cybernews.com /security/billions-passwords-credentials-leaked-mother-of-all-breaches/

# La mère de toutes les violations révèle 26 milliards d'enregistrements et ce que nous savons jusqu'à présent Cybernews

Vilius Petkauskas Rédacteur en chef adjoint :


***La fuite supermassive contient des données provenant de nombreuses violations précédentes, comprenant un nombre incroyable de 12 téraoctets d'informations, réparties sur un nombre ahurissant de 26 milliards d'enregistrements.***

**La fuite, qui contient les données des utilisateurs de *LinkedIn, Twitter, Weibo, Tencent et d'autres plateformes , est presque certainement la plus importante jamais découverte.***

Il y a des fuites de données, et puis il y a ça.

Une mère supermassive de toutes les violations (MOAB en abrégé) comprend des enregistrements provenant de milliers de fuites, de violations et de bases de données vendues à titre privé méticuleusement compilées et réindexées.

La liste complète et consultable est incluse à la fin de cet article.

Bob Dyachenko, chercheur en cybersécurité et propriétaire de SecurityDiscovery.com, en collaboration avec l'équipe Cybernews, a découvert des milliards et des milliards d'enregistrements exposés sur une instance ouverte dont le propriétaire ne sera probablement jamais identifié.

- Vous pouvez vérifier si vos données ont été exposées lors de violations de données historiques à l'aide du vérificateur de fuite de données Cybernews .
  Notre équipe travaille dur pour mettre à jour l'outil et vous fournir les moyens de vérifier si vos données ont été exposées dans le MOAB.

Selon l'équipe, même si l'ensemble de données divulgué contient principalement des informations provenant de violations de données passées, il contient presque certainement de nouvelles données, qui n'avaient pas été publiées auparavant.
Par exemple, le vérificateur de fuites de données de Cybernews, qui s'appuie sur les données de toutes les fuites de données majeures, contient des informations provenant de plus de 2 500 violations de données avec 15 milliards d'enregistrements.

Le MOAB contient 26 milliards d'enregistrements répartis dans 3 800 dossiers, chaque dossier correspondant à une violation de données distincte.
Bien que cela ne signifie pas que la différence entre les deux se traduit automatiquement par des données inédites, des milliards de nouveaux enregistrements indiquent une très forte probabilité, le MOAB contenant des informations jamais vues auparavant.

Les chercheurs pensent que le propriétaire du MOAB a tout intérêt à stocker de grandes quantités de données et pourrait donc être un acteur malveillant, un courtier en données ou un service fonctionnant avec de grandes quantités de données.

« L'ensemble de données est extrêmement dangereux, car les acteurs malveillants pourraient exploiter les données agrégées pour un large éventail d'attaques, notamment le vol d'identité, les programmes de phishing sophistiqués, les cyberattaques ciblées et l'accès non autorisé à des comptes personnels et sensibles », ont déclaré les chercheurs.

Le MOAB supermassif ne semble pas être constitué uniquement de données récemment volées et constitue très probablement la plus grande compilation de violations multiples (COMB).

Même si l'équipe a identifié plus de 26 milliards d'enregistrements, les doublons sont également très probables. Cependant, les données divulguées contiennent bien plus d'informations que de simples informations d'identification : la plupart des données exposées sont sensibles et, par conséquent, précieuses pour les acteurs malveillants.

## BRANDS WITH 100M+ LEAKED RECORDS

| BRAND NAME | RECORDS LEAKED |
|---|---|
| Tencent | 1.5B |
| Weibo | 504M |
| MySpace | 360M |
| Twitter | 281M |
| Wattpad | 271M |
| NetEase | 261M |
| Deezer | 258M |
| LinkedIn | 251M |
| AdultFriendFinder | 220M |
| Zynga | 217M |
| Luxottica | 206M |
| Evite | 179M |
| Zing | 164M |
| Adobe | 153M |
| MyFitnessPal | 151M |
| Canva | 143M |
| JD.com | 142M |
| Badoo | 127M |
| VK | 101M |
| Youku | 100M |

cybernews®

Un rapide parcours dans l'arborescence des données révèle un nombre étonnamment élevé d'enregistrements compilés à partir de violations précédentes.

Le plus grand nombre d'enregistrements, 1,4 milliard, provient de Tencent QQ, une application chinoise de messagerie instantanée.

Cependant, il existerait des centaines de millions d'enregistrements provenant de Weibo (504 millions), MySpace (360 millions), Twitter (281 millions), Deezer (258 millions), Linkedin (251 millions), AdultFriendFinder (220 millions), Adobe (153 millions), Canva (143 millions). , VK (101 M), Daily Motion (86 M), Dropbox (69 M), Telegram (41 M) et de nombreuses autres sociétés et organisations.

La fuite comprend également des dossiers de diverses organisations gouvernementales aux États-Unis, au Brésil, en Allemagne, aux Philippines, en Turquie et dans d'autres pays.

