Les donnÃ©es de connexion, 1re cible des cybercriminels
Internet
PostÃ© par : JulieM
PubliÃ©e le : 9/5/2023 13:00:00

En 2023, le piratage de mots de passe reste lâ□□une des portes dâ□□entrÃ©e privilÃ©giÃ©es des cybercriminels et pour cause, la plupart se composent gÃ©nÃ©ralement de noms communs, dâ□□une suite de chiffres primaires, ou dâ□□informations personnelles facilement identifiables.

Par ailleurs, les utilisateurs changent trÃ¨s rarement leur mot de passe dâ□□un site internet Ã lâ□□autre, du pain bÃ©ni pour les cybercriminels qui peuvent aisÃ©ment recouper les donnÃ©es quâ□□ils possÃ¨dent sur les utilisateurs, trouver la bonne combinaison et sâ□□introduire aisÃ©ment dans la majoritÃ© des espaces ou comptes personnels des utilisateurs.

La JournÃ©e internationale du Mot de Passe qui se tient demain, jeudi 4 mai, est lâ□□occasion de rappeler la nÃ©cessitÃ© de sensibiliser les utilisateurs sur lâ□□importance de crÃ©er des combinaisons plus complexes, et uniques pour chaque plateforme, notamment lorsquâ□□il sâ□□agit de comptes hÃ©bergeant des donnÃ©es sensibles ou financiÃ¨res.

En effet, pour Matt Cooke, responsable de la stratÃ©gie cyber pour lâ□□EMEA chez Proofpoint, Â«â□□Le paysage de la menace actuel oblige Ã redoubler dâ□□efforts pour protÃ©ger les donnÃ©es des particuliers et des entreprises.â□□Â»

Dans son dernier rapport State of the Phish, Proofpoint alerte sur une hausse globale des vols dâ□□identifiants. Dâ□□aprÃ¨s lâ□□Ã©tude, 31 % des entreprises franÃ§aises dÃ©clarent avoir subi une attaque par hameÃ§onnage rÃ©sultant dâ□□un compte compromis. Pour les cybercriminels, ce mode opÃ©ratoire se rÃ©vÃ¨le en effet bien plus efficace puisquâ□□il leur permet de naviguer dans lâ□□ensemble des systÃ¨mes de lâ□□entreprise une fois sâ□□Ãªtre introduit dans un compte utilisateur.

En outre, il est important de retenir que tout mot de passe, aussi complexe soit-il, est sujet au vol. Heureusement, il existe des mÃ©thodes pour limiter le plus possible ces risques. Un premier pas vers une meilleure protection est lâ□□utilisation de lâ□□authentification multifactorielle (MFA) sur le plus de comptes possible.

Chaque utilisateur devra alors prouver Ã deux reprises son identitÃ©, sur deux supports diffÃ©rents (via une alerte SMS par exemple), avant dâ□□accÃ©der Ã son compte. Cette approche se rÃ©vÃ¨le notamment trÃ¨s efficace face aux systÃ¨mes automatisÃ©s utilisÃ©s par les cybercriminels pour deviner les mots de passe ou tester ceux prÃ©cÃ©demment volÃ©s.

Seconde bonne pratique : utiliser un gestionnaire de mot de passe pour gÃ©nÃ©rer des combinaisons alÃ©atoires, qui seront ensuite chiffrÃ©es et stockÃ©es. Ce type de plateforme offre deux avantages : il nâ□□est plus nÃ©cessaire de mÃ©moriser tous ses mots de passe parfois compliquÃ©s, et ils sont accessibles par lâ□□utilisateur en toute sÃ©curitÃ© sur lâ□□ensemble de ses appareils. GÃ©nÃ©ralement, le gestionnaire est protÃ©gÃ© par une phrase secrÃ¨te, Ã lâ□□instar des mots de passe, celle-ci ne doit pas faire rÃ©fÃ©rence Ã des mots courants ou Ã des informations personnelles.

Â«â□□Les acteurs de la menace sont aujourdâ□□hui suffisamment armÃ©s et entraÃ®nÃ©s pour contourner les technologies mises en place et voler les identifiants de connexion. Nous savons Ã©galement que 95 % des problÃ¨mes de cybersÃ©curitÃ© sont liÃ©s Ã lâ□□humain. Il est donc

primordial que chaque utilisateur ait la capacitÃ© dâ□□identifier les tentatives dâ□□hameÃ§onnage de donnÃ©es de connexion pour ne pas devenir la victime de ce type dâ□□attaqueâ□□Â», explique Matt Cooke.Â