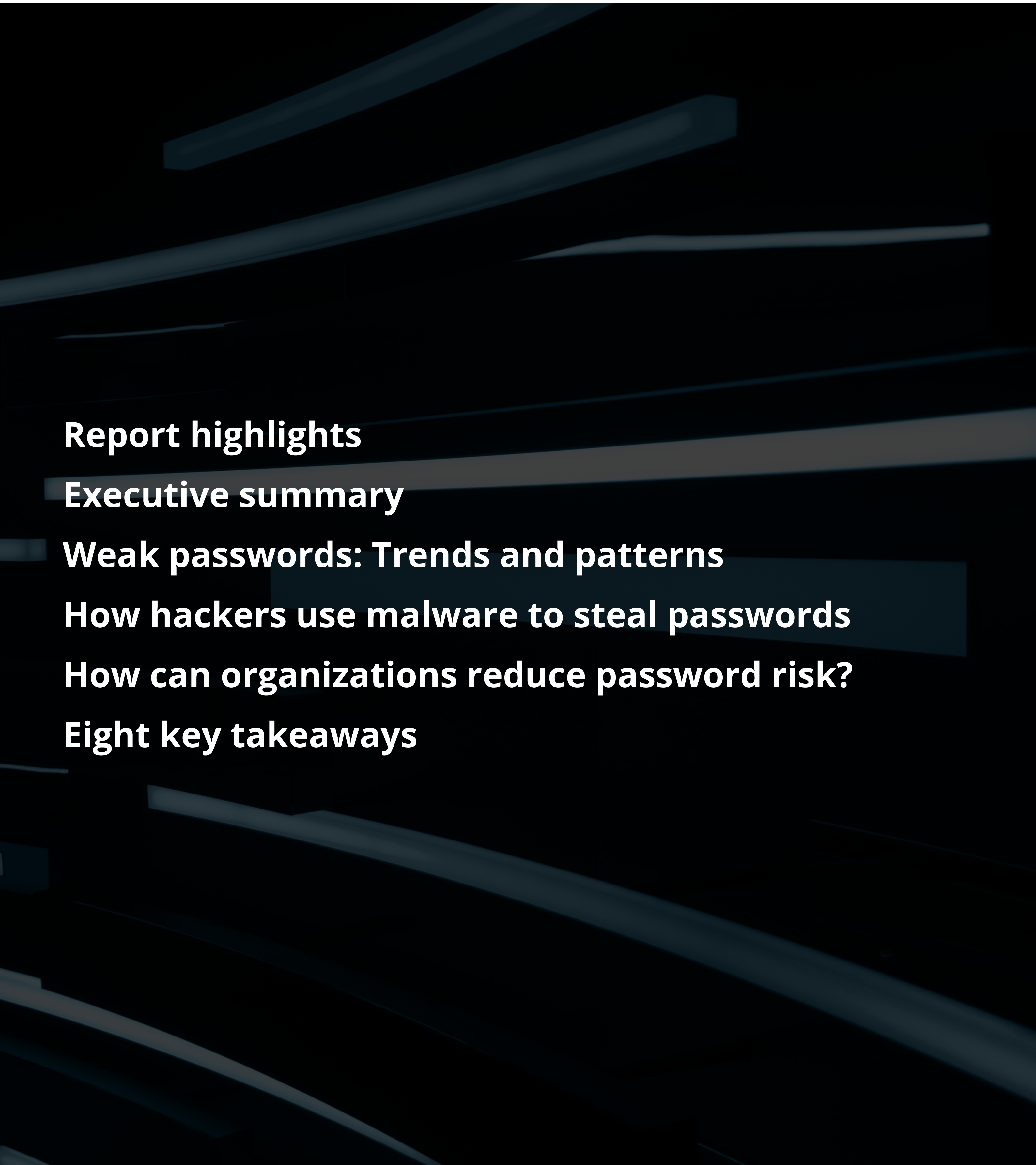
SPECOPS
AN OUTPOST24 COMPANY

Specops breached password report 2025

Analyzing a year's worth of malware-stolen credentials

What’s inside?



Report highlights

Data in this report comes from KrakenLabs, the Threat Intelligence team at Outpost24 (Specops Software's parent company). In total, 1,089,342,532 stolen passwords captured over a 12-month period were analyzed for this report. The data is accurate as of December 2024, however, we expect the overall trends and patterns to remain consistent. The report also references other pieces of individual research carried out by the KrakenLabs teams throughout 2024.

