SPECOPS
AN OUTPOST24 COMPANY

Rapport sur les mots de passe faibles

2023

1. Résumé 3
2. Arguments en faveur de la protection par mot de passe 4
2.1 Password Length and Complexity Alone Is Not the Answer 4
3. Les mots de passe faibles et compromis en action : Comment ils sont utilisés dans les cyberattaques 5
3.1 Force brute et construction de mots de passe 5
3.2 Exemple concret : Nvidia 6
4. Mots de passe compromis : Thèmes et modèles 7
4.1 Le football est une langue universelle (mot de passe) 7
5. Passez à l'action : Protégez votre organisation avec Specops 8

Les mots de passe sont faciles à attaquer car beaucoup de gens utilisent des mots de passe faciles à deviner. Ces mots de passe sont faciles à deviner notamment parce que les gens réutilisent les mots de passe et ont recours à des modèles et des thèmes communs. Ces mots de passe se retrouvent ensuite sur des listes de mots de passe compromis et peuvent être attaqués par force brute ou par pulvérisation de mots de passe. Comprendre les modèles de mots de passe courants et les comportements des utilisateurs est la première étape pour sécuriser les mots de passe et les données cruciales de l'entreprise qu'ils protègent.

À PROPOS DE SPECOPS

Specops Software, une entité du Groupe Outpost24, est le principal fournisseur de solutions de gestion des mots de passe et d'authentification. Specops protège les données de votre entreprise en bloquant les mots de passe faibles et en sécurisant l'authentification des utilisateurs. Chaque jour, des milliers d'organisations utilisent Specops Software pour protéger leurs données professionnelles. Pour plus d'informations, veuillez visiter specopssoft.com/fr.

1. Résumé

Les mauvaises pratiques en matière de mots de passe mettent les entreprises en danger. Les violations de données continuent de menacer tous les types d'organisations à travers le monde, soulignant l'importance d'une plus grande sécurité des mots de passe, comme moyen de protéger nos données d'entreprise, ainsi que notre écosystème numérique.

Le rapport de cette année sur les mots de passe faibles montre pourquoi les mots de passe restent le maillon faible du réseau d'une entreprise et comment l'application d'une politique de mots de passe plus stricte pourrait constituer votre défense la plus efficace.

Les recherches présentées dans ce rapport ont été compilées à l'aide de plusieurs méthodes, parmi lesquelles :

- • Notre analyse de 800 millions de mots de passe piratés, un sous-ensemble de plus de 3 milliards de mots de passe uniques compromis dans la liste Specops Breached Password Protection.
- Notre analyse des mots de passe trouvés dans des attaques en direct sur le réseau de « honeypot » de notre équipe, une autre source de mots de passe compromis bloqués par la liste Specops Breached Password Protection.

Quelques faits marquants du rapport de cette année sont les suivants :

- 83 % des mots de passe compromis sont conformes aux exigences de longueur et de complexité des normes réglementaires en matière de mots de passe.
- 88 % des mots de passe utilisés pour attaquer les ports RDP lors d'attaques réelles comportent 12 caractères ou moins.
- Le terme de base le plus courant que l'on trouve dans les mots de passe utilisés pour attaquer des réseaux sur plusieurs ports reste « password ».

Les données contenues dans ce rapport devraient sensibiliser à ce problème trop courant. L'étape suivante consiste à agir, ce qui signifie bloquer les mots de passe faibles et compromis, appliquer des exigences de longueur de mot de passe et auditer l'environnement de l'entreprise pour mettre en évidence les vulnérabilités liées aux mots de passe. C'est pourquoi Specops Password Auditor a été développé pour aider les organisations à identifier de multiples vulnérabilités, exportables sous forme de rapport, le tout en quelques minutes.

2. Arguments en faveur de la protection par mot de passe

De mauvaises pratiques ou politiques en matière de mots de passe peuvent rendre votre organisation vulnérable aux cyber-attaques. Malheureusement, la plupart des gens ne respectent pas les meilleures pratiques en matière de mots de passe. Selon un récent rapport sur les gestionnaires de mots de passe, 41 % des Américains se fient uniquement à leur mémoire pour retrouver leurs mots de passe numériques, ce qui suggère l'utilisation de mots de passe simples et répétables pour qu'ils soient plus faciles à retenir. En outre, parmi ceux qui choisissent d'utiliser un gestionnaire de mots de passe en ligne pour stocker leurs informations, près de la moitié stockent à la fois leurs mots de passe personnels et professionnels.

