SPECOPS
AN OUTPOST24 COMPANY

Rapport sur les mots de passe compromis Specops 2025

Analyse des identifiants volés par des logiciels malveillants sur une année

Ce que vous trouverez dans ce rapport

Points clés du rapport

Les données de ce rapport proviennent de KrakenLabs, l'équipe de Threat Intelligence d'Outpost24 (la société mère de Specops Software). Au total, 1 089 342 532 mots de passe volés, capturés sur une période de 12 mois, ont été analysés pour ce rapport. Les données sont exactes à la date de décembre 2024 ; cependant, nous prévoyons que les tendances et les schémas globaux resteront cohérents. Le rapport fait également référence à d'autres recherches individuelles menées par les équipes de KrakenLabs tout au long de l'année 2024.

Plus d'un milliard d'identifiants volés par des logiciels malveillants analysés sur une période de 12 mois

230 millions de mots de passe volés répondent aux exigences de complexité standard

- **Les trois exemples les plus courants**
  - Pass@123
  - P@ssw0rd
  - Aa@123456

Les cinq mots de passe volés les plus courants :

- 123456
- admin
- 12345678
- password
- Password

Les termes de base les plus courants trouvés dans les mots de passe volés :

- Cinq caractères : admin
- Six caractères : qwerty
- Sept caractères : welcome
- Huit caractères : password

Les trois longueurs de mots de passe volés les plus courantes

- Huit caractères (189 millions)
- Dix caractères (160 millions)
- Neuf caractères (153 millions)

Les trois logiciels malveillants les plus utilisés pour voler des credentials?

- Redline
- Vidar
- Raccoon Stealer

Résumé exécutif

Le rapport 2024 sur les violations de données de Verizon a révélé que, au cours des 10 dernières années, l'utilisation d'identifiants volés a été impliquée dans près d'un tiers (31 %) de toutes les violations de données. Cette prévalence du vol d'identifiants a eu des répercussions significatives pour les individus comme pour les organisations. Les identifiants volés peuvent permettre un accès non autorisé à des comptes personnels, des réseaux d'entreprise et des systèmes financiers, entraînant des violations de données, des pertes financières et des dommages à la réputation.

Au cours de l'année écoulée, notre équipe de Threat Intelligence a méticuleusement recueilli et analysé des données sur un problème critique et croissant en cybersécurité : le vol d'identifiants via des logiciels malveillants. Ce rapport propose une analyse unique de plus d'un milliard d'identifiants volés par des logiciels malveillants, offrant aux organisations une compréhension approfondie des mots de passe choisis (et réutilisés) par les utilisateurs finaux, des méthodes utilisées dans ces attaques et des mesures pouvant être prises pour atténuer les risques.

Les données recueillies offrent une vue d'ensemble complète du paysage actuel du vol d'identifiants, mettant en lumière la sophistication et la persistance de ces menaces. L'analyse des tendances et des schémas liés aux mots de passe volés permet de mieux comprendre les pratiques des utilisateurs finaux réels et d'identifier les domaines où les politiques de mots de passe des organisations pourraient nécessiter des améliorations. Nous examinerons également les méthodes, les tendances et les impacts des logiciels de vol d'informations (infostealers) et d'autres types de logiciels malveillants spécifiquement conçus pour voler des informations sensibles, telles que les noms d'utilisateur, les mots de passe et d'autres données d'authentification.

En examinant des données réelles sur les mots de passe et en analysant les techniques utilisées par les attaquants, nous espérons vous fournir des informations exploitables et des recommandations pour renforcer vos protocoles de sécurité et vous protéger contre la menace des identifiants volés par des logiciels malveillants.

Mots de passe faibles : Tendances et modèles

L'utilisation d'outils de Threat Intelligence pour analyser les mots de passe volés nous donne l'opportunité d'examiner les mots de passe que les utilisateurs finaux créent réellement – et que les cybercriminels volent réellement. Une enquête menée par LastPass a révélé que 91 % des utilisateurs finaux déclarent comprendre les risques liés à l'utilisation des mêmes mots de passe sur plusieurs comptes, mais 59 % le font malgré tout.

Cela signifie qu'il existe une réelle possibilité que ces identifiants volés soient également utilisés comme mots de passe Active Directory au sein des organisations du monde entier. Ces tendances et schémas mettent en évidence à quel point de nombreux mots de passe restent encore faibles et indiquent où votre propre politique de mots de passe pourrait nécessiter un renforcement.