Over **one billion** credentials stolen by malware over a 12-month period analyzed

230 million stolen passwords meet standard complexity requirements

- **Three most common examples**
  - Pass@123
  - P@ssw0rd
  - Aa@123456

Top five stolen passwords:

- 123456
- admin
- 12345678
- password
- Password

Most common base terms found in stolen passwords:

- Five characters: admin
- Six characters: qwerty
- Seven characters: welcome
- Eight characters: password

Top three stolen password lengths

- Eight characters (189 million)
- Ten characters (160 million)
- Nine characters (153 million)

Most used credential-stealing malware?

- Redline
- Vidar
- Raccoon Stealer

Executive summary

Verizon's 2024 Data Breach Investigations Report found that over the past 10 years, the use of stolen credentials has appeared in almost one-third (31%) of all breaches. This prevalence of credential theft has had significant implications for both individuals and organizations. Stolen credentials can lead to unauthorized access to personal accounts, corporate networks, and financial systems, resulting in data breaches, financial losses, and reputational damage.

Over the past year, our threat intelligence team has meticulously gathered and analyzed data on a critical and growing cybersecurity issue: the theft of credentials via malware. This report offers unique analysis into over one billion malware-stolen credentials, helping to equip organizations with a deeper understanding of the passwords end users are choosing (and reusing), how these attacks are carried out, and the measures that can be taken to mitigate the risks.

The data collected provides a comprehensive overview of the current credential theft landscape, highlighting the sophistication and persistence of these threats. Looking into the trends and patterns of these stolen passwords helps build a picture of the passwords real end users are creating and informs where organizations' password policies may need strengthening. We'll also dig into the methods, trends, and impacts of infostealers and other types of malware that are specifically designed to steal sensitive information such as usernames, passwords, and other authentication data.

By examining real-world password data and analyzing the techniques used by attackers, we hope to provide you with actionable insights and recommendations to enhance your security protocols and protect against the threat of malware-stolen credentials.

Weak passwords: Trends and patterns

Using Threat Intelligence tools to analyze stolen passwords gives us the opportunity to look at the passwords real end users are creating – and real cybercriminals are stealing. A LastPass survey found 91% of end users say they understand the risks of using the same passwords across multiple accounts, but 59% did so anyway.

This means there's a real chance these stolen credentials are also in use as Active Directory passwords within organizations around the world. These trends and patterns highlight how weak a lot of passwords out there still are, and where your own password policy might need strengthening.

Most common weak passwords and base terms

As you can see below, passwords like 123456, admin, and password still show up with depressing regularity. The below table lists the number of exact matches for the five most commonly stolen passwords. This shows the importance of organizations blocking end users from creating weak Active Directory passwords – as if given the chance, many end users will still choose to do so.

Top five stolen passwords	Number of exact matches
123456	3.7 million
admin	1.9 million
12345678	1.5 million
password	558,000
Password	474,000

Out of the billion passwords analyzed, some common base terms cropped up millions of times. Despite being encouraged to create unique passwords, the data below shows end users still use weak and easily-guessed base terms to build their passwords. Words like guest and student suggest many end users are keeping or reusing temporary training and first day passwords. People also still often go for keyboard walks like qwerty and azerty. We also saw Pakistan commonly used across Pakistani government websites as well as general sites such as Facebook, Amazon, and Netflix.

Most common five character base terms
admin
guest
hello

Most common six character base terms
qwerty
secret
azerty

Most common seven character base terms
welcome
zxcvbnm
student

Most common eight character base terms
password
adminisp
pakistan

Most common password lengths

The table below details the different lengths of the stolen passwords. Eight was the most common password length, which likely reflects the common requirement for end users to create a password of eight characters or more. We've also shared the three most commonly breached passwords for each password length. In this data, you can see how end users are often taking the simple base terms from the previous section and simply adding consecutive numbers to the end.

Password length	Number of times found	Top three most commonly stolen passwords
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

How many passwords match standard complexity requirements?

Out of the over one billion malware-stolen passwords analyzed, almost a quarter (230 million) would be considered complex. That means they would pass the standard requirements that many organizations set:

- Minimum eight characters
- One capital letter
- One number
- One special character

As you can see from the most commonly stolen 'complex' passwords table on the next page, end users often simply adjust weak base terms by adding capital letters, numbers, or special characters in predictable places (usually starting with a capital and ending with consecutive numbers). These passwords could be quickly guessed by brute force techniques, as they follow simple and predictable patterns. Because of this, compliance standards such as NIST are moving away from complexity recommendations and towards increasing password length instead.

