SPECOPS
AN OUTPOST24 COMPANY

# Specops 2025 Weak Password ReportBericht über kompromittierte Passwörter

Eine jährliche Analyse von durch Malware gestohlenen Zugangsdaten und Passwörter

# Inhalt

# Highlights

Die Daten für diesen Reportwurden durch KrakenLabs, dem Threat Intelligence-Team von Outpost24 (dem Mutterunternehmen von Specops Software), gesammelt. Insgesamt wurden 1,089,342,532 Passwörter, die über einen Zeitraum von 12 Monaten gestohlen wurden, für diesen Bericht analysiert. Die Daten sind aktuell bis Dezember 2024, wir erwarten jedoch, dass die allgemeinen Trends und Muster auch für 2025 konsistent bleiben. Der Bericht bezieht sich auch auf weitere Analysen, die von dem KrakenLabs-Team im Laufe des Jahres 2024 durchgeführt wurden.

Für den Report wurden über eine Milliarde, durch Malware gestohlene Zugangsdatenaus den letzten 12 Monaten analysiert.

**230 Millionen gestohlene Passwörter erfüllen die gängigsten Komplexitätsanforderungen**

- **Die drei häufigsten Beispiele:**
  - Pass@123
  - P@ssw0rd
  - Aa@123456

**Die fünf am häufigsten gestohlenen Passwörter:**

- 123456
- admin
- 12345678
- password
- Password

**Die häufigsten Basisbegriffe, die in gestohlenen Passwörtern gefunden wurden:**

- Fünf Buchstaben: admin
- Sechs Buchstaben: qwerty
- Sieben Buchstaben: welcome
- Acht Buchstaben: password

**Diese Passwortlängen waren am stärksten vertreten:**

- Acht Buchstaben (189 Millionen)
- Zehn Buchstaben (160 Millionen)
- Neun Buchstaben (153 Millionen)

**Die Top-3 Malware, mit denen Zugangsdaten gestohlen wurden:**

- Redline
- Vidar
- Raccoon Stealer

# Einleitung

Der Verizon Data Breach Investigations Report 2024 ergab, dass in den letzten 10 Jahren gestohlene Zugangsdaten die Ursache für fast ein Drittel (31%) aller Datenschutzverletzungen waren. Dies verdeutlicht die Wichtigkeit des Themas für Einzelpersonen als auch Organisationen. Gestohlene Anmeldeinformationen können letztendlich Angreifern unbefugten Zugang zu persönlichen Konten, Unternehmensnetzwerken und Zahlungsinformationen bieten, was wiederum zu Datenverlusten, finanziellen Verlusten sowie Reputationsschäden und Bußgeldern führen kann.

Über das vergangene Jahr hinweg hat unser Threat Intelligence-Team sorgfältig Daten zu diesem kritischen und anhaltend wachsenden Cybersecurity-Problem gesammelt und analysiert. In diesem Report finden Sie eine einzigartige Analyse von über einer Milliarde durch Malware gestohlener Anmeldeinformationen. So erhalten Sie ein besseres Verständnis über die von Endbenutzern gewählten (und oftmals wiederverwendeten) Passwörtern, der Art und Weise, wie diese Infostealer-Infektionen durchgeführt werden, und den Gegenmaßnahmen, die ergriffen werden können.

Die gesammelten Daten bieten einen umfassenden Überblick über die aktuelle Bedrohungslage rund um Infostealer und betonen das Ausmaß der Bedrohung. Ein Blick auf die Trends und Muster, die sich bei den analysierten Passwörtern abzeichnen, hilft, ein Bild der von Nutzern erstellten Passwörter abzuleiten und zeigt, wo Organisationen ihre Passwortrichtlinien möglicherweise verstärken müssen.

Durch die Analyse realer Passwortinformationen und der von Angreifern verwendeten Techniken hoffen wir, Ihnen handfeste Erkenntnisse und Empfehlungen zur Verbesserung Ihrer Sicherheitsmaßnahmen und -prozesse zum Schutz vor durch Malware gestohlenen Zugangsdaten zu geben.

# Trends und Muster in schwachen Passwörtern

Die Nutzung von Threat Intelligence-Tools zur Analyse gestohlener Passwörter bietet uns die Möglichkeit, Passwörter zu untersuchen, die von Nutzern aktuell verwendet, und von Cyberkriminellen gestohlen werden. Eine Umfrage von LastPass ergab, dass 91% der Endbenutzer sich der Risiken des Wiederverwendens derselben Passwörter für mehrere Konten bewusst sind, aber 59% dies dennoch tun.

Dies bedeutet, dass es eine reelle Chance gibt, dass gestohlene, private Anmeldeinformationen auch als Active Directory-Passwörter in Organisationen weltweit verwendet werden. Die folgenden Trends und Muster unterstreichen, wie schwach viele Passwörter immer noch sind, und wo Passwortrichtlinien in Organisationen möglicherweise verstärkt werden müssen.

