Enero de 2025

América Latina

INTELLIGENCE INSIGHTS

HECHO DESTACADO DEL MES

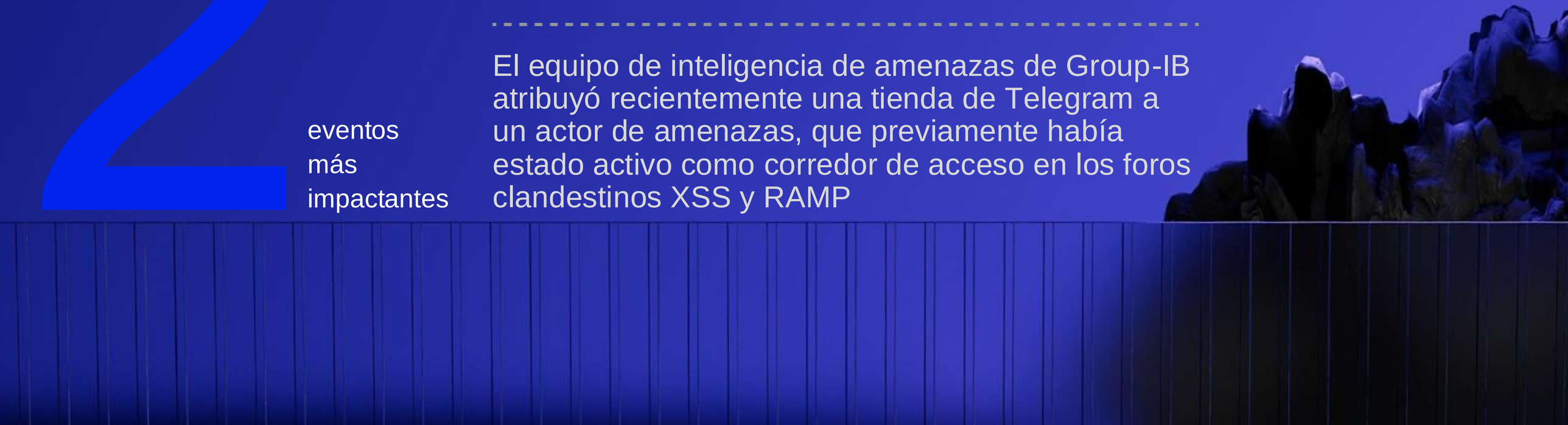
En este documento, se incluye información sobre los eventos de ciberseguridad más importantes que ocurrieron en el mundo y en América del Norte durante el mes pasado

2

eventos más impactantes

El CERT de Group-IB descubrió una ola de estafas relacionadas con préstamos en Brasil, con las que los estafadores utilizan anuncios que presentan figuras públicas para hacerse pasar por bancos e instituciones financieras

El equipo de inteligencia de amenazas de Group-IB atribuyó recientemente una tienda de Telegram a un actor de amenazas, que previamente había estado activo como corredor de acceso en los foros clandestinos XSS y RAMP



TENDENCIAS MUNDIALES

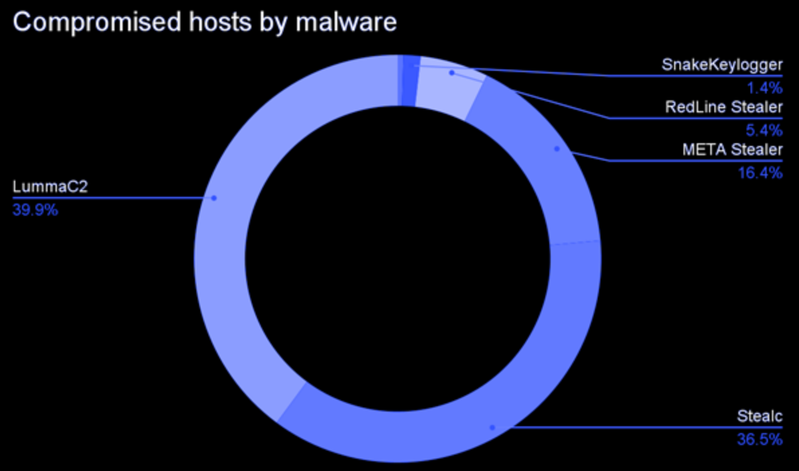
Breve descripción de las tendencias mundiales:

