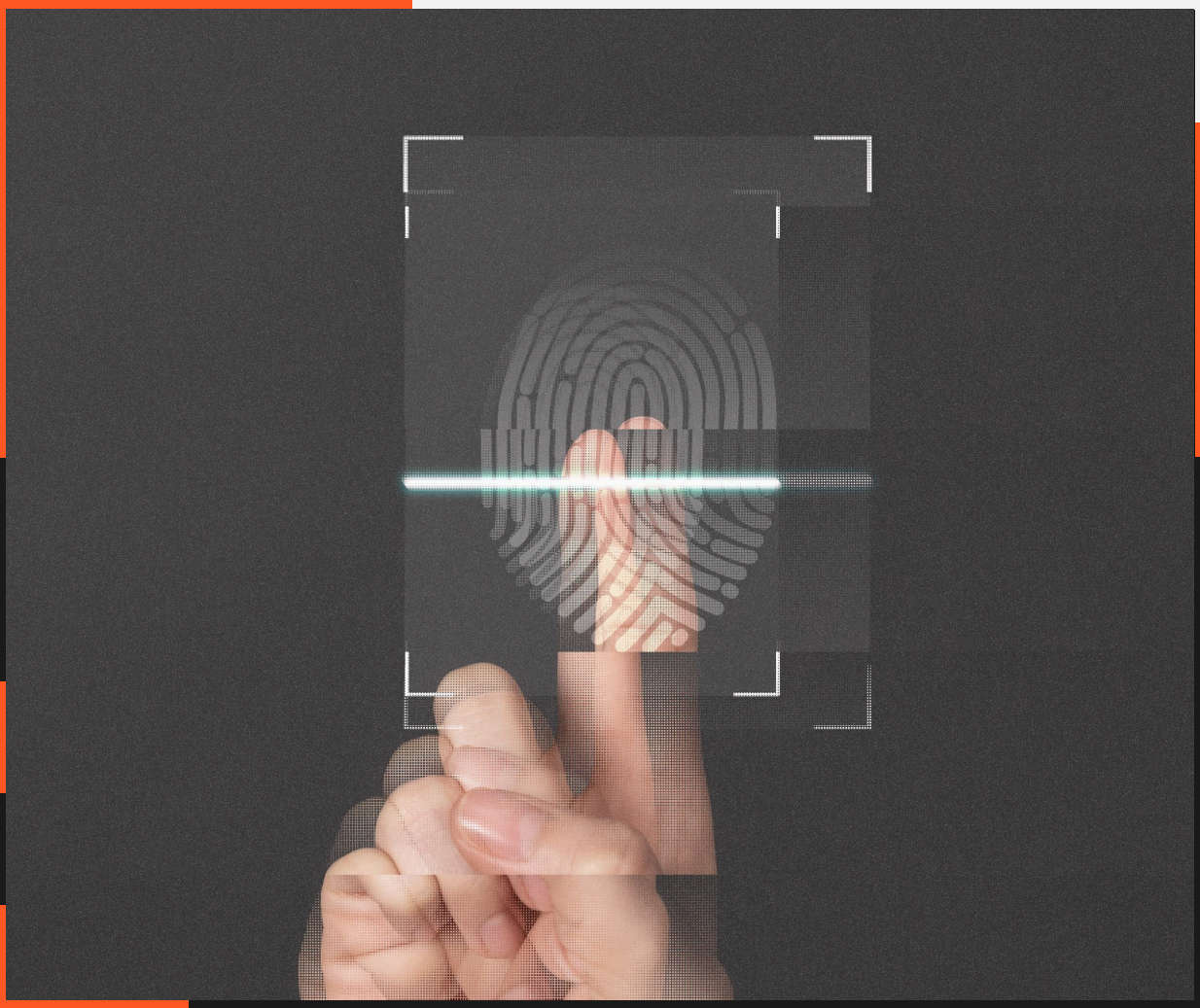


Credenciales en juego

Novedades en las últimas filtraciones: reflexiones y aprendizajes

AXUR

Resumen ejecutivo

Las filtraciones masivas de credenciales pueden generar alarma y acaparar titulares en la prensa de vez en cuando. El caso reciente de un actor malicioso que ofrecía un paquete con 16 mil millones de credenciales es solo el último ejemplo —pero no es nuevo ni especialmente relevante. Este tipo de recopilaciones ya se ha vuelto una práctica regular, aunque esporádica.

Por ahora, no hay razones para creer que estos datos sean originales. Sin embargo, la publicación de un gran conjunto de credenciales antiguas puede representar un nuevo riesgo, ya que más actores maliciosos tendrán acceso a esa información. Aun así, este no debería ser el principal foco de atención.

