Piratage de LastPass : Commentaires et conseils
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 5/12/2022 13:00:00

Commentaires et les conseils de Chris Vaughan, vice-prÃ©sident â Technical Account Management, EMEA, chez Tanium, Ã propos de la rÃ©vÃ©lation du nouvel incident de sÃ©curitÃ© qui a touchÃ© le gestionnaire de mots de passe LastPass :

" Il est inquiÃ©tant d'apprendre que LastPass a connu un autre incident de sÃ©curitÃ©, aprÃ¨s celui qui a Ã©tÃ© rendu public en aoÃ»t dernier. L'attaque concernait le code source et des informations techniques provenant d'un accÃ¨s non autorisÃ© Ã un service de stockage tiers utilisÃ© par la sociÃ©tÃ©.

La nouvelle compromission est plus grave car des informations sur les clients ont Ã©tÃ© consultÃ©es, ce qui n'Ã©tait pas le cas auparavant. L'intrus s'est servi des donnÃ©es exposÃ©es lors de l'incident prÃ©cÃ©dent pour accÃ©der Ã l'environnement informatique de LastPass.

L'entreprise affirme que les mots de passe restent chiffrÃ©s en toute sÃ©curitÃ© et qu'elle s'efforce de mieux comprendre la portÃ©e de l'incident, et d'identifier exactement les donnÃ©es qui ont Ã©tÃ© volÃ©es.

Il y a fort Ã parier que l'Ã©quipe de sÃ©curitÃ© informatique travaille sans relÃ¢che sur cette affaire et que sa visibilitÃ© sur le rÃ©seau et les appareils qui y sont connectÃ©s sera mises Ã rude Ã©preuve.Â

La plupart des organisations n'ont pas une visibilitÃ© totale, ce qui peut rendre trÃ¨s difficile, au lendemain d'une attaque, l'analyse des dommages causÃ©s et l'identification du point d'entrÃ©e de l'attaquant.

Les gestionnaires de mots de passe sont une cible difficile mais attrayante pour un acteur de la cybermenace, car ils peuvent potentiellement dÃ©bloquer un trÃ©sor d'accÃ¨s aux comptes et aux donnÃ©es sensibles des clients en un instant s'ils sont compromis.

Cependant, je pense que les avantages de l'utilisation d'une solution sÃ©curisÃ©e de gestion des mots de passe dÃ©passent souvent de loin les risques d'une compromission potentielle.

AssociÃ©e aux autres recommandations en matiÃ¨re de sÃ©curitÃ©, cette solution reste l'une des meilleures pour prÃ©venir le vol de justificatifs et les attaques associÃ©es. Il ne nous reste plus qu'Ã espÃ©rer que la confiance des clients n'a pas Ã©tÃ© trop affectÃ©e par ces rÃ©centes attaques.

Les clients de LastPass doivent continuer de rester attentifs aux communications officielles de l'Ã©diteur pour obtenir de nouvelles instructions. Si la brÃ¨che s'Ã©tend, les utilisateurs devraient alors envisager d'Ã©valuer leur position de sÃ©curitÃ©.

Cela pourrait impliquer une rotation proactive des mots de passe ou l'utilisation temporaire d'un autre gestionnaire de mots de passe.Â

J'encourage Ã©galement tout le monde Ã utiliser l'authentification multifactorielle pour leur solution de gestion des mots de passe, cette couche de sÃ©curitÃ© supplÃ©mentaire peut Ãªtre

vitale en cas de compromission. "