Mots de passe et termes de base les plus courants

Comme vous pouvez le voir ci-dessous, des mots de passe tels que 123456, admin et password apparaissent encore avec une régularité déprimante. Le tableau ci-dessous répertorie le nombre de correspondances exactes pour les cinq mots de passe les plus fréquemment volés. Cela illustre l'importance pour les organisations d'empêcher les utilisateurs finaux de créer des mots de passe Active Directory faibles – car, si l'occasion leur est donnée, de nombreux utilisateurs finaux choisiront encore de le faire.

Les cinq mots de passe volés les plus courants	Nombre d'occurrences exactes
123456	3.7 million
admin	1.9 million
12345678	1.5 million
password	558,000
Password	474,000

Parmi le milliard de mots de passe analysés, certains termes de base courants sont apparus des millions de fois. Malgré les incitations à créer des mots de passe uniques, les données ci-dessous montrent que les utilisateurs finaux continuent d'utiliser des termes de base faibles et faciles à deviner pour construire leurs mots de passe. Des mots comme guest et student suggèrent que de nombreux utilisateurs conservent ou réutilisent des mots de passe temporaires, tels que ceux attribués pour des formations ou un premier jour d'utilisation. On observe également une utilisation fréquente de motifs de clavier comme qwerty et azerty. Enfin, le mot Pakistan a été couramment utilisé, notamment sur les sites gouvernementaux pakistanais, ainsi que sur des sites plus généraux comme Facebook, Amazon et Netflix.

Termes de base les plus courants de cinq caractères
admin
guest
hello

Termes de base les plus courants de six caractères
qwerty
secret
azerty

Termes de base les plus courants de sept caractères
welcome
zxcvbnm
student

Termes de base les plus courants de huit caractères
password
adminisp
pakistan

Longueurs de mots de passe les plus courantes

Le tableau ci-dessous présente les différentes longueurs des mots de passe volés. La longueur de huit caractères est la plus courante, ce qui reflète probablement l'exigence fréquente pour les utilisateurs finaux de créer un mot de passe d'au moins huit caractères. Nous avons également inclus les trois mots de passe les plus fréquemment compromis pour chaque longueur de mot de passe. Dans ces données, on peut observer comment les utilisateurs finaux utilisent souvent les termes de base simples mentionnés dans la section précédente, en ajoutant simplement des chiffres consécutifs à la fin.

Longueur des mots de passe	Nombre de fois trouvé	Top trois des mots de passe les plus souvent volés
6	43.6 million	123456 000000 123123
7	26 million	1234567 a123456 welcome
8	189 million	12345678 Password Password
9	153 million	123456789 Aa@123456 Admin@123
10	160 million	1234567890 qwertyuiop 987654321
11	115 million	12345678910 Welcome@123 qwerty12345
12	92 million	admintelecom Password@123 Pakistan@123

Combien de mots de passe correspondent aux exigences de complexité standard ?

Parmi le milliard de mots de passe volés par des logiciels malveillants qui ont été analysés, près d'un quart (230 millions) peuvent être considérés comme complexes. Cela signifie qu'ils répondraient aux exigences standard définies par de nombreuses organisations :

- Minimum de huit caractères
- Une majuscule
- Un chiffre
- Un caractère spécial

Comme vous pouvez le constater avec les mots de passe "complexes" les plus couramment volés présentés ci-dessous, les utilisateurs finaux ajustent souvent de simples termes de base faibles en ajoutant des majuscules, des chiffres ou des caractères spéciaux à des endroits prévisibles (généralement en commençant par une majuscule et en terminant par des chiffres consécutifs). Ces mots de

passe peuvent être facilement devinés par des techniques de force brute, car ils suivent des schémas simples et prévisibles. Pour cette raison, des normes de conformité telles que le NIST s'éloignent des recommandations basées sur la complexité pour se concentrer davantage sur l'augmentation de la longueur des mots de passe.

Cela montre également qu'un mot de passe répondant aux standards d'une organisation n'est pas forcément sécurisé. Tout mot de passe peut être volé par des logiciels malveillants et compromis – quelle que soit sa longueur ou sa complexité. Même si vous avez une politique de mots de passe robuste, il est essentiel de disposer d'un outil permettant de vérifier si votre Active Directory contient des mots de passe compromis.

Mots de passe volés qui passeraient les règles de complexité dans de nombreuses organisations
Pass@123
P@ssw0rd
Aa@123456
Admin@123
Aa123456@
Pass@1234
Abcd@1234
Demo@123
Password@123
India@123

Conseil Specops : Bloquez les mots de passe faibles avec un dictionnaire d'exclusion personnalisé

Même après des décennies de formation à la sécurité et de sensibilisation, les gens continuent de créer des mots de passe faibles. C'est dans la nature humaine de suivre le chemin de la moindre résistance. Que ce soit en choisissant un terme de base facile à mémoriser pour un mot de passe ou en apportant une légère modification à un précédent. Les utilisateurs ne souhaitent tout simplement pas mémoriser un nouveau mot de passe long et complexe à chaque fois qu'ils sont contraints de le changer – ils recherchent donc des solutions de contournement.

