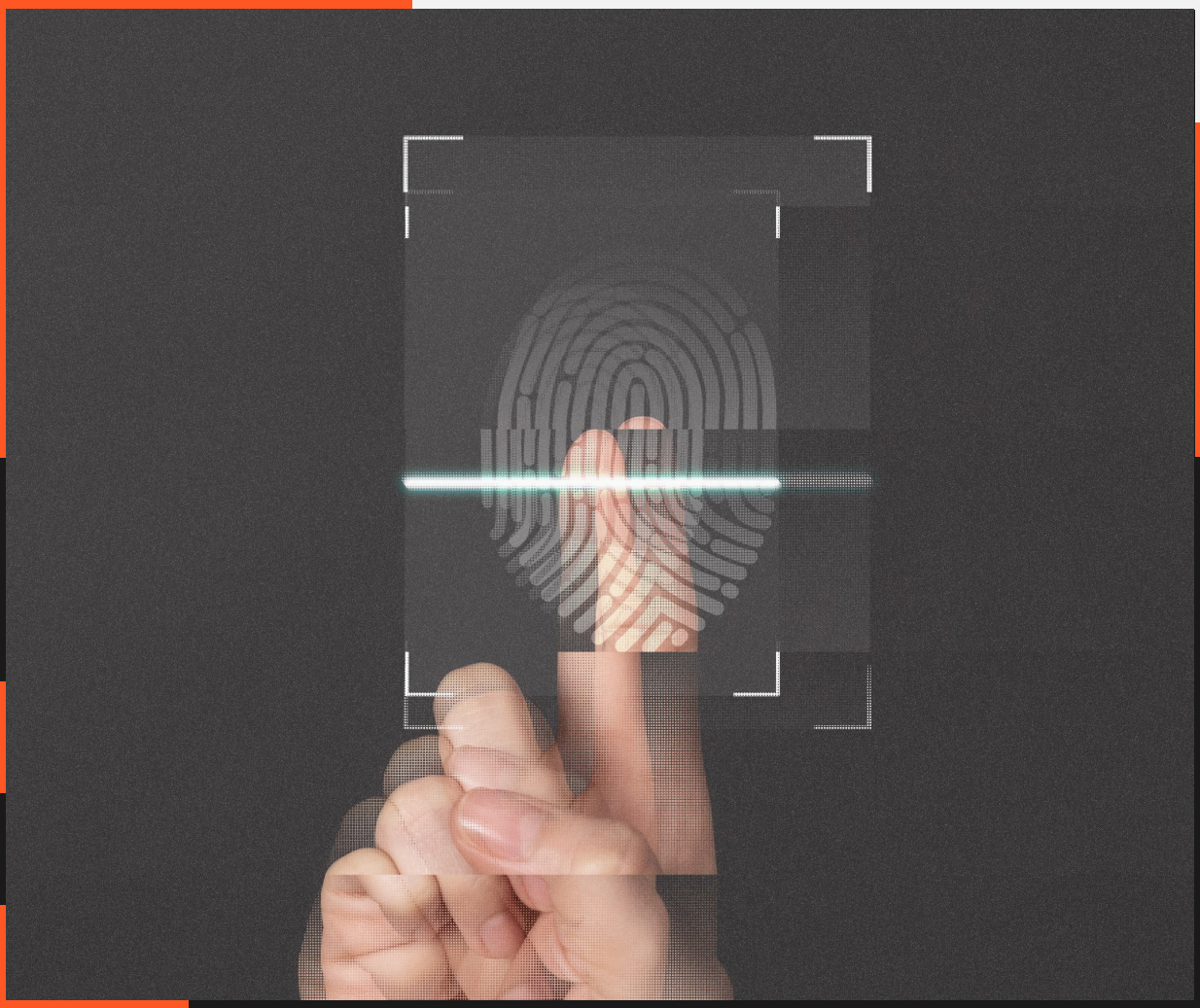


Credentials at Risk

What's New in the Latest Breaches — Key Takeaways

AXUR

Executive Summary

Massive credential leaks can be alarming and make headlines from time to time. The recent case of a threat actor offering a package with 16 billion credentials is just the latest example—but it's neither new nor particularly relevant. These massive compilations have become a regular (if sporadic) occurrence.