## Die häufigsten kompromittierten Passwörter und deren Basisbegriffe

Wie unten zu sehen ist, tauchen Passwörter wie 123456, admin und password immer noch mit beunruhigender Regelmäßigkeit auf. Dies verdeutlicht, dass Organisationen Nutzern das Erstellen schwacher Active Directory-Passwörter via Passwortfilter und starker Passwortrichtlinien verbieten müssen. Ansonsten greifen Nutzer auf schwache Passwörter zurück, wenn ihnen die Möglichkeit dafür gegeben wird.

| Die fünf häufigsten Passwörter | Anzahl der Funde in der Stichprobe |
|---|---|
| 123456 | 3.7 million |
| admin | 1.9 million |
| 12345678 | 1.5 million |
| password | 558,000 |
| Password | 474,000 |

Aus der Analyse von einer Milliarde Passwörtern tauchten einige gängige Grundbegriffe millionenfach auf. Trotz der Forderung einzigartige Passwörter zu erstellen, zeigen die untenstehenden Daten, dass Nutzer weiterhin schwache und leicht zu erratende Grundbegriffe für ihre Passwörter verwenden. Wörter wie “guest” und “student” deuten darauf hin, dass viele Endbenutzer temporäre Trainings- und Initialpasswörter beibehalten oder wiederverwenden. Menschen greifen auch oft zu Tastaturmuster wie “qwerty”, „qwertz“ und “azerty”. Beispielsweise sahen wir, dass “Pakistan” häufig auf pakistanischen Regierungswebseiten sowie auf allgemeinen Seiten wie Facebook, Amazon und Netflix verwendet wurde.

| Häufigsten Basisbegriffe mit fünf Zeichen |
|---|
| admin |
| guest |
| hello |

| Häufigsten Basisbegriffe mit sechs Zeichen |
|---|
| qwerty |
| secret |
| azerty |

| Häufigsten Basisbegriffe mit sieben Zeichen |
|---|
| welcome |
| zxcvbnm |
| student |

| Häufigsten Basisbegriffe mit acht Zeichen |
|---|
| password |
| adminisp |
| pakistan |

## Schützen längere Passwörter vor Kompromittierung?

Die untenstehende Tabelle zeigt die verschiedenen Längen der gestohlenen Passwörter. Acht Zeichen war die häufigste Passwortlänge, was wahrscheinlich auf die aktuell noch gängigen Anforderungen an Passwörtern zurückzuführen ist. Wir haben auch die drei am häufigsten kompromittierten Passwörter für jede Passwortlänge aufgelistet. In diesen Daten kann man sehen, wie Endbenutzer oft kürzere Grundbegriffe nehmen und dann inkrementell Zahlen ans Ende hinzufügen.

| Passwortlänge | Anzahl der in der Sitchprobe | Top-3 am häufigsten kompromittierten Passwörter |
|---|---|---|
| 6 | 43.6 million | 123456<br>000000<br>123123 |
| 7 | 26 million | 1234567<br>a123456<br>welcome |
| 8 | 189 million | 12345678<br>Password<br>Password |
| 9 | 153 million | 123456789<br>Aa@123456<br>Admin@123 |
| 10 | 160 million | 1234567890<br>qwertyuiop<br>987654321 |
| 11 | 115 million | 12345678910<br>Welcome@123<br>qwerty12345 |
| 12 | 92 million | admintelecom<br>Password@123<br>Pakistan@123 |

## Wie viele kompromittierten Passwörter erfüllen gängige Komplexitätsanforderungen?

Von den über einer Milliarde durch Malware gestohlenen Passwörter, die analysiert wurden, würden fast ein Viertel (230 Millionen) als ausreichend komplex betrachtet werden. Das bedeutet, sie würden die Standardanforderungen (auch die in Active Directory im Bezug auf Komplexitätsanforderungen) erfüllen, die viele Organisationen festlegen:

- Mindestens acht Zeichen
- Ein Großbuchstabe
- Eine Zahl
- Ein Sonderzeichen

Wie man an den am häufigsten gestohlenen "komplexen" Passwörtern unten sehen kann, passen Nutzer oft gängige Begriffe an, indem sie Großbuchstaben, Zahlen oder Sonderzeichen an vorhersagbaren Stellen hinzufügen (in der Regel mit einem Großbuchstaben am Anfang und aufsteigenden Zahlen oder Sonderzeichen am Ende). Diese Passwörter könnten durch entsprechende Algorithmen bei Brute-Force-Versuchen schneller erraten werden, da sie einfachen und vorhersagbaren Mustern folgen. Aus diesem Grund bewegen sich Compliance-Standards wie NIST von Komplexitätsanforderungen weg und richten sich stattdessen auf die Verlängerung der Passwörter.

