**LastPass Security Breach: What You Need to Know**

**Executive Summary:** One of the prominent password management software companies, LastPass suffered two cyber-attacks from August to October 2022. In the first incident, a hacker got access to a cloud-based development environment by breaking into a software engineer's laptop. The hacker acquired login credentials, source code, technical data, and internet system secrets. The attacker utilized this information to get access to the corporate vault of LastPass, resulting in the second incident three months later. In the second incident the attacker was able to get access to customer account details, API keys and third-party data, LastPass customer information, and LastPass vault data including website usernames and passwords, secure notes, and form-filled data. LastPass responded to the breaches by collaborating with security experts, installing new security technologies and procedures, and replacing any susceptible certificates. The incidents had a minor impact. But still they highlighted the significance of solid password management rules and continual assessment and upgrading of security safeguards.

**Introduction:** LastPass is a technology business that focuses on security, password management software, and cybersecurity. LastPass, situated in Fairfax, Virginia, was founded in 2008. The company provides innovative technologies such as password managers, autofill, and multi-factor authentication to secure users' digital identities. With over 1,200 workers as of September 2021, LastPass has established itself as an industry leader. However, in a recent security incident labeled "Data Theft," LastPass stated that a third-party cloud storage service used to hold archived backups of production data had been accessed by an unauthorized source. The event emphasizes the significance of constant awareness and continuous enhancement of security measures in today's quickly expanding digital ecosystem.

According to the LastPass published update, there were two incidents reported from August to October 2022.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** |  |  | **Event** |
| 12th of August 2022 |  |  | An unauthorized third party hacked a LastPass software engineer's laptop, stealing login information, source code, technical information, and specific LastPass internet system secrets by getting access to a cloud-based development environment. |
| 11 October 2022 |  |  | The attacker uses information obtained from the first incident to get access to LastPass' corporate vault. Customer account information, API keys and third-party data, LastPass customer information, and LastPass vault data, including website usernames and passwords, secure notes, and form-filled data, are obtained by the attacker. |
| 14 October 2022 |  |  | LastPass detects the incident and investigates. |
| 18 October 2022 |  |  | LastPass makes the breaches public and notifies affected users. |
| 19 October 2022 |  |  | LastPass acknowledges that the breaches have been isolated and is taking multiple steps to resolve the incidents, including working with security experts, adopting new security technologies and procedures, and replacing any susceptible certificates. |

Table 1: LastPass breach timeline

**Incident 1: How it happened:** On August 12, 2022, a corporate laptop of a software engineer of LastPass was hacked by an unauthorized threat actor and the threat actor successfully stole login information, source code, technical information, and certain LastPass internet system secret by gaining access to a cloud-based development environment. The cyber attacker used the software engineer’s legitimate MFA verification for accessing the cloud-based programming environment. The tampering of the laptop’s EDR was correctly configured and did not activate. To hide the identity and behavior in the cloud environment, the cyber attacker used “anti-forensic” techniques and a third-party VPN service.

**What was stolen from the first incident:** According to theLastPass blog,there were no customer or vault data available in the development environment. So, the threat attacker could not steal any customer information during the first event.But, based on the LastPass technical details and LastPass blog, the attacker obtained both proprietary and consumer information from LastPass. This data set contains 14 of the 200 software repositories, LastPass secrets and certificates, and technical information about how the development environment functioned. Data collected in August was used to acquire access to users' data three months later, allowing the second incident to begin.

**What measures were taken by LastPass after the first incident:** LastPass worked with Mandiant and their own internal security teams to uncover the first incident. They neutralized the contaminated environment and created a new one. All-important clear text secrets used by their teams were changed, new security technologies and controls were implemented, and any vulnerable certificates were replaced. LastPass went on to fix the problem.

**Second Incident:** Only four LastPass employees had access to the corporate vault, along with the hacked DevOps engineer. The threat actor targeted a senior DevOps engineer’s personal laptop.It was assumed that the attacker used plex media software to gain access to this computer, which enabled remote code execution, enabled the threat actor to implant keylogger malware. The employee’s master password was entered. That helped the attacker to capture it and alter it. The attacker gained access to the corporate vault by using the employee authentication with MFA. Because the hacker used the employee's authentic credentials, their activity was difficult to identify as malicious.