For now, there's no reason to believe this data is original. That said, publishing a large bundle of old credentials can still pose a renewed risk to companies and individuals, simply because more criminals now have access to it. Still, that's not where the main threat lies.

It's important to understand that the risks associated with credential leaks go far beyond these newsworthy events. In reality, credential theft and misuse are constant threats, leading to millions of new credentials being leaked every month.

Attackers are deeply interested in this type of data. According to Verizon's Data Breach Investigations Report (DBIR), credential misuse is the initial attack vector in 22% of breaches. While less flashy, these recurring leaks may be even more serious than the mega dumps that grab attention.

Those massive compilations often contain outdated, repeated data—many passwords long since useless. In contrast, the credential files being dumped daily by cybercriminal groups often contain credentials freshly stolen from a machine that might still be in use.

These dumps are a symptom of a criminal ecosystem that financially rewards the trade of stolen credentials—and develops malware specifically for this purpose. Infostealers are a key part of that pipeline, fueling the ecosystem with new data every single day.

That's the context we should keep in mind when reading these stories. Inside our organizations, we need to focus on the most dangerous aspects of the threat—like infostealers and their ability to bypass multi-factor authentication.

In this report, we'll review the history of major credential leaks, how and why these massive dumps are created, and how organizations can strengthen their identity and credential management. You'll find practical recommendations to prevent and mitigate the impact of credential-based attacks.

A History of Major Credential Leaks

Large-scale credential leaks are nothing new in the cybercrime world. Back in 2012, platforms like LinkedIn, eHarmony, and Last.fm were hit by attacks where hackers managed to steal millions of passwords. At the time, the LinkedIn dump—with 6.5 million credentials—seemed massive. But that same leak resurfaced four years later, in 2016, this time with 165 million accounts and 117 million passwords.

This updated LinkedIn dataset was being sold openly by a threat actor—something that soon became a recurring pattern. Often, criminals will share part of the credentials as a "free sample" to boost their credibility and drive sales for the full package.

We saw this tactic again in 2019 with the so-called Collection #1, the first in a series of five massive dumps. While four of them were for sale, Collection #1 was made public as a teaser to promote the rest.

Altogether, those five Collection dumps included 2.2 billion credentials—the largest dataset of its kind at the time.

The ability to make money selling giant credential packages became a strong incentive. It pushed hackers to build ever-larger collections—and gave rise to a financial motivation to specialize in harvesting or stealing credentials.

One common technique linked to this trend is credential stuffing—a method best described as automated password reuse. Cybercriminals use previously leaked credentials and try them across other services, hoping that victims reused the same password.

This tactic helps mitigate attackers' losses, since breached services typically force password resets after a leak. For instance, when the LinkedIn leak occurred in 2012, the platform quickly made users reset their credentials, which limited the usefulness of the stolen passwords for further attacks on LinkedIn itself.

However, through credential stuffing, attackers can identify other services where the same username and password combo was reused. Since those services weren't directly breached, users were never prompted to reset their passwords there—unlike what happened on LinkedIn. And because most people don't update passwords across every service they use, this revalidation process can end up being even more effective than the original leak itself.

Credential stuffing also enables criminals to sell "new" credentials that are, in fact, recycled from older leaks—but now validated on new services.
The effects of password reuse and credential stuffing were already visible in Collection #1. While the dump contained only 21 million unique passwords, it had 1.1 billion username-password combinations. That means many passwords appeared multiple times—either because users reused the same ones or because a single password had been revalidated across different platforms.