Dies zeigt auch, dass ein Passwort, welches Komplexitätsstandards erfüllt, nicht automatisch „sicher" ist. Letztendlich kann jedes Passwort durch Malware gestohlen und kompromittiert werden – unabhängig von Länge oder Komplexität. Daher ist es wichtig, dass selbst bei strengen Passwortrichtlinien eine regelmäßige Überprüfung der Passwörter auf Kompromittierung durchgeführt wird.

| Die am häufigsten vorkommenden Passwörter, die die Komplexitätsregeln vieler Organisationen erfüllen würden |
|---|
| Pass@123 |
| P@ssw0rd |
| Aa@123456 |
| Admin@123 |
| Aa123456@ |
| Pass@1234 |
| Abcd@1234 |
| Demo@123 |
| Password@123 |
| India@123 |

## Specops-Tipp: Schwache Passwörter mithilfe einer Passwort-Blocklist sperren

Selbst nach Jahrzehnten von Sicherheitsschulungen und Cyberangriffen vergeben Nutzer weiterhin schwache Passwörter. Das kann man ihnen auch nicht unbedingt vorwerfen, da es menschliche Natur ist, den Weg des geringsten Widerstands zu wählen. Das kann ein leicht zu merkender Grundbegriff für ein Passwort oder aber eine geringfügige Anpassung eines vorherigen Passworts (um strengeren Anforderungen zu entsprechen) sein. Daher wählen Nutzer bequeme und für sie benutzerfreundliche Passwörter, auch wenn diese aus sicherheitstechnischer Sicht nicht optimal sind.

Inspiriert von den Olympischen Spielen in Paris hat unser Analystenteam am Anfang des Jahres herausgefunden, dass in den vorangegangenen 12 Monaten 157.048 sportbezogene Passwörter durch Malware kompromittiert wurden. Am häufigsten wurden Passwörter zum Thema Golf gestohlen, nämlich in 40.294 Fällen. Es folgte Fußball mit 20.550 Fällen. Zwar ist Sport ein generisches Thema in dieser Studie gewesen, aber schwache oder leicht erratbare Grundbegriffe werden zum Problem, wenn Benutzer spezifische Passwörter mit Bezug auf ihre Rolle, Abteilung oder Organisation wählen, da Hacker diese bei einem gezielten Angriff mit großer Wahrscheinlichkeit ausprobieren werden.

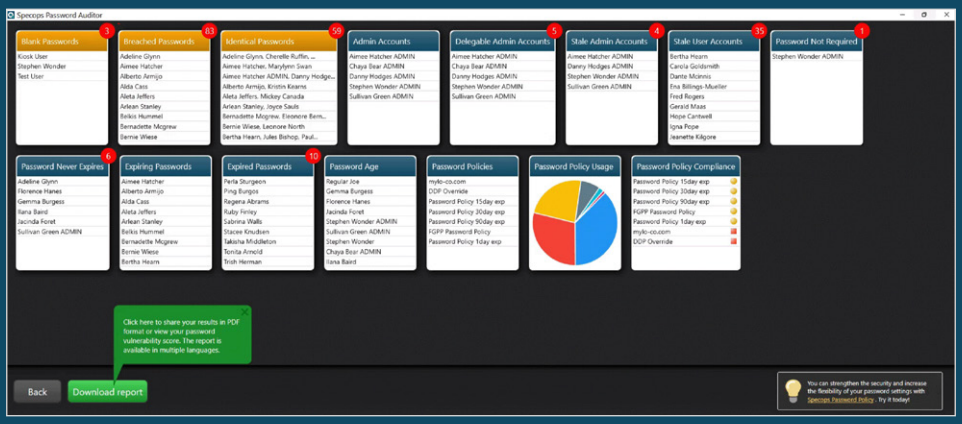
Das Erstellen einer individuellen Ausschlussliste für Ihre Organisation ist eine hervorragende Möglichkeit, Benutzer daran zu hindern, schwache oder leicht zu erratenden Grundbegriffe zu wählen. Mithilfe von AI-Tools wie ChatGPT, Leak-Listen und Studien wie dieser, können Sie erste Inspirationen und Einträge für solche Listen sammeln. Dies wird helfen, ein umfassendes und robustes Wörterbuch zu erstellen, das regelmäßig verfeinert werden kann.

## Schlummern bereits kompromittierte Kennwörter in Ihrem Active Directory? Starten Sie noch heute eine erste Analyse!

Der Weg zu stärkeren Passwörtern beginnt mit einer Analyse des Ist-Zustands. Mit dem kostenlosen Specops Password Auditor, können Sie innerhalb von wenigen Minuten eine Reihe von passwortrelevanten Schwachstellen identifizieren. Dabei unterstützt ein Read-Only-Scan Ihres Active Directory über 1 Milliarde kompromittierte Passwörter zu identifizieren sowie Ihre aktuellen Passwortrichtlinien mit Industriestandards und Empfehlungen von Behörden zu vergleichen.

