LexisNexis®
RISK SOLUTIONS

EL NUEVO PANORAMA DEL DELITO CIBERNÉTICO

RIESGOS GLOBALES, TENDENCIAS REGIONALES, OPORTUNIDADES SECTORIALES

Informe de LexisNexis® Risk Solutions sobre el ciberdelito
Julio a diciembre de 2020

01 INTRODUCCIÓN

CONTENIDO

EL CAMBIO GLOBAL SIN PRECEDENTES CREA NUEVAS OPORTUNIDADES PARA LOS CIBERDELINCUENTES

En un año de cambio irreversible, los estafadores mantuvieron la consistencia: buscando nuevas oportunidades, aislando objetivos que ofrezcan las mayores ganancias y ejerciendo presión adicional sobre empresas globales que se vieron forzadas a adaptarse y evolucionar ante una demanda sin precedentes.

Hubo un fuerte foco sobre varias nuevas líneas de crédito. Los estafadores se aprovecharon de la ansiedad del consumidor con fraudes relacionados con la pandemia que ofrecían productos y servicios que estaban en demanda o muy escasos. Pymnts.com, por ejemplo, informó que las tasas de fraude aumentaron 55 % desde el comienzo de la pandemia*, mientras que Experian afirmó que las tasas de fraude en el Reino Unido crecieron 33 % durante el primer confinamiento por Covid-19 en abril**.

Sin embargo, este aumento del fraude no se registró en todos los negocios digitales; muchas plataformas establecidas reportaron un descenso de la cantidad de ataques en 2020. Por ejemplo, las organizaciones que son parte de la LexisNexis® Digital Identity Network® han visto una significativa reducción de las tasas de ataque de año a año. Las defensas contra el fraude bien establecidas y en capas parecen ser un disuasivo importante para los ciberdelincuentes, quienes en cambio prefieren enfocar su atención en nuevas oportunidades creadas por la pandemia global.

A pesar de las bajas tasas de ataque registradas por empresas de la Digital Identity Network®, persisten vectores de ataque nocivos:

- Los ataques de bots automatizados siguen siendo generalizados; se registran en muchas regiones globales y atacan a una amplia gama de sectores con casos de uso que hacen pruebas masivas de credenciales de identidad. Estos ofrecen a los defraudadores un método de ataque inicial barato, rápido y eficaz.
- Del mismo modo, la creación de cuentas nuevas continúa sufriendo altas tasas de ataque, siendo un punto de entrada clave para los defraudadores que buscan monetizar credenciales recolectadas de las vulneraciones de los datos.

La pandemia ha puesto en línea a muchos usuarios adicionales. Nuevos análisis en este informe señalan que los menores de 25 años, son los más vulnerables a los ataques de fraude, mientras que el grupo etario más viejo tiene el riesgo de mayores pérdidas monetarias. Este severo riesgo en ambos extremos del espectro hace que para toda empresa digital global sea altamente prioritaria la necesidad de proteger clientes que están recién llegados a lo digital y son vulnerables.

** https://www.pymnts.com/fraud-prevention/2021/swap-data-analytics-holiday-fraud/*
*** https://www.experianplc.com/media/news/2020/fraud-rate-rises-33-during-covid-19-lockdown/*

EL CAMBIO GLOBAL SIN PRECEDENTES CREA NUEVAS OPORTUNIDADES PARA LOS CIBERDELINCUENTES

Independientemente de la abundante incertidumbre que afrontan las empresas en 2021, pueden estar seguras de que sus usuarios finales seguirán demandando acceso a bienes y servicios dónde y cuándo lo deseen:

- Los vendedores de comercio electrónico, por ejemplo, deben priorizar las experiencias de cliente holísticas y omnicanal. Las vías hacia la compra están convergiendo cada vez más a medida que las experiencias dentro de la tienda están siendo reemplazadas o combinadas con ofrecimientos digitales. El reconocimiento del cliente en toda esta travesía se vuelve más crítico que nunca.
- Asimismo, la diversificación de soluciones de pago digitales que evolucionan para satisfacer la creciente demanda de los consumidores pone el enfoque en métodos de autenticación confiables que puedan detectar la utilización de credenciales robadas y falsificadas.

Dentro de este panorama de cambio rápido, la inteligencia de identidad digital aparece como uno de los activos más preciados, tanto para consumidores como para empresas. Las identidades digitales en línea se pueden adaptar y evolucionar a medida que cada consumidor hace transacciones en línea, y así se construye una huella digital de su comportamiento, historial transaccional e inteligencia de dispositivos.

Cuando esta inteligencia se lleva a un esquema colaborativo [crowdsourcing] con empresas digitales y se actualiza casi en tiempo real, ofrece una vista inigualable de la confianza y el riesgo. Para los consumidores, esto implica una experiencia en línea de baja fricción, ya que las empresas tienen mayor capacidad de reconocer clientes existentes confiables. Al mismo tiempo, las organizaciones pueden identificar comportamientos que se apartan de perfiles confiables. Este enfoque de capas con soluciones de identidad física y autenticación, así como datos de biometría del comportamiento puede ofrecer una estrategia antifraude sólida y preparada para el futuro.

2020: REVISIÓN DEL AÑO

Resumen de transacciones y ataques de enero a diciembre de 2020

El desplazamiento forzoso del consumidor a los canales digitales impulsó un rápido crecimiento de transacciones confiables, con un descenso general de ataques a empresas en la red Digital Identity Network. Las economías en desarrollo tuvieron la mayor porción del crecimiento del volumen de ataques. El análisis que aparece a continuación representa el resumen anual de patrones de transacciones y ataques.

TRANSACCIONES PROCESADAS

47.100 M — **35.500 M** en 2019

Penetración de transacciones móviles:

67 % — **65 %** en 2019

ATAQUES INICIADOS POR HUMANOS

495 M — **679 M** en 2019

Porcentaje de ataques provenientes de un dispositivo móvil

56 % — **55 %** en 2019

Mayor atacante por volumen:

Estados Unidos

Mayor aumento de ataques desde:

1. Guatemala
2. Baréin
3. Zimbabue

ATAQUES DE BOT AUTOMATIZADOS

2.100 M — **2.000 M** en 2019

Mayor atacante por volumen:

Estados Unidos

Mayor aumento de ataques desde:

1. Isla de Man
2. Emiratos Árabes Unidos
3. Nigeria

SUPLANTACIÓN DE IDENTIDAD
Vector de ataque más frecuente

02

EL PANORAMA DEL DELITO CIBERNÉTICO:
JULIO-DICIEMBRE 2020
RIESGOS GLOBALES

ASPECTOS DESTACADOS A NIVEL GLOBAL: JULIO-DICIEMBRE 2020

TRANSACCIONES

+29 % ▲

aumento del volumen de transacciones globales de año a año:

▲ **+29 %**
aumento de transacciones de servicios financieros.

▲ **+38 %**
aumento de transacciones de comercio electrónico.

▲ **+9 %**
aumento de transacciones de medios.

ATAQUES INICIADOS POR HUMANOS

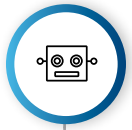
-58 % ▼

descenso en tasa de ataques iniciados por humanos de año a año:

▼ **-58 %**
descenso en tasa de ataques a servicios financieros.

▼ **-58 %**
descenso en tasa de ataques a comercio electrónico.

▼ **-54 %**
descenso en tasa de ataques a medios.



ATAQUES DE BOTS AUTOMATIZADOS

-2 % ▼

descenso en ataques de bots automatizados de año a año:

▼ **-8 %**
descenso de volumen de bots en servicios financieros.

▲ **+32 %**
aumento de volumen de bots en comercio electrónico.

▲ **+10 %**
aumento de volumen de bots en medios.

PATRÓN GLOBAL DE TRANSACCIONES EN CIFRAS

TRANSACCIONES

Covid-19 ha creado nuevas oportunidades para empresas digitales y ha obligado a más consumidores a ponerse en línea

En los últimos 6 meses de 2020, el volumen de transacciones mantuvo un fuerte crecimiento en la red Digital Identity Network, a medida que empresas y consumidores continuaban migrando a ambientes en línea.

Aunque el volumen de creación de cuentas nuevas decreció de año a año, esto fue impulsado más que todo por un volumen extremadamente alto de ataques a la creación de cuentas nuevas en servicios financieros al final de 2019.

Los dispositivos móviles siguen facilitando un amplio acceso a bienes y servicios; casi 7 de cada 10 transacciones provienen de un dispositivo móvil.

Las empresas deberán priorizar progresivamente no solo una estrategia digital primero, sino una estrategia móvil primero para atender a aquellos consumidores que rara vez utilizan, o no tienen acceso a un dispositivo de escritorio.

TRANSACCIONES PROCESADAS JULIO-DICIEMBRE 2020

24.600 M

Aumento de año a año **+29 % ▲**

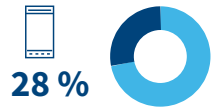
TRANSACCIONES DIVIDIDAS POR CANAL

Escritorio / Móvil

31 % **69 %**

Aumento de año a año **+2 % ▲**

Navegador móvil / Aplicación móvil



28 % **72 %**

TRANSACCIONES DIVIDIDAS POR CASO DE USO*

		Aumento/descenso de año a año
Creación de cuentas nuevas	495 M	-43 % ▼
Inicios de sesión	17.000 M	+26 % ▲
Pagos	4.300 M	+34 % ▲

El volumen de transacciones restante está compuesto de casos de uso no principales, como el restablecimiento de contraseña y el cambio de datos.

PATRÓN GLOBAL DE ATAQUES EN CIFRAS

ATAQUES

El volumen de ataques continúa decreciendo en la red Digital Identity Network®

ATAQUES INICIADOS POR HUMANOS

No obstante los numerosos riesgos de fraude reportados en los medios, las organizaciones de la red Digital Identity Network vieron un descenso en los ataques entre julio y diciembre de 2020.

Las transacciones por navegadores móviles continúan teniendo la tasa más alta de ataques, mientras que las transacciones de aplicaciones móviles tienen la tasa de ataques más baja.

VOLUMEN DE ATAQUES

235 M — Descenso de año a año: **-42 % ▼**

Ataques divididos entre **Escritorio** / **Móvil**

El porcentaje de ataques provenientes de dispositivos móviles ha decrecido de año a año: **-16 % ▼**

TASA DE ATAQUES

		Descenso de año a año
General	1,1 %	-58 % ▼
Escritorio	1,6 %	-41 % ▼
Navegador móvil	2,3 %	-45 % ▼
Aplicación móvil	0,4 %	-79 % ▼

ATAQUES DE BOTS AUTOMATIZADOS

Los sectores de comercio electrónico y medios observaron un aumento de ataques de bots automatizados entre julio y diciembre de 2020.

Aunque las organizaciones de servicios financieros observaron un descenso general en el volumen de bots, el volumen absoluto de ataques dirigidos contra el sector sigue siendo extremadamente alto.

VOLUMEN DE ATAQUES

1.200 M — Descenso de año a año: **-2 % ▼**

		Aumento/ Descenso de año a año
Servicios financieros	812 M	-8 % ▼
Comercio electrónico	207 M	+32 % ▲
Medios	170 M	+10 % ▲

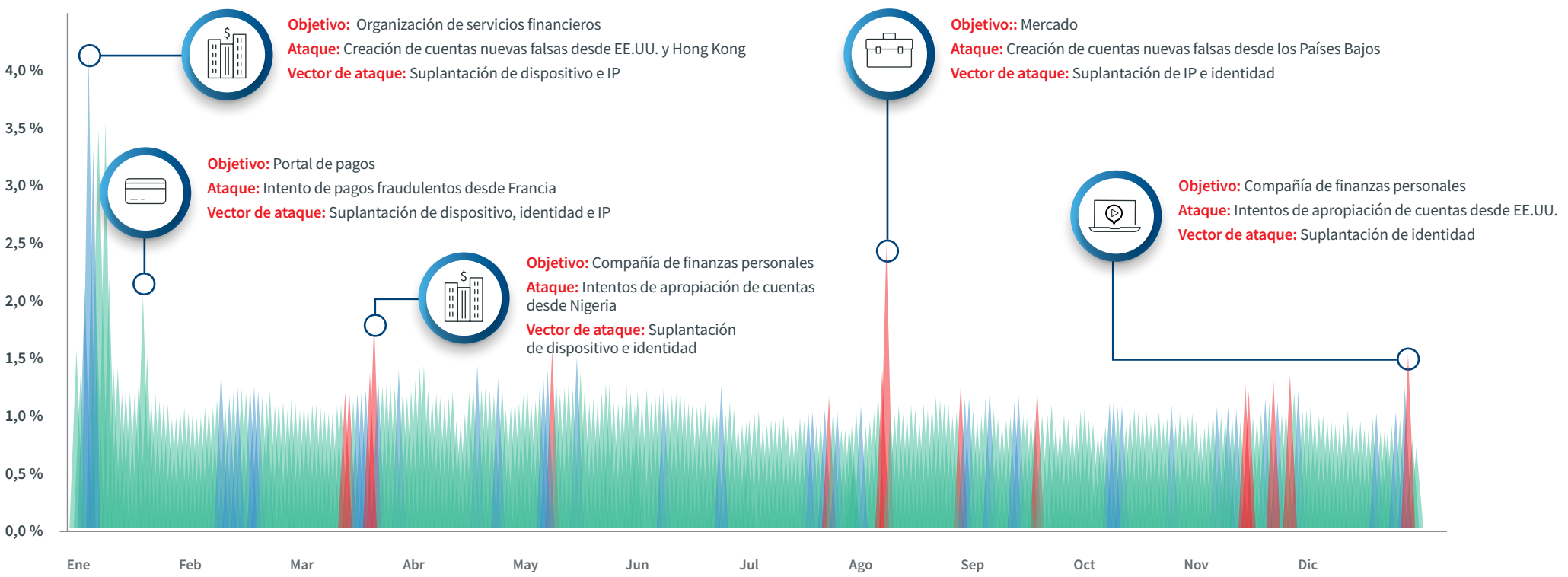
Los ataques en la red Digital Identity Network® se dividen entre ataques iniciados por humanos, que usualmente retornan datos de perfilado digital pleno relacionados con eventos individuales, y ataques de bots automatizados de alta velocidad.

