GROUP-IB

América Latina

INTELLIGENCE INSIGHTS

ABRIL DE 2025

HECHO DESTACADO DEL MES

Este informe contiene información sobre los hechos de ciberseguridad más importantes que tuvieron lugar en el mundo y en América Latina durante el mes pasado

2

hechos más llamativos

El CERT de Group-IB ha identificado una nueva estafa de *phishing* en Brasil en la cual los ciberdelincuentes utilizan torres de telefonía móvil fraudulentas para enviar mensajes SMS y robar datos personales y financieros.

Los especialistas de Group-IB descubrieron varios directorios abiertos en la web con *scripts* de Python. Al parecer, estos directorios se utilizan para acceder mediante ataques de fuerza bruta a cuentas de correo electrónico, con el fin de obtener acceso no autorizado a servidores SMTP de empresas brasileñas.

TENDENCIAS MUNDIALES

Breve descripción de las tendencias mundiales:

01 Un actor de amenazas conocido como rose87168 puso a la venta datos supuestamente robados de Oracle

En marzo de 2025, un actor de amenazas conocido como **rose87168** puso en venta datos supuestamente robados de Oracle, la empresa multinacional de tecnología informática estadounidense: concretamente sus servicios de Oracle Cloud.

El atacante afirmaba que la filtración había tenido lugar en enero de 2025 e inicialmente se proponía negociar una venta privada con Oracle. Aparentemente la operación no tuvo éxito

02 Group-IB publicó un blog exhaustivo en ClickFix

Group-IB publicó un blog exhaustivo en el que se describe una técnica de ingeniería social llamada ClickFix, que suelen utilizar los atacantes para engañar a los usuarios y hacer que ejecuten *scripts* maliciosos de PowerShell. Se engaña a las víctimas para que hagan clic en botones falsos tipo "Reparar" o mensajes CAPTCHA, que copian códigos de programas maliciosos en su portapapeles y les indican que los ejecuten manualmente. Este método se ha utilizado para distribuir programas que roban información, como Lumma, y se ha vuelto muy popular entre los ciberdelincuentes (incluso entre los grupos de amenazas persistentes avanzadas). Group-IB advierte sobre su uso creciente y propone una mayor toma de conciencia entre los usuarios para evitar situaciones peligrosas

TENDENCIAS MUNDIALES

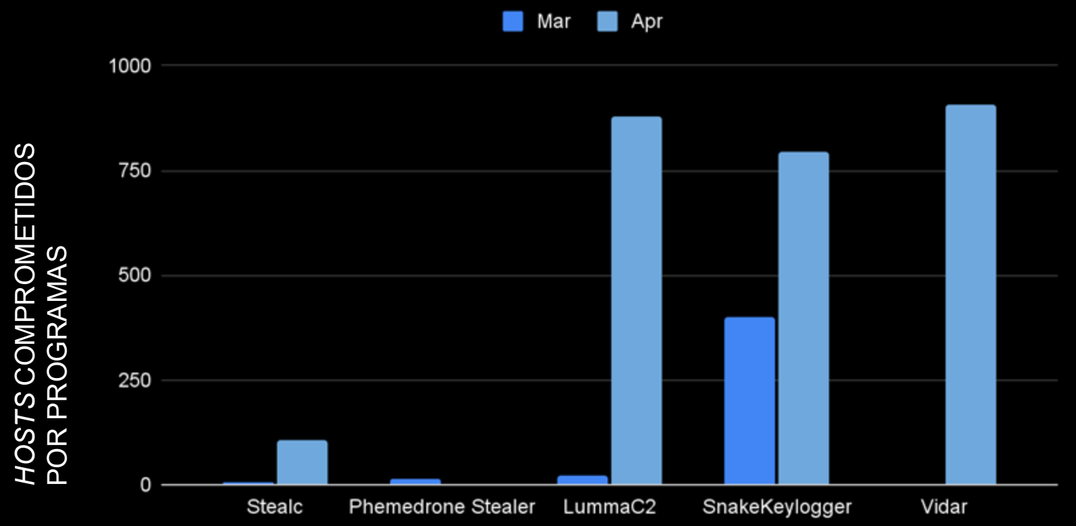
Breve descripción de las tendencias mundiales:

