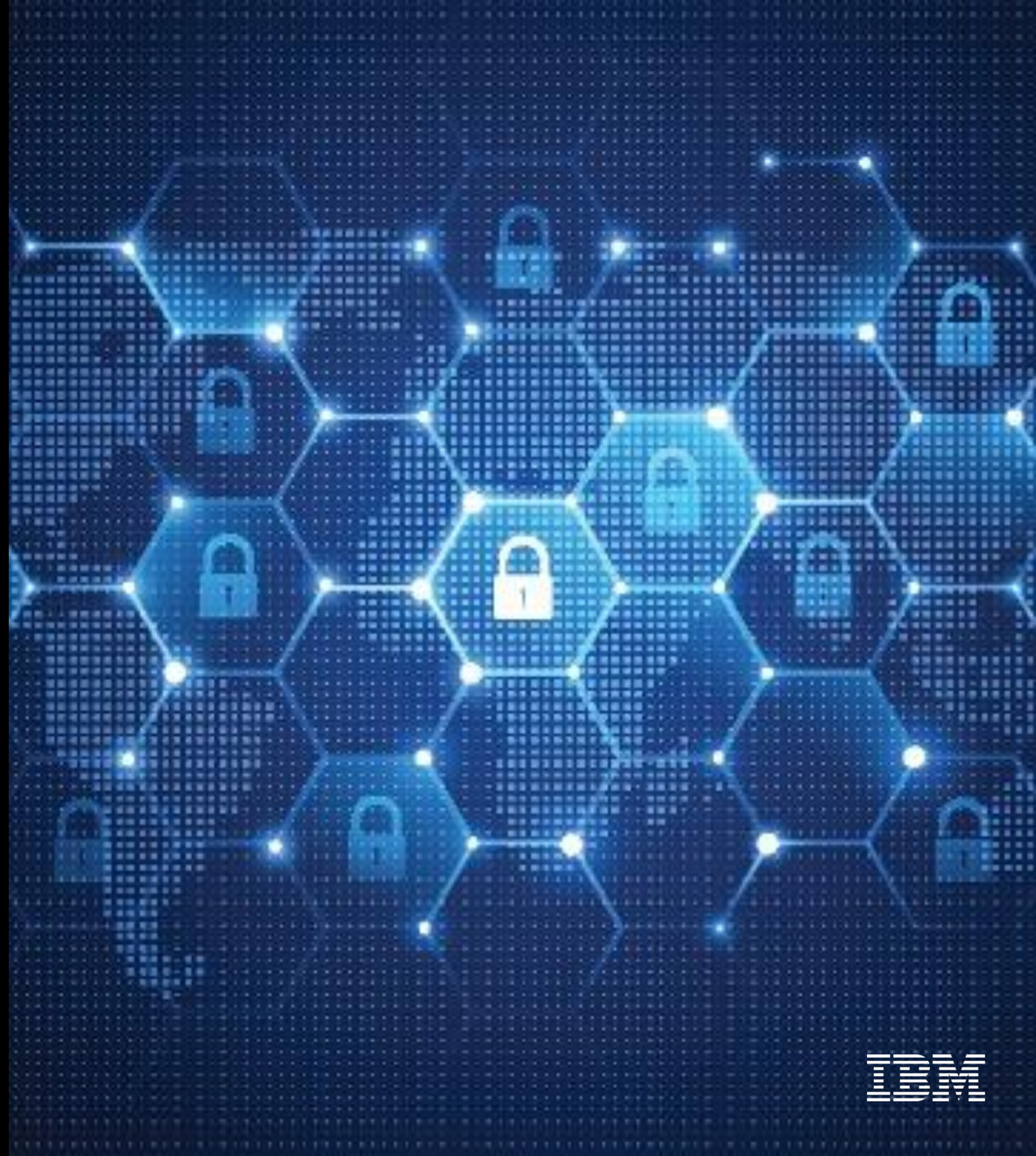
Case Study

Supply Chain Attack

TicketMaster
VIA
Snowflake



Attack Category:
Supply Chain Attack

This incident could be considered as two separate incidents. From my research, Ticketmaster themselves were hit by a Supply Chain Attack because Snowflake was affected by a cloud account hijacking. A Supply Chain Attack is a cyberattack where the attacker targets the supply chain to compromise the security of a larger target. A cloud account hijacking occurs when an attacker gains unauthorized access to a user's cloud computing account. It is likely that Snowflake was hacked via phishing.

Supply chain attacks are devastating to the company and its consumers. According to *Sonatype's State of the Software Supply Chain Report* "here has been an astonishing 742% average annual increase in software supply chain attacks over the past 3 years.". Cybersecurity Ventures predicts that the global annual cost of software supply chain attacks to businesses will reach a staggering $138 billion by 2031.

My sources mainly include blogs, articles, and the press statement provided by Ticketmaster. The list will be provided at the end.