Los riesgos asociados a las filtraciones de credenciales van mucho más allá de estos casos puntuales. El robo y uso indebido de credenciales es una amenaza constante, que resulta en la exposición de millones de credenciales nuevas cada mes.

Este tipo de dato es altamente valioso para los atacantes. Según el informe Verizon Data Breach Investigations Report (DBIR), el uso indebido de credenciales es el vector inicial en el 22 % de los incidentes. Aunque no sean tan mediáticas, estas filtraciones recurrentes pueden ser aún más graves que los grandes paquetes de credenciales.

Mientras las recopilaciones masivas suelen contener datos repetidos y contraseñas obsoletas, los archivos diarios compartidos por grupos criminales traen credenciales recién robadas—muchas veces desde una máquina que aún se encuentra en uso.

Estas recopilaciones reflejan un ecosistema criminal que incentiva económicamente el comercio de credenciales robadas y que desarrolla software malicioso especializado—los infostealers—para nutrir ese ecosistema a diario.

Es bajo esta perspectiva que deben interpretarse noticias como esta. En nuestras organizaciones, es fundamental centrarse en los aspectos más peligrosos de esta amenaza, como la capacidad de los infostealers de evadir la autenticación multifactor (MFA).

Este material repasa la historia de las grandes filtraciones de credenciales, sus orígenes, y las motivaciones detrás de su publicación. Al final, ofrecemos recomendaciones prácticas para mejorar la gestión de identidades y credenciales, con medidas que ayudan a prevenir y mitigar los ataques.

Un repaso a las principales filtraciones de credenciales

Las filtraciones masivas no son novedad. En 2012, sitios como LinkedIn, eHarmony y Last.fm fueron víctimas de ciberataques que expusieron millones de contraseñas. El paquete inicial de LinkedIn, con 6,5 millones de credenciales, pareció alarmante en su momento, pero fue solo una fracción: en 2016, resurgió con 165 millones de cuentas y 117 millones de contraseñas.

Ese nuevo paquete fue ofrecido públicamente a cualquier interesado, una práctica que se volvió común. Es habitual que los criminales publiquen una parte del contenido como "muestra gratis" para ganar credibilidad y aumentar las ventas.

Así ocurrió en 2019 con la Collection #1, la primera de cinco recopilaciones. Cuatro de ellas estaban en venta, mientras que la primera fue publicada como forma de promoción.

En total, las cinco colecciones sumaban 2.200 millones de credenciales, el mayor paquete hasta esa fecha.

El potencial de lucro por vender estos paquetes incentivó la creación de recopilaciones aún mayores.

También motivó la especialización de actores en el robo y la revalidación de credenciales a través de técnicas como el credential stuffing—que consiste en probar credenciales filtradas en distintos servicios para identificar combinaciones que aún funcionan.

Cuando los datos de LinkedIn fueron expuestos en 2012, muchos usuarios tuvieron que cambiar sus contraseñas, reduciendo el impacto. Pero si esas mismas credenciales funcionaban en otros servicios, los atacantes podían seguir aprovechándolas.

Sin embargo, mediante ataques de credential stuffing, los atacantes pueden identificar otros servicios donde se reutilizó la misma combinación de nombre de usuario y contraseña. Como esos servicios no fueron comprometidos directamente, los usuarios nunca recibieron una alerta para restablecer sus contraseñas allí, al contrario de lo que ocurrió con LinkedIn. Y como la mayoría de las personas no actualiza sus contraseñas en todos los servicios que usa, este proceso de revalidación puede terminar siendo incluso más eficaz que la filtración original.

El credential stuffing permite descubrir credenciales reutilizadas en otros servicios donde no se forzó un cambio de contraseña. Así, credenciales aparentemente obsoletas pueden volverse valiosas otra vez.

También permite a los atacantes ofrecer "nuevas" credenciales que en realidad son antiguas, pero reutilizadas o revalidadas.

Este fenómeno fue evidente en Collection #1, que contenía solo 21 millones de contraseñas únicas, pero más de 1.100 millones de combinaciones usuario/contraseña—una clara señal de reutilización.

