

HACKER_

EXCELSIOR MARTES 16 DE ABRIL DE 2024

TAMBIÉN LOS ESTAFADORES

CIBERCRIMINALES CONTINÚAN APUNTANDO A LA BANCA

un incremento de 154% entre 2022 y 2023.

Hugo Werner, vicepresidente regional de Akamai para América Latina, detalló que el sector financiero de la región Europa, Oriente Medio y África fue el más afectado. Entre las razones destaca que este tipo de ataque se puede usar con motivos políticos, hacktivismo y guerra cibernética, especialmente en relación con el conflicto armado entre Rusia y Ucrania.

Añadió que se trata de un tipo de ataque que cuesta poco al cibercriminal y puede causar grandes daños a las empresas, de ahí que se enfoquen en acosar y tratar de extorsionar a los bancos de mayor tamaño y con gran reconocimiento de marca, aunque estos suelen tener buenos sistemas de seguridad.

“Estas campañas de DDoS son más persistentes y multivectoriales, ya que se dirigen a todas las áreas del sector financiero, como la gestión patrimonial, la banca, las tarjetas de crédito, los pagos digitales y los seguros”, añadió la directora de Inteligencia y directora ejecutiva de EMEA en el FS-ISAC, Teresa Walsh.

A lo que se añade que este no es el único método de ataque porque Netskope Threat Labs halló que el sector financiero sigue siendo uno de los más atacados por los grupos de ransomware.

Entre los principales atacantes del año pasado destacan las bandas Clop y LockBit, aunque ésta última ya fue perseguida y desmantelada por las fuerzas de seguridad.



Las instituciones y los usuarios deben incrementar sus medidas de seguridad para no ser una cifra más

POR AURA HERNÁNDEZ
aura.hernandez@gimm.com.mx

La industria financiera en México y el resto del mundo se mantiene como uno de los principales objetivos de ataque de los ciberdelincuentes y estafadores, una tendencia que seguirá al alza y que urge a las instituciones y usuarios a incrementar sus medidas de seguridad.

La Encuesta de Consumidores 2023: Fraude, Identidad y Banca Digital capítulo México, realizada por Fico, encontró que la población se preocupa más por los fraudes bancarios que por otros problemas relacionados con la banca como el robo de efectivo o las estafas al hacer compras online.



El sector financiero sigue siendo uno de los más atacados por los grupos de ransomware, que se centran en la explotación de vulnerabilidades a gran escala.”

PAOLO PASSERI
DIRECTOR DE CIBERINTELIGENCIA DE NETSKOPE



“Las organizaciones pueden mitigar el impacto de estos ataques a través de minuciosas políticas de ciberhigiene, incluida la evaluación periódica de sus redes, aplicaciones y medidas de seguridad.”

HUGO WERNER
VICEPRESIDENTE REGIONAL DE AKAMAI PARA AMÉRICA LATINA

Lo anterior se debe a que muchas veces los defraudadores en la red obtienen no sólo dinero, también adquieren información personal de la víctima que pueden usar para robo de identidad u otras

ATAQUES DDOS A SERVICIOS FINANCIEROS

Números por año



Fuente: Akamai

actividades maliciosas.

Por ejemplo, 63% de los encuestados temen que roben su identidad para abrir una cuenta bancaria sin su conocimiento y 6% indicó que ya fue víctima de esto.

Rafael Caballero, global business consulting para México y Colombia de Fico, consideró que este último porcentaje “no parece mucho, pero podría equivaler a 6 millones de víctimas.

De ahí que 75% de los encuestados consideren que tener una buena protección de fraudes es una de sus tres

consideraciones principales al elegir un banco, siendo las otras facilidad de uso, buen valor por el dinero y el uso ético de los datos del cliente.

Ante esto, Caballero consideró que las instituciones financieras deben gestionar varios tipos de fraudes a lo largo del ciclo de vida del cliente, sin que esto impacte la experiencia. Algunas medidas son usar datos de fuentes internas y externas para verificar la identidad, compartir datos para obtener mejores resultados que reduzcan las pérdidas por fraude y adoptar un

enfoque que incorpore todos los posibles tipos de fraude y funcione en diferentes carteiras y canales.

¿Y LOS GRUPOS MALICIOSOS?

Además del fraude, tanto las instituciones financieras como los usuarios pueden ser víctimas de campañas maliciosas realizadas por grupos de ciberdelincuentes.

El informe DDoS: Here to Stay, realizado por Akamai Technologies y FS-ISAC, encontró un aumento de los ataques distribuidos de denegación de servicio (DDoS) enfocados en servicios financieros y sus clientes.

Esto porque 35% de todos los ataques DDoS alrededor del mundo al cierre del año pasado se dirigieron a dicha industria, lo que representa

63.0

POR CIENTO

de los encuestados temen que roben su identidad para abrir una cuenta bancaria sin su conocimiento

35.0

POR CIENTO

de todos los ataques DDoS en el mundo en 2023 se dirigieron a la industria financiera

6.0

POR CIENTO

indicó que ya fue víctima de un robo de identidad y tienen cuentas bancarias falsas