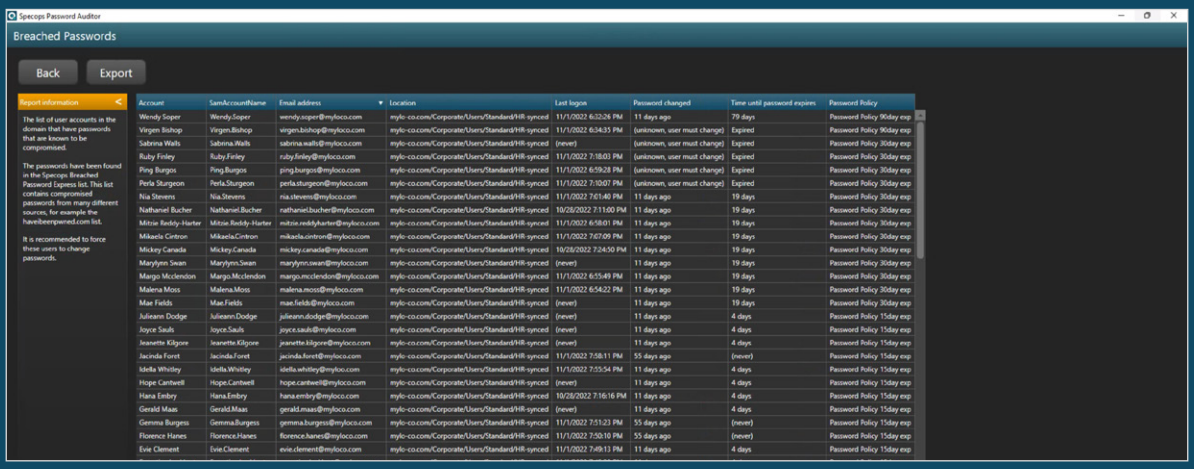
Die interaktiven und exportbierbaren Reports geben erste Einblicke in folgende Bedrohungen:

- Kompromittierte Passwörter
- Leere Passwörter
- Identische Passwörter
- Veraltete Admin-Konten
- Konten, bei denen kein Passwort erforderlich ist
- Verwaiste Benutzerkonten
- Konten, bei denen das Passwort nie abläuft
- Abgelaufene Passwörter
- Passwortrichtlinien und -nutzung
- Einhaltung der Passwortrichtlinien




*Specops Password Auditor: Übersicht der Ergebnisse*

Denken Sie daran, besondere Aufmerksamkeit den Nutzern zu schenken, die bereits kompromittierte Passwörter verwenden, da diese Konten Angreifern einen einfachen Weg in Ihre Organisation bieten.




*Specops Password Auditor: Bericht, der Endbenutzer mit bereits kompromittierten Passwörtern zeigt*

**Holen Sie sich Ihr kostenloses Auditing-Tool.**

# Wie Malware von Cyberkriminellen genutzt wird, um Anmeldeinformationen zu stehlen

In den Untergrundforen sind gestohlene Zugangsdaten sehr gefragt. Sie bieten einen einfachen und direkten Weg zu oftmals wertvollen Daten, einschließlich persönlicher Informationen, Finanzdetails und Geschäftsgeheimnissen. Initial Access Brokers (IABs) spezialisieren sich darauf, gestohlene Anmeldeinformationen im Dark Web und auf unterirdischen Foren zu verifizieren und Zugänge zu Unternehmen gewinnbringend zu handeln. Für Organisationen ohne Zugang zu Threat Intelligence-Tools ist es schwierig zu wissen, ob die Anmeldeinformationen ihrer Benutzer auf solchen Foren und Marktplätzen angeboten werden.

Gestohlene Zugangsdaten können auch verwendet werden, um zusätzliche Angriffskanäle, wie Phishing-Kampagnen oder Ransomware-Angriffe, zu eröffnen. Sobald ein Angreifer mit gestohlenen Anmeldeinformationen unbemerkt Zugang zu einem System erhält, kann er damit beginnen, sich im System auszubreiten und sich einzunisten. Dies ermöglicht es ihm, im Laufe der Zeit mehr Daten zu sammeln und potenziell innerhalb des Netzwerks lateral zu agieren, um auf zusätzliche Systeme zuzugreifen. Gültige Zugangsdaten, die eine vertrauenswürdige Identität darstellen, machen es für Sicherheitssoftware schwieriger, solche Aktivitäten als bösartig zu erkennen.

