COLOMBIA >

Así funciona The Gentlemen, el grupo de 'ransomware' que robó los datos de Ecopetrol

Estos hackers han empleado técnicas avanzadas para infiltrarse, robar información confidencial y extorsionar a organizaciones en más de 50 países

Por **Angie Julieth Cicua Caballero**

22 Jul, 2026 01:59 p. m. CO

La petrolera estatal perdió información de más de 3 mil cuentas - crédito (Imagen Ilustrativa Infobae)

El reciente ataque cibernético contra Ecopetrol el pasado 17 de julio de 2026, la mayor empresa petrolera de Colombia, reveló el sofisticado modo de operar de uno de los grupos de ransomware (programa que bloquea archivos o equipos y exige dinero para liberarlos) más activos del mundo: The Gentlemen.

Te puede interesar:
Isabel Zuleta pidió al Congreso frenar la posesión de Abelardo de la Espriella tras la demanda impuesta por Gustavo Petro: "Para no ser cómplice de un posible fraude"

La compañía detectó el acceso irregular a sus sistemas y logró impedir el cifrado masivo de sus archivos, **aunque no pudo evitar la filtración y descarga no autorizada de información de aproximadamente 3.300 cuentas de usuarios y datos almacenados en la nube de 15 empresas del grupo empresarial.**

Cómo actúan los grupos de ransomware como The Gentlemen

La mecánica de estos ataques no se limita a irrumpir en los sistemas y pedir un rescate. El grupo realiza un mapeo previo de la infraestructura de la víctima utilizando herramientas como Advanced IP Scanner y Nmap. Esta fase les permite identificar los puntos débiles, así como los usuarios y cuentas con mayores privilegios dentro de la red.

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.

A la fecha, Ecopetrol S.A. no ha identificado ninguna interrupción material de sus operaciones críticas, capacidad de producción o servicios esenciales, ningún impacto financiero directo que le impida seguir desarrollando su objeto social o la divulgación efectiva de la información objeto de acceso ilegal. Sin embargo, continúa evaluando la posible exposición de información corporativa que podría incluir datos confidenciales, de carácter reservado, de propiedad exclusiva o datos personales, pues no es posible asegurar que este incidente no vaya a tener algún tipo de efecto adverso material sobre el negocio, la reputación, los resultados operacionales o la situación financiera de la Compañía.

Ecopetrol S.A. continuará monitoreando la evolución de esta situación y, en caso de identificarse hechos o información material que deba ser divulgada al mercado, informará oportunamente de conformidad con la normativa aplicable.

El grupo criminal exige rescates bajo amenaza de publicar información robada en la dark web - crédito Ecopetrol

