Ticketmaster breached in suspected cyberattack targeting Snowflake clients

Description

Snowflake, a cloud storage provider, has reported that several of its customers' accounts were hacked by threat actors who obtained credentials through info-stealing malware or by purchasing them on online crime forums. Among the affected customers is Ticketmaster parent company Live Nation, which disclosed that the hack occurred through an unnamed third-party provider, later revealed to be Snowflake.

According to independent security researcher Kevin Beaumont, Ticketmaster is one of six Snowflake customers targeted in the hacking campaign. The Australian Signal Directorate also confirmed successful compromises of several companies using Snowflake environments. Additionally, Santander, Spain's largest bank, was reportedly hacked in the same campaign.

This news comes after a hacking group known as ShinyHunters claimed responsibility for breaching Santander and Ticketmaster, posting data online as evidence. The group sought millions of dollars for the stolen data, which included customer records and credit card information.

Snowflake has urged all customers to ensure their accounts are protected with multifactor authentication, as compromised credentials were used in the attacks against its customers. While investigations are ongoing, no evidence has been found linking the breaches to any vulnerabilities or misconfigurations in Snowflake's platform.

Beaumont criticized Snowflake for not prioritizing secure authentication, suggesting that the company needs to review its authentication processes to prevent future breaches.

In conclusion, the recent hacks targeting Snowflake customers highlight the importance of robust cybersecurity measures in today's digital landscape. It serves as a reminder for companies to prioritize security to protect their data and customers from potential threats.

Vocabulary List:

1. **credentials** // (noun): Pieces of information that prove a person identity.
2. **malware** // (noun): Malicious software designed to infiltrate or damage a computer system.
3. **breaches** // (noun): Instances where security is compromised.
4. **vulnerabilities** // (noun): Weaknesses or gaps in a system security.
5. **misconfigurations** // (noun): Errors in the setup or configuration of a system.
6. **authenticat** // (verb): To prove or confirm the validity of something or someone.

Vocabulary quizzes

Multiple Choice (Select the Correct answer for each question.)

1. What term is used to describe a significant stage or point in development?

Option: Robustness
Option: Milestone
Option: Enticing
Option: Popularity

2. What term refers to the state or condition of being liked or admired by many people or the general public?

Option: Surpassing
Option: Popularity
Option: Benchmark
Option: Ecosystem

3. What term describes the capability of a system to handle a growing amount of work or its potential to be enlarged to accommodate that growth?

Option: Consistent
Option: Gas fees
Option: Scalability
Option: Innovative

4. Which term refers to gaps or violations especially related to security or protocols?

Option: Credentials
Option: Malware
Option: Breaches
Option: Vulnerabilities

5. What term is used to signify a pact coalition or partnership between individuals or groups?

Option: Exploratory
Option: Alliance
Option: Robust
Option: Sentiment

6. Who are individuals usually consulted for advice or guidance especially in decision-making processes?

Option: Traumatic
Option: Apologized
Option: Advisers
Option: Bias

7. What legal action is started by a plaintiff against a defendant based on a complaint or allegations?

Option: Confidential
Option: Allegedly
Option: Lawsuit
Option: Discrimination

8. What term describes something attractive or tempting usually encouraging engagement or participation?

Option: Credentials
Option: Compromised
Option: Reassures
Option: Enticing

9. Which term describes an event or experience that is emotionally disturbing or distressing?

Option: Spark
Option: Traumatic
Option: Surged
Option: Alliance

10. What term is used to describe malicious software designed to harm or disable computer systems?

Option: Insights
Option: Malware
Option: Surged
Option: Discrimination

Gap-Fill (Fill in the blanks with the correct word from the vocabulary list.)

11. _____ focuses on meeting the needs of the present without compromising the ability of future generations to meet their own needs.

12. The company entered into a _____ with a leading tech firm to develop innovative solutions.

13. Regular physical _____ is essential for maintaining good health and well-being.

14. The software's _____ allowed it to handle large amounts of data without crashing.

15. The field of _____ involves the application of scientific and mathematical principles to design and develop structures machines and systems.

16. The company denied the _____ of corruption made by the whistleblower.

17. Sales of the new product _____ after receiving positive reviews from consumers.

18. The company prides itself on its _____ approach to product development.

19. Public _____ towards the new policy was largely negative.

20. Users complained about the high _____ associated with using the platform.

Matching Sentences (Match each definition to the correct word from the vocabulary list.)

21. The new smartphone set a high for performance and features in its price range.
22. The social media campaign led to awareness of the charity's mission.
23. The singer's latest album gained immense among fans and critics alike.
24. The organization implemented strict policies against any form of in the workplace.
25. Following the public backlash the company for the product defect and offered refunds.
26. Candidates must provide valid to be considered for the job.
27. The cybersecurity analyst identified several in the network's defenses.
28. It is crucial to ensure that the information provided is accurate and before making decisions.
29. Proper authentication protocols are essential to verify the identity of users.
30. All employees are required to keep sensitive information to maintain data security.

Answer

Multiple Choice: 1. Milestone 2. Popularity 3. Scalability 4. Breaches 5. Alliance 6. Advisers 7. Lawsuit 8. Enticing

9. Traumatic 10. Malware
Gap-Fill: 11. Sustainability 12. partnership 13. activity 14. robustness 15. engineering 16. allegations 17. surged 18. innovative 19. sentiment 20. gas fees
Matching sentence: 1. benchmark 2. widespread 3. popularity 4. discrimination 5. apologized 6. credentials 7. vulnerabilities 8. trustworthy 9. authenticate 10. confidential

CATEGORY

1. Business - LEVEL5

Date Created
2024/06/04
Author
aimeeyoung99