Rapport Specops 2026 sur les mots de passe compromis

Analyse annuelle des identifiants volés par des malwares

Specops Software, une société du groupe Outpost24, est un acteur de référence dans les solutions de gestion des identités et d'authentification.

Contenu du rapport

Temps forts du rapport

Les données présentées dans ce rapport proviennent de l'équipe de renseignement sur les menaces d'Outpost24, société mère de Specops Software. Au total, plus de six milliards de mots de passe compromis ont été collectés et analysés entre janvier et décembre 2025. Ces travaux s'appuient également sur des recherches complémentaires menées par Specops Software tout au long de l'année. L'ensemble des données est exact à la date de décembre 2025.

lus de **six milliards** de mots de passe volés en 12 mois

En 2025, LummaC2 était le logiciel malveillant de vol d'identifiants le plus actif, avec **60 934 662** comptes compromis

Les mots de passe à huit caractères restent les plus ciblés, avec **1 077 202 230** identifiants compromis

Les trois longueurs **de mot de passe les plus volées :**

- **Huit caractères (1,1 milliard)**
- **Dix caractères (926 millions)**
- **Neuf caractères (882 millions)**

Les termes les plus utilisés dans les mots de passe volés :

- admin
- guest
- cisco
- Hello

Les 5 mots de passe les plus volés :

- 123456
- 123456789
- 12345678
- admin
- Password

Résumé

L'utilisation abusive d'identifiants reste l'une des méthodes d'accès initiales les plus fiables et les plus évolutives pour les hackers. L'analyse continue des violations de données confirme que les mots de passe volés restent au cœur des attaques modernes.
Selon le rapport Data Breach Investigations Report 2025 de Verizon (DBIR), l'utilisation abusive d'identifiants est à l'origine de 22 % des violations de données confirmées. Par ailleurs, 54 % des victimes de rançongiciel avaient leur domaine présent dans des bases d'identifiants compromis, et 40 % disposaient d'adresses e-mail professionnelles exposées. Ces chiffres illustrent la capacité des mots de passe volés à alimenter des attaques en cascade, à grande échelle.

Ces résultats confirment une réalité persistante : les mots de passe figurent parmi les éléments les plus exposés et les plus exploités de la sécurité en entreprise. Une fois compromis, les identifiants offrent aux hackers un accès de confiance aux environnements d'entreprise, en contournant souvent entièrement les défenses périmétriques. Cette tendance se reflète également dans les données plus larges sur les intrusions. Selon IBM X-Force., les attaques basées sur l'identité ont représenté 30 % des intrusions observées en 2025.

Le vol d'identifiants étant désormais un phénomène continu plutôt qu'épisodique, le risque lié aux mots de passe ne peut plus être évalué uniquement au moment de leur création. Il ne s'agit plus seulement de savoir si un mot de passe respecte une politique donnée, mais s'il demeure sécurisé dans un écosystème où les identifiants sont collectés, agrégés et revendus de manière permanente.

Dans ce contexte, l'équipe de renseignement sur les menaces d'Outpost24 a analysé plus de six milliards de mots de passe volés par des malwares, collectés tout au long de l'année 2025. Ce rapport met en lumière les schémas de mots de passe activement exploités par les hackers, la manière dont les malwares de type infostealer collectent et diffusent des identifiants à grande échelle, ainsi que ce que ces tendances révèlent sur les limites des politiques de mot de passe traditionnelles.

En s'appuyant sur des données réelles issues de l'activité des hackers, ce rapport permet aux organisations de mieux comprendre leur niveau d'exposition aux attaques basées sur les mots de passe et d'identifier des mesures concrètes pour réduire les risques liés aux identifiants compromis.

Mots de passe faibles : tendances et modèles

Parmi les **6 004 274 474** mots de passe volés analysés, les schémas faibles et prévisibles restent largement dominants. Malgré des années de sensibilisation et des politiques de mot de passe toujours plus complexes, les hackers retrouvent encore les mêmes structures de base, répétées d'un environnement à l'autre, entre applications et à travers les régions.

Les mots de passe les plus fréquemment volés

Les suites numériques simples et les termes par défaut représentent toujours la majorité des identifiants volés par des malwares, ce qui confirme les résultats du Rapport 2025 de Specops Software sur les mots de passe compromis.

