¿Quién es The Gentlemen, la 'mafia digital' que *hackeó* a Ecopetrol y le robó miles de datos?

The Gentlemen, el grupo de ransomware (programa malicioso) que atacó a Ecopetrol, dice haber robado un terabyte de archivos, más allá de los 3.300 usuarios reconocidos por la petrolera.

The Gentlemen hackeó a Ecopetrol y dice haber robado 1 TB de datos, más de lo que reconoce la petrolera. FOTO: Colprensa.

Toca para escuchar ×
ESCUCHA EL RESUMEN
00:00 powerbeans 00:49

Miguel Orlando Alguero
Economía

hace 3 horas

Un grupo malicioso que roba información en internet entró a los sistemas de Ecopetrol la semana pasada, descargó información de cerca de 3.300 cuentas de usuario en 15 empresas del grupo petrolero y exigió dinero a cambio de no publicarla.

Así lo reconoció Ecopetorl en un comunicado tras el ataque, revelado el viernes 17 de julio. Pero el grupo que se atribuye el golpe, conocido como The Gentlemen,

Las más leídas


Valentina Ramos, promesa del ballet antioqueño, busca apoyo para seguir sus estudios en Roma
hace 28 minutos


¿Qué significa para el Centro Democrático haberle ganado el pulso a De la Espriella en el Senado?
hace 4 horas


"180 votos para Simón Bolívar": así revivió la congresista María Fernanda Carrascal al libertador
hace 1 hora


Fiebre del Mundial se sintió en Colombia: consumo de internet creció 30% y gasto de viajeros 500%
hace 44 minutos


Así quedó la Comisión de Acusación, donde se investiga al presidente: Petro tiene más de 200 casos
hace 52 minutos

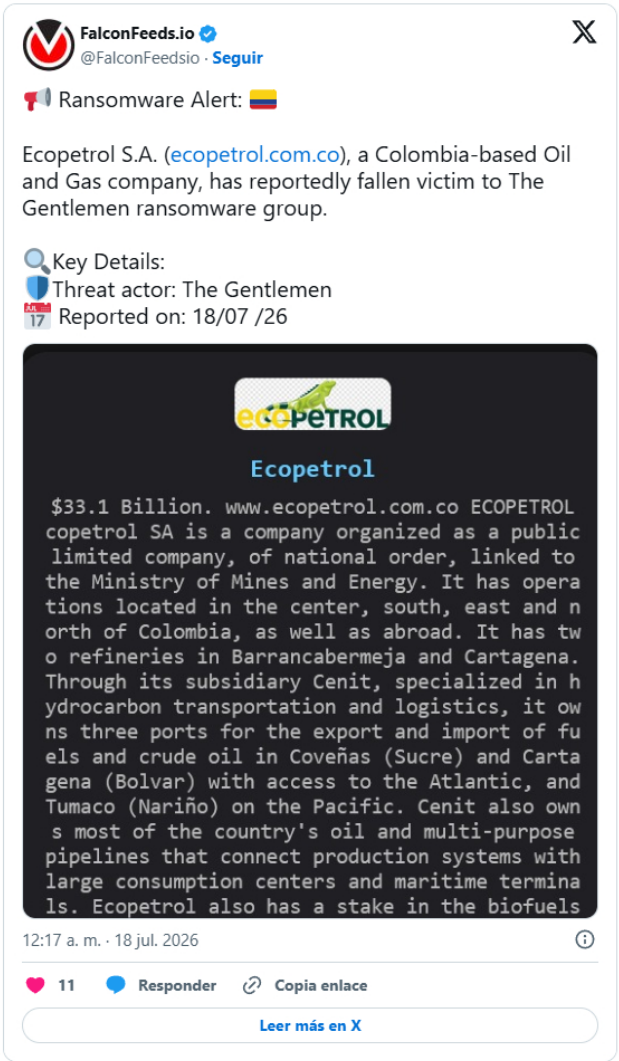
Te recomendamos

asegura que la cifra real es mucho más alta, habla de 1 terabyte completo de documentos corporativos.

Entérese: Ciberataque a Ecopetrol: 15 empresas del grupo afectadas y hackers están extorsionando tras robar datos de 3.300 cuentas

Asimismo, Ecopetrol, responsable de más del 60% de la producción de hidrocarburos del país, confirmó el "ingreso irregular a sus sistemas" y afirmó que logró frenar la fase final del ataque. Según la empresa, los criminales intentaron desplegar un *ransomware* (programa malicioso que bloquea el acceso a archivos o dispositivos y exige un pago) para cifrar la información y bloquear la operación, pero los controles de seguridad detuvieron esa etapa.

