TIGR Threat Bulletin

SecurityRisk ADVISORS

LastPass Security Breach

January 6, 2023

Executive Summary

LastPass, a password management service, disclosed a security incident in late December indicating an unauthorized user accessed unencrypted metadata related to users' password vaults. After obtaining decryption keys in a previous attack against a LastPass employee, the adversaries accessed and exfiltrated decrypted metadata surrounding the stored credentials, such as company names, websites, email addresses, and more.

Adversaries also copied password vaults; however, the passwords within the vault and the master password remain safely encrypted with 256-bit AES encryption. Cracking a master password without the accurate decryption tool is difficult but not impossible, especially when adversaries already have access to relevant metadata. One should always assume that an offline cryptographic attack is feasible, given enough time, resources, and effort, regardless of the encryption's complexity.

Safeguards/Recommendations

Adversaries will likely abuse the compromised metadata to determine popular websites visited by victims and leverage the information in credential phishing emails. Organizations should educate users on how to spot and report potential phishing attacks.

Because the password vaults are already stolen, it is not necessary to change their master passwords. Instead, organizations should encourage users to change all credentials in the leaked password vault. If a threat actor discovers the master password, the data inside the vault will no longer be accurate if users reset all existing credentials.

If users feel that changing their password vault's master password would provide additional security, ensure the new password is both strong and unique from existing passwords. Avoid using common phrases, words, patterns, or any personal information.

An effective password recommendation is to pick several random words, numbers, and symbols that are memorable. Use the first letter of each word in both lower and upper case, intertwined with numbers and symbols. Avoid picking common words such as months or colors to prevent dictionary attacks. For example: "University Soccer France Daisy Chocolate Water Music Tiger 5 9 $ @" could be used to create a password such as "TcmW5Fs$u9d@"

For further advice for creating strong, unique passwords, users can view CISA's guide here.

References

- https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/
- https://www.cisa.gov/sites/default/files/publications/NCSAM_CreatingPasswords_2020.pdf