Nro. Alerta:	AL-2025-026	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	20-jun-2025	**Filtración Masiva de Credenciales**	Pág.: **1** of **3**

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de Incidente: Información
Nivel de riesgo: Alta

II. ALERTA

Gráfica 1. Figura referencial – Fuente: DPL NEWS

Según un informe publicado, el equipo de investigación de Cybernews revisó *"30 conjuntos de datos expuestos que contenían entre decenas de millones y más de 3.500 millones de registros cada uno". En total, eso supuso "la enorme cifra de 16.000 millones de credenciales de inicio de sesión expuestas".*

III. INTRODUCCIÓN

El equipo de investigación de Cybernews, un medio especializado en ciberseguridad, ha informado sobre una de las mayores exposiciones de datos de la historia. Se trata de aproximadamente 16 mil millones de credenciales de inicio de sesión que quedaron accesibles en línea a través de bases de datos sin protección.

Estas credenciales incluyen accesos a plataformas como Apple, Google, Facebook, Telegram, y VPNs, entre otros. Los datos probablemente provienen de diferentes tipos de malware conocidos como ladrones de información, programas

que capturan contraseñas y datos confidenciales directamente de los dispositivos infectados.

IV. VECTOR DE ATAQUE

Las credenciales provienen principalmente de infostealer malware que extrae contraseñas, tokens y cookies de dispositivos comprometidos, así como del acceso a instancias en la nube mal configuradas (Elasticsearch, almacenamiento de objetos).

V. IMPACTO

- El volumen y frescura del dato implican un riesgo real e inminente de ataques automatizados.
- Especial atención en el sector cripto, posibilidad real de apropiación de wallets y acceso a semillas de recuperación.
- Filtraciones contienen cuentas personales, corporativas e incluso gubernamentales.
- Base para una "explotación masiva", al proporcionar "información nueva y utilizable a gran escala.
- Probablemente algunos de los conjuntos sean utilizados o comercializados por grupos criminales.

VI. RECOMENDACIONES:

- Cambiar inmediatamente todas las contraseñas, especialmente las reutilizadas.
- Activar autenticación multifactor (idealmente basada en Apps, no solo SMS).
- Adoptar gestores de contraseñas y sustituirlas por Passkeys donde sea posible.
- Monitorear activamente alertas en Dark Web y proteger entornos Cloud contra configuraciones inseguros.
- Implementar un monitoreo de seguridad continuo para detectar actividades inusuales en la red y sistemas que podrían indicar un ataque en curso o intentos de infiltración futuros.
- De ser víctima, contacte a las Autoridades competentes en base a la Normativa Legal Vigente.

VII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta; se proporciona con fines informativos.
- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.

- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

VIII. REFERENCIAS:

COINTELEGRAPH (2025). Filtración masiva de 16.000 millones de contraseñas genera temores sobre la seguridad cripto. https://es.cointelegraph.com/news/16b-passwords-from-apple-facebook-and-google-leaked

CICESE (2025). Una de las mayores filtraciones de la historia expone 16 mil millones de cuentas y contraseñas, advierte Cybernews. https://seguridad.cicese.mx/alerta/2486/Una-de-las-mayores-filtraciones-de-la-historia-expone-16-mil-millones-de-cuentas-y-contrase%C3%B1as,-advierte-Cybernews

LEVANTE (2025). Filtran 16.000 millones de contraseñas de Apple, Google y Facebook en uno de los mayores robos de datos de la historia. https://www.levante-emv.com/vida-y-estilo/tecnologia/2025/06/19/filtran-millones-contrasenas-datos-ciberataque-mayor-robo-historia-google-apple-facebook-118816441.html