## So funktionieren Infostealer

Um bessere Sicherheits- und Gegenmaßnahmen zu erarbeiten, ist es wichtig zu verstehen, wie Infostealer funktionieren. Vorweg ist zu sagen, dass es wichtig ist, Software regelmäßig zu aktualisieren, starke und einzigartige Passwörter zu verwenden und Multifaktor-Authentifizierung (MFA) einzusetzen. Zudem können regelmäßige Sicherheitsaudits und -überwachungen helfen, die Anwesenheit von Infostealern zu erkennen. Hier eine allgemeine Übersicht über die Vorgehensweise von Infostealer-Infektionen:

**1. Infektion:** Infostealer können ein System auf verschiedene Weise infizieren, wie zum Beispiel durch Phishing-E-Mails, bösartige Downloads oder der Ausnutzung von Software-Schwachstellen. Sobald die Malware ausgeführt wird, beginnt die Infiltration des Systems.

**2. Persistenz:** Um sicherzustellen, dass sie über eine längere Zeitspanne hinweg Daten sammeln können, etablieren Infostealer oft Persistenzmechanismen. Dazu können folgende Maßnahmen gehören:

**3. Datensammlung:** Infostealer suchen und sammeln verschiedene Arten sensibler Informationen. Bei Anmeldeinformationen zielen sie typischerweise auf folgende Ziele ab:

- **Webbrowser**: Sie extrahieren gespeicherte Passwörter, Cookies und Autocomplete-Daten aus Webbrowsern wie Chrome, Firefox und Edge.
- **E-Mail-Clients**: Sie stehlen Anmeldeinformationen und andere Daten aus E-Mail-Clients wie Outlook.
- **FTP-Clients**: Sie greifen zu und stehlen Anmeldeinformationen, die in FTP-Clients gespeichert sind.
- **Dateisysteme**: Sie durchsuchen das Dateisystem nach Anmeldeinformationen in Konfigurationsdateien, Textdateien und anderen Datenspeicherorten.
- **Zwischenablage**: Sie überwachen die Zwischenablage, um sensible Informationen zu erfassen, die kopiert und eingefügt werden.

**4. Exfiltration:** Sobald die Daten gesammelt wurden, müssen Infostealer sie an den Angreifer senden. Dies kann auf verschiedene Weise erfolgen:

- **HTTP/HTTPS-Anfragen**: Sie senden die Daten an einen Remote-Server über Web-Protokolle.
- **E-Mail**: Sie senden die Daten per E-Mail an den Angreifer.
- **FTP**: Sie laden die Daten auf einen FTP-Server hoch.
- **Command and Control (C2) Server**: Sie kommunizieren mit C2-Servern, um die Daten zu senden und weitere Anweisungen zu erhalten.

**5. Vermeidung der Erkennung:** Um der Erkennung zu entgehen, verwenden Infostealer oft Techniken, um Antivirus-Software und andere Sicherheitsmaßnahmen zu umgehen. Dazu können folgende Methoden gehören:

- **Code-Obfuscation**: Das Malware-Code wird so verändert, dass er schwer zu lesen und zu analysieren ist.

- **Packing**: Das Malware wird komprimiert, um die Identifizierung zu erschweren.
- **Rootkit-Techniken**: Die Malware versteckt seine Anwesenheit im System.
- **Heimliche Kommunikation**: Es werden verschlüsselte oder versteckte Kommunikationskanäle verwendet, um Netzwerküberwachung zu vermeiden.

**6. Ausführung:** Infostealer können so programmiert sein, dass sie zu bestimmten Zeiten oder unter bestimmten Bedingungen ausgeführt werden. Zum Beispiel könnten sie nur aktiv werden, wenn der Benutzer das Computer nicht aktiv nutzt.

## Die beliebteste Malware zu Diebstahl von Zugangsdaten

Analysen von Specops zeigen, dass Redline das bevorzugte Tool für den Diebstahl von Passwörtern ist und für fast die Hälfte aller analysierten gestohlenen Passwörter verantwortlich ist. In unserer Datenbank hatten Hacker mit Redline 170 Millionen einzigartige Anmeldeinformationen innerhalb von nur 6 Monaten gestohlen. Vidar und Raccoon Stealer sind ebenfalls nennenswert und tragen jeweils 17% und 11,7% der gestohlenen Passwörter unserer Stichprobe bei. Hier sind weitere Informationen zu den Top-3 Stealern:

### 1. Redline

Redline ist ein extrem beliebter Stealer. Es wurde erstmals im März 2020 entdeckt, und sein Hauptziel ist es, alle Arten persönlicher Informationen wie Anmeldeinformationen, Kryptowallets und Finanzinformationen zu exportieren und diese dann an die C2-Infrastruktur der Angreifer hochzuladen. In vielen Fällen wird eine Redline-Payload zusammen mit einem Krypto-Miner auf dem System des Opfers installiert. Dies ist besonders in Kampagnen, bei denen Gamer mit leistungsstarken GPUs das Ziel sind, lukrativ..