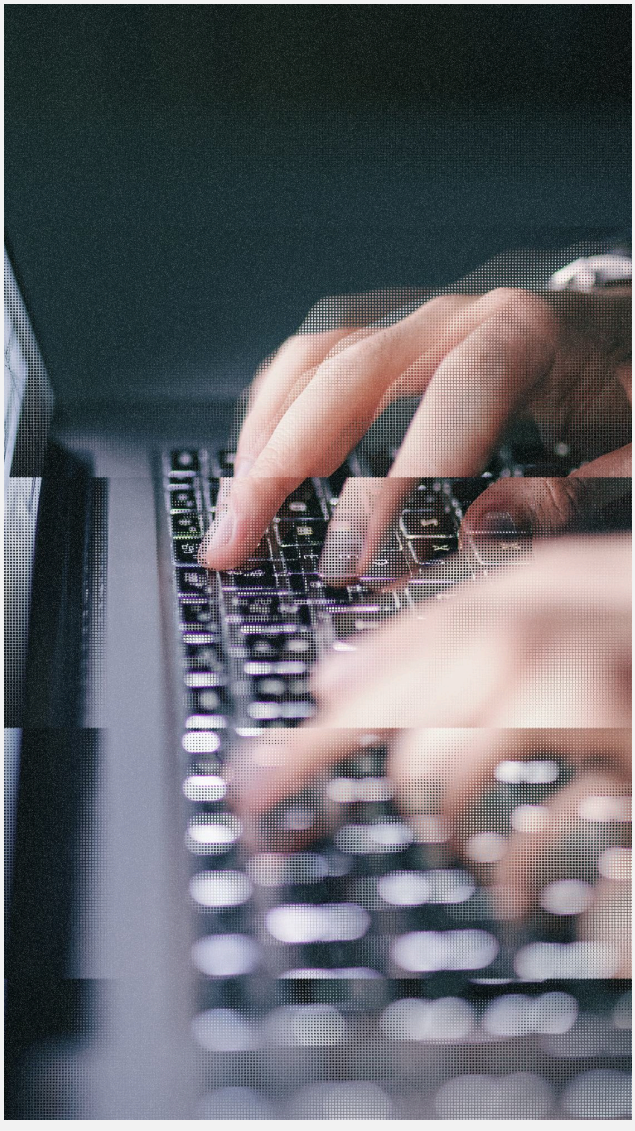
Al mismo tiempo, crecía el uso de infostealers: malware diseñado para robar credenciales desde navegadores u otras aplicaciones. Estos programas suelen difundirse a través de dispositivos personales (especialmente en ambientes BYOD), usando cebos como redes sociales.

En ese contexto, no pasó mucho tiempo antes de que los números de la Collection fueran superados. Eso ocurrió en 2021, cuando se publicó una nueva recopilación llamada “RockYou2021”. El nombre hacía referencia a un ciberataque ocurrido en 2009 contra RockYou, una empresa conocida por desarrollar aplicaciones para redes sociales como MySpace y Facebook. Aquella filtración original expuso los datos de 32 millones de usuarios de RockYou.

RockYou2021 no se limitaba a los datos de aquella filtración antigua. Con 8.400 millones de registros, se trataba de una nueva recopilación de credenciales extraídas de muchas otras filtraciones anteriores, además de combinaciones revalidadas, brechas causadas por botnets, campañas de phishing, infostealers e incluso datos posiblemente inventados.

El paquete fue actualizado y republicado en 2024 bajo el nombre de “RockYou2024”, alcanzando un total de 9.940 millones de credenciales.

En 2025, se publicó otro volcado masivo de credenciales, esta vez con la afirmación de contener 16 mil millones de registros.



16 mil millones de credenciales: contexto y riesgos

Aunque algunos medios lo trataron como una nueva filtración, este paquete parece repetir el patrón anterior: datos antiguos, combinaciones recicladas y muchos registros duplicados o inválidos. Es probable que pocas credenciales sean inéditas, y no todas sean auténticas.

Un análisis preliminar de Axur sugiere que el paquete tiene baja relevancia, por las siguientes razones:

- Fue publicado el 23 de mayo por una cuenta reciente y sin reputación.
- No se ofreció una muestra para validar la calidad del contenido.
- No generó interés significativo entre otros actores delictivos.

Dado que el objetivo del actor malicioso es vender este paquete a otros criminales, no hay ninguna garantía sobre la autenticidad del material ni sobre las afirmaciones realizadas. Y como el autor de esta filtración no tiene un historial conocido ni una reputación establecida, sus declaraciones deben ser tomadas con cautela.

En la práctica, esto significa que es muy probable que el conjunto de datos contenga registros de baja calidad, incluyendo:

→ Credenciales de filtraciones anteriores, con poco o ningún valor nuevo;

→ Datos preparados para revalidación pero nunca verificados—esencialmente credenciales falsas o inválidas;

→ Credenciales muy antiguas, cuyas contraseñas probablemente ya fueron cambiadas y están fuera de uso;

