bgr.com /tech/10-billion-stolen-passwords-shared-online-in-record-breaking-leak/

# 10 milliards de mots de passe volés partagés en ligne dans une fuite record

Jacob Siegal ⁝

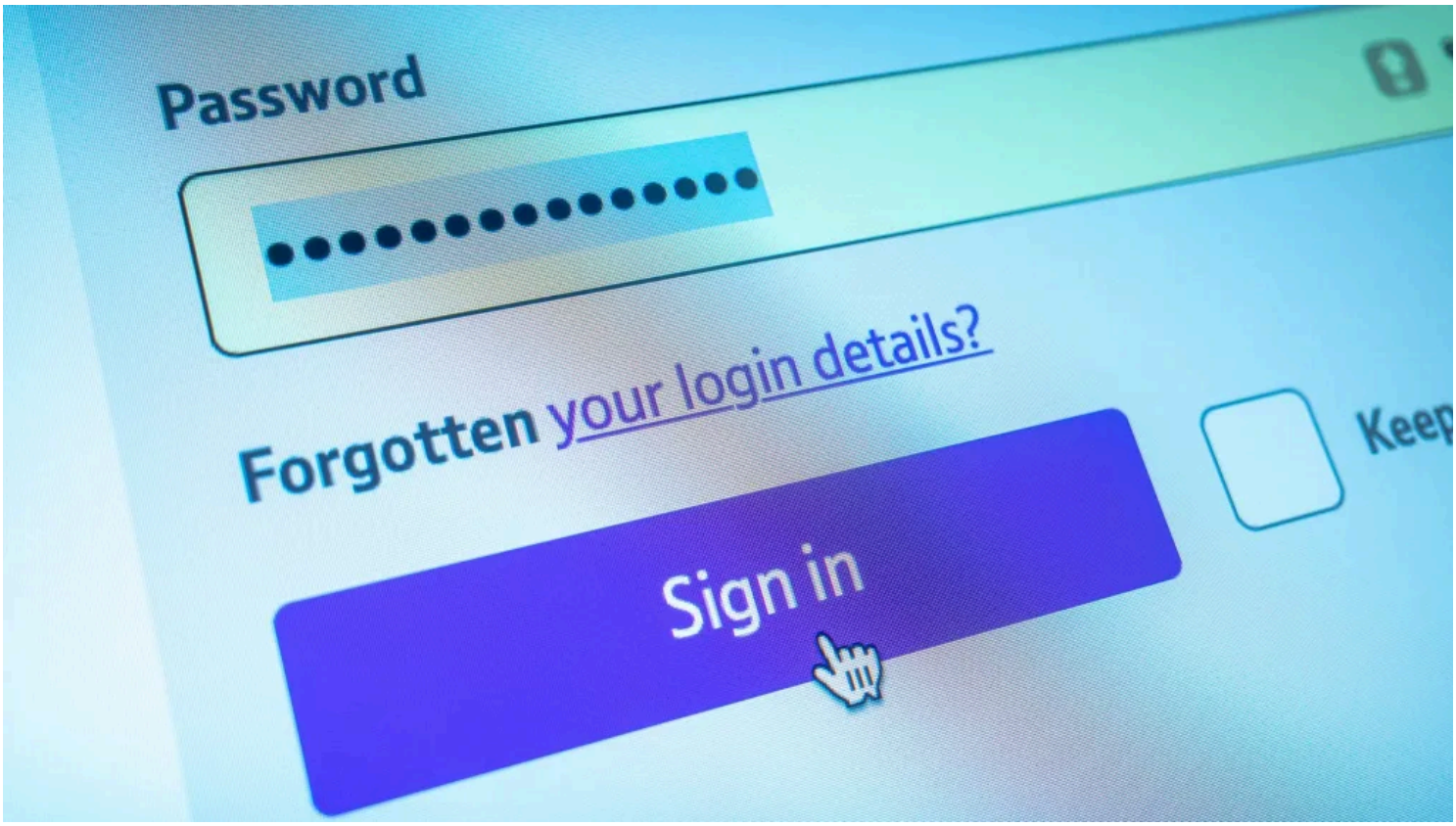
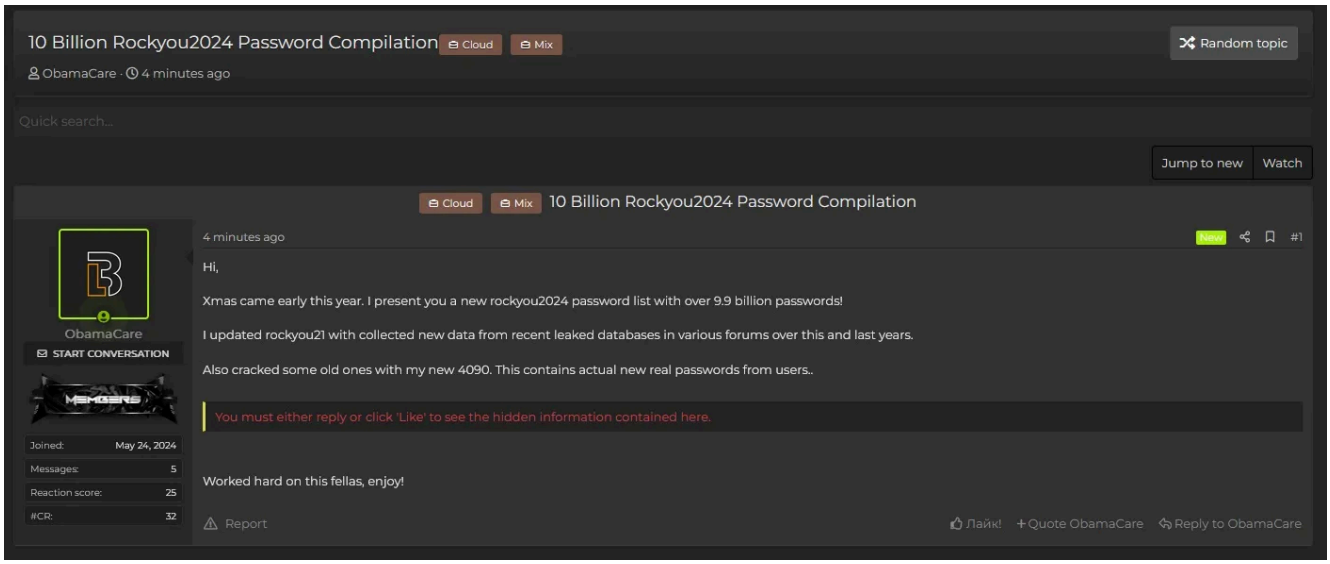



