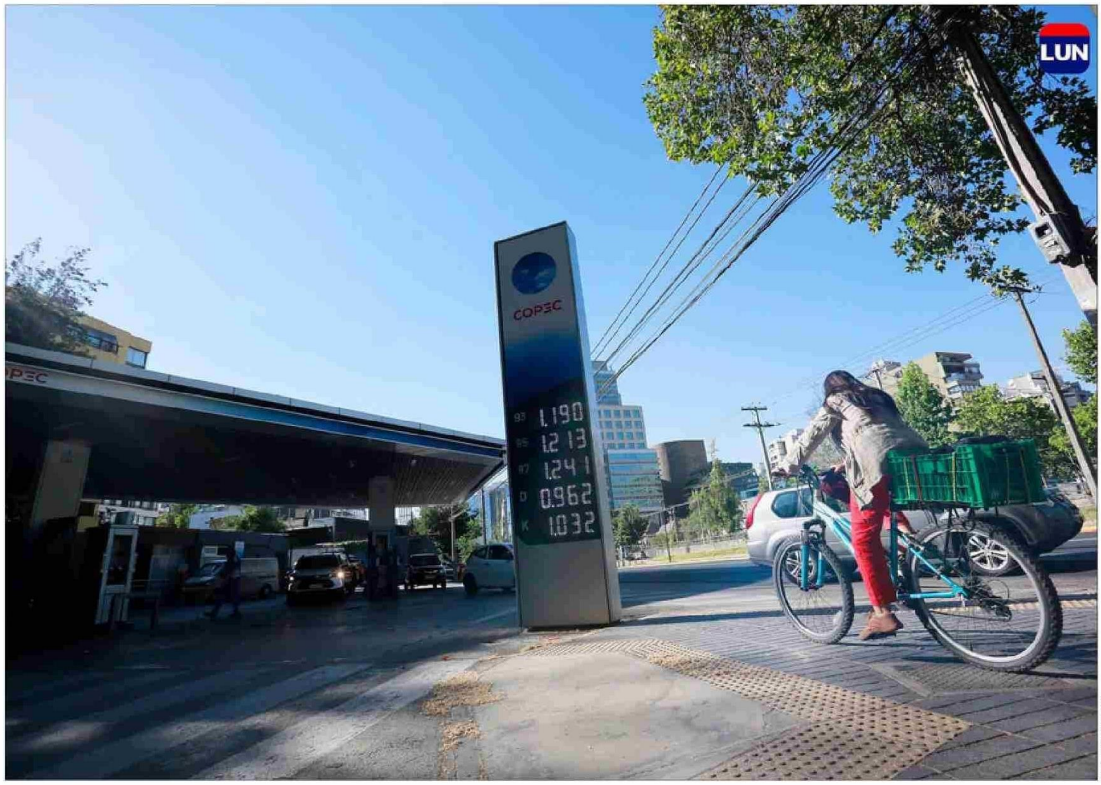
LITORALPRESS

Fecha: 11-01-2026
Medio: Las Últimas Noticias
Supl. : Las Últimas Noticias
Tipo: Noticia general
Título: **Expertos analizan ciberataque de hackers a Copec: "Nunca hay que pagarles"**

Pág. : 4
Cm2: 613,0

Tiraje: 91.144
Lectoría: 224.906
Favorabilidad: No Definida



En un comunicado, la empresa informó que la operación de Copec y de sus filiales no se vio afectada por el ciberataque.

RICHARD ULLOA

Delincuentes informáticos habrían exigido 6 millones de dólares para no revelar información robada

Expertos analizan ciberataque de hackers a Copec: "Nunca hay que pagarles"

El grupo Anubis dice haber extraído 6 terabytes de datos corporativos; la empresa asegura que no hay riesgo para los clientes.

CIRO COLOMBARA C.

En la religión del antiguo Egipto, Anubis era el dios de la muerte, la momificación y el más allá. Representado como un hombre con cabeza de lobo, era quien acompañaba a los muertos al inframundo, protegiéndolos en su viaje, además de cuidar las tumbas.

En la pagana actualidad, este es el nombre de un grupo de cibercriminales que acaban de sumar a su prontuario un ataque a Copec.