Company Description and Breach Summary

Ticketmaster is a global leader in the sale and distribution of tickets for live events, including concerts, sports events, theater performances, and more. Snowflake is a cloud-based data warehousing company that provides a platform for storing and analyzing large volumes of data. Ticketmaster also used Snowflake to help optimize its operations by supplying cloud data.

In this case, Snowflake reported a cloud account hijacking attack, where stolen credentials were used to access sensitive data. This was performed by the infamous cyber hacker group, ShinyHunters, who put 1.3 terabytes of stolen data up for sale on the cybercrime forum, Breach Forums, priced at $500,000. This included customers' PII, such as their full name, address, and partial credit card information. Almost three months after the attack occurred, the public consumers were informed of the incident.

Timeline

1. Event 1
April 2 - May 18: Unauthorized third party accessed information from a cloud database hosted by a third-party data services provide

2. Event 2
May 20, 2024: parent company Live Nation identified unauthorized activity within Snowflake, a third-party cloud database.

3. Event 3
May 27, 2024: A criminal threat actor offered the alleged data stolen for sale on the dark web.

4. Event 4 May 27:
Media outlets begin to report on the data breach, including it’s timeline and scale. It is reported over 560 Million Users Data were sold.

5. Event 5:
May 28: Parent company Live Nation confirms the data breach in a SEC (U.S. Securities and Exchange Commission) filing.

6. Event 6
Late may - Early June: TicketMaster officially begins notifying affected customers about the data breach.

Vulnerabilities

The data breach form TicketMaster exposed over 560 million customer’s data due to unauthorized access to a third party database control. This breach is a great example of a **Supply Chain Vulnerability.** It emphasizes the risks in associating with third party service providers and the need to have robust cyber security measures across an organization's digital infrastructure.

Third-party Cloud Security

Unauthorized access to Snowflake's cloud database environment containing Ticketmaster data.

Insufficient monitoring

TicketMaster were slow in detecting the potential threat and responding. They should increase motoring in their 3rd party infostructure.

Insufficient authentication

There are reports of clients failing to implement multi-factor authentication (MFA) especially on snowflake’s side.

Credential compromise

Multiple reports of employee’s accounts not being terminated or disabled from being inactive leading to a potential attack vector.

Costs and Prevention

Costs

- Over 560 million Ticketmaster users' personal and payment information was exposed.
- The breach compromised names, addresses, email addresses, phone numbers, ticket sales and event details, order information, and partial payment card data (last four digits, expiration dates)
- While Live Nation stated the breach would not significantly affect operations, it raises concerns about customer data security and potential fraud risks

Prevention

- Adopt a zero-trust, data-centric approach to managing third-party vendors
- Classify any sensitive data. You have to know where user private data is.
- Audit third party supply chains regularly.
- Use next generation DLP solutions.

Sources

State of Vermont Attorney General's Office. (2024, July 5). *Ticketmaster Data Breach Notice to Consumers*. Retrieved from https://ago.vermont.gov/sites/ago/files/documents/2024-07-05%20Ticketmaster%20Data%20Breach%20Notice%20to%20Consumers.pdf

Cybersecurity Ventures. (2023). *Software supply chain attacks to cost the world $60 billion by 2025*. Retrieved from https://cybersecurityventures.com/software-supply-chain-attacks-to-cost-the-world-60-billion-by-2025/

Votiro. (2024). *Navigating the aftermath of the Ticketmaster breach*. Retrieved from https://votiro.com/blog/navigating-the-aftermath-of-the-ticketmaster-breach/

Polymer. (2024). *Prevent third-party data breaches with SaaS DLP (Data Loss Prevention)*. Retrieved from https://www.polymerhq.io/blog/cloud-security/prevent-third-party-data-breaches-with-saas-dlp-dep/

Dark Reading. (2024). *Ticketmaster breach showcases SaaS data security risks*. Retrieved from https://www.darkreading.com/cloud-security/ticketmaster-breach-showcases-saas-data-security-risks

Cside. (2024). *Ticketmaster data breach deja vu: What you need to know*. Retrieved from https://cside.dev/blog/ticketmaster-data-breach-deja-vu-what-you-need-to-know

Polymer. (2024). *Ticketmaster data breach: Everything you need to know*. Retrieved from https://www.polymerhq.io/blog/ticketmaster-data-breach-everything-you-need-to-know/

Polymer. (2024). *What is cloud account hijacking?*. Retrieved from https://www.polymerhq.io/blog/insider-threat/what-is-cloud-account-hijacking/

Netrise. (2024). *The continued increasing wave of software supply chain cyber-attacks*. Retrieved from https://www.netrise.io/xiot-security-blog/the-continued-increasing-wave-of-software-supply-chain-cyber-attacks

HackRead. (2024). *Hackers behind Ticketmaster data breach selling data of 560M users*. Retrieved from https://hackread.com/hackers-ticketmaster-data-breach-560m-users-sale/