



PASSWORD MANAGEMENT WOES CONTINUE ZEROFOX INTELLIGENCE

F-2023-01-20a

Classification: TLP:CLEAR

Criticality: HIGH

Intelligence Requirements: Compromised Account Credentials,
Compromise Impacts, Breach

January 20, 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 10:00 AM (EST) on January 20, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Password Management Woes Continue

Key Findings

- Another password manager has indicated that threat actors gained access to hundreds of thousands of customer accounts using credential stuffing.
- This breach differs from the LastPass breach in that the organization itself was not compromised, although a subset of accounts using the password manager were accessed.
- Users should update their passwords and avoid password reuse for multiple accounts.

Analyst Commentary

On the heels of news that the LastPass password manager service had been impacted by a breach in August 2022, another password manager has indicated that it was impacted by a security breach in December 2022. The parent company of the password manager indicates that its own systems were not compromised but that threat actors utilized credential stuffing in order to gain access to its accounts.¹ Credential stuffing is a tactic in which threat actors utilize already-compromised account credentials to attempt to gain access to other accounts. Because of the high prevalence of password reuse, threat actors have good success using this methodology; and in this case, they were successful on several fronts.

The notice indicates that the data accessed by threat actors includes first names, last names, phone numbers, and mailing addresses. The password manager impacted this time has a user base of around 500 million, and not all accounts were impacted; however, the company did indicate that it had to secure about one million accounts that had been targeted with credential stuffing attacks.² This also indicates that the

¹ [hXXps://www.businessinsider\[.\]com/personal-finance/what-is-credential-stuffing](https://www.businessinsider.com/personal-finance/what-is-credential-stuffing)

² *Ibid.*



threat actors now know the usernames and passwords for any accounts successfully accessed, and thus any sensitive information stored on the password manager accounts could be at risk. The company has stated that it continues to monitor accounts for suspicious activity and has reset passwords on impacted accounts.³

Recommendations

- Update current master and stored passwords utilized on any password management service; while this will not change any impacts of 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 multifactor authentication (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.

³ *Ibid.*



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.