# Specops Breached Password Report 2026

Analyzing a year's worth of malware-stolen credentials

Specops Software, an Outpost24 company, is the leading provider of identity management and authentication solutions.

SPECOPS
AN OUTPOST24 COMPANY

# What's inside?

# Report highlights

Data in this report comes from Outpost24's threat intelligence team, the Threat Intelligence team at Outpost24, Specops Software's parent company. In total, over six billion stolen passwords were captured and analyzed over a 12-month period between January and December 2025. The report also references additional research carried out by Specops Software throughout 2025. The data in this report is accurate as of December 2025.

Over **six billion** passwords stolen in a 12-month period

Top **credential-stealing malware** in 2025 was **LummaC2** with **60,934,662** credentials compromised

Eight-character passwords remain the most commonly stolen, with **1,077,202,230** compromised

Top three **stolen password** lengths:

- **Eight characters** (1.1 billion)
- **Ten characters**  (926 million)
- **Nine characters** (882 million)

Most **common base terms** found in **stolen passwords:**

- admin
- guest
- cisco
- Hello

**Top 5 stolen passwords:**

- 123456
- 123456789
- 12345678
- admin
- Password

# Executive summary

Credential abuse remains one of the most reliable and scalable initial access methods available to attackers. Industry breach analysis continues to show how deeply embedded stolen credentials are in modern attacks. According to **Verizon's 2025 Data Breach** Investigations Report, credential abuse accounted for 22% of confirmed breaches, while 54% of ransomware victims had their domains appear in credential dumps and 40% had corporate email addresses exposed, demonstrating how stolen passwords continue to enable downstream attacks at scale.

These findings reinforce a persistent reality: passwords are one of the most exposed and abused elements of enterprise security. Once compromised, credentials provide attackers with trusted access into corporate environments, often bypassing perimeter defenses entirely. This is reflected in broader intrusion data, with identity-based attacks accounting for 30% of intrusions in 2025, according to **IBM X-Force.**

As credential theft has become continuous rather than episodic, the risk associated with passwords can no longer be assessed only at the point of creation. The question is no longer whether a password meets policy when it's set, but whether it remains safe over time in an environment where credentials are constantly harvested, aggregated, and resold.

Against this backdrop, Outpost24's threat intelligence team analyzed over six billion malware-stolen passwords collected during 2025. This report examines the password patterns attackers are actively exploiting, how infostealer malware captures and distributes credentials at scale, and what these trends reveal about the limitations of traditional password policies.

By grounding its analysis in real-world attacker data, this report helps organizations better understand their exposure to password-based attacks and identify practical ways to reduce the risk posed by compromised credentials.

# Weak passwords: Trends and patterns

Across the **6,004,274,474** stolen passwords analyzed, weak and predictable patterns continue to dominate. Despite years of awareness training and increasingly complex password policies, attackers are still encountering the same basic structures, repeated across environments, applications, and regions.

## The most commonly stolen passwords

Simple numeric sequences and default terms continue to account for the majority of malware-stolen credentials, which is consistent with the results of Specops Software's 2025 Breached Password Report.

| Top five stolen passwords of 2025 |
|---|
| **123456** |
| **123456789** |
| **12345678** |
| **admin** |
| **password** |

These passwords are easy to guess, widely reused, and frequently associated with shared, functional, or privileged access. Numeric sequences dominate across multiple password lengths, often alongside default terms such as *admin* and *password*, which commonly appear in infrastructure and enterprise environments.

When users are allowed to choose their own credentials without meaningful restrictions, many will still default to the simplest possible option. In enterprise environments, this creates a real risk that malware-stolen credentials are reused as Active Directory (AD), virtual private network (VPN), or cloud identity passwords, giving attackers trusted access to corporate systems.

## Common base terms and predictable structures

Beyond exact password matches, the dataset shows consistent reuse of weak base terms that users rely on when constructing passwords. Commonly observed base terms included *admin* (and case variations such as *Admin* and *ADMIN*), *guest, cisco,* and *hello.*

| 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 |

These patterns closely align with previous years, indicating little change in user behavior. Keyboard walks such as *qwerty* and *azerty* remain common, reflecting highly predictable structures that attackers routinely exploit.

