Lavontay Johnson

Prof. Zehra

CS 462

11 November 2024

The Dissection of the 23andMe Breach

(CS 462 REPORT)

I decided to do my paper on a fairly recent cyberattack that may raise some eyebrows when you first mention it and that's the 23andMe breach. In October 2023, a hacker by the name of 'Golem' shifted their focus towards one of the more popular and well known genetic testing companies, 23andMe. To be honest, I think everyone could agree that one of the worst and scariest places that could potentially be breached is either a bank or a genetic testing company. In my opinion, this breach highlights critical vulnerabilities in how companies protect sensitive genetic and personal data. This breach has widespread implications for data security, privacy, and ethical standards in the tech and healthcare industries. In this paper, I'll analyze the attack methods, technologies involved, and its impact on society.

I think to start this out, I should give a little background to 23andMe and what makes them so significant to the point of being a potential target for a huge cyber attack. 23andMe is a well-known genetic testing company that provides consumers with insights into their ancestry, health risks, and genetic predispositions through DNA testing kits. From my knowledge, there's only really two well known DNA testing kits that everyone uses, and that's either Ancestry or 23andMe. With over a millions users worldwide, 23andMe, holds a vast database of highly sensitive and important genetic data.

Around October 2023, the company came out and acknowledged a data breach that resulted in unauthorized access to millions of users' data, including full names, genetic profiles, ancestry, and users' locations. Millions being around 7 million exactly, which caused heads to turn all around the world as some people learned that their genetic data and other information may be in the hands of someone else.

You might ask yourself, how were they able to pull off this massive attack? Well, the answer may sound a bit simple hearing it, but it's way more complex than you think to the common human brain. Stealing 7 million peoples' information, genetic information I might add, is no easy feat and "it turns out that it was a classic credential-stuffing attack, which means criminals used credentials from other data breaches to gain access to 23andMe accounts" (Bitdefender 2023). Credential stuffing is a widespread cyberattack method that capitalizes on the tendency of individuals to reuse passwords across multiple sites. It usually involves exploiting email and password combinations leaked from prior data breaches on other websites. It also relies heavily on automated bots as well. These bots use scripts to rapidly enter credentials on login pages. This technique takes advantage of poor rate limiting measures on websites, where multiple rapid login attempts might otherwise trigger a security alert. So, after that, once they gained entry to a small number of the accounts through the breach, attackers utilized the platform's own "DNA Relatives" feature, which allows users to connect with genetic relatives. This part to me is kind of wild, as they scraped data from connected relatives, the hacker accessed data for millions of additional users who were connected but had not reused compromised credentials, vastly multiplying the scale of the breach.

To say this is all on 23andMe is not entirely true as some of the users, who partake in reusing their passwords across multiple sites and platforms are partly to blame as well, as wild as that sounds. However, I was astonished as 23andMe's initial response largely attributed the breach to user negligence in reusing passwords, though it has since mandated MFA for additional security. A few months after the incident, "the company said in a letter to some individuals that "users negligently recycled and failed to update their passwords following … past security incidents, which are unrelated to 23andMe" (Wired 2024). I actually do believe they have a point here and I can see where they're coming from, but I don't think that was the right approach. Also, in terms of preventing the breach in the first place, if they knew a problem like a good portion of their users not updating their passwords was going to bite them in the foot later down the road, they should've made it an absolute priority that each account needed to update their passwords to gain access towards their account and made MFA mandatory from when you first create your account. You don't do all of that once you've already been breached, especially considering how advanced hackers are nowadays and how easily some of them can breach your systems.

Aside from the weak user authentication practices and failing to get their users to update their passwords, the scale of data exposure indicates that large sets of genetic information and personal data was readily accessible once the hacker accessed the users' accounts. Enhanced compartmentalization of sensitive data, ensuring genetic data and personal data are not stored in the same easily accessible environment, could have reduced the breach's scale. Also, if I had a say in all this, I would vote to store and keep the majority or all of the highly sensitive information in cold storage. In my opinion, doing this would reduce the risk of breach by a high margin as cold storage is typically disconnected from the internet, making it much harder for attackers to access. 23andMe could have easily minimized the amount of data vulnerable to a credential stuffing attack, as the attackers could only access data stored on accessible servers online for the most part. What I mean by that is that the data stored in cold storage can also be encrypted and accessible only through multiple layers of authentication. This approach means that even if attackers gain access to user accounts, they wouldn't have an immediate path to the data, as it would require separate, highly restricted authentication to decrypt and access the stored genetic information, which is 1000x more complicated compared to being able to obtain and steal that data online through the servers.

To be honest, I think this topic in general has affected our society a great deal and when I say affected, I mean affected in the most frightening way possible. I mean this whole incident seems like it's straight out of a movie before the world becomes overrun due to a genetic breach like this one. I honestly think that the breach has affected the general public's trust in genetic testing. I mean a lot of people were already hesitant about giving away their DNA to big companies like this because they have no clue what their plans are for it in the future. With that being said, Many users entrust companies like 23andMe with their most personal data, expecting it to be safeguarded. So, high profile breaches like this could scare off people from engaging in genetic testing, which could hinder valuable research and progress in personalized medicine for the future.

With all that being said, I hope this has some upside to our society as well when it comes to proper security awareness because if this isn't a wake up call for most people, then I don't know what is. This should also be a wake up call for most companies as well. Using a method like credential stuffing, doesn't really need to take advantage of your systems, in fact, it takes advantage of your user's who fail to change up their passwords when it comes to using them across multiple platforms. So, this should urge companies to stay up to date when it comes to making routine password changes and MFA absolutely mandatory, so they don’t have to worry about their users being a weak point in their defense.

In the end, the 23andMe breach has turned out to be a stark reminder of good cybersecurity and its need for implementation, particularly in firms operating with sensitive personal and genetic information. The breach also reveals the vulnerabilities that have been created both at the level of the individual user for instance, password reuse and at the company level, such as not having enforced multi-factor authentication or proper compartmentalization of data. The scale of the breach, with credential-stuffing attacks on the rise, shows how high the stakes are when genetic data is involved. Blaming users somewhat when it comes to updating passwords 23andMe underlined a wider problem in the industry: security practices need to expect and account for user behavior with rigorous standards.

Because of this, companies should install various measures to help better safeguard against such attacks: mandatory MFA from the outset, periodic updating of passwords, and stronger compartmentalization of data. Storing the most sensitive data in cold storage, in my opinion, would be extremely beneficial. Systems disconnected from the internet would drastically reduce exposure. On an individual note, this breach speaks to the necessity of good password hygiene; personal habits can directly affect the security of both personal and genetic data. Fundamentally, the 23andMe breach serves as a strong indicator for organizations and users to show how both parties are considered responsible in adapting to emerging threat points and to introduce measures that provide security for highly sensitive information in today's digital world.

References

Hay, L., & Greenberg, A. (2024, January 6). *23andMe blames users for recent data breach as it's hit with dozens of lawsuits*. Wired. https://www.wired.com/story/23andme-blames-users-data-breach-security-roundup/

Stahie, S. (2023, December 5). *23andMe confirms data breach that started as a credential stuffing attack*. Hot for Security. https://www.bitdefender.com/en-gb/blog/hotforsecurity/23andme-confirms-data-beach-that-started-as-a-credential-stuffing-attack