Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

FILTRACIÓN HISTÓRICA: 16 BILLONES DE CONTRASEÑAS DE GIGANTES TECNOLÓGICOS COMO APPLE Y GOOGLE EXPUESTAS.

20/ 06 / 2025

CONTENIDO

INTRODUCCIÓN

Investigadores encontraron la filtración de credenciales más grande de toda la historia teniendo una cifra de 16 mil millones de credenciales dentro de ellas muchas son de carácter crítico.

Dentro de la filtración de credenciales se estima que hay credenciales de inicios de sesión en redes sociales como Facebook, Apple, Google, GitHub, Telegram, y algunos servicios gubernamentales.

FILTRACIÓN HISTÓRICA: 16 BILLONES DE CONTRASEÑAS DE GIGANTES TECNOLÓGICOS COMO APPLE Y GOOGLE EXPUESTAS.

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

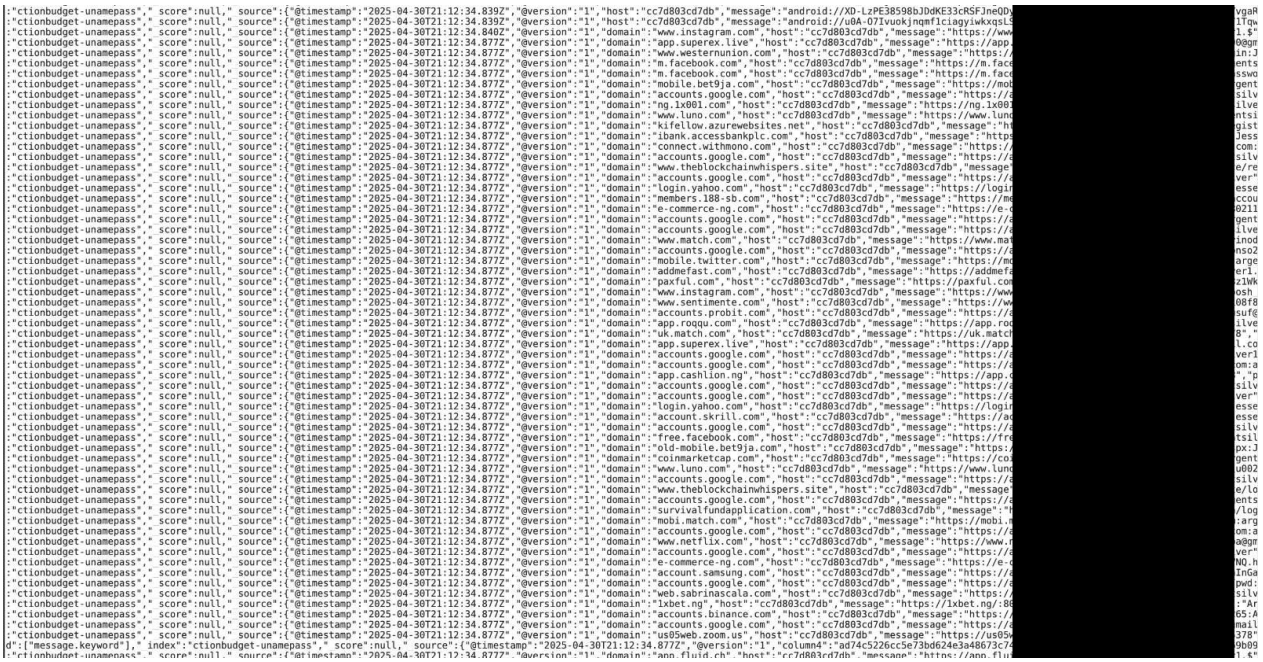
ID de alerta:	DSOC-CERT_2025_06_20_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	20/06/2025
Es día cero (0 day):	No

RESUMEN

Investigadores encontraron la filtración de credenciales más grande de toda la historia teniendo una cifra de 16 mil millones de credenciales dentro de ellas muchas son de carácter crítico.

Dentro de la filtración de credenciales se estima que hay credenciales de inicios de sesión en redes sociales como Facebook, Apple, Google, GitHub, Telegram, y algunos servicios gubernamentales.

Los investigadores lograron encontrar 30 conjuntos de datos, dentro de cada uno se incluyen 3.5 billones de registros. Siendo esta la información que incluye inicios de sesión en muchas de las redes sociales existentes. Así como plataformas corporativas y de desarrolladores.



Eso es importante puesto que los atacantes pueden aprovechar esta información para hacer campañas de phishing y así obtener cuentas de víctimas.

El gigante tecnológico Google está recomendando de manera crucial que actualicen sus cuentas a claves de acceso, de igual forma se insta a que se active el doble factor de autenticación (MFA) en caso de que no esté activo. Esto de igual forma con las redes sociales.

Es importante recalcar que las credenciales filtradas son únicas y recientes, no son credenciales que se hayan encontrado simplemente en filtraciones anteriores. Lo cual vuelve esta información de alta importancia.

El robo de las credenciales no fue dirigido directamente a las grandes empresas, si no que fue mediante malware tipo infostealer, esto extrajo información de muchos dispositivos individuales y guardó las URL de ingreso, como cookies o historiales de navegación.

¿Qué es infostealer?

Este un malware diseñado para el robo de información importante como: Credenciales, datos de tarjetas, cookies, historial de navegación, etc.

¿Cómo funciona?

Se instala de forma encubierta:

- A menudo llega a través de correos de phishing, descargas falsas, software pirata, juegos crackeados, etc.

Empieza a recolectar datos:

- Revisa los navegadores, archivos de sistema, cachés, y bases de datos locales.

Envía los datos robados:

- Los sube a un servidor remoto o los guarda en un “log” que luego es vendido o distribuido.

RECOMENDACIONES

- **Cambia todas tus contraseñas de inmediato:** Este es la parte más crítica. Asume que tus contraseñas han sido comprometidas y cambia las contraseñas de todas tus cuentas importantes lo antes posible.
- **Usa contraseñas fuertes y únicas:** Deja de usar la misma contraseña para múltiples sitios. Cada cuenta debe tener una contraseña única y compleja.
- **Activa la autenticación de dos factores (2FA/MFA):** La autenticación de dos factores (multifactor) añade una capa extra de seguridad. Además de tu contraseña, requerirá un segundo método de verificación.
- **Utiliza un gestor de contraseñas:** Esto te servirá para almacenar de manera segura contraseñas además de recomendarte contraseñas robustas.
- **Revisa la actividad de tus cuentas:** Permanece atento a cualquier actividad inusual en tus cuentas.

NOTICIA COMPLETA

https://devel.group/blog/filtracion-historica-16-billones-de-contrasenas-de-gigantes-tecnologicos-como-apple-y-google-expuestas/

CONTACTOS DE SOPORTE

Correo electrónico: cti@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://devel.group