Les cinq mots de passe les plus volés en 2025
123456
123456789
12345678
admin
password

Ces mots de passe sont faciles à deviner, largement réutilisés et souvent associés à des comptes partagés, fonctionnels ou à privilèges élevés. Les suites numériques dominent, quelle que soit la longueur du mot de passe, souvent combinées à des termes par défaut comme admin ou password, fréquemment présents dans les infrastructures et les environnements d'entreprise.

Lorsque les utilisateurs peuvent choisir leurs identifiants sans restrictions réellement efficaces, beaucoup optent encore pour les options les plus simples. Dans les environnements d'entreprise, cela représente un risque majeur : des identifiants volés par des malwares peuvent être réutilisés comme mots de passe Active Directory (AD), VPN ou d'identités cloud, offrant aux hackers un accès légitime aux systèmes de l'organisation.

Termes de base courants et structures prévisibles

Au-delà des correspondances exactes, l'analyse met en évidence une forte récurrence de termes de base faibles intégrés dans les mots de passe. Parmi les termes les plus courants figurent admin (et ses variantes comme Admin ou ADMIN), guest, cisco et welcome.

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

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

Termes de base les plus courants à sept caractères
Welcome
zxcvbnm
student

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

Ces tendances, largement inchangées par rapport aux années précédentes, démontrent une évolution limitée des comportements utilisateurs. Les combinaisons de touches telles que qwerty et azerty restent très répandues, produisant des structures hautement prévisibles et systématiquement exploitées par les hackers.

La présence récurrente de termes comme password et hello suggère un usage davantage opérationnel que personnel. L'analyse des 500 mots de passe les plus fréquemment récupérés révèle une forte prédominance d'identifiants fonctionnels, liés à l'infrastructure, aux accès VPN et aux services internes, avec de nombreuses variantes de « admin », « root » et « user ».

Modèles de mots de passe selon les régions et les langues

Bien que les mots de passe les plus couramment compromis soient similaires à l'échelle mondiale, certaines variations régionales apparaissent, tout en reposant sur des modèles structurellement identiques.

Termes de base régionaux les plus courants
Pakistan@123, Pakistan123
India@123
Nepal@123
senha123 (mot de passe en portugais)
hola1234 (salutation espagnole

Ces mots de passe suivent des structures familières, et associent généralement un terme culturel, géographique ou linguistique à une suite numérique simple. Si les termes varient selon les régions, les modèles sous-jacents restent hautement prévisibles et facilement exploitables par les attaquants.

Modèles d'identifiants basés sur des noms et partagés

Parmi les identifiants les plus fréquemment collectés, un modèle récurrent se distingue : l'utilisation de mots de passe basés sur des noms et combinés à des suffixes numériques ou symboliques simples. Un grand nombre de mots de passe volés suivent la structure Prénom@123.

Termes de base les plus courants basés sur des noms
Kumar@123
Rahul@123
Rohit@123
Amit@123
Akash@123

Ces mots de passe apparaissent fréquemment dans plusieurs environnements sans lien direct et ne sont probablement pas rattachés à des comptes individuels. Ils reflètent davantage des usages partagés ou fonctionnels, notamment pour l'accès à des services, des identifiants d'intégration, ou des comptes associés à des portails internes et à des systèmes d'accès à distance.

Longueurs de mot de passe les plus courantes

Le tableau ci-dessous présente le nombre de mots de passe volés observés en 2025, répartis par longueur. Comme les années précédentes, les mots de passe de huit caractères restent les plus fréquemment compromis, avec plus de 1,07 milliard d'identifiants concernés. Cela montre que de nombreuses organisations continuent de se limiter à des exigences minimales de longueur.

Les mots de passe plus longs ont également été largement exposés. Des centaines de millions de mots de passe de toutes les longueurs courantes ont été volés : 882 millions pour neuf caractères, 925 millions pour dix caractères et 672 millions pour onze caractères. Au total, plus de 4,4 milliards de mots de passe volés comptaient entre huit et douze caractères, confirmant que la longueur seule ne suffit pas à protéger contre la compromission.