Inspirée par les Jeux Olympiques de Paris, notre équipe de recherche a révélé plus tôt cette année que 157 048 mots de passe liés au sport avaient été compromis par des logiciels malveillants au cours des 12 mois précédents. Les mots de passe liés au golf étaient les plus fréquemment volés, avec 40 294 occurrences, suivis par ceux liés au football, avec 20 550 occurrences. Le sport constituait un thème générique dans cette étude, mais les termes de base faibles deviennent encore plus problématiques lorsque les utilisateurs choisissent des termes spécifiques à votre organisation, car les hackers sont plus susceptibles de les utiliser dans une attaque ciblée.

Créer un dictionnaire personnalisé pour exclure certains mots de passe est un excellent moyen d'empêcher les utilisateurs de choisir des termes de base faibles. Vous pourriez utiliser des outils d'intelligence artificielle comme ChatGPT pour générer une liste de mots de passe courants et prévisibles, tels que admin et password. Ensuite, vous pouvez chercher des suggestions de mots de passe et leurs variations basées sur des termes spécifiques à votre organisation, comme les noms de votre entreprise ou de vos produits. Cela permettra de créer un dictionnaire complet et robuste, qui peut être affiné périodiquement.

Votre Active Directory cache-t-il des mots de passe faibles ? Découvrez-le aujourd'hui

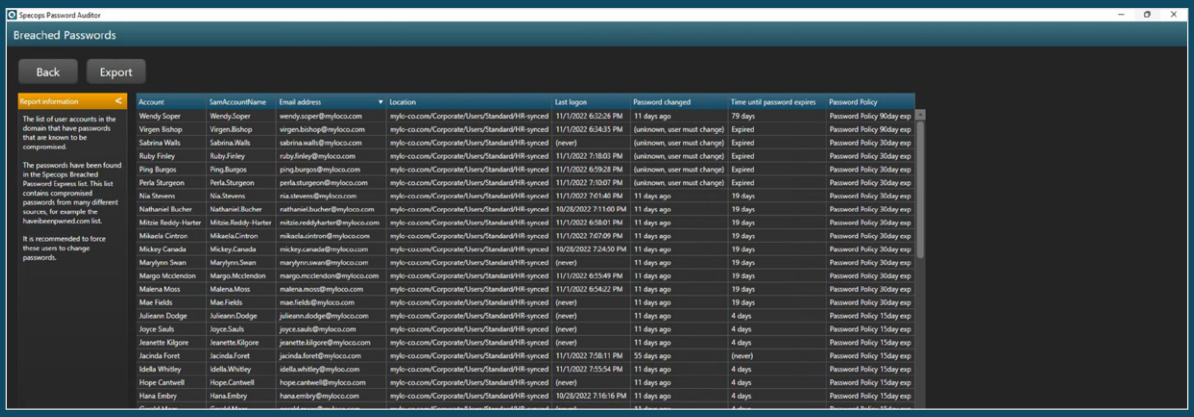
Un audit est la première étape vers une meilleure sécurité des mots de passe. Specops Password Auditor est un outil gratuit qui peut identifier en quelques minutes plusieurs types de vulnérabilités liées aux mots de passe. Effectuez une vérification en lecture seule de votre Active Directory en le comparant à plus d'un milliard de mots de passe compromis et analysez vos politiques de mots de passe de domaine ainsi que vos politiques de mots de passe à granularité fine. Vous pouvez également déterminer si vos politiques sont conformes aux réglementations courantes en matière de cybersécurité.

Votre rapport exportable vous fournira une visibilité sur les informations suivantes et les vulnérabilités liées aux mots de passe :

- Mots de passe compromis
- Mots de passe vides
- Mots de passe identiques
- Comptes administrateur obsolètes
- Comptes marqués comme « Mot de passe non requis »
- Comptes utilisateur obsolètes
- Comptes marqués comme « Mot de passe ne expire jamais »
- Mots de passe expirés
- Politiques de mots de passe + utilisation
- Conformité des politiques de mots de passe

Specops Password Auditor : Tableau de bord des résultats

N'oubliez pas d'accorder une attention particulière aux utilisateurs finaux dont les mots de passe sont connus pour être compromis ou violés, car ceux-ci offrent une voie d'accès simple à votre organisation pour les hackers :