This also shows that a password meeting an organization's password standards doesn't mean it's safe. Any password could be stolen by malware and compromised – no matter its length or complexity. Even if you have a strong password policy, it's still vital to have a tool for checking your Active Directory for compromised passwords.

Top stolen passwords that would pass complexity rules in many organizations
Pass@123
P@ssw0rd
Aa@123456
Admin@123
Aa123456@
Pass@1234
Abcd@1234
Demo@123
Password@123
India@123

Specops tip: Block weak passwords with a custom password-exclusion dictionary

Even after decades of security and awareness training, people are still creating weak passwords. It's human nature to take the path of least resistance. Whether that's choosing an easily-remembered base term for a password or making a slight iteration on a previous one. People simply don't want to memorize a new long and complex password each time they're forced to change – so they look for workarounds.

Inspired by the Paris Olympics Games, earlier in the year our research team revealed that 157,048 sport-related passwords were compromised by malware in the preceding 12 months. Golf-related passwords were the most frequently stolen, appearing in 40,294 instances. This was followed by football, with 20,550 instances. Sport was a generic theme in that piece of research, but weak base terms become more problematic when users choose terms specific to your organization as hackers are more likely to try these in a targeted attack.

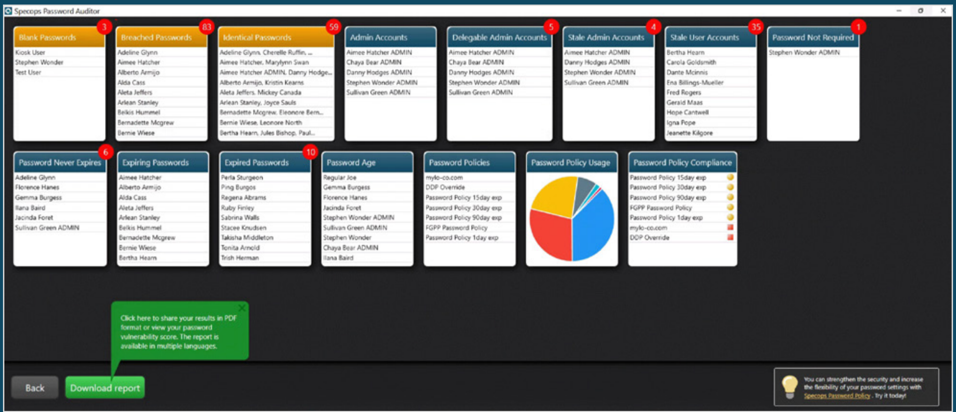
Compiling a custom password-exclusion dictionary is a great way to block users from choosing weak base terms. You could use AI tools like ChatGPT to generate a list of common and predictable passwords, such as 'admin' and 'password'. From there, you can look for password suggestions and their variations based on organization-specific terms like your company names and product name. This will help in creating a comprehensive and robust dictionary, which can be periodically refined.

Is your Active Directory hiding weak passwords? Find out today.

An audit starts your journey towards better password security. Specops Password Auditor is a free tool that can identify multiple types of password-related vulnerability in minutes. Carry out a read-only check of your Active Directory against over 1 billion compromised passwords and analyze your domain password policies and fine-grained password policies. You can also learn whether your policies are compliant with common cybersecurity regulations.

Your exportable report will give you visibility over the following information and password-related vulnerabilities:

- Breached passwords
- Identical passwords
- ‘Password not required’ accounts
- ‘Password never expires’ accounts
- Password policies + usage
- Blank passwords
- Stale admin accounts
- Stale user accounts
- Expired passwords
- Password policy compliance



Specops Password Auditor

Blank Passwords (3)
Kiosk User
Stephen Wonder
Test User

Breached Passwords (83)
Adeline Glynn
Aimee Hatcher
Alberto Armijo
Alda Cass
Aleta Jeffers
Arlean Stanley
Belkis Hummel
Bernadette Mcgrew
Bernie Wiese

Identical Passwords (59)
Adeline Glynn, Cherelle Ruffin, ...
Aimee Hatcher, Marylynn Swan
Aimee Hatcher ADMIN, Danny Hodge...
Alberto Armijo, Kristin Kearns
Aleta Jeffers, Mickey Canada
Arlean Stanley, Joyce Sauls
Bernadette Mcgrew, Eleonore Bern...
Bernie Wiese, Leonore North
Bertha Hearn, Jules Bishop, Paul...

