GROUP-IB

Febrero de 2025

América Latina

PERSPECTIVAS DE INTELIGENCIA

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 Chile, que se dirige a los usuarios mediante mensajes de SMS con la intención de robarles datos personales y financieros.

El equipo de inteligencia de amenazas de Group-IB descubrió cientos de archivos LNK que se utilizaron en una campaña reciente del troyano bancario Coyote que, al parecer, se difundió a través de WhatsApp y se dirigió a usuarios brasileños de Windows.

TENDENCIAS MUNDIALES

Breve descripción de las tendencias mundiales:

01 "The Dark Side of Automation and Rise of AI Agents: Emerging Risks of Card Testing Attacks" (El lado oscuro de la automatización y el auge de los agentes de la IA: riesgos emergentes de los ataques de prueba de tarjetas) por Group-IB

Group-IB analiza con mayor detenimiento la manera en que los criminales informáticos están aprovechando la automatización avanzada y las tecnologías de IA para llevar a cabo ataques de prueba de tarjetas. En ataques de este tipo, los estafadores utilizan información de tarjetas de crédito robadas para realizar compras pequeñas, que a veces pasan inadvertidas, con el fin de verificar la validez de la tarjeta antes de llevar a cabo transacciones fraudulentas más grandes. Los atacantes suelen aprovechar bots, *proxies* y herramientas de automatización para probar grandes cantidades de tarjetas de manera eficiente sin que los puedan detectar. En este artículo, se hace hincapié en los desafíos que esto plantea para la prevención del fraude en tiempo real, y se subraya la necesidad de contar con sistemas de detección avanzados que permitan identificar y mitigar estas amenazas automatizadas.
Leer más

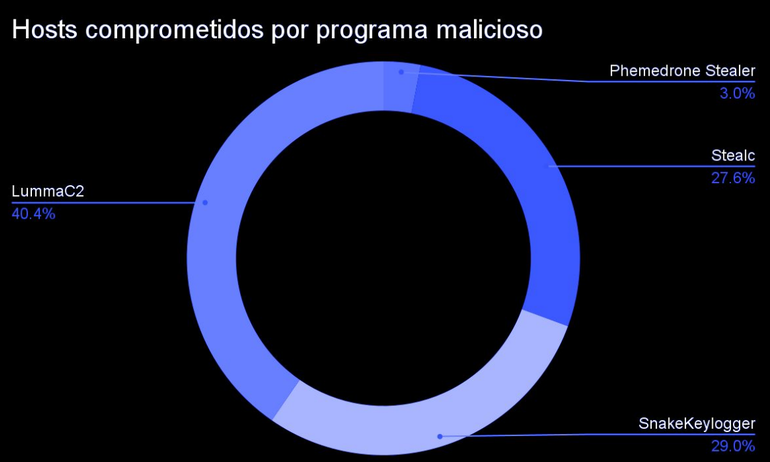
02 Group-IB publicó una entrada de blog sobre el grupo de *ransomware* RansomHub

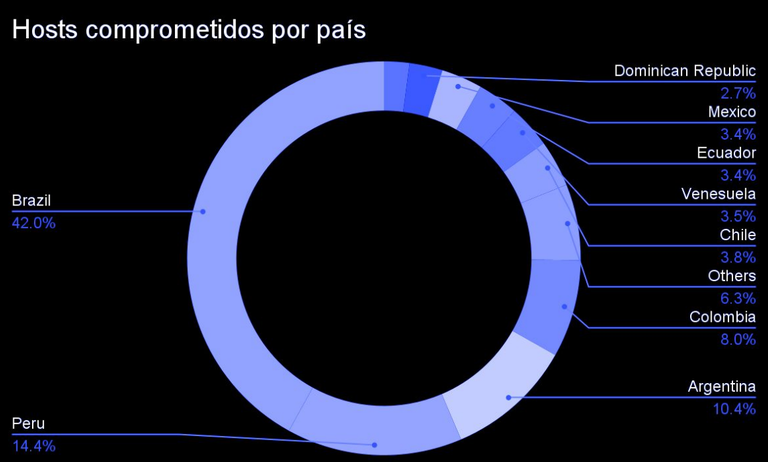
En esta entrada de blog de Group-IB, se analiza la emergencia de RansomHub, un grupo de *ransomware* como servicio (RaaS) que surgió a comienzos de 2024. RansomHub capitalizó las medidas de aplicación de la ley que se tomaron contra grupos como LockBit y ALPHV para reclutar afiliados y adquirir el código fuente del *ransomware* del extinto grupo Knight. Su *ransomware* es versátil y ataca a diversos sistemas operativos, entre los que se incluyen Windows, ESXi, Linux y FreeBSD. Cabe destacar que RansomHub ha afectado a más de 600 organizaciones en todo el mundo y muestra un interés significativo en el sector de la atención sanitaria. En el artículo se destaca el nivel de adaptabilidad del grupo así como el carácter evolutivo de las amenazas de *ransomware*.
Leer más