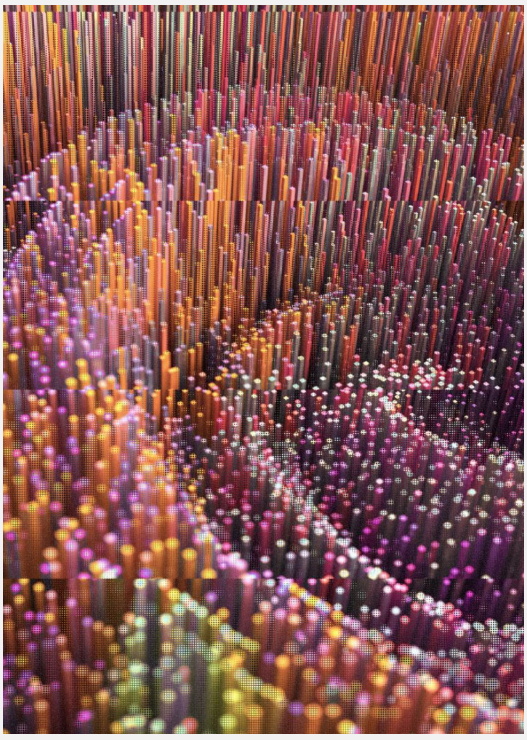
→ Datos inventados o falsificados, agregados solo para inflar el volumen total—difíciles de verificar debido a la magnitud del archivo;

→ Credenciales duplicadas, resultado de la mezcla de recopilaciones de filtraciones anteriores.

La re-publicación de credenciales filtradas anteriormente es una práctica muy común en los foros criminales. En 2024, los sistemas de Axur detectaron 56 mil millones de credenciales filtradas. Sin embargo, tras el procesamiento y depuración de los datos —para reducir falsos positivos y priorizar exposiciones que representan un riesgo real—menos de una quinta parte podía considerarse única y no vista previamente.

Desde la perspectiva del atacante, es casi imposible distinguir entre una credencial antigua ya invalidada y una completamente falsa. La mayoría de los sistemas modernos siguen buenas prácticas que evitan revelar si una cuenta existe, utilizando mensajes de error genéricos que no especifican si la contraseña es incorrecta o si la cuenta no está registrada.

Por ello, los estafadores que buscan lucrar vendiendo paquetes de credenciales tienen un fuerte incentivo para manipular los datos, inflando los volúmenes con registros de bajo valor. Esto es aún más probable cuando la oferta proviene de un actor sin reputación establecida, como ocurre con este nuevo paquete que afirma contener 16 mil millones de credenciales.



¿Cuáles son los riesgos?

Incluso si el paquete de credenciales contiene pocos registros nuevos o válidos, el hecho de que circule como un conjunto unificado tiende a ampliar su difusión dentro del ecosistema criminal—tal como ocurrió con Collection #1 y RockYou.

Si una organización ya gestionó correctamente un incidente previo relacionado con credenciales ahora presentes en este paquete, es poco probable que vuelva a ser atacada usando esos mismos datos. Sin embargo, aún existe riesgo para empresas e individuos que no han sido atacados con esas credenciales.

Los grupos criminales suelen buscar credenciales valiosas que aún no han sido explotadas, lo que puede dar lugar a campañas de gran impacto. En 2024, por ejemplo, esto sucedió con empresas que utilizaban el servicio de almacenamiento en la nube Snowflake.

Según el informe Verizon Data Breach Investigations Report de 2025, el 22 % de las brechas comienzan con una credencial robada. Dicho esto, la ausencia de credenciales nuevas o válidas en este paquete no significa que las filtraciones de credenciales no representen una amenaza para el negocio.