Admin Accounts
Aimee Hatcher ADMIN
Chaya Bear ADMIN
Danny Hodges ADMIN
Stephen Wonder ADMIN
Sullivan Green ADMIN

Delegable Admin Accounts (5)
Aimee Hatcher ADMIN
Chaya Bear ADMIN
Danny Hodges ADMIN
Stephen Wonder ADMIN
Sullivan Green ADMIN

Stale Admin Accounts (4)
Aimee Hatcher ADMIN
Danny Hodges ADMIN
Stephen Wonder ADMIN
Sullivan Green ADMIN

Stale User Accounts (35)
Bertha Hearn
Carola Goldsmith
Dante Mcinnis
Ena Billings-Mueller
Fred Rogers
Gerald Maas
Hope Cantwell
Igna Pope
Jeanette Kilgore

Password Not Required (1)
Stephen Wonder ADMIN

Password Never Expires (6)
Adeline Glynn
Florence Hanes
Gemma Burgess
Ilana Baird
Jacinda Foret
Sullivan Green ADMIN

Expiring Passwords
Aimee Hatcher
Alberto Armijo
Alda Cass
Aleta Jeffers
Arlean Stanley
Belkis Hummel
Bernadette Mcgrew
Bernie Wiese
Bertha Hearn

Expired Passwords (10)
Perla Sturgeon
Ping Burgos
Regena Abrams
Ruby Finley
Sabrina Walls
Stacee Knudsen
Takisha Middleton
Tonita Arnold
Trish Herman

Password Age
Regular Joe
Gemma Burgess
Florence Hanes
Jacinda Foret
Stephen Wonder ADMIN
Sullivan Green ADMIN
Stephen Wonder
Chaya Bear ADMIN
Ilana Baird

Password Policies
mylo-co.com
DDP Override
Password Policy 15day exp
Password Policy 30day exp
Password Policy 90day exp
FGPP Password Policy
Password Policy 1day exp

Password Policy Usage

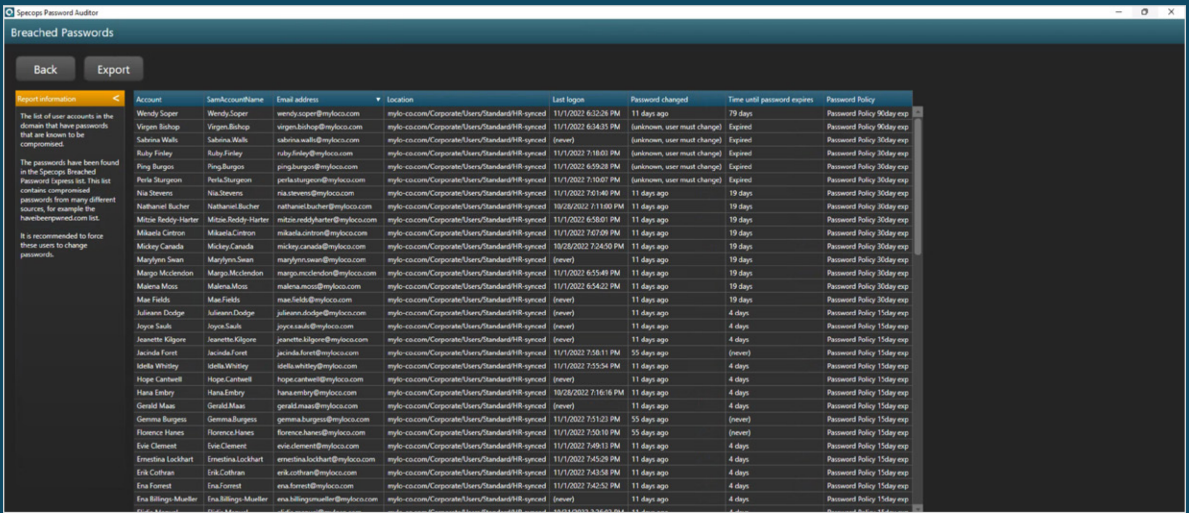
Password Policy Compliance
Password Policy 15day exp ●
Password Policy 30day exp ●
Password Policy 90day exp ●
FGPP Password Policy ●
Password Policy 1day exp ●
mylo-co.com 🟥
DDP Override 🟥

Click here to share your results in PDF format or view your password vulnerability score. The report is available in multiple languages.

You can strengthen the security and increase the flexibility of your password settings with Specops Password Policy. Try it today!

Specops Password Auditor: Results dashboard

Remember to pay particular attention to end users with known breached or compromised passwords, as these offer a simple route into your organization for hackers:



Specops Password Auditor

Breached Passwords

Report information

The list of user accounts in the domain that have passwords that are known to be compromised.

The passwords have been found in the Specops Breached Password Express list. This list contains compromised passwords from many different sources, for example the haveibeenpwned.com list.