Specops Password Auditor: Rapport montrant les utilisateurs finaux ayant des mots de passe compromis connus

Obtenir mon outil d'audit gratuit

Comment les hackers utilisent des malwares pour voler des identifiants

Les identifiants volés sont très recherchés. Ils offrent un accès simple et direct à des données précieuses, notamment des informations personnelles, des dossiers financiers et des secrets d'entreprise. Les **Initial Access Brokers (IABs)** se spécialisent dans le commerce d'identifiants volés sur le dark web et les forums clandestins. Sans accès à des outils de Threat Intelligence, il peut être difficile pour les organisations de savoir si les identifiants de leurs utilisateurs sont proposés sur des marchés fréquentés par des pirates.

Les identifiants volés peuvent également être utilisés pour lancer des attaques supplémentaires, telles que des campagnes de phishing ou des violations plus sophistiquées. Une fois qu'un pirate accède à un système en utilisant des identifiants volés, il peut maintenir un accès à long terme, ce qui lui permet de collecter davantage de données au fil du temps et éventuellement de se déplacer latéralement au sein d'un réseau pour accéder à d'autres systèmes. Des identifiants légitimes représentant une identité de confiance rendent plus difficile pour les logiciels de sécurité d'identifier ces activités comme malveillantes, car les actions semblent être effectuées par des utilisateurs autorisés.

Comment fonctionnent les infostealers ?

Comprendre comment fonctionnent les **infostealers** peut aider à développer de meilleures pratiques de sécurité et des défenses contre ces menaces. Il est essentiel de maintenir les logiciels à jour, d'utiliser des mots de passe forts et uniques, et d'employer l'authentification multifactorielle lorsque cela est possible. De plus, des audits de sécurité réguliers et une surveillance active peuvent aider à détecter et atténuer la présence des infostealers. Voici un aperçu général de leur fonctionnement :

1. Infection : Les infostealers peuvent infecter un système par divers moyens, tels que les emails de phishing, les téléchargements malveillants ou l'exploitation de vulnérabilités dans les logiciels. Une fois le malware exécuté, il accède au système.

2. Persistance : Pour garantir leur capacité à continuer de collecter des données sur le long terme, les infostealers mettent souvent en place des mécanismes de persistance. Cela peut inclure la création d'entrées dans le registre, la modification de fichiers système ou l'ajout de leur exécution aux processus de démarrage.

3. Collecte de données : Les infostealers recherchent et collectent divers types d'informations sensibles. En ce qui concerne les identifiants, ils ciblent généralement :

- **Navigateurs :** Ils peuvent extraire les mots de passe enregistrés, les cookies et les données de saisie automatique des navigateurs web tels que Chrome, Firefox et Edge.
- **Clients de messagerie :** Ils peuvent voler les identifiants de connexion et d'autres données provenant de clients de messagerie comme Outlook.
- **Clients FTP :** Ils peuvent accéder aux identifiants stockés dans les clients FTP et les voler.
- **Systèmes de fichiers :** Ils peuvent rechercher et extraire des identifiants à partir de fichiers de configuration, de fichiers texte et d'autres emplacements de stockage de données.
- **Presse-papiers :** Ils peuvent surveiller le presse-papiers pour capturer toute information sensible copiée et collée.

4. Exfiltration : Une fois les données collectées, les infostealers doivent les transmettre à l'attaquant. Cela peut se faire par divers moyens :

- **Requêtes HTTP/HTTPS :** Ils peuvent envoyer les données à un serveur distant en utilisant des protocoles web.
- **Email :** Ils peuvent transmettre les données par email à l'attaquant.
- **FTP :** Ils peuvent télécharger les données sur un serveur FTP.
- **Serveurs de Commande et Contrôle (C2) :** Ils peuvent communiquer avec des serveurs C2 pour envoyer les données et recevoir des instructions supplémentaires.

5. Évasion : Pour éviter d'être détectés, les infostealers utilisent souvent des techniques pour contourner les logiciels antivirus et autres mesures de sécurité. Ces techniques peuvent inclure :

- **Obfuscation du code :** Rendre le code difficile à lire et à analyser.
- **Packing :** Compresser le malware pour le rendre plus difficile à détecter.
- **Techniques de rootkit :** Masquer la présence du malware sur le système.
- **Communication furtive :** Utiliser des canaux de communication chiffrés ou obfusqués pour éviter la surveillance du réseau.

6. Exécution : Les infostealers peuvent être programmés pour s'exécuter à des moments précis ou dans certaines conditions afin d'éviter de susciter des soupçons. Par exemple, ils peuvent s'activer uniquement lorsque l'utilisateur n'est pas en train d'utiliser activement l'ordinateur.