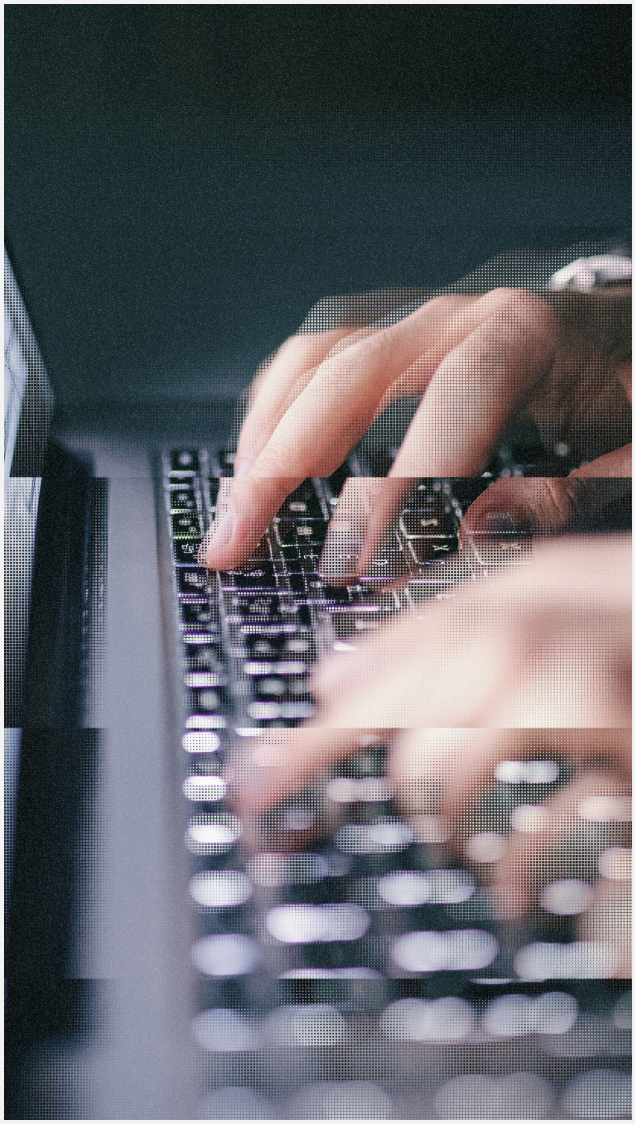
In parallel with credential stuffing, the use of password-stealing malware—known as infostealers—was also on the rise. Cybercriminal groups began specializing in developing and operating these malicious tools to steal as many credentials as possible, often without a specific target, and reselling them in bulk packages or recurring subscriptions.

In that environment, it didn't take long for the Collection numbers to be surpassed. That happened in 2021, when a new compilation named "RockYou2021" was published. The name was a reference to a 2009 cyberattack against RockYou, a company known for creating social media apps for platforms like MySpace and Facebook. That original breach had exposed data from 32 million RockYou users.

RockYou2021 wasn't limited to data from that older breach. With 8.4 billion records, it was a new compilation of credentials pulled from many other previous leaks—as well as revalidated combos, botnet breaches, phishing campaigns, infostealers, and possibly even fabricated data.

The package was later updated and re-released in 2024 under the name "RockYou2024," reaching a total of 9.94 billion credentials.

In 2025, yet another massive credential dump was published—this time claiming to contain 16 billion records.



16 Billion Leaked Credentials: Risk and Context

While some media outlets reported it as a “new” breach, the package claiming to contain 16 billion credentials likely follows the same pattern as its predecessors: a mix of old leaks, revalidated passwords via credential stuffing, and likely a large number of duplicates and invalid entries. Very few of these credentials are likely to be new—and even then, not all of them are necessarily real.

A preliminary analysis by Axur suggests the dataset has low relevance, based on the following:

The package was published on May 23 by a newly created account, not a known or reputable threat actor.

Unlike previous cases, no sample was shared to demonstrate the quality of the data.

The dump doesn’t seem to have sparked much interest among other cybercriminals.

Since the goal of the threat actor is to sell this package to other criminals, there’s no guarantee regarding the authenticity of the material or the claims being made. And because the author behind the dump has no known track record or reputation, their statements should be treated with caution.