It is recommended to force these users to change passwords.

Account	SamAccountName	Email address	Location	Last logon	Password changed	Time until password expires	Password Policy
Wendy Soper	Wendy.Soper	wendy.soper@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 6:32:26 PM	11 days ago	79 days	Password Policy 90day exp
Virgen Bishop	Virgen.Bishop	virgen.bishop@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 6:34:35 PM	(unknown, user must change)	Expired	Password Policy 90day exp
Sabrina Walls	Sabrina.Walls	sabrina.walls@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	(never)	(unknown, user must change)	Expired	Password Policy 30day exp
Ruby Finley	Ruby.Finley	ruby.finley@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 7:18:03 PM	(unknown, user must change)	Expired	Password Policy 30day exp
Ping Burgos	Ping.Burgos	ping.burgos@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 6:59:28 PM	(unknown, user must change)	Expired	Password Policy 30day exp
Perla Sturgeon	Perla.Sturgeon	perla.sturgeon@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 7:10:07 PM	(unknown, user must change)	Expired	Password Policy 30day exp
Nia Stevens	Nia.Stevens	nia.stevens@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 7:01:40 PM	11 days ago	19 days	Password Policy 30day exp
Nathaniel Bucher	Nathaniel.Bucher	nathaniel.bucher@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	10/28/2022 7:11:00 PM	11 days ago	19 days	Password Policy 30day exp
Mitzie Reddy-Harter	Mitzie.Reddy-Harter	mitzie.reddyharter@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 6:58:01 PM	11 days ago	19 days	Password Policy 30day exp
Mikaela Cintron	Mikaela.Cintron	mikaela.cintron@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 7:07:09 PM	11 days ago	19 days	Password Policy 30day exp
Mickey Canada	Mickey.Canada	mickey.canada@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	10/28/2022 7:24:50 PM	11 days ago	19 days	Password Policy 30day exp
Marylynn Swan	Marylynn.Swan	marylynn.swan@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	(never)	11 days ago	19 days	Password Policy 30day exp
Margo Mcclendon	Margo.Mcclendon	margo.mcclendon@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 6:55:49 PM	11 days ago	19 days	Password Policy 30day exp
Malena Moss	Malena.Moss	malena.moss@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 6:54:22 PM	11 days ago	19 days	Password Policy 30day exp
Mae Fields	Mae.Fields	mae.fields@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	(never)	11 days ago	19 days	Password Policy 30day exp
Julieann Dodge	Julieann.Dodge	julieann.dodge@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	(never)	11 days ago	4 days	Password Policy 15day exp
Joyce Sauls	Joyce.Sauls	joyce.sauls@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	(never)	11 days ago	4 days	Password Policy 15day exp
Jeanette Kilgore	Jeanette.Kilgore	jeanette.kilgore@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	(never)	11 days ago	4 days	Password Policy 15day exp
Jacinda Foret	Jacinda.Foret	jacinda.foret@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 7:58:11 PM	55 days ago	(never)	Password Policy 15day exp
Idella Whitley	Idella.Whitley	idella.whitley@myloo.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 7:55:54 PM	11 days ago	4 days	Password Policy 15day exp
Hope Cantwell	Hope.Cantwell	hope.cantwell@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	(never)	11 days ago	4 days	Password Policy 15day exp
Hana Embry	Hana.Embry	hana.embry@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	10/28/2022 7:16:16 PM	11 days ago	4 days	Password Policy 15day exp
Gerald Maas	Gerald.Maas	gerald.maas@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	(never)	11 days ago	4 days	Password Policy 15day exp
Gemma Burgess	Gemma.Burgess	gemma.burgess@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 7:51:23 PM	55 days ago	(never)	Password Policy 15day exp
Florence Hanes	Florence.Hanes	florence.hanes@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 7:50:10 PM	55 days ago	(never)	Password Policy 15day exp
Evie Clement	Evie.Clement	evie.clement@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 7:49:13 PM	11 days ago	4 days	Password Policy 15day exp
Ernestina Lockhart	Ernestina.Lockhart	ernestina.lockhart@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 7:45:29 PM	11 days ago	4 days	Password Policy 15day exp
Erik Cothran	Erik.Cothran	erik.cothran@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 7:43:58 PM	11 days ago	4 days	Password Policy 15day exp
Ena Forrest	Ena.Forrest	ena.forrest@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	11/1/2022 7:42:52 PM	11 days ago	4 days	Password Policy 15day exp
Ena Billings-Mueller	Ena.Billings-Mueller	ena.billingsmueller@myloco.com	mylo-co.com/Corporate/Users/Standard/HR-synced	(never)	11 days ago	4 days	Password Policy 15day exp

Specops Password Auditor: Report showing end users with known compromised passwords

Download Specops Password Auditor

How hackers use malware to steal credentials

Stolen credentials are in high demand. They provide a simple and direct pathway to valuable data, including personal information, financial records, and corporate secrets. Initial access brokers (IABs) specialize in the trade of stolen credentials on the dark web and underground forums. Without access to Threat Intelligence tools, it can be hard for organizations to know whether their users' credentials are being touted on marketplaces frequented by hackers.