La compañía dijo que "no encontró afectaciones sobre su capacidad de producción ni sobre la prestación de servicios esenciales". Como respuesta, revocó accesos, bloqueó nuevas descargas, reforzó el monitoreo de su infraestructura y notificó a las autoridades colombianas.



1 TB contra 3.300 cuentas en Ecopetrol


Él es Nicolás Barguil, el nuevo presidente de la Cámara: su trayectoria en el sector gremial y en la política
hace 7 horas


'Lujo-zaa': fotos y videos de los extravagantes bienes ocupados a Charlie Zaa avaluados en 45 mil millones de pesos


Declaración de renta 2026: quiénes deberán declarar, quiénes quedan exentos y cuáles son las sanciones por incumplir


Equipo de empalme de Abelardo De La Espriella denuncia cuatro presuntos casos de corrupción en el gobierno Petro

Como lo reveló *Primera Página,* The Gentlemen publicó a Ecopetrol en su sitio de filtraciones de la red oscura y sostiene que la cifra oficial se queda corta.

El investigador independiente conocido como chum1ng0, especializado en seguridad informática, lo confirmó así: "Todo lo publicado sobre Ecopetrol es verdad salvo el volumen: 'The Gentlemen' afirman haber extraído 1 TB, no solo datos de 3.300 cuentas".

Un terabyte equivale a 1.024 gigabytes. Es decir, esa cantidad de información permite almacenar cerca de 250.000 fotografías de 12 megapíxeles, 500 horas de video en alta definición o hasta 6,5 millones de documentos. Hasta el momento no existe una verificación independiente que confirme cuál de las dos cifras, la de Ecopetrol o la de los atacantes, refleja el tamaño real de la fuga.

Un reporte de Cybernews precisa además que el número de subsidiarias afectadas fueron 14, cifra cercana a las 15, según el reporte oficial, pero no idéntica a la que maneja la petrolera.

Economía

"Primero debemos recuperar a Ecopetrol; vender ahora no tiene sentido": Miguel Gómez

Quién es The Gentlemen, el grupo que *hackeó* a Ecopetrol

The Gentlemen apareció en los foros clandestinos a mediados de 2025 y, en menos de un año, escaló hasta convertirse en el segundo actor más dañino del ecosistema global de *ransomware*, según firmas de inteligencia de amenazas como SOCRadar.

El grupo ya representa cerca del 10% de los ataques de este tipo en el mundo y comprometió a más de 200 organizaciones confirmadas en más de 50 países. Una investigación reciente encontró que un servidor de la organización mantenía ocultas otras 1.570 víctimas que nunca fueron expuestas públicamente.

Su nombre rinde homenaje a la película "The Gentlemen: los señores de la mafia", del director británico Guy Ritchie, conocida por su humor negro y sus tramas de crimen organizado.

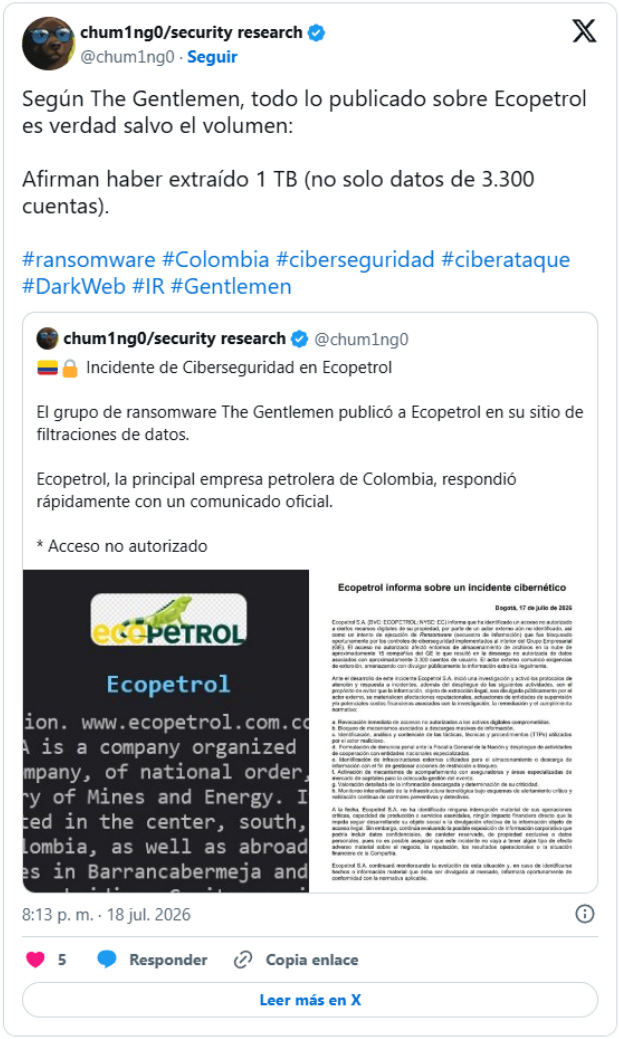
Como lo contó *Primera Página*, los analistas de SOCRadar describen al grupo como "una amenaza capaz y coordinada, operando con notable rapidez en múltiples regiones y entornos empresariales", con posibles vínculos con estructuras de *ransomware* anteriores.

