Computer Security – CSI1101.2

Ticketmaster Data Breach

Name – Gunarathne Janith Deshan

Student Number – 10676638

Campus - ECU Sri Lanka

Lecture Name – Thaunja Dheemathi Irugalbandara

Table of Contents

1.Introduction

Ticketmaster, a modern global leader in the ticket sales and distribution industry, which operates in over 38 countries worldwide, was hit by a cyberattack this year (May 2024) that revealed the financial and personal information of more than 560 million consumers (Abrams,2024). A highly skilled hacker group planned the attack and took advantage of the Ticketmaster system's vulnerabilities, which resulted in many data breaches. This data breach involves access to information of the customers such as name, email addresses, and credit card details. This incident received much media attention and raised serious questions about cyber security and data privacy (Ulubay ,2024). The significance of strong cybersecurity procedures in safeguarding sensitive customer data. It illustrates how well-planned attacks may affect even large companies with strong safety protocols. It is very significant because attackers demand ransom and expose their target publicity or sell stolen information to other criminals. On the other hand, many adverse impacts resulted from the Ticketmaster attack, such as harm to the brand of business, trust passed down, financial losses for the company, and millions of customers at risk of fraud as well as identity theft (Range, 2024).

This Ticketmaster report is structured by two primary sections such as Hack and Hackers. The first component is Hack, and it gives an in-depth review of the Ticketmaster attack. It starts with an outline of the incident and a timeline of significant occasions. After that will illustrate the type of techniques hackers used to gain access to the system, what type of data they stole and how it affected the major security principles in compromising confidentiality, integrity and availability (CIA). The second main component is Hackers. It examines who or what group was responsible for this attack and includes their methods of entry, fraud and motivations that they retrieved.

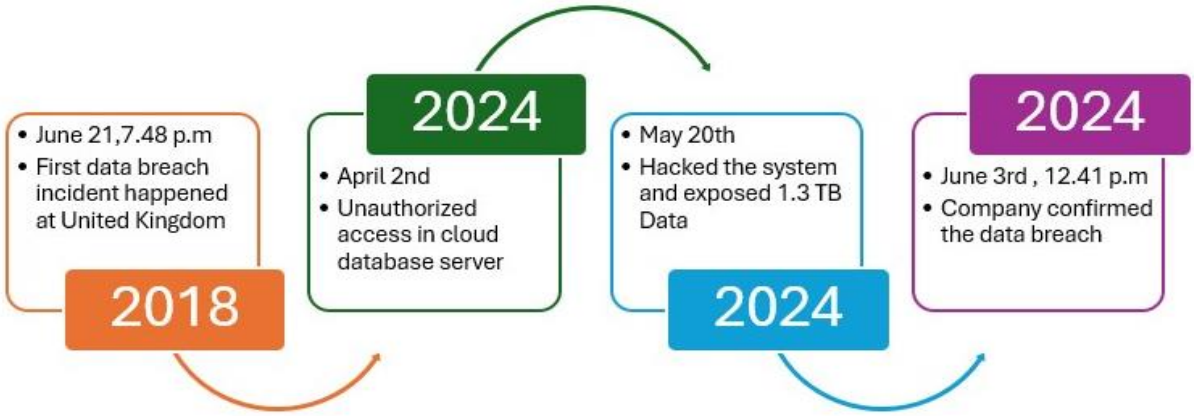
2. The Hack

2.1. Overview of the Ticketmaster Incident

The Ticketmaster is a huge limitless profitable entertainment company located in the United States that retails tickets to worldwide people for entertainment events. In January 2010 they merged with an entertainment company called Live Nation then they called Live Nation Entertainment (Lorsch, 2023). Firstly, this company sells their paper tickets hand to hand but after August 2015 they started to issue digital tickets online. At this moment the company has taken a policy that someone who buys the tickets from websites or any online platforms, first must identify themselves and then they can buy

their tickets. According to this in 2019 they earned 11.9 billion US dollars by selling tickets on online platforms for their events (Gallo, 2023). Even though two times Ticketmaster system got hacked by using various types of cyber-attacks. The first one happened in 2018 in the United Kingdom by using malicious software by a customer support tool provided by a third-party company. It confirmed exposed data in 40,000 customers who bought tickets between February and June 2018 (*What Happened in the Ticketmaster Data Breach? | Twingate*, n.d.). The second one appeared on April 2 and May 18, 2024, unauthorized access in a cloud database hosted by third-party service provider to access the personal information of consumers including payment details. But the administration recognized it on May 20, 2024, and hacked the cloud database of the Ticketmaster system with exposed information of 560 million people in the world. Even though the main company of Ticketmaster, Live Nation Entertainment didn't confirm and publish this data breach until 12.41 pm Monday, June 3, 2024 (Waqas, 2024).