**What was stolen from the second incident:** Once in possession of the decrypted vault, the threat actor exported the entries, including "decryption keys needed to access the AWS S3 LastPass production backups, other cloud-based storage resources, and some related critical database backups." Those backups contained system configuration data, API secrets, third-party integration secrets. The attacker also gained access to personal information such as corporate names, end-user names, billing addresses, email addresses, phone numbers, and IP addresses used by clients to use LastPass services. They copied a copy of client vault data, which contained both unencrypted data and encrypted data fields including website usernames and passwords, secure notes, and form-filled data.

|  |  |
| --- | --- |
| **Affected Data Type** | **Description** |
| Customer Account Details | Email addresses, password reminders, authentication hashes, and other information. |
| API Keys and Third-Party Data | Credentials for a variety of LastPass integrations. |
| LastPass Customer Information | Email addresses of users, authentication hashes, and other sensitive data. |
| Data from the LastPass Customer Vault | LastPass vaults stored user data such as passwords and notes. |

Table 2: What data was affected by attacker from both incidents

**Impact of the incidents:** The incident had a minor impact, with no instances of unauthorized access to users' LastPass accounts or critical information. However, the incident emphasized the necessity of robust password management policies and the need for businesses to constantly review and enhance their security safeguards.

|  |  |
| --- | --- |
| Impact Category | Estimated Impact |
| Number of Affected Users | LastPass acknowledged that the assault affected a small number of its users but did not indicate how many. |
| Types of Data Exposed | End-user names, corporate names, billing addresses, email addresses, phone numbers, and IP addresses are all examples. They made a duplicate of the client vault data, which included both unencrypted and encrypted data fields such as website usernames and passwords, secure notes, and form-filled data. |
| Financial Impact | The breach's exact monetary impact is unknown; however, it could result in expenditures related to investigation, remediation, and legal fees. |
| Reputational Damage | The incident has the potential to create moderate to serious reputation harm for LastPass, as customers could lose trust in the platform's security. |
| Legal Consequences | LastPass did not face any legal consequences for the security breach incidents in 2021. But in future LastPass may have to face legal consequences. |

Table 3: Estimation of the impact of both incidents

**What measures were taken by LastPass after the second incident:** According to LastPass's official blog, LastPass is now giving the utmost priority in securing their data. Hiring security specialists is one of the steps. The organization has already implemented several security steps, such as platform, infrastructure, and end-user security updates, product improvements, and mid-term strategic expenditures.

Among the specific actions they have taken or intend to take are:

* Tuning their production environment's investigative and preventative controls, hardening their cloud storage environment, and adopting a Cloud Security Posture Management (CSPM) platform across all cloud estates.
* Endpoint security measures for developer and engineering workstations are being improved, including the deployment of a new managed Endpoint Detection and Response (EDR) service and further detection settings, as well as the distribution of hardware security keys to developers and engineers.
* Increasing the “default PBKDF2 SHA256 iterations to a minimum of 600,000, encrypting URL and URL-related fields in vault BLOBs”, and discontinuing Password Apps (Push Sites/Apps) capability.
* Mid-term strategic investments focused on increasing the encryption of customer data and metadata in databases, accelerating, and improving cryptographic primitives, and ensuring the “use of a standardized set of modernized and standards-based cryptographic APIs across” all client platforms where encryption is used.

To show the concern for their customers, the company prepared two separate bulletins; One security bulletin was for their free, premium, and families consumer suggesting them to secure their accounts by confirming that they are following the best practices. Another security bulletin was for their business and teams customers with relevant information.

Furthermore, LastPass is focusing on strengthening master password recovery options, providing additional automatic reports for commercial customers, and preparing to force-improve master password selection hygiene. In addition, the company is changing its software factory/development environment by introducing updated cloud-based CI/CD pipelines and guaranteeing “compliance with Software Bill of Materials (SBOM) and Supply Chain Levels for Software Artifacts (SLSA) Level 3+/NIST 800-218 standards”.

|  |  |
| --- | --- |
| **Attempts at Mitigation** | **Acted** |
| Security bulletins | LastPass published two different security bulletins for its free, premium, and family consumer, as well as business and teams users, to propose best practices and provide pertinent information. |
| Notification of affected users | LastPass notified affected users to reset their passwords. |
| Investigation and analysis | LastPass initiated an investigation. |
| Resetting the password | As a precaution, LastPass suggested all affected users to reset their passwords. |
| Communication with stakeholders | LastPass provided regular updates to its users and stakeholders throughout the crisis period. |
| Internal evaluation and improvement | To identify areas for improvements in security practices, internal reviews were conducted. |
| Additional security measures | Following the hack, LastPass implemented many security steps, including adding security specialists, strengthening endpoint security, expanding client data encryption, and introducing updated cloud-based CI/CD pipelines. They have also prepared individual security warnings for their clients and are working to improve master password recovery alternatives. |

Table 4: Severity mitigation attempts by LastPass

**Who was the cyber attacker:** The attacker who was responsible for this LastPass breach remains unknown. The investigation conducted by the company did not disclose the identity of the attacker.

**Conclusion:** The LastPass security breaches pointed out the importance of cybersecurity and the need for constant effort in securing sensitive data in today's digital world. Despite LastPass' attempts to deploy rigorous security measures, attackers were able to exploit weaknesses and obtain access to proprietary and customer information, underscoring the importance of ongoing security improvements. Although the attacks had minor impact on LastPass users, they could result in legal, remedial, and reputational costs for the corporation. As a result, LastPass and other businesses must continue to invest in cybersecurity technologies and staff to limit the dangers of data breaches and protect their customers' information.