James Costello | A00326601

Object Oriented Programming 2

Assignment

OOP 2 Project Report

Introduction

For the OOP2 project, we reused the OOP1 code base. This application is based on a restaurant. Where the customer can view a range of menus from vegan, kids, main, and special menu.

Where the customer can place an order and pay. The restaurant also has employees such as waiters and managers along with contractors and delivery drivers.

For the OOP2 project we added the rewards card and offers class to the project.

List Of User Stories

Below is a list of user stories assigned as part of the assignment and completed.

Code	Descriptions	Status
[01_00P2]	Lambdas. for example: Consumer, Predicate, Supplier, Functio etc.	Done
[02_00P2]	Streams terminal operations such as. min(), max(), count(), findAny(), findFirst(), allMatch(), anyMatch(), noneMatch(), forEach() collect() - Collectors.toMap(), Collectors.groupingBy() and Collectors.partitioningBy()	Done
[03_00P2]	Streams intermediate operations e.g. filter(), distinct(), limit(), map() and sorted()	Done
[04_00P2]	Switch expressions and pattern matching.	Done
[05_00P2]	Sealed classes and interfaces.	Done
[06_00P2]	Date/Time API.	Done
[07_00P2]	Records.	Done

[A1_00P2]	Collections/generics use of Comparator.comparing() for sorting.	Pending
[A2_00P2]	Concurrency e.g. using ExecutorService to process of Callables.	Pending
[A3_00P2]	NIO2.	Pending

[A4_00P2]	Localisation.	Done

Evaluation

There were no major problems doing the assignment. There were a couple of challenges, these are as follows.

References

GIT Repo -> [https://github.com/jc6310/OOP1-Assignment]

Video ->

Research

Ticketmaster is the world's largest ticket marketplace. Its main service is where people can buy primary and secondary tickets to events such as concerts like Taylor Swift or to sporting events. [1] The company is based in Beverly Hills, California with over 6,600 employees whose services are worldwide.

Who Were The Hackers?

The group that hacked Ticketmaster is called 'ShinyHunters'. [2] This group is an international criminal hacker group that appeared in early 2020, which is when it is believed they were founded.

This group typically carries out sophisticated attacks on large-scale enterprises, with the intention to steal data and sell on the dark web for profit or sell back to the company it was stolen from.

Hacking Techniques They Used

ShinyHunters uses the cyber kill chain process, which is a process of how hackers plan their attacks, which are in phases to gain access to a system. This is a process of monitoring and probing for weaknesses. And then deliver and exploit the system.

[3] These phases are as follows.

- **[**[4] TA0043**] Reconnaissance** - The hacker chooses a target, investigates it, and looks for weaknesses in the target network.
- **Weaponization –** This is the process by which an intruder crafts a malware weapon for remote access, like a virus or worm, that is specific to one or more vulnerabilities.
- **[**[4] TA0001**] Delivery** - The intruder sends the weapon to the target (for example, through USB drives, websites, or email attachments).
- **Exploitation** - The computer code of a malware weapon initiates an operation on the target network in order to take advantage of a vulnerability.
- **[**[4] TA0002**] Installation** - A malware weapon creates an intruder-usable access point (such as a "backdoor").
- **[**[4] TA0011**] Command and Control** - An intruder can gain "hands on the keyboard" and continuous access to the target network thanks to malware.
- **[**[4] TA0040**] Actions** - The hacker takes action to accomplish their objectives, such as destroying data, exfiltrating data, or encrypting data for ransom.

ShinyHunters Major Data Breaches

[2] ShinyHunters has completed major data breaches, some of these are as follows.

- Santander had a data breach in May 2024 that is believed to be caused by a Snowflake vulnerability where all Santander staff and '30 million' customer's data was stolen.
- AT&T data breach in April 2024 stole data on over 110 million customers and AT&T paid $370,000 ransom to delete the data.
- Microsoft, it was alleged in May 2020 by ShinyHunters to have stolen over 500 GB of Microsoft source code from the company's private GitHub account.
- Mathway data breach in January 2020 stole stealing about 25 million users' data.
- Pixlr data breach in January 2021 stole stealing about 1.9 million users' data.

