BioCatch

Tendencias de fraude bancario en canales digitales en la región de LATAM en 2024

Informe de BioCatch sobre las tendencias y el panorama actual de fraude digital en la región de LATAM, con análisis regional y un caso práctico.

Septiembre de 2024

Acerca de este informe

Para elaborar este informe, el equipo de expertos de BioCatch, llevó a cabo una investigación sobre las últimas tendencias del fraude en América Latina.

El reporte ofrece una visión completa del panorama del fraude bancario en la región, incluyendo un análisis por nuestros equipos locales. Además, se focaliza en el problema del malware, tras haber observado un incremento de casos en múltiples países.

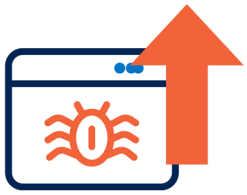
Este informe contiene las siguientes secciones:

- Tendencias principales en LATAM
- Las estafas en LATAM: La historia interminable
- Caso práctico: La evolución del malware

Tendencias principales en LATAM

32%
de aumento en los informes de fraude en la primera mitad del año (2024 frente a 2023)

En términos generales, el fraude está creciendo en la región. Los volúmenes de fraude reportado han aumentado de forma significativa en la primera mitad de este año en comparación con el mismo periodo de 2023. A nivel regional se observa un incremento del 32%, pero al analizar la situación de cada país, apreciamos situaciones diferentes. En Colombia y Argentina por ejemplo, el fraude aumenta, mientras que en Perú y Ecuador, el fraude baja.



113%
de aumento en casos de malware

El malware reaparece con fuerza en la región, con un aumento del 113% en los volúmenes de casos reportados durante la primera mitad del año. Donde más han aumentado los casos es en Argentina y Colombia, aunque se detectan subidas en México, Brasil y Perú. A diferencia de otras regiones que hemos analizado este año, donde predomina el malware en dispositivos móviles, el malware que vemos en América Latina es principalmente para dispositivos que usan navegadores web.

Aumento de fraude desde dispositivos móviles

Al igual que en el resto del mundo, los dispositivos móviles se emplean en el 79% de los casos de fraude – un aumento del 12% respecto al año pasado.

LOS TRES TIPOS DE FRAUDE MÁS COMUNES

Estafas de ingeniería social

Dispositivos robados

Apropiación de cuentas

Mientras que en el resto del mundo existe una tendencia hacia el uso de aplicaciones bancarias para ejecutar fraude desde los dispositivos móviles, vemos que el 30% de los fraudes se realizan desde **navegadores web en los dispositivos móviles**, lo cual representa un **aumento del 55%** en la primera mitad de 2024.

Panorama de amenazas en LATAM

México

- Estafas con llamadas telefónicas
- Suplantación de identidad
- Acceso remoto en dispositivos web y móvil
- Malware
- Dispositivos robados

Colombia, Costa Rica y Panamá

- Estafas con llamadas telefónicas
- Apropiación de cuentas tradicional
- Malware

Brasil

- Dispositivos robados
- Malware
- Estafas con llamadas telefónicas

Ecuador y Perú

- Apropiación de cuentas
- Dispositivos robados
- Estafas con llamadas telefónicas
- Fraude por suplantación de identidad (familiares)
- Malware

Chile

- Phishing
- Dispositivos robados
- Ingeniería social

Argentina y Uruguay

- Ingeniería social
- Apropiación de cuentas tradicional
- Cuentas mulas
- Dispositivos robados
- Malware

"Cada mensaje es diferente, pero el objetivo es el mismo: ***engañar a las víctimas para que proporcionen información personal.*** *"*

Josué Martínez
Director del equipo de Global Advisory para la región de LATAM

Las estafas en LATAM: La historia interminable

En muchos países de Latinoamérica, recibir llamadas, mensajes de texto y correos electrónicos sospechosos se ha convertido en algo cotidiano, hasta tal punto que la gente se ha vuelto insensible a las estafas por mensaje de texto o llamadas telefónicas. Somos capaces de analizar rápidamente un SMS y extraer información clave que nos permite identificar si el mensaje puede ser legítimo o no. Esto nos lleva a preguntarnos: ¿Por qué tienen tanto éxito?