Longueur du mot de passe	Nombre d'occurrences	Les trois mots de passe les plus fréquemment volés
6	239 588 682	123456 123123 000000
7	152 581 176	1234567 A123456 welcome
8	1 077 202 230	12345678 Password Aa123456
9	882 149 149	123456789 Aa@123456 Admin@123
10	925 692 295	1234567890 Qwertyuiop 0987654321
11	672 515 189	12345678910 Welcome@123 qwerty12345
12	540 238 382	Password@123 Pakistan@123 admintelecom

Quelle que soit leur longueur, les mots de passe les plus fréquemment volés respectent les mêmes modèles prévisibles que ceux décrits ailleurs dans ce rapport. Les données montrent que des termes de base faibles et des séquences simples sont souvent allongés par des caractères supplémentaires, permettant aux mots de passe de répondre aux exigences des politiques tout en restant faciles à réutiliser une fois compromis. Le fait

que cette répartition reste stable dans le temps montre que les méthodes de création de mots de passe ont peu évolué.

Les mots de passe et passphrases de 15 caractères ou plus restent un outil important pour se protéger contre les attaques par force brute ou par devinette. Cependant, les données de ce rapport montrent que les mots de passe sont souvent volés via des infostealers ou des attaques de phishing, plutôt que par piratage direct.

Cela signifie que même les identifiants forts et conformes aux politiques peuvent être exposés, en particulier lorsque les employés réutilisent leurs mots de passe professionnels sur des appareils, applications ou sites web personnels moins sécurisés. Les organisations doivent donc mettre en place des solutions permettant de scanner en permanence leurs Active Directory (AD) pour détecter les mots de passe compromis, au lieu de se fier uniquement aux règles de longueur et de complexité.

Les mots de passe complexes restent vulnérables

De nombreuses organisations continuent de se baser sur des règles de complexité standard pour réduire les risques liés aux mots de passe, qui imposent généralement :

- au moins huit caractères
- une lettre majuscule
- un chiffre
- un caractère spécial

L'analyse des identifiants volés par des malwares a révélé que les mots de passe respectant ces exigences sont encore régulièrement compromis.

Exemples courants de mots de passe complexes compromis
Aa@123456
Admin@123
Pass@1234
Abcd@1234
Aa123456@

La fréquence de ces mots de passe montre que la conformité aux règles lors de leur création ne garantit pas leur sécurité une fois les identifiants exposés. Même les mots de passe conformes à la politique peuvent être réutilisés immédiatement dans tous les environnements d'entreprise, ce qui les rend directement exploitables dans les ensembles de données d'identifiants agrégés.

Principaux enseignements de l'analyse des modèles d'identifiants

Les points ci-dessous mettent en évidence les modèles de mots de passe les plus fréquents observés dans l'analyse des identifiants, et montrent comment les structures prévisibles continuent de faciliter l'exposition des comptes.

1

Les 500 mots de passe les plus fréquemment récupérés sont clairement liés à l'infrastructure et à l'accès partagé, avec des termes tels que admin, root, user, guest et administrator.

2

Les modèles de mots de passe par défaut et d'intégration restent très répandus.
Les identifiants tels que Welcome@123 indiquent que les mots de passe attribués le premier jour sont souvent conservés plutôt que modifiés ou supprimés.

3

Les mots de passe basés sur des noms avec des suffixes simples restent courants.
Les modèles tels que Kumar@123 présentent une variation minimale et sont conçus pour satisfaire aux règles de complexité plutôt que pour améliorer la sécurité.

4

Les termes régionaux et spécifiques à une langue apparaissent fréquemment, mais suivent les mêmes structures faibles.

5

Les chaînes de caractères séquentielles et structurées restent courantes. Des exemples tels que Aa123456 et Abc123 réduisent considérablement les efforts de l'attaquant.

Essayez Specops Password Auditor

Activité des logiciels de type infostealer et familles de malware les plus actives

Pourquoi les identifiants volés suscitent-ils autant d'intérêt ?

Les malwares de type « infostealer » sont devenus l'un des moyens les plus efficaces pour collecter des identifiants à grande échelle. Contrairement aux attaques ciblées exploitant des vulnérabilités spécifiques, les infostealers opèrent de manière opportuniste, récupérant les données d'authentification depuis les navigateurs, les applications et le stockage local des systèmes infectés. Cette approche permet aux attaquants de collecter rapidement d'importants volumes d'identifiants avec un effort limité et un risque opérationnel faible.