Les principaux logiciels malveillants utilisés pour voler des identifiants

Les recherches de Specops mettent en évidence le malware Redline comme l'outil préféré des hackers pour le vol de mots de passe, représentant près de la moitié de tous les mots de passe volés analysés. Dans notre ensemble de données, les hackers ont volé 170 millions de jeux d'identifiants uniques en seulement six mois grâce à Redline. Vidar et Raccoon Stealer sont également notables, responsables respectivement de 17 % et 11,7 % des mots de passe volés. Voici quelques informations supplémentaires sur les trois principaux logiciels malveillants identifiés :

1. Redline

Redline est un logiciel malveillant extrêmement populaire. Découvert en mars 2020, son principal objectif est d'exporter toutes sortes d'informations personnelles, telles que des identifiants, des portefeuilles de cryptomonnaie et des données financières, pour ensuite les transférer vers l'infrastructure C2 du malware. Dans de nombreux cas, une charge utile de Redline est livrée avec un mineur de cryptomonnaie à déployer sur la machine de la victime, notamment dans des campagnes ciblant les joueurs équipés de GPU puissants.

Depuis la mi-2021, YouTube a également été utilisé comme méthode de distribution pour Redline, selon le processus suivant :

- **Compromission d'un compte Google/YouTube :** Le cybercriminel prend le contrôle d'un compte.
- **Création de chaînes ou publication de vidéos :** Une fois le compte compromis, le cybercriminel crée différentes chaînes ou publie directement des vidéos.
- **Ajout de liens malveillants dans les descriptions :** Les vidéos publiées (souvent des vidéos proposant des triches et cracks pour les jeux vidéo, ou des instructions pour pirater des logiciels et jeux populaires) incluent dans leur description un lien malveillant en rapport avec le thème de la vidéo.
- **Téléchargement non intentionnel par l'utilisateur :** Les utilisateurs cliquent sur le lien et téléchargent sans le savoir Redline sur leur appareil, ce qui entraîne le vol de leurs mots de passe et autres informations privées.

2. Vidar

Vidar est une évolution du célèbre **Arkei Stealer**. Il vérifie les préférences linguistiques de la machine infectée afin de mettre certains pays sur liste blanche pour une éventuelle infection ultérieure. Ensuite, il génère un **Mutex** et initialise les chaînes nécessaires à son fonctionnement. Deux versions de serveurs de commande et contrôle (**C2**) sont disponibles pour les hackers :

La version originale est associée à la version payante de Vidar, appelée **Vidar Pro**.

Une autre version de C2 est utilisée dans la version crackée de Vidar, distribuée sur des forums clandestins, appelée **Anti-Vidar.**

Au début de 2022, Vidar a été observé dans des campagnes de phishing sous forme de fichiers **Microsoft Compiled HTML Help (CHM**). De plus, il a été détecté que ce malware est distribué via les services de logiciels malveillants **PrivateLoader**, le kit d'exploitation **Fallout Exploit Kit**, et le chargeur Colibri Loader. À la fin de 2023, Vidar a également été observé comme charge utile du chargeur de logiciels malveillants **GHOSTPULSE**.

3. Raccoon Stealer

Raccoon Stealer est un malware voleur d'informations proposé à la vente dans les milieux cybercriminels clandestins. L'équipe derrière Raccoon Stealer utilise un modèle de **"malware-as-a-service"**, permettant aux clients de louer ce logiciel malveillant sur une base mensuelle. Il a été mis en vente pour la première fois sur le forum de haut niveau en langue russe **Exploit** le 8 avril 2019. Raccoon Stealer est promu avec le slogan : **"Nous volons, vous gérez !"**

Principalement, il a été proposé sur des forums clandestins russophones tels **qu'Exploit** et **WWH-Club**. Le 20 octobre 2019, le cybercriminel a également commencé à proposer Raccoon Stealer sur le célèbre forum anglophone **Hack Forums**. Les personnes faisant la promotion de Raccoon Stealer sur ces forums clandestins mentionnent parfois des **"semaines de test"**, suggérant que des hackers potentiels peuvent essayer le produit avant de l'acheter.

L'opérateur derrière Raccoon Stealer a récemment été arrêté et condamné à cinq ans de prison.

Peut-on voler des mots de passe Active Directory avec des malwares ?