Los defraudadores comprenden a sus objetivos y saben aprovecharse de sus debilidades para contar historias creíbles. Por ejemplo, saben que todos los días se entregan 436 millones de paquetes en todo el mundo, por lo que una campaña de smishing que alerta a los destinatarios de que su paquete se encuentra detenido en la aduana, probablemente tenga éxito, sobre todo en esta nueva normalidad en la que cada vez más personas vuelven a la oficina tras el teletrabajo provocado por el COVID-19.

Al aprovecharse de lo desensibilizados que nos hemos vuelto a estos mensajes, los defraudadores pueden sorprender a algunas de sus víctimas con la guardia baja, utilizando situaciones cotidianas creíbles para convencerles a que entreguen información personal. Como estas historias son factibles, las víctimas no dudan en proporcionar esta información. Tener un paquete retenido en la aduana con un cargo lógicamente supondría utilizar una tarjeta de crédito. Asimismo, si no estaba en casa cuando se intentó entregar un paquete, es normal tener que confirmar una dirección.

En muchos casos, estas víctimas estaban esperando paquetes reales y como éstas llegan a sus casas, es posible que ni siquiera cuestionen el proceso por el que pasaron, por lo que no soy conscientes de haber entregado información confidencial a unos defraudadores, que no esperarán para aprovecharla, bien sea retirando dinero de su cuenta bancaria a veces a través de la apropiación de cuenta, o bien sea a través de la ingeniería social (la opción más frecuente).

La información que los defraudadores obtienen a través de estos ataques de ingeniería social les ayuda para crear, una vez más, una historia creíble. "Llamo de parte de su banco sobre un problema con su cuenta. Para demostrar que soy del banco, los últimos cuatro dígitos de su tarjeta de crédito/débito son XXXX". Una vez que el defraudador ha convencido a la víctima de su (falsa) identidad como trabajador del banco, le indica el proceso a seguir para realizar pagos.

Los datos de BioCatch muestran un crecimiento de estos casos de fraude en la región de LATAM. Chile y Argentina son los países que más los sufren. En Chile, durante los primeros seis meses de este año, estas estafas han triplicado en comparación con 2023. Mientras tanto, otros países (por ejemplo, México) han comenzado a observar una disminución de estas cifras, gracias a los controles adicionales implementados por los bancos para proteger a sus clientes.

La regulación como medida de protección

Debido a la envergadura de este problema y el impacto que tiene para los consumidores, sobre todo quienes llegan a perder todos sus, muchos países han recurrido a la regulación para promover y reforzar el reembolso de estas estafas.

- En Chile, la Ley 21234 establece el proceso y los mecanismos a través de los cuales un usuario puede solicitar un reembolso cuando cae víctima de un fraude o estafa.
- En Colombia, una ley, coloquialmente conocida como "si es estafa, no paga", requiere que los bancos reembolsen a las víctimas de fraude, si pueden verificar sus alegaciones. También ayuda a las víctimas de robo de identidad a reconstruir su puntaje crediticio en bancos y otras instituciones financieras.
- Otros países como Brasil y México están trabajando en ampliar cada vez más la regulación para ofrecer protecciones adicionales a los usuarios que son víctimas de estafas. Estas medidas contemplan que los bancos comparten información entre ellos.

Si bien estas medidas ayudan a proteger el dinero de las víctimas cuando ocurre la estafa, no evitan que las estafas ocurran. Además, las víctimas deben informar del fraude, y los estudios muestran que muchos fraudes/estafas no se informan, o por desconocimiento de que los importes se pueden recuperar, o debido a un sentimiento de vergüenza.