Une fois récupérées, ces informations d'identification sont rarement utilisées seules. Elles sont regroupées, enrichies et redistribuées via des écosystèmes criminels établis, notamment des courtiers en accès et des marchés d'identifiants. Une seule infection peut ainsi alimenter des campagnes d'attaque répétées sur de longues périodes, transformant la compromission ponctuelle d'un mot de passe en une exposition durable pour les organisations concernées.

Les courtiers en accès initiaux (IABs) jouent un rôle clé en revendant l'accès aux organisations compromises via des marchés clandestins et des plateformes de messagerie telles que Telegram. Sur ces canaux, l'accès à des environnements d'entreprise peut être acquis pour quelques centaines de dollars seulement, ce qui réduit les barrières à l'entrée pour les attaquants et contribue à l'industrialisation et à l'accélération des attaques à grande échelle reposant sur l'exploitation d'identifiants.

Une fois cet accès obtenu à l'aide d'identifiants légitimes, les attaquants sont en mesure d'établir une présence durable au sein des environnements compromis, de se déplacer latéralement entre les systèmes et d'étendre progressivement leur périmètre d'action afin de collecter davantage de données. Comme cette activité semble provenir d'utilisateurs autorisés, elle est souvent difficile à détecter pour les outils de sécurité classiques.

Par conséquent, les entreprises doivent étendre leur visibilité au-delà de leur périmètre interne et surveiller les marchés criminels et dépôts d'identifiants afin d'identifier rapidement toute exposition ou revente de leurs informations d'authentification.

Fonctionnement des infostealers

Les malwares de type « infostealer » sont conçus pour extraire discrètement les identifiants tout en minimisant leur impact sur le système infecté. Comprendre leur mode de fonctionnement permet aux équipes de défense de repérer les points où les identifiants sont les plus exposés et d'identifier les contrôles les plus efficaces pour interrompre la chaîne de vol.

La majorité des infostealers suivent un processus opérationnel relativement simple, privilégiant la rapidité et l'échelle plutôt que la persistance à long terme ou la furtivité avancée. Bien que chaque famille présente ses spécificités, ces logiciels sont généralement des charges utiles légères, conçues pour s'exécuter rapidement, collecter les données et les exfiltrer avec un minimum d'interaction.

1. Infection initiale

Les infostealers sont généralement diffusés via des campagnes de phishing, des téléchargements malveillants, des logiciels piratés, du malvertising, de fausses mises à

jour logicielles ou de sites web compromis. Dans de nombreux cas, la charge utile de l'infostealer est déployée par un chargeur (loader) ou un dropper distinct, chargé de l'exécution, de l'installation et de mécanismes d'évasion basiques.

Une fois exécuté, le logiciel s'exécute généralement dans l'espace utilisateur et démarre immédiatement la collecte des données, sans nécessiter de privilèges élevés.

2. Collecte d'identifiants et de données

Plutôt que de cibler une application unique, les infostealers collectent systématiquement les données d'authentification et les informations associées à partir de multiples sources présentes sur le système infecté, notamment :

- Navigateurs Web : identifiants enregistrés, cookies, jetons de session, données de remplissage automatique et informations de paiement stockées provenant de navigateurs tels que Chrome, Firefox et Edge.
- Clients de messagerie électronique : identifiants de connexion et données de configu-ration provenant d'applications telles qu'Outlook et Thunderbird
- Outils FTP et d'accès à distance : identifiants stockés utilisés pour le transfert de fichiers ou l'administration à distance
- Applications de messagerie et de collaboration : jetons de session ou données locales provenant d'applications telles que Telegram ou Discord
- Portefeuilles de cryptomonnaies : fichiers de portefeuille et extensions de portefeuille basées sur un naviga-teur
- Fichiers locaux et données de configuration : fichiers texte ou fichiers de configu-ration d'applications dans lesquels des identifiants ou des clés API peuvent être stockés
- Données du presse-papiers : contenu récemment copié, pouvant inclure des noms d'utilisateur, des mots de passe, des phrases de récupération ou des jetons d'accès

De plus, de nombreux infostealers collectent également des informations système de base (version du système d'exploitation, nom d'hôte, logiciels installés, outils de sécurité) afin d'enrichir et de contextualiser les données volées.

