Analyzing ID Theft Service Exploitation of USInfoSearch Data and Strategies for Mitigation

Prabhjot Singh Sains, Ali Mahmoud, Rahul Patel, Dax Patel, Revanth Madala

George Brown College

Author Note

Prabhjot Singh Sains, Web Development, Humber College. Revanth Madala, MERN Stack Developer, LTIMindtree, Ali Mahmoud. Rahul Patel, Project Management, Mohawk College. Dax Patel, ISBM, Northern College.

Prabhjot Singh Sains, Ali Mahmoud, Rahul Patel, Dax Patel, and, Revanth Madala are now all students of George Brown College studying Cybersecurity.

This research is done for the Legality and Compliance in Security Course of the Cybersecurity Program at George Brown for Professor John Wang.

Correspondence concerning this article should be addressed to Group 5, Cybersecurity Program, George Brown College, Toronto, ON M5T 2T9.

Abstract

This report explores the Chief investigation security officer's (CISO) view on preventing additional leaks of data and safeguarding the organization and client's data due to the data leak using compromised vetted client accounts with the help of account credentials that were stolen by malicious software tied to a bot called USiSLookups made by a cybercriminal who uses the nicknames JackieChan which is used to target and access the API USInfoSearch uses, which is used by customers to integrate the lookup service with other web-based services, databases, or applications. This report explores the article published by Brian Kerbs, Investigative reporter at KerbsonSecurity.com who was able to identify the compromise. This report uses the McCumber Cube to provide recommendations to USInfoSearch, and its employees to prevent further damage as well as mitigate them. The analysis investigates how a specific exploit impacts the principles of Confidentiality, Integrity, and Availability, along with recommendations on rectifying and preventing such occurrences in the future. It explores the influence of the exploit on different aspects of information states which includes transmission, storage, and processing, while also considering the three main safeguards for information which include policy and practices, human factors, and technology. Although the primary security concern lies with confidentiality, there is a potential for exploitation of integrity and availability as well. Therefore, the report offers suggestions for enhancing these aspects.

Analyzing ID Theft Service Exploitation of USInfoSearch Data and Strategies for Mitigation

A cybercriminal known as JackieChan has been pulling data from hacked accounts at USinfoSearch, a consumer data broker since February 2023. JackieChan operates a service called USiSLookups, which offers access to detailed consumer background reports using an automated bot on Telegram, enabling anyone to obtain sensitive personal information for a price. This has resulted in unauthorized access to SSNs, background reports, and other personal information of American citizens. (KrebsonSecurity, 2023)

JackieChan managed to successfully compromise all aspects of confidentiality. The customers' data is getting compromised and this will cause identity theft and use for fraudulent purposes.

On November 21, 2023, general manager of USinfoSearch parent Martin Data LLC acknowledged that the breach occurred from an account belonging to a USinfoSearch client (Hostettler, Nov 21, 2023).

The cybercriminal gained access to USinfoSearch account credentials that were stolen by malicious software attacked with the botnet, made by JackieChan., These are used to get into the API used by USinfoSearch customers to integrate the lookup services, which were then used to run the ID fraud service on Telegram. This highlights the vulnerability in the authentication and credential management processes.

While there is no indication that this breach impacts the availability of data, it poses a significant threat by enabling attackers to manipulate login credentials. This allows them to alter passwords for accounts and can even change the API system, effectively denying access to the customers.

The integrity of data is not impacted directly. But it exposes data to potential misuse like making fake EDRs. Additionally, the stolen credentials could be sold to various groups, who could then use the acquired login details to manipulate data integrity per their needs.

Literature Review

The breach in the system of USinfoSearch was learned by KrebsOnSecurity's Investigative reporter Brian Kerbs on November 28, 2023, and the article related to this will be found on the website KrebsOnSecurity.com. Krebs has mentioned all the aspects of this breach in this article. (Krebs, 2023)

The NSTISSI No. 4011 document introduces the McCumber Cube also known as the Committee of National Security Systems (CNSS) Security Model, a framework for Information Security (InfoSec) developed by John McCumber. This model illustrates three key dimensions: information characteristics, information location, and security control categories. By considering the relationships among these dimensions, a 3 x 3 x 3 cube with 27 cells is formed. Each cell signifies an intersection point to develop or evaluate it's essential to ensure that all 27 cells are addressed by the relevant stakeholders. (Whitman et al.'s, 2018, Page. 5)

McCumber Cube Analysis

The analysis investigates how the exploit impacts the principles of confidentiality, integrity, and availability, along with recommendations on rectifying and preventing such occurrences in the future. It explores the influence of the exploit on different aspects of information states which includes transmission, storage, and processing, while also considering the three main safeguards for information which include policy and practices, human factors, and technology. When someone requests data from API, the request goes through various stages, including transmission from the client to the server, processing on the server side, and then transmission of the response back to the client. As such, we will use the McCumber Cube to provide recommendations to assure confidentiality, integrity, and availability, and contain the breach.