Figure 1 –Timelines Of Ticketmaster



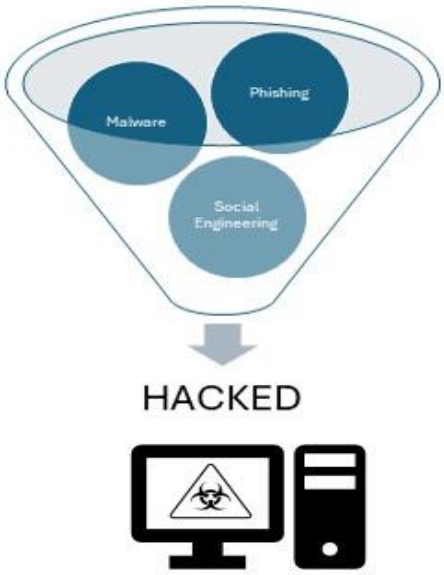
Note. This timeline diagram shows incidents happening at Ticketmaster scenario according to the report of (Waqas, 2024). (self constructed)

2.2 The hacking group compromised the system

The first cyber-attack on the system in the United Kingdom was affected by some using of malicious software by providing third-party applications. The attackers use Phishing attacks to trick the customer with supportive tools and links (Page, 2020). This malware attack affects all data of the user's computer by viruses, worms, trojan horse concepts etc. In second the attack, hackers enter the system through a third-party cloud database used by Ticketmaster company which stores tons of customer information. Taking advantage of vulnerability in cloud services is the major thing that worked for them to get access to the system (Team, 2024). According to that, this incident shows how supply chain vulnerabilities make issues in big network server companies that may be affected without attaching directly to the main server. A lot of

companies do this because they only focus on their main servers' data protection. Another main component of this hacking is they used to get some sensitive information such as passwords, IPs, and user IDs about the system by tricking employees of the company. This method is called social engineering. According to the records of 2024, presently 6,678 employees work in this company. After the data breach, hackers take 1.3 Terabytes of data from the server, and they demand a ransom of 500,000 dollars or they sell the data on the dark web. However, the parent company of Ticketmaster, Live Nation didn't respond anything to the threat (Whittaker, 2024).

Figure 2 - Methods used by hackers to breach a system



Note. Basic techniques used for hacking a system or cloud server (Self-Constructed)

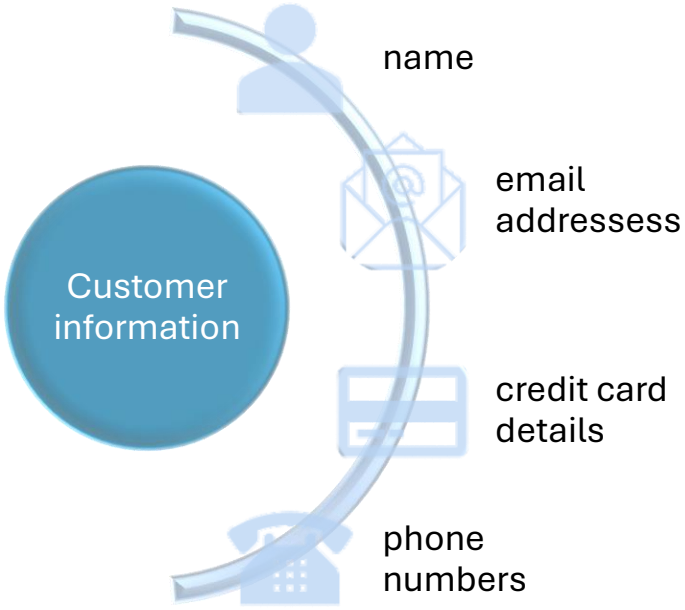
2.3 Type of data steals in the incident

Firstly, the company mentions when logged into their accounts customers must prove their identity (Wikipedia contributors, 2024). So, Ticketmaster users must create an account in the Ticketmaster server with personal information such as name, age, address (if needed for refund) and email address data like sensitive information of the customer. According to that they breached the data of names, addresses, event details, payment details, phone numbers and ticket sales. On the other hand, the major thing among these details is the financial details of customers. Credit card and Debit card details including the last four digits, CVV numbers, and expiration dates of over half a billion people data breached from the servers (Bond, 2024).