Stolen credentials can also be used to launch additional attacks, such as phishing campaigns or more sophisticated breaches. Once a hacker gains access to a system using stolen credentials, they can maintain long-term access, allowing them to gather more data over time and potentially move laterally within a network to access additional systems. Legitimate credentials representing a trusted identity make it harder for security software to identify the activity as malicious, as the actions appear to be performed by authorized users.

How do infostealers work?

Understanding how infostealers work can help in developing better security practices and defenses against them. It's important to keep software up to date, use strong and unique passwords, and employ multi-factor authentication where possible. Additionally, regular security audits and monitoring can help detect and mitigate the presence of infostealers. Here's a general overview of how they work:

1. **Infection:** Infostealers can infect a system through various means, such as phishing emails, malicious downloads, or exploiting vulnerabilities in software. Once the malware is executed, it gains access to the system.

2. **Persistence:** To ensure they can continue to gather data over time, infostealers often establish persistence mechanisms. This can include creating registry entries, modifying system files, or adding themselves to startup processes.

3. **Data collection:** Infostealers search for and collect various types of sensitive information. For credentials, they typically target:
   - Browsers: They can extract saved passwords, cookies, and autofill data from web browsers like Chrome, Firefox, and Edge.
   - Email clients: They can steal login credentials and other data from email clients like Outlook.
   - FTP clients: They can access and steal credentials stored in FTP clients.
   - File systems: They can search for and extract credentials from configuration files, text files, and other data storage locations.
   - Clipboard: They can monitor the clipboard to capture any sensitive information that is copied and pasted.

4. **Exfiltration:** Once the data is collected, infostealers need to send it to the attacker. This can be done through various methods:
   - HTTP/HTTPS requests: They can send the data to a remote server using web protocols.
   - Email: They can send the data via email to the attacker.
   - FTP: They can upload the data to an FTP server.
   - Command and Control (C2) Servers: They can communicate with C2 servers to send the data and receive further instructions.

5. **Evasion:** To avoid detection, infostealers often employ techniques to evade antivirus software and other security measures. These can include:
   - Code obfuscation: Making the code difficult to read and analyze.
   - Packing: Compressing the malware to make it harder to detect.
   - Rootkit techniques: Hiding the malware's presence on the system.
   - Stealth communication: Using encrypted or obfuscated communication channels to avoid network monitoring.

6. **Execution:** Infostealers can be programmed to run at specific times or under certain conditions to avoid suspicion. For example, they might only activate when the user is not actively using the computer.

Top malware used to steal credentials

Specops research highlights Redline malware as hackers' favorite tool for password theft, accounting for nearly half of all the stolen passwords analyzed. In our dataset, hackers had stolen 170 million unique sets of credentials in just six months with Redline. Vidar and

Raccoon Stealer are also notable, responsible for 17% and 11.7% of stolen passwords, respectively. Here's some more info on the top three stealers we found:

1. Redline

Redline is an extremely popular stealer. It was discovered in March 2020 and its main goal is to export all sorts of personal information, such as credentials, cryptocurrency wallets, and financial data, then upload it to the malware's C2 infrastructure. On many occasions, a Redline payload is delivered along with a cryptocurrency miner to be deployed on the victim's machine, especially in campaigns where gamers with powerful GPUs are the preferred target.

From mid-2021 onwards, YouTube has also been used as a distribution method for Redline, in a process as follows:

- Firstly, the threat actor compromises a Google/YouTube account
- Once compromised, the threat actor creates different channels or directly publishes videos on them
- In the description of the uploaded videos (usually ones that advertise gaming cheats and cracks, providing instructions on hacking popular games and software) threat actors will include a malicious link related to the theme of the video
- Users click the link and unwittingly download Redline onto their device, resulting in their passwords and other private information being stolen

2. Vidar

Vidar is an evolution of the well-known Arkei Stealer. It checks for the language preferences of the infected machine to whitelist some countries for further infection. Following that, it generates a Mutex and initializes the strings needed to operate. There are two different C2 versions available to hackers. The original one is associated with the paid version of Vidar, Vidar Pro. There's also another C2 version used in the cracked version of Vidar that is distributed in underground forums, called Anti-Vidar.

