JUDICIAL

Así opera The Gentlemen, el grupo de ransomware que atacó y robó datos a Ecopetrol

miércoles, 22 de julio de 2026

GUARDAR

¿Qué es The Gentlemen?

Foto: SOCRadar, Microsoft, Check Point Research, Trend Micro y WeLiveSecurity

> Según la estatal petrolera, el acceso no autorizado del 17 de julio resultó en la descarga de datos asociados a 3.300 cuentas de usuarios

SARA IBAÑEZ PITA

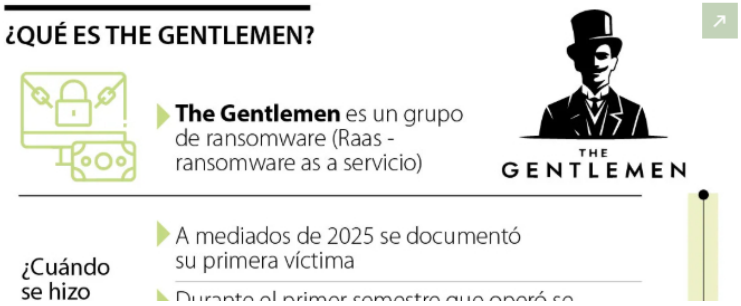
El viernes 17 de julio, la primera de Las Cien Empresas Más Grandes del país, *Ecopetrol*, fue víctima de un **ataque cibernético** por parte de un actor externo que intentó robar información de la compañía y sus usuarios. Días después, se conoció que la 'mafia digital' que llevó a cabo esta operación fue 'The Gentlemen', un grupo de ransomware as a service que ya acumula más de 250 víctimas en diferentes países.

Según detalles oficiales, *Ecopetrol* identificó "un acceso no autorizado a ciertos recursos digitales de su propiedad por parte de un actor externo aún no identificado, así como un intento de ejecución de ransomware (secuestro de información)", el cual fue bloqueado por los controles de ciberseguridad del grupo empresarial.

En el mismo comunicado, la estatal petrolera confirmó que ese acceso afectó los entornos de almacenamiento en la nube de 15 compañías del grupo y resultó en la descarga no autorizada de datos asociados a aproximadamente 3.300 cuentas de usuarios.

No obstante, un día después, el grupo 'The Gentlemen' se atribuyó el ataque y señaló que obtuvo cerca de un terabyte de documentos corporativos, lo que equivaldría a aproximadamente 250.000 fotos de 12 megapixeles, 500 horas de video en alta definición y hasta 6,5 millones de archivos.

Según información revelada por el *Grupo de Respuesta a Emergencias Cibernéticas de Colombia* del *MinTIC*, 'The Gentlemen' es un grupo de Raas que se hizo conocido en julio de 2025 y que escaló hasta convertirse "en una de las amenazas más sofisticadas". Su **modelo de negocio** es de doble extorsión; por lo que, primero extrae grandes volúmenes de información sensible y luego cifra los sistemas de la víctima.



ARTÍCULO RELACIONADO

Ecopetrol descartó impactos en usuarios y sus operaciones luego del ciberataque

ARTÍCULO RELACIONADO

Ecopetrol recibió un ataque cibernético con el fin de robar información de la empresa

LR MAS

Agregue a sus temas de interés

Ecopetrol +
The Gentlemen +

LR MAS

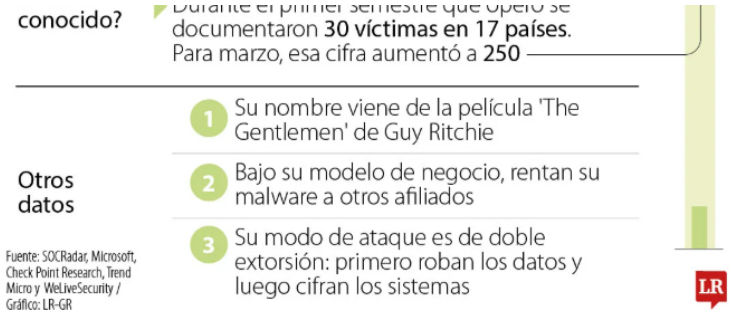
Agregue a sus temas de interés

Ecopetrol +
The Gentlemen +
Ataque cibernético +
ransomware +

LR MAS

Agregue a sus temas de interés

Ecopetrol +
The Gentlemen +
Ataque cibernético +
ransomware +



SOCRadar, Microsoft, Check Point Research, Trend Micro y WeLiveSecurity

Con corte a abril de 2026, el grupo ha reconocido más de 200 ataques en 50 países, principalmente a compañías que pertenecen a los sectores de manufactura, construcción, salud, finanzas y energía. La escala a la que operan es tan grande que, incluso, los reportes oficiales advierten que representan cerca de 10% del total de ataques de ransomware, consolidándose como el segundo actor más daño después de *Qilin*.