The well-known hacking group called ShinyHunters claimed that they were responsible for this attack (Snider, 2024). Also, the customers have a risk of identifying themselves

as theft because attackers use these details for pretend open bank accounts, take out loans and commit to other crimes like criminals.

Figure-3 Sensitive data of customer

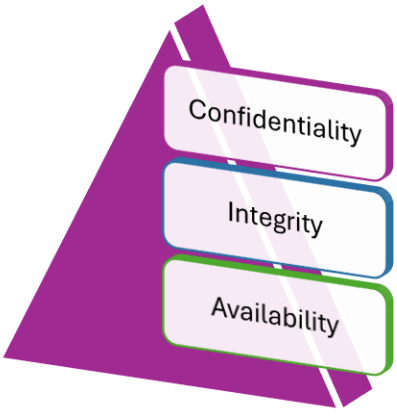


Note. The diagram illustrates the types of data breaches from the customer (Self-Constructed)

2.4 Security Triad (CIA) of Impact on the Ticketmaster

Confidentiality, Integrity and Availability are the three fundamental tents in the CIA triad which were compromised immediately in the Ticketmaster incident on 24th May 2024. These three concepts constitute the main foundation of any security plan and are important for preserving a system's reliability and trustworthiness.

Figure-4 CIA Triad



Note. The diagram includes the main components of breaches in cybersecurity (Self-Constructed)

2.4.1 Confidentiality Breach

The most significant in this case is confidentiality because it only allows to access users who are only authorized by the cloud server. Although several vulnerabilities of the cloud server such as poor security measures, weak encryption of data, outdated software and third-party hosting services in the cloud server. According to the video of BBC News on the 23rd of June 2024, attackers identified Ticketmaster using a third-party cloud service provider to store the sensitive data of customers. This hack shows several risks to the supply chain in servers of companies that even have strong security in Ticketmaster headquarters but outside, vendors can still trigger vulnerabilities on their systems. Full names, Email addresses, Phone numbers, Physical addresses, Order details and financial data were breached by hackers to demand their ransom from Ticketmaster (Tara Deschamps, The Canadian Press, 2024). In many cases, poor encryption of clients' data was poorly encrypted or was encrypted just partially, which made it easier for hackers to steal the data. Strong encryption of data protocols has limited the scope of the hack and it harder to break by hackers (*Data Confidentiality*, n.d.)

2.4.2 Availability Breach

Availability is not a special target in this attack, but it was necessarily affected by the breach's functional aspects. Ensuring that system and data are available when needed is known as availability. After the attack, Ticketmaster had to temporarily shut down their systems to mitigate the breach and examine what happened to the system (Schneid, 2024). According to that, this availability could affect the platform's ability to serve the service to users rapidly such as delayed ticket sales and loss of their incomes.

2.4.3 Integrity Breach

The main goal of this attack is to steal the data. It’s important to take seriously any integrity threats that could result from the breach. Trustworthiness, reliability and accuracy of data are guaranteed by integrity in cyber security (Security, 2024). In this scenario, unauthorized access may have allowed the attackers the ability to change or destroy the data, even though there were no verified complaints of data being changed. They might have changed order histories, interfered with client information, or even introduced malicious data into the system. According to that it affected the company's business, attackers could damage revenue and customer trust by manipulating inventory data or ticket availability, which could result in overselling or underselling events. These kinds of integrity violations can result in monetary losses, legal troubles, and reputational harm. Live Nation said it did not believe the breach would have “a material impact on our overall business operations or our financial condition or results of operations.”(The New York Times)

2.5 Post–Breach Remediation Actions by Ticketmaster

> Following to the incident in May 2024, Ticketmaster moved quickly to repair the breach,minimize the harm, and win back the trust of its customers.(New York Times)
>
> -- (*Ticketmaster Entertainment Inc.*, n.d.)

Ticketmaster responded quickly to the cyberattack handling the situation and determining the scope of the attack to avoid further attacks. Managing this attack is protecting the systems that were compromised, and being open and honest with the impacted consumers were the company's primary objectives.

2.5.1 Initially Shutdown the services

When the Ticketmaster's incident happened, the security group of Live Nation Entertainment identified unauthorized access on their third-party cloud database cooperating with a company called Snowflakes (Whittaker, 2024b). The admins of the system immediately shut down the servers temporarily to become aware of the breach and examine the vulnerable areas of the servers (CityNews, 2024). This is the fundamental action gained from any server admins when a data breach incident happens to their system. This step stops the attacker's activity and limits the amount of sensitive data exposed by the database.

