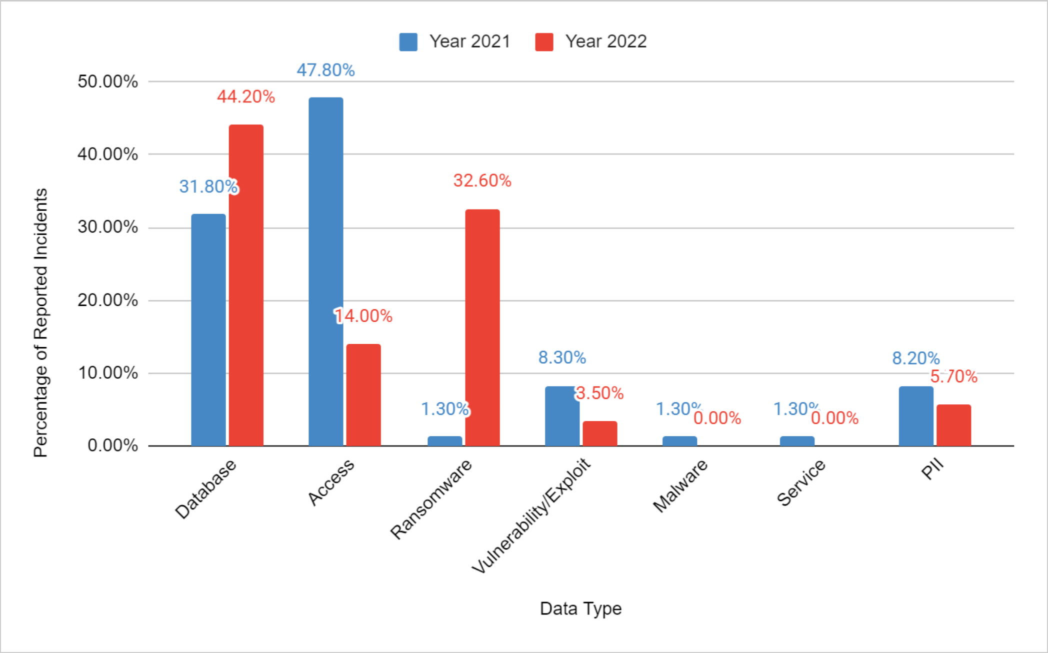
- The attacks related to the government sector increased so much that it became the industry with the maximum number of reported incidents, accounting for 15.1% of the total incidents. This number was equal to the number of incidents targeting multiple industries in this region.
- The number of incidents reported under the Healthcare & Pharma and Engineering & Manufacturing industries increased in 2022 and they became the **second and third** most targeted sectors in 2022.
- BFSI, Service Sector, and IT & Technology; the top 3 three targeted industries of 2021; all witnessed a drop in the number of recorded incidents, however, they still managed to be the **fourth, fifth, and sixth** most targeted sectors.



Trends observed in the most targeted industries in North America

The data types exploited by threat actors to compromise entities in this region also differed greatly in 2021 and 2022.

- Access (primarily initial access) was the most exploited data type in this region in 2021. It accounted for nearly 50% of the employed TTPs, which is significant because such a pattern has almost never been noticed.
- Ransomware activity increased tremendously in 2022, accounting for 32% of incidents reported in this region. Whereas, other malware activity and threat actor services became almost negligible.
- Database was the most targeted data type in North America in the last quarter of 2022.



Trends observed in the data types exploited in North America in the last quarter of 2021 & 2022

Interesting Campaigns Uncovered

Black Friday Themed Cyber Threats

While scourging through the various cybercrime forums on the dark web, XVigil uncovered a series of posts/advertisements discussing the various scam campaigns based on the Black Friday holiday. Multiple threat actors were seen planning and looking for advertisements featuring Black Friday sales in order to target the customers of various e-commerce, cryptocurrency, and travel brands.

FIFA World Cup Qatar 2022 Cyber Threat Landscape

The international football tournament FIFA has attracted millions of people from all over the world and has a large fan base. It has also caught the attention of cybercriminals across the globe, who have begun coordinating in organized campaigns to scam and exploit football fans in order to make a quick buck. XVigil findings indicate that APT campaigns, phishing, credit card fraud, DDoS attacks, and identity theft were among the threats faced by organizations and audiences involved in FIFA.

Conclusion

Although Q4 of 2022 saw a slight decline in cyber incidents as compared to Q4 of 2021, it doesn't necessarily mean that cyber activity has decreased in the past year. In fact, the total number of incidents recorded in 2022 has surpassed the total number of recorded cyber incidents in 2021. Cybercriminals around the world have developed a more sophisticated skill set and have become more specialized. Phishing campaigns have become more common than ever and have taken newly improved forms. The number of cybercrime forums has also increased over the past year. Hence, it is necessary to keep ourselves updated with the latest security trends and exercise precautionary measures where ever possible.

References

- Series of Black Friday 2022 Cyber Threats and Malicious Campaigns
- Unauthorized Access to FIFA World Cup Via Hayya Cards - CloudSEK
- FIFA World Cup Qatar 2022 Cyber Threat Landscape - CloudSEK
- Rise of Initial Access Brokers: Threat actors who facilitate cyber-attacks, APT groups, and ransomware campaigns - CloudSEK