LexisNexis® RISK SOLUTIONS

ÍNDICE DE ABUSO DE IDENTIDAD

Los bots siguen siendo el método preferido para pruebas de identidad en todo el espectro de casos de uso

El LexisNexis® Identity Abuse Index muestra el porcentaje de ataques por día en toda la red Digital Identity Network. Incluye ataques iniciados por humanos y sofisticados ataques de bots.



Un nivel alto del Índice de abuso de identidad (en rojo) representa una tasa de ataque de dos desviaciones estándar de la tendencia de mediano plazo.

LOS MAYORES CONTRIBUYENTES A ATAQUES INICIADOS POR HUMANOS, POR VOLUMEN

Arabia Saudita se une a la lista de los primeros 10 atacantes globales por país de origen

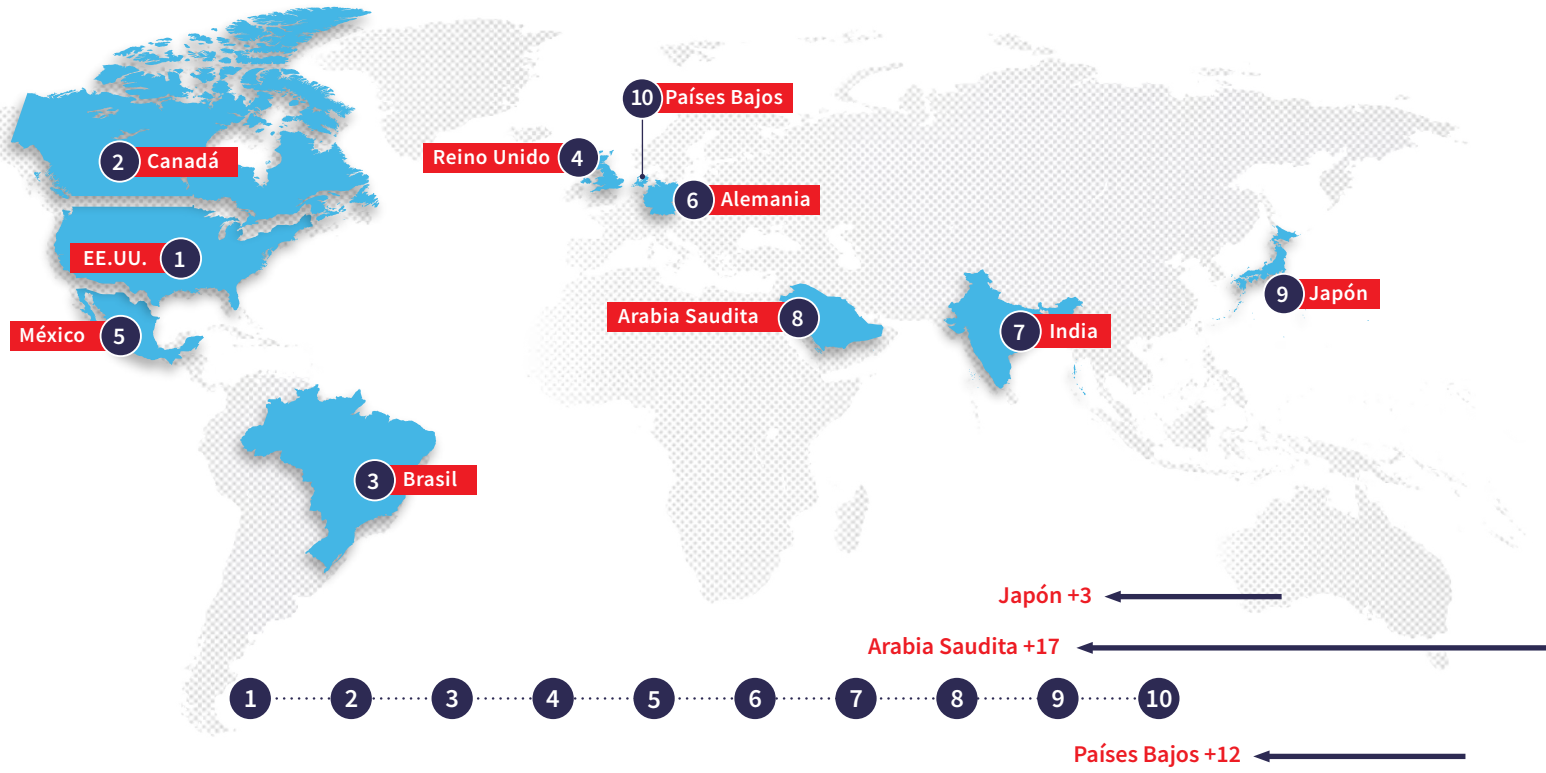
Ataques iniciados por humanos

EE.UU., Canadá y el Reino Unido han sido los atacantes más constantes en la lista de los 5 primeros en años pasados, pero se les siguen uniendo varias economías en desarrollo más pequeñas y nuevas potencias regionales.

Brasil y México siguen estando en la lista de los primeros 5 atacantes por país de origen – México apareció por primera vez en la lista en 2019 – ratificando aún más a LATAM como región que genera un alto volumen de ciberataques.

En comparación al mismo período el año anterior:

- Arabia Saudita subió 17 posiciones en la lista.
- Países Bajos subió 12 posiciones en la lista.
- Japón subió 3 posiciones en la lista.



LOS MAYORES CONTRIBUYENTES A ATAQUES DE BOTS AUTOMATIZADOS, POR VOLUMEN

Irlanda, Australia y Países Bajos todos registran aumentos significativos de originación de ataques de bots de año a año

Ataques de bots automatizados

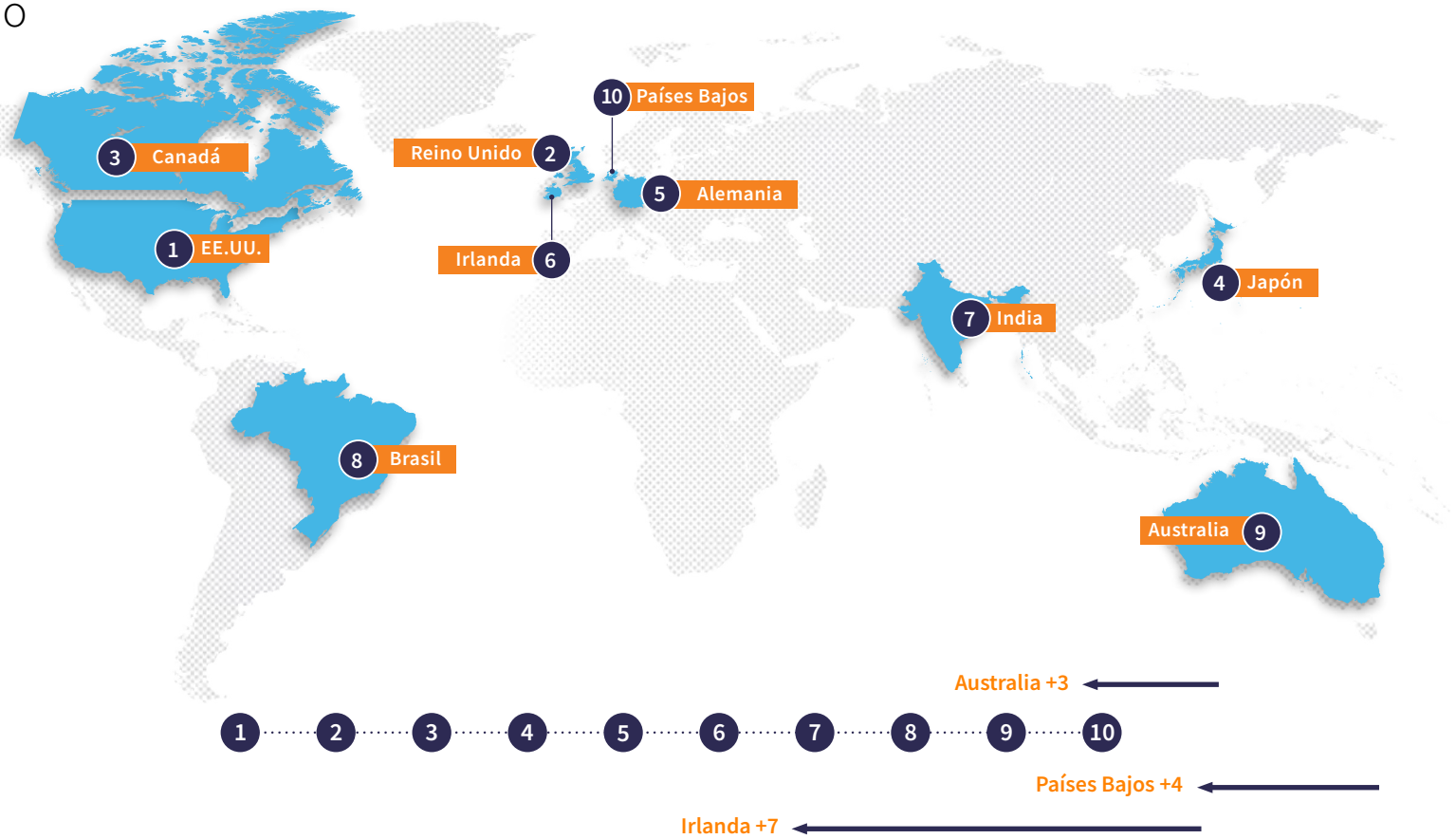
Brasil se une nuevamente a la lista de los primeros 10 originadores de ataques de bots después de haber descendido en el primer semestre de 2020.

El resurgimiento de Brasil como gran originador de ataques de bots significa que las 4 regiones globales están representadas nuevamente en la lista de los primeros 10.

APAC, LATAM y América del Norte registraron un aumento en el volumen de bots entre julio y diciembre de 2020 en comparación al primer semestre del año.

En comparación al mismo período el año anterior:

- Irlanda subió 7 posiciones en la lista.
- Países Bajos subió 4 posiciones en la lista.
- Australia subió 3 posiciones en la lista.



LexisNexis® RISK SOLUTIONS

LOS DEFRAUDADORES EXPLOTAN EL PODER DE LAS REDES PARA FACILITAR LOS ATAQUES

Las redes hiperconectadas siguen teniendo como objetivo a numerosos sectores y organizaciones

La red Digital Identity Network continúa registrando un fuerte patrón de fraude interinstitucional, intersectorial e incluso interregional.

Es probable que cada red esté compuesta de varios grupos de defraudadores que utilizan las mismas listas de datos de identidad robados, los cuales están siendo explotados en regiones y sectores.

Los dispositivos asociados con eventos de fraude confirmados probablemente estén vinculados al mismo individuo o banda de defraudadores, ya que el hardware no se comparte de la misma forma que los datos robados.

El análisis de este informe incluye:

- Los vínculos claves entre dispositivos y datos de identidad robados, entre ellos direcciones de correo electrónico y números telefónicos.
- Volumen de transacciones de redes fraudulentas para ilustrar el tamaño y la escala del comportamiento fraudulento.
- La asignación de valores monetarios a toda la red de fraude con base en valores conocidos de transacciones de pago.

La red Digital Identity Network permite a las organizaciones compartir inteligencia relacionada con eventos de fraude confirmados de tal forma que una entidad denominada de alto riesgo o fraudulenta por una organización puede ser revisada por organizaciones subsiguientes antes de que se procesen más transacciones.

RED GRANDE DE SERVICIOS FINANCIEROS DE NORTEAMÉRICA PRESENTA INDICIOS DE ACTIVIDAD DE MULAS

La visualización de la siguiente página muestra una red de fraude activa enfocada en el sector de servicios financieros que opera en varias instituciones de servicios financieros de EE.UU. y Canadá.

Cada flecha ilustra una entidad asociada con un evento de fraude confirmado en una organización, el cual se pasa a otra organización en la red Digital Identity Network.

Las entidades que forman parte de esta red y fueron analizadas incluyen dispositivos, direcciones de correo electrónico y números telefónicos; sin embargo, hay un fuerte patrón de fraude vinculado con dispositivos, indicando que el mismo defraudador o banda de fraude opera en varios bancos, billeteras digitales e instituciones de crédito.

