Diciembre 2024

América Latina

Intelligence Insights

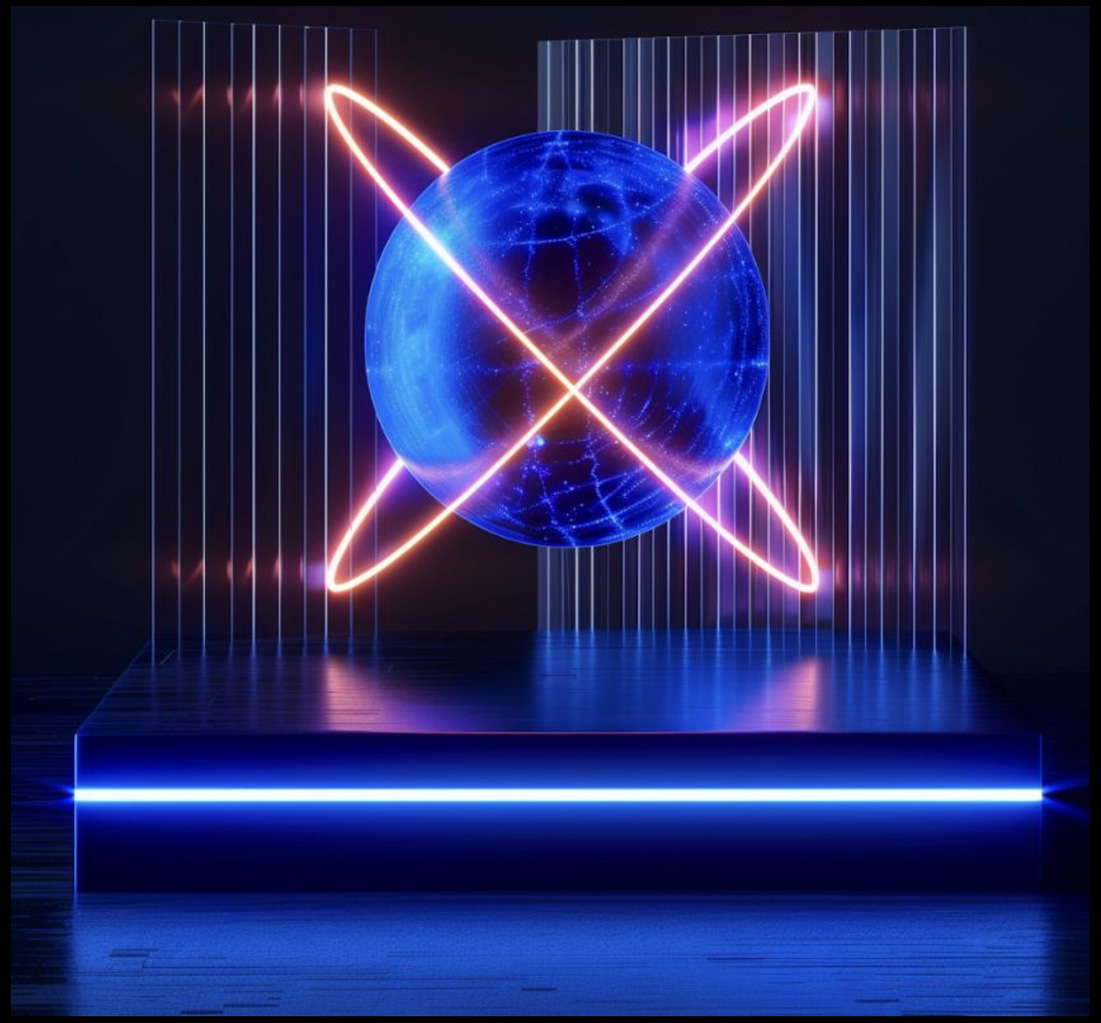
INTRODUCCIÓN

Este documento presenta un análisis de los eventos de ciberseguridad más relevantes ocurridos durante el mes de diciembre a nivel global y con foco en la región de América Latina

2 eventos más llamativos del mes:

- **El CERT de Group-IB descubrió un sofisticado esquema de estafas dirigido a compañías de seguros y sistemas de pago de Colombia.**

- **Group-IB descubrió una campaña de correo basura malicioso que estaba diseminando el troyano bancario Grandoreiro, el cual tenía como objetivo países de habla hispana, como España y Argentina.**



