# Case Study

## Unauthorized Access And Data Theft.

### **Linkedin**:

During the year 2012, LinkedIn encountered a breach of its data, in which malevolent individuals managed to obtain password hashes. It was later revealed that around 6.5 million sets of account credentials were openly shared on a Russian password forum. Currently, an individual going by the name "Peace" is offering to sell the pilfered database for a sum of 5 bitcoins, which is approximately equal to 2,200 USD.

# Attack Category: **Credential Theft:**

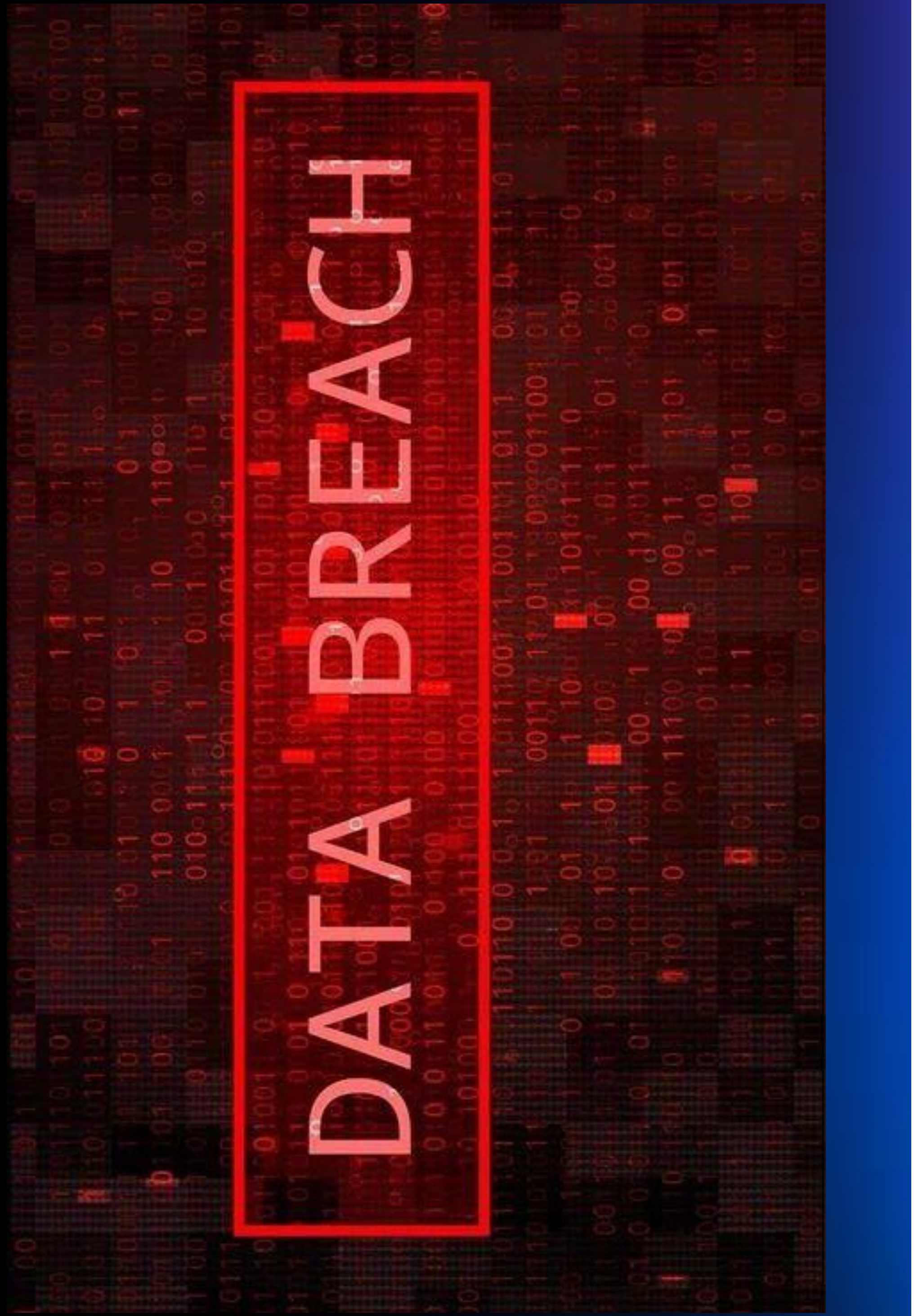
In this particular form of attack, cybercriminals direct their efforts towards ***acquiring user credentials, including usernames and passwords,*** with the ultimate goal of illegitimately accessing systems or accounts. In the instance of the LinkedIn breach, the attackers triumphed in obtaining password hashes, which they subsequently disclosed on a public forum. This type of attack revolves around the acquisition and exploitation of user credentials to compromise accounts, ***gain unauthorized entry, or carry out additional malicious actions.***

In 2021, about 23.9 million people ***(9% of U.S. residents age 16 or older)*** had been victims of identity theft during the prior 12 months. For 76% of identity-theft victims in 2021, the most recent incident involved the misuse of only one type of existing account, such as a credit card or bank account