Este patrón de fraude es típico del comportamiento de mula, ya que los manejadores de mulas mueven dinero a lo largo de múltiples cuentas para evitar detección.

LA RED EN CIFRAS

100.000 +

Eventos relacionados con fraude confirmado que se registró en una organización fuente.

Al menos $1,5 M de dólares

Fraude bloqueado.

500.000 +

Eventos registrados en otras organizaciones de la red Digital Identity Network que estuvieron asociados ya sea con un dispositivo, dirección de correo electrónico y/o número telefónico que estuvo involucrado en estos eventos fraudulentos originales en las organizaciones fuente.

Al menos $8,7 M de dólares

Exposición monetaria al fraude en toda la red. Algunas de estas transacciones pueden haber sido bloqueadas por instituciones de la red que no comparten datos de fraude.

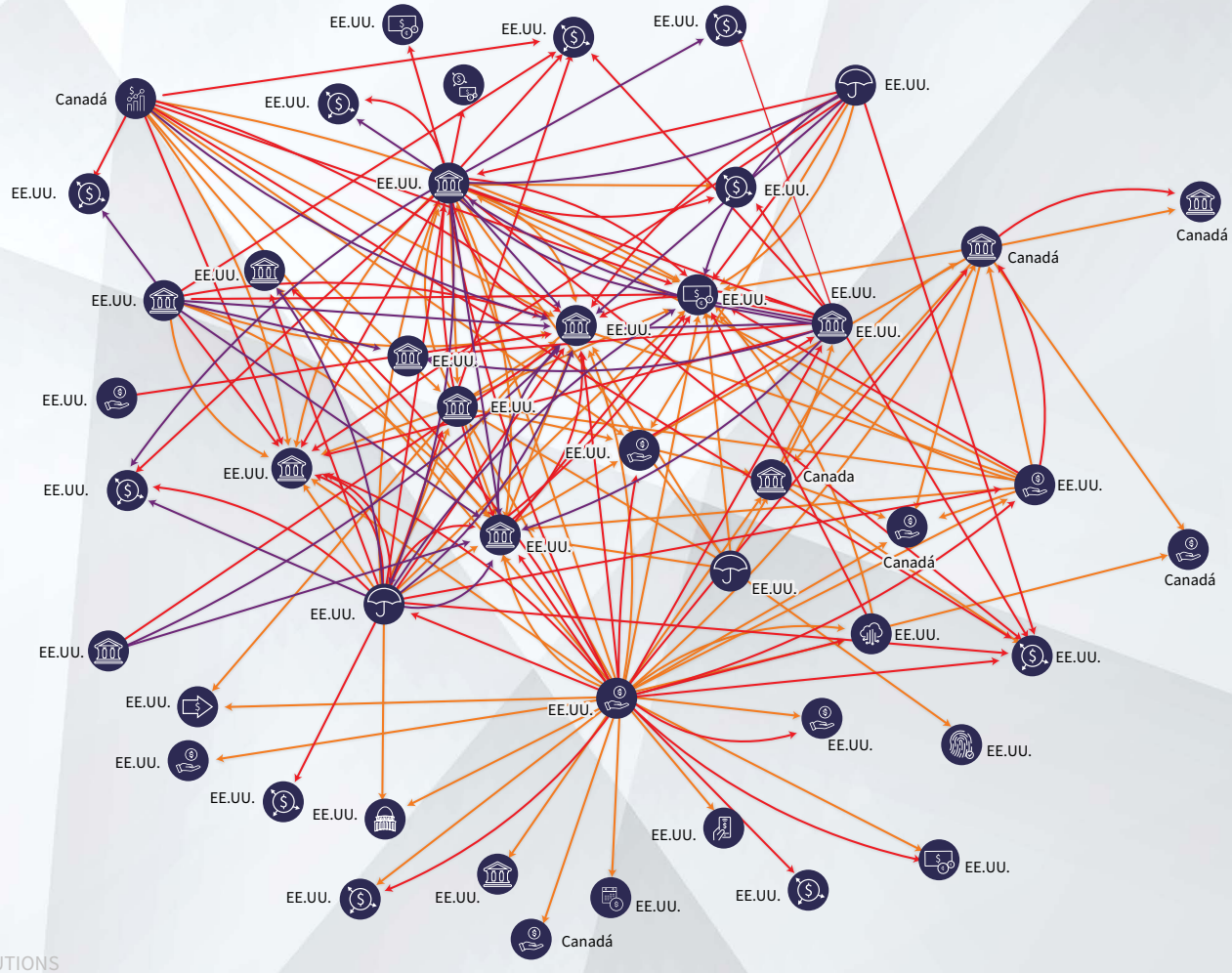
Referirse a la página siguiente para la visualización del fraude

América del Norte incluye EE.UU. y Canadá. México es parte de la región de LATAM.

RED DE FRAUDE NORTEAMERICANA EXHIBE FUERTE PATRÓN DE ENTIDADES DE FRAUDE INTERINSTITUCIONALES

ENTIDADES:

- **DISPOSITIVO**
- **CORREO ELECTRÓNICO**
- **TELÉFONO**



SERVICIOS FINANCIEROS

- PORTAL DE PAGOS
- FINANZAS PERSONALES
- GOBIERNO
- CRÉDITO
- CORREDOR DE BOLSA
- SEGUROS
- BILLETERA DIGITAL
- BANCO
- VERIFICACIÓN DE IDENTIDAD
- REMISIÓN
- NÓMINA

Menos de 100 superposiciones de entidades entre compañías han sido removidas.

América del Norte incluye EE.UU. y Canadá. México es parte de la región de LATAM.

LexisNexis® RISK SOLUTIONS

RED DE FRAUDE DE PAGOS REGISTRADA EN VARIOS MINORISTAS DE COMERCIO ELECTRÓNICO EN EMEA

La visualización de la siguiente página muestra una red de fraude activa enfocada en el sector de comercio electrónico que opera en:

- Minoristas, un mercado y un portal de pagos en Alemania
- Una organización minorista y de viajes en Francia
- Un minorista en Países Bajos
- Un mercado en España
- Un programa de lealtad en Emiratos Árabes Unidos
- Un minorista en Letonia
- Un minorista en Italia

Al igual que la red anterior, cada flecha ilustra una entidad asociada con un evento de fraude confirmado en una organización, el cual se pasa a otra organización en la red Digital Identity Network. Sin embargo, esta red de fraude presenta una mayor proliferación de eventos de fraude conectados mediante direcciones de correo electrónico.

Esto muestra grupos de defraudadores trabajando juntos para atacar varios minoristas utilizando credenciales robadas compartidas.

LA RED EN CIFRAS

2.000 +

Eventos relacionados con fraude confirmado que se registró en una organización fuente.

Al menos $750 mil dólares

Fraude bloqueado.

3.000 +

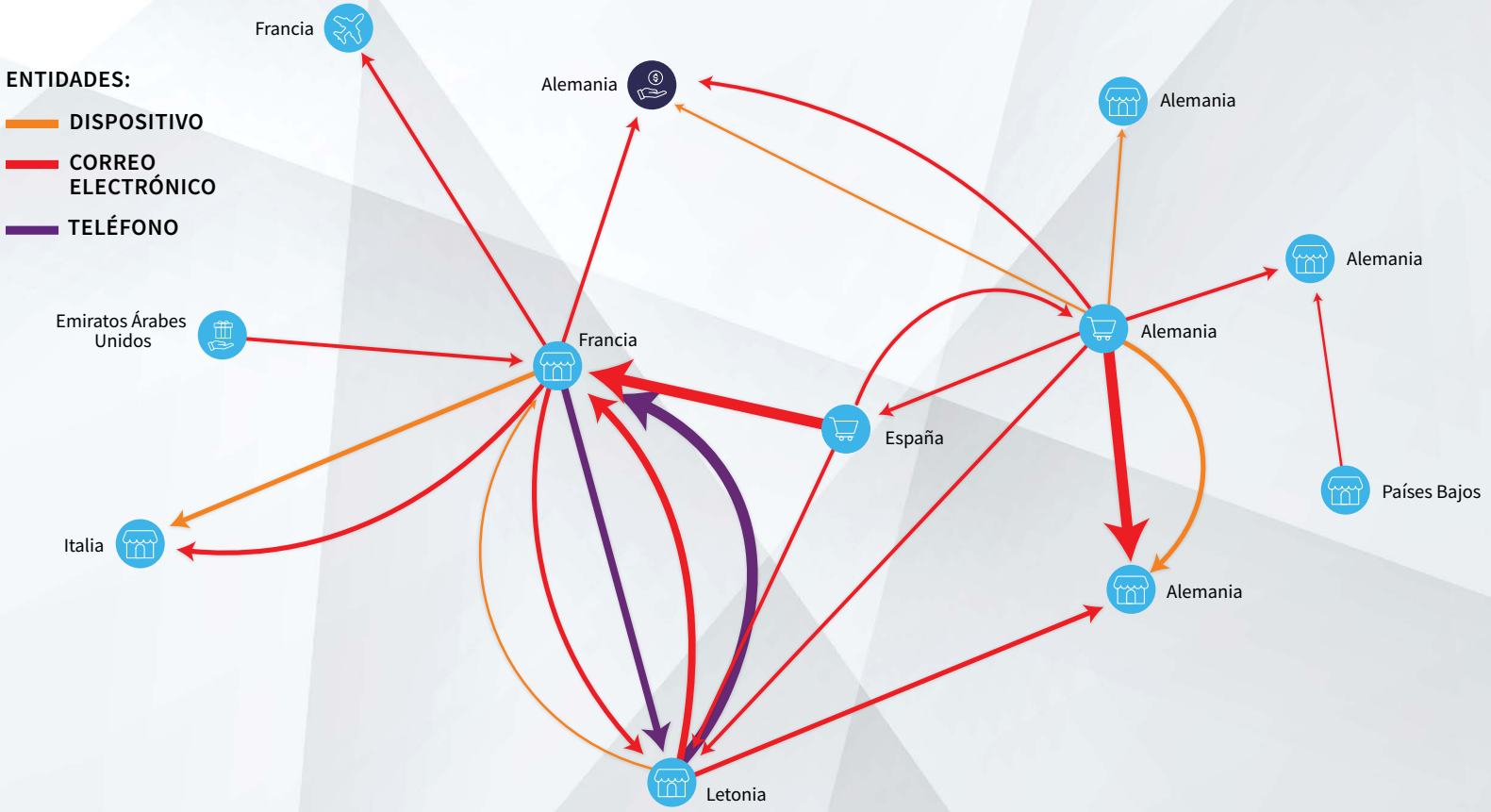
Eventos registrados en otras organizaciones de la red Digital Identity Network que estuvieron asociados ya sea con un dispositivo, dirección de correo electrónico y/o número telefónico que estuvo involucrado en estos eventos fraudulentos originales en las organizaciones fuente.

Al menos $250 mil dólares

Exposición monetaria al fraude en toda la red. Algunas de estas transacciones pueden haber sido bloqueadas por instituciones de la red que no comparten datos de fraude.

Referirse a la página siguiente para la visualización del fraude

CREDENCIALES ROBADAS COMPARTIDAS UTILIZADAS POR CIBERDELINCUENTES PARA APROPIACIÓN DE CUENTAS Y PAGOS FRAUDULENTOS



SERVICIOS FINANCIEROS:
- PORTAL DE PAGOS

COMERCIO ELECTRÓNICO:
- MERCADO
- PROGRAMA DE LEALTAD
- MINORISTA
- VIAJES

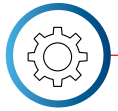
Esta red de fraude solo muestra conexiones de más de 10 entidades. Una línea más gruesa indica un volumen más alto de fraude.

ENFOQUE EN: ANÁLISIS DE IMPACTO DE LA VULNERACIÓN DE DIRECCIONES DE CORREO ELECTRÓNICO EN LA RED DIGITAL IDENTITY NETWORK

FRAUDE:
Ataques de pruebas de identidad en numerosas organizaciones en la red Digital Identity Network utilizando direcciones de correo electrónico aparentemente robadas.

La mayoría de los dominios de correo electrónico son genuinos (gmail. com, hotmail. com, yahoo.com), lo cual indica que estos correos probablemente fueron robados de clientes genuinos en lugar de ser creados artificialmente.

OBJETIVO:
Un operador de juego y apuestas, un minorista y una aerolínea.



MÉTODO:
Alto volumen de ataques de bots probando múltiples direcciones de correo electrónico durante ataques breves y sostenidos.

ATAQUE:

- **Aerolínea** 13.000 intentos de apropiación de cuentas relacionados con 3.200 correos electrónicos robados.
- **Operador de juegos y apuestas** Más de 2.500 intentos de apropiación de cuentas relacionados con 10 correos electrónicos robados que también se vieron en el ataque a la aerolínea.
- **Minorista** 11.150 intentos de apropiación de cuentas relacionados con más de 800 correos electrónicos robados, uno de los cuales también se vio en la aerolínea.
- Los correos electrónicos siguen siendo utilizados por clientes genuinos en otras organizaciones en la red Digital Identity Network.