"El grupo mantiene actividad de intrusión activa y confirmada, con capacidad demostrada de comprometer el dominio completo de una organización y desplegar el cifrado en cuestión de minutos una vez alcanzados privilegios de administrador de dominio", agregó el *Grupo de Respuesta a Emergencias Cibernéticas de Colombia.*

¿Qué es The Gentlemen?

El presunto hacker de *Ecopetrol* es un grupo que irrumpió en los cibercrímenes a mediados de 2025 con una identidad de marca pulida e inspirada en la película 'The Gentlemen' de **Guy Ritchie**, además de que cuenta con un sitio propio en la dark web.

Distinto a otros modelos de secuencia fija, el grupo opera con una metodología mucho más profunda que emplea sistemas como Advanced IP Scanner y Nmap para efectuar un mapeo de la infraestructura de la víctima antes de desplegar el ataque. Con estos pasos, logra identificar las cuentas con mayor jerarquía y los puntos que debe seguir para desplegar el ransomware sin mucha resistencia.

Los análisis que se han hecho sobre la **'anatomía' de sus ataques** revelaron que comienzan aprovechando accesos puestos en internet de administración abierta o, incluso, con credenciales robadas. Ya adentro, 'The Gentlemen' despliega sus herramientas para explorar la red interna y entender cómo está organizado el sistema de las empresas y quiénes son los usuarios con mayor acceso.

Hacia la etapa final de su despliegue, roban información sensible y la envían a servidores externos de forma cifrada. Finalmente, borran su rastro, eliminan sus registros de actividad y cualquier otra evidencia.

De su más de 250 víctimas, destaca que la mayoría son de países como Estados Unidos y Tailandia, aunque también han hecho ataques a compañías de India, México, España, Francia y Colombia. De hecho, según información publicada en su propio sitio web, también hicieron incursiones de ransomware en *BCN Medical* y *Canal Capital*.

TENDENCIAS

1 BANCOS
Cambios en directiva de Davivienda con renuncia de Elsa Noguera y retiro de Rodrigo Arango

2 HACIENDA
Dian habilitó consulta de información exógena para preparar declaración de renta

3 JUDICIAL
Así opera The Gentlemen, el grupo de ransomware que atacó y robó datos a Ecopetrol

4 COMERCIO
Estos son los cinco principales dueños de los malls que tienen 22% del mercado nacional

5 BOLSAS
El precio del dólar cerró $31 a la baja y está cerca de romper la barrera de los $3.200

6 BOLSAS
Precio del euro llegó nuevamente a mínimos no vistos desde 2020 en $3.669

MÁS DE ECONOMÍA

HACIENDA | 21/07/2026

Quinta tributaria de Petro está en vilo porque no hay comisiones económicas

Estas comisiones conjuntas están conformadas por las terceras y cuartas del Senado y la Cámara de Representantes

TURISMO | 22/07/2026

Vaupés, Guaviare y Guainía, los de mayor crecimiento en llegada de extranjeros

Por ciudades, Bogotá fue la más visitada con 869.000 visitantes, a esta le siguen Medellín con 568.000, Cartagena de Indias con 457.000 y Cali con 96.000

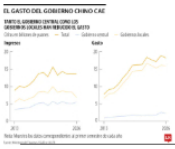
ENERGÍA | 22/07/2026

Los subsidios a la gasolina y el diésel podrían dejar un hueco fiscal por cerca de $10 billones

Moody's Ratings advirtió que congelar los precios internos de los combustibles aumentaría déficit del Fepc

MÁS ECONOMÍA

MÁS DE LA REPÚBLICA



CHINA
El gasto público de China se desploma y cae a su nivel más bajo desde octubre

TRANSPORTE
Invías asumió a partir de hoy la operación del corredor de carga Cartagena – Barranquilla

SOCIALES
La empresa alemana Schaeffler apuesta por la innovación para la movilidad del futuro

BANCOS
Las entidades financieras tardan más de seis meses en lanzar un nuevo producto

JUDICIAL
Corte Suprema ordena adoptar plan para superar incumplimiento de tutelas

TECNOLOGÍA
Conozca cómo la economía de las suscripciones transforma los hábitos de consumo

SUSCRÍBASE

TODAS LAS SECCIONES

Agronegocios
Asuntos Legales
Consumo
Empresas
Finanzas
Indicadores
Internet Economy
Alta Gerencia
Caja Fuerte
Directorio Empresarial
Especiales
Finanzas Personales
Infraestructura
Obituarios
Análisis
Comunidad Empresarial
Economía
Eventos
Globoeconomía
Inside
Ocio

MANTÉNGASE CONECTADO

Mesa de Generación de Contenidos
Nuestros Productos
Contáctenos
Aviso de privacidad
Términos y Condiciones
Política de Tratamiento de Información
Política de Cookies
Superintendencia de Industria y Comercio