Le point faible réside dans le fait que les utilisateurs stockent leurs identifiants Active Directory dans des navigateurs ou des applications comme FileZilla, ce qui les rend vulnérables aux logiciels malveillants voleurs d'identifiants. Les identifiants Active Directory correspondent souvent à ceux utilisés dans Microsoft 365/Outlook, car ils sont gérés par **Entra ID** (anciennement Azure AD), un annuaire basé sur le cloud synchronisé avec l'Active Directory local. De nombreuses organisations mettent également en œuvre le **Single Sign-On** (**SSO**), ce qui relie encore davantage ces systèmes.

Nos chercheurs ont également récemment découvert plus de deux millions de mots de passe VPN compromis par des logiciels malveillants, soulignant un risque majeur pour la sécurité organisationnelle. Ces mots de passe, essentiels pour l'accès des utilisateurs aux VPN, constituent désormais des points d'entrée potentiels pour les cybercriminels, sapant l'objectif principal des VPN : sécuriser et privatiser les communications grâce au chiffrement des données.

Le risque le plus important survient lorsque les mots de passe Active Directory sont également utilisés comme mots de passe VPN. Cela pourrait permettre aux attaquants d'accéder à tous les systèmes et ressources pour lesquels un utilisateur a des autorisations, entraînant des dommages importants et des vols de données.

Conseils Specops : Recherche d'identifiants volés sur le dark web

Les équipes de **Threat Intelligence** peuvent aider les organisations à déterminer si les identifiants de leurs utilisateurs ont été compromis et mis en vente sur le dark web, leur permettant ainsi de prendre des mesures immédiates pour sécuriser leurs comptes en incitant les utilisateurs à changer leurs mots de passe. Ces équipes mènent des activités telles que l'infiltration de botnets, l'interception de communications et l'accès à des informations privilégiées sur les forums clandestins pour collecter des données sur les mots de passe récoltés par des logiciels malveillants.

Les renseignements ainsi collectés sont essentiels pour mettre à jour la vaste base de données de mots de passe compromis de **Specops**, qui contient plus de 4 milliards de mots de passe uniques. Ces informations proviennent de l'équipe qui a alimenté une grande partie des recherches présentées dans ce rapport. Cela contribue à protéger les organisations contre le véritable danger des stealers : des groupes de **traffers** (groupes spécialisés dans le trafic d'identifiants) qui vendent ces mots de passe à d'autres hackers et groupes de ransomware.

Comment les organisations peuvent-elles réduire les risques liés aux mots de passe ?

Il existe deux moyens clés pour les organisations de réduire les risques liés aux mots de passe. Tout d'abord, il est essentiel de s'assurer que votre **Active Directory** contient des mots de passe longs et complexes, capables de résister aux attaques par force brute. Cependant, l'analyse du milliard de mots de passe volés par des logiciels malveillants présentée dans ce document met en évidence la nécessité d'utiliser un outil capable de détecter les mots de passe compromis à l'insu de votre organisation.

Exiger des mots de passe longs et forts

Notre équipe de recherche s'est penchée sur la robustesse de l'algorithme de hachage SHA-256 face aux techniques actuelles de cassage de mots de passe. Bien qu'il ne s'agisse pas de l'algorithme le plus avancé, il est encore largement utilisé dans de nombreux environnements. Le principal danger réside dans la réutilisation des mots de passe : même si les mots de passe professionnels de vos utilisateurs sont stockés de manière très sécurisée, dès qu'un utilisateur réutilise ce mot de passe sur un site moins sécurisé, et que ce site subit une fuite de données, un attaquant pourrait s'en servir pour cibler votre réseau.

Comme le montre le tableau de cassage produit par cette recherche, même un algorithme relativement moderne comme SHA-256 ne peut pas protéger des mots de passe courts et simples contre les attaques par force brute. En revanche, il apparaît également qu'un hacker perdrait probablement son temps à essayer de casser un mot de passe long et complexe haché avec SHA-256. Cela prouve l'importance d'encourager les utilisateurs finaux à créer des phrases de passe longues et sécurisées.

Il est temps de craquer: mots de passe hachés SHA-256

Number of characters	Numbers Only	Lowercase Only	Upper and Lower	Number, Upper, Lower	Number, Upper, Lower, Symbols
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	14 minutes
8	Instantly	Instantly	11 minutes	41 minutes	21 hours
9	Instantly	Instantly	9 hours	2 days	3 months
10	Instantly	27 minutes	19 days	3 months	22 years
11	Instantly	12 hours	2 years	19 years	2052 years
12	Instantly	13 days	141 years	1164 years	195k years
13	2 minutes	9 months	7332 years	73k years	19m years
14	19 minutes	24 years	381k years	4474k years	1760m years
15	4 hours	605 years	19m years	277m years	167.2b years
16	2 days	15732 years	1031m years	18b years	16t years
17	14 days	410k years	54b years	1067b years	1509t years
18	5 months	11m years	2788b years	67t years	144q years
19	4 years	277m years	145t years	4099t years	14Q years
20	37 years	7189m years	8q years	255q years	1294Q years