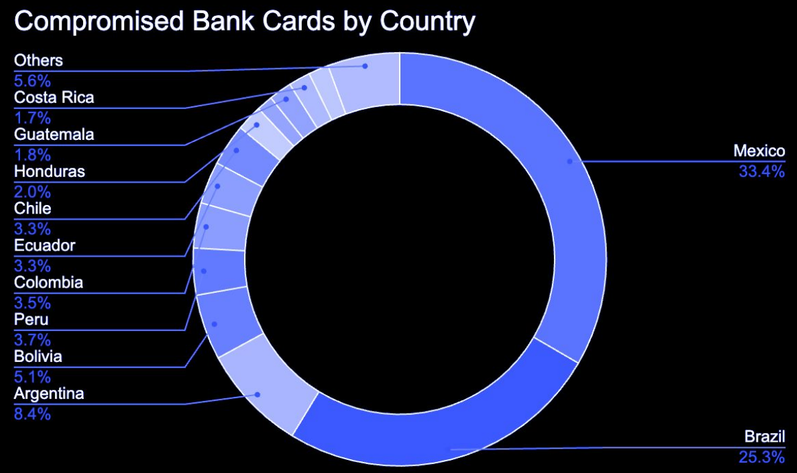
ESTADÍSTICAS: **DATOS COMPROMETIDOS**

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 *ransomware* (cibersecuestro), 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 que están más activas en la región.







TENDENCIAS REGIONALES
Percepciones del CERT: América Latina

Breve descripción de las tendencias regionales:

01	El CERT de Group-IB ha identificado una nueva estafa de *phishing* en Chile, que se dirige a los usuarios mediante mensajes de SMS con la intención de robarles datos personales y financieros.	El CERT de Group-IB ha identificado una estafa de *phishing* en Chile donde los ciberdelincuentes envían mensajes SMS a los usuarios, haciéndose pasar por empleados de empresas legítimas. En estos mensajes, se les anuncia a los usuarios que tienen puntos que están por vencer y que pueden canjearse por premios. El SMS incluye un enlace que conduce a un formulario falso en el que se solicita información personal y financiera, con datos de tarjetas de crédito incluidos. Esta estafa se dirige, en primer lugar, a clientes de empresas proveedoras de servicios de telecomunicación en Chile.
02	El CERT de Group-IB ha detectado un esquema de *phishing* en Perú, en el que se hacen pasar por instituciones financieras para robar credenciales bancarias.	El CERT de Group-IB también ha identificado una estafa de *phishing* en Perú, por la que captan personas a través de procesos de solicitud de préstamos fraudulentos. Se les solicita a las víctimas que ingresen su número de DNI y datos de contacto, y luego se les pide que verifiquen su identidad mediante reconocimiento facial o información de tarjeta bancaria. La opción de reconocimiento facial se configura de forma tal que no funcione; de este modo, los usuarios se ven obligados a brindar datos de su tarjeta, contraseña de banca en línea y PIN. El plan se ha diseñado para recopilar solo credenciales válidas, que luego se utilizan para actividades fraudulentas. Al finalizar, se dirige a las víctimas a un sitio web bancario legítimo, sin que se den cuenta de que se han comprometido sus datos.