In practice, this means there’s a strong chance the dataset contains low-quality records, including:

→ Credentials from previous leaks, with little or nothing new;

→ Data prepped for revalidation but never actually tested—essentially fake or invalid credentials;

→ Very old credentials, where the passwords have likely been changed and are no longer in use;

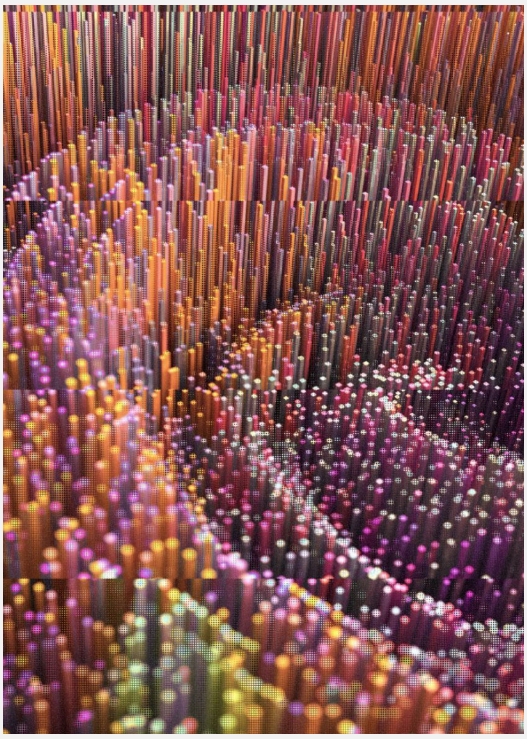
→ Fabricated or false data added just to inflate the total count—data that’s unlikely to be verified due to the sheer volume;

→ Duplicated credentials, resulting from the mix of older leak compilations.

Reposting previously leaked credentials is a very common practice in criminal forums. In 2024, Axur systems detected 56 billion leaked credentials. However, after processing and refining the data to reduce false positives and highlight exposures that represent real risk, less than one-fifth could be considered unique and previously unseen.

From the attacker's perspective, it's nearly impossible to tell the difference between an old, already-invalid credential and a completely fake one. Most modern systems follow best practices by not revealing whether a login exists—using generic error messages that don't specify whether the password is wrong or the account doesn't exist.

Because of this, fraudsters trying to make money from selling credential dumps are incentivized to manipulate the data—padding the package with low-value records just to inflate the numbers. That's especially likely when the offer comes from a source with no established reputation, as is the case with this new dump claiming to include 16 billion credentials.



What Are the Risks?

Even if the credential dump contains few new or valid records, the fact that it's now circulating as a unified package tends to spread those credentials further within the cybercrime ecosystem—just like what happened with Collection #1 and RockYou.

If an organization properly handled a previous incident involving credentials now included in this dump, it's unlikely they'll be targeted again using the same data. However, there is still risk for companies and individuals who haven't yet been attacked using those credentials.

Criminal groups often look for valuable credentials that haven't been exploited yet—triggering large-scale attacks. In 2024, for example, that happened to companies using Snowflake's cloud storage service.

According to the 2025 Verizon Data Breach Investigations Report, 22% of breaches start with a stolen credential.

That said, the lack of new or valid credentials in this dump doesn't mean credential leaks aren't a threat to business.