Confidentiality

Confidentiality refers to restricting access to data to only authorized individuals. Maintaining confidentiality implies that the data hasn't been accessed or compromised by unauthorized parties, and sensitive information isn't disclosed to those who do not need it or should not have access to it.

JackieChan was able to get the customer's data by gaining access to USinfoSearch account credentials that were stolen by malicious software attached with the help of a botnet. These are used to get into the API used by USinfoSearch customers to integrate the lookup services. This service features a small number of sample background reports. The data in those reports includes the date of birth, address, previous addresses, previous phone numbers and employers, known relatives and associates, and driver’s license information of the American citizens. The compromised data also includes President Joe Biden and podcaster Joe Rogan.

Transmission. According to the McCumber Cube model, it's essential to maintain data confidentiality during the transmission phase of information to other devices. The USinfoSearch uses an API (Application Programming Interface) to provide data to customers. APIs facilitate communication between two software components by utilizing a defined set of protocols and specifications. The data of USinfoSearch is transmitted over an API, to which the hacker managed to get hands-on by using the stolen account credentials of a customer. To protect the confidentiality of the data in the transmission phase, we will define some policies and practices, human factors, and technological recommendations.

Policies and practices. Some of the policies and practices that can be followed to prevent this type of thing from happening again is to adhere to some best practices. APIs should be designed with security, beginning with a thorough risk assessment, considering threat modeling, data classification, attack surface reduction, and robust authentication mechanisms. The security team should regularly audit and update, which can be done by conducting periodic security audits, vulnerability assessments, and patch management to stay ahead of emerging risks. The DevOps and security team of API should align with security standards such as OWASP Top 10, industry regulations like HIPAA or FISMA, and security frameworks like NIST Cybersecurity Framework to ensure compliance and robust security posture.

Human factors. Training is essential for ensuring API security, as it empowers individuals to understand and implement best practices effectively. Provide comprehensive security awareness training to all users involved in API development, deployment, and maintenance. This training should cover the fundamentals of API security, common vulnerabilities, and best practices for mitigating risks. Offer specialized training courses that focus on the unique security challenges and requirements associated with various roles. Use real-world case studies to illustrate the importance of API security and the potential consequences of security breaches. API security is an evolving field, so encourage continuous learning and professional development among the team members. Provide access to training resources, industry conferences, and certification programs to help individuals stay in the loop with the latest security trends and best practices. Moreover, regularly assessing the effectiveness of training programs through performance evaluations and feedback mechanisms.

Technology. Deploy endpoint security solutions, such as endpoint protection platforms (EPP) and endpoint detection and response (EDR) systems, to detect and prevent the installation of malicious software on endpoints, endpoints are user systems. These solutions can help identify and block malware that attempts to steal account credentials and mitigate the risk of unauthorized access through compromised endpoints. Focus on setting up authentication mechanisms for API like OAuth, API keys, or tokens to control access to authorized users only. Using HTTPS to encrypt data while it's being transmitted, preventing unauthorized access, and encrypting sensitive data in transit using secure algorithms and proper key management. User input must be validated and sanitized to prevent injection attacks and block malicious data. Implementing rate limiting to restrict the number of requests a user can make within a specific time frame, preventing misuse or DoS attacks. Enforcing data access controls to avoid revealing sensitive data.

Storage

Storage refers to the state of the information in which data is in a still state and can be accessed at any time, storage concerning confidentiality refers to the point where data’s confidentiality is not compromised when it is in the rest state means when in storage. In the case of USiSLookups its developer JackieChan got the hands-on customer account credentials that were stolen by malicious software attached with the help of a botnet. This is the reason that the data also got compromised in the storage phase, as JackieChan used the account to compromise the API and the customer's data in the database. Every website or tool on the internet used by the users utilizes data from some storage like databases. In this case, the main issue that comes to light is the customer's accounts are not secured. As no official data is available to find out how this hacking software works to get the credentials, some common beliefs can be taken into consideration such as phishing attacks and fake “password reset” emails, the most common methods hackers use to steal information by sending emails that include links to trick people into visiting an original looking fake website which downloads malware or malicious software on the system. Another one can be a brute-force attack that uses hit and trial to access crack password combinations because people use weak passwords.