3. Exfiltration des données

Les données collectées sont transmises à une infrastructure contrôlée par les attaquants. Pour les infostealers, les mécanismes de commande et de contrôle sont généralement simples et étroitement liés à l'exfiltration, et reposent notamment sur :

- des points de terminaison HTTP ou HTTPS
- des serveurs FTP
- des boîtes de réception de courrier électronique ou plateformes de messagerie

Ces points de terminaison servent principalement de points de collecte automatisés, plutôt que de véritables infrastructures de commande interactives, et alimentent souvent directement des tableaux de bord opérés par les attaquants ou des chaînes de revente d'identifiants.

4. Persistance et évasion limitées

Contrairement aux familles de malwares plus sophistiquées, les infostealers ne reposent généralement pas sur des mécanismes de persistance avancés ou des techniques au niveau du noyau. Beaucoup sont conçus pour s'exécuter une seule fois, exfiltrer des données, puis se terminer.

Lorsque des mécanismes de persistance ou d'évasion plus avancés sont présents, ils sont le plus souvent assurés par des composants auxiliaires tels que des chargeurs, des crypteurs ou des packers, plutôt que par l'infostealer lui-même. Les techniques courantes incluent l'emballage basique, l'obfuscation ou des méthodes d'évasion de signatures visant à retarder la détection.

Cette conception volontairement légère reflète l'économie du vol d'identifiants à grande échelle, dont l'objectif est de multiplier les infections et de collecter rapidement des données, plutôt que de maintenir un accès durable à chaque système.

Principaux malwares utilisés pour le vol d'identifiants

Un nombre limité de malwares spécialisés dans le vol d'informations continue de représenter une part importante des activités de collecte d'identifiants. Ces outils sont largement disponibles, faciles à déployer et conçus spécifiquement pour récolter des identifiants à grande échelle sur les appareils infectés.

Selon l'analyse menée par l'équipe de renseignement sur les menaces d'Outpost24 en 2025, les familles de malwares suivantes étaient les plus fréquemment associées au vol d'identifiants :

Famille de malware	Nombre d'identifiants volés
LummaC2	**60 934 662**
RedLine	**31 144 858**
Vidar	**5 965 748**
StealC	**3 441 423**
Raccoon Stealer	**1 656 673**

Ensemble, ces familles de malware représentent des dizaines de millions d'identifiants volés, ce qui confirme l'efficacité continue des infostealers en tant que mécanisme d'accès initial, en particulier lorsque les infections sont réalisées à grande échelle par l'exécution volontaire de l'utilisateur plutôt que par l'exploitation technique de vulnérabilités.

L'analyse met en évidence un changement notable dans la domination des infostealers par rapport à l'année précédente. Le rapport 2024 montrait que RedLine dominait les activités de vol d'identifiants, représentant près de la moitié des mots de passe volés analysés, tandis que Vidar et Raccoon Stealer occupaient également une place importante.

L'ensemble de données de 2025 montre que LummaC2 est désormais le malware de type infostealer le plus prolifique, représentant près de 60 % des identifiants volés dans cette catégorie. RedLine suit avec un peu plus de 30 %, tandis que Vidar, Stealc et Raccoon Stealer représentent ensemble moins de 11 %.

L'analyse révèle que le vol d'identifiants est soutenu par un écosystème dynamique d'opérateurs, de trafiquants, d'agrégateurs et de courtiers. Ces opérations reposent largement sur des utilisateurs non techniques, incités à distribuer des malwares et à convaincre les victimes de les exécuter elles-mêmes. En conséquence, la prééminence des groupes peut évoluer rapidement.

Les voleurs d'informations changent fréquemment de nom, se font concurrence pour attirer l'attention et font évoluer leurs offres de services, en intégrant des chargeurs, des packers, des crypters et des structures d'incitation destinées à séduire les groupes de trafiquants. Si leurs objectifs restent globalement les mêmes, la domination sur le marché dépend surtout de la portée de la distribution, du volume d'infection et de l'efficacité du modèle « malware-as-a-service », plutôt que de la seule innovation technique.