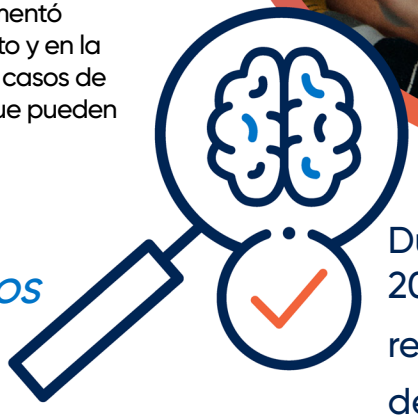
Por ello, se debe animar a los bancos a que también tomen medidas proactivas, que van desde informar a sus clientes sobre las estafas y las señales de advertencia a las que deben prestar atención, hasta advertencias sobre estafas durante los procesos de pago en la banca digital.

Creación de perfiles de comportamiento

Es evidente que no existe una solución única para combatir las estafas, pero una medida común entre muchas instituciones financieras de todo el mundo es la implementación de preguntas e indicaciones dinámicas basadas en la creación de perfiles de comportamiento durante la sesión de banca digital. Al analizar de qué manera se comporta un usuario, los bancos pueden detectar patrones que indican que se está llevando a cabo una estafa. Con esta información, el banco puede proporcionar alertas y advertencias a los usuarios durante los procesos de pago en la banca digital, lo que fomenta una reflexión y razonamiento adicional por parte de la víctima sobre el pago que está ejecutando. El objetivo final es ayudar al usuario a darse cuenta de lo que está pasando en estas situaciones para que no caiga en la estafa y evite realizar pagos a los defraudadores.

Hemos sido testigos de esto en México. Un banco implementó estas medidas gracias a la biometría del comportamiento y en la primera mitad de 2024, vio una reducción del 60% en los casos de estafas con llamada telefónica, lo cual ilustra el poder que pueden proporcionar los datos del comportamiento.

"Al analizar de qué manera se comporta un usuario, los bancos pueden detectar patrones que indican que se está llevando a cabo una estafa".



Durante los primeros seis meses de 2024, un banco mexicano vio una reducción del **60%** en los casos de estafas con llamada telefónica.

CASO PRÁCTICO:

La evolución del malware

Una tendencia algo inesperada para 2024 ha sido el aumento de casos de malware, específicamente los malwares para dispositivos web. Desde Brasil, Colombia, México y Argentina, hemos notado un aumento de casos de malware. Para ilustrarlo en este caso práctico, profundizaremos sobre la situación en Argentina

Grandoreiro

Grandoreiro es un troyano de malware bancario que lleva más de siete años controlando las sesiones bancarias de instituciones financieras en América Latina y España. A principios de este año, volvió a ser protagonista por dos motivos. En primer lugar, una operación policial capturó a varios miembros de la banda responsable de estos ataques, así como a más de 130 operadores de cuentas mulas.[1] En segundo lugar, Grandoreiro volvió a atacar con rapidez y con más fuerza todavía, probablemente bajo un modelo de "malware como servicio".[2]

Varios análisis sugieren que este malware se extiende por todo el mundo, apuntando a más de 1500 instituciones financieras a nivel global, de las cuales más del 20% se encuentran en LATAM.[2]

En 2023, Argentina sufrió las mayores pérdidas por fraude debido al malware Grandoreiro, seguida por México y Brasil (de los países de LATAM).[3]

Mekotio

Desde hace una década, hemos visto al malware Mekotio en la región. En sus orígenes, se parece a Grandoreiro, ya que utiliza correos electrónicos de phishing para engañar a sus víctimas a que pinchen en enlaces corruptos que descargan el malware en el dispositivo del usuario. Esto permite a los defraudadores robar credenciales, y más adelante, realizar transacciones fraudulentas.

Países en los que al menos una institución financiera se ha convertido en objetivo del malware Grandoreiro