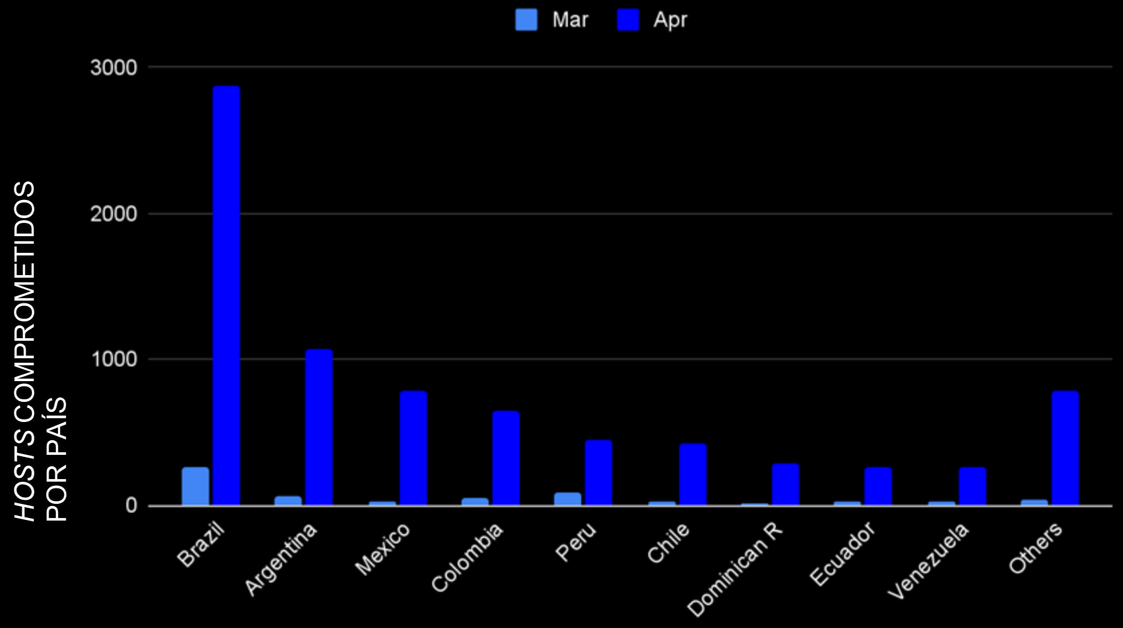
01 Ciberdelincuente responsable de más de 90 filtraciones de datos en todo el mundo detenido en una operación conjunta

