

Ciberataques bancarios

LA VULNERABILIDAD DE LOS SISTEMAS DE PAGOS TRANSFRONTERIZOS.

EDICIÓN IMPRESA

Yanos sorprenden los robos masivos de datos de tarjetas de crédito, pues tales delitos son cometidos a diario. Pero cuando los fondos bancarios son perforados, hay que prestar atención—en especial, cuando el hurto involucra el secuestro de las conexiones de los bancos con el sistema global de pagos—.

La semana pasada, la Sociedad para las Telecomunicaciones Interbancarias y Financieras Mundiales (Swift, por sus siglas en inglés), detalló una reciente ola de ataques cibernéticos que totalizó US\$ 90 millones. Swift es una red de 11,000 bancos que realizan transferencias de efectivo. Su CEO, Gottfried Leibbrandt, describió esa serie de robos como un “momento decisivo” y agregó que no solo afecta la reputación de los bancos, sino que amenaza la existencia de los que no consigan protegerse.

Los investigadores todavía intentan determinar cómo se estructuró un espectacular ciberataque que en febrero desvió US\$ 81 millones del banco central de Bangladés y quién estuvo involucrado. Este fue uno de los mayores atracos bancarios, pero pudo haber sido peor: US\$ 850 millones de las solicitudes de transferencia fueron bloqueados.

El dinero sustraído fue a parar a un banco en Filipinas y luego a casinos, aunque el destino final de la mayor parte es incierto. Un monto terminó donde un operador chino de intermediarios para apostadores, quien niega haber sabido que era robado.

El timo obligó a bancos y Swift a hurgar por más infiltraciones, lo cual ha resultado en al menos un caso similar, aunque menor: en diciembre, los ciberpiratas intentaron desviar US\$1 millón del vietnamita Tien Phong Bank. Otro sa-



Swift procesa 25 millones de mensajes diarios, cubriendo la mitad de todas las grandes transferencias transfronterizas.

lió a la luz en los tribunales: el Banco del Austro (Ecuador) ha demandado a Wells Fargo por autorizar transferencias fraudulentas a cuentas en Hong Kong por US\$ 12 millones (US\$ 3 millones fueron recuperados posteriormente).

Según los expertos, probablemente existan docenas de otros intentos o ataques realizados que no se hayan detectado. Los criminales cibernéticos han mejorado el encubrimiento de sus fechorías. Por ejemplo, en el caso de Bangladés, crearon un ma-

lware que interfirió en los listados que utilizaba el banco para verificar las transacciones. Jens Monrad, de la firma de ciberseguridad FireEye, que conduce una auditoría del robo, señala que el tiempo medio que toma a las compañías atacadas descubrir que sus sistemas han sido afectados es 146 días.

Ya es bastante malo el que las arcas bancarias estén siendo asaltadas por los ladrones del ciberespacio, pero lo peor es que estos robos expongan debilidades en una parte vi-

tal de la intermediación financiera: las conexiones de los bancos a la red Swift. En cada uno de los casos desvelados, los ladrones entraron en los sistemas de los bancos, utilizaron malware para penetrar la red Swift con el código único del banco atacado y desviaron las transacciones.

Swift procesa 25 millones de mensajes diarios, cubriendo la mitad de todas las grandes transferencias transfronterizas. Si la seguridad se viera comprometida, la confianza en este sistema podría evaporarse. Swift insiste en que su red y sus servicios de mensajería no han sido penetrados, y que los problemas de seguridad ocurrieron en los bancos. Sus funcionarios se han mostrado frustrados de que los

guladores, cuyo desempeño en este cambio varía notablemente. Entre los más efectivos figura el banco central de Reino Unido, que maneja un programa de testeo de resistencia para grandes bancos que incluye ciberataques simulados. Los bancos británicos que no pasan estas pruebas pueden ser forzados a mantener un capital que exceda los requisitos reglamentarios.

Los estándares en algunos países emergentes son más bajos y, por ello, no es coincidencia que los ciberpiratas hayan atacado bancos en mercados relativamente subdesarrollados y no en los que ofrecen mayores botines como Reino Unido o Estados Unidos, pero que están mucho mejor protegidos.

“Los estándares en algunos países emergentes son más bajos y, por ello, no es coincidencia que los ciberpiratas hayan atacado bancos en mercados relativamente subdesarrollados”.

bancos atacados demoran en compartir información al respecto, lo que impide a otros actuar con medidas preventivas.

Sin embargo, los pedidos de que Swift haga más aumentan (algunos expertos sugieren su reemplazo con tecnología blockchain, que es más segura). Leibbrandt respondió el 24 de mayo con el anuncio de un plan de “seguridad del cliente” dirigido a incentivar una mayor protección de la red, intercambio de información y detección de fraudes.

También pidió una nueva ola de innovación en ciberseguridad —que cubra “la detección de tendencias y anomalías, monitoreo, autenticación y biométrica”— que haga frente a la creciente amenaza de “maleantes agazapados detrás de un teclado”.

Pero Swift no tiene poder sobre los bancos. Eso corresponde a los re-

Claro que los bancos ubicados en los bastiones de las altas finanzas no deben dormirse en sus laureles. Incluso si sus defensas cibernéticas son fuertes, siempre existe el riesgo de la presencia de cómplices dentro de sus instalaciones (por ejemplo, no se ha descartado esta incidencia en el caso de Bangladés).

Varios grandes bancos, incluido JPMorgan Chase, han comenzado a restringir el número de empleados con acceso a sus plataformas de transferencias vía mensajes Swift. Es que los expertos no se cansan de decir que la ciberseguridad no es solo un asunto de tecnología sino también de personas.

Traducido para Gestión por Antonio Yonz Martínez
© The Economist Newspaper Ltd, London, 2016