$120 millones

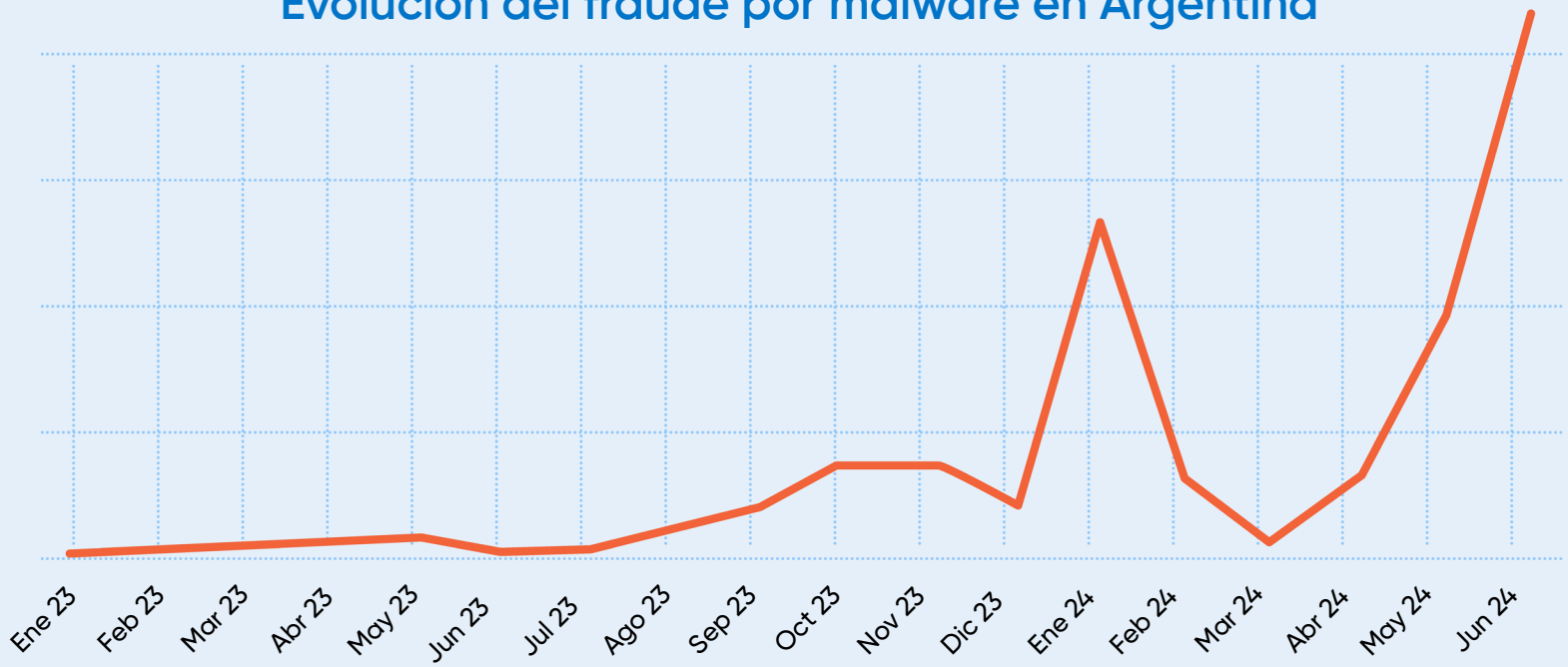
en pérdidas debido al malware Grandoreiro (estimación)

1. https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=16066
2. https://www.bleepingcomputer.com/news/security/banking-malware-grandoreiro-returns-after-police-disruption/#google_vignette
3. https://www.trendmicro.com/en_us/research/24/d/trend-micro-collaborated-with-interpol-in-cracking-down-grandore.html

CASO PRÁCTICO:

La evolución del malware

Evolución del fraude por malware en Argentina



El aumento de casos de malware

Cuando analizamos los volúmenes de casos en los que se identifica al malware como la causa principal del fraude, observamos un aumento sostenido durante la segunda mitad de 2023, lo cual llamó la atención de nuestros expertos en fraude.

Luego, en enero de 2024, observamos que el número de casos alcanzó su nivel máximo (hasta entonces), con volúmenes más de tres veces mayores, en comparación con los tres meses previos.