The repeated appearance of terms such as *password* and *hello* suggests operational rather than personal use. Analysis of the 500 most frequently recovered passwords shows a clear bias toward functional credentials tied to infrastructure, VPNs, and internal services, including variations of admin, root, and user.

## Regional and language-linked password patterns

While the most commonly stolen passwords are globally consistent, the dataset also shows regional and language-linked variations built on the same weak templates.

| Most common regional base terms |
|---|
| **Pakistan@123, Pakistan123** |
| **India@123** |
| **Nepal@123** |
| **senha123 (Portuguese for "password")** |
| **hola1234 (Spanish greeting)** |

These passwords follow familiar structures, typically combining a familiar word, place, or language-specific term with simple numeric sequences. Although the specific terms vary by region, the underlying patterns remain highly predictable, making them easy for attackers to anticipate and reuse.

## Name-based and shared credential patterns

One of the clearest patterns in the most frequently recovered credentials is the use of name-based passwords combined with simple numeric or symbolic suffixes. A large cluster of commonly stolen passwords follows the structure FirstName@123.

| Most common name base terms |
|---|
| **Kumar@123** |
| **Rahul@123** |
| **Rohit@123** |
| **Amit@123** |
| **Akash@123** |

These passwords appear consistently across multiple unrelated environments and are unlikely to represent individual user accounts. Instead, they strongly indicate shared or functional use, including departmental access, onboarding credentials, and accounts tied to internal portals or remote access systems.

## Most common password lengths

The table below shows the number of stolen passwords observed during 2025, broken down by password length. As in previous years, eight characters remain the most commonly stolen length, with over 1.07 billion passwords captured. This shows a continued reliance on minimum-length requirements across many organizations.

Longer passwords were also widely exposed. Attackers stole hundreds of millions of passwords at every common length, including 882 million (nine-characters), 925 million (ten-characters), and 672 million (eleven-characters) passwords. In total, more than 4.4 billion stolen passwords were between eight and twelve characters, reinforcing that password length alone isn't sufficient to prevent compromise.

| Password length | Number of times found | Top three most commonly stolen passwords |
|---|---|---|
| **6** | 239,588,682 | 123456<br>123123<br>000000 |
| **7** | 152,581,176 | 1234567<br>A123456<br>welcome |
| **8** | 1,077,202,230 | 12345678<br>Password<br>Aa123456 |
| **9** | 882,149,149 | 123456789<br>Aa@123456<br>Admin@123 |
| **10** | 925,692,295 | 1234567890<br>Qwertyuiop<br>0987654321 |
| **11** | 672,515,189 | 12345678910<br>Welcome@123<br>qwerty12345 |
| **12** | 540,238,382 | Password@123<br>Pakistan@123<br>admintelecom |

Across all lengths, the most commonly stolen passwords follow the same predictable patterns seen elsewhere in this report. The data shows that weak base terms and simple sequences are extended with additional characters, allowing passwords to meet policy requirements while remaining easy to reuse once compromised. The persistence of this distribution over time suggests little change in password creation behavior.

Long passwords and passphrases of 15 characters or more remain important for defending against brute-force and guessing attacks, but the data in this report shows that passwords are often stolen through infostealers or phishing rather than cracked.

This means even strong, policy-compliant credentials can be exposed, particularly when employees reuse work passwords on personal devices, applications, or websites with weaker security. As a result, organizations need a way to continuously scan their ADs for compromised passwords, rather than relying on password length and complexity controls alone.

## Complex passwords are still commonly compromised

Many organizations continue to rely on standard complexity rules to reduce password risk. These typically require passwords to be:

- Minium eight characters
- One uppercase letter
- One number
- One special character

Analysis of malware-stolen credentials revealed that passwords meeting these requirements are still routinely compromised.

| Common examples of compromised complex passwords |
|---|
| **Aa@123456** |
| **Admin@123** |
| **Pass@1234** |
| **Abcd@1234** |
| **Aa123456@** |

The prevalence of these passwords shows that compliance at the point of creation does not equate to resilience once credentials are exposed. Passwords that already conform to policy can be reused immediately across enterprise environments, making them particularly valuable within aggregated credential datasets.

# Key highlights from credential pattern analysis

The highlights below summarise the most common password patterns identified through credential analysis and illustrate how predictable structures continue to drive credential exposure.

