ATAQUES NACIONALES

Ecopetrol: el grupo atacante publicó los archivos que había anunciado

julio 27, 2026 hyperconectado

El grupo de extorsión *The Gentlemen* publicó en su sitio de filtraciones los documentos que, según había anunciado previamente, sustrajo de Ecopetrol.

MuchoHacker.lol accedió al sitio y confirmó que los archivos ya están disponibles públicamente. Esto marca una diferencia con la etapa anterior del caso, cuando el grupo solo había difundido un catálogo con la descripción de lo que decía tener en su poder.

El leak de datos está dividido en dos carpetas. El archivo Ecopetrol 1 tiene 1294 archivos y el la carpeta Ecopetrol 2 tiene 1217 carpetas. Cada una de estas 2511 archivos digitales tiene en su interior cientos o miles de documentos. Muchos de ellos con el nombre del funcionario al que pertenecería. Dentro de los archivos se pueden leer todo tipo de documentos en extensiones como excel, doc y otros.

Qué se pudo verificar

El sitio de filtración muestra ahora una carpeta con un listado extenso de archivos, organizados por nombre y tipo de documento.

Revisamos tres muestras de esos archivos. Al menos dos de ellos son consistentes, en formato y contenido, con documentación corporativa real de uso interno.

Uno de los documentos que ya es de acceso público está nombrado como 251027 Reporte Confidencial Compensacion y Beneficios. Es un archivo en Excel con varias pestañas. En este documento se incluyen los nombres y cédulas de funcionarios asi como posible información financiera.

También identificamos, dentro del listado, referencias a nombres de usuario que corresponderían a funcionarios de la entidad. Confirmamos de forma independiente, a través de fuentes abiertas, que al menos una de esas personas existe y ocupa un cargo compatible con el tipo de documentos expuestos a su nombre.

Entre el material publicado hay categorías que la propia empresa no ha detallado en sus comunicados oficiales, incluyendo información que por su naturaleza sería de carácter confidencial: registros financieros, formularios de control interno y documentación de personal.

1 Un correo de los atacantes habría salido desde la infraestructura de la Secretaría de Movilidad
2 ETB administraba la plataforma vulnerada y Movilidad cifra en 1,6 millones de bogotanos los afectados
3 Ataque a Ecopetrol: el catálogo de datos que el grupo atacante dice tener en su poder
4 Ecopetrol: el grupo atacante publicó los archivos que había anunciado
5 Cuerpos desnudos e historias clínicas a la venta: Filtración que expone a pacientes colombianos

Qué sigue sin confirmación independiente

Que estos archivos estén publicados no equivale, por sí solo, a que la totalidad del catálogo que el grupo había anunciado —cerca de 327.000 archivos y un terabyte de datos, según sus propias cifras— sea auténtico en su totalidad.

MuchoHacker.lol no pudo verificar de forma independiente si el conjunto completo de los documentos publicados proviene efectivamente de los sistemas de Ecopetrol, o si incluye material de otro origen mezclado para inflar el volumen de la filtración. Este patrón ha sido documentado previamente en operaciones de otros grupos de extorsión de datos.

Tampoco fue posible confirmar si los archivos fueron alterados antes de su publicación.

Por qué no detallamos el contenido específico

Esta redacción decidió no reproducir ni describir en detalle el contenido de los documentos publicados, ni identificar a las personas cuyos nombres aparecen asociados a ellos.

Publicar ese nivel de detalle no añade valor informativo adicional sobre el hecho central —que la información ya está expuesta públicamente— y sí incrementa el riesgo para las personas identificables cuyos datos forman parte del material filtrado.

Los funcionarios de la entidad deben saber que información privada puede estar pública en este momento y deben tomar dobles medidas de seguridad.

Ecopetrol fue consultada

MuchoHacker.lol cla mañána de hoy contactó a la oficina de Relaciones con los Medios de Ecopetrol para conocer si la compañía tiene conocimiento de esta publicación y si puede confirmar o descartar la autenticidad del material. Este artículo se actualizará con la respuesta de la empresa si esta se produce.

En su comunicado del 17 de julio, Ecopetrol ya había advertido que el actor externo amenazaba con divulgar públicamente la información como mecanismo de extorsión. Esta publicación sería, de confirmarse su origen, la materialización de esa amenaza.

A pesar de que tenemos en nuestro poder archivos que incluso están etiquetados como "confidenciales" no los vamos a publicar sus muestras o parte como siempre lo hacemos. Esta es información extremadamente sensible.

Por qué esto importa, más allá de la cifra exacta

La relevancia de este hecho no depende de que cada archivo publicado sea genuino. Que un grupo de extorsión haya logrado exponer públicamente documentación con apariencia corporativa real, asociada a una empresa de infraestructura crítica y mayoría estatal, es en sí mismo un hecho de interés público.

Mientras la autenticidad completa del material no se confirme ni se descarte oficialmente, empleados, contratistas y ciudadanos que dependen de esta empresa permanecen en una situación de incertidumbre sobre el alcance real de lo expuesto.

En este momento cualquier persona con una habilidad mínima puede entrar y descargar los miles de archivos que se robaron a la estatal petrolera.

← Ataque a Ecopetrol: el catálogo de datos que el grupo atacante dice tener en su poder

6 ¿Recibo de Nequi Falso? Descubre Qué es NequiDz y la Guía Definitiva para Evitar Estafas

7 Sitio falso de Jelpit roba pagos de administración

8 Movilidad de Bogotá: atacantes dicen haber borrado multas

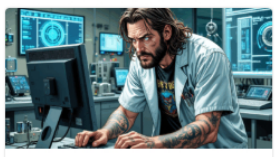
9 DaviTrampa: un clon de Daviplata que simula transferencias de dinero y con el cual estarían estafando a usuarios de este servicio

10 Filtración confirmada expone datos de 1,4 millones de colombianos de la plataforma de Defensores de la Patria

Categorías

Seleccionar Categoría

También te puede gustar



Más de 5 millones de archivos habrían sido robados a la Justicia Penal Militar

junio 24, 2025

6.276 comunicaciones de carácter sensible radicados presumiblemente ante la Unidad para

Filtración confirmada expone datos de 1,4 millones de colombianos de la plataforma de

la Restitución de Tierras fueron robados y expuestos públicamente

julio 22, 2024

Defensores de la Patria

junio 20, 2026

Deja un comentario

Tu dirección de correo electrónico no será publicada. Los campos obligatorios están marcados con *

Comentario *

Nombre *

Correo electrónico *

Web

Publicar comentario

CONGRATS, BIG GUY!

Attacking an education and knowledge site? Wow, look at you, such a "dangerous hacker." If you're looking for money or glory, you're in the wrong place; we're just an independent blog. Don't be a *script kiddie* with a power trip. If you actually know your stuff, report the bug like a pro to `editor@muchohacker.lol` or go play somewhere else.:D

¡FELICIDADES, CAMPEÓN!

Atacando un sitio de educación y conocimiento? Wow, qué "hacker" tan peligroso. Si buscas dinero o gloria, aquí no hay nada; solo somos un blog independiente. No seas un *script kiddie* con complejo de superioridad. Si de verdad sabes algo, repórtalo como un profesional a `editor@muchohacker.lol` o vete a jugar a otro lado.