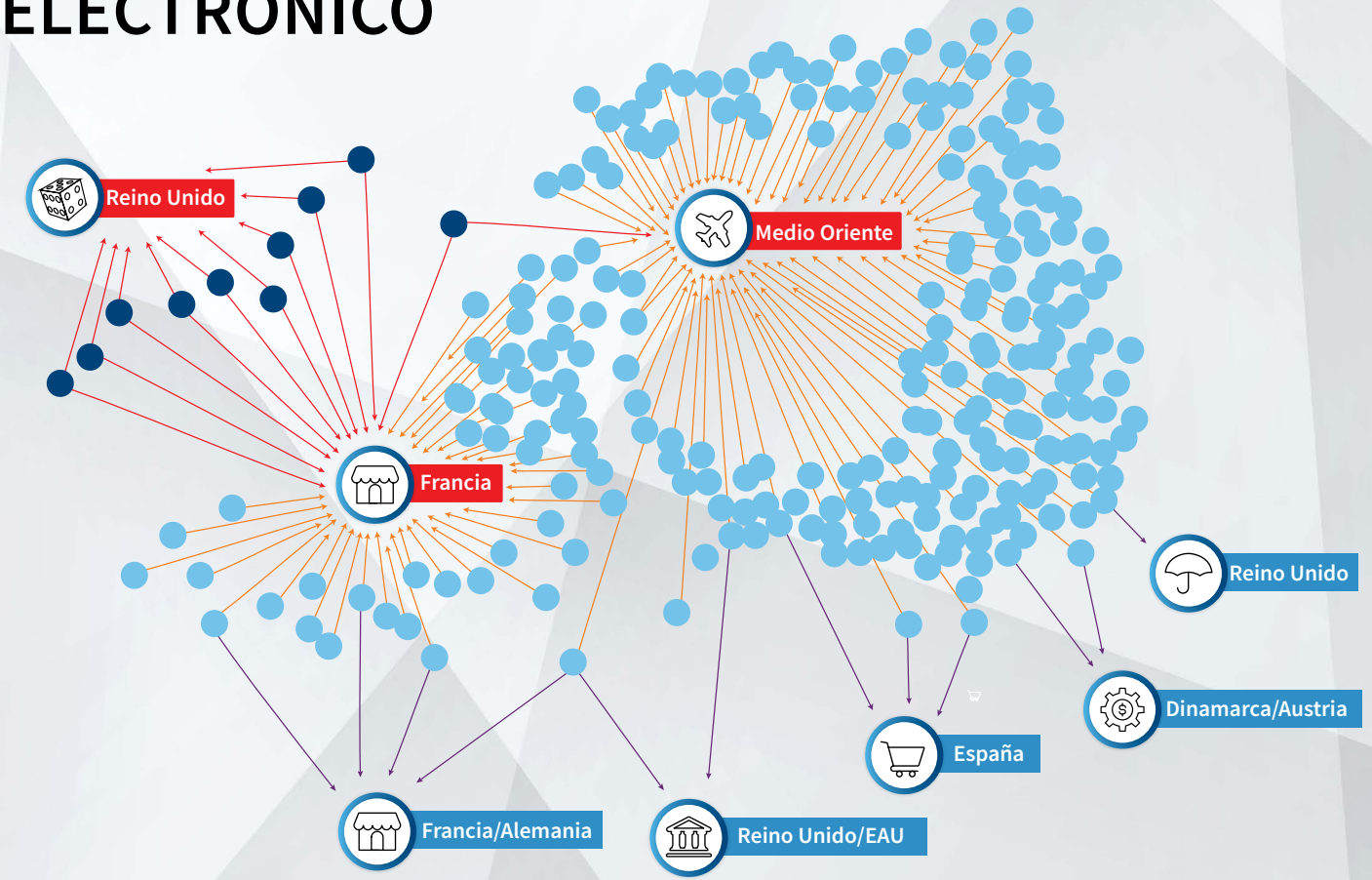
DETECCIÓN:
La evaluación de riesgo de correo electrónico de la red Digital Identity Network distingue entre la utilización legítima y fraudulenta de direcciones de correo electrónico.

LA UTILIZACIÓN DE DIRECCIONES DE CORREO ELECTRÓNICO ROBADAS EN VARIAS ORGANIZACIONES RESALTA LA IMPORTANCIA DE UNA EVALUACIÓN ROBUSTA DEL RIESGO DE CORREO ELECTRÓNICO

Dirección de correo electrónico robada utilizada en ataques en **varias organizaciones**

Dirección de correo electrónico robada utilizada en ataque contra **una organización**

Dirección de correo electrónico **utilizado por cliente genuino en otras organizaciones**



- OPERADOR DE JUEGOS Y APUESTAS
- AEROLÍNEA
- MINORISTA
- BANCO
- MERCADO
- FINTECH
- SEGUROS

LexisNexis® RISK SOLUTIONS

ENFOQUE EN: ANÁLISIS DE ATAQUES DE FRAUDE EN RED RELACIONADOS POR DISTINTAS PIEZAS DE DATOS DE IDENTIDAD DIGITAL

La unión de todos los elementos de datos de la identidad digital revela conexiones de alto riesgo que eran invisibles previamente

Ataque de fraude

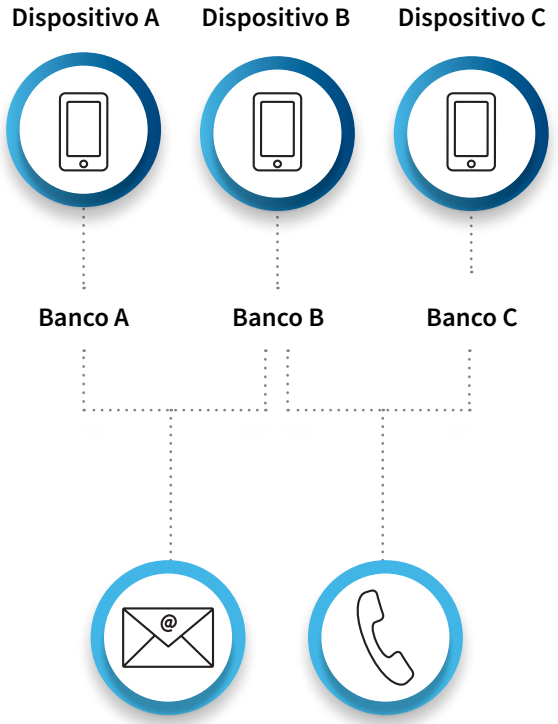
Defraudador utilizando 3 dispositivos diferentes en 3 bancos diferentes.

Tres transacciones fraudulentas no pueden ser relacionadas ya que no hay identificador común.

Inclusión de datos adicionales

Conecta Dispositivo A y Dispositivo B por dirección de correo electrónico.

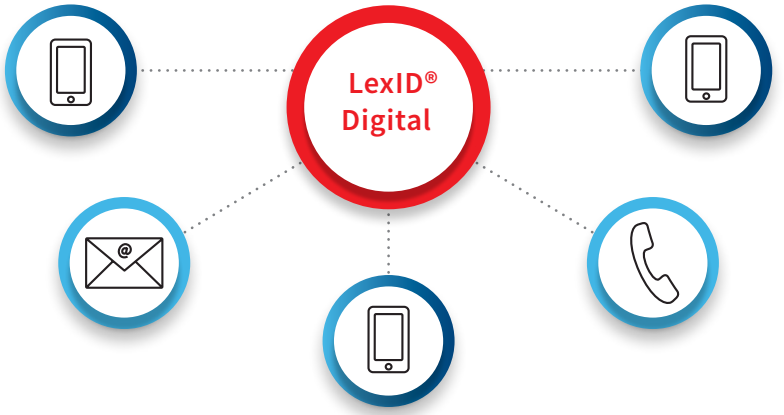
Conecta Dispositivo B y Dispositivo C por número telefónico.



Construcción de esta identidad digital en la red Digital Identity Network

Se puede construir una identidad digital en línea en la red Digital Identity Network conectando las 3 transacciones fraudulentas mediante la dirección de correo electrónico y el número telefónico.

Cuando alguna de estas entidades individuales es vista en una transacción nueva, se puede revisar la historia de la identidad digital en busca de fraude.



03

EL PANORAMA DEL DELITO CIBERNÉTICO:
JULIO-DICIEMBRE 2020

A TRAVÉS DEL RECORRIDO DIGITAL DEL CLIENTE

LO MÁS DESTACADO DEL RECORRIDO DIGITAL DEL CLIENTE: JULIO-DICIEMBRE 2020

CREACIÓN DE CUENTAS NUEVAS

- Tasa de ataque más alta de todos los casos de uso.
- Una de cada 10 transacciones en la red Digital Identity Network es un intento de ataque.

INICIOS DE SESIÓN

- Tasa general de ataques baja.
- Aumento del 9 % en el porcentaje de ataques móviles de año a año.

PAGOS

- Aumento significativo del volumen de transacciones de año a año, ya que los consumidores dependen de métodos de pago digitales más que nunca.
- Mayor volumen de intentos de ataque a transacciones de pago que en cualquier otro caso de uso.

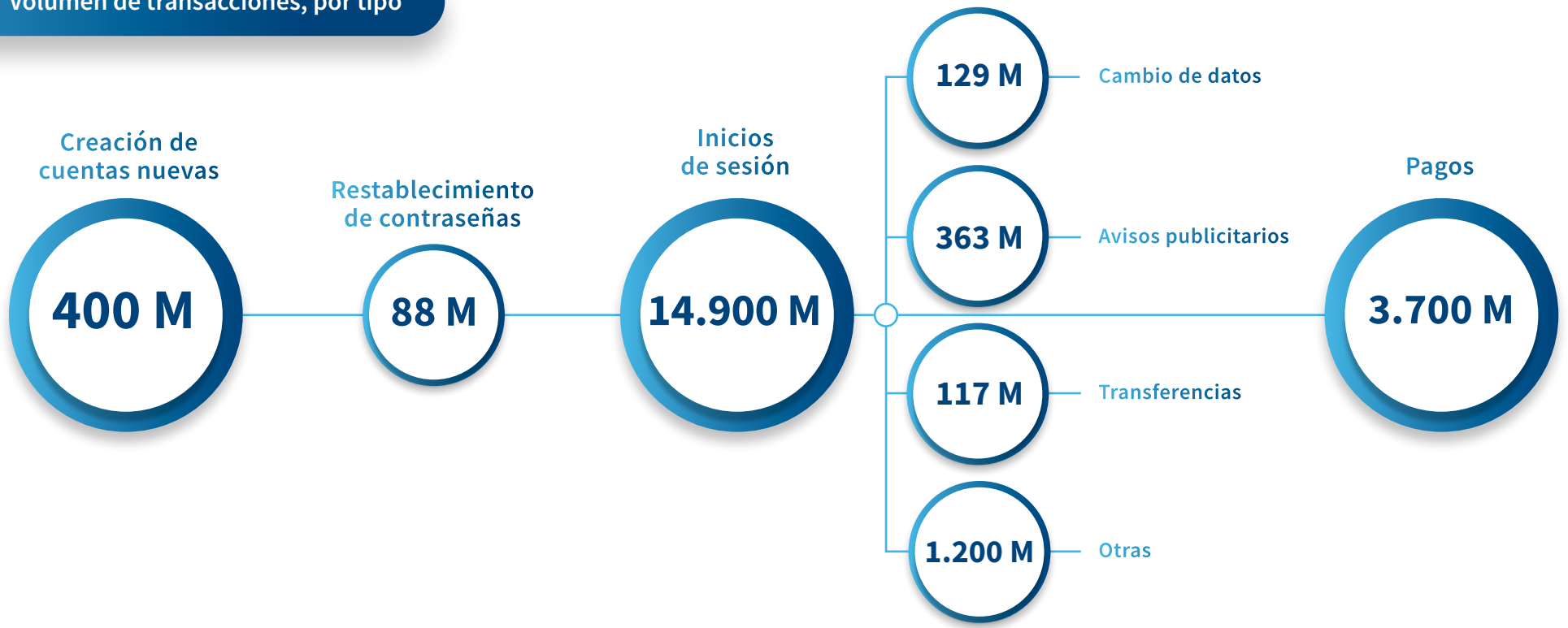
CAMBIO DE DATOS

- De todos los casos de uso no principales, las transacciones de cambio de datos tienen la tasa más alta de ataque: 2,2 %.

VOLUMEN DE TRANSACCIONES POR CASO DE USO A LO LARGO DEL RECORRIDO DIGITAL

Rastreo de todos los puntos de contacto del cliente para mejorar la toma de decisiones sobre riesgo

Volumen de transacciones, por tipo



Otras transacciones incluyen: Registro de dispositivo nuevo, descarga digital, saldo de cuenta, aceptación de préstamo, oferta de subasta y más.