Malgré la formation des utilisateurs finaux, la réutilisation des mots de passe et d'autres pratiques à risque sont trop courantes, tant pour un usage personnel que professionnel. Pour protéger les données de l'entreprise, des mesures d'application supplémentaires sont nécessaires. Pour la plupart des entreprises, cela commence par la protection d'Active Directory, la solution d'authentification universelle pour les réseaux de domaines Windows. Un logiciel de sécurité des mots de passe tiers peut renforcer les comptes Active Directory. Une politique de mot de passe sécurisée, de préférence capable de bloquer l'utilisation de mots de passe compromis, est essentielle.

2.1 La longueur et la complexité des mots de passe ne sont pas la solution à elles seules

Plusieurs règles de conformité fixent les normes en matière de cybersécurité, y compris les politiques de mot de passe des organisations. Traditionnellement, ces réglementations ont principalement approuvé les exigences de longueur et de complexité dans la conception de la politique de mot de passe. Toutefois, compte tenu de la sophistication croissante des attaques par mot de passe, les exigences actuelles incluent désormais la vérification des informations d'identification par rapport à une liste de mots de passe violés.

L'équipe de recherche de Specops Software a analysé plus de 800 millions de mots de passe compromis et les a testés par rapport à cinq normes réglementaires différentes pour voir s'ils répondaient aux exigences fixées par chacune de ces normes. Notre analyse a révélé que 83 % des mots de passe compromis répondaient aux exigences de complexité et de longueur des mots de passe des normes de conformité.

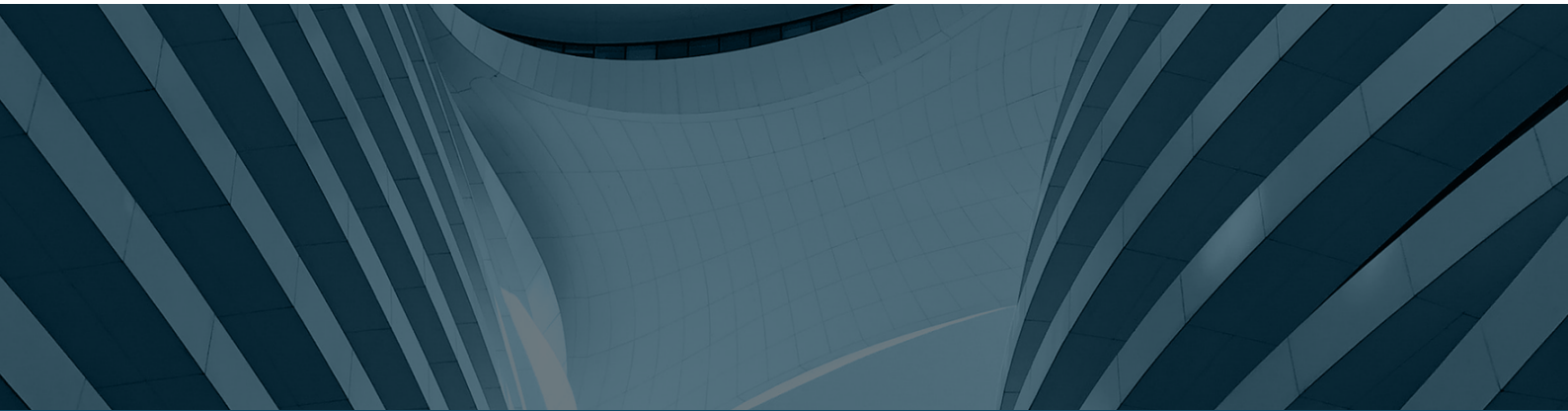
Les normes réglementaires que nous avons examinées sont les suivantes :

- ANSSI
- CNIL
- NIST
- HITRUST pour HIPAA
- PCI
- ICO pour le GDPR
- Cyber Essentials pour le NCSC

Que vous suiviez une norme réglementaire ou non, ces données nous indiquent qu'une vérification des mots de passe compromis est essentielle pour toutes les organisations.