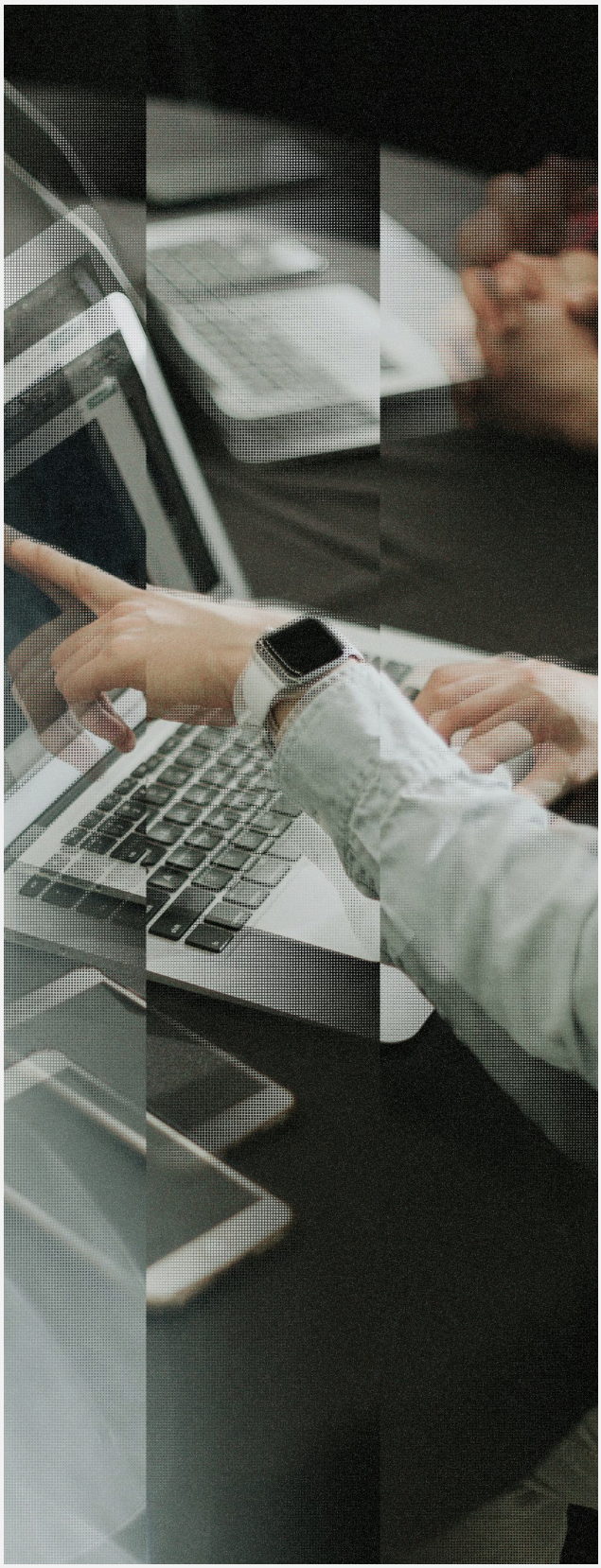
Las filtraciones más pequeñas—aunque menos visibles—son más frecuentes y suelen contener credenciales recientes y válidas. Eso las convierte, potencialmente, en un riesgo mayor que los paquetes masivos y reciclados. El verdadero peligro de una filtración no está en su volumen, sino en la posibilidad de que contenga una contraseña válida que brinde acceso a un sistema sensible o corporativo.

Muchas credenciales corporativas se utilizan en sistemas expuestos a internet, como plataformas SaaS y accesos remotos mediante VPN. Los ciberdelincuentes muestran un gran interés por estas credenciales, ya que pueden utilizarlas para lanzar ataques contra las empresas objetivo.

La principal fuente de credenciales recientes y valiosas son los infostealers. Los empleados pueden infectarse sin saberlo con este tipo de malware, que extrae todas las credenciales almacenadas en el sistema. Y debido a las políticas de Bring Your Own Device (BYOD), los operadores de infostealers pueden valerse de una amplia variedad de cebos para distribuir el malware, incluso aquellos relacionados con el uso personal del dispositivo, como contenido en redes sociales.

Como consecuencia, los infostealers pueden robar credenciales corporativas desde dispositivos personales, lo que genera serios desafíos para las empresas en términos de visibilidad y respuesta.

Los paquetes masivos de credenciales se publican ocasionalmente, pero no son más que un síntoma de una amenaza mayor y constante: el robo diario de credenciales mediante infostealers y otras técnicas.



Estrategias de mitigación más allá del MFA

La autenticación multifactor (MFA) puede impedir que credenciales simples (como usuario y contraseña) sean utilizadas con éxito para comprometer un sistema. Sin embargo, los atacantes aún pueden aprovechar credenciales válidas para ejecutar ataques dirigidos específicamente contra la MFA.

El tipo de ataque viable dependerá del método específico de MFA implementado.

Ataques según el tipo de MFA

Método de MFA	Amenazas
Autorización mediante app	Error del usuario (explotable mediante push bombing / MFA fatigue)
Código por SMS o llamada	Phishing, SIM swapping, ataques a red (SS7)
OTP (clave física o app)	Phishing

En el contexto de filtraciones masivas de contraseñas—generalmente con datos antiguos y simples—el MFA sigue teniendo un papel importante para mitigar intentos de explotación.

Dicho esto, el MFA no siempre es eficaz frente a los infostealers ni frente a las consecuencias de las filtraciones diarias de credenciales que estos generan.

Los infostealers pueden extraer credenciales en formato de token almacenadas en cookies del navegador o por software instalado en el sistema. Estos tokens permiten clonar sesiones autenticadas, eludiendo por completo el proceso de autenticación multifactor.

También existen casos en los que los propios usuarios desactivan el MFA debido a dificultades en el uso del segundo factor de autenticación.

Además, los atacantes pueden aprovechar el acceso obtenido mediante infostealers para autorizar nuevos tokens de acceso o incluso configurar nuevos mecanismos de MFA en la cuenta de la víctima. Por ejemplo, si la víctima usaba SMS como segundo factor, el atacante podría configurar una aplicación generadora de OTP para seguir accediendo sin necesidad del número de teléfono.