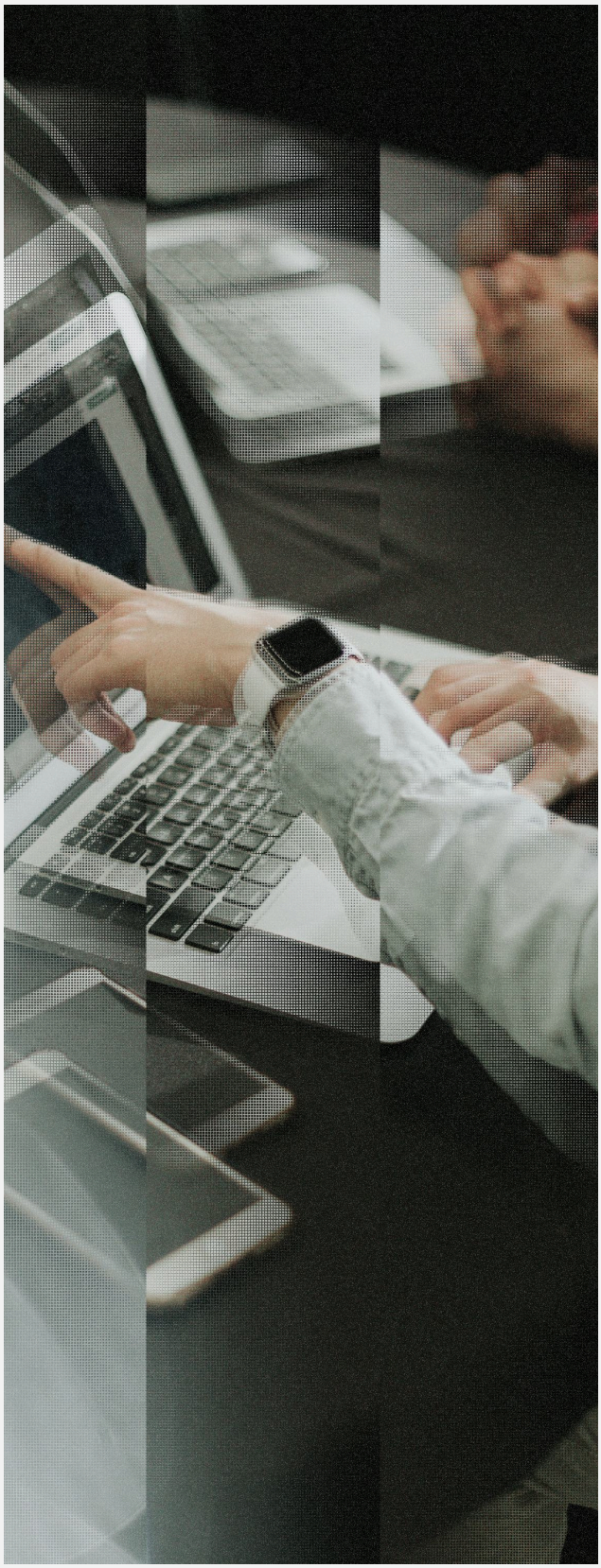
Smaller leaks—though less flashy—are more frequent and often include fresher, valid credentials. That makes them potentially more dangerous than the massive, recycled dumps.The real risk of a credential leak isn't in its size, but in the possibility that it contains a valid password granting access to a sensitive or corporate system.

Many corporate credentials are used in internet-facing systems—such as SaaS platforms and remote access via VPN. Cybercriminals are especially interested in these credentials, as they can be leveraged to launch attacks against the targeted companies.

The primary source of fresh, high-value credentials is infostealers. Employees may unknowingly be infected with these malware strains, which extract all stored credentials from the system. And because of Bring Your Own Device (BYOD) policies, infostealer operators can use a wide range of lures to distribute the malware—including those targeting personal use, like social media content.

As a result, infostealers can steal corporate credentials from personal devices—creating serious challenges for companies in terms of visibility and response.

Massive credential dumps are published from time to time, but they are only a symptom of a broader, ongoing threat: the daily theft of credentials through infostealers and other tactics.



Mitigation Strategies Beyond MFA

Multi-factor authentication (MFA) can prevent simple credentials (like usernames and passwords) from being used successfully to breach a system. However, valid access credentials can still be leveraged by attackers to launch MFA-targeted attacks.

The type of attack that can bypass MFA depends on the specific method in use.

Attacks Targeting Different MFA Methods

MFA Method	Threats
App-based Authorization	User error (can be exploited through push bombing / MFA fatigue)
SMS/Voice Code	Phishing, SIM swapping, network attacks (SS7)
OTP (One-Time Password via physical key or app)	Phishing attacks

When dealing with large-scale password leaks—typically involving old and simple credentials—MFA still plays an important role in mitigating potential exploitation.

That said, MFA is not always effective against infostealers or the consequences of the daily credential leaks they generate. Infostealers can extract token-based credentials stored in browser cookies or by installed software. These tokens allow attackers to clone authenticated sessions—completely bypassing the MFA process.

There are also cases where users disable MFA due to usability issues with the second authentication factor.

Additionally, attackers can use access gained through infostealers to authorize new access tokens or even set up new MFA mechanisms on the victim's account. For example, if the victim originally used SMS for MFA, the attacker might configure an OTP generator app—maintaining access without needing the phone number.

For these reasons, MFA alone doesn't cover all scenarios involving compromised credentials.