## Sources

https://www.cyberscoop.com/nikulin-trial-linkedin-oleksandr-ieremenko/
https://pldeb.ru/en/haker-nikulin-poplatilsya-za-nezdorovoe-lyubopytstvo-k-hillari/
https://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised
https://www.vice.com/en/article/78kk4z/another-day-another-hack-117-million-linkedin-emails-and-password
https://krebsonsecurity.com/2016/05/as-scope-of-2012-breach-expands-linkedin-to-again-reset-passwords-for-some-users/
•https://www.rferl.org/a/in-u-s-hacker-trial-the-tangled-web-of-russia-s-cyberunderground-is-further-exposed/30472603.html
Video: Arrest of Yevgeny Nikulin

# Company Description and Breach Summary



**LinkedIn is a renowned professional networking platform that enables individuals to create profiles, connect with colleagues, and establish professional relationships. It serves as a hub for job seekers, recruiters, and professionals to engage, exchange industry knowledge, and explore career prospects. With a vast user base spanning the globe, LinkedIn stands as a prominent platform for professional networking and interaction.**

**Summary of the Breach:**

- **During 2012, LinkedIn encountered a significant data breach.**
- **The breach involved unauthorized access to the user database and the theft of password hashes.**
- **Approximately 6.5 million password hashes were illicitly acquired.**
- **The stolen password hashes were subsequently published on a public forum dedicated to Russian password discussions.**
- **Immediate measures were taken in response, including password resets for affected accounts and the implementation of enhanced security protocols.**
- **This incident serves as a reminder of the critical importance of employing strong passwords and adhering to robust cybersecurity practices.**

# Timeline

1

**Event 1**

Pre-Breach: Attack Planning and Execution

Hackers plan and execute the attack on LinkedIn's systems.

They identify vulnerabilities and exploit them to gain unauthorized access..

2

**Event 2**

Breach Discovery and Investigation

LinkedIn's security team detects suspicious activity and investigates the incident.

They notice signs of unauthorized access and potential data compromise.

3

**Event 3**

Confirmation of Data Breach

LinkedIn confirms that a data breach has occurred and user account credentials are compromised.

They notify affected users and provide instructions for password resets.

4

**Event 4**

Public Disclosure of Breach

LinkedIn publicly discloses the data breach, acknowledging the theft of password hashes.

They emphasize the importance of strong passwords and security measures.

5

**Event 5**

Stolen Password Hashes Posted Online

The stolen password hashes are discovered on a Russian password forum.

The compromised credentials become publicly accessible to potential attackers.

6

**Event 6**

Response and Mitigation Measures

LinkedIn takes immediate action to mitigate the impact of the breach.They reset passwords for affected accounts and implement enhanced security measures to prevent future breaches.

# Vulnerabilities

Vulnerabilities refer to weaknesses or gaps in security measures that can be exploited by attackers. In the case of the LinkedIn data breach, several vulnerabilities contributed to the unauthorized access and compromise of user data. These vulnerabilities highlight the importance of robust security practices to protect against potential breaches.

## Vulnerability 1

Insufficient password hashing measures were employed by LinkedIn, as the passwords stored were hashed using the SHA-1 algorithm without the implementation of proper salting. This oversight facilitated attackers in their endeavors to decipher the hashed passwords through the utilization of precomputed rainbow tables or brute-force techniques.

## Vulnerability 2

A significant number of LinkedIn users employed weak or easily predictable passwords, rendering them susceptible to exploitation. This vulnerability enabled attackers to more easily decipher the passwords once they gained access to the hashed values.

## Vulnerability 3

During the time of the breach, LinkedIn did not implement robust authentication measures, such as multi-factor authentication (MFA), to ensure strong account security. Consequently, user accounts were left more exposed to unauthorized access, as attackers only needed to successfully crack the password hashes without the added layer of MFA protection.

## Vulnerability 4

LinkedIn's systems suffered from inadequate monitoring and detection capabilities, which resulted in a lack of effective mechanisms to identify suspicious activities or irregular behaviors. This deficiency in monitoring and detection considerably delayed the detection of the breach, enabling the attackers to remain undetected for an extended duration.

# Costs and Prevention

## Costs

- **Reputational Damage**: The data breach resulted in significant reputational damage for LinkedIn, eroding user trust and potentially affecting user engagement and adoption rates.
- **Financial Losses**: Remediation efforts, including investigations, incident response, and implementing enhanced security measures, incurred substantial financial costs.
- **Legal Consequences**: LinkedIn faced potential legal consequences, including regulatory fines and lawsuits from affected users for failing to adequately protect their data.

## Prevention

- **Strong Password Practices**: Encourage users to create strong, unique passwords and implement password complexity requirements. Enforce regular password updates and educate users on the importance of password security.
- **Robust Password Storage**: Implement strong encryption algorithms with proper salting to protect user passwords. Avoid using outdated or weak hashing algorithms.
- **Multi-Factor Authentication** (MFA): Implement MFA as an additional layer of security to protect user accounts. Require users to provide an additional verification factor, such as a code sent to their mobile device, in addition to their passwords.
- **Regular Security Audits**: Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in the system. This includes reviewing access controls, network security configurations, and application security measures.
- **Employee Education and Awareness**: Train employees on best practices for data security, including identifying phishing attempts, practicing good password hygiene, and recognizing suspicious activities.
- **Incident Response Planning**: Develop a comprehensive incident response plan to ensure a swift and effective response in the event of a breach. This includes establishing clear roles and responsibilities, communication protocols, and procedures for investigation and containment.
- **Ongoing Monitoring and Detection**: Implement robust monitoring and detection systems to identify and respond to suspicious activities promptly. This includes real-time monitoring of network traffic, system logs, and user behavior analytics.