Por estas razones, el MFA por sí solo no cubre todos los escenarios relacionados con credenciales comprometidas.

Afortunadamente, la circulación de credenciales robadas dentro del ecosistema delictivo permite monitorearlas y revocarlas antes de que los atacantes puedan explotarlas.

El monitoreo de credenciales filtradas añade una capa crítica de defensa, ayudando a proteger identidades en diversos contextos.

Funciona como un complemento al MFA y a otras medidas de gestión de accesos privilegiados, reforzando la protección general de los sistemas corporativos.

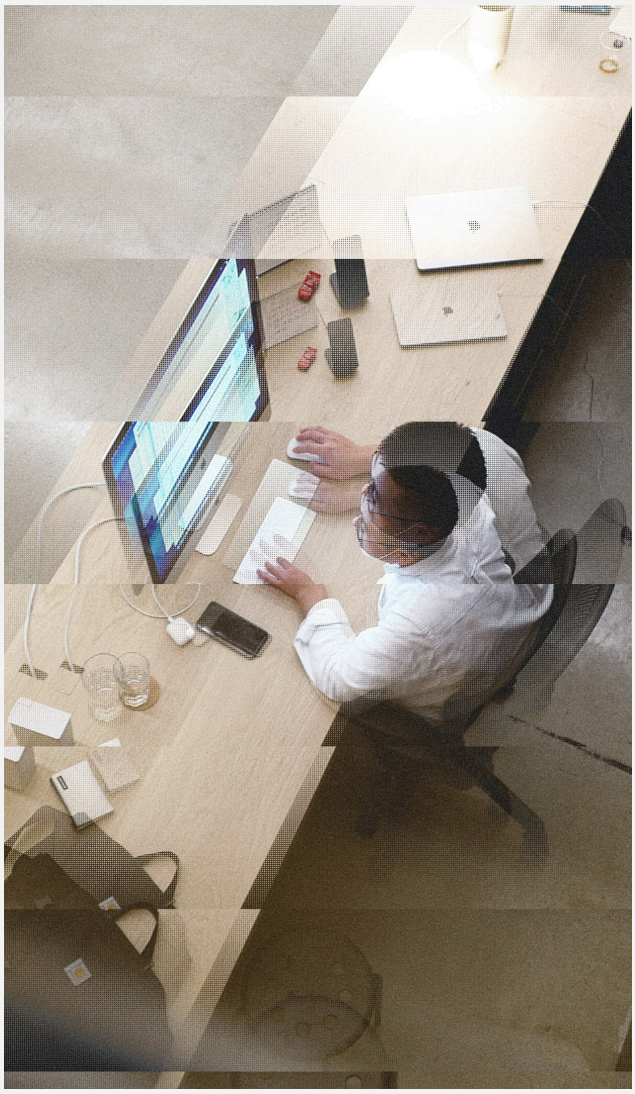
Recomendaciones para la gestión de identidades

Monitorear credenciales filtradas

El monitoreo de credenciales filtradas permite a su empresa identificar cuándo credenciales corporativas están circulando en redes criminales. Es una señal de inteligencia clave que posibilita acciones preventivas inmediatas—como restablecer contraseñas, investigar el origen de la filtración y mejorar programas de capacitación interna o políticas de BYOD.

En un enfoque de resiliencia o defensa en profundidad, este monitoreo ayuda a prevenir ataques que podrían originarse en fallos de procesos que dejaron expuestas credenciales antiguas. También cumple un papel fundamental en la protección de sistemas vulnerables al robo de tokens o en plataformas donde la adopción de MFA no es viable. Es una de las medidas más sencillas de implementar, ya que no requiere cambios en la red corporativa.

Hable con un experto de Axur y descubra cómo el monitoreo de credenciales puede ayudar a proteger su negocio.



