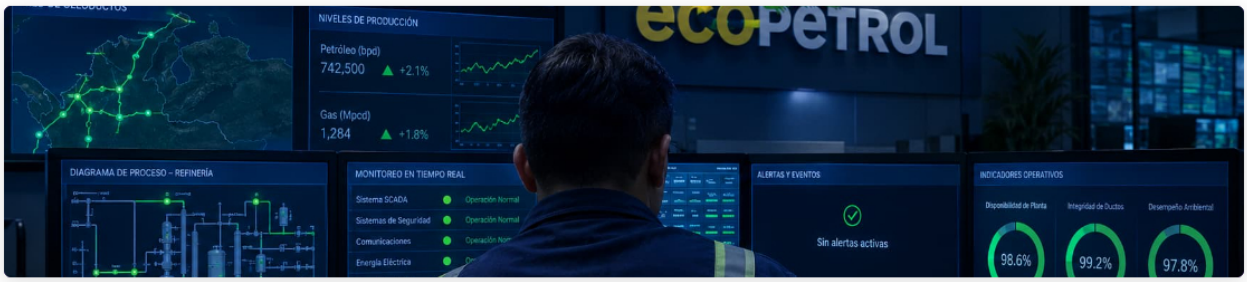
Ecopetrol: el ransomware que no funcionó y por qué eso importa para tu empresa

22 de julio de 2026 por Gerardo Rios



¿Qué ocurrió?

La noche del 17 de julio, Ecopetrol confirmó que un actor externo no identificado accedió a los entornos de almacenamiento en la nube de aproximadamente 15 empresas de su grupo, incluida la petrolera más grande de Colombia. El resultado: descarga no autorizada de datos asociados a cerca de 3,300 cuentas de usuario, y un intento de desplegar ransomware para cifrar esa información.

Aquí está la parte que casi nadie destaca cuando habla de ransomware: el intento de cifrado fue bloqueado. Los controles de seguridad de Ecopetrol detectaron y detuvieron el intento de secuestro de información antes de que los atacantes pudieran encriptar los archivos. Los datos fueron descargados, pero no destruidos ni cifrados. Días después, los responsables del ataque comenzaron a exigir un pago, amenazando con divulgar públicamente la información robada.

¿A quién afecta?

Directamente, a las 15 empresas del Grupo Ecopetrol y a los dueños de las 3,300 cuentas comprometidas. Pero el patrón detrás de este ataque no es exclusivo de una petrolera colombiana: es el mismo esquema de "doble extorsión" que golpea a empresas medianas en toda América Latina todos los días. Robar primero, cifrar después si se puede, y si no se puede cifrar, extorsionar de todos modos con la simple amenaza de publicar lo robado.

Para una empresa mexicana, el tamaño de Ecopetrol puede sentirse lejano. La lección no lo es. Cualquier negocio que guarde información de clientes, empleados o proveedores en almacenamiento en la nube (que hoy es prácticamente cualquier empresa con Office 365, Google Workspace o un ERP en la nube) es un blanco igual de válido para este mismo esquema, solo que con menos capacidad de respuesta que una empresa del tamaño de Ecopetrol.

¿Cuál es el riesgo real?

El riesgo real no es solo perder archivos. Es la combinación de tres cosas que ocurrieron aquí en simultáneo: acceso no autorizado, exfiltración de datos, e intento de cifrado. Cuando las tres fallan al mismo tiempo, es cuando una empresa cierra operaciones por semanas. Ecopetrol logró contener dos de las tres. Eso no es suerte, es el resultado de tener controles de seguridad activos antes de que ocurriera el ataque, no después.

El dato que más debería inquietar a cualquier empresa mexicana es este: casi 7 de cada 10 organizaciones en el país ya sufrieron al menos un ciberataque en el último año, y la mayoría no tiene la capacidad de detección que permitió a Ecopetrol frenar el cifrado a tiempo. La diferencia entre "tuvimos un incidente que contuvimos" y "tuvimos una crisis que nos paró meses" casi siempre se decide antes del ataque, no durante.

¿Cómo funciona este tipo de ataque?

Imagina que un ladrón entra a tu bodega. Primero, se lleva copias de todo lo que puede cargar (esa es la exfiltración). Luego intenta prender fuego a lo que queda para que no puedas usarlo

tú tampoco (ese es el cifrado del ransomware). Si el sistema de rociadores automáticos apaga el fuego antes de que se propague, el ladrón se queda solo con las copias que ya sacó, pero no logró destruir el original. Aun así, ya tiene algo con qué extorsionarte: "págame, o publico lo que me llevé."

Eso es exactamente lo que pasó en Ecopetrol. El acceso inicial casi siempre ocurre por credenciales robadas, un enlace de phishing, o un proveedor externo con acceso mal controlado, no por una falla mágica e inevitable. Una vez adentro, el atacante explora, encuentra dónde están los archivos valiosos, los copia, y solo después intenta cifrar. Ese "después" es la ventana donde un sistema de detección bien configurado puede intervenir, como ocurrió aquí.

Recomendaciones

Esta semana: revisa si tu proveedor de nube (Microsoft 365, Google Workspace, o el que uses) tiene activada la autenticación multifactor para todas las cuentas, sin excepción, incluyendo cuentas de proveedores externos con acceso a tu información.

Este mes: confirma que tus respaldos estén realmente aislados de tu red principal y que se prueben periódicamente. Un respaldo que vive en el mismo entorno que se puede cifrar no es un respaldo, es una copia más para el atacante.

Largo plazo: invierte en capacidad de detección temprana, no solo en prevención. Ecopetrol no evitó el acceso no autorizado, lo que evitó fue que ese acceso se convirtiera en una crisis total. Esa capacidad de "detectar y contener a tiempo" es exactamente lo que separa un incidente manejable de un cierre de operaciones, algo que ya vimos con el robo de credenciales de FortiGate que terminó en ransomware de las bandas INC y Lynx.

Conclusión

Ecopetrol no salió ilesa de este ataque, hubo robo de datos y hay extorsión activa en curso. Pero tampoco vivió el peor escenario posible, y esa diferencia se construyó con controles que ya estaban funcionando antes de que el ataque comenzara. Para cualquier empresa mexicana, la pregunta que vale la pena hacerse hoy no es "¿nos va a pasar?", los números dicen que la probabilidad ya es alta. La pregunta es: si pasa mañana, ¿tus controles detienen el cifrado a tiempo, o vas a enterarte del ataque hasta que ya sea demasiado tarde?

Si no sabes la respuesta con certeza, ese es exactamente el punto de partida de un diagnóstico. En Código Vigía lo hacemos sin costo y sin tecnicismos. Agenda el tuyo aquí.

en **Ciberseguridad**

Código Vigía
Tu seguridad es nuestra prioridad