Case Study:

Stolen Credentials/3rd Party Software/2FA Fatigue

LastPass Data Breach 2022

Attack Category:

Stolen Credentials/3rd Party Software/2FA Fatigue

1. According to sources, LastPass' devops engineer's plex server was compromised due to security flaw in the plex(old version), and it was then used to gain access to the corporate vault which contains the encryption keys for s3 vault of production backups.

2. The customer data included customers' names, billing addresses, phone numbers, email addresses, IP addresses and partial credit card numbers, and the number of rounds of encryption used, MFA seeds and device identifiers.

3. The LastPass themselves didn't disclose the number of customer passwords stolen, but there's big possibility to be a large number or even all of them.

Sources:

https://arstechnica.com/information-technology/2023/02/lastpass-hackers-infected-employees-home-computer-and-stole-corporate-vault/

https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/

https://proton.me/blog/lessons-from-lastpass

Company Description and Attack Summary

LastPass is password manager with over **30 million** customers worldwide. The breach started by gaining access to the **software engineer's** laptop by using **stolen credentials**. Though his account was secured with 2FA, but the attackers bombard him with the 2FA request and eventually due to phenomenon known as **2FA fatique**, he accepted the login request, and the attackers was in. From that account, they stole coroporate record of other employees including the **four principle engineers** who have access to the lastpass **s3** bucket of **production backups**. The employee compromised was a **DevOps engineer**, who was using a very old version of **plex** on this machine. It led the to the exploitation of known vulnerability, and then from there they stole the encryption keys to access the **Amazon s3 bucket**, which hosted production backups of the lastpass database.

Timeline

1

Event 1

Hackers gained access to LastPass software engineer’s account.

2

Event 2

AWS cloud devlopment environment was compromised, valuable corporate assets were stolen, but no customer data.

3

Event 3

Unkown to lastpass at that time, the attackers examined the aws logs to discover where encryption keys were stored, who had accessed to them, and from which IP addresses they were accessed.

4

Event 4

Sr. DevOps engineer was running 3 years old plex server with RCE.

5

Event 5

Using the RCE, attackers installed a keylogger, and when the engineer accessed the s3 bucket with his credentials, they stole them.

6

Event 6

Now, they had access to both development and production environment and all the in their hand to streal whatever they want.

Vulnerabilities

Stolen credentials, 3rd party software, 2FA fatigue and lack of network seggregation was the major contributors to the LastPass breach.

Stolen Credentials

Stolen credentials from old breach were the entry point for this attack.

3rd Party Software

The vulnerability in the old version of the plex server was exploited. It was an Remote Code Exploitation (RCE), which allowed attacker to upload/execute any script on the victim device.

2FA Fatigue

When the first event happened, it was the 2FA fatigure the led the attackers in. The software engineer was bombareded with the 2FA request, and eventually he accepted it.

Lack of Network/Device Segregation

The home computer was used to access the company resouces, which had RCE in the 3rd party software that led to the stolen customer data.

Cost and Prevention

Costs	Prevention
1. The customers database was stolen.	1. Build system, that is attack resistent to even the state level attacks.
2. The company faced a lawsuit where the plaintiff accused LastPass breach of stolen crypto assets of worth $53000.	2. Use more modern hashing algorithms, lastpass used **PBKDF2**, which is now superseded by the state of the art algorithms like **Argon2** etc.
3. The customers were agry as there was no true E2EE for all the data, instead some of the important data was stored in the plaintext.	3. Encrypt all data, lastpass didn’t encrypt all the data like, login urls which can leak important information.
4. The old lastpass customers before 2018, are at greater risk due to weak default values for the encryption. Their passwords and username are at the risk of being decrypted by the attackers.	4. Segregation of network and devices to avoid 3rd party software vulnerabilities.

Sources

1) https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/
2) https://www.wired.com/story/lastpass-engineer-breach-security-roundup/
3) https://securityintelligence.com/news/lastpass-breaches-cast-doubt-on-password-manager-safety/
4) https://proton.me/blog/lessons-from-lastpass
5) https://arstechnica.com/information-technology/2023/02/lastpass-hackers-infected-employees-home-computer-and-stole-corporate-vault/
6) https://www.pcmag.com/news/lastpass-faces-class-action-lawsuit-over-password-vault-breach
7) https://securityintelligence.com/articles/whats-going-on-with-lastpass-and-is-it-safe-to-use/