RIESGOS DE ATAQUE EN PUNTOS DE CONTACTO PRINCIPALES

Descenso de todas las tasas de ataque en todos los casos de uso de julio a diciembre de 2020

	CREACIÓN DE CUENTAS NUEVAS	INICIOS DE SESIÓN	PAGOS
TENDENCIAS DE LOS RIESGOS	El volumen de ataques ha decrecido significativamente de año a año. Esto se debe a un inmenso ataque de bots contra la creación de cuentas nuevas en servicios financieros entre diciembre de 2019 y enero de 2020, lo cual aumentó radicalmente los volúmenes de ataques. En comparación, los volúmenes de ataques de S2 2020 son bajos.	Las transacciones de inicio de sesión siguen teniendo tasas generales de ataque bajas debido al alto volumen de transacciones de clientes existentes y confiables. Sin embargo, el número absoluto de ataques es significativo, lo cual ilustra el riesgo potencial para cuentas de usuarios legítimos.	Las transacciones de pago tienen el volumen de ataques más alto de todos los casos de uso, y las transacciones de navegador móvil tienen la mayor tasa de ataque.
VOLUMEN DE ATAQUES	39 M	62 M	108 M
TASA DE ATAQUES			
GENERAL	9,8 %	0,4 %	2,9 %
ESCRITORIO	**13,9 %**	**0,8 %**	3,3 %
NAVEGADOR MÓVIL	9,1 %	0,7 %	**3,4 %**
APLICACIÓN MÓVIL	5,4 %	0,1 %	1,7 %

S2 se refiere al período de julio a diciembre.

RIESGOS DE ATAQUE EN OTROS PUNTOS DE CONTACTO DE ALTO RIESGO

Las transacciones de cambio de datos pueden presentar un antecedente de ataques futuros

	RESTABLECIMIENTO DE CONTRASEÑAS	CAMBIO DE DATOS	AVISOS PUBLICITARIOS	TTRANSFERENCIAS	OTROS
TENDENCIAS DE LOS RIESGOS	El restablecimiento de contraseñas permite a los defraudadores capturar cuentas, utilizando a menudo credenciales robadas. El acceso a la cuenta permite que acciones futuras, tales como pagos, sean iniciadas por el defraudador.	Los cambios a los datos de la cuenta les permiten a los defraudadores modificar información clave de la cuenta. Modificar un número telefónico, por ejemplo, significa que eventos subsiguientes tales como las verificaciones de autenticación de una clave de acceso SMS de uso único (OTP, por su sigla en inglés) son envidas al defraudador. Los ataques grandes dirigidos contra transacciones de cambio de datos en servicios financieros contribuyeron a la alta tasa de ataques a aplicaciones móviles durante este período.	Los avisos publicitarios permiten a los defraudadores controlar la venta o promoción de bienes y servicios. De esta forma se tiene una manera de monetizar bienes robados, al publicar avisos falsos de propiedades o servicios o crear reseñas mentirosas para facilitar ventas.	Las transferencias permiten el movimiento de dinero a otra cuenta dentro del perfil general de un cliente. Esta acción a veces precede a un evento de pago fraudulento después de la apropiación de una cuenta.	Están incluidos otros varios puntos de contacto de alto riesgo tales como el registro de nuevos canales, órdenes bancarias, débitos directos y modificación de beneficiarios.
VOLUMEN DE ATAQUES	0,7 M	2,9 M	1,8 M	1,1 M	19,3 M
TASA DE ATAQUES					
GENERAL	0,8 %	2,2 %	0,5 %	0,9 %	1,6 %
ESCRITORIO	**0,9 %**	1,2 %	0,5 %	**1,8 %**	**2,2 %**
NAVEGADOR MÓVIL	**0,9 %**	1,3 %	**1,5 %**	1,2 %	1,2 %
APLICACIÓN MÓVIL	0,2 %	**3,8 %**	0,4 %	0,6 %	1,2 %

04

EL PANORAMA DEL DELITO CIBERNÉTICO:
JULIO-DICIEMBRE 2020
TENDENCIAS REGIONALES

ASPECTOS DESTACADOS A NIVEL REGIONAL: JULIO-DICIEMBRE 2020

APAC

+24 %
aumento del volumen de transacciones de año a año.

-42 %
descenso en ataques iniciados por humanos de año a año.

-2 %
descenso en volumen de bots de año a año.

EMEA

+23 %
aumento del volumen de transacciones de año a año.

-54 %
descenso en ataques iniciados por humanos de año a año.

-6 %
descenso en volumen de bots de año a año.

LATAM

+18 %
aumento del volumen de transacciones de año a año con un aumento de 16 % en la penetración de transacciones móviles – la mayor de todas las regiones.

-26 %
descenso en ataques iniciados por humanos de año a año.

-20 %
descenso en volumen de bots de año a año.

NORTEAMÉRICA

+37 %
aumento del volumen de transacciones de año a año.

-37 %
descenso en ataques iniciados por humanos de año a año.

+1 %
aumento de bots de año a año.

América del Norte incluye EE.UU. y Canadá. México está incluido en el análisis regional de LATAM.

ÍNDICE DE ABUSO DE IDENTIDAD POR REGIÓN

LATAM y APAC experimentan las tasas de ataques más volátiles

APAC EMEA LATAM **AMÉRICA DEL NORTE**

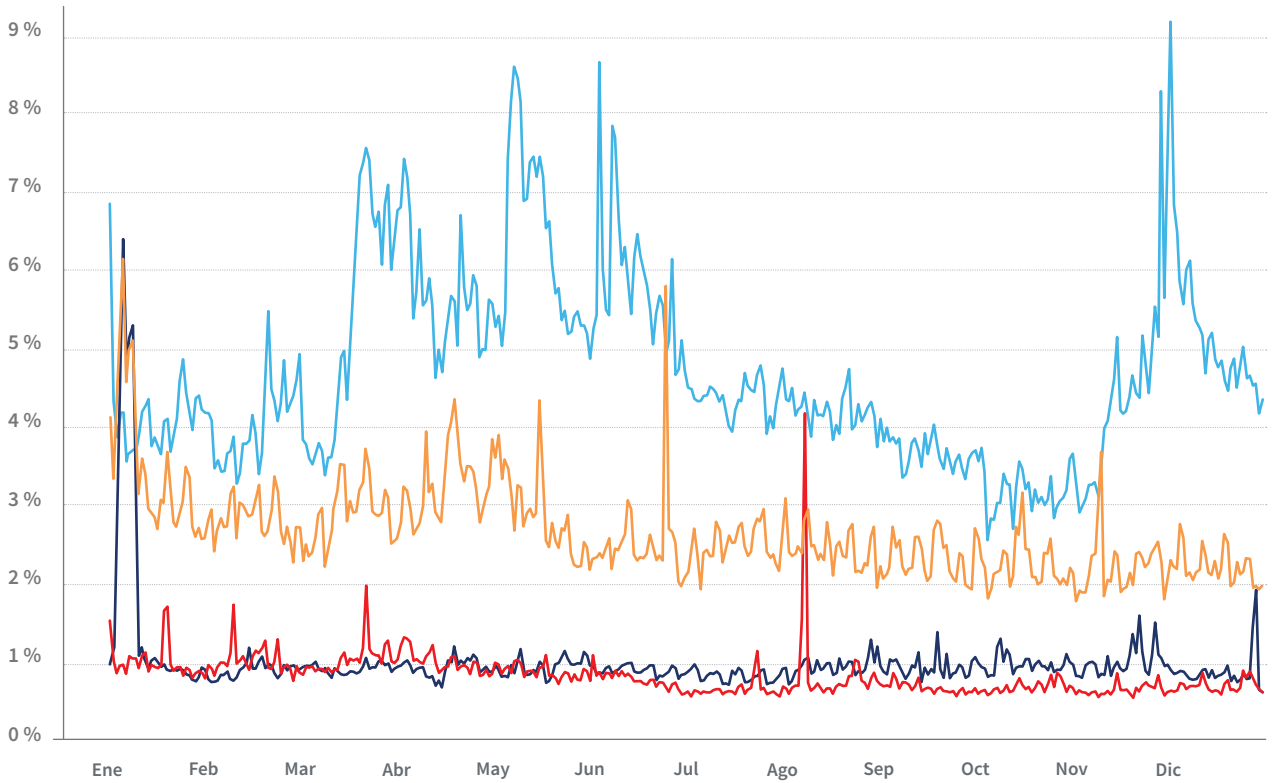
LATAM sigue registrando las tasas de ataques diarios más altas de todas las regiones, presentando varios picos de ataques a lo largo del año.

Un ataque grande a servicios financieros en diciembre incrementó la tasa general de ataques al 9 % de todas las transacciones diarias.

APAC registra una tendencia decreciente constante en las tasas de ataques diarios de la segunda mitad de 2020, a pesar de alguna actividad significativa de bots en noviembre, que se originó en la India e iba dirigida a la apropiación de cuentas de un minorista norteamericano.

América del Norte y **EMEA** continúan registrando tasas generales de ataque más bajas a lo largo del tiempo en comparación con otras regiones globales.

No obstante, hubo un ataque grande de bots en agosto, dirigido contra un mercado en línea y originado en los Países Bajos, lo cual hizo que la tasa general de ataques aumentara a más del 4 % de todas las transacciones en EMEA.



PATRONES DE TRANSACCIONES Y ATAQUES EN APAC

APAC

PRIMEROS 5 ATACANTES

1. India
2. Japón
3. Bangladesh
4. Filipinas
5. Malasia

PRIMEROS 5 DESTINOS DE ATAQUES

1. EE.UU.
2. Reino Unido
3. Australia
4. Japón
5. Malasia

TRANSACCIONES

TRANSACCIONES PROCESADAS

1.700 M

Aumento de año a año
+24 % ▲

TRANSACCIONES DIVIDIDAS POR CANAL

Escritorio / **Móvil**

Navegador móvil / **Aplicación móvil**

ATAQUES

VOLUMEN DE ATAQUES INICIADOS POR HUMANOS

33 M

Descenso de año a año
-42 % ▼

VOLUMEN DE ATAQUES DE BOTS AUTOMATIZADOS

142 M

Descenso de año a año
-2 % ▼

ATAQUES DIVIDIDOS POR CANAL

Escritorio / **Móvil**

El porcentaje de ataques provenientes de dispositivos móviles ha **decrecido de año a año**

-15 % ▼

POSICIÓN DE APAC CONTRA CIFRAS GLOBALES

APAC

APAC observa tasas de ataque más altas en todos los canales en comparación con cifras globales

	GLOBAL	APAC
TASA DE ATAQUES GENERAL	1,1 %	2,3 %
TASA DE ATAQUES CONTRA ESCRITORIO	1,6 %	2,8 %
TASA DE ATAQUES CONTRA NAVEGADOR MÓVIL	2,3 %	3,0 %
TASA DE ATAQUES CONTRA APLICACIÓN MÓVIL	0,4 %	1,3 %

Las tasas de ataque en APAC siguen siendo más altas que los promedios globales, aunque continúan cayendo en todos los canales de año a año.

La región de APAC sigue siendo un gran contribuyente de ataques de bots globales, y Japón, India y Australia aparecen en la lista de principales originadores de bots a nivel global.

El volumen de ataques de bots automatizados que se origina en la región de APAC es en gran medida constante de año a año.

PATRONES DE TRANSACCIONES Y ATAQUES EN EMEA

EMEA

PRIMEROS 5 ATACANTES

1. Reino Unido
2. Alemania
3. Arabia Saudita
4. Países Bajos
5. Rusia

PRIMEROS 5 DESTINOS DE ATAQUES

1. EE.UU.
2. Reino Unido
3. Canadá
4. Rusia
5. Suecia

TRANSACCIONES

TRANSACCIONES PROCESADAS

8.700 M

Aumento de año a año
+23 % ▲

TRANSACCIONES DIVIDIDAS POR CANAL

Escritorio / Móvil

Navegador móvil / Aplicación móvil

ATAQUES

VOLUMEN DE ATAQUES INICIADOS POR HUMANOS

60 M

Descenso de año a año
-54 % ▼

VOLUMEN DE ATAQUES DE BOTS AUTOMATIZADOS

256 M

Descenso de año a año
-6 % ▼

ATAQUES DIVIDIDOS POR CANAL

Escritorio / Móvil

El porcentaje de ataques provenientes de dispositivos móviles ha **decrecido de año a año**

-13 % ▼

POSICIÓN DE EMEA CONTRA CIFRAS GLOBALES

EMEA

EMEA tiene la penetración más alta de transacciones en aplicaciones móviles de cualquier región global

	GLOBAL	EMEA
TASA DE ATAQUES GENERAL	1,1 %	0,8 %
TASA DE ATAQUES CONTRA ESCRITORIO	1,6 %	1,4 %
TASA DE ATAQUES CONTRA NAVEGADOR MÓVIL	2,3 %	1,8 %
TASA DE ATAQUES CONTRA APLICACIÓN MÓVIL	0,4 %	0,2 %

EMEA continúa observando tasas generales de ataques que son bajas en comparación con los promedios globales y son impulsadas por un alto volumen de transacciones de aplicaciones móviles confiables.

En comparación con otras regiones, la región tuvo la reducción más grande en la tasa de ataques iniciados por humanos.

Sin embargo, a pesar de esto, varios países de EMEA aparecen en las listas de los mayores contribuyentes de ataques, tanto los iniciados por humanos como de bots, por volumen.