Además, fuentes de inteligencia de amenazas señalan que The Gentlemen nació como una escisión del grupo criminal Qilin, tras disputas internas por el reparto del

dinero de los rescates. Un operador identificado con el alias “hastalamuerte” habría filtrado bases de datos de Qilin antes de pasarse a la nueva organización.

Aunque no hay un país de origen confirmado, un patrón que llama la atención de los investigadores es que el grupo tiene una regla estricta de no atacar objetivos en Rusia ni en los países de la antigua Comunidad de Estados Independientes. Ese comportamiento sugiere que la organización opera desde Europa del Este.

Siga leyendo: Los contratos millonarios en Ecopetrol que Petro quiere destrabar antes de dejar el poder



¿Cómo opera el negocio de “franquicia” criminal por The Gentleman?

The Gentlemen trabaja bajo el modelo de *ransomware* como servicio, conocido en inglés como RaaS. Los desarrolladores del *malware (software malicioso)* no ejecutan los ataques directamente, sino que alquilan su infraestructura a afiliados a cambio de una comisión.

En este caso, la comisión es especialmente generosa, ya que el grupo ofrece a sus afiliados el 90% de las ganancias de cada rescate pagado, uno de los repartos más altos que se conocen en este mercado ilegal. Para entrar a la organización, los nuevos reclutas deben demostrar su capacidad de ataque aportando al menos un gigabyte de información confidencial robada previamente.

La estrategia de ataque combina dos presiones simultáneas, lo que los expertos llaman doble extorsión. Primero, el grupo extrae grandes volúmenes de información sensible de la víctima. Después, cifra los sistemas para impedir que la empresa opere con normalidad. Si la organización se niega a pagar por recuperar el acceso, los criminales amenazan con publicar toda la información robada en su sitio de filtraciones.

Economía

Denuncian que directivos de Ecopetrol se blindaron con estabilidad laboral hasta el 2030

Asimismo, Microsoft y Check Point Research, dos de las firmas que más han investigado al grupo, señalan que The Gentlemen desarrolla sus herramientas principalmente en el lenguaje de programación Go y que cuenta con capacidad para propagarse dentro de una misma red corporativa, comprometiendo varios equipos a la vez.

El *malware* tiene variantes para Windows, Linux, sistemas NAS, BSD y entornos virtualizados ESXi, lo que amplía su alcance sobre la infraestructura de las empresas. Su ejecución requiere una contraseña específica, un diseño que refleja un despliegue controlado por el operador y no una propagación al azar.

La puerta de entrada favorita del grupo son los dispositivos de conexión remota que las empresas dejan sin actualizar. Su vía principal es la explotación de una falla conocida en las redes VPN de la marca Fortinet FortiGate, identificada como CVE-2024-55591.

En ese orden, una vez adentro, los atacantes usan técnicas avanzadas para apagar los antivirus y neutralizar las defensas, lo que les permite tomar el control del sistema y desplegar el ataque en cuestión de minutos.

Trend Micro y Microsoft coinciden en que los sectores más golpeados por el grupo son manufactura, que concentra cerca del 30% de sus ataques, seguido por construcción, salud, finanzas, transporte, educación y energía.