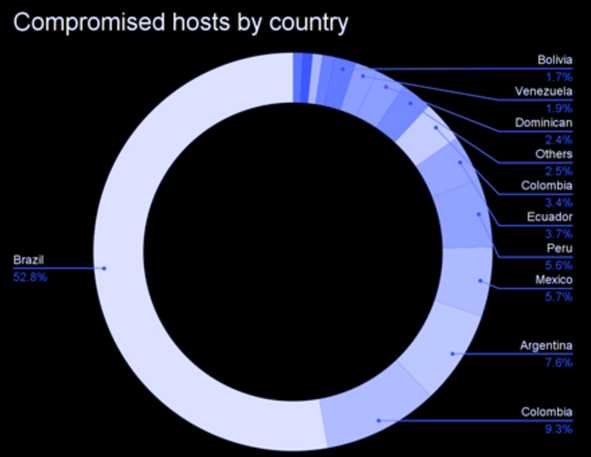
01	Halcyon publicó el blog dedicado al cifrado de los datos en los *buckets* de Amazon S3.	En la entrada de blog "Abusing AWS Native Services: Ransomware Encrypting S3 Buckets with SSE-C" (Abuso de los servicios nativos de AWS: cibersecuestro que cifra los *buckets* de S3 con SSE-C) de Halcyon, se describe una nueva campaña de cibersecuestro en la que el actor de amenazas, apodado Codefinger, utiliza credenciales de AWS para cifrar datos en los *buckets* de Amazon S3 a través de cifrado del lado del servidor, con claves brindadas por el cliente (SSE-C). Mediante este método, los datos no se pueden recuperar sin la clave de cifrado del atacante, dado que AWS no almacena estas claves y CloudTrail solo registra un HMAC que no es suficiente para el descifrado.
02	Descubrimiento de OtterCookie: una campaña de ataques contra Japón vinculada a Corea del Norte.	En la entrada "Contagious Interview and the Newly Identified Malware OtterCookie" (Encuesta contagiosa y el *malware* identificado recientemente OtterCookie) del Blog Técnico de NTT, se analiza una campaña de ataque vinculada a Corea del Norte, "Contagious Interview," que se vale de un programa malicioso recientemente identificado, llamado "OtterCookie". Este programa malicioso utiliza Socket.IO para recibir órdenes remotas, permitir acciones, como ejecutar comandos de shell, robar información de dispositivos y extraer claves de billeteras de criptomonedas, con casos informados en Japón que enfatizan la necesidad de estar alertas.

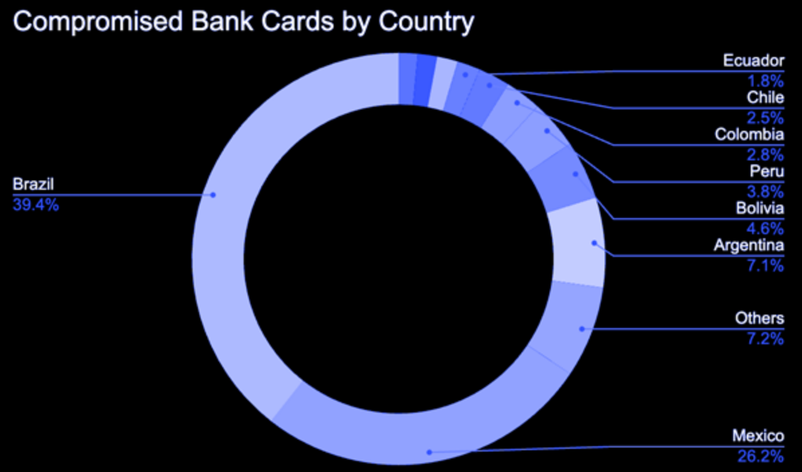
ESTADÍSTICAS: DATOS COMPROMETIDOS

Los *stealers* 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 cibersecuestro (*ransomware*), extorsión y espionaje. A las cuentas válidas, es decir, las credenciales filtradas por *stealers* 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 más activas en la región.