PATRONES DE TRANSACCIONES Y ATAQUES EN LATAM

LATAM

PRIMEROS 5 ATACANTES

1. Brasil
2. México
3. Argentina
4. Colombia
5. Perú

PRIMEROS 5 DESTINOS DE ATAQUES

1. EE.UU.
2. Brasil
3. Reino Unido
4. Chile
5. México

TRANSACCIONES

TRANSACCIONES PROCESADAS

875 M

Aumento de año a año
+18 % ▲

TRANSACCIONES DIVIDIDAS POR CANAL

Escritorio / Móvil

Navegador móvil / Aplicación móvil

ATAQUES

VOLUMEN DE ATAQUES INICIADOS POR HUMANOS

33 M

Descenso de año a año
-26 % ▼

VOLUMEN DE ATAQUES DE BOTS AUTOMATIZADOS

44 M

Descenso de año a año
-20 % ▼

ATAQUES DIVIDIDOS POR CANAL

Escritorio / Móvil

El porcentaje de ataques provenientes de dispositivos móviles ha **aumentado de año a año**

+2 % ▲

POSICIÓN DE LATAM CONTRA CIFRAS GLOBALES

LATAM

Tasas de ataque en todos los canales más altas que las de cualquier otra región global

GLOBAL **LATAM**

Aunque las tasas generales de ataques en LATAM han descendido de año a año, siguen siendo las más altas de todas las regiones a nivel global, especialmente para transacciones de aplicaciones móviles.

El volumen de bots automatizados también se redujo en 20 % de año a año. Brasil es el único país de LATAM que aparece en la lista de mayores originadores de bots.

El porcentaje de transacciones móviles en LATAM ha aumentado 16 % de año a año, lo cual sugiere que posiblemente los móviles están facilitando la inclusión financiera en la región. LATAM ya alcanzó a EMEA como la región con la penetración más alta de transacciones móviles: casi 4 de cada 5 transacciones provienen de un dispositivo móvil.

PATRONES DE TRANSACCIONES Y ATAQUES EN AMÉRICA DEL NORTE

AMÉRICA DEL NORTE

PRINCIPALES ATACANTES

1. EE.UU.
2. Canadá

PRIMEROS 5 DESTINOS DE LOS ATAQUES

1. EE.UU.
2. Canadá
3. Australia
4. Reino Unido
5. Brasil

TRANSACCIONES

TRANSACCIONES PROCESADAS

12.600 M

Aumento de año a año
+37 % ▲

TRANSACCIONES DIVIDIDAS POR CANAL

Escritorio / **Móvil**

37 %

63 %

Navegador móvil / **Aplicación móvil**

30 %

70 %

ATAQUES

VOLUMEN DE ATAQUES INICIADOS POR HUMANOS

105 M

Descenso de año a año
-37 % ▼

VOLUMEN DE ATAQUES DE BOTS AUTOMATIZADOS

747 M

Aumento de año a año
+1 % ▲

ATAQUES DIVIDIDOS POR CANAL

Escritorio / **Móvil**

48 %

52 %

El porcentaje de ataques provenientes de dispositivos móviles ha **decrecido de año a año**

-24 % ▼

América del Norte incluye EE.UU. y Canadá. México está incluido en el análisis regional de LATAM.

POSICIÓN DE AMÉRICA DEL NORTE CONTRA CIFRAS GLOBALES

AMÉRICA DEL NORTE

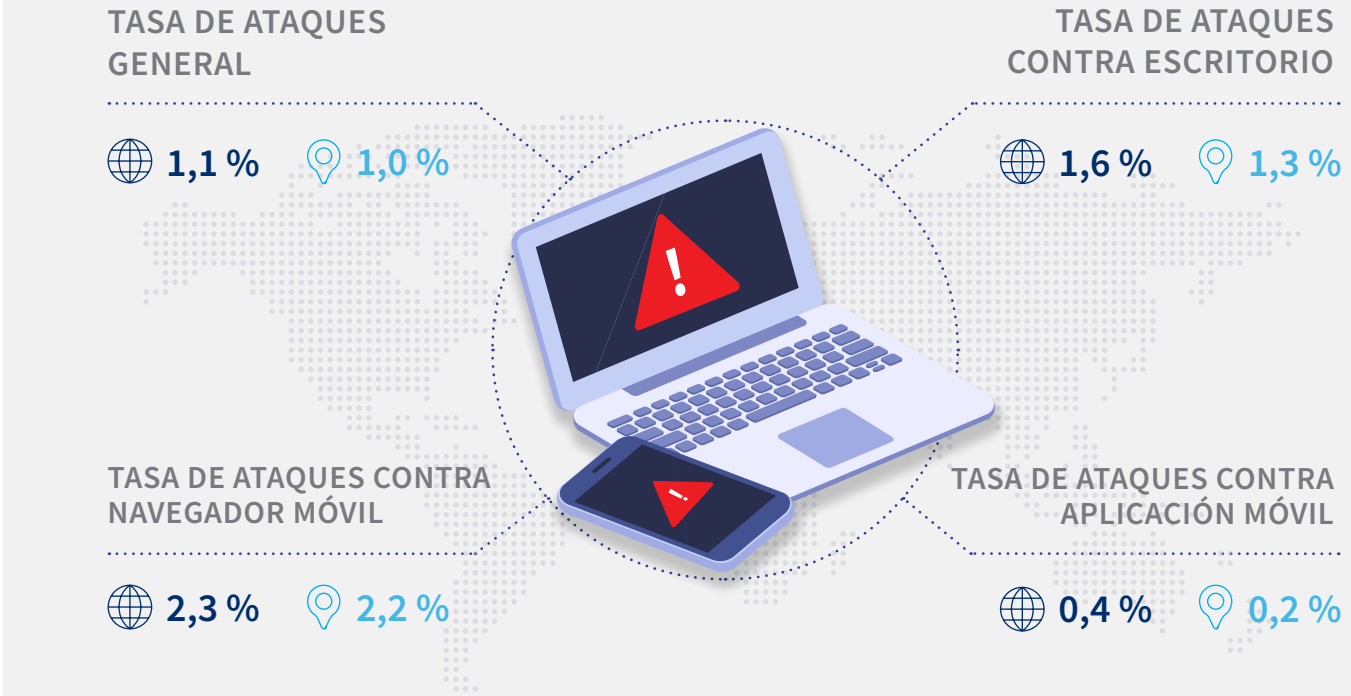
Gran aumento de volumen de bots automatizados entre julio y diciembre de 2020

GLOBAL **AMÉRICA DEL NORTE**

América del Norte continúa sufriendo tasas generales de ataques que son bajas en comparación con los promedios globales, siguiendo así un patrón similar al de la región de EMEA.

La tasa de ataques iniciados por humanos también ha decrecido en esta región, mientras que el volumen de ataques de bots se ha mantenido constante en gran medida, registrando un aumento del 1 % de año a año.

No obstante, EE.UU. es el primer originador de ataques iniciados por humanos y de bots, mientras que Canadá aparece constantemente entre los primeros 3.



05

EL PANORAMA DEL DELITO CIBERNÉTICO:

JULIO-DICIEMBRE 2020

OPORTUNIDADES SECTORIALES

ASPECTOS DESTACADOS DEL SECTOR: JULIO-DICIEMBRE 2020

SERVICIOS FINANCIEROS

- Bajas tasas generales de ataque, impulsadas por un alto volumen de transacciones reiteradas de inicio de sesión de clientes confiables.
- La excepción son las transacciones de pago, que tienen una tasa de ataques más alta que en cualquier otro sector y constituyen una oportunidad clave para que los defraudadores liquiden ganancias.
- Hay un aumento de ataques dirigidos contra la creación de cuentas nuevas desde dispositivos de escritorio y navegadores móviles.

COMERCIO ELECTRÓNICO

- Comercio electrónico observó el mayor aumento de volumen de bots en comparación con otros sectores, a pesar de las tasas decrecientes de ataques iniciados por humanos.
- La tasa de ataques a pagos de comercio electrónico hechos desde una aplicación móvil es mayor que la de cualquier otro sector, lo cual representa un punto de riesgo en potencia.

MEDIOS

- La creación de cuentas nuevas tiene una tasa de ataques mayor que la de cualquier otro sector, con defraudadores que utilizan organizaciones de medios para probar datos de identidad robados.
- Hay un aumento en las tasas de ataques contra la creación de cuentas nuevas desde dispositivos de escritorio y navegadores móviles, y también contra las transacciones de inicio de sesión desde navegadores y aplicaciones móviles.

VISIÓN GENERAL DE LA INDUSTRIA: TENDENCIAS Y PATRONES DE ATAQUES

El sector de medios sufre las tasas de ataque más altas en todos los casos de uso, mientras que las transacciones de escritorio son las más atacadas de todos los canals

VISIÓN GENERAL DE LA INDUSTRIA	RESUMEN POR SECTORES	SERVICIOS FINANCIEROS	COMERCIO ELECTRÓNICO	MEDIOS
TENDENCIAS DE LOS RIESGOS	Las transacciones de escritorio tienen la mayor tasa de ataque de todos los canales.	No obstante, el alto volumen de ataques, las tasas generales de ataques son las más bajas de todos los sectores, debido al alto volumen de transacciones repetidas confiables.	La tasa de ataques a aplicaciones móviles (subconjunto de la tasa de ataque a móviles) para transacciones de pago es mayor para vendedores de comercio electrónico que en cualquier otro sector.	La creación de cuentas nuevas constituye el riesgo más grande en el recorrido del cliente de medios, tanto en volumen como en tasas de ataques.
VOLUMEN DE ATAQUES	235 M	123 M	65 M	46 M
TASA DE ATAQUES				
GENERAL	1,1 %	0,8 %	1,4 %	**4,5 %**
ESCRITORIO	**1,6 %**	**1,3 %**	**1,8 %**	**4,2 %**
MÓVIL	0,9 %	0,7 %	1,1 %	**4,7 %**

SERVICIOS FINANCIEROS: VISIÓN GENERAL DE TENDENCIAS Y PATRONES DE ATAQUES

Las transacciones de pagos en servicios financieros registran la tasa de ataques más grande de todos los sectores

RESUMEN DE SERVICIOS FINANCIEROS	CREACIÓN DE CUENTAS NUEVAS	INICIOS DE SESIÓN	PAGOS
TENDENCIAS DE LOS RIESGOS	Descenso significativo en tasas de volumen de ataques y ataques a aplicaciones móviles debido a un ataque grande de bots contra la creación de cuentas nuevas en aplicaciones móviles entre diciembre de 2019 y enero de 2020, lo cual llevó a un inmenso pico en los ataques durante este período. Sin embargo, se registró aumento de tasas de ataques en transacciones de escritorio y navegador móvil.	La tasa general de ataques contra transacciones de inicio de sesión sigue siendo baja debido al alto volumen de transacciones normales de clientes confiables. Sin embargo, los 36 millones de intentos de apropiación de cuentas constituyen un riesgo significativo para las cuentas de cliente legítimas. Las transacciones desde dispositivos de escritorio y navegadores móviles tienen la mayor tasa de ataques a pesar de que las tasas de ataques descendieron de año a año.	Así como el volumen de transacciones de pago ha aumentado de año a año, también el volumen de ataques. No obstante, el aumento del volumen de ataques fue menos pronunciado que el del volumen de transacciones, lo cual lleva a una reducción general de las tasas de ataque.
VOLUMEN DE ATAQUES	5 M (94 M)	36 M (48 M)	69 M (58 M)
TASA DE ATAQUES			
GENERAL	4,1 % (18,3 %)	0,3 % (0,5 %)	3,6 % (4,5 %)
ESCRITORIO	**7,1 %** (5,0 %)	**0,7 % (1,2 %)**	4,1 % (4,2 %)
NAVEGADOR MÓVIL	3,4 % (3,1 %)	**0,7 %** (1,0 %)	**4,9 % (6,3 %)**
APLICACIÓN MÓVIL	2,3 % **(20,8 %)**	0,1 % (0,2 %)	1,0 % (2,2 %)

Las cifras en paréntesis son del segundo semestre de 2019

COMERCIO ELECTRÓNICO: VISIÓN GENERAL DE TENDENCIAS Y PATRONES DE ATAQUES

Reducción general de las tasas de ataque con énfasis en un aumento de 32 % en el volumen de bots de año a año

RESUMEN DE COMERCIO ELECTRÓNICO	CREACIÓN DE CUENTAS NUEVAS	INICIOS DE SESIÓN	PAGOS
TENDENCIAS DE LOS RIESGOS	La creación de cuentas nuevas desde el escritorio tiene la más alta tasa de ataques de todos los casos de uso, con más de 1 de cada 10 transacciones identificadas como un ataque en potencia. No obstante, las tasas de ataque se están reduciendo en todos los canales.	Aunque los vendedores de comercio electrónico tienen una tasa de intentos de apropiación de cuentas más alta en comparación con servicios financieros, las tasas generales de ataques siguen siendo relativamente bajas y están decreciendo en todos los canales de año a año.	Las transacciones de pago en el recorrido del cliente por el comercio electrónico constituyen una significativa oportunidad para que los defraudadores liquiden ganancias y moneticen credenciales robadas. Aunque las tasas de ataques están decreciendo en todos los canales, la tasa de ataques a aplicaciones móviles es mayor para vendedores de comercio electrónico que en cualquier otro sector.
VOLUMEN DE ATAQUES	6 M (8 M)	19 M (49 M)	36 M (44 M)
TASA DE ATAQUES			
OVERALL	5,2 % (11,3 %)	1,0 % (3,4 %)	2,3 % (3,8 %)
ESCRITORIO	**10,7 % (25,9 %)**	**1,3 %** (3,3 %)	**2,7 % (4,7 %)**
TASA DE ATAQUES	2,7 % (4,5 %)	0,8 % (2,9 %)	1,6 % (2,9 %)
APLICACIÓN MÓVIL	1,3 % (4,0 %)	0,2 % **(4,3 %)**	**2,7 %** (3,8 %)