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:

VERIFIQUE LOS MENSAJES DIRECTAMENTE

Póngase en contacto con la empresa a través de los canales oficiales para confirmar cualquier oferta promocional antes de hacer clic en algún enlace

NO HAGA CLIC EN ENLACES ENVIADOS POR SMS

No abra enlaces que lleguen dentro de mensajes no solicitados, especialmente aquellos que mencionan una urgencia o premios

REVISE CON CUIDADO LA URL

Los sitios web fraudulentos pueden parecer legítimos, pero a veces tienen pequeñas diferencias en el nombre de dominio

DENUNCIE LOS MENSAJES SOSPECHOSOS

Reenvíe los SMS de *phishing* a las autoridades de ciberseguridad locales o a su proveedor de servicios, para ayudar a prevenir más ataques

TENGA CUIDADO CON LAS SOLICITUDES DE PRÉSTAMOS

Solicite préstamos únicamente a través de canales oficiales y evite las ofertas que no haya solicitado y que le pidan información personal

HABILITE LA AUTENTICACIÓN DE DOS FACTORES

Proteja sus cuentas con 2FA para reducir el riesgo de accesos no autorizados

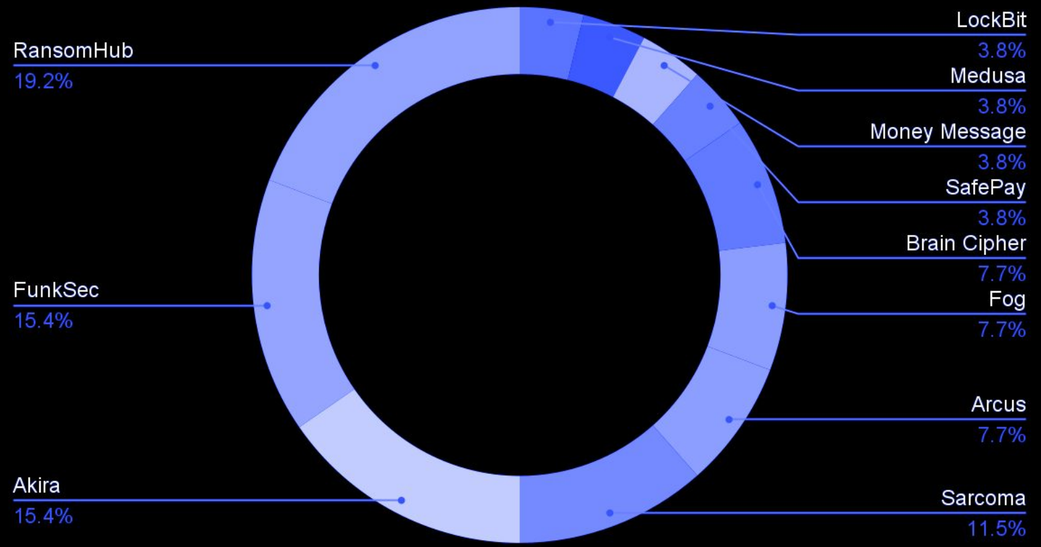
ESTADÍSTICAS: **ATAQUES**

ACTIVIDADES DE *RANSOMWARE* Y EXTORSIÓN

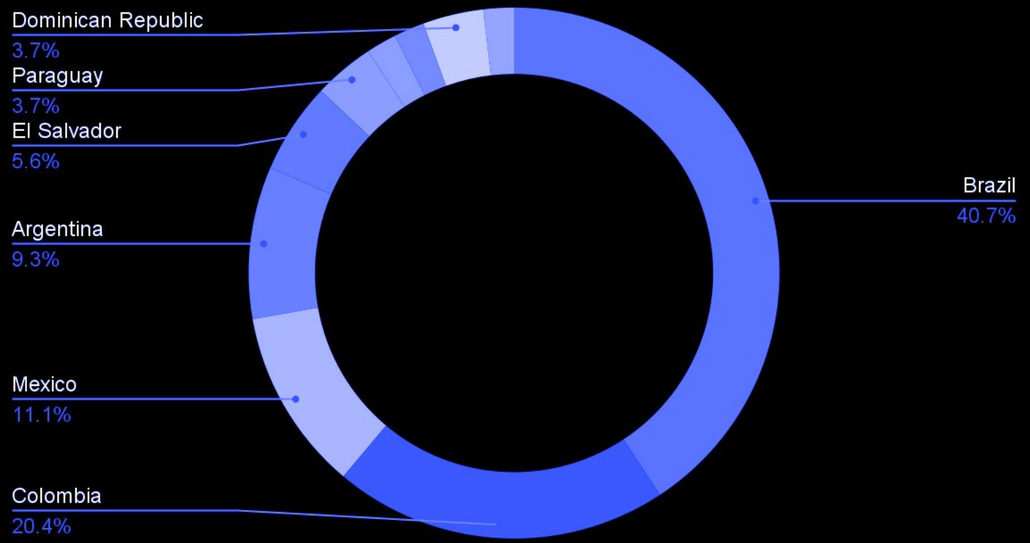
Este mes observamos que aumentó **de 26 a 54** la cantidad de empresas divulgadas en sitios de filtración de datos (DLS), en el marco de operaciones de extorsión y *ransomware.*

Akira, una presunta operación de *ransomware* basada en Conti, fue el grupo que más divulgaciones realizó en la región de LATAM, con seis empresas de Brasil, dos de Argentina y dos de Colombia.

Ataques de ransomware por grupo:



Divulgación de sitios de filtración de datos por país



HECHOS DESTACADOS SOBRE INCIDENTES Y AMENAZAS EN LATAM

Hechos destacados a nivel regional con una breve descripción:

01 Group-IB detectó una campaña maliciosa que difundía el troyano bancario Coyote.

El equipo de inteligencia de amenazas de Group-IB se enteró de una reciente campaña maliciosa destinada a robar datos confidenciales de usuarios brasileños de Windows: se los infectaba con una nueva versión del programa malicioso Coyote que se distribuía aparentemente a través de WhatsApp.