**Seit Mitte 2021 wird YouTube auch als Verteilungsmethode für Redline verwendet, wobei der Prozess wie folgt abläuft:**

- Zunächst kompromittiert der Angreifer ein Google/YouTube-Konto.
- Sobald das Konto kompromittiert ist, erstellt er damit verschiedene Kanäle oder veröffentlicht direkt Videos auf ihnen.
- In der Beschreibung der hochgeladenen Videos (meist solche, die Cheats und Cracks für Spiele werben und Anleitungen zum Hacken beliebter Spiele und Software bieten), fügen Angreifer einen bösartigen Link ein, der zum Thema des Videos passt.
- Benutzer klicken auf den Link, um den Cheat oder Crack herunterzuladen und laden zusätzlich auch Redline unbewusst auf ihre Geräten herunter, was dazu führt, dass ihre Passwörter und andere private Informationen gestohlen werden.

### 2. Vidar

Vidar ist eine Weiterentwicklung des bekannten Arkei Stealers. Es überprüft die Spracheinstellungen des infizierten Rechners, um bestimmte Länder für weitere Infektionen auf die Whitelist zu setzen. Danach generiert es ein Mutex und initialisiert die für den Betrieb notwendigen Befehlsketten. Es gibt zwei verschiedene C2-Versionen, die Hackern zur Verfügung stehen. Die ursprüngliche Version ist mit der bezahlten Version von Vidar, Vidar Pro, verbunden. Es gibt auch eine andere C2-Version, die in der geknackten Version von Vidar verwendet wird, die in Untergrund-Foren verteilt wird; diese wird als Anti-Vidar bezeichnet.

Im Frühjahr 2022 wurde Vidar in Phishing-Kampagnen als Microsoft Compiled HTML Help (CHM)-Dateien entdeckt. Zudem wurde festgestellt, dass die Malware über den PPI-Malware-Dienst PrivateLoader, das Fallout Exploit Kit und den Colibri Loader verteilt wird. Ende 2023 wurde die Malware auch durch den GHOSTPULSE Malware-Loader verbreitet.

### 3. Raccoon Stealer

Raccoon Stealer ist eine Infostealer-Malware, die im Darknet zum Verkauf angeboten wird. Das Team hinter Raccoon Stealer verwendet ein 'Malware-as-a-Service'-Modell, das es Kunden ermöglicht, den Stealer monatlich zu mieten. Es wurde erstmals am 8. April 2019 auf dem führenden russischsprachigen Forum Exploit zum Verkauf angeboten. Raccoon Stealer wird mit der Werbespruch "Wir stehlen, du handelst!" beworben.

Hauptsächlich wird es auf russischsprachigen Untergrund-Foren wie Exploit und WWH-Club zum Verkauf angeboten. Am 20. Oktober 2019 begann der Threat-Actor auch, Raccoon Stealer auf dem berüchtigten englischsprachigen Hack Forums anzubieten. Dabei wird auch erwähnt, dass sogenannte „Testwochen" möglich sind, was darauf hindeuten kann, dass mögliche Angreifer das Produkt in einem Trialzeitraum testen können.

Der Betreiber hinter Raccoon Stealer wurde kürzlich gefasst und zu fünf Jahren Haft verurteilt.

## Kann Malware Active Directory-Passwörter stehlen?

Oftmals sind Nutzer, die ihre Active Directory-Anmeldeinformationen in Browsern oder Anwendungen wie FileZilla speichern anfällig für Credential Stealer. Active Directory-Anmeldeinformationen stimmen oft mit denen überein, die in Microsoft 365/Outlook verwendet werden, da sie von Entra ID (früher Azure AD), einem cloudbasierten Verzeichnis das mit dem lokalen AD synchronisiert ist, verwaltet werden. Viele Organisationen implementieren auch Single Sign-On (SSO), was diese Systeme noch stärker verknüpft.

Unsere Forscher haben kürzlich über zwei Millionen VPN-Passwörter entdeckt, die durch Malware kompromittiert wurden, was ein erhebliches Sicherheitsrisiko für Organisationen darstellt. Diese Passwörter, die für den Benutzerzugriff auf VPNs essentiell sind, dienen nun als potenzielle Einstiegspunkte für Cyberkriminelle, was den Hauptzweck von VPNs, die Kommunikation durch Datenverschlüsselung zu sichern und zu privat zu halten, untergräbt. Das größte Risiko entsteht, wenn Active Directory-Passwörter auch als VPN-Passwörter verwendet werden, da dies Angreifern ermöglichen könnte, auf alle Systeme und Ressourcen zuzugreifen, zu denen der Benutzer Berechtigungen hat. Das kann zu erheblichen Schäden und Datendiebstählen führen.