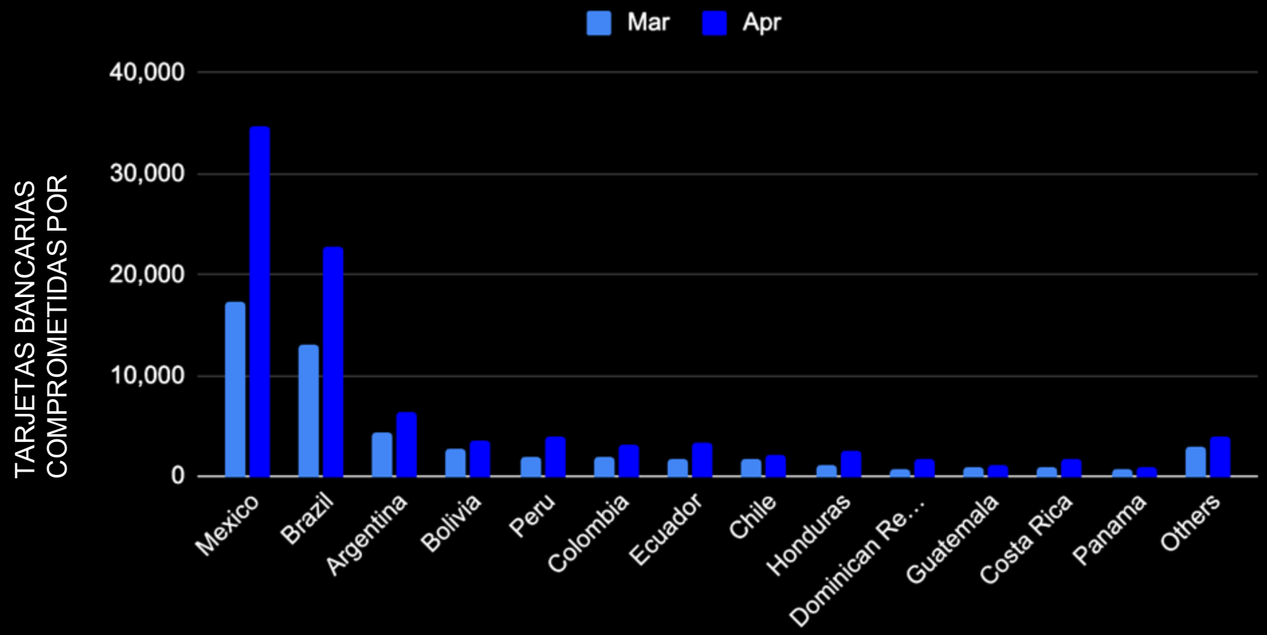
Group-IB, en colaboración con la Real Policía Tailandesa y la Fuerza de Policía de Singapur, logró detener a un ciberdelincuente responsable de más de 90 filtraciones de datos en todo el mundo. Esta persona, que operaba bajo alias tales como ALTDOS, DESORDEN, GHOSTR y 0mid16B, atacaba a grandes empresas privadas de diversos sectores, como el financiero, el comercio minorista y el sector manufacturero. Los equipos Threat Intelligence y High-Tech Crime Investigation de Group-IB rastrearon al ciberdelincuente con sus diversos alias, lo que resultó en un gran aporte a la investigación. El arresto tuvo lugar el 26 de febrero de 2025, en Tailandia, lo que marca un hito importante en la lucha contra el delito informático mundial

DATOS COMPROMETIDOS

Los ladrones desempeñan un importante papel en la cadena logística de delitos cibernéticos, ya que los datos robados de la computadora infectada por este tipo de programas maliciosos pueden dar lugar a incidentes de mayor impacto, como *ransomware* (cibersecuestro), extorsión y espionaje. A las cuentas válidas — es decir, las credenciales filtradas por ladrones — las suelen utilizar los actores de amenazas para obtener acceso inicial a las empresas, así como para escalar privilegios y llevar a cabo evasiones de defensa.
En esta parte del informe, brindaremos estadísticas sobre *hosts* infectados y tarjetas comprometidas, lo que ayudará a entender qué familias de programas maliciosos son las que están más activas en la región







TENDENCIAS REGIONALES
Percepciones del CERT: América Latina

Breve descripción de las tendencias regionales clave:

01

El CERT de Group-IB ha identificado una nueva estafa de *phishing* en Brasil en la cual los ciberdelincuentes utilizan torres de telefonía móvil fraudulentas para enviar mensajes SMS y robar datos personales y financieros.

El CERT de Group-IB ha descubierto una campaña de *phishing* en Brasil, en la que los atacantes utilizan estaciones base móviles portátiles, por ejemplo, simuladores de sitios celulares o femtoceldas, para enviar mensajes SMS. Estos dispositivos fraudulentos evaden los filtros de telecomunicaciones y atacan a usuarios incluso sin conexión celular activa. En el mensaje SMS se informa a los destinatarios sobre aproximadamente 100 000 puntos de fidelidad que están por vencer y se les ofrece recompensas en forma de reembolsos, productos electrónicos o millas. A través de un enlace malicioso se los dirige a un sitio de *phishing* diseñado para robar datos personales y financieros, que pueden incluir datos sobre tarjetas de crédito.

02

El CERT de Group-IB ha identificado una estafa de inversión generalizada que afecta a varios países de América Latina, en la que los ciberdelincuentes utilizan sitios web basados en WordPress para promover esquemas de generación de ingresos falsos que incluyen operaciones bursátiles, inteligencia artificial y comercio electrónico.