Fortunately, the circulation of stolen credentials within the cybercrime ecosystem makes it possible to monitor and revoke them before attackers can exploit them.

Leaked credential monitoring adds a critical layer of defense—helping protect identities in a range of scenarios. It acts as a complement to MFA and other privileged access management measures, strengthening the overall protection of corporate systems.

Identity Management Recommendations

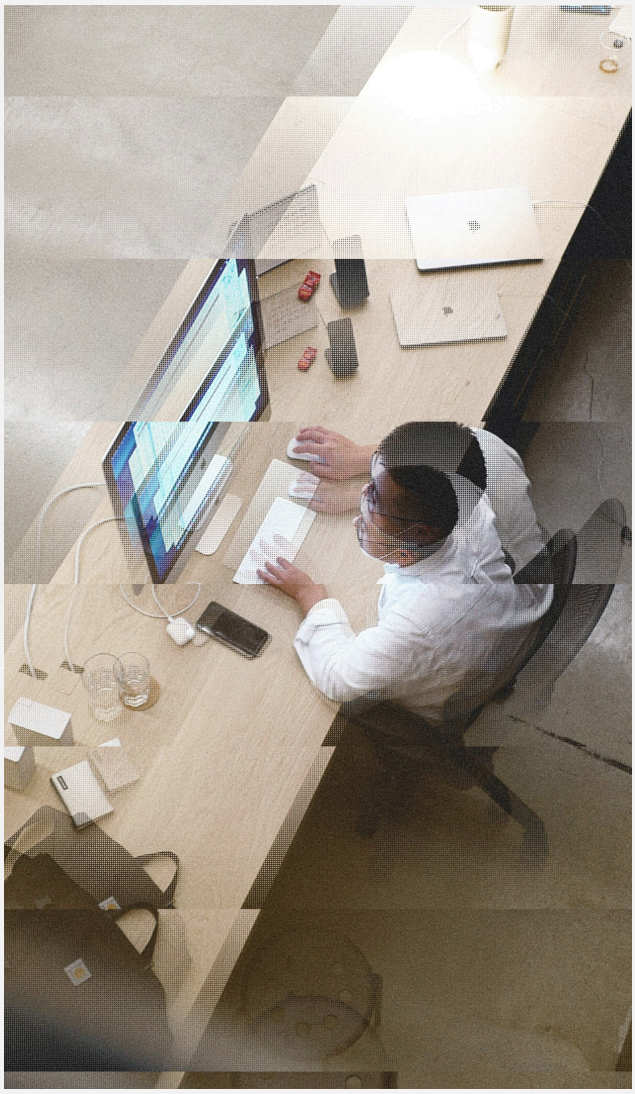
Monitor Leaked Credentials

Leaked credential monitoring helps your company identify when corporate credentials are circulating in criminal networks. It's a key intelligence signal that enables immediate preventive actions—such as resetting the password, investigating the source of the leak, and improving internal training programs or BYOD policies.

In a resilience or defense-in-depth context, monitoring helps prevent attacks that could stem from process failures that left old credentials exposed. It also plays a critical role in protecting systems vulnerable to token theft or platforms where MFA adoption is not feasible.

It's one of the simplest measures to implement—requiring no changes to your corporate network.

Talk to an Axur expert to learn how credential monitoring can help protect your business.