1

The top 500 most commonly recovered passwords are clearly tied to infrastructure and shared access, including terms such as *admin, root, user, guest,* and *administrator.*

2

Onboarding and default password templates remain widespread. Credentials such as *Welcome@123* indicate that first-day passwords are often retained rather than rotated or retired.

3

Name-based passwords with simple suffixes remain common. Patterns such as *Kumar@123* show minimal variation and are designed to satisfy complexity rules rather than improve security.

4

Regional and language-specific terms appear frequently but follow the same weak structures.

5

Sequential and patterned character strings remain prevalent. Examples such as *Aa123456* and *Abc123* significantly reduce attacker effort.

Try Specops Password Auditor

# Infostealer activity and most active malware families

## Why stolen credentials are in such high demand

Infostealer malware has become one of the most effective mechanisms for harvesting credentials at scale. Rather than exploiting individual vulnerabilities or targeting specific organizations, infostealers operate opportunistically, collecting authentication data from browsers, applications, and local storage across infected systems. This approach enables attackers to acquire large volumes of credentials with minimal effort and low risk.

Once harvested, stolen credentials are rarely used in isolation. They are aggregated, enriched, and redistributed through established criminal ecosystems, including access brokers and credential marketplaces. As a result, a single infection event can fuel repeated downstream attacks over extended periods, transforming password compromise from a point-in-time incident into a persistent source of risk.

Initial Access Brokers (IABs) play a key role by reselling access to compromised organizations through underground marketplaces and messaging platforms such as Telegram. Corporate access can be bought for as little as a few hundred dollars on the underground market, thereby lowering the barrier to entry for attackers and accelerating credential-based attacks at scale.

Once attackers gain access using legitimate credentials, they can maintain long-term persistence, move laterally across systems, and collect additional data over time. Because this activity appears to originate from authorized users, it's often harder for security tools to detect. As a result, organizations need visibility beyond their own environments, including the ability to monitor criminal marketplaces and credential dumps to identify when corporate credentials are being traded or resold.

## How do infostealers work

Infostealer malware is designed to quietly extract credentials from infected devices with minimal disruption. Understanding how these tools operate helps defenders identify where credential exposure is most likely to occur, and which controls are most effective at breaking the theft chain.

Most infostealers follow a relatively simple operational flow that prioritizes speed and scale over long-term persistence or advanced stealth. While individual families vary, modern stealers are generally lightweight payloads designed to execute quickly, collect data, and exfiltrate it with minimal interaction.

### *1. Initial infection*

Infostealers are commonly delivered through phishing emails, malicious downloads, cracked or pirated software, malvertising campaigns, fake software updates, or compromised websites. In many campaigns, the stealer payload is deployed by a separate loader or dropper responsible for execution, staging, and basic evasion.

Once executed, the stealer typically runs in user space and begins its collection activity immediately, often without requiring elevated privileges.

### *2. Credential and data harvesting*

Rather than targeting a single application, infostealers systematically collect authentication material and related data from multiple sources on the infected system, including:

- Web browsers: Saved credentials, cookies, session tokens, autofill data, and stored payment information from browsers such as Chrome, Firefox, and Edge
- Email clients: Login credentials and configuration data from applications such as Outlook and Thunderbird
- FTP and remote access tools: Stored credentials used for file transfer or remote administration
- Messaging and collaboration apps: Session tokens or local data from applications such as Telegram or Discord
- Cryptocurrency wallets: Wallet files and browser-based wallet extensions
- Local files and configuration data: Text files or application configuration files where credentials or API keys may be stored
- Clipboard data: Recently copied content, which may include usernames, passwords, recovery phrases, or access tokens

In addition, many stealers collect basic system information (OS version, hostname, installed software, security tools) to enrich the stolen dataset.

### *3. Exfiltration*

Collected data is transmitted to attacker-controlled infrastructure. For infostealers, command-and-control is typically simple and tightly coupled with exfiltration, and may use:

- HTTP or HTTPS endpoints
- FTP servers
- Email inboxes or messaging platforms

These endpoints function primarily as automated collection points rather than interactive command frameworks, often feeding directly into attacker-managed dashboards or resale pipelines.