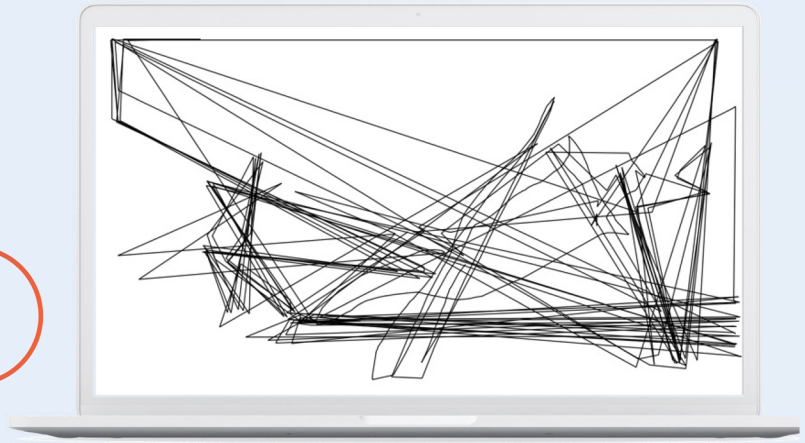
Debido a la rápida reacción de los bancos, que fue posible gracias a la implementación de la inteligencia de biometría del comportamiento, el volumen de casos volvió a su nivel anterior con bastante rapidez.

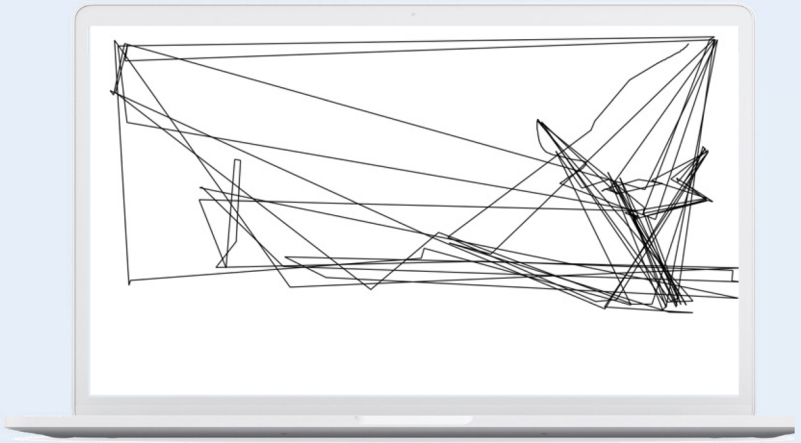
Sin embargo, tras unos meses, se aprecia una nueva subida, con más intensidad, en los meses de mayo y junio. Además, vemos que las variantes del malware evolucionaron en un intento de evadir los controles establecidos por los bancos.

CASO PRÁCTICO:

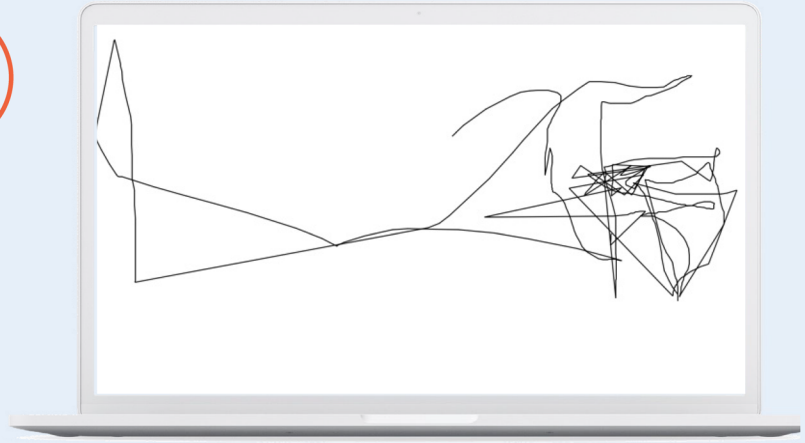
La evolución del malware

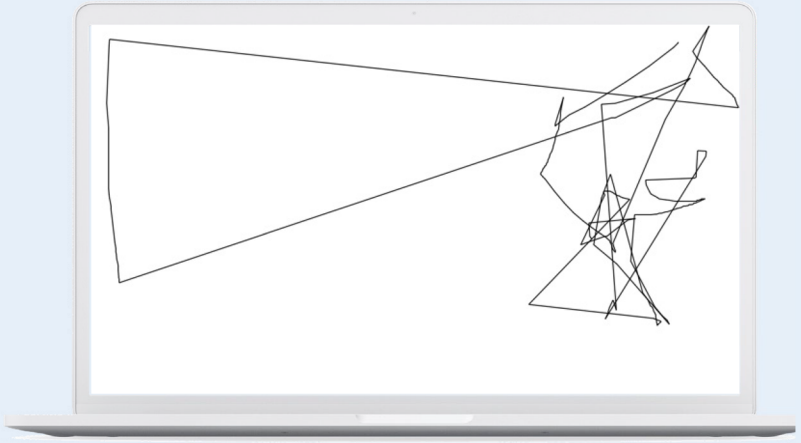
Primera versión del malware (enero)





Segunda versión (mayo/junio)





BioCatch

CASO PRÁCTICO:

La evolución del malware

La detección de casos de malware a través del comportamiento

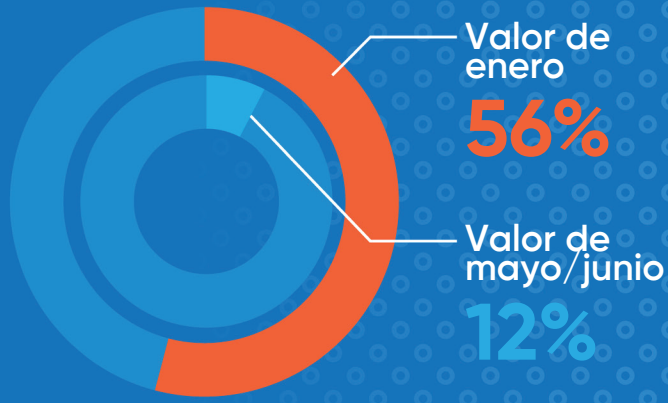
Los ejemplos que se muestran nos permiten ver el comportamiento del ratón a lo largo de cuatro sesiones diferentes que se reportaron como fraude con malware. Los primeros dos ocurrieron en enero, y corresponden al ataque original, mientras que los siguientes dos son de junio, donde observamos un repunte de casos.

Los comportamientos demuestran un cambio en la manera en la que el malware interactúa con las sesiones de banca digital.

Si bien las sesiones de enero muestran un movimiento de ratón de un área de la pantalla a otra de una manera muy robótica, los comportamientos observados en las sesiones de mayo/junio son mucho más humanos (aunque con pequeñas señales de comportamiento de tipo bot).

Este cambio es solo un ejemplo de muchos cambios posibles que pueden sufrir los diferentes malware a medida que evolucionan, lo cual demuestra la importancia de tener unos controles de fraude dinámicos y capaces de seguirle el ritmo a estos cambios. Afortunadamente, el análisis del comportamiento es capaz de proporcionar información de valor incalculable a los bancos, permitiéndoles proteger a sus clientes.

Casos de malware con la función de comportamiento de ratón activada



ACERCA DE BIOCATCH

BioCatch se encuentra en la vanguardia de la detección de fraudes digitales y es pionero en la inteligencia de biometría del comportamiento basada en ciencia cognitiva avanzada y en aprendizaje automático. BioCatch analiza miles de interacciones de usuarios para apoyar un ambiente bancario digital donde coexistan la identidad, la confianza y la facilidad. Hoy en día, más de 32 de los 100 bancos líderes y 210 de todas las instituciones financieras confían en BioCatch Connect™ para combatir el fraude, facilitar la transformación digital y desarrollar las relaciones con los clientes. La Junta de innovación para clientes de BioCatch, una iniciativa dirigida por la industria, con American Express, Barclays, Citi Ventures, HSBC y National Australia Bank, colabora para ser pionera en formas creativas e innovadoras de aprovechar las relaciones con los clientes para la prevención del fraude. Con más de una década de análisis de datos, 92 patentes registradas y una experiencia sin igual, BioCatch continúa siendo el líder en la innovación para abordar desafíos a futuro. Para obtener más información, visite www.biocatch.com.

BioCatch