Policy and Practices. Make a policy to implement strong password requirements and a mandatory policy should be implemented to make sure that everyone is using Multi-Factor Authentication (MFA). To prevent brute-force attacks an account lockout policy is to be used to lock user accounts after a certain number of failed login attempts. User roles and permissions should be defined, granting users only the necessary access as per their roles this is referred to as the access control policy. Session management policy should also be used which is a mechanism that automatically logout users from their accounts after a period of inactivity. Implement monitoring tools and processes to track user account activity and detect any unauthorized behavior in other words Account Monitoring Policy. Moreover, establish a secure account recovery process that requires users to verify their identity through multiple factors before regaining access to their accounts. This helps prevent unauthorized access through social engineering attacks. At last, Develop and maintain an incident response plan that outlines procedures for responding to security incidents involving user accounts. Policy should be made to check the customer is legitimate before creating their account by using some government-issued IDs.

Human factor. Customers and employees' awareness and training to educate them about common security threats such as phishing attacks, social engineering, and password hygiene should be implemented. Users should create strong, unique passwords and must not use any old and same passwords. Users should keep in mind not to share their passwords or any type of information like security questions that can be used for login. Moreover, Customers and team members should not write down or store passwords anywhere just store them in their minds. Users should not leave their system without locking it or storing it in a secure place when not in use. Users must not install any software without checking with the security department.

Technology. To safeguard the data's confidentiality from getting compromised while in storage securing the user accounts is the main focus. When storing user passwords, instead of storing passwords in plain text, they should be hashed and salted to slow down the hashing process to repel automated brute-force attacks, using algorithms such as SHA-256 and salting which refers to adding random data to a user's password before hashing it, which enhances the complexity of the resulting hash. This makes it significantly more challenging to crack passwords. Use Identity and Access Management (IAM) systems to manage user identities, access permissions, and authentication processes, which can also be integrated with MFA. Utilize encryption technologies to encrypt sensitive data stored within the USinfoSearch database. Encryption ensures that even if unauthorized parties gain access to the database, the data remains unreadable without the decryption key. Implementing strong encryption algorithms for data-at-rest encryption helps maintain the confidentiality of stored data.

Processing

Processing is the state in which the data is being operated by performing some actions on it to get desired results, processing concerning confidentiality refers to the action of performing operations on data without compromising its confidentiality. As mentioned in the storage section every website or tool on the internet relies on manipulating, transforming, or utilizing data to achieve specific objectives. It is not mentioned whether the data got compromised on the server side or not because processing normally occurs on the server side. Some of the methods that can be used to hack the data while in the processing state are Injection Attacks in which attackers can inject malicious code into input fields being processed by applications and SQL injection is a code injection technique that might destroy a database. When these scripts are executed in the browsers, they can steal data, modify page content, or perform other malicious actions. APIs used for processing data may have security vulnerabilities that can be exploited by attackers. This includes issues such as inadequate authentication, authorization, or input validation.

Policy and Practices. To keep data safe while it's being worked on, organizations can create policies and practices. These rules include role-based and use-based access to the data and how to access the data. For example, only giving access to people who need it and making sure they prove who they are with things like passwords or fingerprint scans. Also encrypt the data, which means turning it into a secret code so only authorized people with the right key or token can understand it. It's important to teach employees about these rules and what to do if something goes wrong. Establish a data processing policy outlining procedures for handling and processing sensitive information within the USinfoSearch system. This policy should define permissible data processing activities, access controls, and data handling practices to ensure the confidentiality of data in processing.

Human factors. Humans have a big part in keeping data safe while it's being worked on. This means train and aware employees how to spot bad stuff like fake emails or tricky websites, and telling them what to do if they see something wrong and they should tell them about it right away to the security team. They should also follow rules about passwords and not leave important stuff easily accessible. It’s also important to keep computers and software up to date to stop unwanted personnel from getting in. Overall, making sure employees know what to do and how to keep things safe can help keep data secure while it's being used. Implement role-based access control mechanisms to restrict access to sensitive data during the processing phase. Ensure that employees only have access to the data and resources necessary for performing their job roles, minimizing the risk of unauthorized access or data exposure.

Technology. There are many tools and ways to keep data safe while it's being used. For instance, encryption changes data into a secret code so only the right people can understand it. Access control systems make sure only the right people can access and use the data. Data loss prevention systems stop people from sending sensitive data where it shouldn't go. Implement robust security controls at the application level to prevent unauthorized access and manipulation of data during processing. This includes measures such as input validation, output encoding, and access control mechanisms within the application logic to ensure that only authorized users can access and modify data. Deploy security information and event management (SIEM) systems to monitor and analyze activity logs from applications and infrastructure components involved in data processing. SIEM systems can correlate events, detect anomalies, and alert on suspicious activities, helping organizations identify and respond to potential security incidents in real time.

