



FLASH

LASTPASS BREACH UPDATE

ZEROFOX INTELLIGENCE

F-2023-01-09a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Hacking, Data Leak

January 9, 2023



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 1:00 PM (EST) on January 9, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

LastPass Breach Update

Key Findings

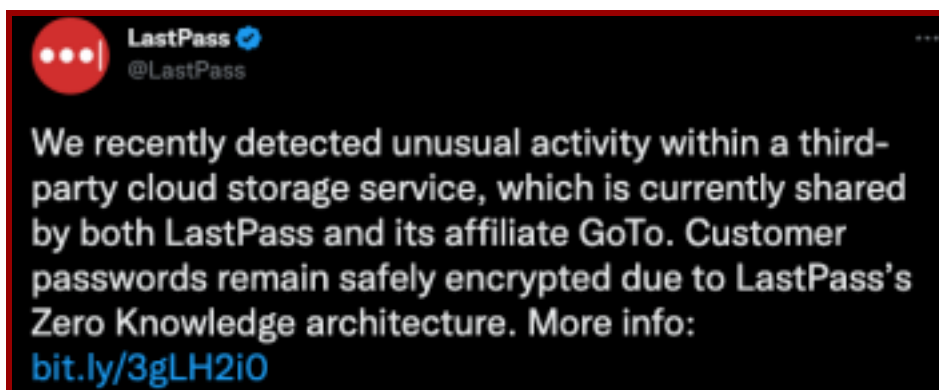
- Concern over an August 2022 security incident at LastPass has grown considerably from initial assessments.
- The number of LastPass users impacted by the breach remains unknown.
- In December 2022, LastPass determined that the threat actor gained access to customers' company names, end-user names, billing addresses, email addresses, telephone numbers, and IP addresses.
- A class action lawsuit has been filed against LastPass seeking damages and restitution for any LastPass users who had data stolen in the breach..

Analyst Commentary

In August 2022, LastPass indicated on its blog that it had been impacted by unauthorized third-party access to source code and some proprietary technical information.¹ Subsequently, on November 30, 2022, LastPass announced an unauthorized party accessed a third-party cloud storage service shared with its affiliate, GoTo. According to the company's official statement, the cloud storage service contained "certain elements" of customer information.²

¹ [hXXps://blog.lastpass\[.\]com/2022/12/notice-of-recent-security-incident/](https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/)

² [hXXps://twitter\[.\]com/LastPass/status/1598047380305104896](https://twitter[.]com/LastPass/status/1598047380305104896)



LastPass Announces Breach of Third-Party Cloud Storage Service

Source: [hXXps://twitter\[.\]com/LastPass/status/1598047380305104896](https://twitter.com/LastPass/status/1598047380305104896)

While LastPass provided few details about the scope of the unusual activity within the third-party cloud storage service, it revealed that the unauthorized party leveraged information obtained from the August 2022 breach of its development environment. During the August 2022 breach, a threat actor exfiltrated portions of source code and proprietary technical information. In a subsequent September 2022 update, LastPass revealed the actor maintained access for a four-day period and confirmed they did not access customer data. The company added that the actor carried out the attack by compromising a developer's endpoint and impersonating the developer after they had authenticated using multi-factor authentication (MFA).

On December 22, 2022, LastPass released an update on the security incident involving the November breach of a third-party cloud service shared with GoTo.³ LastPass determined that once the cloud storage access key and dual storage container decryption keys were obtained, the threat actor copied information from a backup that contained basic customer account information and related metadata. The threat actor was also able to copy a backup of customer vault data from the encrypted storage container, which is stored in a proprietary binary format that contains both unencrypted data and fully-encrypted sensitive fields.⁴ According to the statement, significantly more content associated with users was also accessed as a result of the breach, including company names, end-user names, billing addresses, email addresses, telephone numbers, and customers' IP addresses.⁵

At this time, LastPass continues to indicate that while the threat actor *did* obtain the user password vaults, the associated master passwords *were not* accessed. This would require the threat actor to utilize tactics such as brute force or credential stuffing to

³ [hXXps://blog.lastpass\[.\]com/2022/12/notice-of-recent-security-incident/](https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/)

⁴ *Ibid.*

⁵ [hXXps://arstechnica\[.\]com/information-technology/2022/12/lastpass-says-hackers-have-obtained-vault-data-and-a-wealth-of-customer-info/](https://arstechnica.com/information-technology/2022/12/lastpass-says-hackers-have-obtained-vault-data-and-a-wealth-of-customer-info/)



access the actual password vaults. In addition, according to LastPass, there has not been any indication that credit card information was accessed, as LastPass does not store it in its entirety, nor is that information stored in the same place as the other data was accessed.⁶

Lastly, a class action lawsuit was filed against LastPass on January 3, 2023, in the United States District Court for the District of Massachusetts, alleging that LastPass did not adequately protect its users' information and that the breach has led to financial losses for users.⁷ In the lawsuit, the plaintiff is suing LastPass for negligence, breach of contract, and deceptive acts. The plaintiff also alleges that the LastPass breach led to the theft of his Bitcoin cryptocurrency using private keys stored with LastPass.⁸

Recommendations

- Update current master and stored passwords with LastPass; while this will not change any impacts of the affected breached vaults, it is a best practice for getting ahead of potential future attacks.
- Enforce best practices on passwords, such as complexity, uniqueness, forced expiration, and prohibiting password reuse.
- Do not share passwords, and do not reuse the same password on different websites and applications.
- Enable two-factor authentication for all organizational accounts to help mitigate phishing and credential-stuffing attacks.
- Remain vigilant against potential phishing attempts.
- If not already enabled, engage with ZeroFox for ongoing compromised credential monitoring. Immediate password changes should be implemented for any affected account.
- ZeroFox recommends remaining vigilant and denying MFA requests not specifically triggered by logging in or requesting device enrollment. These requests are typically immediate and should not randomly appear throughout the day.

⁶

[hXXps://arstechnica\[.\]com/information-technology/2022/12/lastpass-says-hackers-have-obtained-vault-data-and-a-wealth-of-customer-info/](https://arstechnica.com/information-technology/2022/12/lastpass-says-hackers-have-obtained-vault-data-and-a-wealth-of-customer-info/)

⁷ [hXXps://regmedia\[.\]co\[.\]uk/2023/01/06/lastpass-august-breach-lawsuit.pdf](https://regmedia[.]co[.]uk/2023/01/06/lastpass-august-breach-lawsuit.pdf)

⁸ [hXXps://www.theregister\[.\]com/2023/01/08/in_brief_security/](https://www.theregister[.]com/2023/01/08/in_brief_security/)



Appendix: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.