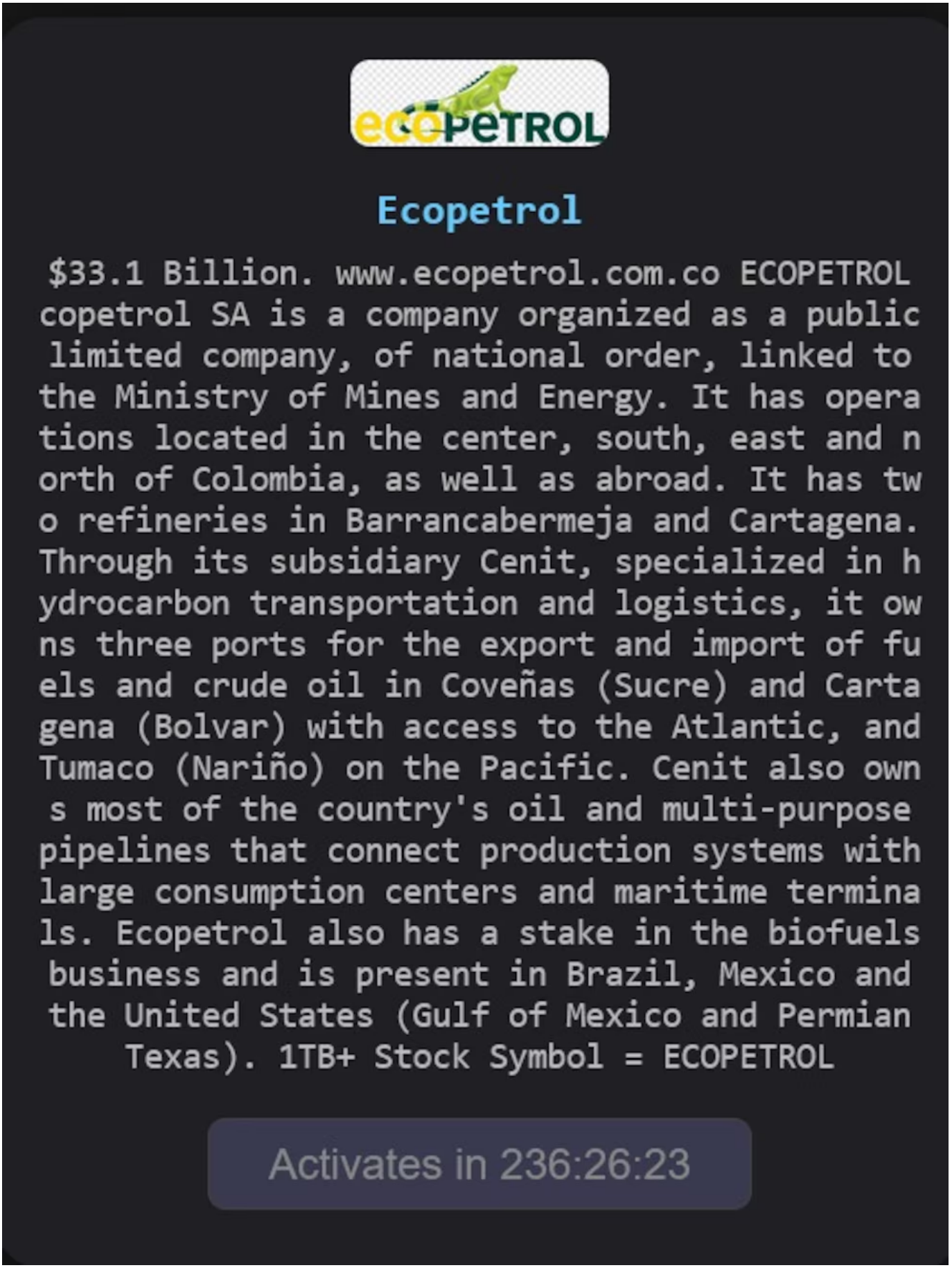
Los expertos en ciberseguridad han documentado que el grupo suele acceder a través de dispositivos de administración remota mal protegidos o utilizando credenciales robadas. Una vez dentro, exploran la red interna y localizan los datos más sensibles, preparándose para la extracción y el cifrado.

En el ataque a Ecopetrol, los atacantes consiguieron descargar datos confidenciales antes de que la compañía pudiera bloquear el intento de ransomware. El grupo criminal sostiene que robó un terabyte de documentos corporativos, una cantidad que excede ampliamente la cifra oficial reconocida por la empresa.

Te puede interesar:
Madre e hijo que viajaron como turistas a Santa Marta fueron hallados sin vida en un apartamento en El Rodadero: el fuerte olor alertó al personal de limpieza

Metodología y herramientas utilizadas por los hackers

La operación se caracteriza por su doble extorsión: primero, extraen los archivos y luego amenazan con publicarlos si la víctima se niega a pagar. Esta estrategia incrementa la presión sobre las empresas al poner en riesgo tanto su actividad diaria como su reputación y la privacidad de sus usuarios.



The Gentlemen compromete la seguridad de empresas en sectores clave mediante técnicas de doble extorsión y sofisticadas herramientas digitales - crédito @FalconFeedsio / X

La ejecución del cifrado no es azarosa ni automática. Los atacantes esperan a obtener privilegios de administrador de dominio para poder comprometer la totalidad de la red empresarial y desplegar el ransomware en cuestión de minutos. Según el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, una vez alcanzado ese nivel de acceso, los hackers pueden cifrar sistemas críticos con gran rapidez.