TENDENCIAS MUNDIALES

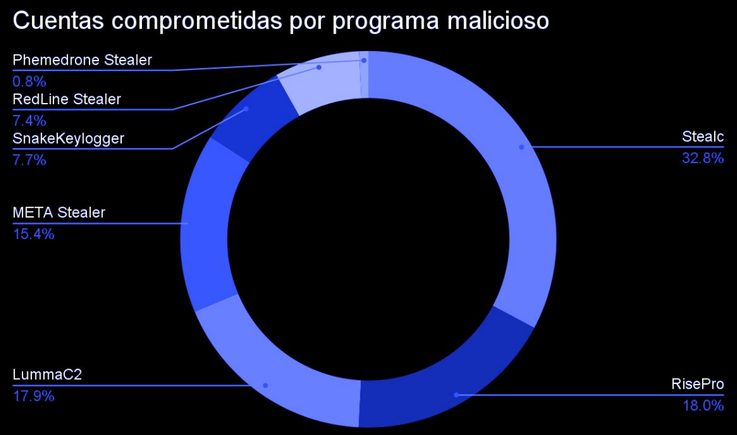
Breve descripción de las tendencias globales:

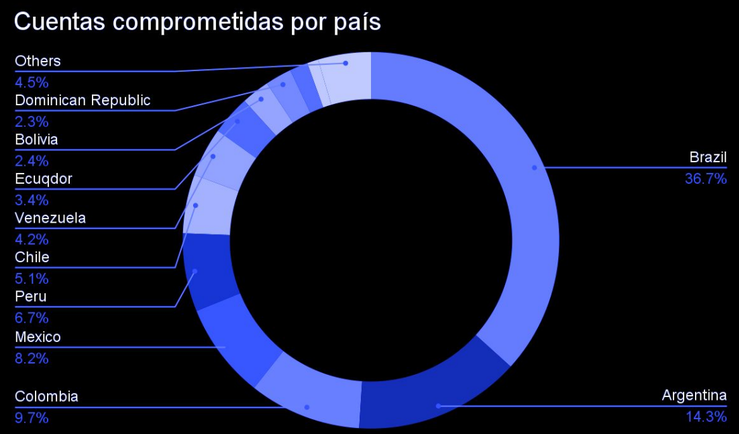
01 Group-IB publicó una investigación detallada sobre el grupo Cicada3301 de ransomware como servicio	Recientemente, Group-IB ha obtenido acceso, de forma satisfactoria, al panel de afiliados de ransomware de Cicada3301. En este blog, compartimos sus procesos internos en función de nuestro análisis exhaustivo de las versiones de ransomware disponibles que se ofrecen en el panel de afiliados y todas las secciones a las que se puede acceder, a fin de ofrecer una evaluación definitiva de esta amenaza
02 Las tácticas de sigilo de Lazarus APT con atributos extendidos descubiertas por especialistas de Group-IB	Los especialistas de Group-IB han descubierto una novedosa técnica de Lazarus APT que permite ocultar código malicioso en atributos extendidos y, de este modo, se impide su detección en macOS. Este método, que no está presente en la infraestructura MITRE ATT&CK, incluye un nuevo troyano, «RustyAttr», desarrollado con el marco Tauri y que VirusTotal no puede detectar. Aunque macOS Gatekeeper bloquea las aplicaciones sin firma, la ingeniería social plantea un riesgo significativo, lo que pone de relieve la necesidad de contar con medidas de seguridad sólidas contra las amenazas en desarrollo. Leer más
03 Group-IB descubrió el uso de la técnica de reCAPTCHA falsa por parte del grupo MuddyWater APT	Se llevó a cabo una campaña que utiliza la técnica ClickFix para distribuir la herramienta RMM, supuestamente dirigida a empleados de las fuerzas de seguridad en uno de los países que limitan con Irán. Evaluamos, con un grado de confianza moderado, que el atacante detrás de esta campaña es MuddyWater
04 El equipo CERT de Group-IB descubrió una estafa con leña falsa dirigida en línea a consumidores franceses	Estafadores conocidos como «Les brouteurs» aprovechan las redes sociales para vender leña inexistente a residentes franceses durante el invierno. A través de documentos falsos generados por IA y haciéndose pasar por empresas legítimas, engañan a las víctimas para que les transfieran dinero. La investigación de Group-IB pone de manifiesto el creciente nivel de sofisticación de estas estafas. Tanto los consumidores como las empresas deben estar atentos, verificar las credenciales y tomar medidas de prevención de fraudes, con el fin de atenuar las pérdidas económicas. Leer más

