API CHILE E.I.R.L
ISSLA RISK CHILE SPA
DOZA

Santiago, 17.SEP.020

“Hackeo a Banco Estado de Chile”

Las primeras indagaciones que realizan las agencias federales de Estados Unidos confirmarían la pista de que los responsables del ataque al banco estado de chile, habrían sido hackers asiáticos, como los responsables del ataque cibernético hacia la entidad.

El ataque cibernético produjo problemas de soporte, caída de página web, problemas en la Aplicación de Android, todo esto conlleva que se suspendieron durante varios días la atención directa a los clientes del banco estado, si bien la entidad del banco informa que no fueron comprometidas las cuentas bancarias de los clientes adscritas a esta, informaron a través de redes sociales del banco, correos hacia los clientes y a través de su página web que, recomendaban que no hicieran transferencias ni compras a través de internet, ya que aún estaban resolviendo el problema y que también cerrarían sucursales a lo largo del país.

Por el modus operandis del ataque, diversas entidades ligadas a la seguridad informática coinciden que el ataque habría sido obra de hackers de Corea del Norte, esta pista para los investigadores es una de las principales líneas de investigación.

Igualmente, no hay antecedentes o datos de que haya podido participar en el hecho algún hacker chileno, especialmente por la sofisticación del ataque. Según antecedentes se hicieron los rastreos

periciales que indican que se trataría de dos grupos asociados a Corea del Norte y que habrían operado desde diversos países coordinadamente.

Cabe señalar que en el 24 de mayo del 2018 el Banco de Chile fue víctima de un ataque informático, en el cual un virus había logrado ingresar a la red de la institución y comenzaba a utilizar computadores anulando sus discos de arranque. Mientras el equipo de ciberseguridad se enfocaba en proteger datos e informaciones de clientes, decenas de transferencias de ejecutaban automáticamente desde cuentas del banco hacia el extranjero. Este hecho encendió las alertas y en ese momento la institución bancaria se dio cuente de que el virus en los computadores fue una distracción y que el peligro fue el robo de millones de dólares.

Volviendo al caso anterior del banco estado, los ciberataques llegaron para quedarse y van a ocurrir continuamente en Chile, por lo que las instituciones gubernamentales, empresas públicas o privadas tendrán que invertir en ciberseguridad y en formar equipos de monitoreo constante, para poder tomar decisiones y prevenir, esto conlleva una gran inversión de capital, que no todos tendrán acceso por su alto costo en equipamiento y recursos humanos, esto quiere decir la formación de equipos de personas con constante capacitación tecnológica, uso de plataformas, sistemas operativos, etc.

Se debe señalar que las sospechas recaen en varios grupos de hackers, pero especialmente en BeagleBoyz, hackers de corea del norte que roban dineros de cuentas y cajeros automáticos en todo el mundo. Hackers norcoreanos ya habían sido señalados por empresa de ciberseguridad, como responsables del ataque a gran escala contra bancos en todo el mundo en el 2018. Además, en el año 2019 la ONU también denuncio al régimen de Kim Jong-un de orquestar el robo de cerca de 2.000 millones de dólares de instituciones financieras.

Uno de las motivaciones y objetivo que puede tener este grupo de hackers para cometer este tipo de delitos transnacionales, es el de proveer recursos al régimen de Corea del Norte, acorralado por las sanciones internacionales de parte del Consejo de Seguridad de las Naciones Unidas., precisamente este tipo de fondos robados por medio de ciberataques pueden ser utilizados para financiar actividades ilegales, como el desarrollo de armas nucleares y misiles balísticos de corto, medio y largo alcance. También uno de los motivos de que se haya efectuado este ataque informático al banco estado, es el conocimiento del retiro del 10 % desde las cuentas de pensiones de todos los chilenos, el cual sería depositada por las afp a las distintas cuentas bancarias dispuestas por los afiliados en su solicitud. Esto consecuencia de los problemas financieros que ha acarreado en la economía chilena la pandemia del Covid-19.

El banco estado de chile deberá adoptar medidas de alta seguridad cibernética y modernización estructural, ya que cuenta con 12 millones de clientes aproximadamente y que tiene una amplia cobertura en el territorio chileno, por lo que ahora o en el futuro se puede ver nuevamente afectado por ataques cibernéticos.

API CHILE GLOBAL INTELLIGENCE
INTELIGENCIA - CONTRAINTELIGENCIA - CIBERSEGURIDAD - GEOPOLÍTICA - CONTRATERRORISMO

SANTIAGO - CHILE
(56-2) 3249 7444 - (56-2) 3205 5963
APICHILEAGENCIA@GMAIL.COM - APICHILEAGENCIA@PROTONMAIL.COM
FACEBOOK: APICHILEGLOBALINTELLIGENCE
WEB: WWW.APICHILEGLOBALINTELLIGENCE.COM