2.5.2 Customer Assistance and Notification

In this occurrence, Ticketmaster found every customer who was affected by this data breach, and they informed all about this incident in accordance to laws including the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). These CCPA and GDPR frameworks govern big tech companies on how to manage personal data regarding data breaches (Newsnation,2024). The company took support from customers who were affected by this attack and informed them how to mitigate it by doing some protection actions such as changing the usernames and passwords of their accounts, changing credit card and financial details etc (Tidy, 2024).

2.5.3 Boosted Safety Protocols of the system

After the data breach, Live Nation Entertainment's CEO decide increasing the frequency of their security inspections, implement advanced systems for detecting breaches, and improve their encryption techniques to give high protection of their customer's sensitive data (Uliss, 2024). Also, Ticketmaster redesigned their vendor risk management policies, enforcing stronger identification protocols and ongoing oversight of third-party providers.

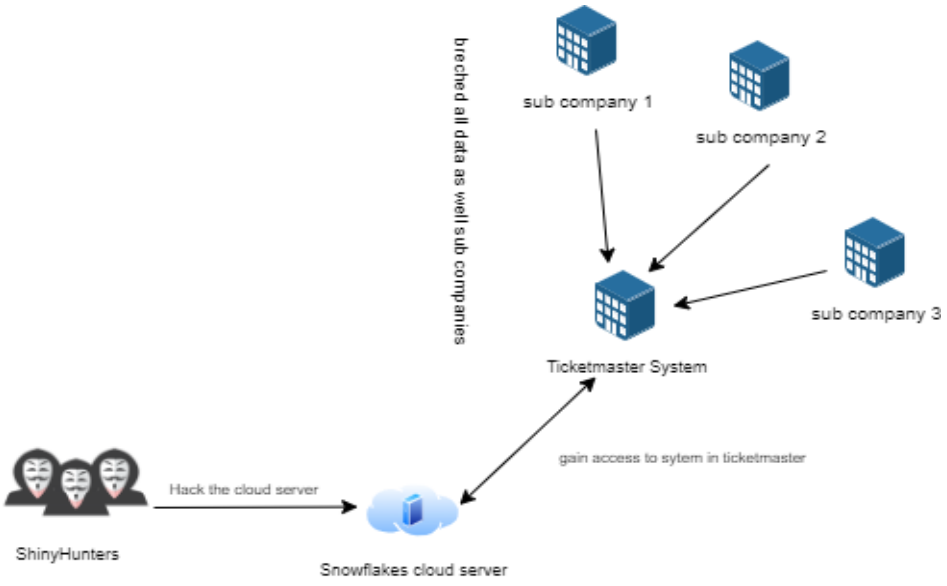
2.6 Is Ticketmaster was unprepared for this attack?

This attack was a breach of a sub-server of Ticketmaster company which is handled by a third-party cloud database server managed by Snowflakes company. In my point of view, the major blame goes to the Ticketmaster company because, Ticketmaster was affected by data breaches in 2018, according to that the company has been responsible and pre-prepared for the protection of their client's information due to they have experienced breach on earlier.

2.7 Ticketmaster breach was a random incident or target attack

The incident of Ticketmaster was considered about specially targeted attack due to the value of its data (sensitive personal information) and financial gain for the attackers. The highly skilled attackers were well planned this attack by taking advantage of vulnerabilities of third-party cloud servers and weak encryption of customers' data. According to that attackers know this data has a highly valuable price in the dark web (Sky News, 2024). Hackers used an organized plan to find the weak points of Ticketmaster supply chain servers for access to their main target. Such demonstrates their records this was a random incident done by hackers unplanned, but examining the inside of the attack illustrates they attacked the cloud server, but its main achievement is the fall down of Ticketmaster company. Not only that, but this self-serving hack also hit several businesses at once. Attackers were focused on Ticketmaster, but that aim compromised to affect one single organization with maximum impact on other sub-joined companies as well.