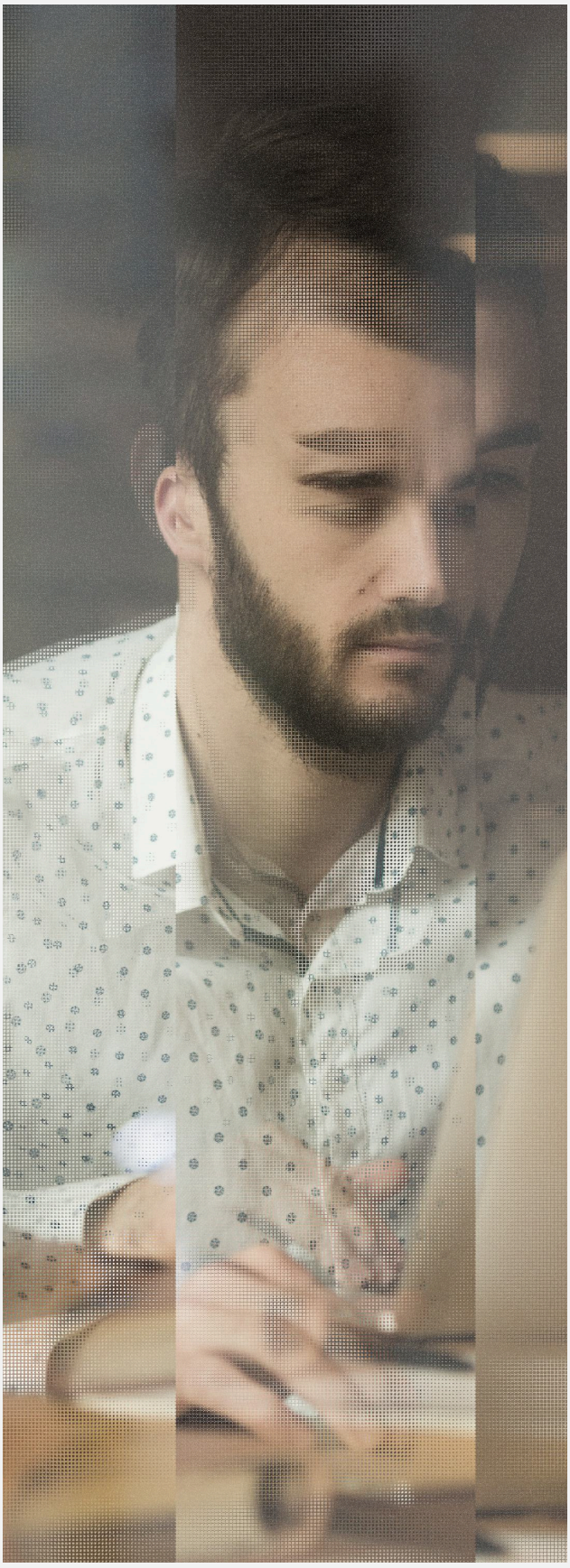
Protect Exposed External Assets

VPN systems, externally accessible dashboards, and web applications are frequent targets for credential-based attacks because they're exposed to the internet. External Attack Surface Management (EASM) helps maintain an up-to-date inventory of these assets—supporting both identity management and vulnerability management efforts.

Adopt Least Privilege and Zero Trust

Applying the principle of least privilege helps reduce the impact of a credential leak by limiting the attacker's access within corporate systems. However, many work activities still require some level of privilege—meaning that even limited access can have serious consequences.

Whenever possible, least privilege should be extended with a zero trust approach. In this model, users must re-authenticate before performing sensitive actions—using mechanisms like just-in-time access or access session monitoring.