Integrity

Integrity means information should not be changed, or corrupted**.** There is no direct compromise to the integrity of the data stored within the USInfoSearch database, As JackieChan's main motive was to sell the data online not to change it, there are vulnerabilities in the system that could indirectly lead to data integrity issues. Unauthorized access to login credentials is dangerous since it can lead to data integrity modification, including forging Electronic Data Records (EDRs). Furthermore, the risk to data integrity is further highlighted by the potential for credentials to be stolen and data to be sold to different groups.

Storage. No specific mention of a data integrity compromise during the storage phase is made in the article. On the other hand, it talks about the hazards associated with confidentiality, specifically concerning illegal access to USInfoSearch user credentials. There is no proof that the data kept in the USInfoSearch database has been directly changed, even if compromised credentials may allow for unauthorized access to data that has been stored. Organizations could use access controls, encryption, and routine audits to spot and stop illegal changes to stored data to guarantee integrity during storage.

Processing. The article does not mention any direct compromise of data integrity that may have occurred during processing. Without specific details on data manipulation during processing, the integrity of the data remains intact. To ensure integrity, organizations could implement input validation, secure coding practices, and regular security assessments to detect and prevent unauthorized changes to data during processing operations.

Transmission. Similar to storage and processing, the article does not directly mention any compromise to data integrity during transmission. However, it discusses potential risks related to unauthorized access to API services and transmission of data over APIs, these primarily relate to confidentiality. There's no indication that the actual content and accuracy of the transmitted data are tampered with. To ensure integrity during transmission, organizations could implement secure communication protocols, data encryption, and message authentication mechanisms to prevent unauthorized modifications to transmitted data.

Availability

Availability means information should be accessed whenever it is needed by the organization or the customers without any problems or delays. There is no information about the direct compromise of data availability. The unauthorized access to USInfoSearch account credentials poses direct risks related to confidentiality; however, some risks may happen in the future it could indirectly affect availability if attackers manipulate login credentials or change the API system, leading to risks in data availability for legitimate users. To mitigate these risks, organizations can implement strategies such as investing in robust network infrastructure, utilizing redundancy and failover mechanisms, deploying DDoS protection solutions, and regularly testing incident response plans.

Storage There's no indication that the availability of stored data is impacted. While unauthorized access to account credentials is highlighted, this primarily poses risks related to confidentiality. To ensure availability during storage, organizations could implement failover mechanisms in their storage infrastructure or backup servers, ensuring continuous access to data even in the event of hardware failures or network disruptions.

Processing. Similarly, there's no indication that the availability of data is impacted. Although potential vulnerabilities in processing are discussed, such as injection attacks or API security weaknesses, these primarily relate to confidentiality. To ensure availability during processing, organizations could implement scalable processing infrastructure and monitor for performance issues using SEIM tools to prevent service disruptions.

Transmission. The article does not directly mention any compromise to data availability during transmission. While potential risks related to unauthorized access to API services and transmission of data over APIs are discussed, these primarily relate to confidentiality. To ensure availability during transmission, organizations could implement redundant network connections and utilize load-balancing techniques to distribute traffic evenly, preventing network congestion and ensuring continuous access to transmitted data.

Conclusions and Future Study

This analysis highlights how important it is for companies like USInfoSearch to protect people's personal information from hackers like JackieChan. The need for better security measures to stop this from happening again is a necessary and important thing to do.

To make things safer, looking into ways to verify who's accessing data, implementing stronger ways to keep data secret, and better rules and policies about who can see what. It's also important to keep studying how people interact with security measures and what helps them understand the risks. By working on these things, we can make sure that people's information stays safe, and companies can keep their systems secure from cyber-attacks.

References

The three-pillar approach to cyber security: Data and information protection: https://www.dnv.com/article/the-three-pillar-approach-to-cyber-security-data-and-information-protection-165683/

What is an API: https://aws.amazon.com/what-is/api/

8 Best Practices for Securing APIs: https://www.ninjaone.com/blog/8-best-practices-for-securing-apis/

Securing APIs: 10 Best Practices for Keeping Your Data and Infrastructure Safe: https://www.f5.com/labs/learning-center/securing-apis-10-best-practices-for-keeping-your-data-and-infrastructure-safe

What Is API Security: https://www.paloaltonetworks.com/cyberpedia/what-is-api-security

Information Security: The John McCumber Model: https://www.123helpme.com/essay/Information-Security-The-John-McCumber-Model-408048

How Do Hackers Get Passwords? (And How to Stop Them): https://www.aura.com/learn/how-do-hackers-get-passwords

Securing Account Credentials to Protect Your Organization: https://blog.netwrix.com/2023/04/21/secure-credentials-and-protection/