Ecopetrol descarta afectación a sus operaciones tras ciberataque

La compañía estatal fue blanco de un intento de ransomware, un tipo de ciberataque que busca secuestrar información para, usualmente, exigir un pago a cambio de su rescate. Esto es lo que se sabe.

Diego Ojeda
19 de julio de 2026 - 02:23 p. m.

Ecopetrol detala que no fue afectada la identidad de los usuarios de las 3.300 cuentas que fueron ilegalmente infiltradas, ni se capturaron las credenciales de acceso de los usuarios.

Foto: Imagen generada con IA.

Para entender el potencial dañino de esta amenaza, hay que comprender qué es lo que está describi
los cibercriminales que están detrás de esta actuación.

Por un lado, está el acceso no autorizado a bases de datos, un hecho que, por sí solo, representa un i
gravedad. Sin embargo, la magnitud del impacto dependerá del tipo de información que contenían l
es lo mismo la exposición de archivos administrativos que la de datos personales, información finar
estratégicos de la compañía.

Si entre la información descargada hay datos sensibles, como información personal de usuarios o d
carácter reservado, Ecopetrol podría enfrentar un importante impacto reputacional. Además, la ev
material podría traducirse en consecuencias económicas, ya sea por demandas, sanciones regulato
afectaciones en la confianza de inversionistas, clientes y aliados.

Le puede interesar

Empresas
Ecopetrol confirma ataque digital con acceso a 3.300 cuentas

Suscriptores Empresas
Monómeros se reorganiza: claves del proceso y su impacto para los insumos del agro

Empresas
Apple supera a Nvidia y se queda con el título de la empresa más valiosa del mundo

Este tipo de accesos no autorizados puede lograrse de distintas maneras. Una de ellas es mediante ataques de fuerza bruta, en los que los ciberdelincuentes prueban de forma automatizada múltiples combinaciones de contraseñas hasta encontrar la correcta. Otra de las más frecuentes es el **phishing**, una técnica de ingeniería social que utiliza correos electrónicos, mensajes o sitios web falsos para engañar a los usuarios y hacer que revelen sus credenciales de acceso.

“El acceso no autorizado afectó entornos de almacenamiento de archivos en la nube de aproximadamente 15 compañías del GE, lo que resultó en la descarga no autorizada de datos asociados con aproximadamente 3.300 cuentas de usuario. El actor externo comunicó exigencias de extorsión, amenazando con divulgar públicamente la información extraída ilegalmente”, informó Ecopetrol

Por otro lado, está el intento de infección mediante un **ransomware**, un tipo de software malicioso (*malware*) que, una vez ejecutado, cifra o encripta los archivos de la víctima para impedir el acceso a ellos. Aunque una de las formas más comunes de infección es la apertura de archivos adjuntos o enlaces maliciosos enviados mediante correos electrónicos fraudulentos (*phishing*), los atacantes también pueden aprovechar vulnerabilidades en los sistemas o credenciales robadas para desplegar este tipo de software.

En palabras simples, es como si el atacante metiera todos los archivos en una caja fuerte para, posteriormente, pedir dinero a cambio de revelar la clave para abrirla y recuperarlos.

Cuando esto ocurre, la operación de una empresa puede verse gravemente afectada. Al quedar cifrados los archivos y sistemas críticos, los empleados pierden acceso a la información necesaria para desarrollar sus actividades, lo que puede paralizar procesos internos, interrumpir servicios y generar pérdidas económicas.

Recientemente Ecopetrol informó que, tras los últimos análisis realizados, el impacto de este ataque informático solo implicó la descarga de archivos de la compañía.

Es decir, el ataque de malware no se ejecutó, pues pudo ser contrarrestado por la defensa cibernética con la que cuenta Ecopetrol. Sin embargo, no deja de ser un asunto menor, ya que la empresa no precisa qué tan sensible es la información que lograron descargar los cibercriminales.

Estas son las medidas que sigue ejecutando la empresa tras el incidente de ciberseguridad:

• La clasificación del tipo de información descargada producto del incidente.

• Las exigencias de extorsión y amenaza con base en la información descargada ilegalmente por el a
las autoridades competentes.

• Trabajar de manera continua con el Equipo de Respuesta a Emergencias Cibernéticas de Colombia
criterio de infraestructura crítica del país; la Dirección Especializada contra los Delitos Informátic
Nación; el Comando Conjunto Cibernético de las Fuerzas Militares, CCOCI, y el Centro Cibernético

Por Diego Ojeda
@DiegoOjeda95 Dojeda@elespectador.com

Temas recomendados:

Noticias ecoómicas | Economia | Ecopetrol | Malware | Ransomware | Ataque informático | Empresas | Reputación organizacional | Breaking

Comentarios

Sé el primero en compartir tu opinión

Publicar

Suscriptores Mundial 2026

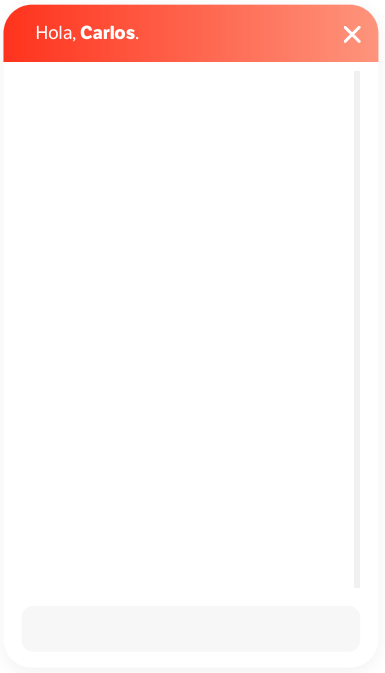
España, campeón del

Suscriptores Política

“Le reiteré a Rubio la

Suscriptores Mundial 2026

Ferrán Torres, el renegado


Hola, **Carlos**.