Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CIBERATAQUE MASIVO A MOVISTAR DATOS DE 21 MILLONES DE USUARIOS EXPUESTOS

05/ 06 / 2025

CONTENIDO

INTRODUCCIÓN

En el dinámico panorama de las amenazas cibernéticas, la velocidad de respuesta ante vulnerabilidades críticas marca una diferencia significativa en la protección de datos y activos digitales. El 19 de mayo de 2025, Google emitió una actualización de seguridad urgente para su navegador Chrome, dirigida a mitigar una falla de seguridad ya identificada como explotada en entornos reales. Esta vulnerabilidad, catalogada como CVE-2025-4664, afecta directamente la integridad del proceso de carga de recursos web y expone a los usuarios al robo de información sensible.

Dado que Chrome es ampliamente utilizado tanto en entornos personales como corporativos, este incidente subraya la importancia de mantener una postura proactiva frente a actualizaciones de seguridad críticas. A continuación, se detallan los aspectos técnicos, el impacto potencial y las recomendaciones clave para usuarios y administradores de TI.

CIBERATAQUE MASIVO A MOVISTAR DATOS DE 21 MILLONES DE USUARIOS EXPUESTOS

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

ID de alerta:	DSOC-CERT_2025_06_05_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	05/06/2025
Es día cero (0 day):	No

RESUMEN

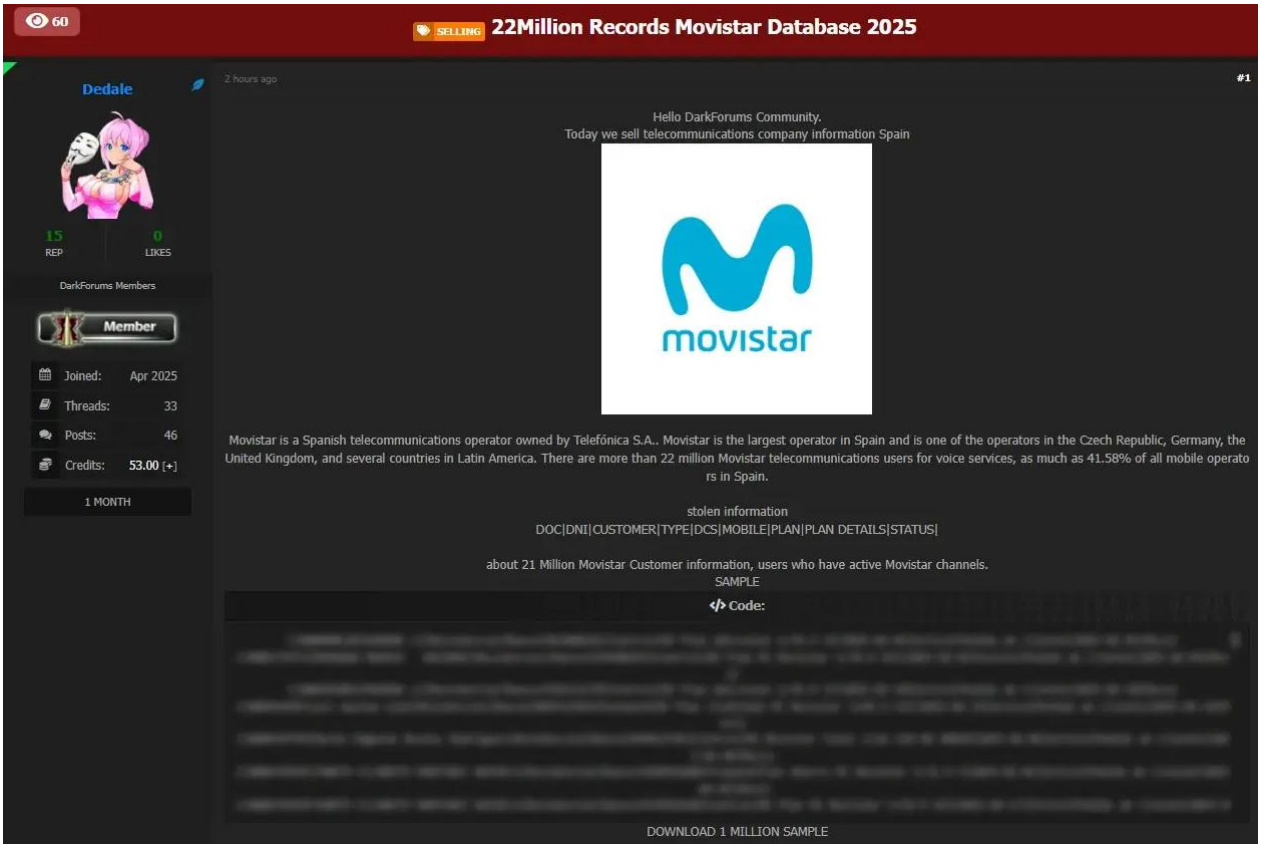
El 2 de junio de 2025, un presunto ciberataque dirigido a Movistar —el gigante de las telecomunicaciones operado por Telefónica— ha generado alarma en el ecosistema digital. De acuerdo con diversas fuentes en foros de la dark web, un actor malicioso identificado como *Dedale* asegura haber sustraído y puesto a la venta información confidencial de 21 millones de usuarios. Esta filtración representa uno de los mayores incidentes de datos reportados en el sector telco de habla hispana en lo que va del año.