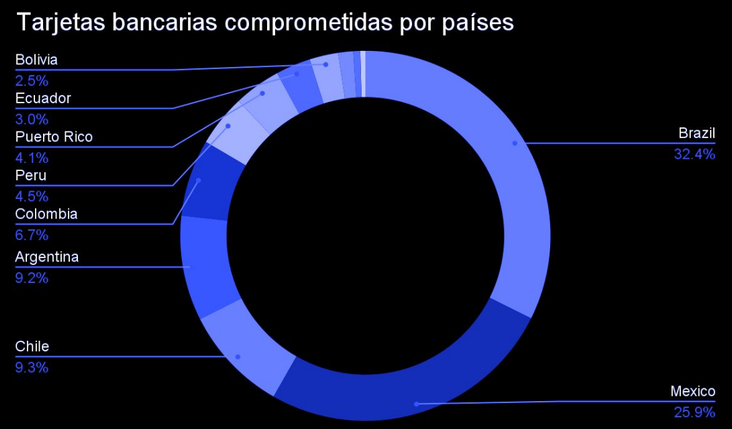
ESTADISTICAS: DATOS COMPROMETIDOS

Los stealers desempeñan un importante papel en la cadena logística de delitos cibernéticos, ya que los datos robados de las computadoras infectadas por este tipo de programas maliciosos pueden dar lugar a incidentes de mayor impacto, como cibersecuestro (ransomware) o extorsión y espionaje. Los atacantes suelen utilizar las cuentas válidas (es decir, las credenciales que obtienen los stealers) para acceder inicialmente a las empresas, conseguir cada vez más privilegios y evadir defensas.

En esta parte del informe, presentaremos estadísticas en relación con losservidores infectados y las tarjetas comprometidas; esto le permitirá entender cuáles son las familias de programas maliciosos más activas en la región







TENDENCIAS REGIONALES, PERCEPCIONES DEL CERT: AMÉRICA LATINA

Breve descripción de las tendencias regionales:

01	El equipo CERT de Group-IB identificó una estafa dirigida a bancos de Argentina, que utiliza anuncios falsos para hacerse pasar por canales de contacto oficiales	Estos anuncios, que suelen diseñarse para atraer a personas mayores mediante ofertas de beneficios y descuentos, incluyen enlaces de WhatsApp donde los estafadores utilizan la ingeniería social para extraer información personal y bancaria confidencial. Este esquema se vale de la confianza que infunden las marcas reconocidas y forma parte de una tendencia más amplia que tiene como objetivo a instituciones financieras de Argentina
02	El CERT de Group-IB ha identificado un sofisticado esquema de estafas dirigido a compañías de seguros y sistemas de pago de Colombia	La estafa implica un proceso que consta de varias etapas y utiliza sitios web fraudulentos que se hacen pasar por marcas legítimas. En la primera etapa, se utilizan bases de datos públicas de licencias de vehículos para convencer a los usuarios de la autenticidad del sitio, mostrando datos exactos del seguro del vehículo. Aquellas víctimas cuyo seguro ha vencido se redirigen a un segundo sitio, en el que se les solicita que brinden información bancaria confidencial, bajo el pretexto de la adquisición de un seguro. Por último, el esquema termina en un tercer sitio que imita sistemas de pago, con el fin de ejecutar transacciones fraudulentas. Este método permite aprovechar la confianza en marcas reconocidas y en datos públicos para engañar a los usuarios y facilitar el robo financiero

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 subrayan la necesidad de contar con medidas de seguridad sólidas y con una gestión proactiva de las amenazas. Para proteger su organización, considere la posibilidad de implementar las siguientes recomendaciones:

VERIFICAR LA AUTENTICIDAD DE LOS CANALES OFICIALES

Verifique siempre la autenticidad de los canales de contacto. Para esto, puede visitar el sitio oficial de su banco o ponerse en contacto con su servicio oficial de atención al cliente

TENER PRECAUCIÓN CON LA INFORMACIÓN PERSONAL

Nunca comparta información personal o bancaria confidencial, como datos de la cuenta, números de tarjetas, códigos PIN o contraseñas de un solo uso, a través de llamadas telefónicas, correos electrónicos o aplicaciones de mensajería, como WhatsApp