In early 2022, Vidar was spotted being distributed in phishing campaigns as Microsoft Compiled HTML Help (CHM) files. Additionally, it has been detected that the malware is being distributed by the PPI malware service PrivateLoader, the Fallout Exploit Kit, and the Colibri loader. In late 2023, the malware has been observed being delivered by the GHOSTPULSE malware loader.

3. Raccoon Stealer

Raccoon Stealer is an information-stealing malware offered for sale on the cybercriminal underground. The team behind Raccoon Stealer uses a 'malware-as-a-service' model, allowing customers to rent the stealer on a monthly basis. It was first offered for sale on the top-tier Russian-language forum Exploit on April 8, 2019. Raccoon Stealer is promoted using the tagline: "We steal, You deal!"

Primarily, it's been offered for sale on Russian-language underground forums such as Exploit and WWH-Club. On October 20, 2019, the threat actor also began offering Raccoon Stealer on the infamous English-language Hack Forums. The threat actor marketing Raccoon Stealer on underground forums occasionally refer to "test weeks," perhaps indicating that prospective hackers are able to enjoy a trial run of the product.

The operator behind Raccoon Stealer was recently caught and sentenced to five years in prison.

Can malware steal Active Directory passwords?

The weak point is users storing their Active Directory credentials in browsers or applications like FileZilla, making them vulnerable to credential stealers. Active Directory credentials often match those used in Microsoft 365/Outlook, as they are managed by Entra ID (formerly Azure AD), a cloud-based directory synced with on-premises AD. Many organizations also implement Single Sign-On (SSO), which further links these systems.

Our researchers also recently uncovered over two million VPN passwords that were compromised by malware, highlighting a major risk to organizational security. These passwords, essential for user access to VPNs, now serve as potential entry points for cybercriminals, undermining the primary purpose of VPNs to secure and privatize communications through data encryption. The biggest risk is when Active Directory passwords are also reused as VPN passwords, which could allow attackers to access all systems and resources a user has permissions for, leading to extensive damage and theft.

Specops tips: Hunting for stolen credentials on the dark web

Threat Intelligence teams can help organizations determine if their users' credentials are compromised and available for sale on the dark web, thereby enabling them to take immediate action to secure their accounts by prompting users to change their passwords. They engage in activities such as infiltrating botnets, intercepting communications, and accessing insider information from underground forums to collect data on malware-harvested passwords.

This gathered threat intelligence is crucial for updating Specops' extensive breached password database of over 4 billion unique compromised passwords – and comes from the team that helped power much of the research in this report. This information helps protect organizations from the real risk behind stealers: groups of traffers (credential trafficking groups) which sell the passwords to other hackers and ransomware groups.

How can organizations reduce password risk?

There are two key ways for organizations to reduce their risk around passwords. First, you need to make sure your Active Directory is full of long and complex passwords that are resistant to brute-force attacks. However, the billion malware-stolen passwords analyzed in this report underpins the need for a tool to scan for passwords that have become compromised without your organization's knowledge.

Enforce long, strong passwords

Our research team looked into the strength of the SHA-256 hashing algorithm against current password cracking techniques. It's not the most advanced algorithm, but it's still used in plenty of environments. The threat is password reuse, as your users' work passwords could be stored in the most secure way but the minute they reuse that password on some less secure website and that website gets leaked; that attacker could be coming for your network.

As you can see below in the cracking table produced from this research, even a relatively modern algorithm like SHA-256 can't protect short, simple passwords from brute-force attacks. On the other hand, it also shows that a hacker would likely be wasting their time trying to crack a long, complex password that's been hashed with SHA-256. This proves the value in encouraging end users to create long, secure passphrases.

Time to crack: SHA-256 Hashed Passwords

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

Attackers will always prefer to go in search of easy targets and low-hanging fruit. For example, Active Directory passwords that have already been compromised in data breaches. One way this can happen is through password reuse. You could encourage your end users to create long, strong Active Directory passwords and store them very securely. But this work is undone if end users reuse those passwords on personal devices, sites, and applications with weak security.