Las cifras en paréntesis son del segundo semestre de 2019

MEDIOS: VISIÓN GENERAL DE TENDENCIAS Y PATRONES DE ATAQUES

La creación de cuentas nuevas en medios registra tasas de ataque significativamente mayores a las de cualquier otro sector

RESUMEN DE MEDIOS	CREACIÓN DE CUENTAS NUEVAS	INICIOS DE SESIÓN	PAGOS
TENDENCIAS DE LOS RIESGOS	Cerca de 1 en cada 6 transacciones de creación de cuenta nueva es un ataque en potencia, con aumento de tasas de ataque registrados en escritorio y navegador móvil. Es probable que muchos de estos intentos de creación de cuentas nuevas vengan de defraudadores haciendo prueba de datos de identidad robados en compañías que usualmente tienen barreras de entrada más bajas. Se hacen intentos de abuso de bonificaciones a clientes nuevos o de reventa de periodos de prueba buscando ganancias financieras.	La tasa de ataques a inicios de sesión es comparable a la de comercio electrónico. Las organizaciones de medios han visto, no obstante, un aumento de las tasas de ataques a navegadores móviles y aplicaciones móviles de año a año.	Las tasas de ataque a pagos en medios son menores que en otros sectores, probablemente porque representan menos oportunidad de liquidar ganancias que en pagos de comercio electrónico o servicios financieros. Sin embargo, el sector registró un aumento significativo de bots de año a año haciendo transacciones de pago. Probablemente son defraudadores probando datos de tarjeta de crédito robados, antes de utilizar las tarjetas validadas en otro ataque más lucrativo en alguna otra parte.
VOLUMEN DE ATAQUES	29 M (30 M)	7 M (9 M)	3 M (3 M)
TASA DE ATAQUES			
GENERAL	16,6 % (15,5 %)	1,1 % (1,9 %)	1,8 % (2,5 %)
ESCRITORIO	**21,9 %** (18,3 %)	0,7 % **(2,8 %)**	**2,0 % (2,9 %)**
NAVEGADOR MÓVIL	14,9 % (12,1 %)	0,8 % (0,6 %)	1,9 % (2,8 %)
APLICACIÓN MÓVIL	15,7 % **(25,4 %)**	**5,1 %** (0,8 %)	1,1 % (1,5 %)

Las cifras en paréntesis son del segundo semestre de 2019

JUEGOS DE AZAR Y APUESTAS (SUBCONJUNTO DE MEDIOS): VISIÓN GENERAL DE TENDENCIAS Y PATRONES DE ATAQUES

Las oportunidades de abuso de bonificaciones y apropiación de cuentas atraen a los defraudadores a los juegos de azar y apuestas

RESUMEN DE JUEGOS DE AZAR Y APUESTAS	CREACIÓN DE CUENTAS NUEVAS	INICIOS DE SESIÓN	PAGOS
TASA DE ATAQUES			
GENERAL	9,4 %	0,9 %	0,8 %
ESCRITORIO	**12,6 %**	**1,3 %**	0,7 %
NAVEGADOR MÓVIL	9,0 %	0,9 %	**1,0 %**
APLICACIÓN MÓVIL	3,6 %	0,1 %	0,3 %

- Las bonificaciones para jugadores nuevos hacen que los operadores de juegos de azar y apuestas sean susceptibles a mucha creación fraudulenta de cuentas nuevas. Los defraudadores a menudo hacen una explotación a gran escala de oportunidades gratuitas en juegos de azar, aumentando así su probabilidad de ganarse el premio mayor.
- Esto explica la elevada tasa de ataques a la creación de cuentas nuevas, especialmente en transacciones de escritorio.
- Aunque la tasa de ataques a los inicios de sesión se mantiene baja, el significativo volumen de intentos de apropiación de cuentas es muestra del riesgo que plantean al sector los defraudadores que buscan acceder a saldos de cuentas de usuario legítimas o simplemente lavar las ganancias del delito en distintos sectores y regiones geográficas.

TELECOMUNICACIONES (SUBCONJUNTO DE MEDIOS): VISIÓN GENERAL DE TENDENCIAS Y PATRONES DE ATAQUES

Las organizaciones de telco tienen un alto riesgo de exposición monetaria por creación fraudulenta de cuentas nuevas y captura de cuentas

RESUMEN DE TELCO	CREACIÓN DE CUENTAS NUEVAS	INICIOS DE SESIÓN	PAGOS
TASA DE ATAQUES			
GENERAL	1,1 %	0,2 %	1,9 %
ESCRITORIO	1,0 %	**0,3 %**	1,8 %
NAVEGADOR MÓVIL	**1,1 %**	0,1 %	**2,0 %**

- Las compañías de telecomunicaciones (telco) representan una oportunidad para que los defraudadores laven hardware de alto valor y registren contratos telefónicos móviles en prepago y pospago para poder cometer más fraude.
- Debido a que el desplazamiento desde almacenes físicos a transacciones digitales se ha acelerado aún más por los confinamientos relacionados con COVID-19, las organizaciones de telco han tenido que priorizar su transformación digital, alejándose de las ventas persona a persona y verificaciones de clientes que eran típicas de la experiencia en almacenes físicos.
- Aunque las tasas generales de ataque siguen siendo bajas, a nivel individual la exposición monetaria por creación de cuentas nuevas y captura de cuentas puede ser extremadamente alta. Esto se debe en gran parte al alto valor de los teléfonos móviles y la posibilidad de acumular rápidamente grandes cargos a las cuentas, especialmente en descarga de contenido y streaming de medios.

Los datos de aplicaciones móviles han sido excluidos debido al bajo volumen de transacciones.

06

EL DELITO CIBERNÉTICO EN UNA PANDEMIA: TENDENCIAS DEL CONSUMIDOR Y TIPOLOGÍAS DE FRAUDE

RESUMEN:

- Aunque ciertos tipos de tipologías de fraude han proliferado durante la pandemia global, las tasas generales de ataques en la red Digital Identity Network han decrecido.
- Automatización y suplantación de identidad siguen siendo vectores de ataque clave durante 2020.
- Con muchos clientes recién llegados a la red digital que entran en línea por primera vez, el grupo etario más joven - menos de 25 años - es el más susceptible a ataques de fraude.
- Sin embargo, el grupo etario más viejo tiene la segunda tasa de ataques más alta, lo cual también lo hace vulnerable.
- Las pérdidas por fraude aumentan progresivamente con la edad, haciendo que la población de mayor edad tenga el riesgo más alto de sufrir las mayores pérdidas por fraude.

EL DELITO CIBERNÉTICO EN UNA PANDEMIA

Resumen de tendencias del consumidor y tipologías de fraude durante 2020

TENDENCIAS DEL CONSUMIDOR

Aumento del 34 % en pagos en línea de año año.

Aumento del 26 % de año a año en transacciones de inicio de sesión.

Aumento del volumen de transacciones provenientes de dispositivos nuevos e identidades digitales nuevas, así como más transacciones de clientes existentes.

El descenso en las tasas generales de ataques indica que hay una mayor proporción de transacciones de clientes confiables.

Aumento de nuevos clientes de banca en línea que se registran para servicios web y móviles.

Menos actividad de inicio de sesión por parte de consumidores que habían viajado más de 1.000 km en una semana, así como un desplazamiento de los inicios de sesión de áreas metropolitanas a suburbanas.

TIPOLOGÍAS DE FRAUDE

La suplantación de identidad fue el vector de ataque más frecuente y se vio en el 5 % de todas las transacciones globales. Fue seguida por la suplantación de dispositivos, con un 4,2 %.

El aumento de ataques generalmente proviene del volumen de bots automatizados, lo cual indica que la automatización es el método preferido para los ataques actuales.

Medios sigue siendo el sector con las mayores tasas generales de ataques, aunque en servicios financieros se observa la mayor tasa de ataques contra pagos.

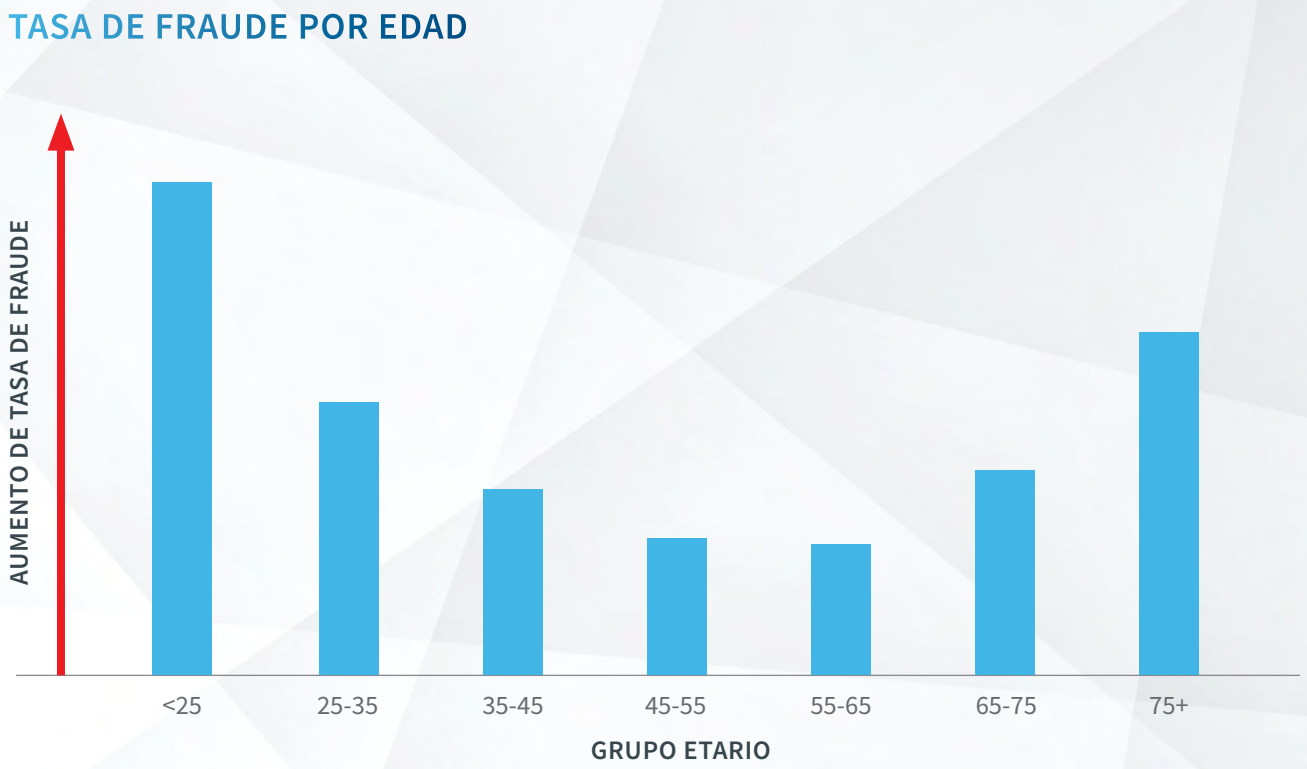
Fraude registrado contra paquetes de estímulo gubernamental en numerosos bancos; p.ej., contra el esquema de préstamos Bounce Back en el Reino Unido.

Primeros indicios de que los consumidores están sintiendo la presión económica, con el aumento en la tasa de fraude de cargo revertido en comercio electrónico.

RIESGO DE FRAUDE POR EDAD: ¿CUÁLES CLIENTES SON LOS MÁS VULNERABLES A ATAQUES DE FRAUDE?

Con clientes recién llegados a la red digital que se conectan en línea en grandes cantidades, ¿están en mayor riesgo?

- El mayor aumento de clientes nuevos que se pusieron en línea en 2020 fue en el grupo etario de menores de 25 años de edad, con un aumento del 10 % registrado a lo largo de cuatro meses.
- El análisis muestra que este grupo etario también es el más vulnerable a ataques de fraude, seguido de cerca por el grupo de más de 75 años de edad.
- Los informes de prensa a menudo sugieren que los millennials son bastante relajados para compartir datos en línea, lo cual los hace más vulnerables a una posible infracción de datos o robo de identidad.
- El grupo de más de 75 años edad, a veces denominada la generación silenciosa, en general está menos familiarizada con las últimas tecnologías digitales y por lo tanto, podría ser más susceptible a fraudes e intentos de phishing.



RIESGO DE FRAUDE POR EDAD ¿CUÁLES CLIENTES PIERDEN LA MAYOR CANTIDAD DE DINERO POR ATAQUES DE FRAUDE?

¿Cómo pueden las organizaciones proteger a quienes tienen el mayor riesgo de perder más?