## Specops-Tipps: So jagen Sie gestohlene Zugangsdaten Ihrer Nutzer im Dark Web

Threat Intelligence-Teams können Organisationen helfen, festzustellen, ob die Anmeldeinformationen ihrer Benutzer kompromittiert und im Dark Web zum Verkauf angeboten werden. Dies ermöglicht es den Organisationen, sofortige Maßnahmen zu ergreifen, um die betroffenen Konten zu sichern, indem sie die Benutzer auffordern, ihre Passwörter zu ändern. Durch Eindringen in Botnets, dem Abfangen von Kommunikation und Insider-Informationen aus Untergrund-Foren, können TI-Analysten Bedrohungsinformationen zu gestohlenen Passwörtern sammeln.

Auch Specops nutzt solche Informationsquellen, um die umfangreiche Datenbank mit über 4 Milliarden einzigartigen kompromittierten Passwörtern zu aktualisieren. Informationen aus unserem internen TI-Team KrakenLabs hilft also direkt dabei, die Gefahr durch gestohlene oder anderweitig kompromittierte Passwörter zu verringern.

# Wie können Unternehmen das Kennwortrisiko verringern?

Wie können Organisationen die Gefahr durch kompromittierte Passwörter wirkungsvoll reduzieren? Es gibt zwei wesentliche Methoden, mit denen Organisationen ihre Passwortsicherheit verbessern können. Erstens sollten Sie sicherstellen, dass Ihr Active Directory mit langen und komplexen Passwörtern gefüllt ist, die widerstandsfähig gegen Brute-Force-Angriffe sind. Zweitens ist es wichtig, ein Tool zu verwenden, das nach Passwörtern sucht, die unbemerkt kompromittiert wurden.

### Lange, starke Passwörter erzwingen

Unser Forschungsteam hat die Stärke des SHA-256-Hashing-Algorithmus aktuellen Techniken zum Erraten von Passwörtern gegenübergestellt. Obwohl es nicht der fortschrittlichste Algorithmus ist, wird er in vielen Umgebungen weiterhin verwendet. Hier ist oftmals die Wiederverwendung von Passwörtern das Hauptproblem, da berufliche Passwörter der Benutzer zwar auf sichere Weise gespeichert sein können, aber sobald sie diese auf weniger sicheren Websites wiederverwenden werden und diese Websites dann kompromittiert werden, können Angreifer mithilfe von Credential Spraying versuchen, in Ihr Netzwerk einzudringen.

Wie die folgende Tabelle aus unserer Analyse zeigt, kann selbst ein relativ moderner Algorithmus wie SHA-256 kurze, einfache Passwörter nicht vor Brute-Force-Angriffen schützen. Andererseits zeigt die Tabelle auch, dass ein Hacker wahrscheinlich seine Zeit verschwendet, wenn er versucht, ein langes, komplexes Passwort zu knacken, das mit SHA-256 gehasht wurde.

## Zeit zum Knacken: Mit SHA-256 gehashte Passwörter

| 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 |

Angreifer werden immer lieber nach leichten Zielen suchen. Zum Beispiel Active Directory-Passwörter, die bereits bei Datenleaks kompromittiert wurden. Ein Weg, wie dies passieren kann, ist das Wiederverwenden von Passwörtern. Sie können Ihre Endbenutzer dazu ermutigen, lange, starke Active Directory-Passwörter zu erstellen und diese sehr sicher zu speichern. Aber diese Arbeit wird zunichtegemacht, wenn Nutzer diese starken Passwörter dann auf unsicheren Endgeräten oder Anwendungen wiederverwenden.

## Zeit zum Knacken: Bekannte kompromittierte Passwörter

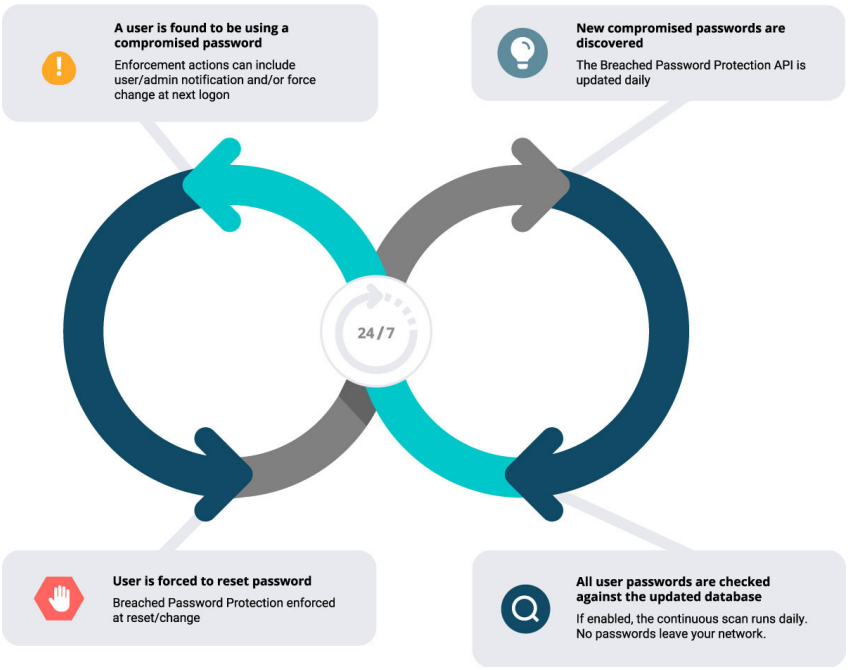
| Number of characters | Numbers Only | Lowercase Only | Upper and Lower | Number, Upper, Lower | Number, Upper, Lower, Symbols |
|---|---|---|---|---|---|
| 6 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 7 | Instantly | Instantly | Instantly | Instantly | Instantly |
| 8 | Instantly | 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 |