### *4. Limited persistence and evasion*

Unlike more sophisticated malware families, infostealers do not typically rely on advanced persistence mechanisms or kernel-level techniques. Many are designed to execute once, exfiltrate data, and exit.

Where persistence or stronger evasion is present, it's usually provided by accompanying components such as loaders, crypters, or bundlers rather than the stealer itself. Common techniques include basic packing, obfuscation, or signature-evasion methods to delay detection.

This lightweight design reflects the economics of credential theft at scale, where infection volume and rapid data collection are prioritized over long-term access to individual systems.

## Top malware used to steal credentials

A relatively small number of infostealer malware families continue to account for a significant proportion of credential theft activity. These tools are widely available, easy to deploy, and designed specifically to harvest credentials at scale from infected devices.

Based on Outpost24's threat intelligence team analysis during 2025, the following malware families were most frequently associated with stolen credentials:

| Malware family | Number of credentials stolen |
|---|---|
| **LummaC2** | **60,934,662** |
| **RedLine** | **31,144,858** |
| **Vidar** | **5,965,748** |
| **StealC** | **3,441,423** |
| **Raccoon Stealer** | **1,656,673** |

Together, these families account for tens of millions of stolen credentials, reinforcing the continued effectiveness of infostealers as an initial access mechanism, particularly when infections are achieved at scale through user-driven execution rather than technical exploitation.

Outpost24's threat intelligence team analysis shows a clear shift in infostealer dominance compared to the previous year. Last year's report showed RedLine dominating credential theft activity, accounting for nearly half of the stolen passwords analyzed, with **Vidar** and **Raccoon Stealer** also featuring prominently.

The 2025 dataset shows **LummaC2** emerging as the most prolific infostealer, accounting for nearly 60% of credentials attributed to infostealer malware. **RedLine** followed with just over 30%, while **Vidar, Stealc,** and **Raccoon Stealer** together accounted for less than 11%.

Outpost24's threat intelligence team analysis shows that credential theft is sustained by a fluid ecosystem of stealer operators, traffers, aggregators, and brokers. These operations rely heavily on non-technical users who are incentivized to distribute malware and convince victims to execute it themselves. As a result, group prominence shifts quickly.

Stealer families frequently rebrand, compete for attention, and evolve their service offerings, adding bundled loaders, packers, crypters, and incentive structures aimed at attracting traffer groups. Attacker objectives remain broadly consistent, but dominance is determined by distribution reach, infection volume, and the effectiveness of the malware-as-a-service model rather than technical novelty alone.

> *"In the infostealer ecosystem, success is driven by scale and distribution rather than technical sophistication, which is why families like **Lumma** or **RedLine** continue to dominate through strong malware-as-a-service models and effective traffer networks."*
>
> **Borja Rodriguez**, Head of Threat Intelligence
> *Outpost24*

### Credential aggregation and the Username-Login-Password (ULP) economy

ULPs are compiled credential collections created by aggregating data from multiple stealer logs, historical breaches, and other collection methods. Unlike raw stealer logs, ULP datasets are structured for immediate use and often include associated login URLs, making them easier to test, trade, and reuse at scale.

In 2025, Outpost24's threat intelligence team identified **5,899,505,920** credentials present within ULP datasets. This figure does not represent passwords newly stolen in a single year. Instead, it reflects how stolen credentials accumulate over time, as data from successive malware campaigns and historical breaches are consolidated into long-lived datasets.

This growth does not indicate a fundamental change in attacker technique. Rather, it highlights a shift in how stolen credentials are retained, combined, and reused. Threat actors increasingly prioritize volume and usability, aggregating credentials from multiple sources into datasets designed for repeated testing, resale, and downstream attacks long after the original compromise occurred.

Changes to Telegram policies during 2025 have also influenced how these datasets circulate. While some smaller groups reduced activity or moved platforms, larger aggregator channels grew in prominence, consolidating stealer logs and ULPs from multiple sources and acting as centralized distribution points for compromised credentials.