Le puede interesar: ¿Se cayó el regreso de Ricardo Roa? Junta de Ecopetrol responde si negó o no su retorno

Responder Copia enlace

Leer más en X

Voces críticas: “el colmo del fracaso en la alineación de riesgos”

No todos los analistas coinciden con la lectura optimista de Ecopetrol sobre el alcance del ataque. Por ejemplo, Lanark AI, firma que provee inteligencia artificial para el comercio mayorista, cuestionó que la petrolera presente el incidente como una mitigación exitosa.

Según la firma, “cuando 3.300 identidades corporativas de 15 subsidiarias quedan expuestas, bloquear la etapa final del cifrado resulta secundario frente al daño ya hecho”, porque la información filtrada incluye identificadores de usuario, nombres, contraseñas cifradas, correos electrónicos, fechas de registro y llaves de activación de cuentas.

Lanark AI también llamó la atención sobre el momento del ataque, ocurrido 48 horas antes de la final del Mundial, y lo calificó de movimiento táctico y no casual, capaz de pasar desapercibido bajo la atención mediática del torneo.

Por eso, la firma advirtió que, “si la infraestructura de una compañía no aísla de forma estricta a cada subsidiaria y no trata la exposición de directorios entre nubes como una falla arquitectónica grave, su postura de seguridad seguirá siendo una apuesta reactiva”.

Economía

Estos son los cinco acuerdos entre la USO y Ecopetrol que ponen fin al conflicto colectivo

Ante esto, el Ministerio de las Tecnologías de la Información y las Comunicaciones confirmó, a través de un comunicado del 18 de julio de 2026, que el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, ColCERT, recibió el reporte de Ecopetrol un día antes y activó de inmediato la coordinación con los organismos pertinentes.

La entidad indicó que los equipos de defensa de la petrolera lograron contener los ataques recibidos.

ColCERT mantiene canales de coordinación directa con la Dirección Especializada contra los Delitos Informáticos de la Fiscalía General de la Nación, además de contacto con los equipos de investigación de la DIJIN de la Policía Nacional y el CTI de la Fiscalía.

El Ministerio TIC señaló que continuará acompañando a Ecopetrol durante todo el proceso y que informará oportunamente sobre las acciones que se desarrollen.

Ecopetrol
@ECOPETROL_SA · **Seguir**

#InformaciónRelevante | Ecopetrol informa sobre un incidente cibernético. Lee más aquí 👇

Información relevante

ecopetrol

Ecopetrol informa sobre un incidente cibernético

Bogotá, 17 de julio de 2026

Ecopetrol S.A. (BVC: ECOPETROL; NYSE: EC) informa que ha identificado 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) que fue bloqueado oportunamente por los controles de ciberseguridad implementados al interior del Grupo Empresarial (GE). 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.

Ante el desarrollo de este incidente Ecopetrol S.A. inició una investigación y activó los protocolos de atención y respuesta a incidentes, además del despliegue de las siguientes actividades, con el


propósito de evitar que la información, objeto de extracción ilegal, sea divulgada públicamente por el actor externo, se materialicen afectaciones reputacionales, actuaciones de entidades de supervisión y/o potenciales costos financieros asociados con la investigación, la remediación y el cumplimiento normativo:

a. Revocación inmediata de accesos no autorizados a los activos digitales comprometidos.
b. Bloqueo de mecanismos asociados a descargas masivas de información.
c. Identificación, análisis y contención de las tácticas, técnicas y procedimientos (TTPs) utilizados por el actor malicioso.
d. Formulación de denuncia penal ante la Fiscalía General de la Nación y despliegue de actividades de cooperación con entidades nacionales especializadas.
e. Identificación de infraestructuras externas utilizadas para el almacenamiento o descarga de información con el fin de gestionar acciones de restricción o bloqueo.
f. Activación de mecanismos de acompañamiento con aseguradoras y áreas especializadas de mercado de capitales para la adecuada gestión del evento.
g. Valoración detallada de la información descargada y determinación de su criticidad.
h. Monitoreo intensificado de la infraestructura tecnológica bajo esquemas de alertamiento crítico y validación continua de controles preventivos y detectivos.