Actions recommandées pour éviter l'utilisation de mots de passe compromis

- ICO/GDPR : Empêcher l'utilisation de mots de passe communs et faibles.
- Comparez les mots de passe à une liste des mots de passe les plus couramment utilisés, des mots de passe ayant fait l'objet d'une fuite et des mots de passe devinables liés à l'organisation. Mettez régulièrement à jour la liste des mots de passe divulgués et expliquez aux utilisateurs pourquoi leurs mots de passe ont été rejetés.



3. Les mots de passe faibles et compromis en action : Comment ils sont utilisés dans les cyberattaques

Les cybercriminels accèdent souvent aux données sensibles et aux réseaux des organisations par le biais d'attaques par force brute.

Ces attaques consistent à utiliser une liste de mots de passe courants, probables et même frauduleux pour les comparer systématiquement au courrier électronique d'un utilisateur afin d'obtenir l'accès à un compte donné.

Cette section explique comment les mots de passe peuvent constituer un point d'entrée dans le réseau de votre organisation et ce que vous pouvez faire pour vous protéger.

3.1 Force brute et construction de mots de passe

En octobre 2022, notre équipe de recherche a examiné les mots de passe utilisés pour attaquer les ports RDP lors d'attaques réelles et a analysé un sous-ensemble de plus de 4,6 millions de mots de passe collectés sur une période de plusieurs semaines. Nous avons identifié des modèles dans les attaques récentes et découvert que plus de 88 % des mots de passe utilisés dans les attaques étaient composés de 12 caractères ou moins. La longueur de mot de passe la plus courante dans ces données d'attaques était de 8 caractères, soit près de 24 %.

L'utilisation de caractères spéciaux est un autre élément clé de la construction des mots de passe. Les mots de passe ne contenant que des lettres minuscules étaient la combinaison de caractères la plus courante, représentant 18,82 % de l'ensemble.

Terme de base le plus couramment
utilisé pour attaquer les réseaux à travers plusieurs ports en octobre 2022

1. password
2. admin
3. welcome
4. p@ssw0rd
5. qaz2wsx
6. homelesspa
7. p@ssword
8. qwertyuiop
9. q2w3e4r5t
10. q2w3e4r

SPECOPS AN OUTPOST24 COMPANY

Il s'agit de termes courants que les gens utilisent encore et encore sur différents comptes, tant professionnels que personnels. Les pirates réussissent encore à attaquer les ports avec des listes de mots faibles, courants et alimentés par le leetspeak. Même si des attaques plus sophistiquées sont dans le collimateur d'une organisation, il est tout aussi important de se protéger contre les tactiques les plus basiques qui ciblent le maillon le plus faible.

Le plus intéressant dans cet ensemble de données pourrait être l'inclusion de "homelesspa" - un terme de base de mot de passe trouvé dans la fuite MySpace de 2016, nous donnant un aperçu des listes utilisées par les attaquants pour attaquer les réseaux. Ce terme figure également dans la liste NCSC Top 100k publiée en 2019.

Ce terme de base indique que même si une liste de mots ou une brèche est "ancienne", il vaut toujours la peine de s'en protéger, car les attaquants les utilisent encore pour compiler leurs listes d'attaques.

Les organisations qui cherchent à empêcher l'utilisation de tels mots de passe doivent appliquer des règles de construction des mots de passe, telles que l'utilisation de phrases de passe et le vieillissement des mots de passe en fonction de leur longueur, afin d'encourager les mots de passe longs et mémorisables. Ces exigences, associées à un dictionnaire personnalisé ou à un filtrage des mots de passe compromis, constituent la meilleure défense contre les mots de passe susceptibles d'aider les acteurs de la menace à accéder au réseau de votre organisation.

3.2 Exemple concret : Nvidia

En février 2022, le fabricant de GPU Nvidia a été victime d'une violation massive de données menée par le groupe de ransomware LAPSUS$.

L'auteur de la menace s'est introduit dans leur réseau pour voler les mots de passe des employés, ainsi que des informations exclusives sur l'entreprise, et a procédé à la fuite des données en ligne pour obtenir une rançon.

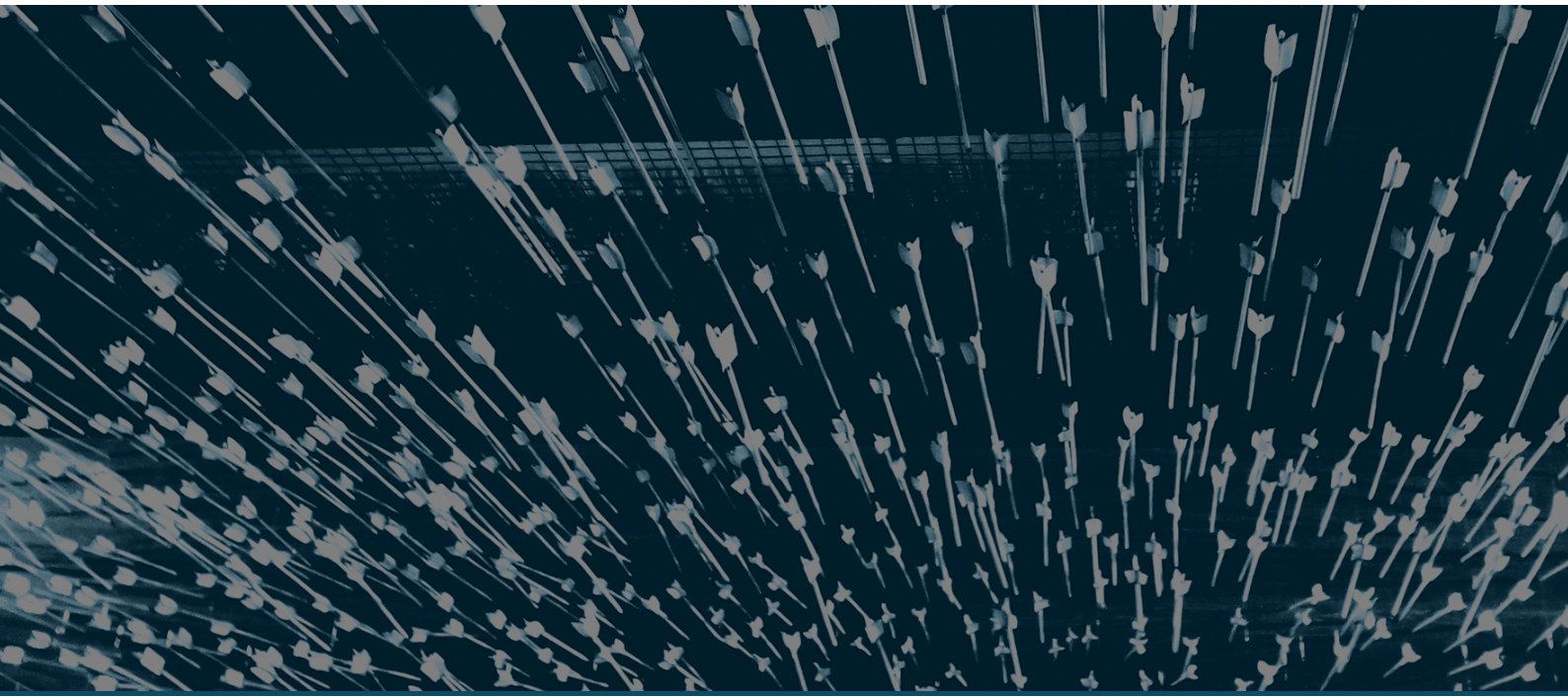
Au cours de la violation, des milliers de mots de passe d'employés ont été divulgués. Specops Software a obtenu 30 000 de ces mots de passe et les a ajoutés à sa base de données de mots de passe compromis. Nvidia a ensuite indiqué que tous les employés devaient modifier leurs mots de passe. Maintenant que ces mots de passe ne sont plus utilisés, nous pouvons examiner quelques exemples pour identifier les facteurs qui ont conduit à leur compromission.