El CERT de Group-IB ha descubierto una campaña de *phishing* en América Latina en la que los atacantes utilizan sitios web basados en WordPress para promover esquemas de inversión falsos. En este tipo de sitios se les promete a los usuarios que aprenderán a ganar dinero a través de operaciones con acciones de empresas o vendiendo productos en línea. Los estafadores recopilan información personal, como nombre, correo electrónico y número telefónico, y les dicen a los usuarios que se comunicarán con ellos dentro de las 24 horas. Sin embargo, después de enviar sus datos, las víctimas no reciben correos electrónicos ni llamadas de seguimiento. La estafa se propaga a través de anuncios de Facebook e Instagram, dirigidos a usuarios de Chile, Colombia, Brasil, Perú, Costa Rica, México, El Salvador y Ecuador. La campaña utiliza técnicas de ingeniería social para fomentar el envío de datos personales.

CONCLUSIONES Y RECOMENDACIONES

En definitiva, el panorama de amenazas en constante evolución plantea riesgos significativos para las organizaciones en diversos sectores. Los incidentes que se abordan en este informe destacan la necesidad de contar con medidas de seguridad sólidas y con una gestión proactiva de las amenazas. Para proteger su organización, le sugerimos implementar las siguientes recomendaciones:

VERIFIQUE EL ORIGEN DE LOS SMS

Asegúrese de que cualquier mensaje SMS provenga de fuentes legítimas. Tenga cuidado con los números desconocidos o códigos abreviados sospechosos, especialmente cuando el mensaje insta a realizar una acción inmediata

UTILICE CANALES OFICIALES PARA SOLICITAR REEMBOLSOS

Póngase en contacto con la empresa directamente a través de los canales oficiales de atención al cliente, para confirmar cualquier oferta, promoción o programa de puntos de fidelidad antes de canjearlos. Evite utilizar enlaces o números telefónicos provistos en mensajes SMS

HABILITE LA AUTENTICACIÓN DE DOS FACTORES (2FA)

Habilite siempre la autenticación de dos factores en las cuentas que la admitan, en especial para servicios financieros y personales. Esto agrega una capa adicional de seguridad en caso de que se vean afectadas sus credenciales

CONTROLE SUS CUENTAS REGULARMENTE

Vigile de cerca los extractos bancarios, operaciones con tarjetas de crédito y cuentas de programas de fidelización. Informe inmediatamente sobre cualquier actividad sospechosa para evitar daños mayores

TENGA CUIDADO CON LOS ANUNCIOS EN REDES SOCIALES

Evite hacer clic en anuncios sospechosos en plataformas como Facebook e Instagram, especialmente aquellos que promueven esquemas para ganar dinero u oportunidades de inversión

NUNCA COMPARTA INFORMACIÓN PERSONAL CON FUENTES NO SOLICITADAS

Absténgase de compartir datos personales, como su nombre, correo electrónico y número telefónico, con sitios web o plataformas cuya legitimidad no pueda verificar.

ACTIVIDADES DE *RANSOMWARE* Y EXTORSIÓN

En febrero se observó una disminución significativa de las divulgaciones, con solo 23 empresas publicadas en DLS, 11 de ellas de Brasil y 3 de Chile. Aunque solo hubo una divulgación, Akira todavía está presente en el panorama de cibersecuestro de LATAM, como ocurrió en los tres últimos meses. Si bien Arcus, KillSec y APT73 (también conocido como Bashe) divulgaron igualmente datos de empresas de la región, cabe destacar que estos grupos suelen llevar a cabo ataques que son solo extorsivos, aunque proporcionan *ransomware* a sus afiliados. Por otra parte, en comparación con Akira, representan un riesgo bajo para las organizaciones.

DIVULGACIONES POR GRUPO

BABUK_v2 nuevo 9 ataques	CLOP 6 ataques + 500 %	AFEPAY 5 ataques - 28 %	AKIRA 4 ataques - 60 %
ARCUS nuevo 4 ataques	FUNKSEC 4 ataques - 33 %	RANSOMHUB 3 ataques	FOG nuevo APOS_SECURITY ELDORADO 2 ataques

Incidentes de *ransomware*

DIVULGACIÓN DE SITIOS DE FILTRACIÓN DE DATOS POR PAÍS

Brasil 21 incidentes - 4 %	México 30 incidentes + 33 %
Colombia 5 incidentes -54 %	Perú 4 incidentes + 300 %
Argentina 4 incidentes -20 %	República Dominicana 2 incidentes

ASPECTOS DESTACADOS SOBRE INCIDENTES Y AMENAZAS EN LATAM

Hechos destacados a nivel regional con una breve descripción:

01 Group-IB identificó una campaña de correo basura malicioso que diseminaba Grandoreiro

El equipo de inteligencia de amenazas de Group-IB detectó una campaña de correo basura malicioso cuyo objetivo era robar datos confidenciales a usuarios de Windows españoles y colombianos infectándolos con el troyano bancario Grandoreiro.

