

Brasil sufre el mayor ciberataque financiero de su historia bancaria

La venta de credenciales de cuenta privilegiada permitió a ciberdelincuentes transferir fondos del Banco Central brasileño a cuentas en el extranjero y convertirlos en criptomonedas.

El miércoles pasado, Brasil experimentó el ciberataque más grave de su historia bancaria. En apenas dos horas y media, un grupo de ciberdelincuentes obtuvo acceso a los sistemas vinculados al Banco Central de Brasil y sustrajo más de 800 millones de reales (148 millones de dólares), provocando un terremoto en la confianza de la infraestructura financiera del país. La operación afectó al sistema de pagos instantáneos PIX, que se ha convertido en el motor de la digitalización económica de Brasil desde su lanzamiento en 2020.

El punto de entrada fue sorprendentemente sencillo: la compra de credenciales legítimas pertenecientes a un empleado de C&M Software, la empresa tecnológica responsable de integrar a bancos de menor tamaño y fintechs con los sistemas centrales del Banco Central. Según la Policía Civil de São Paulo, João Nazareno Roque, de 48 años, entregó sus claves de acceso y explicó detalladamente cómo funcionaba la interfaz. A cambio, recibió alrededor de 2.700 dólares. Este detalle es relevante porque confirma que la explotación de vulnerabilidades humanas sigue siendo más efectiva que cualquier sofisticado malware.

El funcionamiento del ataque

C&M Software actúa como intermediario tecnológico en la llamada cadena de suministro financiera. No es la primera vez que una intrusión ocurre a través de un proveedor externo, pero sí es la más impactante en términos de volumen económico e impacto en los servicios.

Una vez obtenidas las credenciales, los delincuentes se conectaron a los sistemas que gestionan las cuentas de reserva: depósitos que los bancos mantienen en el Banco Central para garantizar liquidez, participar en operaciones interbancarias y realizar inversiones en títulos públicos. A través de instrucciones aparentemente legítimas, ejecutaron transferencias millonarias que fueron procesadas sin activar alertas automáticas.

El destino inicial del dinero fueron cuentas abiertas en corredoras de bolsa regionales y entidades no bancarias en Brasil, Paraguay y Argentina. Posteriormente, una parte de los fondos se convirtió en criptomonedas, incluyendo Bitcoin, Ethereum y Tether (USDT), con el propósito de dificultar su rastreo y recuperación.

Según los primeros análisis de la unidad especializada en delitos financieros, entre 30 y 40 millones de dólares se transformaron en activos digitales durante las primeras horas posteriores a las transacciones, antes de que se activaran los bloqueos judiciales.

El impacto en bancos y fintechs

Al menos seis instituciones financieras resultaron afectadas. La mayor damnificada fue BMP, un operador que no trabaja con clientes minoristas y que desarrolla soluciones de Banking as a Service (BaaS) para terceros. BMP perdió casi 100 millones de dólares. También se identificaron afectaciones a Credsystem y Banco Paulista, aunque el Banco Central no ha publicado la lista completa de entidades comprometidas.

Para contener la propagación del incidente, el Banco Central suspendió de inmediato todas las conexiones de C&M Software al sistema PIX. Durante varias horas, miles de empresas y millones de usuarios particulares se vieron imposibilitados de realizar pagos y transferencias. El servicio se restableció parcialmente dos días después, cuando se verificó que la infraestructura central no había sufrido alteraciones técnicas.

Una intrusión que evidencia una crisis de confianza

El propio Banco Central reconoció que el incidente representa un hito sin precedentes y que requerirá una revisión de protocolos de seguridad y gobernanza en todas las entidades que utilizan proveedores externos.

Uno de los aspectos más inquietantes es la forma en que los delincuentes captaron al empleado. Roque relató a las autoridades que fue abordado a la salida de un bar por un intermediario que le ofreció un pago inmediato y la promesa de no ser descubierto. Para evitar rastreo, cambiaba de teléfono cada dos semanas y jamás conoció en persona a sus contactos.

El incidente refuerza la necesidad de medidas como la autenticación multifactorial obligatoria, la segmentación de privilegios y la supervisión continua de accesos.

La ruta de blanqueo: criptomonedas y casas de cambio

Una vez ejecutadas las transferencias, los delincuentes recurrieron a la infraestructura de casas de cambio y plataformas OTC (Over The Counter) en América Latina. Estas entidades permiten transformar rápidamente dinero fiduciario en criptoactivos que, gracias a su naturaleza descentralizada, son más difíciles de rastrear.

Aun así, las autoridades brasileñas consiguieron bloquear aproximadamente 270 millones de reales (50 millones de dólares) antes de que salieran del sistema financiero tradicional. El resto permanece en direcciones de criptomonedas que están siendo monitoreadas con la ayuda de analistas en cadena y proveedores internacionales de inteligencia blockchain.

Fuente: https://bitlifemedia.com/

LINK DE LA NOTICIA