Les 10 mots de base les plus utilisés dans les fuites de mots de passe Nvidia

1. nvidia
2. nvidia3d
3. mellanox
4. ready2wrk
5. welcome
6. password
7. mynvidia3d
8. nvda
9. qwerty
10. september

Le fait de trouver "nvidia" dans cette liste indique que l'organisation n'utilisait pas de dictionnaire personnalisé dans ses protections de mots de passe. Une liste de dictionnaires personnalisés est établie pour rejeter les mots de passe courants et prévisibles au cours du processus de création du mot de passe. Il peut s'agir de mots de passe relatifs à votre organisation, y compris le nom, les sites, les services, tout acronyme pertinent, et même les mois de l'année, comme dans l'exemple de "septembre" ci-dessus.

La cyberattaque dont a été victime la plus grande société américaine de puces électroniques a, à juste titre, suscité des inquiétudes quant à la sécurité des données. Mais ce n'est pas une surprise si l'on considère que les entreprises commerciales sont les plus touchées par les attaques de ransomware, selon le rapport sur les ransomwares 2023 d'Outpost24. Ces données suggèrent que les acteurs de la menace ciblent principalement les organisations qui ont une plus grande capacité à payer une rançon.



4. Mots de passe compromis : Thèmes et modèles

Notre analyse des plus de 800 millions de mots de passe compromis que nous avons recueillis fait apparaître plusieurs thèmes et schémas.

En matière de création de mots de passe, il existe une forte tendance à s'inspirer d'événements mondiaux ou culturels. De nombreuses personnes s'inspirent de leur environnement pour créer leurs mots de passe et utilisent leurs centres d'intérêt ou les tendances culturelles pour influencer les phrases qu'elles utilisent pour leurs mots de passe.

Les pirates informatiques sont conscients de cette tendance et en profitent pour exploiter des termes ou des phrases connus de tous afin de cibler des victimes peu méfiantes.

4.1 Le football est une langue universelle (mot de passe)

On dit souvent que le football est un langage universel. Nos recherches ont révélé que c'était également le cas pour les mots de passe.

Au moment de la Coupe du monde de la FIFA 2022 au Qatar, notre équipe de recherche a découvert de nombreux termes liés à la Coupe du monde dans la base de données de mots de passe compromise, dont beaucoup sont fréquemment mentionnés. Le terme "Soccer" arrive en tête de la liste des termes associés avec plus de 140 000 inclusions, le terme "Football" arrivant en deuxième position. Le stade international anglais de Wembley figure également dans le top 10, apparaissant plus de 1 600 fois dans les mots de passe.

En ce qui concerne les joueurs, actuels et anciens, certains se distinguent dans les mentions. Grzegorz Lato, ancien joueur de la génération dorée polonaise, arrive en tête de liste avec plus de 174 000 mentions. Pelé, sans doute le plus grand joueur de tous les temps, apparaît lui aussi fréquemment, mais juste à côté du top 10, avec plus de 70 000 mentions. Les footballeurs actuels Messi et Ronaldo figurent également sur la liste des mentions, ce qui n'est pas surprenant compte tenu de l'importance des bases de fans de chacun de ces joueurs.

Classement des légendes de la Coupe du monde
(en mots de passe)

1.	Lato	**11.**	Pele
2.	Carlos	**12.**	Santos
3.	Kane	**13.**	Moore
4.	Didi	**14.**	Messi
5.	Villa	**15.**	Vava
6.	Henry	**16.**	Walter
7.	Hagi	**17.**	Kopa
8.	Milla	**18.**	Ronaldo
9.	Xavi	**19.**	Monti
10.	Rossi	**20.**	Zico