7:30 p. m. · 17 jul. 2026

33 Responder Copia enlace

Leer 6 respuestas

Qué recomiendan las autoridades a otras empresas

ColCERT emitió una alerta de riesgo alto para el sector empresarial colombiano. La recomendación central pasa por actualizar de manera urgente los parches de seguridad en los dispositivos Fortinet FortiGate y en otras soluciones VPN, el punto de entrada favorito del grupo.

La segunda medida es obligar la doble autenticación en todos los accesos remotos, un control que habría dificultado buena parte de las intrusiones documentadas hasta ahora.

La tercera recomendación es mantener copias de seguridad de la información crítica desconectadas de la red principal y protegidas contra modificaciones, de forma que un cifrado del sistema principal no deje a la empresa sin respaldo.

Por lo tanto, según coinciden Microsoft, Check Point Research, Trend Micro, SOCRadar y DeXpose, es que The Gentlemen ya se consolidó como uno de los actores de ransomware de crecimiento más rápido en el mundo, y que Ecopetrol se convirtió en su víctima de mayor peso estratégico en Colombia hasta ahora.

Para consultar contenido premium o profundizar sobre sus temas de interés de Medellín, Antioquia, Colombia y el Mundo, *regístrese aquí.*

Bloque de preguntas y respuestas

¿Qué tipo de información específica quedó expuesta de las cuentas de Ecopetrol?

La información filtrada incluye identificadores de usuario, nombres de usuario y contraseñas cifradas, correos electrónicos, fechas de registro y llaves de activación de cuentas. Este detalle proviene del análisis de Lanark AI sobre los datos exfiltrados, no de un comunicado oficial de Ecopetrol.

¿Por qué hay una diferencia entre los datos de Ecopetrol y The Gentlemen?

La diferencia responde a dos versiones distintas del mismo incidente que hasta ahora no tienen verificación técnica independiente. Ecopetrol habla de una descarga asociada a cerca de 3.300 cuentas de usuario, mientras el grupo atacante sostiene haber extraído un terabyte completo de archivos corporativos, una cifra mucho mayor.

¿Qué países o empresas evita atacar The Gentlemen?

El grupo tiene una regla estricta de no atacar objetivos en Rusia ni en países de la antigua Comunidad de Estados Independientes. Ese patrón lleva a los investigadores a creer que la organización opera desde Europa del Este, aunque no hay confirmación independiente de su país de origen.

Temas recomendados

Empresas | Ecopetrol | Tecnología | Internet | Software | Ciberataque | Hacker | Hackers | Ciberseguridad | Rusia | Colombia | Europa

Para seguir leyendo

Economía

Terminó la ventana de oportunidad: 166.000 trabajadores se trasladaron de régimen pensional

hace 8 horas

Economía

La pelea entre Hidralyte y Electrolit reabre el debate sobre la identidad visual de las marcas; estos han sido los otros casos

hace 3 horas

Economía

¿Cómo Rappi pasó de perder dinero a ganar $210 mil millones en Colombia?

hace 2 horas

Economía

Gobierno Petro propone recaudar $21,9 billones en nueva reforma tributaria, ¿cuáles son los nuevos impuestos?

hace 6 horas

Medellín suma una nueva vitrina *premium* de las marcas BMW, MINI y Motorrad

Autogermana abrió en Medellín su nueva vitrina Retail Next, un concepto global de BMW Group que apuesta por tecnología, diseño y experiencias premium para clientes.

Autogermana refuerza su apuesta por Antioquia en pleno auge del mercado automotor. FOTO: Cortesía.

El Colombiano

hace 40 minutos

Autogermana continúa fortaleciendo su presencia en Colombia con la inauguración de una nueva vitrina en Medellín bajo el concepto global Retail Next, la estrategia con la que BMW Group busca transformar la experiencia de compra y relacionamiento con los clientes de sus marcas alrededor del mundo.

La nueva sede, ubicada en LeMont, en Medellín, reúne en un mismo espacio a BMW, MINI y BMW Motorrad, con una propuesta que deja atrás el modelo tradicional de concesionario para dar paso a una experiencia enfocada en la tecnología, el diseño, la hospitalidad y la atención personalizada.

La apertura también llega en un momento de fuerte recuperación para el mercado automotor colombiano, que durante el primer semestre de 2026 registró un crecimiento de 50,1% en las matrículas de vehículos nuevos, mientras Medellín se consolidó entre las ciudades con mayor dinamismo del país.

Siga leyendo: 4 de cada 10 carros nuevos en Colombia son eléctricos e híbridos: