Selected Topic: Alibaba Cloud Data Breach July 2022
Group Members: Asya Dente, Kelvin Lin, Lily Jihyun Son, Alim Kura

Introduction

The Alibaba data breach in July 2022, a significant event in cybersecurity history, involved the exposure of personal data such as names, addresses, and ID numbers of over one billion Chinese citizens. The data was stolen from the Shanghai Police database which was improperly secured on Alibaba Cloud for over a year, as reported by TechHQ[TechHQ]. This naturally resulted in widespread international mainstream media attention due to its unprecedented scale and the circumstances affecting large companies and over 70% of the Chinese population. The breach's revelation was ironic in a country where regulations of data privacy and the tech industry are increasing [Reuters], and domestic data breaches are rarely disclosed, making this story particularly newsworthy. This incident underscores the significance of digital data security and the potential consequences of vulnerabilities in protecting sensitive information.

Technical Issues

IP addresses are the identifier that allows information to be sent between devices on a network. There are thousands of ports to any given IP address, and if the hacker knows which port your content is stored on, for example, a police database, then they would be able to access it. This was the underlying technical issue.

Shanghai's police database was left unsecured online for almost 14 months. The database was hosted on Alibaba's cloud servers. Alibaba offers cloud services on a pay as you go basis, very similar to the cloud services offered by AWS. To be more specific, there existed a 'backdoor' link (which is an unprotected IP address that offers unrestricted access to anyone who finds it) and using this, the hacker was able to gain access to Shanghai's police database.

The New York Times (which cited the cybersecurity consultancy firm, Security Discovery) said that Shanghai police data had been stored on a secure, closed network until a gateway was created, essentially punching a hole in the firewall. Such gateways are common practice for developers to easily access the database. But such getaways should be protected by passwords, which were lacking in the case of the Shanghai database.

According to Wall Street Journal, "The Shanghai police records—containing the names, government ID numbers, phone numbers and incident reports of nearly 1 billion Chinese citizens—were stored securely, according to the cybersecurity experts. But a dashboard for managing and accessing the data was set up on a public web address and left open without a password, which allowed anyone with relatively basic technical knowledge to waltz in and copy or steal the trove of information, they said."

According to CNN, the fault of the data breach doesn't lie with Alibaba, rather, it was the people who set it up. The Shanghai police were using an old version of Alibaba's cloud servers, which meant that there were no security features, including password, without installing a separate add on, which they did not.

What could have been done was to not have the gateway in the first place, or if you do, use security measures to protect it.

Prevention

We will address the issues identified in the previous section *Technical Issues,* emphasizing on countermeasures. First, there should be enhanced security for IP addresses and ports, which could be done by deploying comprehensive network security measures, including advanced firewalls and intrusion detection systems like honeypots. Second, the engineers should have reinforced password protection for backdoor links, ensuring all access points are safeguarded with strong and regularly updated passwords. Another critical step to take is to ensure that gateways facilitating access to databases are meticulously managed and secured with proper authentication and monitoring systems. Furthermore, regularly updating server software is crucial to protect the system with the latest security features and significantly reduce vulnerabilities. Similarly, higher-level specialists should be conducting frequent audits of cloud services and databases to identify potential vulnerabilities. Lastly, the staff should be trained in CyberSec best practices to ensure compliance with established security protocols. These measures would be successful in preventing such issues in the future.

Discussion of Incentives

Motivation

According to Reuters, [the anonymous internet user, identified as "ChinaDan", posted on the hacker forum Breach Forums offering to sell more than 23 terabytes (TB) of data for 10 bitcoin, which was about $200,000]. Nothing was specifically mentioned in the news or other media, but based on the news information, the motivation of the adversary to attack Alibaba Data was for financial gain. Reuters wasn't able to authenticate the validity of the Forum post and also wasn't able to reach the self-proclaimed hacker.

Harm Caused

Because of this data breach, there might be lots of harm caused to Alibaba. A few things are financial loss, damage to reputation, and operational disruption. First, regarding the financial loss, their shares fell by 5.98% only a few days after the post of the attacker [Reuters]. Moreover, the ministry that is in charge of the technology suspended a cybersecurity partnership with Alibaba's cloud computing in December of that year after [Beijing alleged the company "failed to report a global software vulnerability to it in a timely manner"]. The loss of the partnership means that they lost a contract, which leads to the loss of financial gain. Not only the financial loss, there was reputation damage as well. Because of this data breach, which is now known as the biggest data breach in history, Alibaba may have lost its reputation as a cloud computing company, even though it wasn't explicitly mentioned in any of the news or other forms of media. As said above, its loss of partnership with the ministry in charge of technology might have also affected its reputation. Lastly, there is operational disruption. Because of this attack, it might take an enormous amount of time and money to recover the system and make their data cloud system more secure. Despite these harms, however, Jack Ma - the founder of Alibaba - claimed that [Big Data "would help the public security agencies track down thieves and predict terrorist attacks" has helped Alibaba become "the biggest public cloud-service provider in China"].