> *« Dans l'écosystème des infostealers, le succès repose davantage sur l'échelle et la distribution que sur la sophistication technique. C'est pourquoi des familles telles que Lumma ou RedLine continuent de dominer le marché grâce à des modèles solides de malware-as-a-service et à des infrastructures de distribution optimisées. »*
>
> **Borja Rodriguez**, Head of Threat Intelligence
> *Outpost24*

Agrégation des identifiants et économie des noms d'utilisateur, identifiants et mots de passe (ULP)

Les ensembles ULP (Usernames, Logins, Passwords) regroupent des identifiants issus de journaux de vol multiples, de violations historiques et d'autres sources de collecte. Contrairement aux journaux bruts, ces ensembles sont structurés pour une exploitation immédiate et incluent souvent les URL de connexion associées, ce qui facilite leur test, leur échange et leur réutilisation à grande échelle.

En 2025, l'équipe de renseignement sur les menaces d'Outpost24 a recensé 5 899 505 920 identifiants au sein d'ensembles de données ULP. Ce volume ne correspond pas aux mots de passe dérobés sur une seule année. Il reflète l'accumulation progressive d'identifiants compromis dans le temps, résultant de la consolidation de données issues de campagnes successives de malware et de violations historiques, regroupées dans des ensembles à longue durée de vie.

Cette augmentation ne traduit pas une rupture dans les techniques d'attaque. Elle révèle une évolution structurelle dans la gestion des identifiants volés. Les acteurs malveillants privilégient désormais le volume, la standardisation et la réutilisation. Ils agrègent des identifiants provenant de sources multiples au sein de jeux de données conçus pour être testés de manière répétée, revendus à grande échelle et exploités lors d'attaques ultérieures, bien après la compromission initiale.

Les changements apportés aux politiques de Telegram en 2025 ont également modifié les dynamiques de diffusion de ces ensembles. Si certains groupes de petite taille ont réduit leur activité ou migré vers d'autres plateformes, les grands canaux d'agrégation ont gagné en importance. Ils concentrent les journaux de vol et les ULP issus de sources multiples et s'imposent comme des points de distribution centralisés pour les identifiants compromis.

> *« L'essor de l'économie des ULP souligne un défi fondamental pour les défenseurs. Une fois les identifiants agrégés à cette échelle, l'exposition devient persistante plutôt qu'isolée, ce qui renforce la nécessité d'une visibilité continue sur les identifiants compromis, plutôt que de se fier uniquement à des contrôles ponctuels. »*
>
> **Alejandro Benito**, Threat intelligence Analyst
> *Outpost24*

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

Pour limiter les risques liés aux mots de passe, il ne suffit pas de se concentrer sur leur création : il faut également tenir compte de leur exposition et de leur réutilisation au fil du temps. La question n'est plus de savoir si un mot de passe respecte la politique lors de sa création, mais s'il demeure sûr dans un environnement où les identifiants volés sont régulièrement collectés et revendus.

Même dans les organisations qui adoptent une authentification sans mot de passe ou résistante au phishing, les mots de passe sont rarement complètement supprimés. Les identifiants existent souvent encore en arrière-plan pour prendre en charge les systèmes hérités, les comptes de service, l'authentification basée sur des répertoires ou les workflows de récupération. Par conséquent, l'exposition des mots de passe reste un risque réel, même lorsque les modèles d'authentification évoluent.

Réduire efficacement ces risques implique donc de mettre en place des contrôles compensatoires en partant du principe que les mots de passe continueront d'exister quelque part dans l'environnement. Cela passe par une détection continue, une gouvernance renforcée et des protections supplémentaires autour des identifiants, plutôt que de considérer l'exposition des mots de passe comme un problème résolu.

1. Bloquer en permanence les mots de passe compromis

Pour réduire ce risque, il est nécessaire d'avoir une visibilité continue sur les identifiants compromis, plutôt que de se fier uniquement à des contrôles ponctuels. Specops Password Policy avec Breached Password Protection permet une analyse continue des mots de passe AD par rapport à un ensemble de données de plus de cinq milliards de mots de passe compromis uniques, mis à jour quotidiennement via les honeypots, le renseignement sur les menaces et les fuites récemment découvertes. Lorsqu'un mot de passe compromis est détecté, l'utilisateur doit le modifier à sa prochaine connexion. Cela réduit la fenêtre d'exposition aux attaquants et améliore la visibilité sur l'ensemble du domaine.