Les attaquants préféreront toujours cibler les cibles faciles et les solutions de facilité. Par exemple, les mots de passe Active Directory déjà compromis lors de violations de données. Cela peut notamment se produire en raison de la réutilisation des mots de passe. Vous pouvez encourager vos utilisateurs finaux à créer des mots de passe Active Directory longs et robustes et à les stocker de manière très sécurisée. Cependant, cet effort est réduit à néant si ces utilisateurs réutilisent ces mots de passe sur des appareils personnels, des sites ou des applications dotés d'une sécurité faible.

Il est temps de craquer: mots de passe compromis connus

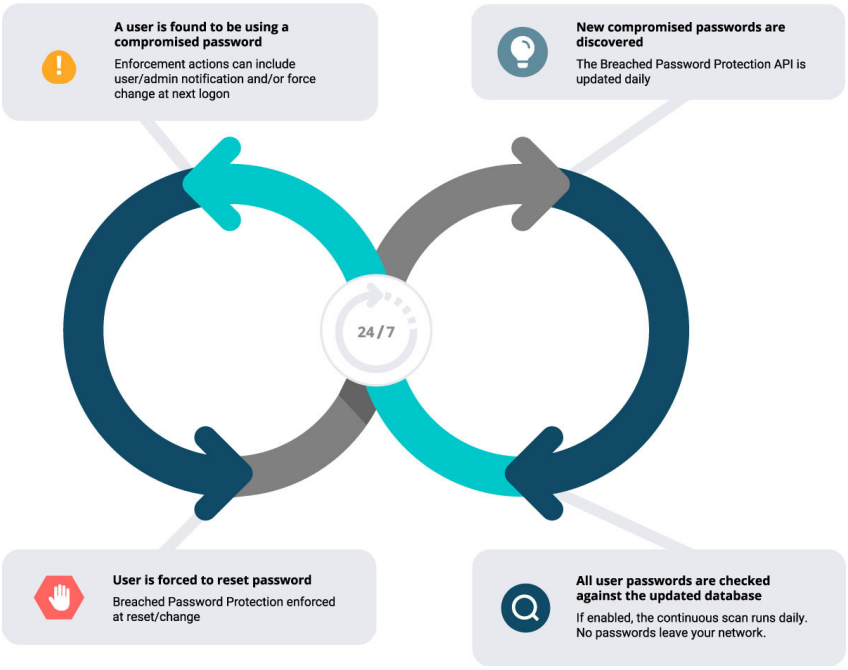
Number of characters	Numbers Only	Lowercase Only	Upper and Lower	Number, Upper, Lower	Number, Upper, Lower, Symbols
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	Instantly
9	Instantly	Instantly	Instantly	Instantly	Instantly
10	Instantly	Instantly	Instantly	Instantly	Instantly
11	Instantly	Instantly	Instantly	Instantly	Instantly
12	Instantly	Instantly	Instantly	Instantly	Instantly
13	Instantly	Instantly	Instantly	Instantly	Instantly
14	Instantly	Instantly	Instantly	Instantly	Instantly
15	Instantly	Instantly	Instantly	Instantly	Instantly
16	Instantly	Instantly	Instantly	Instantly	Instantly
17	Instantly	Instantly	Instantly	Instantly	Instantly
18	Instantly	Instantly	Instantly	Instantly	Instantly
19	Instantly	Instantly	Instantly	Instantly	Instantly
20	Instantly	Instantly	Instantly	Instantly	Instantly

Vérifier continuellement les mots de passe compromis

La fonctionnalité de scan continu de **Specops Password Policy** effectue des vérifications quotidiennes à l'aide du service **Specops Breached Password Protection**, mis à jour quotidiennement avec des mots de passe collectés à partir de réseaux honeypot, de données de Threat Intelligence et de nouvelles fuites de mots de passe découvertes. Cela garantit que les professionnels de l'informatique ont un accès constant à l'une des bases de données de mots de passe compromis les plus complètes et à jour du marché.

En scannant en continu les mots de passe Active Directory via l'API de **Breached Password Protection**, vos équipes informatiques peuvent identifier de manière proactive les mots de passe compromis au sein de votre organisation. Les scans continus des mots de passe permettent de détecter des points d'accès potentiels à des violations de sécurité et de prendre des mesures rapides pour atténuer les risques liés à la réutilisation des mots de passe. Cette fonctionnalité permet aux équipes informatiques d'identifier automatiquement les mots de passe compromis et d'obliger immédiatement les utilisateurs finaux à les changer lors de leur prochaine connexion.

