Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

# CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

# THE MOTHER OF ALL BREACHES REVELA 26 MIL MILLONES DE REGISTROS

*24/ 01 / 2024*

# CONTENIDO

## INTRODUCCIÓN

En lo que podría considerarse la madre de todas las brechas, se ha descubierto una filtración masiva que involucra una asombrosa cantidad de 26 mil millones de registros, abarcando 12 terabytes de información. Este supermasivo evento de seguridad combina datos de filtraciones anteriores, incluyendo información de plataformas como LinkedIn, Twitter, Weibo, y Tencent. La magnitud de esta brecha la convierte, sin duda, en la más grande jamás descubierta.

## THE MOTHER OF ALL BREACHES REVELA 26 MIL MILLONES DE REGISTROS

A continuación, se encuentra en cuadro de identificación de la amenaza.

| | |
|---|---|
| **ID de alerta:** | DSOC-CERT_2024_01_24_1 |
| **Clasificación de alerta:** | Noticia |
| **Tipo de Impacto:** | Alta |
| **TLP (Clasificación de información):** | **CLEAR** |
| **Fecha de publicación:** | 24/01/2024 |
| **Es día cero (0 day):** | No |

## Resumen

En lo que podría considerarse una pesadilla para la seguridad cibernética, ha surgido la noticia de una brecha de datos masiva, la "Mother of all breaches" (MOAB), con un volumen extraordinario de 26 mil millones de registros. Esta brecha, descubierta por el experto en ciberseguridad Bob Dyachenko, amalgama datos de numerosas filtraciones anteriores, generando una preocupación significativa para empresas y usuarios.

Con una impresionante capacidad de 12 terabytes, la MOAB contiene información de plataformas prominentes como Tencent QQ, Weibo, MySpace, Twitter, LinkedIn, y muchas más. Cada una de las 3,800 carpetas dentro de esta brecha representa una filtración de datos previa, creando un compendio inmenso de información.

| BRAND NAME | RECORDS LEAKED |
|---|---|
| Tencent | 1.5B |
| Weibo | 504M |
| MySpace | 360M |
| Twitter | 281M |
| Wattpad | 271M |
| NetEase | 261M |
| Deezer | 258M |
| LinkedIn | 251M |
| AdultFriendFinder | 220M |
| Zynga | 217M |
| Luxottica | 206M |
| Evite | 179M |
| Zing | 164M |
| Adobe | 153M |
| MyFitnessPal | 151M |
| Canva | 143M |
| JD.com | 142M |
| Badoo | 127M |
| VK | 101M |
| Youku | 100M |

Aunque en su mayoría la brecha recopila datos de filtraciones pasadas, los investigadores alertan sobre la presencia de información potencialmente nueva. La herramienta de verificación de filtraciones de CyberNews, que normalmente utiliza datos de alrededor de 2,500 filtraciones con 15 mil millones de registros, destaca la posibilidad de que la MOAB contenga datos nunca vistos.

Los expertos sugieren que el propietario de esta monstruosa brecha podría ser un actor malicioso, un intermediario de datos o un servicio que trabaja extensamente con grandes volúmenes de información. La amplia gama de datos, incluyendo registros gubernamentales de diversos países, plantea interrogantes sobre las intenciones detrás de esta compilación masiva.

La MOAB presenta riesgos sustanciales, ya que los actores malintencionados podrían aprovechar estos datos para llevar a cabo ataques de robo de identidad, esquemas de phishing sofisticados, ciberataques dirigidos y acceso no autorizado a cuentas personales y sensibles. El hecho de que muchos usuarios reutilicen nombres de usuario y contraseñas aumenta la amenaza de ataques de relleno de credenciales.

## RECOMENDACIONES

- Utilice contraseñas fuertes y únicas para cada cuenta, evitando la reutilización de credenciales. La diversificación de contraseñas minimiza el riesgo de ataques de relleno de credenciales.
- Refuerce la seguridad de tus cuentas habilitando la autenticación de dos factores. Esta capa adicional de protección dificulta el acceso no autorizado incluso si las credenciales primarias están comprometidas.
- Ante correos electrónicos sospechosos, verifique cuidadosamente la autenticidad del remitente. La MOAB puede ser aprovechada para ataques de phishing, por lo que la precaución es clave
- Establezca alertas para detectar cualquier actividad inusual en tus cuentas. Un monitoreo activo puede ayudar a identificar intentos de acceso no autorizado a tiempo
- Cambie sus contraseñas periódicamente, especialmente aquellas vinculadas a datos sensibles. La rotación frecuente de contraseñas disminuye el riesgo de compromisos prolongados.
- Proporcione capacitación continua sobre las mejores prácticas de seguridad cibernética. Sensibilizar a los empleados reduce la probabilidad de caer en trampas digitales.
- Aproveche las herramientas de validación en línea, para verificar si tus datos han sido comprometidos. Estas herramientas le permiten tomar medidas preventivas rápidamente.
- Preste atención especial a la seguridad en dispositivos móviles, ya que estos son objetivos comunes para ataques. Instale actualizaciones de seguridad y utiliza soluciones antivirus en dispositivos móviles.

## NOTICIA COMPLETA

https://devel.group/blog/the-mother-of-all-breaches-revela-26-mil-millones-de-registros/

# CONTACTOS DE SOPORTE


**Correo electrónico:** cert@develsecurity.com

**Teléfonos directos:**

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

**Sitio Web:** https://www.devel.group/reporta-un-incidente