## Kontinuierliche Überwachung auf kompromittierte Kennwörter

Die kontinuierliche Scan-Funktion von Specops Password Policy überprüft die Passwörter Ihrer Benutzer in Active Direktory täglich. Indem wir unsere Breached Password Protection-Datenbank regelmäßig mit neuen Informationen von unseren Honeypots, gefunden Datenleaks und Input aus unserem TI-Team erweitern, stellen wir sicher, dass diese Datenbank immer auf dem aktuellen Stand ist.

So können Sie proaktiv kompromittierte Passwörter in Ihrer Organisation identifizieren und Ihre Benutzer auffordern diese zu ändern. Dadurch wird auch die Gefahr durch die Wiederverwendung von Passwörtern verringert.

Specops Password Policy ermöglicht es Ihnen auch starke und benutzerfreundliche Passwortrichtlinien umzusetzen, um die Einhaltung von Branchenstandards und regulatorischen Anforderungen sicherzustellen. Die Ergebnisse der kontinuierlichen Scans können leicht überprüft werden und geben einen klaren Überblick über kompromittierte Passwörter in einem Netzwerk.




*Specops Breached Password Protection kontinuierliche Scan-Funktion*

Fordern Sie noch heute eine kostenlose Demo von Specops Password Policy an!

**Demo von Specops Password Policy**

# Acht wichtige Erkenntnisse

1. Durch Malware-gestohlene Anmeldeinformationen sind weit verbreitet, innerhalb von 12 Monaten konnten wir über eine Milliarde finden.

2. Trotz bekannter Risiken erstellen Nutzer, wenn es ihnen gestattet wird, weiterhin kurze, schwache Passwörter wie ‘password’, ‘12345’ und ‘admin’. Daher ist es essentiell, dass die Verwendung schwacher Grundbegriffe in den Passwortrichtlinien von Organisationen verhindert wird.

3. Komplexitätsanforderungen sind kein Garant für Sicherheit, da Passwörter oftmals durch Malware kompromittiert werden und nicht nur durch pures Brute-Forcing. Aus einer Stichprobe aus einer Milliarden Passwörter erfüllten ca. 230 Millionen gängige Komplexitätsanforderungen.

4. ‘Komplexe’ Passwörter können aufgrund des Benutzerverhaltens und Muster bei der Erstellung von Passwörtern immer noch vorhersagbar sein. Länge ist ein besserer Indikator für die Stärke von Passwörtern.

5. Hacker bevorzugen durch Malware gestohlene Anmeldeinformationen, da sie einfach zu erlangen, zu verwenden und zu verkaufen sind. Redline ist laut unseren Nachforschungen der beliebteste Stealer.

6. Sogar starke Passwörter können durch Malware gestohlen werden, was Hashing-Algorithmen überflüssig macht. Daher sollten alle Nutzeraccounts durch MFA gesichert sein.

7. Malware ist auch einer der Gründe, warum die Wiederverwendung von Passwörtern auf unsicheren privaten Anwendungen und Geräten eine Gefahr für die Sicherheit von Unternehmensnetzwerken darstellt.

8. Eine regelmäßige Überwachung der Passwörter in Active Directory ist daher ein entscheidender erster Schritt, um Passwörter wieder zu einem vertrauenswürdigen Authentifizierungsfaktor zu machen.

# ÜBER SPECOPS SOFTWARE GMBH

Specops Software, ein Outpost24 Unternehmen, ist der führende Anbieter von Passwort-Management- und Authentifizierungslösungen. Specops Software schützt Ihre Geschäftsdaten, indem es schwache Passwörter blockiert und die Benutzerauthentifizierung sichert. Mit einem kompletten Portfolio von Lösungen, die nativ in Active Directory integriert sind, stellt Specops sicher, dass sensible Daten vor Ort und unter Ihrer Kontrolle gespeichert werden. Specops Software wurde 2001 gegründet und hat seinen Hauptsitz in Stockholm, Schweden, sowie weitere Niederlassungen in den USA, in Kanada, Großbritannien, Frankreich und Deutschland.

DEMO BUCHEN >>

INDIVIDUELLE PREISE ANFORDERN >>

## KONTAKTIEREN SIE UNS


**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