Intégrer la fonctionnalité de scan continu dans votre politique de mots de passe permet aux administrateurs de garantir la conformité avec les meilleures pratiques du secteur et les exigences réglementaires. Les résultats des scans continus peuvent être facilement consultés, offrant une vue claire des mots de passe compromis au sein d'un réseau.



Fonctionnalité de scan continu de Specops Breached Password Protection

Vous souhaitez discuter de la manière dont Specops Password Policy avec Breached Password Protection pourrait s'intégrer à votre organisation ?

Contactez-nous ici.

Huit points clés

1. Les identifiants volés par des logiciels malveillants sont courants – nous en avons identifié plus d'un milliard au cours des 12 derniers mois.
2. Malgré la connaissance des risques, les utilisateurs finaux créent encore des mots de passe courts et faibles comme "password", "12345" et "admin" lorsqu'ils en ont la possibilité. Bloquer ces termes faibles dans votre politique de mots de passe est essentiel.
3. De nombreux identifiants volés respectent les exigences standard de complexité – y compris 230 millions analysés dans ce rapport.
4. Les mots de passe "complexes" peuvent encore être prévisibles en raison du comportement des utilisateurs. La longueur est un meilleur indicateur de la robustesse d'un mot de passe.
5. Les hackers privilégient les identifiants volés par logiciels malveillants, car ils sont faciles à obtenir, à utiliser et à vendre. Selon nos recherches, Redline est le voleur d'informations le plus populaire.
6. Même des mots de passe forts peuvent être volés par des logiciels malveillants, rendant les algorithmes de hachage obsolètes. Tous les comptes utilisateurs doivent être sécurisés avec une authentification multifactorielle (MFA).
7. Les logiciels malveillants illustrent pourquoi la réutilisation des mots de passe est si dangereuse. Vos utilisateurs réutilisent-ils leurs mots de passe professionnels sur des appareils et applications personnels avec une sécurité faible ?
8. Il est crucial de pouvoir scanner en continu votre Active Directory pour détecter les mots de passe compromis.

L'HISTOIRE DU SPECOPS

Specops Software, une société Outpost24, est le principal fournisseur de solutions de gestion de 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. Avec une gamme complète de solutions intégrées nativement à Active Directory, Specops garantit que les données sensibles sont stockées sur site et sous votre contrôle. Specops Software a été fondée en 2001 et son siège social est à Stockholm, en Suède, avec des bureaux supplémentaires aux États-Unis, au Canada, au Royaume-Uni et en Allemagne..

RÉSERVEZ UNE DÉMO >> **DEMANDER UN TARIF PERSONNALISÉ >>**

CONTACTEZ-NOUS

GLOBAL HQ
Karlskrona, Sweden
Blekingegatan 1,
371 57 Karlskrona, Sweden
info@outpost24.com

US HQ
Philadelphia, United States
123 S Broad St Suite 2530,
Philadelphia, PA 19109, United States
Phone +1 877 773 2677

Stockholm, Sweden
Vasagatan 7A,
111 20 Stockholm, Sweden
info@outpost24.com

Copenhagen, Denmark
Axel Towers 2F, 4th floor,
1609 Copenhagen V, Denmark
+45 53 73 05 67

Sophia Antipolis, France
950 Route Des Colles Les Templiers
CS30505
06410 Biot, France

London, United Kingdom
2 Stephen St, London W1T 1AN,
United Kingdom

Plymouth, United Kingdom
Poseidon House, Neptune Park,
Plymouth PL4 0SJ, United Kingdom

Reading, United Kingdom
Thames Tower, Station Rd,
Reading RG1 1LX, United Kingdom

Amsterdam, Netherlands
Strawinskylaan 257
1077 XX Amsterdam, Netherlands
+31 20 420 9560

Leuven, Belgium
Kapeldreef 60,
3001 Leuven, Belgium
+32 16 22 76 60

Barcelona, Spain
Plaça de Gal·la Placídia,
1-3, Oficina 303,
08006 Barcelona, Spain

Chicago, United States
35 S Washington St., Suite 308,
Naperville, IL 60540

Toronto, Canada
517 Wellington Street West, Suite 400
Toronto, ON M5V 1G1
+1 877 773 2677

Berlin, Germany
Gierkezeile 12, 10585 Berlin
+49 30166 37218

Hanoi, Vietnam
15th Floor, Peakview Tower Building, 36 Hoang Cau, Dong Da, Hanoi,
Vietnam

SPECOPS
AN OUTPOST24 COMPANY