Image : Sean Gladwell / Getty Images

Des mois après la découverte de la soi-disant « mère de toutes les violations » en janvier, une autre fuite record a été publiée en ligne.
Selon l'équipe de recherche de Cybernews, une compilation de mots de passe contenant près de 10 milliards de mots de passe uniques en clair (9 948 575 739 pour être exact) a été publiée sur un forum de pirates le 4 juillet.

Le fichier de compilation de mots de passe de l'utilisateur ObamaCare s'intitule rockyou2024.txt - une référence à RockYou2021, qui était auparavant la plus grande compilation de mots de passe jamais enregistrée.
RockYou2021 était un fichier texte de 100 Go contenant 8,4 milliards de mots de passe en clair.

Cybernews affirme que RockYou2024 combine la fuite précédente avec une collection de plus de 1,5 milliard de nouveaux mots de passe collectés entre 2021 et 2024.



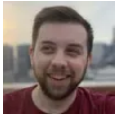

RockYou2024 contient près de 10 milliards de mots de passe.
Source de l'image : Cybernews

L'équipe de recherche de Cybernews prévient que les acteurs de la menace utiliseront tous les mots de passe divulgués pour le bourrage d'identifiants, qui est une cyberattaque qui utilise les identifiants de compte volés pour accéder aux comptes des utilisateurs. Combiné à d'anciennes bases de données divulguées, les chercheurs pensent que « RockYou2024 peut contribuer à une cascade de violations de données, de fraudes financières et d'usurpations d'identité ».

Il n'y a évidemment rien que vous puissiez faire pour inverser cette fuite, mais Cybernews a partagé quelques mesures que vous pouvez prendre pour vous assurer que vos comptes sont à l'abri des acteurs malveillants :

- Réinitialisez immédiatement les mots de passe de tous les comptes associés aux mots de passe divulgués.
  Il est fortement recommandé de sélectionner des mots de passe forts et uniques qui ne sont pas réutilisés sur plusieurs plateformes
- Activez l'authentification multifacteur (MFA) dans la mesure du possible.
  Cela renforce la sécurité en exigeant une vérification supplémentaire au-delà d'un mot de passe
- Utilisez un logiciel de gestion de mots de passe pour générer et stocker en toute sécurité des mots de passe complexes.
  Les gestionnaires de mots de passe atténuent le risque de réutilisation des mots de passe sur différents comptes

Il vaut toujours la peine de vérifier HaveIBeenPwned.com tous les mois environ pour voir si vos mots de passe doivent être mis à jour en raison de la compromission de vos comptes en ligne.



Jacob Siegal est rédacteur en chef adjoint chez BGR, après avoir rejoint l’équipe des nouvelles en 2013.
Il a plus d’une décennie d’expérience professionnelle en rédaction et en édition, et aide à diriger le lancement de nos produits technologiques et de divertissement et la couverture des sorties de films.

*Recherche et mise en page par:*
*Michel Cloutier*
*CIVBDL*
*20240707*
*"C'est ensemble qu'on avance"*