La historia detrás del hackeo a Ecopetrol: así operan “Los Caballeros”

La empresa más grande del país ha sido víctima de una joven agrupación cibercriminal. ¿Cómo se cree que lograron vulnerar sus sistemas de defensa? ¿Qué tan grave es la situación?

Diego Ojeda
28 de julio de 2026 - 08:30 p. m.

Ecopetrol señaló que los atacantes ya publicaron la información obtenida y que la compañía, con la ayuda de la Unidad de Delitos Informáticos y el Ministerio de las TIC, está realizando esfuerzos para limitar el acceso a la misma.

Foto: Imagen creada con IA

La iguana fue hackeada (o crackeada, para los más rigurosos de la seguridad informática). En la noch
poco habitual para la emisión de comunicados, Ecopetrol, la empresa más grande de Colombia, alert
lograron vulnerar sus sistemas y extraer información de 15 compañías que integran su grupo empre

Las primeras señales indican que el impacto del ataque habría sido significativo. Se sabe que la infor
asociada a cerca de 3.300 cuentas de usuario y que los datos extraídos tendrían un carácter sensible
compañía, ya que los ciberdelincuentes exigieron un pago a cambio de la no divulgación.

También que los cibercriminales intentaron ejecutar un ransomware, un tipo de malware (lo que un
llamaría “un virus”) diseñado para secuestrar información y exigir dinero a cambio de devolver el ac

En palabras simples, es como si los atacantes lograran escabullirse en la seguridad de una compañía
valiosos y encerrarlos bajo llave en una habitación. Después, utilizan esa información como mecani
la “llave” si se les hace un pago.

Le puede interesar

Empresas
Ciberataque a Ecopetrol: la empresa activó protocolo ante divulgación ilegal de información

Macroeconomía
Qué está pasando con el precio del petróleo y qué podría pasar en Oriente Medio

Economía
Ley minera: el Gobierno Petro la radicó por segunda vez en el Congreso

Desde el primer día, la compañía resaltó que el ransomware no logró ejecutarse, es decir, Ecopetrol sigue teniendo acceso a los archivos que se vieron comprometidos pero, hay que recordar, los atacantes sí lograron descargar información.

En su comunicado más reciente, con fecha del 27 de julio, Ecopetrol señaló que los atacantes ya publicaron la información obtenida y que la compañía, con la ayuda de la Unidad de Delitos Informáticos y el Ministerio de las TIC, está realizando esfuerzos para limitar el acceso a la misma.

De nuevo, la opinión pública sigue sin conocer con precisión qué tipo de información fue extraída por la agrupación de ciberdelincuentes. Sin embargo, se presume que una parte de estos datos pudo haber sido publicada en foros clandestinos de la web profunda, espacios donde otros actores maliciosos pueden acceder a la información (usualmente pagando) y utilizarla como punto de partida para nuevos ataques.

La exposición de estos datos representa un riesgo adicional, pues podría permitir que otros delincuentes diseñen amenazas dirigidas contra la compañía o contra las personas cuyas información resultó comprometida.

“Ecopetrol planea continuar con las investigaciones y con los esfuerzos de colaboración con las autoridades competentes con el fin de mitigar y/o atenuar los efectos de las publicaciones ilegales por parte de los agentes externos. Ecopetrol también confirma que no se ha identificado ningún compromiso o afectación de las soluciones tecnológicas transaccionales dentro de su ecosistema digital, ni de las de sus subordinadas o de su red de socios comerciales y financieros, proveedores y clientes. El alcance total, el impacto y los costos de este incidente de ciberseguridad aún son inciertos”, explicó la compañía.

El daño ya está hecho: la iguana fue vulnerada y, aunque los directivos de la compañía adelantan esfuerzos para contener las consecuencias, no pueden garantizar que no surjan nuevos impactos derivados del uso malintencionado que la agrupación cibercriminal responsable del ataque, o terceros, puedan darle a la información extraída.

“Los caballeros”

Acceder a ella no siempre es sencillo, pues se requiere de navegadores especiales y ciertos conocimi
específicos en donde se encuentran este tipo de páginas. ¿Por qué se ocultan? Porque en su mayoría
como la comercialización de datos robados, mercados de contrabando y sitios de extorsión, solo por
ejemplos más “suaves”.

Es en ese mundo que se mueve “The Gentlemen” (Los Caballeros, por su traducción del inglés), una j
cibercriminal que se ha hecho fama por ofrecer ransomware como servicio, es decir, venden este ma
como usuarios) interesadas en afectar una compañía.

Recientemente, portales especializados en inteligencia de amenazas y monitoreo de la dark web, co
“Los Caballeros” se adjudicaron el ataque informático del que fue víctima Ecopetrol. Gracias a este e
información robada pesa 1 terabyte (para que se haga una idea, en ese espacio se podrían almacenar

Según lo explicado por firmas de seguridad informática, esta organización delincuencial se presenta
parte de su estrategia consiste en la manipulación psicológica de sus víctimas, proyectando una ima
completo la naturaleza agresiva y criminal de sus ataques.

Se venden como una entidad, disciplinada, educada y caballerosa en sus notas de rescate, imitando e
persona recibiría en el servicio al cliente de cualquier compañía.

En entrevista con El Espectador, el especialista en seguridad informática de ESET Latinoamérica, Mario Micucci, señala que, con base en sus investigaciones, se ha encontrado que esta es una organización conformada por varias personas. Aunque es complicado determinar el número exacto de sus integrantes, por antecedentes de otras organizaciones se presume que el número de “Los Caballeros” es de por lo menos siete. “Esto se debe a que sus operaciones no son improvisadas: cada ataque responde a una planificación detallada y sigue un ciclo de vida claramente definido”, detalla.