Figure 5 – Breach of attack affecting to supply chain of Ticketmaster



Note. Supply chain attacks in Ticketmaster affected other servers/companies from breach of data in third-party cloud server in the system (Self-Constructed)

3.The Hackers

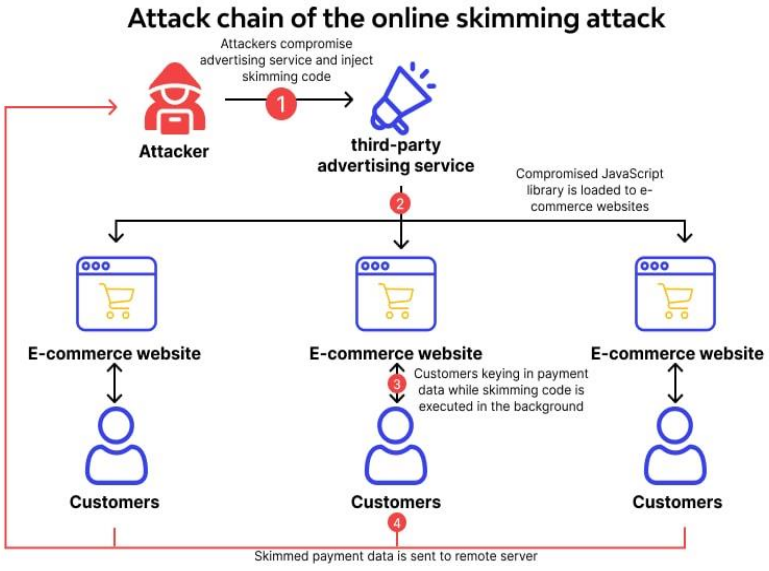
3.1 Hacking Group Capabilities, Motivation and Type of Attack

3.1.1 Capabilities of Hackers

A lot of reports record the master mind hackers of this Ticketmaster scenario is ShineyHunters but on the other hand, some of the reports illustrate the hacking group called Magecart was directly responsible for this attack (*Report URI: Case Study - Ticketmaster*, n.d.). According to that, this case was done by several teams of hackers because it's anonymous. But it cannot be proved 100% who was really behind this scenario, because investigation progress is going on. (The recommendation for this report accepts the ShineyHunters involved in this attack.)

This group of hackers (ShineyHunters) did this cyber attack to target insecure third-party e-commerce websites by injecting JavaScript-based malware to exploit financial and credit card details (Turnkey Cybersecurity and Privacy Solutions, LLC, 2024). Cybercriminals compromise third-party services such as chatbots, advertising and payment gateways to spread inject the malicious code (Human, 2023). According to that attackers can capture the customer's sensitive information in real time as they input data.

Figure – 6 shows the attack chain of digital skimming



Note. Lee, I. (2024, February 26). What is Magecart Attack? ⚔️ How to prevent it? Wallaarm https://www.wallarm.com/what/what-is-magecart-attack-how-to-prevent-it

3.1.2 Motivations of Hackers

The primary goal of this Ticketmaster attack was to take profit from stolen sensitive information by selling it at marketplaces on the dark web. According to the year 2024, attackers used to breach the data by using bots in Automated Attacks (*Engadget Is Part of the Yahoo Family of Brands*, n.d.). Mostly in this modern generation

hackers use them to run automated tasks in attacks such as data indexing and attack execution. So, this takes minimal risk to identify themselves and less effort to do their attack (Brogniart, 2022) while getting high financial benefits. Not only that they take the opportunity of time that they must breach the data because May to June has the biggest entertaining events held in Europe and the United States due to the summer. So a huge amount of people participated in those events, and according to that period, they can increase the volume of their data exploited.

3.1.3 Types Of Ticketmaster Attack

- Attack on the supply chain

  Exploit the vulnerabilities of third-party services to access the main target and attackers use it to spread the malware across all sites using the Ticketmaster service (Team, 2024).

- E- Skimming

  Injecting some malicious JavaScript code to gain access to check pages of payment gateways in e-commerce platforms like Ticketmaster, and collect financial information such as card numbers, transactions, and CVVs.Then attackers can hack the servers by exfiltrating data (*What Is Skimming: Examples and How Does It Work?*, 2023).