Time to crack: Known compromised passwords

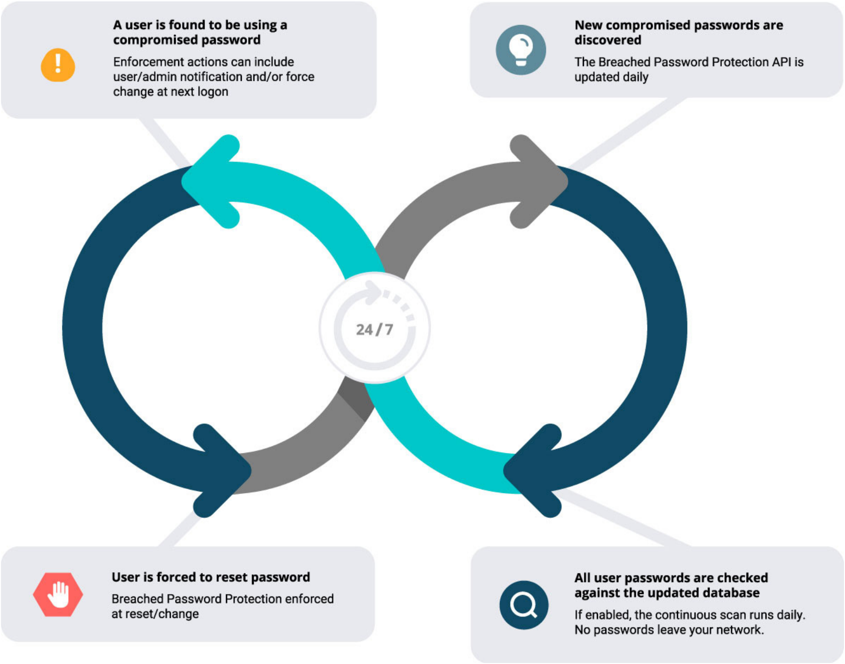
Number of characters	Numbers Only	Lowercase Only	Upper and Lower	Number, Upper, Lower	Number, Upper, Lower, Symbols
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	Instantly
9	Instantly	Instantly	Instantly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

Continuously scan for compromised passwords

The Specops Password Policy continuous scan feature provides daily checks against the Specops Breached Password Protection service, which is updated daily with passwords collected from honeypot networks, threat intelligence data, and newly discovered password leaks. This ensures that IT professionals have constant access to one of the most complete and up-to-date compromised password databases on the market.

By continuously scanning Active Directory passwords against the Breached Password Protection API, your IT teams can proactively identify compromised passwords within your organization. Continuous password scans can help detect potential security breach access points and enable prompt action to mitigate the risks associated with password reuse. It enables IT teams to automatically identify compromised passwords and immediately enforce the end user to change it at their next logon.

Incorporating the continuous scan feature into your password policy lets admins ensure compliance with industry best practices and regulatory requirements. The continuous scan results can be easily reviewed, giving a clear overview of compromised passwords within a network.


A user is found to be using a compromised password
Enforcement actions can include user/admin notification and/or force change at next logon
New compromised passwords are discovered
The Breached Password Protection API is updated daily
24 / 7
User is forced to reset password
Breached Password Protection enforced at reset/change
All user passwords are checked against the updated database
If enabled, the continuous scan runs daily. No passwords leave your network.

Specops Breached Password Protection continuous scan feature

Want to discuss how Specops Password Policy with Breached Password Protection could fit in with your organization?

Arrange a free trial

Eight key takeaways

1. Malware stolen credentials are common – we've found over a billion in the last 12 months.
2. Despite knowing the risks, end users will create short, weak passwords like 'password,' '12345,' and 'admin' when they're allowed to. Blocking weak terms within your password policy is essential.
3. Many stolen credentials meet standard complexity requirements – including 230 million analyzed in this report.
4. 'Complex' passwords can still be predictable thanks to user behavior. Length is a better indicator of password strength.
5. Hackers favor malware-stolen credentials as they're easy to obtain, use, and sell. Redline is the most popular stealer according to our research.
6. Even strong passwords can be stolen by malware, rendering hashing algorithms obsolete. All end user accounts should be secured with MFA.
7. Malware is one reason password reuse is so dangerous. Are your end users reusing work passwords on personal devices and applications with weak security?
8. It's vital to be able to continuously scan your Active Directory for compromised passwords.

THE SPECOPS STORY

Specops Software, an Outpost24 company, is the leading provider of password management and authentication solutions. Specops protects your business data by blocking weak passwords and securing user authentication. With a complete portfolio of solutions natively integrated with Active Directory, Specops ensures sensitive data is stored on-premises and in your control. Specops Software was founded in 2001 and is headquartered in Stockholm, Sweden with additional offices in the US, Canada, the UK, and Germany.

BOOK A DEMO >> REQUEST CUSTOMIZED PRICING >>

CONTACT US

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