Beyond Alibaba, there were few other parties affected or harmed by the attack. The party that was influenced the most was the Chinese citizens. Since their personal information - their names, government

ID numbers, phone numbers, and incident reports of nearly 1 billion Chinese citizens - were leaked to the attacker and the attacker was willing to sell the information, it might have led to potential identity theft, fraud, or other cybercrimes. Moreover, since the database was left unsecured and publicly accessible for more than a year - according to CNN news - the data might have leaked to other parties, which might lead to other potential cyber crimes by other attackers. Other than Alibaba and customers, the partners, who were working with Alibaba Cloud might have got affected as well. Since the Shanghai National Police (SHGA) were using the Alibaba cloud database to store their data - the data that got leaked - the SHGA might face reputational and financial risks due to their association with the breached entity. After this data breach, the ministry in charge of technology ended the partnership with Alibaba and moved to another company, which might have caused the ministry additional tasks.

Misalignment of Incentives

Similar to the Equifax breach example, there was a misalignment of incentives that led to the attack. Alibaba's customer, the Shanghai National Police, was using the Alibaba Cloud platform to store the data, which had all of the personal information, and the users - Chinese citizens - were not the direct customers of Alibaba. This misalignment could result in insufficient incentives to prioritize user data security adequately.

Ethical Issues Raised by the Attack

Ethical Issues Raised by the Incident

This incident involves the unauthorized access and possible acquisition of personal information from over a billion Chinese residents by an anonymous hacker (ChinaDan). It has brought to light a multitude of ethical and legal concerns. This breach could very well stand as one of the largest data breaches in history and raises different questions ranging from individuals' privacy, government transparency and corporate responsibility to the adequacy of the existing legal frameworks.

Some of the ethical issues raised by this breach are privacy violations, which represent a severe violation as personal information of Chinese residents including their names, addresses, national ID numbers, and crime details, was able to be accessed without the owner's consent. Many now could potentially face issues such as identity theft, and fraud. Additionally, another important ethical issue discovered is the Government transparency and accountability as the Shanghai government and police department were trying to hide the breach by blocking hashtags and posts raising ethical concerns. However, it is in the citizen's rights to be informed of such situations, especially one where their personal information was compromised.

Finally, since Alibaba's cloud platform is implicated, questions could arise about their corporate responsibility. We found that there were warnings regarding the security of Alibaba's cloud not being very secure in 2021 already, this meaning about a year before the breach was known to the public. Chinese regulators had suspended an information-sharing partnership with Alibaba Cloud Computing as they had failed to report and address a cybersecurity vulnerability regarding the logging framework. The MIIT (ministry of industry and information technology) issued a notice that Alibaba's failure to report the vulnerabilities led to the suspension of the cooperative partnership in addressing cybersecurity threats. The government was already then urging state-owned companies to shift their data from private operators

such as Alibaba and Tencent to a state-backed cloud system. Major tech companies are entrusted with safeguarding user data, so a failure to do so does raise a few ethical concerns. This incident highlights the ethical responsibilities of corporations, especially those handling big amounts of sensitive information.

Legal Issues Raised by the Incident

In terms of legal issues, we could think about the data protection laws, where this breach highlights the need for rather robust data protection laws in China. If the existing laws were sufficient and enforced, such a massive data breach might've been prevented. As we highlighted earlier, there was an effort given into following a few laws, however, it was clearly not well handled as in the end, it didn't help the 1 billion residents that had their information stored there. Something to underline is that legal frameworks are essential; thus, strengthening them could help prevent future potential incidents. As mentioned above, the involvement of Alibaba's cloud platform brings potential regulatory issues related to the security practices of cloud service providers.

Misalignments of Incentives

There were a few incentives misalignments as mentioned previously, and thus a couple legal solutions we found were maybe having stricter penalties and bigger fines to better align incentives. It would serve to make these companies aware of the severity of the subject. Hopefully they will then start investing in greater cybersecurity measures. Additionally, mandatory reporting of data breaches could be made into a bigger priority as it would allow authorities to possibly take action earlier and potentially avoid having bigger consequences and thus minimize the impact. We would also need to make sure the government practices are being well handled as well as regularly reported as it is crucial to ensure a fully transparent, honest and trustworthy system.

Other Countries' Laws and Regulations

Lastly, just as a more general good practice, learning from the data protection practices of other countries could help improve domestic regulations. Each country has their own laws and regulations, so communication between countries might just help look at their defenses from a different point of view. For instance, the EU General Data Protection Regulation (GDPR) has imposed fines that could go up to 20 million euros, and knowing this, companies might have more incentive to have certain levels of security put in place. Moreover, it is also that same legislation that specifies that in the case of a personal data breach, it should be reported to the Data Protection Authority (DPA) within 72 hours. So, having these strict deadlines and heavy fines might motivate companies to ensure having a safe working environment. On the other hand, China has somewhat of a weak regulatory system where the laws do exist but are under the name of the Personal Information Protection Law (PIPL). The PIPL only came out towards the end of 2021 and was known to be China's first comprehensive data protection law.

To conclude, the Shanghai police database breach raises many ethical and legal issues such as: privacy violations, government transparency and corporate responsibility. Addressing these concerns requires a complicated approach able to enhance the legal frameworks and place stricter regulations. We just mentioned the GDPR has quite interesting regulations and maybe China could refer itself to these laws a little bit more, or at least improve on its own laws, namely the PIPL. It's important to note that as technology continues to advance, ensuring the security and privacy of individuals' data has to be a priority for governments, corporations, and regulatory bodies alike.