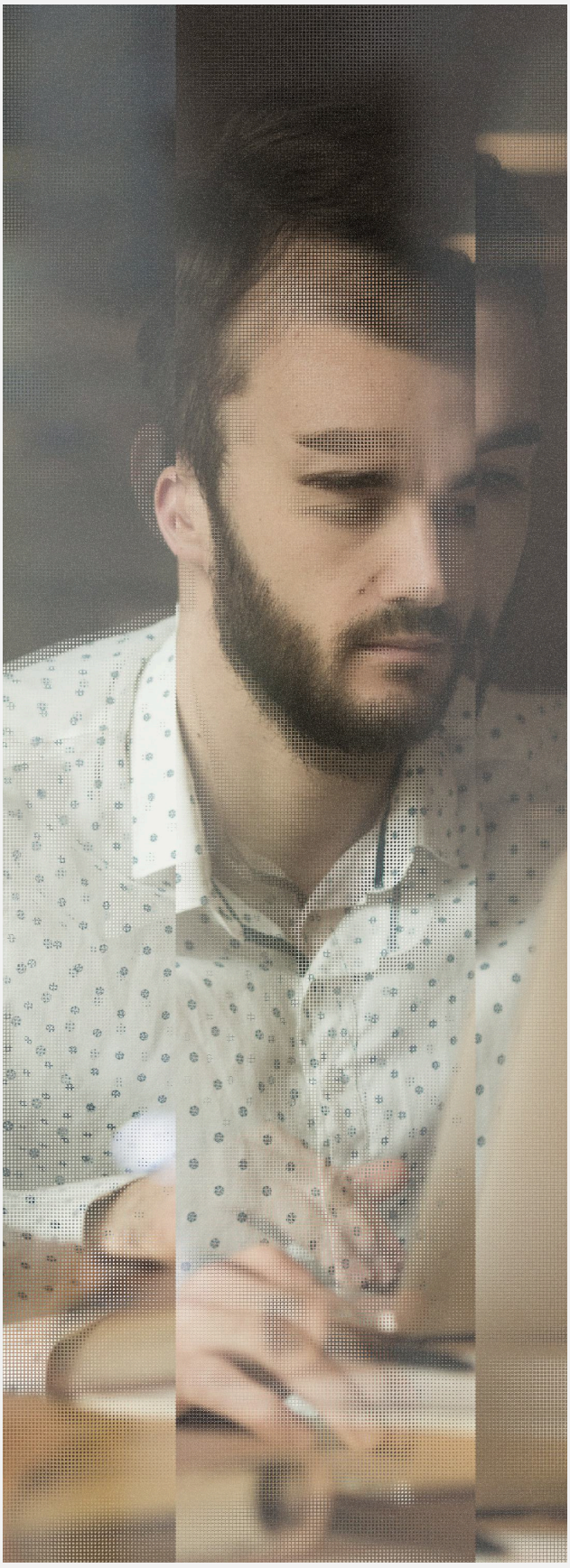
Proteger activos externos expuestos

Los sistemas VPN, dashboards con acceso externo y aplicaciones web son objetivos frecuentes de ataques basados en credenciales, ya que están expuestos a internet. La Gestión de la Superficie de Ataque Externa (External Attack Surface Management – EASM) permite mantener un inventario actualizado de estos activos, lo que contribuye tanto a la gestión de identidades como a la gestión de vulnerabilidades.

Adoptar privilegios mínimos y enfoque Zero Trust

Aplicar el principio de privilegio mínimo ayuda a reducir el impacto de una filtración de credenciales, ya que limita el acceso del atacante dentro del entorno corporativo. Sin embargo, muchas tareas laborales requieren cierto nivel de privilegio, lo que significa que incluso un acceso limitado puede tener consecuencias relevantes.

Siempre que sea posible, el privilegio mínimo debe complementarse con un enfoque de Zero Trust. En este modelo, el usuario debe volver a autenticarse antes de realizar acciones sensibles, utilizando mecanismos como acceso just-in-time o monitoreo de sesiones de acceso.