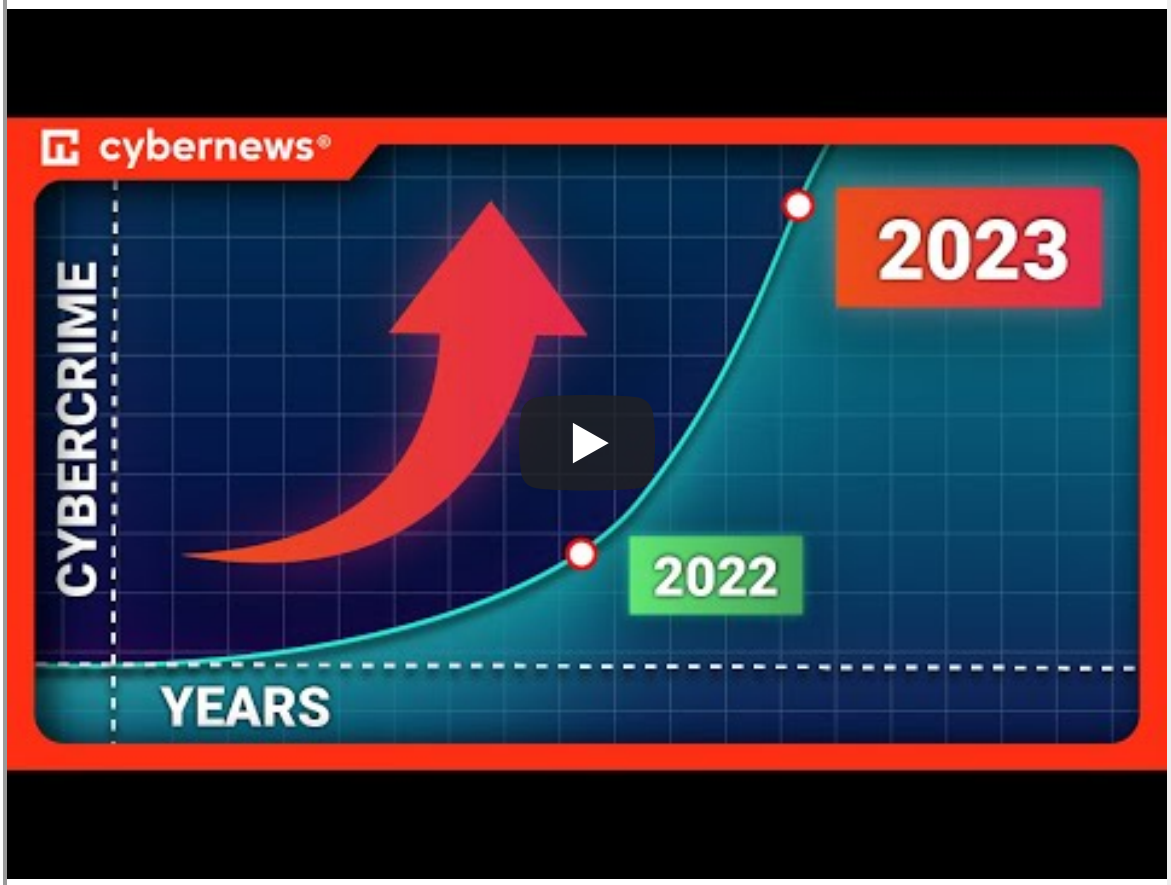
Selon l'équipe, l'impact du MOAB supermassif sur les consommateurs pourrait être sans précédent.
Étant donné que de nombreuses personnes réutilisent leurs noms d'utilisateur et leurs mots de passe, les acteurs malveillants pourraient se lancer dans un tsunami d'attaques de type credential stuffing.

« Si les utilisateurs utilisent les mêmes mots de passe pour leur compte Netflix que pour leur compte Gmail, les attaquants peuvent s'en servir pour pivoter vers d'autres comptes plus sensibles.
En dehors de cela, les utilisateurs dont les données ont été incluses dans le MOAB supermassif peuvent devenir victimes d'attaques de spear phishing ou recevoir des niveaux élevés de spam », ont indiqué les chercheurs.

L'ampleur de la fuite est d'une ampleur encore inédite.
Par exemple, en 2021, Cybernews a rapporté un COMB contenant 3,2 milliards d'enregistrements , soit seulement 12 % du MOAB supermassif de 2024.

Nous mettons à jour le vérificateur de fuite de données de Cybernews pour inclure les informations du MOAB, ce qui permettra aux utilisateurs de voir si leurs données ont été incluses dans la plus grande fuite de données connue.
En attendant, il est fortement conseillé aux utilisateurs de rester vigilants et de veiller à leur cyber-hygiène.

Tout le monde doit utiliser des mots de passe forts et difficiles à deviner, activer l'authentification multifacteur sur tous les comptes importants, garder un œil sur les tentatives de phishing et de spear phishing, vérifier les doublons de mots de passe et configurer immédiatement une nouvelle protection pour les comptes partageant les mêmes mots de passe.




---

## En savoir plus sur Cybernews :

Big Tech mène la transition au-delà des mots de passe

Aperçu du paysage des ransomwares 2023

Métro revendiqué par le rançongiciel LockBit

Mozilla accuse Apple, Google et Microsoft de sales tours qui nuisent à Firefox

Escroqueries aux achats sur TikTok et comment les éviter

**Abonnez-vous** à notre newsletter

*Recherche et mise en page par:*
*Michel Cloutier*
*CIVBDL*

*2024125*

*"C'est ensemble qu'on avance"*