Information security and assurance

Project report

(Priyanka Malla)

2020 Zoom bombing data breach

Introduction:

The security incident in the discussion here is the 2020 “Zoom bombing” breach. Zoom was at peak popularity at the time due to the rise in the need for virtual meeting platforms due to covid-19 pandemic, their user base had a spike from around 10 million to 300 million in a matter of months due to the pandemic, these lucrative numbers combined with poor password management practices, and bad security practices by many new users made zoom a valuable and easy target. Using credential stuffing technique hackers were able to disrupt meetings and get hold of confidential information of schools and companies using zoom as the platform, the breach directly affected mostly schools and companies and indirectly led to the leak of information the schools or corporation’s clients. As an effect zoom was banned by major corporations including NASA and was under several lawsuits from their clients. Zoom addressed the issues gradually and started adding countermeasures like MFA, and single-use meeting IDs. With the involvement of the FBI, the zoom bombing was made a criminal offense.

Who was the victim of the breach?

In 2020, Zoom experienced a huge data breach that affected over half a million subscribers. The 'Zoom bombing' phenomenon was caused by user credential sharing, open meetings, and poor password management. Hackers would disrupt Zoom calls, which were primarily intended for schools and colleges, by using obscene language or otherwise disrupting the conference. The situation became so serious that the FBI was called in, and several organizations and state offices throughout the world banned the use of Zoom. The use of zoom bombing is now illegal in the United States, and the perpetrators may face legal action.

Most of the Zoom credentials belonged to faculty members and students in schools and universities. Many well-known corporate clients, including Chase and Citibank, were also included on the list.

Who/What was the source for this breach?

According to Cybel, the Zoom login credentials of the users were most likely obtained through a technique known as "credential stuffing." Credential stuffing is a type of cyberattack in which hackers steal login credentials from one website or application and use them to gain access to another. Users that use the same username (or email address) and password for many websites and applications are vulnerable to this type of attack. Assume you use the same email address and password for Facebook, Amazon, Zoom, Twitter, Instagram, and your energy provider. In that case, a hacker only needs to compromise one of these apps to obtain your login credentials for all six accounts. To extract users' email addresses and passwords, cybercriminals frequently attack a website or application with minimal security. The hackers then test these credentials against millions of websites and applications using automation tools like Selenium, cURL, and PhantomJS. If the login credentials are valid for another account, the user's information is added to a list (in this case, a Zoom list of over 530,000 users) and subsequently sold on the dark web.

"If your username and password are compromised from Company A—who suffered a data breach—and you use that same username and password to login to your social media account, then that account could also be in jeopardy." A statement from the NSA following Zoom's credential hack.

What mitigation steps were taken to address the breach/incident?

Zoom deployed three types of mitigation methods to prevent data loss in the future.

Preventative Mitigation

1. Implementation of single-use meeting IDs and random meeting pins to minimize attackers replaying the previous meeting invites or guessing new meetings.
2. Separating meeting access and administrative duties to control zoom bombing.

3. Technical measures through threat modeling to prevent publicly displayed meeting information and proper random numbering sequences.

Detective Mitigation

1. Checking account credentials against compromised password lists to monitor account password abuse.
2. Auditing administrative settings for deletion and inactive account monitoring.
3. Data exfiltration through chat or other virtual environment methods.

Corrective Mitigation

1. Immediate clean-up by the Incident Response Team.
2. Forensic investigations to determine accurate evidence.
3. Training users on new security changes.

What could have been done to possibly prevent the initial compromise?

This credential attack is the responsibility of both Zoom and its users. Zoom should have had security measures in place to prevent credential stuffing, and users should practice better credential and password etiquette. Preventing credential stuffing is relatively inexpensive and simple for websites and applications. For example, Google's reCAPTCHA creates a problem for users to solve before verifying authentication. These challenges are too complex for bots and inhibit credential stuffing efforts, despite being simple for people. Two-factor authentication is another approach for programs to prevent credential stuffing (2FA). While zoom may not have been solely responsible for the April 2020 credential hack, there are actions Zoom could have done to prevent credential stuffing attempts.

How Users can Prevent a Credential Stuffing Attack -

- Never Use the Same Passwords

- Never Share Login Credentials

- Create Strong Unique Passwords

When did this occur?

Around April 1, 2020, cybersecurity experts discovered the Zoom accounts on the dark web. Hackers must have worked relentlessly in the months before the breach to harvest all of the usernames and passwords, which they then sold for a penny each.

What lessons were learned as a result of the breach and aftermath?

The first rule is to use a unique password for every account. The Zoom credential attack would not have happened in 2020 if everyone used this password strategy.

Passwords should be changed frequently. Passwords should be changed every 90-180 days, according to TeamPassword, a password management tool. If you suspect any account is being used fraudulently, change the password right away and alert the app or website's customer service.

For every account that permits it, enable two-factor authentication. The extra step might be annoying, but nothing is worse than being hacked, especially if you lose money in the process.

To create strong, unique passwords that are nearly impossible to guess, use a password generator. Use uppercase, lowercase, symbols, and numerals in a minimum of 12 characters.