A Recent Cybersecurity Attack: Tencent Holdings

Mary Lelina-Ford

CS 462 Term Project

Fall 2024

**Recent Cyber Attack**

There has been a recent report of a significant increase in cyber-attacks. According to Google, in 2024 alone, during the third quarter of the year, there was a seventy-five percent increase from the same quarter last year. In August 2024, one of the most recent and major data breaches occurred at Tencent Holdings Limited. According to their website, Tencent Holdings Limited is a “world-leading internet and technology company that develops innovative products and services to improve the quality of life of people around the world.” Tencent Holdings' headquarters is based in Shenzhen, China. They have offices around the world and in every continent. The one closest to Old Dominion University is in Washington, DC.

Tencent Holdings is a large company that includes six groups: Corporate Development Group, Cloud and Smart Industries Groups, Interactive Entertainment Group, Platform and Content Group, Technology Engineering Group, and Weixin Group. If you play video games, you may have heard of Honor of Kings and/or PUBG Mobile. These two highly grossing games bring Tencent Holdings most of their gaming revenue. The company has been in business for twenty-six years and has a revenue of at least $86 billion in United States dollars. Tencent Holdings provides products and services that many of us have probably used. Given all this information, you can only imagine the significant damage the data breach had to this company and the people who were also affected, according to the Cyber News website. The hacker who was responsible for the data breach goes by the name Fenice.

Fenice is the same threat actor who was responsible for the data leak of three billion users from a platform called National Public Data, which also took place in 2024. There is not much more information on this hacker online, except for a claim of its connection to Mother of All Breaches (MOAB), according to the online source CyberNews.com. MOAB is another massive data breach that took place this year.

**Technologies Used**

The technology used by hacker Fenice was not fully disclosed in any articles I collected regarding the attack on Tencent Holdings. According to the Tac Security website, such breaches normally involve tactics like exploiting vulnerabilities in the company’s security infrastructure, phishing to obtain user credentials, SQL injections or other methods to access databases, and credential stuffing using stolen credentials from other breaches. It is safe to say the hacker is a professional type. I also believe he or she is in possession of a type of technology that has been solely used to hack other organizations. It is some type of technology that cannot be traced and has very limited user access. Whatever technology the hacker used to access Tencent Holdings’ network was unique to many hackers.

**How Vulnerability, Breach or Attack Worked**

According to the Up Guard website, the security that was attacked were website, email, and network security. From what it sounds like, Tencent Holdings’ security across the board, from email to network security, was easily exploited because of many possible reasons. One reason could be the system was not up to date. Tencent Holdings was probably using a security system that had not been updated for a significant amount of time. The security version could also be a factor. You would think that such a big company as Tencent Holdings would have the most sophisticated version of security. I will also add with the website security, Tencent Holdings’ anti-virus was weak and could easily be manipulated. I can say that they used an anti-virus that cannot handle the traffic of such a large corporation. The email security was poor because the users were not well trained in how to avoid scams or possible attacks on the system. It is important to train employees on how to handle or avoid any suspicious materials or activities they find on their computers when performing their daily tasks.

It is surprising to read that such a big company like Tencent Holdings would be attacked by one of the easiest means: email or a website. It’s not an insider job since it’s been reported that a hacker was responsible for the attack. Unfortunately, Tencent Holdings’ network system did not have additional layers of security.

Another item that came up with the security report of Tencent Holdings was phishing and malware. This information tells me that Tencent Holdings lacks the ability to keep its system secure. A company that provides technological services and products should use a state-of-the-art security system. Phishing and malware are two of the most common ways of cyber-attacking. Clearly, the Tencent Holdings security system was not prepared to avoid any potential cyber-attack. According to Google, seventy-five percent of cyber-attacks in 2024 alone were done through phishing.