INSTRUIR A LOS GRUPOS VULNERABLES

Hable con sus familiares y amigos mayores para que tomen conciencia sobre las estafas dirigidas a jubilados, y enséñeles cómo reconocer y evitar estas amenazas

REFORZAR LAS CAMPAÑAS DE CONCIENTIZACIÓN

Implemente iniciativas de concientización pública destinadas a educar a los clientes sobre las estafas a través de phishing y suplantación de identidad, haciendo hincapié en la importancia de verificar los canales de comunicación

MEJORAR LOS PROCESOS DE AUTENTICACIÓN

Implemente un sistema sólido de autenticación multifactor para las transacciones sensibles, a fin de reducir la probabilidad de fraude, incluso si hay información que está en riesgo

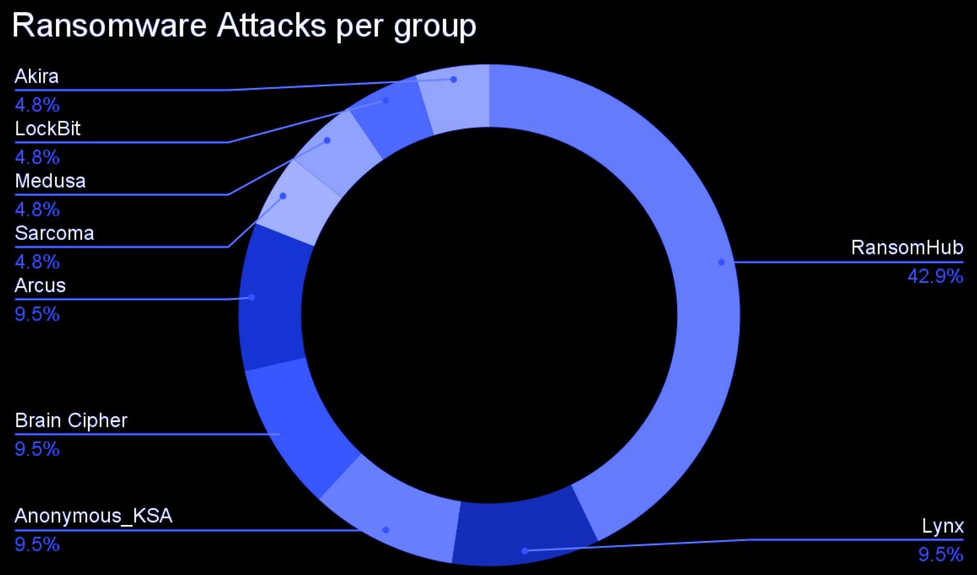
HACER UN USO ESTRATÉGICO DE LA INTELIGENCIA DE LAS AMENAZAS

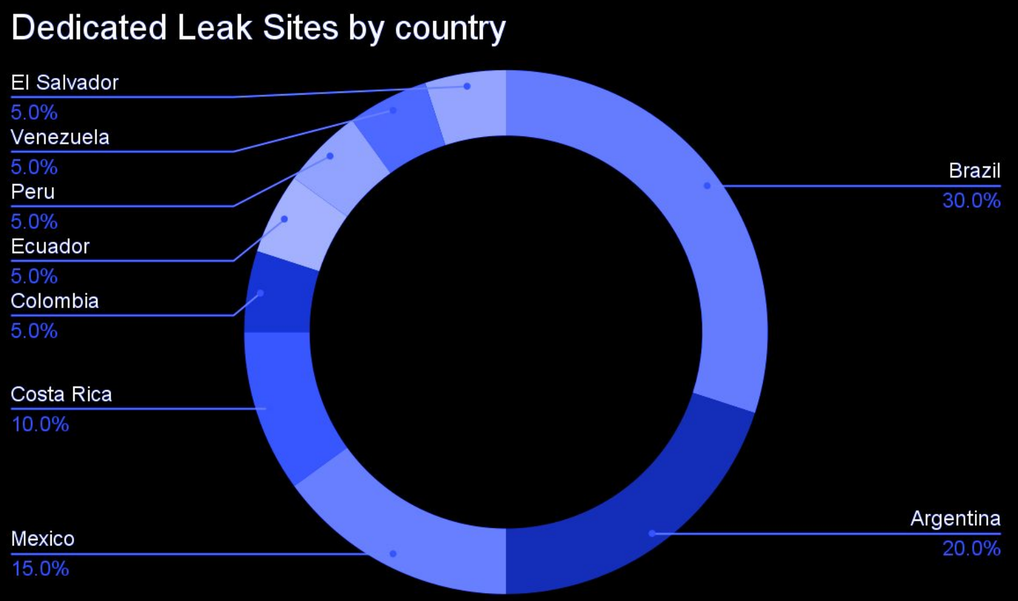
Analice periódicamente las tendencias de estafas y los indicadores de compromiso (IOC) para actualizar los sistemas de detección y adaptar las defensas a las amenazas emergentes