TENDENCIAS REGIONALES
Percepciones del CERT: América Latina

Breve descripción de las tendencias regionales:

01 El CERT de Group-IB identificó una ola de estafas relacionadas con préstamos falsos en Brasil, con las que los estafadores utilizan anuncios engañosos en los que participan figuras públicas para hacerse pasar por bancos e instituciones financieras

Group-IB descubrió una nueva estafa en Brasil en la que los estafadores utilizan anuncios falsos de Facebook para engañar a las personas. En estos anuncios, se muestran fotos de personas famosas para hacerlas parecer reales, y se prometen préstamos fáciles. Cuando una persona hace clic en el anuncio, la dirigen a una página de chat falsa que parece profesional. Una vez allí, se le pide que comparta datos profesionales, como su CPF (Cadastro de Pessoa Física), con el pretexto de solicitar un préstamo, pero la verdadera intención es obtener su información personal de manera ilegal

02 Group-IB CERT detectó un esquema de phishing que utiliza campañas de SMS dirigidas a bancos y servicios de telecomunicaciones colombianos

Group-IB detectó un nuevo esquema fraudulento que comienza con un SMS dirigido a usuarios en Colombia. El mensaje ofrece un 50 % de descuento en servicios móviles y contiene un enlace abreviado que conduce a una página de pago falsa que imita la de un operador móvil conocido. En la página, se solicita el número de teléfono y el tipo de servicio. Se aceptan solo números específicos, y se muestra información de facturación falsa. Luego se solicita a los usuarios que realicen pagos a través de diversas plataformas — que tienen una interfaz adaptada a parecerse a los servicios bancarios en línea y a los sistemas de pago locales más populares — con el fin de robarles credenciales de inicio de sesión y datos de autenticación de dos factores

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 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:

TENGA CUIDADO CON LOS ANUNCIOS FALSOS

Verifique siempre la autenticidad de los canales de contacto. Para ello, visite el sitio oficial de su banco o póngase en contacto con su servicio oficial de atención al cliente

EVITE COMPARTIR INFORMACIÓN PERSONAL

Nunca brinde información personal confidencial — como su número de identificación o sus datos bancarios — en sitios web o páginas de chat que parezcan sospechosos o extraños

VERIFIQUE LA LEGITIMIDAD DE LAS OFERTAS DE PRÉSTAMOS

Antes de solicitar préstamos o cualquier servicio financiero, verifique la legitimidad de la empresa. Para ello, visite su sitio web oficial o póngase en contacto con ella a través de los canales oficiales

VERIFIQUE LOS MENSAJES SMS

Controle dos veces la autenticidad de los mensajes SMS que ofrecen ofertas o descuentos. Si le generan dudas, póngase en contacto directamente con la empresa a través de los canales de comunicación conocidos

UTILICE MÉTODOS DE PAGO QUE SEAN SEGUROS

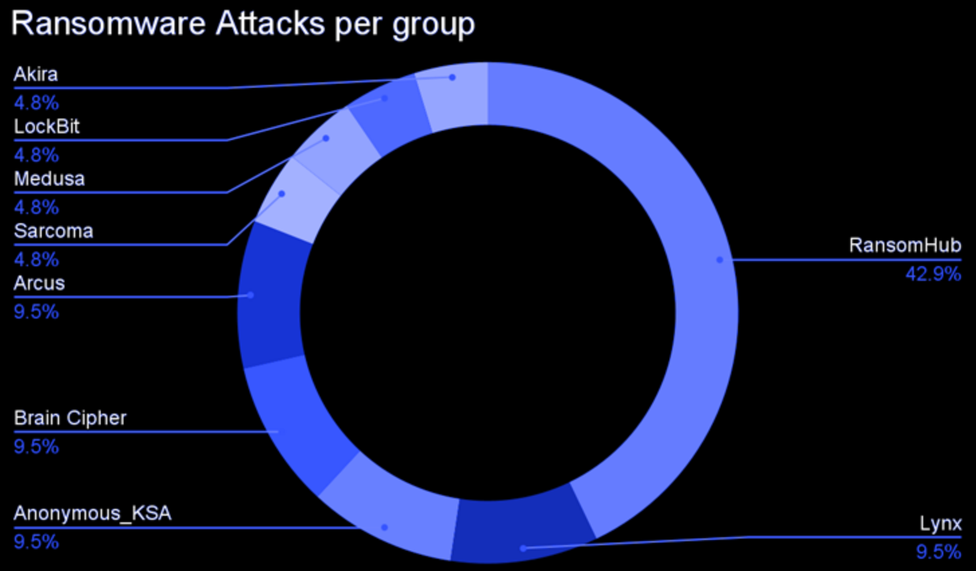
Utilice solamente métodos de pago seguros y confiables cuando realice transacciones en línea. Evite ingresar información confidencial en sitios web desconocidos o sospechosos

