BancoEstado, uno de los tres bancos más grandes de Chile, se vio obligado a cerrar todas sus sucursales este lunes, después de un ataque de ransomware que tuvo lugar el fin de semana.

> *«Nuestras sucursales no estarán operativas y permanecerán cerradas hoy»*, dijo el banco en un comunicado en Twitter.

Los detalles del ataque no se han hecho públicos, pero una fuente cercana a la investigación asegura que la red interna del banco estaba infectada con el ransomware REvil (Sodinokibi).

El incidente ya está siendo investigado por haberse originado en un documento malicioso de Office, recibido y abierto por un empleado. Se cree que el archivo malicioso de Office instaló una puerta trasera en la red del banco.

Los investigadores creen que en la noche del viernes, los hackers utilizaron esa puerta trasera para acceder a la red del banco e instalar el ransomware.

Los empleados del banco que trabajaban en turnos de fin de semana descubrieron el ataque cuando no pudieron acceder a sus archivos de trabajo el sábado.

BancoEstado denunció el incidente a la policía chilena y el mismo día, el gobierno chileno lanzó una alerta de seguridad cibernética a nivel nacional, advirtiendo sobre una campaña de ransomware dirigida al sector privado.

En un principio, el banco esperaba recuperarse del ataque sin ser notado, pero el daño fue tan extenso que el ransomware encriptó la gran mayoría de los servidores internos y estaciones de trabajo de los empleados.

El banco reveló el ataque el domingo, pero con el paso del tiempo, los funcionarios del banco se dieron cuenta de que los empleados no podrían trabajar el lunes y decidieron mantener

las sucursales cerradas mientras se recuperan.

Cabe mencionar que el banco segmentó correctamente su red interna, limitando lo que los hackers podían cifrar. El sitio web, el portal bancario, las aplicaciones móviles y los cajeros automáticos no sufrieron daños, con lo que el banco aseguró a sus clientes que sus fondos estaban seguros.

La banda del ransomware REvil es uno de los pocos grupos que opera un sitio de filtraciones, donde filtra archivos de las redes que viola, en caso de que la víctima no quiera pagar. Hasta ahora, BancoEstado no aparece en el sitio de la filtración, lo que podría significar que el banco pagó el rescato o está negociando con los piratas informáticos.

Esta es la segunda vez que los piratas informáticos atacan a un banco chileno. En junio de 2018, los hackers norcoreanos desplegaron malware de limpieza de discos en la red del Banco de Chile, mientras intentaban ocultar un hackeo bancario.

Un año después, también atacaron a Redbanc, la compañía que interconecta la infraestructura de cajeros automáticos de todos los bancos chilenos, durante un intento de orquestar un esquema de retiro de efectivo en cajeros automáticos.