ESTADÍSTICAS: **ATAQUES**

ACTIVIDADES DE RANSOMWARE

RansomHub no solo es el grupo con la mayor cantidad de víctimas reveladas en su DSL, sino también la operación de RaaS que más empresas ha victimizado en la región de LATAM. Por lo tanto, las organizaciones de la región de LATAM deberían dar prioridad a las TTP relacionadas con las intrusiones llevadas a cabo por afiliados a este grupo. Este mes destacamos los ataques contra las empresas brasileñas **Lojas Marisa** y **Aeris Energy** perpetrados por Medusa y Hunters International, respectivamente





ASPECTOS DESTACADOS DE INCIDENTES Y AMENAZAS EN LATAM

Breve descripción de los aspectos destacados clave a nivel regional:

01	Campaña de colaboración para la distribución del troyano de acceso remoto (RAT) GhostSpy en dispositivos Android	Group-IB identificó una campaña de colaboración que, presuntamente, les da a los delincuentes acceso al código fuente de GhostSpy y una oportunidad de reventa. GhostSpy (también conocido como Brazilian Spy) es un RAT diseñado para dispositivos Android y, probablemente, una nueva marca de GoatRAT, también conocido como FantasyMW y CriminalMW. Si bien se ha arrestado a delincuentes que colaboraron con este grupo, este programa malicioso resurgió a comienzos de 2024 como GhostSpy
02	Campaña maliciosa dirigida a países de habla hispana que disemina Grandoreiro	Group-IB descubrió una campaña de *correo basura malicioso* que estaba diseminando el troyano bancario Grandoreiro, que tenía como objetivo países de habla hispana, como España y Argentina. La campaña maliciosa se hace pasar por la empresa española Endesa y utiliza el dominio «cld.pt» asociado al almacenamiento en la nube MEO Cloud para descargar un archivo zip, que es la primera etapa de la cadena de infección

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 subrayan la necesidad de contar con medidas de seguridad sólidas y con una gestión proactiva de las amenazas. Para proteger su organización, considere la posibilidad de implementar las siguientes recomendaciones:

TIENDA OFICIAL DE APK

Los RAT diseñados para dispositivos Android, incluso GhostSpy, suelen estar disponibles en repositorios de APK de terceros, como APKMirror, APKPure y Uptodown. Recuerde instalar aplicaciones descargadas solo de Google Play

PERMISOS DE APK

La mayor parte de los RAT diseñados para dispositivos Android requiere permisos de *administrador*, así como la activación de funciones de accesibilidad. Por lo tanto, no conceda ningún permiso ni active ninguna función en Android, a menos que sepa que se trata de una aplicación legítima

SITIOS WEB MALICIOSOS

Los atacantes pueden difundir APK maliciosos a través de páginas de phishing. Por lo tanto, no descargue ni instale aplicaciones de fuentes dudosas o desconocidas

VERIFICAR LA INFORMACIÓN DEL CORREO ELECTRÓNICO

Los atacantes pueden difundir campañas de correo basura malicioso desde cuentas legítimas comprometidas. Por eso, además de verificar el correo electrónico del remitente, verifique siempre la información que se presenta en el correo electrónico y confírmela con su banco

NO SEGUIR INSTRUCCIONES SIN VERIFICAR

Las campañas de ingeniería social requieren que los usuarios realicen alguna acción, como hacer clic, descargar y dar información. Entonces, antes de llevar a cabo alguna acción, póngase en contacto con la empresa de la que es cliente

HABILITAR LA AUTENTICACIÓN MULTIFACTOR

Evite utilizar SMS y correo electrónico como autenticación multifactor. Le recomendamos que utilice claves de seguridad de hardware y aplicaciones de autenticación, además de los recursos que proveen los sistemas bancarios

INVESTIGACIÓN, PREVENCIÓN Y LUCHA CONTRA DELITOS CIBERNÉTICOS DESDE 2003

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