El proceso de infección comienza cuando la víctima ejecuta un archivo LNK que simula ser un *comprovante* (confirmación de pago), que a su vez ejecuta un PowerShell para descargar la siguiente etapa de la amenaza.

02 Actividad sospechosa referida a la evasión de la solución de seguridad móvil Appdome.

Los especialistas de Group-IB detectaron a aparentes delincuentes brasileños que buscan un servicio, o bien a una persona, que pueda eludir los mecanismos de seguridad de aplicaciones móviles protegidas con las soluciones antifraude de Appdome.

Los actores de amenazas han pedido ayuda en diferentes fuentes, como el foro Exploit, Facebook y un grupo de Telegram de fraude en idioma chino. En una de las publicaciones, un usuario de un foro compartió registros relacionados con “Caixa Tem”, lo que sugiere que esta podría ser una de las aplicaciones atacadas.

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

La mayoría de los troyanos bancarios que predominan en la región de LATAM, como Astaroth, Mispadu y Mekotio, presentan una cadena de infección de varias etapas que suele comenzar (pero sin limitarse a esto) con la ejecución de un archivo LNK malicioso

Campañas de correo basura malicioso

La mayoría de 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 en WhatsApp

Las instituciones financieras brasileñas que figuran en la lista de objetivos de Coyote no se comunican por WhatsApp con los titulares de cuentas para enviar documentos. No abra ningún archivo supuestamente enviado por su banco que le llegue por WhatsApp

Habilite 2FA y Registrato

Habilite siempre 2FA en todas las cuentas bancarias y aplicaciones de Internet que tenga, y controle periódicamente las cuentas bancarias que tenga asociadas en el sistema BACEN Registrato

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

HABILITE 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, con el fin de reducir la actividad fraudulenta

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