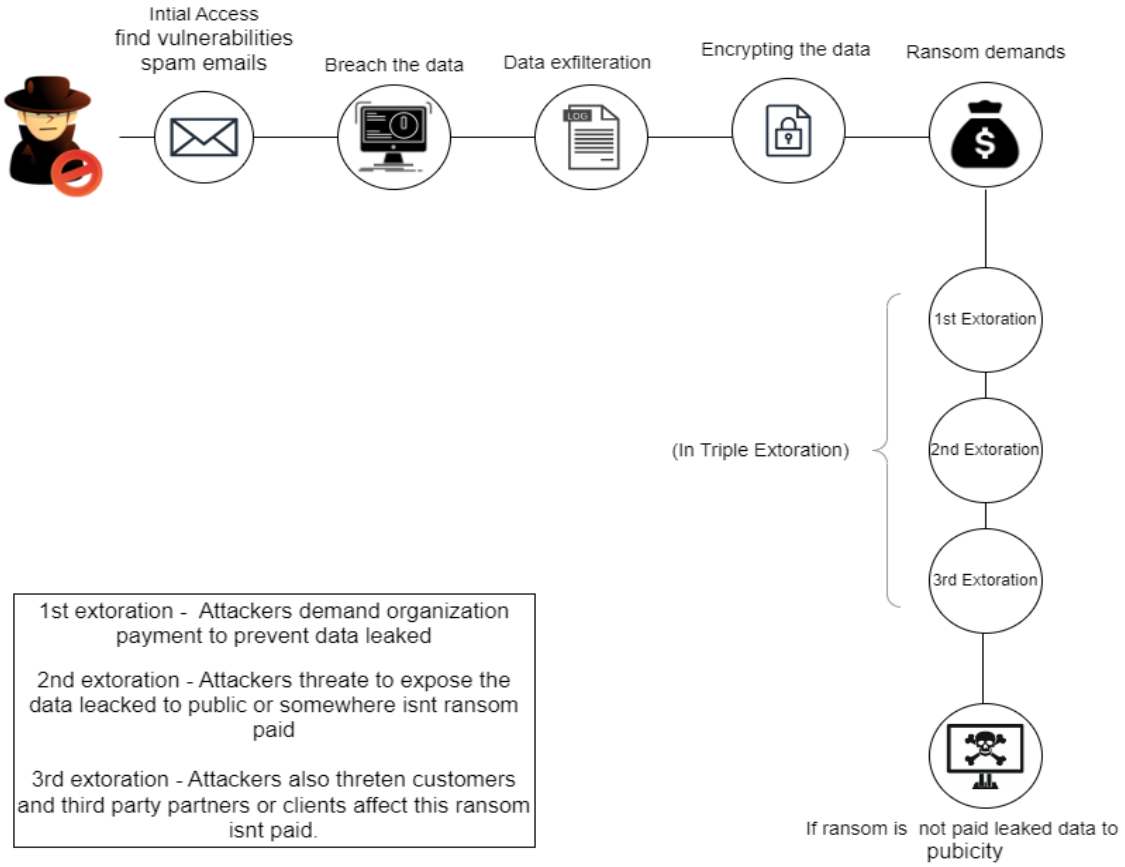
- Social Engineering and Phishing

  Attackers use this method to trick their targets individually such as employees and customers, by sending frudable emails, advertisements and messages to reveal sensitive information to take a chance at accessing the system (Social-Engineer, LLC, 2024).

3.2 Double and Triple Extortion Attacks

Double Extortion attack is initially encrypting the data of some person by using ransomware, then threatening if the ransom is not paid the data must be public on the dark web or any other platforms. In Triple Extortion, attackers demand the same in the target organizations or customers including additional threats (Tatar & Tatar, 2024).

Figure – 7 Steps of Double and Triple Extoration Process



Note. This diagram illustrates the basic steps of double and triple extortion that happen (Self-Constructed)

In this Ticketmaster scenario, was triple extortion after breaching, exfiltrating and encrypting the data, standardly demanding their ransom, but Ticketmaster Admins haven't paid the ransom. According to that hackers have to approach the triple extortion technique.

3.3 Techniques used for infiltration in Ticketmaster

3.3.1 Techniques in Infiltration

- JavaScript Injection Malware

  The malicious JavaScript was injected by attackers to access the payment page of Ticketmaster (*Report URI: Case Study - Ticketmaster*, n.d.).This is responsible for the collection of payment information of the customers.

- Third-party vendor breach

  As referred in above 3.1.3, hackers' main target was Ticketmaster, but they targeted to enter the holes of Ticketmaster infrastructure and then they know they can gain access to the main system (Masas, 2023). According to that hackers can breach their data by undetected to the Ticketmaster main system.

3.3.2 How Hackers Been Successful

The attackers got outside of Ticketmaster's primary defences by concentrating on a third-party provider and didn't detect their malicious code in the Ticketmaster system because it originated from a Ticektsmaster's trusted service provider. These techniques were used by hackers, allowing the attack unnoticed by the Ticketmaster server for several months (King, 2024).

4. Other Identities used by involved threat actors

- Whitewarlock (Wiesel, 2024)
- ShineyHunters
- SpidermanData (Jain, 2024)
- Sp1d3r Hunters (Arntz, 2024)

5. Indicators of compromise (IOC's) steps to protect the system

- Unusual traffic leaving the network

  There has been a lot of traffic leaving the network is an alert to spot possible problems in the system. So the administration and IT management of the company can closely monitor outgoing traffic patterns to see if there is something strange of the system routine. This can be used to neutralize a variety of threats providing immediate actions to them (*Indicators of Compromise (IOCs) | Fortinet*, n.d.).

- Geographical Abnormalities

  If some attempt to log in from other nations which company does not usually conduct business may indicate a possible security breach on the system. It can be evidence hackers trying to attempt to access the system by other nations by hiding their IP addresses (*What Are Indicators of Compromise?*, 2024). A large number of cyber criminals' IPs are in different countries especially unpopular names. According to that admins know or gain details about those countries

- Unauthorized Logins

  Usually, valid users must make a few more attempts to log in to a system, but repeated attempts could be a sign of a malicious attack trying to get access to the system. Also, if they fail to log in to the system, this can indicate someone is testing user accounts to see if any of them will grant them unauthorized access (*Indicators of Compromise (IOCs) | Fortinet*, n.d.).

6. Summary

In the conclusion of this report In May 2024 Ticketmaster cyberattack compromised the sensitive data of over 560 million customers including their names, email addresses, phone numbers and financial details of their credit cards. The components of the CIA triad Confidentiality, Availability and Integrity were severely harmed by this breach of security. The primary breach of confidentiality was caused by risks such as identity theft and phishing fraud to expose sensitive customer information. Integrity was not the main aim of the attackers in this Ticketmaster scenario, but the potential for data manipulation was created by using illegal access. Furthermore, investigation and security measures indirectly harmed the availability of the system by triggering service interruptions. The Ticketmaster incident was a directly targeted attack from a hacker group called ShineyHunters or Magecart because it cannot be selected which group is behind this attack until investigations are finished. Lastly, this breach serves as a reminder of how connected these security principles are and how one weakness can lead to vulnerabilities in the whole system. The Ticketmaster incident was a good experience for other e-platform companies to safeguard confidential client data and preserve trust among the customers in their services.

7. References

- Abrams, L. (2024, June 28). Ticketmaster sends notifications about recent massive data breach. *Bleeping Computer*. https://www.bleepingcomputer.com/news/security/ticketmaster-sends-notifications-about-recent-massive-data-breach/
- Bond, M. (2024, July 9). Ticketmaster reports data breach, users' payment information could've been stolen. *CityNews Vancouver*. https://vancouver.citynews.ca/2024/07/08/ticketmaster-data-breach-payment-credit-card-information-stolen/
- Brogniart, T. (2022, September 22). A new danger: Cyber attacks are increasingly automated. *ChiefExecutive.net*. https://chiefexecutive.net/a-new-danger-cyber-attacks-are-increasingly-automated/
- CityNews. (2024, July 9). *Ticketmaster data breach impacts identity information of countless Canadians* [Video]. YouTube. https://www.youtube.com/watch?v=Q-9TPRxxRGQ
- Engadget is part of the Yahoo family of brands. (n.d.). https://www.engadget.com/ticketmaster-live-nation-senate-judiciary-hearing-195504179.html?_fsig=5bGTn4yH7AV8LBp7nG87WQ--%7EA
- Gallo, G. (2023, July 19). Live Nation Entertainment reports fourth quarter & full year 2019 results. *Live Nation Entertainment*. https://www.livenationentertainment.com/2020/02/live-nation-entertainment-reports-fourth-quarter-full-year-2019-results/
- Human. (2023, September 28). What is digital skimming and how does it work? *HUMAN*. https://www.humansecurity.com/learn/topics/what-is-digital-skimming
- Indicators of compromise (IOCs) | Fortinet. (n.d.). *Fortinet*. https://www.fortinet.com/resources/cyberglossary/indicators-of-compromise
- Jain, S. (2024, May 30). Alleged Live Nation data breach: Shiny Hunters takes credit. *The Cyber Express*. https://thecyberexpress.com/shiny-hunters-claim-live-nation-data-breach/
- King, A. (2024, July 4). Ticketmaster finally confirms massive data breach to customers—weeks after the hack occurred. *Digital Music News*. https://www.digitalmusicnews.com/2024/07/03/ticketmaster-data-breach-alert-to-customers/
- Lorsch, E. (2023, January 25). Why Live Nation and Ticketmaster dominate the live entertainment industry. *CNBC*. https://www.cnbc.com/2023/01/25/the-live-nation-and-ticketmaster-monopoly-of-live-entertainment.html
- Masas, R. (2023, December 20). Supply chain attack | Examples & security best practices. *Imperva*. https://www.imperva.com/learn/application-security/supply-chain-attack/
- Page, C. (2020, November 13). Ticketmaster hit with £1.25 million GDPR fine over 2018 data breach. *Forbes*. https://www.forbes.com/sites/carlypage/2020/11/13/ticketmaster-hit-with-125-million-gdpr-fine-over-2018-data-breach/

- Range, C. (2024, August 13). Analyzing the 2024 Ticketmaster breach. *Cloud Range*. https://www.cloudrangecyber.com/news/analyzing-the-2024-ticketmaster-breach
- Report URI: Case study - Ticketmaster. (n.d.). *Report URI*. https://report-uri.com/case_studies/ticketmaster
- Sansec. (n.d.). What is Magecart? https://sansec.io/what-is-magecart
- Schneid, R. (2024, June 2). Ticketmaster data breach may affect more than 500 million customers. *TIME*. https://time.com/6984811/ticketmaster-data-breach-customers-livenation-everything-to-know/
- Security, S. (2024, July 11). Understanding the Ticketmaster hack and how Skyhigh Security's Zero Trust platform can protect you. *Skyhigh Security*. https://www.skyhighsecurity.com/intelligence-digest/understanding-the-ticketmaster-hack-and-how-skyhigh-securitys-zero-trust-platform-can-protect-you.html
- Sky News. (2024, June 1). Ticketmaster hit by cyber attack - with hackers 'offering to sell customer data on dark web.' *Sky News*. https://news.sky.com/story/ticketmaster-hit-by-cyber-attack-with-hackers-offering-to-sell-customer-data-on-dark-web-13146457
- Snider, S. (2024, May 30). 'ShinyHunters' group claims massive Ticketmaster breach. *InformationWeek*. https://www.informationweek.com/cyber-resilience/-shinyhunters-group-claims-massive-ticketmaster-breach
- Social-Engineer, LLC. (2024, July 9). *TicketMaster Breach Update - 60 second Social Engineering tip* [Video]. YouTube. https://www.youtube.com/watch?v=6FtQBTHc87Y
- Turnkey Cybersecurity and Privacy Solutions, LLC. (2024, July 19). *Ticketmaster hacked AGAIN! Millions of Un-Reissuable tickets exposed* [Video]. YouTube. https://www.youtube.com/watch?v=OYHMx1Bzpqw
- Uliss, R. (2024, June 3). SEC filing confirms massive Ticketmaster data breach. *The National CIO Review*. https://nationalcioreview.com/articles-insights/extra-bytes/live-nation-confirms-massive-ticketmaster-breach-with-an-sec-filing/
- Ulubay, H. (2024, June 7). Understanding the Ticketmaster data breach: A technical perspective. *Timus Networks*. https://www.timusnetworks.com/blog/news/understanding-the-ticketmaster-data-breach-a-technical-perspective/
- What happened in the Ticketmaster data breach? | Twingate. (n.d.). https://www.twingate.com/blog/tips/ticketmaster-data-breach
- What is skimming: Examples and how does it work? (2023, September 21). *KnowledgeHut*. https://www.knowledgehut.com/blog/security/what-is-skimming-in-cyber-security
- Whittaker, Z. (2024a, June 6). Live Nation confirms Ticketmaster was hacked, says personal information stolen in data breach. *TechCrunch*. https://techcrunch.com/2024/05/31/live-nation-confirms-ticketmaster-was-hacked-says-personal-information-stolen-in-data-breach/
- Whittaker, Z. (2024b, June 10). What Snowflake isn't saying about its customer data breaches. *TechCrunch*. https://techcrunch.com/2024/06/07/snowflake-ticketmaster-lendingtree-customer-data-breach/
- Wikipedia contributors. (2024, August 15). *Ticketmaster*. Wikipedia. https://en.wikipedia.org/wiki/Ticketmaster

- Wiesel, Y. (2024, June 9). Snowflake breach: Examination of ‘whitewarlock’ claims. *Cyberint*. https://cyberint.com/blog/threat-intelligence/snowflake-breach-examination-of-whitewarlock-claims/
- What are Indicators of Compromise? (2024, August 20). *Forcepoint*. https://www.forcepoint.com/cyber-edu/indicators-