¿Qué datos fueron comprometidos?

Según publicaciones del usuario *Dedale* en el foro DarkForums, la base de datos en venta incluiría:

- **Nombres completos**
- **Números de teléfono móvil**
- **Números de identificación (DNI)**
- **Detalles del plan de servicio contratado**
- **Información adicional de contacto y servicio**

Como "prueba de legitimidad", se habrían publicado registros de 1 millón de usuarios. El precio por el lote completo asciende a 1,500 dólares.



¿Qué ha dicho Movistar?

Hasta la fecha de esta publicación, Movistar no ha confirmado ni desmentido el incidente. Tampoco lo ha hecho el Instituto Nacional de Ciberseguridad (INCIBE), aunque se presume que la entidad está al tanto del caso a través de redes sociales.

Este sería el segundo incidente que afecta a Telefónica en 2025. Anteriormente, la compañía reportó una brecha en su sistema de ticketing interno, donde fueron expuestos datos de miles de empleados, incluyendo correos y documentación interna.

Impacto potencial y alcance geográfico

Aunque inicialmente se pensó que los usuarios afectados eran únicamente españoles, el set de datos de prueba incluye información de clientes en Movistar Perú, lo que sugiere un alcance internacional aún no delimitado.

Este nuevo ataque refuerza la posición de España en el tercer lugar del ranking global de ciberataques, según diversas firmas de análisis. Los expertos vinculan este repunte con factores geopolíticos, como el apoyo del gobierno español a Ucrania, lo que habría aumentado la actividad de grupos de amenazas persistentes avanzadas (APT) prorrusos y chinos.

Contexto: una tormenta cibernética en aumento

La filtración a Movistar se suma a una larga lista de incidentes recientes en territorio español. Solo en marzo de este año, una veintena de ataques DDoS impactaron a organismos como la Casa Real, la Policía Nacional y la Presidencia del Gobierno. Grupos hacktivistas como NoName057(16) y otros colectivos prorrusos habrían estado detrás de estas acciones.

También se recuerda el incidente de mediados de 2024, cuando Telefónica investigó el robo de datos de 120,000 personas, supuestamente motivado por la participación del Estado español como accionista de la empresa.

Conclusión: ¿qué deben hacer las empresas?

Este nuevo episodio subraya la urgente necesidad de estrategias de ciberseguridad más robustas, especialmente para sectores críticos como telecomunicaciones. Las organizaciones deben:

- **Reforzar sus procesos de gestión de vulnerabilidades**
- **Implementar esquemas de monitorización avanzada (XDR/SIEM)**
- **Tener capacidades claras de respuesta a incidentes y contención**
- **Realizar auditorías regulares sobre el ciclo de vida de los datos**

En un entorno cada vez más hostil, la resiliencia digital no es una opción: es una prioridad estratégica.

NOTICIA COMPLETA

https://devel.group/blog/ciberataque-masivo-a-movistar-datos-de-21-millones-de-usuarios-expuestos/

CONTACTOS DE SOPORTE

Correo electrónico: cti@devel.group

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/