El malware desarrollado por The Gentlemen está programado principalmente en Go (lenguaje de Google) y cuenta con versiones para varios sistemas operativos empresariales, lo que les permite atacar desde servidores Windows hasta infraestructuras Linux, BSD y entornos virtualizados. Una característica distintiva es que su ejecución requiere una contraseña específica, lo que limita la propagación solo a quienes tienen autorización directa del grupo.

El modelo de negocio: ransomware como servicio

La organización funciona bajo el modelo de ransomware as a service (RaaS), en el que desarrolladores del malware alquilan su infraestructura a afiliados externos. Estos afiliados ejecutan los ataques y reciben hasta el 90% de cada rescate pagado, lo que convierte a The Gentlemen en uno de los grupos más atractivos para ciberdelincuentes con experiencia.

Para ingresar como afiliado, los aspirantes deben demostrar su capacidad aportando un botín mínimo de información confidencial previamente robada. Así, la estructura se expande de manera descentralizada y difícil de rastrear.

TIC | COLCERT

Comunicado a la Opinión Pública

Bogotá, julio 18 de 2026 (@Ministerio_TIC) – Frente al incidente cibernético reportado por Ecopetrol en las últimas horas, el Ministerio TIC se permite informar a la ciudadanía que:

- El Grupo de Respuestas a Emergencias Cibernéticas de Colombia (ColCERT) recibió el reporte correspondiente de parte de Ecopetrol el día de ayer. Desde ese momento se iniciaron las actividades de coordinación con los organismos pertinentes para entender lo sucedido y plantear líneas de defensa y atención.

- En el marco de esa coordinación, los grupos de defensa de Ecopetrol confirmaron la contención de los ataques recibidos.

- Como parte de esas acciones, el ColCERT mantiene canales de coordinación directa con la Dirección Especializada contra los Delitos Informáticos de la Fiscalía General de la Nación, con el propósito de apoyar la gestión de incidentes y fortalecer la respuesta institucional. También se mantiene contacto con los equipos de investigación judicial de la DIJIN de la Policía Nacional y el CTI de la Fiscalía.

- Además, continúa el acompañamiento diario a la gestión y definiendo necesidades de apoyo e intercambio de información directa con los equipos especializados de respuesta de Ecopetrol

- El ColCERT, como instancia nacional de coordinación para la gestión de incidentes de seguridad digital, articula esfuerzos con las capacidades del Estado y con actores especializados del ecosistema de ciberseguridad.

- El ColCERT seguirá acompañando a Ecopetrol durante este proceso. El Ministerio TIC informará oportunamente sobre las acciones que se desarrollen en el marco de esta gestión.

Consulte las publicaciones técnicas del ColCERT
Acceda a alertas, advertencias, informes, y demás publicaciones técnicas para fortalecer la prevención, identificar riesgos y mantenerse informado sobre las principales amenazas de seguridad digital.
https://www.colcert.gov.co/800/w3-propertyvalue-412601.html

Canales oficiales del ColCERT:
Sitio web: www.colcert.gov.co
Correo: contacto@colcert.gov.co
Línea telefónica Bogotá: +57 601 344 22 22
X: @colCERT

Pública

En los últimos meses, The Gentlemen ha sido responsable de ataques en más de 50 países, con víctimas en sectores como la manufactura, construcción, salud, finanzas y energía. Los reportes de firmas especializadas indican que el grupo ya representa cerca de un 10% de los ataques de ransomware a nivel global, solo superado por la organización criminal Qilin.

Técnicas de acceso y evasión de defensas

Una de las vías de entrada favoritas del grupo son las vulnerabilidades en redes VPN, especialmente las fallas no corregidas en dispositivos Fortinet FortiGate. Tras conseguir acceso, los hackers emplean tácticas avanzadas para desactivar antivirus y eliminar rastros de su actividad, lo que dificulta la detección y el análisis forense posterior.

La etapa final del ataque implica el robo de datos y su envío a servidores externos, todo ello encriptado para evitar la interceptación. A continuación, los atacantes borran cualquier registro de sus acciones y contacto, lo que complica tanto la atribución como la recuperación de la información sustraída.