Type Of Data Ticketmaster Stores

Ticketmaster stores a wealth of data on their customers that is very valuable. These are as follows.

- Payment methods such as credit cards.
- Personal information such as name, address, email, phone number and more.
- Ticket purchased.
- Ticket history.
- Events that they want to go to.

How Did They Get Access to the Ticketmaster System?

Ticketmaster uses a third-party service called Snowflake. Snowflake is a SaaS data warehouse management tool where you can store, manipulate, and manage data on Snowflake.

Led by the hacker group ShinyHunters found a vulnerability with the Snowflake platform. This vulnerability led to the group getting access to customer account security information, in particular login information that in turn allowed the group access to data that Ticketmaster had stored on Snowflake.

[6] The initial access was gained by the hacker group obtaining credentials of a single former Snowflake employee that enabled access to demo accounts. These demos accounts had no authentication such as a Multi-Factor Authentication (MFA) setup as it was believed they contained only test data not sensitive data. And that they were isolated from Prod systems.

After further investigation of the former Snowflake employee, it was discovered that that employee's device was infected with info stealer malware. This type of malware logs all keystrokes and then sends the information to the attacker. This is how they got the login details to access the demo accounts.

The demo account shouldn't contain sensitive data so there was no authentication like Multi-Factor Authentication (MFA) setup or available. As they were only used for demonstration reasons.

[6] This then comes down to perception. In this case, the perception had 2 effects, these are as follows.

- To most people, a demo account compromise may seem identical to a full-scale production system breach but there is a lack of monitoring, therefore, it goes undetected.
- Even if it is a demo system, companies want their demo, dev, and stage systems to be as close to production as possible, this includes production-like data.

The data breach was only discovered when Ticketmaster data was available for sale online and offered back to Ticketmaster for $500,000.

The Steps ShinyHunters Took to Get Access?

If we go to the cyber kill chain process, the following process occurrs.

- They launched a reconnaissance targeting Snowflake and their employees.
- Next, they weaponize or plan who to target and how to plan the malware.
- Delivered the malware to an employee's device and installed the info stealer malware on the employee's device.
- Now exploit the vulnerability by gathering information from the malware.
- From the information gathered from malware now has access, now intruder-usable access point.
- Now the group had continuous access to the target's software.
- Finally, hackers can take action by extracting data. Which allows them to access major companies' data that is stored on Snowflake.

The Impact

The impact affected Snowflake to a lesser extent as people generally don't know about or deal with Snowflake except for tech companies and workers. It affected Ticketmaster in multiple ways. These are as follows.

- Customers.
- Staff.
- Reputation.

Customers

For Ticketmaster customers it led to concerns, these are as follows.

- This affects customer's confidence in Ticketmaster as this type of data breach creates a perception that they failed to protect their sensitive information, therefore creating a lack of trust in the company.
- This leads to customers having concerns that their personal data and payment details were exposed and available online that could be used for fraudulent activities. This data breach could result in financial losses for customers, that could lead to legal action or regulatory scrutiny against Ticketmaster.

Staff

The data breach was caused by a Snowflake employee being compromised and the hackers got their login credentials.

Even though the Snowflake employee has nothing to do with Ticketmaster, their staff would have to handle the pressure of the crisis and launch an investigation to answer the whys, how, and the impact.

Reputation

Ticketmaster has a reputation as a trusted market leader in selling tickets. So, a data breach where 580 million users' data containing emails, phone numbers, and payment details will naturally lead to bad press and public outcry. And a lack of trust in Ticketmaster.

The reputation of Ticketmaster will suffer in terms of decreased sales, it might affect market share and customer retention.

Immediate Response

Ticketmaster's response had to be in several ways. These are as follows.

- Immediate Containment, Investigate, and the Impact.
- Public Relations.
- Customer Support.

Immediate Containment, Investigate, and the Impact

Ticketmaster's first response was to contain the breach. This involves identifying the point of entry, and how they gained access, then isolating and possibly shutting down compromised systems, and stopping further unauthorized access, which in this case is Snowflake.

Ticketmaster needed to get the scope of the impact and the scale of the data stolen which affected around 580 million users. And if there are any regulatory compliances like GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), or other privacy laws that need to be informed.

Public Relations

Ticketmaster issued a public [7] statement acknowledging the breach, explaining the company's response, and reassuring Ticketmaster customers that measures are being taken to prevent future incidents.

Customer Support

Ticketmaster increased its customer support to help with customer's concerns about the breach data. These concerns may include concerns about payment information, gaining access to their accounts, or ticket information.

This also includes a customer outreach where they advised customers to be aware of suspicious activity, especially around their bank accounts for fraud or identity theft. [7] They also offered a free 12-month identity monitoring service with a leading provider.

Improvements

The improvements in the aftermath Ticketmaster data breach. These are as follows.

- Enabled MFA.
- Secure Third-Party Access.
- Security Audits.
- Regular Training.
- Encrypt Sensitive Data.

Enabled MFA

The data breach ultimately occurred because the hackers were able to put malware on a Snowflake employee's device coupled with companies wanting their demo, dev, and stage systems to be as close to production as possible, this includes production-like data.

There was no MFA (multi-factor authentication) enabled or available on the Snowflake demo environments as it was thought that there was no sensitive data on the demo environments.

Enabling MFA on the demo when available in the demo environment, will add a crucial layer of security that helps prevent unauthorized access attempts.

Secure Third-Party Access

Snowflake is a third-party service that ultimately is where the exploit occurred. There needed to be strict security protocols across all environments including demo accounts when using third-party services. Ticketmaster started to enforce strict security protocols on third-party services.

Security Audits

There needs to be independent and regular security audits from a trusted third party. These audits offer unbiased feedback on the company's defenses and recommend areas for improvement. These audits should include checking third-party services for passwords and usernames.

Regular training

They enforced more regular training provided to Ticketmaster employees, so they are still up to date on the latest threats. This training can include the type of data that is stored and if it is encrypted. As well as training to be aware of phishing emails and not click on any links.

Encrypt Sensitive Data

Ticketmaster claimed that the payment information was all encrypted, this will be extended to usernames, passwords, and emails. This will make the data stolen useless.

Conclusion

The goal of this case study was to describe the data breach with Ticketmaster and the effects it had on Ticketmaster regarding running their business. And the changes made to reduce the risk of it happening again.

To summarize, Ticketmaster was not 100% responsible as Snowflake had to take a lot of responsibility as well. There were a number of factors that led to the data breach. These are as follows.

- Snowflake believed that the demo system was not vulnerable as it contained no sensitive data. They underestimated that companies (their customers like Ticketmaster or Santander) want their demo, dev, and stage systems to be as close to production as possible including data. So never had basic security features like MFA in the demo environment.
- For a Snowflake employee to have had their device infected with info stealer malware, indicates that regular staff training is lacking as well as security audits not being completed, and security protocols are not fully implemented.
- Ticketmaster lacked ensuring that Snowflake were fully security compliant especially since they were storing Ticketmaster data.
- Ticketmaster needed to ensure that production data should only be in the production system. And only have test data in other environments.
- The data breach was only discovered when Ticketmaster data was online for sale. That was offered to Ticketmaster for $500,000. Indicating that there was an overall lack of monitoring.

Learning from this is that if Snowflake had the MFA available and enabled it on the demo environment the data breach would more than likely not have happened. It highlighted the lack of regular security training for employees as well as monitoring all environments for intrusions.

References

[1] About Ticketmaster [https://en.wikipedia.org/wiki/Ticketmaster]
[2] About ShinyHunters [https://en.wikipedia.org/wiki/ShinyHunters]
[3] Cyber Kill Chain [https://en.wikipedia.org/wiki/Cyber_kill_chain]
[4] Mitre Attack Cyber Kill Chain [https://attack.mitre.org/tactics/enterprise/]
[5] Snowflake Data Breach [https://www.1kosmos.com/authentication/understanding-the-snowflake-data-breach-and-its-implications/]
[6] Symmetry Report Snowflake Breach [https://www.symmetry-systems.com/blog/what-we-know-so-far-about-the-snowflake-breach/]
[7] Ticketmaster Statement [https://help.ticketmaster.com/hc/en-us/articles/26110487861137-Ticketmaster-Data-Security-Incident]