Gestionar el ciclo de vida de las identidades

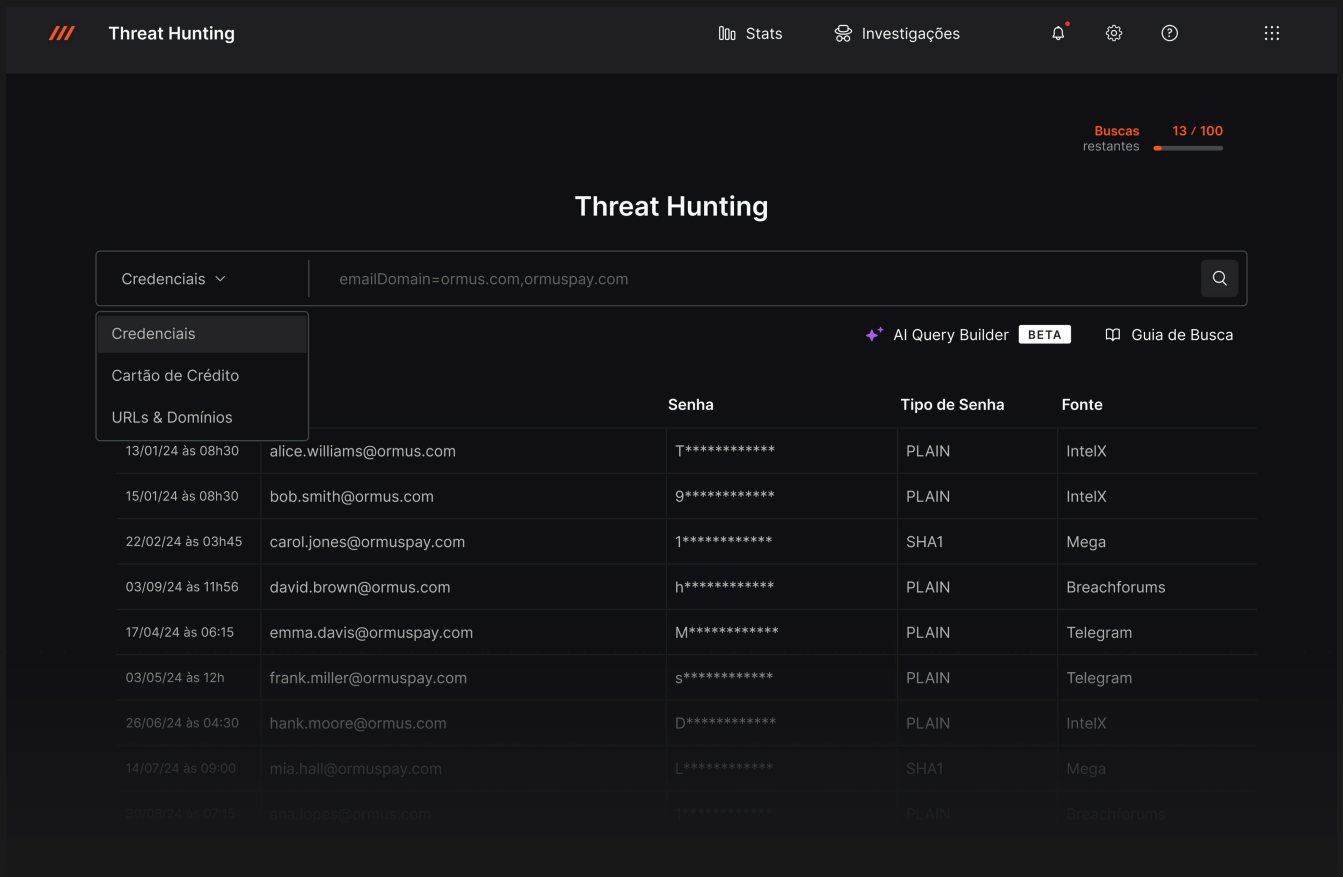
Algunas de las credenciales más vulnerables son aquellas que quedan fuera del proceso de gestión de identidades. Esto ocurre con frecuencia cuando identidades obsoletas no se desactivan ni se les revocan los permisos. Al quedar en desuso, estas credenciales tienden a permanecer estáticas y válidas durante largos períodos—lo que puede exponer datos a los que originalmente no debían tener acceso.

Por eso es fundamental gestionar las credenciales a lo largo de todo su ciclo de vida. Cuando sea necesario, las credenciales corporativas deben ser saneadas, eliminando aquellas que ya no son necesarias.

Utilizar MFA resistente al phishing

Aunque los infostealers pueden eludir algunas implementaciones de MFA, la autenticación multifactor sigue siendo una medida clave para proteger identidades—especialmente frente a ataques de phishing. Por ello, es recomendable utilizar una solución de MFA que sea resistente al phishing. Esto implica evitar métodos basados en contraseñas de un solo uso (OTP) generadas por aplicaciones o enviadas por SMS—este último es el menos recomendable. Las OTP pueden ser fácilmente entregadas por el usuario durante un ataque de phishing, lo que las vuelve inherentemente vulnerables.

Las llaves FIDO y los tokens físicos de seguridad son opciones más sólidas, aunque pueden implicar desafíos técnicos o financieros. La autorización mediante notificaciones push en una app es una alternativa viable, pero debe complementarse con programas de concienciación sobre amenazas como el MFA fatigue o el push bombing.



Sobre Axur

Axur es la empresa líder de ciberseguridad externa que empodera a los equipos de seguridad de la información para gestionar amenazas más allá del perímetro. Nuestra plataforma detecta, inspecciona y responde a la suplantación de marca, estafas de phishing, menciones en la deep & dark web, vulnerabilidades, exposiciones y más.

Con flujos automatizados y el mejor takedown del mercado funcionando 24/7, Axur elimina contenido malicioso de manera rápida y eficiente, gestionando el 86% de las detecciones automáticamente. Nuestras herramientas potenciadas por IA escalan la inteligencia de amenazas x180 veces, liberando a su equipo para que se concentre en iniciativas estratégicas.

Descubra cómo nuestras soluciones transforman su seguridad

AGENDE UNA DEMO

Gartner Peer Insights 4.8

Explore todas nuestras soluciones en **axur.com**

///AXUR