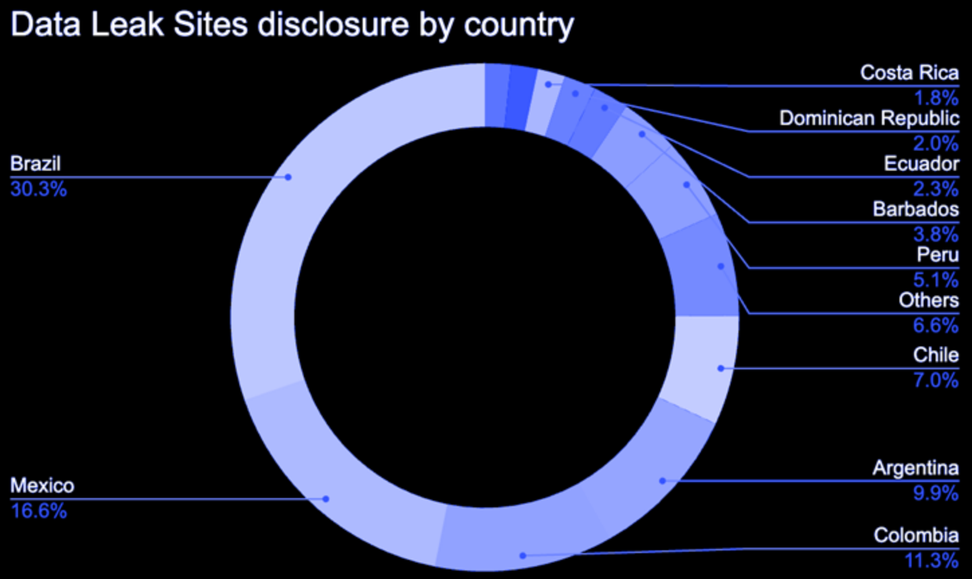
HABILITE LA AUTENTICACIÓN DE DOS FACTORES

Habilite la autenticación de dos factores (2FA) en sus cuentas, especialmente para plataformas bancarias o de pago, a fin de agregar otra capa de seguridad

ESTADÍSTICAS: **ATAQUES**
ACTIVIDADES DE CIBERSECUESTRO

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 América Latina (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 EN RELACIÓN CON INCIDENTES Y AMENAZAS EN LATAM

Breve descripción de los aspectos destacados clave a nivel regional:

01 Group-IB identifica el nuevo troyano de acceso remoto para Android BT-MOB, promovido por GhostSpy en Telegram.

El 14 de diciembre de 2024 se anunció en el grupo de Telegram de GhostSpy un nuevo troyano de acceso remoto para Android llamado **BT-MOB**. Según el anuncio, escrito en portugués, BT-MOB funciona en Android 7 a 13 y tiene la capacidad de eludir Play Protect. Al igual que la mayoría de los RAT de Android, para poder tener un control remoto completo del dispositivo infectado, BT-MOB requiere que esté habilitada la accesibilidad.

Hasta el momento, Group-IB no ha detectado ninguna campaña maliciosa para diseminar este programa malicioso.

02 Robo de tarjetas de crédito mediante la explotación de aplicaciones web.

El equipo de inteligencia de amenazas de Group-IB atribuyó recientemente una tienda de Telegram a un actor de amenazas, que previamente había estado activo como corredor de acceso en los foros clandestinos XSS y RAMP.

Después de que se bloquearan sus cuentas en estos foros, comenzó a publicar en Facebook y Telegram tarjetas de crédito supuestamente robadas, mediante el mismo método que utilizó para obtener acceso inicial a las empresas: explotación de aplicaciones web.

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 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 BT-MOB, 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 mayoría 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

EXPLOTACIÓN DE APLICACIONES WEB

Los delincuentes que se dedican al fraude pueden terminar explotando las vulnerabilidades de los comercios electrónicos y las tiendas en línea. Con el fin de mitigar este tipo de amenazas, es importante estar al tanto de OWASP Top Ten y OWASP API Security Top 10

TARJETA DE CRÉDITO VIRTUAL

Para realizar compras en línea, utilice únicamente tarjetas de crédito virtuales, ya que usan números que se generan de forma aleatoria y ocultan la información real de su tarjeta. Además, puede crear diferentes tarjetas para poder identificarlas mejor en caso de que se filtren datos

HABILITAR 3D SECURE

Los titulares de tarjetas, así como los comercios electrónicos, deberían habilitar 3D Secure, como MasterCard SecureCode, Verified by Visa y American Express SafeKey para contar con una verificación adicional, a fin de reducir la actividad fraudulenta

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