El viernes, a través de un comunicado, la empresa informó que había detectado un incidente de seguridad asociado "a un acceso no autorizado a un sistema de almacenamiento de información de uso interno", precisando que la operación de Copec y de sus filiales no se vio afectada. También destacó que "los sistemas que administran datos personales de clientes, claves o información que permita operar plataformas digitales no se vieron comprometidos; por lo tanto, todos los sistemas y servicios de la compañía continúan funcionando con normalidad y pueden seguir siendo utilizados de manera habitual por nuestros clientes".

Según la información que estos hackers informáticos hicieron llegar al portal SuspectFile.com -especializado en ciberseguridad, que investiga y reporta sobre ciberataques-, exigen el pago de seis millones de dólares para no revelar la información robada, que correspondería a cerca de 6 terabytes de datos corporativos que lograron extraer de servidores comprometidos. La compañía habría ofrecido en una primera instancia 120.000 dólares y luego 400.000. Al no llegar a acuerdo, la amenaza de Anubis era publicar todos esos datos.

Datos encriptados

Según explica Juan Pablo Arias, gerente de ingeniería para Fortinet Chile, uno de los métodos más usados por los ciberdelincuentes es el phishing, que consiste en el envío de mensajes falsos a través de mails o redes sociales, con enlaces que derivan a sitios webs fraudulentos -similares a los reales- para que las personas ingresen ahí información como contraseñas, datos bancarios o números de tarjeta, usando mensajes. "Es algo que ha ido evolucionando, si antes era principalmente a través de un SMS ahora es posible hacerlo en un mensaje de WhatsApp, Instagram o cualquier otro canal de comunicación. Otro es el llamado *ransomware*, algo mucho más sofisticado y dañiño ya que pueden pasar semanas oincluso meses para que una empresa o institución afectada pueda volver a operar normalmente".

El ataque de Anubis fue precisamente con un *ransomware*, un tipo de software malicioso que cifra los datos de la empresa y les permite a los hackers pedir dinero a cambio de desbloquearlos. "Hoy en día es el ataque más popular", dice Gabriel Bergel, CEO de la empresa de seguridad Mantis y también CEO de 8.8 Computer Security Conference. Agrega que, hasta hace algún tiempo, el único objetivo era pedir rescate para desencriptar los datos. En la actualidad hay una doble extorsión, porque también amenazan con hacerlos públicos si es que no pagan, lo que es complicado cuando se trata de información sensible".

En el caso de Copec, Anubis dice que aprovecharon una vulnerabilidad en una VPN corporativa. ¿Qué significa eso?

"Una VPN es una plataforma que les permite a las personas conectarse remotamente y de manera segura a la empresa. Pero si yo no la protejo adecuadamente, podría llegar a ser vulnerable. Los hackers, a través de ataques masivos, buscan debilidades y una vez que las encuentran, por ejemplo a nivel de software o de sistema operativo, ingresan a un servidor y después hacen lo que se llama movimiento lateral, pasando luego a otro y a otro hasta que llegan a aquellos que tienen bases de datos o información privada de trabajadores, clientes, etcétera".

¿Pagar o no pagar?

Juan Pablo Arias subraya que no existe una negociación segura con los hackers. "Pagar no garantiza nada y solo incentiva nuevos ataques. Además, ese dinero financia el cibercrimen". El profesional agrega que las empresas necesitan invertir para tener la mejor protección posible. "Quienes no han hecho inversiones ni tomado medidas en relación con este tema, van a tener que incurrir rápidamente en gastos".

Algo similar plantea Gabriel Bergel, quien con mucho énfasis dice que "nunca hay que pagarles. De partida, porque así se está financiando el cibercrimen. A la vez, tampoco se tiene la garantía de que al hacerlo los hackers vayan a desencriptar la información o no hacerla pública. De hecho, existe harta estadística que demuestra que las empresas que pagan muchas veces vuelven a ser atacadas".

Bergel explica que los datos personales son un tremendo negocio en el mundo de los cibercriminales. "Vender una identidad, como el nombre y datos básicos, les permite ganar alrededor de 10 dólares. Una identidad completa, que incluye credenciales del banco o del retail, entre otros, puede llegar a costar unos 100 dólares. Mientras más completo sea el perfil de la persona, más vale en ese mundo".