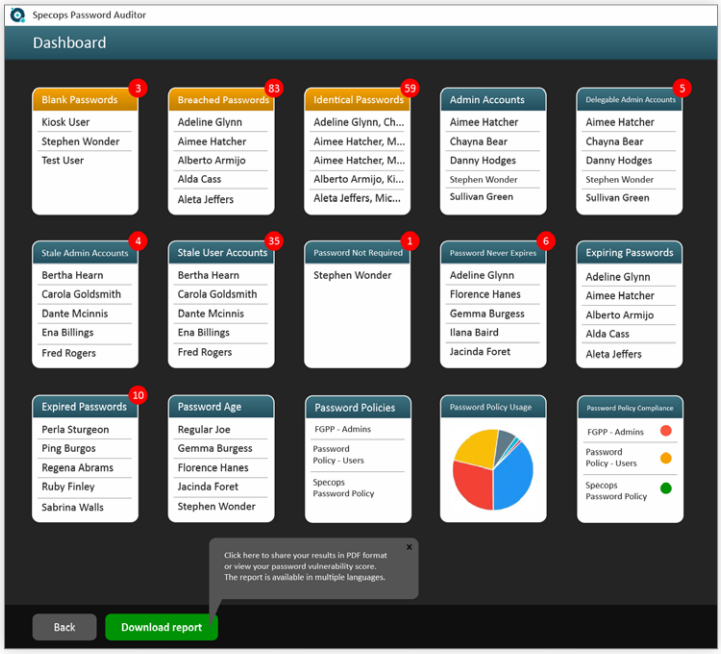
SPECOPS AN OUTPOST24 COMPANY

Bien qu'il ne soit pas garanti que les termes les plus courants contenus dans les mots de passe soient toujours attribués à un joueur, il est courant que les utilisateurs choisissent des termes et des noms bien connus, et il est très probable qu'il y ait une intention lorsque des noms de famille moins courants apparaissent.

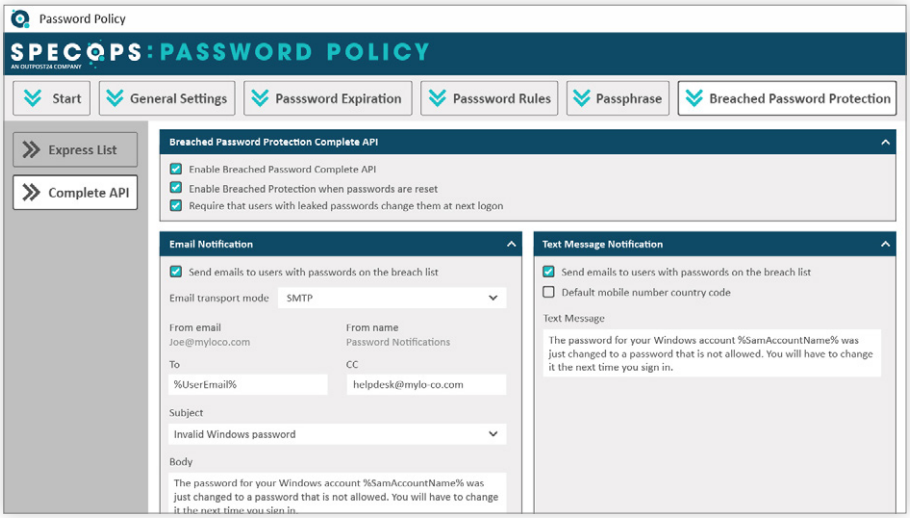
5. Passez à l'action : Protégez votre organisation avec Specops

Qu'il s'agisse de ransomware, de devinettes de mots de passe ou d'attaques par force brute, tant que les acteurs de la menace continueront à faire évoluer leurs tactiques, les organisations devront être proactives en matière de protection des mots de passe afin de défendre la sécurité globale de leur réseau.

Testez votre résilience contre les attaques basées sur les informations d'identification avec l'outil gratuit Specops Password Auditor. Cet outil en lecture seule analyse votre Active Directory à la recherche de vulnérabilités liées aux mots de passe, y compris les comptes qui utilisent des mots de passe compromis.



Pour une meilleure sécurité des mots de passe, Specops Password Policy encourage les mots de passe forts et uniques, qui sont plus difficiles à prédire et à cracker. Avec la fonction de protection contre les mots de passe piratés, vous pouvez même bloquer plus de 3 milliards de mots de passe uniques compromis collectés par Specops Software.



Demandez une démo ou un essai gratuit et découvrez comment nous pouvons vous aider à sécuriser votre maillon le plus faible.