



PHISHING ADS TARGET PASSWORD MANAGERS ZEROFOX INTELLIGENCE

F-2023-01-31a

Classification: TLP:CLEAR

Criticality: High

Intelligence Requirements: Phishing

January 31, 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 3:00 PM (EST) on January 31, 2023**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Phishing Ads Target Password Managers

Key Findings

- Phishing ads aimed at stealing password vault credentials are the latest tactic used to target password managers.
- Recent targeting of password managers has involved security breaches and credential stuffing attacks.
- Threat actors' level of sophistication with creating phishing pages continues to evolve.
- The identified phishing pages targeting the password managers have since been removed; however, this does not abate the threat of this type of activity.

Analyst Commentary

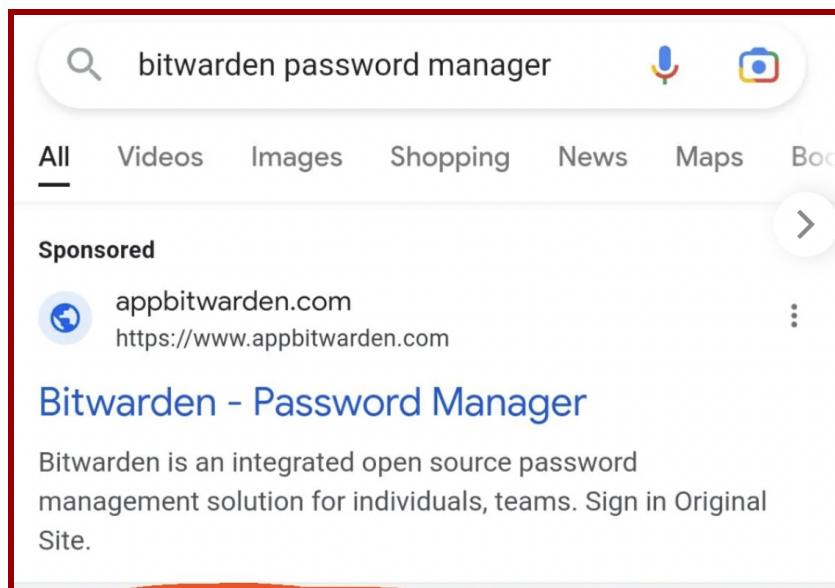
In the wake of recent breaches targeting password managers, another headache has emerged—this time targeting Bitwarden and other password managers. Over the last several weeks, ZeroFox Intelligence has reported on password managers being exploited via a security breach¹ and a credential stuffing attack.² Password managers are once again being targeted utilizing another attack vector—Google Ads phishing campaigns. These campaigns are aimed at stealing users' password vault credentials by creating phishing pages that look very similar to Bitwarden's or other password managers' login sites and then capturing the user's credentials.³ Adding to their perceived authenticity is that once credentials are entered, users are redirected back to the legitimate login pages.

¹ ZeroFox Intelligence. (2023, January 20). Flash Report: Password Management Woes Continue. Retrieved from [hXXps://cloud.zerofox\[.\]com/intelligence/advisories/19426](https://cloud.zerofox.com/intelligence/advisories/19426)

² ZeroFox Intelligence. (2023, January 9). Flash Report: LastPass Breach Update. Retrieved from [hXXps://cloud.zerofox\[.\]com/intelligence/advisories/19334](https://cloud.zerofox.com/intelligence/advisories/19334)

³

[hXXps://www.bleepingcomputer\[.\]com/news/security/bitwarden-password-vaults-targeted-in-google-ads-phishing-attack/](https://www.bleepingcomputer.com/news/security/bitwarden-password-vaults-targeted-in-google-ads-phishing-attack/)



Example of Bitwarden Phishing Site

Source:

[hXXps://www.reddit\[.\]com/r/Bitwarden/comments/10k2aj5/google_search_ads_showing_fake_bitwarden_web/](https://www.reddit.com/r/Bitwarden/comments/10k2aj5/google_search_ads_showing_fake_bitwarden_web/)

While some users claimed the phishing sites were relatively easy to spot, others indicated that they appeared to be legitimate and were challenging to identify.⁴ The phishing pages in question have been removed since being identified. However, depending on how successful the threat actors were in capturing credentials, they are likely to employ similar tactics in the future given the potentially high return on investment if password vaults can be accessed.

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.
-
-
- 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.
- Exercise caution when submitting credentials on websites, ensuring that they are legitimate sites.

⁴ [hXXps://www.komando\[.\]com/security-privacy/password-manager-cyberattacks/874586/](https://www.komando.com/security-privacy/password-manager-cyberattacks/874586/)



- 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.



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.