- Mientras que los millennials y los zillennials son los más susceptibles a ataques de fraude, el promedio de pérdidas por fraude por cliente aumenta progresivamente con la edad, por la probable influencia de una mayor disponibilidad de ingresos con la edad.
- La paradoja de por qué los defraudadores eligen enfocarse en el grupo etario más joven en volúmenes proporcionalmente más altos probablemente se puede responder por el hecho de que tasas de éxito más altas pueden compensar ganancias monetarias más bajas.
- La protección de la población mayor y potencialmente más vulnerable es crítica para las organizaciones que están priorizando una estrategia digital.
- Las empresas deben educar a sus clientes sobre el modus operandi de los ataques de fraude, y a la vez garantizar que el recorrido digital del cliente esté protegido de ataques, enviando según el caso mensajes en línea relevantes y oportunos.

07 CONCLUSIÓN

PREDICCIONES PARA EL AÑO QUE VIENE: LA OPORTUNIDAD PARA LOS NEGOCIOS DIGITALES

Con el cambio, a menudo emergen grandes oportunidades. Estas oportunidades, sin embargo, se le presentan no solo a las empresas digitales con visión futura, sino también a los ciberdelincuentes que se logren mantener un paso adelante de la curva tecnológica. A medida que las organizaciones continúan fusionando sus servicios digitales y físicos, innovando para satisfacer a una base de consumidores cada vez más diversa, las estrategias de prevención de fraude deben mantenerse a la par de esta evolución, transformación y crecimiento. Sin un enfoque robusto en capas, las empresas se están exponiendo a nuevos riesgos de fraude. Los defraudadores siguen siendo maestros del camuflaje y siempre buscan el eslabón más débil bajo un manto de legitimidad.

La innovación que lidera el mercado mantendrá su paso acelerado para facilitar esta compleja serie de oportunidades y mitigar los riesgos asociados para las empresas digitales globales. En esencia, esto debe ofrecer a las empresas la capacidad de poner en capas las soluciones de identidad física y digital y autenticación a través del recorrido omnicanal del cliente.

El eslabón más débil bien puede ser el de los clientes recién llegados a la red digital que se conectaron en línea durante la pandemia. Los adultos más jóvenes y la población mayor han resultado ser los más susceptibles a los ataques de fraude. La prevención del fraude abarca no solo la detección de suplantación de identidad, ataques de bots automatizados y apropiación de cuentas, sino también concientización, educación y comunicación con el cliente para enseñarles cómo reconocer posibles fraudes. Es probable que sigamos viendo a los defraudadores explotar las ansiedades relacionadas con la pandemia, ofreciendo inversiones que parecen ser demasiado buenas para ser ciertas o productos que tienen una alta demanda en línea.

No obstante, no hay que proteger solo a los nuevos clientes. Los clientes existentes confiables podrían sufrir la molestia de pasos de autenticación adicionales, ya que el comportamiento de “regreso a la normalidad” posiblemente sería marcado como inusual dado el cambio sin precedentes en el comportamiento del consumidor en 2020. ¿Cómo pueden las organizaciones garantizar que una prevención confiable del fraude no se traduzca en fricción innecesaria para los clientes legítimos?

Los cambios regulatorios y la incertidumbre económica también se fusionarán con este panorama digital en evolución:

- Las plataformas bancarias abiertas se convertirán en objetivo clave para defraudadores que buscan explotar datos de clientes en cuentas. PSD2 en Europa verá defraudadores buscando vacíos y exenciones en defensas fortalecidas contra el fraude. Nuevamente, los clientes legítimos podrían observar un cambio en las tasas de aceptación de transacciones con la nueva generación de estrategias de autenticación que exigen dos capas de autenticación fuerte del cliente (SCA, por su sigla en inglés).
- También es probable que a medida que las economías responden al impacto de la pandemia, los defraudadores buscarán beneficiarse de la caída por medio de un mayor reclutamiento de mulas, prometiendo a los consumidores dinero fácil a cambio de utilizar su cuenta bancaria para canalizar ganancias del crimen a través de organizaciones globales.
- Los vendedores de comercio electrónico probablemente verán un aumento en el fraude de primera instancia a medida que más consumidores sufren el conflicto económico.

08 GLOSARIO, METODOLÓGÍA, DATOS DE CONTACTO

GLOSARIO

Tipos de sectores

Servicios financieros incluye banca móvil, banca en línea, transferencia de dinero en línea, préstamos, corretaje, pagos alternos y emisión de tarjetas de crédito.

Comercio electrónico incluye minoristas, mercados, emisión de boletos, telecomunicaciones y negocios de bienes digitales.

Medios incluye redes sociales, streaming de contenido, apuestas, juegos de azar y sitios de citas en línea.

Ataques comunes

Fraude de creación de cuenta nueva: Utilización de identidades robadas, comprometidas o sintéticas para crear cuentas nuevas que acceden a servicios en línea u obtienen líneas de crédito.

Fraude de inicio de sesión: Ataques que buscan apropiarse de cuentas de usuario utilizando credenciales previamente robadas que están disponibles en cualquier parte, o credenciales comprometidas por malware o ataques Man in the Midddle.

Fraude de pago: Utilización de credenciales de pago robadas para realizar transferencias de dinero o pagos en línea ilegales mediante métodos digitales alternos, tales como depósito directo.

Porcentajes

Porcentajes de tipo de transacción están basados en el número de transacciones (creación de cuentas, inicios de sesión y pagos) desde dispositivos móviles y computadores de escritorio que son recibidas y procesadas por la red Digital Identity Network.

Porcentajes de ataque están basados en transacciones de alto riesgo identificado y clasificadas como ataques, por caso de uso. Los eventos que son identificados como ataques usualmente son bloqueados o rechazados automáticamente y casi en tiempo real dependiendo de los casos de uso individuales de los clientes.

Escritorio versus móvil

Transacciones de escritorio son transacciones que se originan en un dispositivo de escritorio tal como un computador o portátil.

Ataques de escritorio son ataques dirigidos a una transacción originada en un dispositivo de escritorio.

Transacciones móviles son transacciones que se originan en un dispositivo móvil portátil tal como una tableta o un teléfono móvil. Incluyen transacciones de navegadores y aplicaciones móviles.

Ataques móviles son ataques dirigidos a transacciones que se originan en un dispositivo móvil y están en navegador o aplicación.

Explicación de ataques

Suplantación de dispositivos: Defraudadores borran y modifican ajustes de navegador con el fin de cambiar la identidad o huella digital de su dispositivo o intentar parecer que provienen del dispositivo de una víctima. La patentada identificación de dispositivos sin cookies de LexisNexis® ThreatMetrix® es capaz de detectar visitantes que retornan aún cuando las cookies han sido borradas o se han hecho cambios a los ajustes del navegador. Para distinguir entre ciberdelincuentes y clientes legítimos que ocasionalmente borran cookies, únicamente el borrado con alto riesgo/alta velocidad de cookies (tal como un elevado número de visitas repetidas por hora/día) se incluye en el análisis.

Suplantación de identidad: Utilización de una identidad o tarjeta de crédito robada o de una combinación de usuario/contraseña comprometida, para intentar fraude o apropiación de una cuenta. La suplantación de identidad usualmente se detecta por la alta velocidad de utilización de identidad en un dispositivo, por el acceso de un mismo dispositivo a cuentas de usuario no relacionadas o por vínculos y utilizaciones inusuales.

Suplantación de dirección IP: Los ciberdelincuentes utilizan proxies para eludir los tradicionales filtros de geolocalización de IP y utilizan técnicas de suplantación de IP para eludir filtros de velocidad y listas negras. LexisNexis ThreatMetrix® detecta suplantación de IP directamente, mediante técnicas de toma de huellas de navegador y paquete de red tanto activas como pasivas.

Detección de Man in the Browser (MitB) y bots: Los ataques Man in the Browser son troyanos sofisticados para robar información de ingreso y claves de acceso de uso único del navegador de un usuario. Los bots son scripts automatizados que intentan lograr acceso a cuentas por medio de credenciales robadas o crean cuentas falsas.

LexID® Digital

LexID® Digital es la tecnología que da vida a la inteligencia de identidad digital, creando un identificador en línea único por cada usuario que hace una transacción. El identificador se construye utilizando inteligencia relacionada con dispositivos, datos de identidad, ubicaciones, comportamientos, detalles de transacciones y datos de amenazas. LexID Digital ayuda a las empresas a elevar las decisiones de fraude y autenticación del nivel de dispositivo al nivel de usuario y a unir el comportamiento no en línea con la inteligencia en línea. LexID Digital tiene los siguientes beneficios:

- Une elementos de datos en línea y no en línea por cada usuario que hace una transacción.
- Va más allá del análisis basado en dispositivos y agrupa otras entidades con base en asociaciones complejas que se forman entre eventos. Identifica una persona sin importar los cambios en dispositivos, ubicaciones o comportamiento.
- La inteligencia de la red Digital Identity Network ayuda a reconocer con precisión a un usuario que retorna en múltiples dispositivos, direcciones de correo electrónico, direcciones físicas y nombres de cuentas.

RESUMEN DE METODOLOGÍA

Informe general

- El Informe de LexisNexis Risk Solutions sobre ciberdelito está basado en ataques de ciberdelincuentes detectados por la red LexisNexis Digital Identity Network entre julio y diciembre de 2020 por medio del análisis, casi en tiempo real, de las interacciones de los consumidores durante su recorrido en línea, desde la creación de cuentas nuevas, inicios de sesión y pagos y otras transacciones secundarias, tales como restablecimiento de contraseñas y transferencias.
- La legitimidad de las transacciones se analiza con base en cientos de atributos, incluyendo identificación de dispositivo, geolocalización, historial previo y analítica comportamental.
- La red Digital Identity Network y su motor de políticas que opera casi en tiempo real ofrecen una perspectiva única de identidades digitales globales en aplicaciones, dispositivos y redes.
- Los clientes de LexisNexis Risk Solutions se benefician de un panorama global de riesgos, aprovechando normas globales dentro de políticas particulares que están afinadas específicamente para sus negocios.
- Los ataques mencionados en el informe están basados en transacciones denominadas de alto riesgo según la calificación de usuarios globales.

Vinculación de redes de fraude

- Los datos de actividad de fraude se toman de julio a septiembre de 2020, con base en dispositivos, direcciones de correo electrónico y números telefónicos registrados como fraudulentos en la red Digital Identity Network.
- La exposición monetaria se calcula con base en el valor transaccional del pago que está en riesgo observado entre julio y diciembre de 2020, según la identificación de todas las transacciones asociadas con la transacción fraudulenta (y grupo de entidades asociadas) durante el período. No incluye valores financieros que están en riesgo y pertenecen a clientes que no suministran datos de transacciones de pagos.

DATOS PROCESADOS Y ANALIZADOS

El volumen total de transacciones procesadas por la red Digital Identity Network entre julio y diciembre de 2020 fue 28.400 millones.

El Informe de LexisNexis sobre ciberdelito analiza un subconjunto de estas transacciones que excluye eventos no basados en transacciones (como comentarios de cliente y transacciones de prueba) así como transacciones de organizaciones que se consideran caso aparte debido a unas tasas de rechazo inexistentes o extremadamente altas.

El subconjunto asciende a 24.600 millones de transacciones. El informe de ciberdelito utiliza estas 24.600 millones de transacciones para calcular el volumen total de transacciones a nivel global y por región. Hay 880 K transacciones sin dirección IP. Por lo tanto, estas transacciones no pueden ser asignadas a una región. Se trata de sesiones desconocidas en su mayoría, en las cuales una organización no envía la dirección IP de ingreso.

Este subconjunto de 24.600 millones de transacciones también se utiliza para el análisis de ataques de bots automatizados. Incluye sesiones conocidas relacionadas con eventos individuales, así como sesiones desconocidas que a veces pueden ser una característica del tráfico de bots, dado que la velocidad de ataque no registra datos completos de perfilado.

El volumen de ataques iniciados por humanos se calcula sobre un subconjunto adicional de 20.900 millones de transacciones. Se clasifican como sesiones conocidas relacionadas con eventos individuales.

Este subconjunto excluye eventos para los cuales no se pudo recolectar ningún dato de inteligencia de identidad digital debido a un perfilado no exitoso.

LexisNexis®
RISK SOLUTIONS

PARA MÁS INFORMACIÓN:

risk.lexisnexis.com/fraude

risk.lexisnexis.com/global/es/products/threatmetrix

Acerca de LexisNexis Risk Solutions

LexisNexis® Risk Solutions aprovecha el poder de los datos y la analítica avanzada para entregar conocimiento que ayuda a las empresas y las entidades gubernamentales a reducir el riesgo y mejorar las decisiones para el beneficio de las personas en todo el mundo. Ofrecemos soluciones de información y tecnología para una amplia gama de sectores, entre ellos: seguros, servicios financieros, salud y gobierno. Con sede principal en la ciudad de Atlanta, Georgia, tenemos oficinas en todo el mundo y somos parte de RELX (LSE: REL/NYSE: RELX), un proveedor mundial de herramientas de analítica y toma de decisiones para clientes profesionales y empresariales basadas en información.

NXR14936-00-0621-ES-LA

Para más información, visite risk.lexisnexis.com y relx.com