> *"The rise of the ULP economy underscores a fundamental challenge for defenders. Once credentials are aggregated at this scale, exposure becomes persistent rather than isolated, reinforcing the need for continuous visibility into compromised credentials rather than reliance on point-in-time controls alone."*
>
> **Alejandro Benito**, Threat intelligence Analyst
> *Outpost24*

## How can organizations reduce password risk?

Reducing password risk requires moving beyond how passwords are created and focusing on how they are exposed and reused over time. The issue is no longer whether a password meets policy when it's set, but whether it remains safe in an environment where credentials are routinely harvested and resold.

Even in organizations adopting passwordless or phishing-resistant authentication, passwords are rarely eliminated altogether. Credentials often still exist behind the scenes to support legacy systems, service accounts, directory-based authentication, or recovery workflows. As a result, password exposure remains a relevant risk even as authentication models evolve.

Effective risk reduction therefore depends on compensating controls that assume passwords will continue to exist somewhere in the environment. This means layering continuous detection, stronger governance, and additional protections around credentials, rather than treating password exposure as a solved problem.

### *1. Continuously block compromised passwords*

Reducing this risk requires continuous visibility into compromised credentials, rather than reliance on point-in-time checks. Specops Password Policy with Breached Password

Protection provides continuous scanning of AD passwords against a dataset of more than five billion unique compromised passwords, that is updated daily using honeypot data, threat intelligence, and newly discovered leaks. When compromised passwords are identified, affected users can be required to change their password at their next logon, reducing the window in which attackers can reuse stolen passwords and improving visibility across the domain.

### *2. Eliminate predictable password construction at creation*

Typical password complexity rules allow users to meet policy requirements while still creating passwords that are easy to guess, reuse, or operationalize once stolen. Preventing this exposure requires controls that assess how passwords are constructed, not just which character classes they include.

Blocking weak patterns at the point of creation and change reduces the likelihood that passwords enter large-scale credential aggregation datasets. By stopping weak constructions before they are set, organizations reduce the risk of brute-force attacks, downstream resets, failed logons, and policy exceptions, easing pressure on service desks while lowering the likelihood of credential reuse.

### *3. Reduce exposure from high-risk access paths*

Treat VPNs, RDP, and other externally accessible authentication points as priority targets for credential abuse by strengthening access controls beyond passwords alone. Adding an additional MFA security layer limits the operational value of stolen credentials, reducing the frequency of access-related security incidents that require manual investigation.

Specops Secure Access adds a phishing-resistant MFA layer to Windows logon, RDP, and VPN authentication. Its offline mode ensures MFA enforcement remains in place even during connectivity disruptions, preventing fallback to password-only authentication and supporting compliance requirements such as NIST and PCI.

### *4. Secure password reset and recovery workflows*

Password reset processes are frequent targets for social engineering and re-entry attacks, particularly when attackers already possess partial or exposed credential information. Enforcing strong identity verification during both self-service and helpdesk-driven resets reduces the risk of fraudulent resets, repeat compromise, and account takeover.

Specops uReset secures self-service password resets by verifying user identity before allowing credentials to be changed, reducing account lockouts and unsafe reset practices. Specops Secure Service Desk extends the same identity verification controls to helpdesk-driven resets and account changes, ensuring credentials cannot be reset using guessed or exposed information while reducing call volume, handling time, and the overall cost burden on IT service desks.

### *5. Add device trust to reduce credential abuse*

Credentials are only one part of the access equation. Even when strong password policies or phishing-resistant MFA are in place, stolen credentials remain valuable if attackers can authenticate from their own devices or from unmanaged endpoints. This risk applies equally to corporate-managed devices and bring-your-own-device environments, where visibility and enforcement are often limited.

Infinipoint, part of Specops Software's identity portfolio, adds a zero-trust device security layer by verifying both the user and the device at the point of access and continuously throughout the session. Access is granted only from approved, compliant devices, with real-time posture checks that detect outdated software, disabled security controls, or active threats before credentials can be used. Infinipoint also provides automatic and self-service remediation options for detected device posture problems, reducing IT support burden and user frustration that often block the effectiveness of traditional conditional access and compliance policies.

## Let's Talk

Find out how Specops' solutions help organizations proactively address password exposure and strengthen identity and authentication controls.

Speak to an Expert

**Specops**

Specops Software, an Outpost24 company, is the leading provider of identity 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 and Entra ID, Specops ensures that sensitive data is stored securely, either on-premises or within your Entra ID tenant, and remains under 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.