**Devices, Protocols, or Applications That Were Attacked**

If you are an internet and technology user, chances are you have used products or services that are associated with Tencent Holdings. Tencent Holdings is a huge contributor of products and services that are offered worldwide. The well-known products and services of Tencent Holdings are applications like Instant Messaging, Social Networking, Mobile Games, WeChat, Tencent Holdings Cloud, Tencent Holdings Marketing Solutions, and Utility Software. WeChat has over a billion users. According to Wikipedia, “WeChat has been described as China’s ‘app for everything’ and a super-app because of its wide range of functions.” Tencent Cloud provides a one-stop video solution covering video-on-demand live streaming, real-time video calls, short videos, and more, according to their website, TencentCloud.com. Fortunately, none of these products and services were compromised during the attack. As mentioned earlier, there was a significant number of users that were compromised. There is a possibility that they are the users of these products and services.

**How This Attack Affects Today’s Society**

The attack on Tencent Holdings affects societies everywhere, not just China, where its headquarters are. It is a good example of how an attack will happen if the system is vulnerable, no matter how big the company is. People get scammed for a minimal amount. Normally, big organizations fall victim to such internet crime. This cybercrime can teach society, including big organizations, many lessons. These lessons are how today’s society is affected.

One lesson that can be learned is how to be more vigilant when using electronic mail or the internet. Not everyone is educated on how to spot internet vulnerabilities. Organizations should put more emphasis on training their employees how to use the internet with caution. They should stress not to rely on anti-virus or any security measures. Society (or employees) should learn that security is everyone’s responsibility, not just the organization's.

The attack on Tencent Holdings exposed personal information of their users. Examples of sensitive information that were exposed are phone numbers, email addresses, and QQ IDs. This particular part of the attack could cause personal damage to the user, such as identity theft. The people affected by this attack should learn that some personal information is better left private. They should limit what information should be shared with the services they use.

Another lesson to be learned is potential lawsuits. Tencent Holdings is a huge organization that has customers all over the world. It can face legal challenges against its customers, which organizations should learn from. Legal battles could take years and are time-consuming. Disclosure of private information could damage consumers for life.

One other lesson is the financial impact on the organization. This attack has cost Tencent Holdings millions of dollars. Organizations should learn that this could cause some financial strains during the present and possibly the future of the organizations. The damage may continue for years to come. Re-establishing a new system of security could also cost the company a significant financial burden. The new security system will also require retraining of employees. A new agenda will have to be created for the users.

The last thing I believe every organization should learn from this attack is their reputation. It takes years to build an organization and many more to earn the trust of its customers. Sometimes, organizations end up in bankruptcy because their reputation is significantly damaged. It would take some time for the company to rebuild the trust of its customers, which affects society’s trust.

**Conclusion**

Adding extra layers of security and spending more financially to prevent any future damage is more often worth than not taking any precautions. It is for the long term. From the Department of Homeland Security, “See something say something.” It is everyone’s job to make sure that we secure anything we use whether it’s our employment or personal computer. It affects us personally even if the attack is towards an organization we are associated with. The attack on Tencent Holdings could have been prevented in many ways. I say that both Tencent Holdings and their employees are responsible for letting the attack happen.

**References:**

1. [**https://www.Tencent Holdings.com/en-us**](https://www.tencent.com/en-us)
2. [**https://tacsecurity.com/hackers-leak-1-4-billion-Tencent Holdings-user-accounts-how-tac-securitys-esof-solutions-can-prevent-future-breaches/**](https://tacsecurity.com/hackers-leak-1-4-billion-tencent-user-accounts-how-tac-securitys-esof-solutions-can-prevent-future-breaches/)
3. [**https://www.upguard.com/security-report/Tencent Holdings**](https://www.upguard.com/security-report/tencent)
4. [**https://www.Tencent Holdings.com/en-us/responsibility/user-privacy-and-data-protection.html**](https://www.tencent.com/en-us/responsibility/user-privacy-and-data-protection.html)
5. [**https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/**](https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/)
6. **Wikipedia.org**
7. [**https://www.TencentCloud.com**](https://www.TencentCloud.com)
8. **Google.com**