Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°021	Fecha: 24-01-2024
		Página: 4 de 12

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Filtración masiva de datos: La Madre de Todas las Brechas (MOAB) exponen 26 mil millones de registros		
Tipo de Ataque	Fuga de Información	Abreviatura	FugaInfo
Medios de propagación	Red, Internet, Redes sociales		
Código de familia	K	Código de Sub familia	K02
Clasificación temática familia	Uso inapropiado de recursos		

Descripción

1. **ANTECEDENTES**:

   Bob Dyachenko, investigador de ciberseguridad y propietario de SecurityDiscovery.com, así como el equipo de Cybernews, descubrieron un robo de millones de datos que el sector ya bautizó como "la Madre de Todas las Brechas" (MOAB, por sus siglas en inglés).

   Esta base de datos, con un volumen de 12 terabytes, incluye información de usuarios de servicios tan conocidos como Twitter, Dropbox, LinkedIn, Adobe, Canva y Telegram, entre otros.

2. **DETALLES:**

   Esta compilación representa un riesgo significativo, ya que los actores de amenazas podrían usar los datos agregados para una amplia gama de ataques, que incluyen robo de identidad, esquemas de phishing sofisticados, ciberataques dirigidos y acceso no autorizado a cuentas personales y sensibles.

   Entre las empresas o plataformas más afectadas por esta fuga se encuentran la china Tencent (QQ, Weibo, WeChat) con 2.000 millones de registros, MySpace con 360 millones, Twitter con 281 millones y Wattpad con 271 millones. Otras marcas afectadas incluyen Deezer, LinkedIn, AdultFriendFinder, Adobe, MyFitnessPal, Canva, VK, DailyMotion o Dropbox. Los gobiernos tampoco se han librado de esta fuga: Estados Unidos, Brasil, Alemania, Turquía y Filipinas se encuentran entre los países afectados.

   Aunque en su mayoría la brecha recopila datos de filtraciones pasadas, los investigadores alertan sobre la presencia de información potencialmente nueva. El hecho de que muchos usuarios reutilizan nombres de usuario y contraseñas aumenta la amenaza de ataques de relleno de credenciales.

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

   Para determinar si la información de la empresa o de los empleados ha sido comprometida, se puede utilizar la herramienta de validación en línea de CyberNews (ver enlaces de referencia). Esta herramienta permite verificar si las direcciones de correo electrónico o números de teléfono han sido expuestas en filtraciones de datos históricos.

3. **RECOMENDACIONES:**

   - Cambiar de manera urgente las contraseñas de todas sus cuentas, incluso en redes sociales donde puedan estar usando las mismas credenciales.
   - Practicar una higiene estricta de sus contraseñas. Utilizar contraseñas únicas y complejas, y distintas para cada una de las cuentas, y cambiarlas periódicamente.
   - Habilitar la autenticación de dos factores cuando esté disponible.
   - No hacer clic en enlaces sospechosos ni descargue archivos adjuntos de fuentes desconocidas.

Fuente de Información:	• hxxps://devel.group/blog/the-mother-of-all-breaches-revela-26-mil-millones-de-registros/ • hxxps://www.forbes.com.mx/roban-26000-millones-de-datos-en-lo-que-expertos-llaman-la-madre-de-todas-las-filtraciones/ • hxxps://cybernews.com/personal-data-leak-check/