Manage the Identity Lifecycle

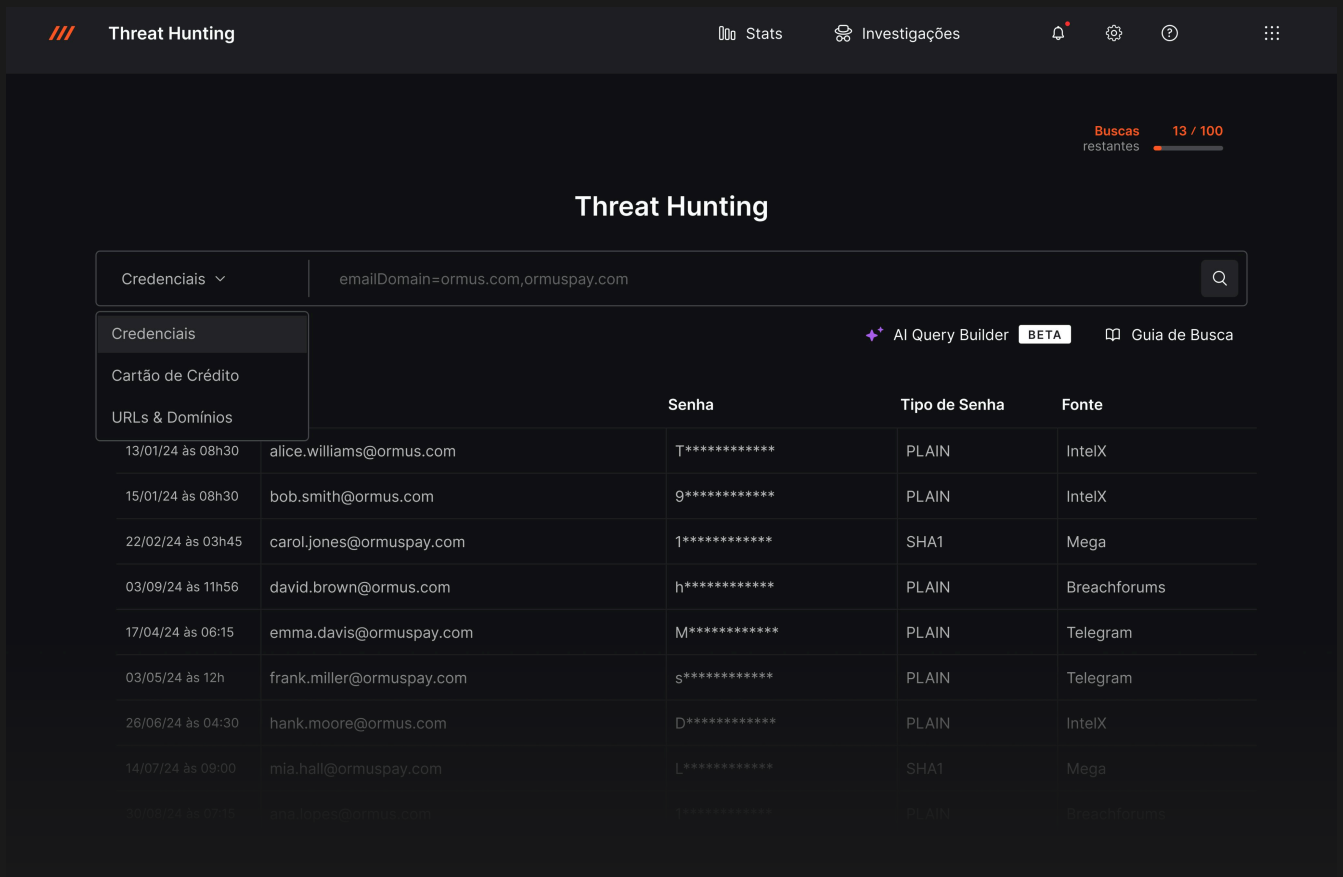
Some of the most vulnerable credentials are those left out of the identity management process. This often happens when outdated identities are never deactivated or stripped of their permissions. Because they're obsolete, these credentials tend to remain static and valid for long periods—potentially exposing data they weren't originally meant to access.

That's why it's critical to manage credentials throughout their full lifecycle. When necessary, corporate credentials should be sanitized—removing any that are no longer needed.

Use Phishing-Resistant MFA

While infostealers can bypass certain MFA implementations, multi-factor authentication still plays an important role in protecting identities—especially in phishing scenarios. For this reason, your MFA solution should be phishing-resistant. That means avoiding one-time passwords (OTP) generated by apps or sent via SMS—the latter being the least recommended method. Since OTPs can be easily handed over by users in a phishing attack, they're inherently more vulnerable.

FIDO keys and physical security tokens are considered stronger options, but they can involve technical and financial constraints. App-based push authorization is a viable alternative, but it should be paired with employee awareness around MFA fatigue and push bombing attacks.



About Axur

Axur is a cost-effective external cybersecurity solution that empowers security teams to handle threats beyond the perimeter. Our platform detects, inspects, and responds to brand impersonation, phishing scams, dark web mentions, threat intel vulnerabilities, and more.

With the world's best takedown, Axur removes malicious content quickly and efficiently 24×7, automatically handling 86% of detections. Our AI-powered tools scale threat intelligence 180x, freeing your security team to focus on strategic initiatives.

See how our solutions can transform your security strategy

BOOK A DEMO

Gartner Peer Insights 4.8

Explore all our solutions at **axur.com**

///AXUR