2. Éliminer la création de mots de passe prévisibles

Les règles classiques de complexité permettent aux utilisateurs de respecter la politique tout en créant des mots de passe faciles à deviner, réutiliser ou exploiter une fois volés.

Pour limiter ce risque, il faut évaluer la structure des mots de passe, pas seulement la diversité des caractères. Bloquer les modèles faibles dès leur création ou modification réduit leur intégration dans des ensembles d'identifiants à grande échelle.

Cette approche permet aux organisations de diminuer le risque d'attaques par force brute, de réinitialisations frauduleuses et de contournements de politique. Elle réduit aussi la charge sur le support informatique et la réutilisation des identifiants.

3. Réduire l'exposition aux chemins d'accès à haut risque

Les VPN, RDP et autres points d'authentification externes sont des cibles privilégiées pour l'utilisation abusive des identifiants. Il est donc essentiel de renforcer les contrôles d'accès au-delà des mots de passe seuls. L'ajout de l'authentification multifactorielle (MFA) résistante au phishing réduit la valeur opérationnelle des identifiants volés et diminue la fréquence des incidents nécessitant une enquête manuelle.

Specops Secure Access applique cette MFA à la connexion Windows, au RDP et à l'accès VPN, assurant que les identifiants seuls ne permettent plus l'accès aux systèmes. Son mode hors ligne garantit le maintien de la MFA même en cas de perte de connectivité, empêchant tout retour à une authentification uniquement par mot de passe et répondant aux exigences de conformité telles que NIST et PCI.

4. Workflows sécurisés de réinitialisation et de récupération des mots de passe

Les processus de réinitialisation sont des cibles fréquentes d'ingénierie sociale ou de réutilisation de mots de passe, en particulier lorsque les attaquants possèdent déjà des informations partielles ou exposées.

Mettre en place une vérification rigoureuse de l'identité lors des réinitialisations en libre-service et via le service d'assistance réduit les risques de réinitialisations frauduleuses, de compromissions répétées et de piratage de comptes.

Specops uReset sécurise les réinitialisations de mot de passe en libre-service en vérifiant l'identité de l'utilisateur avant d'autoriser la modification des identifiants. Cela réduit les verrouillages de compte et les pratiques de réinitialisation non sécurisées.

Specops Secure Service Desk applique les mêmes contrôles aux réinitialisations et modifications effectuées par le service d'assistance, garantissant que les identifiants ne peuvent être réinitialisés avec des informations devinées ou compromises, tout en réduisant le volume d'appels, le temps de traitement et la charge financière sur le support informatique.

5. Ajouter la confiance des appareils pour réduire l'utilisation abusive des identifiants

Les identifiants ne suffisent pas à sécuriser l'accès. Même avec des politiques de mots de passe forts ou une MFA résistante au phishing, les identifiants volés restent précieux si les attaquants peuvent s'authentifier depuis leurs propres appareils ou des terminaux non gérés.

Ce risque concerne aussi bien les appareils gérés par l'entreprise que les environnements BYOD (Bring Your Own Device), où la visibilité et l'application des règles sont souvent limitées.

Infinipoint, qui fait partie du portefeuille d'identités de Specops Software, ajoute une couche de sécurité zéro confiance aux appareils en vérifiant à la fois l'utilisateur et

l'appareil au point d'accès et de manière continue tout au long de la session. L'accès est autorisé uniquement depuis des appareils approuvés et conformes, avec des contrôles en temps réel détectant logiciels obsolètes, protections désactivées ou menaces actives avant que les identifiants puissent être utilisés. Infinipoint propose également des options de correction automatiques et en libre-service pour les problèmes détectés sur les appareils, réduisant ainsi la charge du support informatique et la frustration des utilisateurs, qui limitent souvent l'efficacité des politiques traditionnelles d'accès conditionnel et de conformité.

Parlons-en

Découvrez comment les solutions Specops aident les organisations à prévenir l'exposition des mots de passe et à renforcer les contrôles d'identité et d'authentification.

Parlez à un expert