Los correos electrónicos que se enviaban suplantaban la identidad de empresas como Endesa, Mercadona, Naturgy, Binance y Mapfre. El proceso de infección comenzó cuando una víctima descargó un archivo ZIP malicioso que estaba disponible en cld[.]pt y ejecutó el programa malicioso cuyo nombre de archivo seguía el patrón F{NUM}.{COMPANY}.xxx-A4-IDfecha{NUM}.zip

02 Group-IB detectó una campaña de fuerza bruta destinada a obtener acceso no autorizado a los servidores SMTP

Los especialistas de Group-IB descubrieron varios directorios abiertos en la web con *scripts* de Python que se utilizan presuntamente para acceder mediante ataques de fuerza bruta a cuentas de correo electrónico, con el fin de obtener acceso no autorizado a servidores SMTP relacionados con empresas brasileñas.

Uno de los *scripts* llamado “*crack.py*” tenía una dirección de correo electrónico que pertenecía al delincuente y se utilizaba para probar las credenciales forzadas, así como los servidores SMTP.

Según los registros, aparentemente el atacante comprometió 154 credenciales

CONCLUSIONES Y RECOMENDACIONES

GROUP-IB

En definitiva, el panorama de amenazas en constante evolución plantea riesgos significativos para las organizaciones en diversos sectores. Los incidentes que se abordan en este informe destacan la necesidad de contar con medidas de seguridad sólidas y con una gestión proactiva de las amenazas. Para proteger su organización, le sugerimos implementar las siguientes recomendaciones:

Archivos LNK

Los troyanos bancarios que atacan a usuarios de Europa y la región de LATAM tienen una cadena de infección de varias etapas, que suele comenzar con la descarga de archivos maliciosos disponibles en servicios en la nube legítimos, como cld[.]pt y MediaFire

Campañas de correo basura malicioso

Los troyanos que tienen como objetivo la región de LATAM comparten TTP similares, que incluyen la diseminación del programa malicioso a través de campañas de correo basura malicioso. Para lograrlo, los delincuentes suelen utilizar cuentas de correo electrónico legítimas, pero comprometidas

Ingeniería social

Nunca descargue archivos como EXE, MSI, ISO, LNK y ZIP incluso cuando le hayan enviado el correo desde un remitente conocido. Además, controle siempre el nombre del archivo. Los archivos maliciosos pueden tener extensiones dobles, como “.exe.pdf”

Habilite la autenticación de dos factores (2FA)

Active siempre la autenticación de dos factores en sus cuentas de correo electrónico y, si es posible, evite utilizar SMS y correos electrónicos como 2FA. Es preferible utilizar autenticadores o autenticación de hardware, como Yubikey

Política de contraseñas

No utilice contraseñas fáciles y obvias como Mudar@123 o John2025, evite repetir las últimas 3 contraseñas, configure una contraseña larga y compleja utilizando administradores de contraseñas móviles o de escritorio

Fuerza bruta

Establezca la cantidad máxima de intentos de inicio de sesión en el servidor. De este modo, podrá atenuar los ataques de fuerza bruta. Configure, además, la autenticación de dos factores (2FA) como predeterminada para todos los usuarios.

CASO DE ESTAFA DEL MES:

Technologies · March 27, 2025

Navigating Cybercrime Currents in Latin America: Strengthening the Region's Defenses

MÁS INFORMACIÓN:

INVESTIGACIÓN, PREVENCIÓN Y LUCHA CONTRA LOS DELITOS CIBERNÉTICOS DESDE 2003

GROUP-IB.COM
INFO@GROUP-IB.COM
GROUP-IB.COM/BLOG
+65 3159 3798
LINKEDIN FACEBOOK TWITTER INSTAGRAM