El modus operandi

Antes de cualquier ataque, este tipo de grupos criminales realizan labores de inteligencia sobre sus objetivos para maximizar la probabilidad de éxito. A diferencia de otro tipo de cibercriminales, no le apuntan a un público masivo, se concentran en blancos previamente seleccionados.

Se sabe las tácticas, técnicas y procedimientos que emplea esta banda tiene una primera fase de ataque, conocida como acceso inicial, la cual suele realizarse mediante la técnica Exploit Public-Facing Application (MITRE ATT&CK T1190). No se abrume, si bien encontrará términos complejos en este artículo, justo al lado, o a renglón seguido, descubrirá su significado.

Lo anterior se traduce en que los criminales buscan qué equipos de las empresas están conectados a internet y, entre ellos, cuáles no han sido actualizados con sus correspondientes parches de seguridad. Ejemplos de ello pueden ser servidores, computadores, dispositivos de almacenamiento, equipos de red como *routers* o *firewalls*, e incluso cámaras de seguridad o cualquier otro dispositivo conectado que tenga una vulnerabilidad sin corregir.

Lo que el promedio de la gente ve como un aparato tecnológico, los atacantes lo ven como la puerta de entrada a los sistemas informáticos de la compañía.

Otra técnica utilizada es la de Brute Force: Password Guessing (MITRE ATT&CK T1110.001), también conocido como ataque de fuerza bruta. Aquí lo que hacen los atacantes es intentar adivinar la contraseña, probando combinaciones hasta dar con la correcta.

Una vez dentro, “Los Caballeros” pasan a la etapa de ejecución. En esta fase suelen emplear scripts desarrollados por ellos mismos, es decir, pequeños programas o conjuntos de instrucciones con los que suelen instalar programas que les permite acceder, de forma remota, al sistema y sus equipos.

Sí, desde la comodidad de su casa, uno de estos atacantes puede tener el control de una compañía.

Lo que hacen después es utilizar el programador de tareas del sistema para ejecutar el ransomware, que es lo que constituye la fase final de su ataque. Hay que recordar que, con base en la información divulgada por Ecopetrol, “Los Caballeros” no fueron capaces de hacer esto último.

“Esto demuestra que estamos frente a una organización que opera como una verdadera empresa del… muy bien cómo obtener beneficios económicos en cada etapa de sus operaciones”, resalta Micucci.

El foco está en varios países

También se sabe que “Los Caballeros” hoy tienen una operación transnacional. Firmas de seguridad… su actividad en países como Colombia, Argentina, Chile, Perú y Europa (particularmente en España).

Aunque pudiera presumirse que la agrupación, o parte de ella, es de origen ruso (dado que muchas d… hacen en ese idioma), esto no constituye un indicio suficiente para afirmarlo.

El experto de ESET resalta que uno de los sectores predilectos para este grupo es el de las infraestru… aquellas organizaciones cuya operación resulta esencial para el funcionamiento de un país. En esta… empresas de energía, petróleo y gas, agua, telecomunicaciones, transporte, salud, servicios financie… interrupción podría afectar la prestación de servicios básicos o generar un impacto económico y so…

Por lo general, operan bajo el modelo de Ransomware as a Service (RaaS), es decir, ofrecen este malv… hacen es proporcionar el ransomware y la infraestructura necesaria a afiliados, quienes ejecutan lo… comisión sobre las ganancias obtenidas. Sin embargo, la mayor parte de los beneficios económicos q… organización que administra el servicio”, explica Micucci.

¿Qué hacer?

Que la empresa más grande de Colombia haya sido víctima de una agrupación cibercriminal como esta deja en evidencia la vulnerabilidad del tejido empresarial frente a este tipo de ataques. Ninguna organización, por grande o robusta que sea, está exenta de convertirse en objetivo de los ciberdelincuentes.

La historia reciente también muestra que los atacantes no solo le apuntan a “los peces gordos”, sino que cualquier compañía, sea grande, mediana o pequeña, puede estar en su mira.

Por eso, los expertos en seguridad informática insisten en que las organizaciones deben asumir esta realidad y evolucionar de un modelo reactivo a uno preventivo. En otras palabras, no basta con responder cuando ocurre un ataque: es necesario identificar y corregir las vulnerabilidades antes de que sean explotadas, así como adoptar estrategias de ciberdefensa que fortalezcan los sistemas y reduzcan al máximo las oportunidades de éxito para los ciberdelincuentes.

Por Diego Ojeda
@DiegoOjeda95 Dojeda@elespectador.com

Suscriptores Política

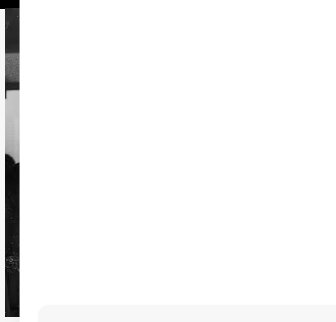
Partidos reparten poder legislativo ad portas del nuevo gobierno: ¿respetarán los acuerdos?

Hace 11 horas

Suscriptores Judicial

Desaparición del ingeniero Camilo Peláez: cuatro capturados y ninguna pista de su paradero

Hace 1 hora



Plinio Apuleyo Mendoza y la memoria plasmada en la literatura

Hace 12 horas