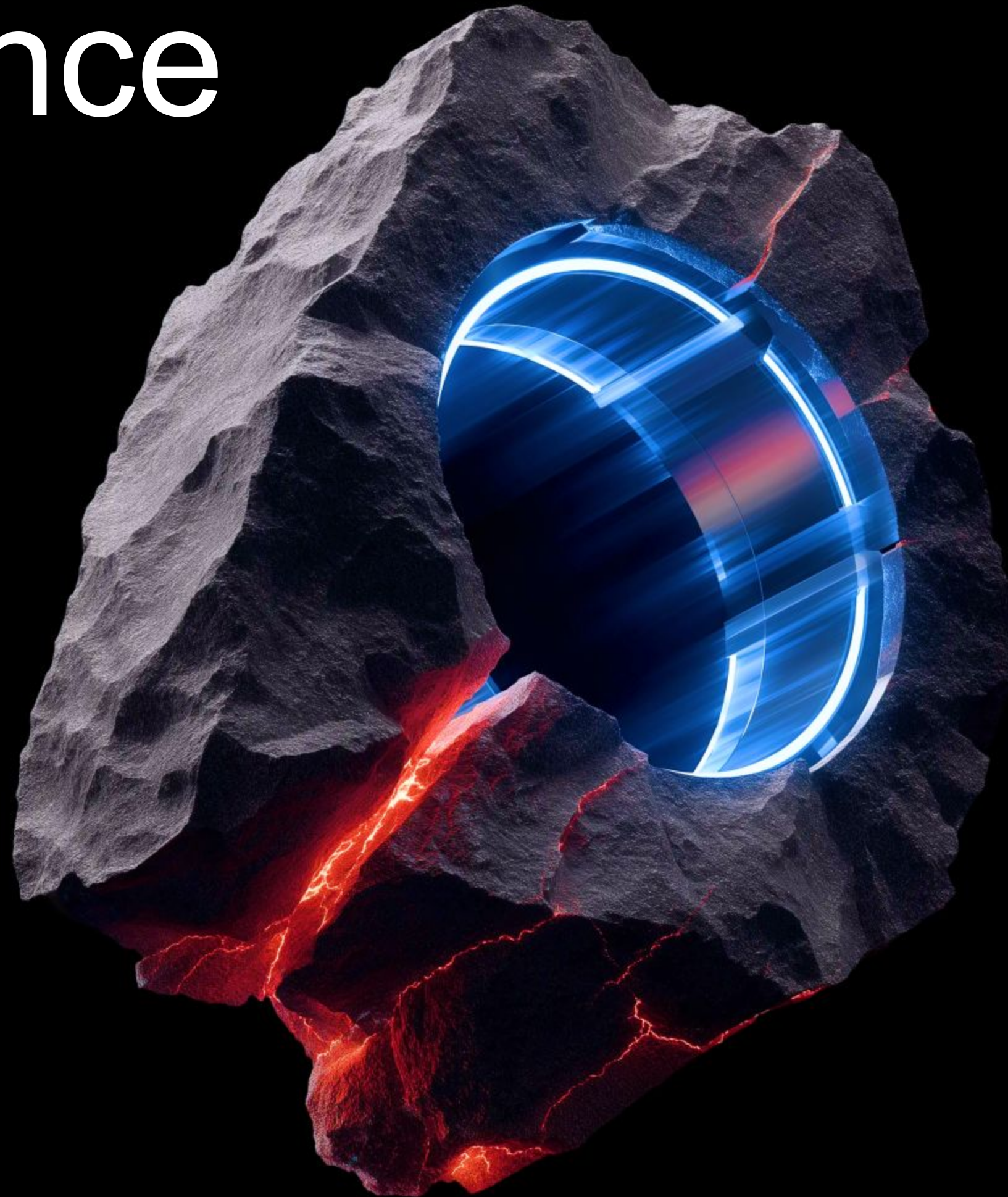


Intelligence Insights Report

Q1, 2026

Latin America



Principales Eventos del Último Trimestre

Este informe contiene información sobre los eventos de ciberseguridad más significativos que ocurrieron a nivel mundial y en América Latina durante el último trimestre.

2

eventos más destacados



Mexico: Group-IB CERT identificó sitios web que suplantaban a bancos mexicanos bajo la apariencia de soporte TI, diseñados para manipular a los usuarios mediante ingeniería social e inducirlos a instalar Remote Utilities, permitiendo así el acceso remoto no autorizado.



Brazil: Desde septiembre del 2025, ciudadanos brasileños han sido objeto de campañas maliciosas agresivas que distribuyen malware a través de WhatsApp con el objetivo de robar información financiera de los titulares de cuentas bancarias para sustraer fondos. (Since September 2025)

Algunos de los troyanos bancarios distribuidos en estas campañas

ASTAROTH

CABANEIRO

COYOTE

Global Insights

Tendencias globales con una pequeña descripción

01



Stranger Threats Are Coming: Predicciones de Ciberseguridad de Group-IB para 2026 y más allá

Explore nuestras predicciones estratégicas sobre el panorama de amenazas cibernéticas en 2026, con foco en ataques autónomos, malware impulsado por IA, extorsión agéntica, amenazas AIM y explotación de criptomonedas y stablecoins mediante IA, y su impacto en las organizaciones a nivel global. El análisis se basa en investigación anual propia, analítica avanzada, principales eventos del sector y colaboración con expertos.

[Click for more information](#)

02



Ghosts in /proc: Manipulación y corrupción de líneas de tiempo

Descubra cómo los actores de amenazas abusan del sistema de archivos /proc en Linux para ocultar actividad maliciosa y alterar cronologías forenses. Este análisis aborda técnicas como la suplantación de línea de comandos, la manipulación del tiempo de inicio de procesos y las medidas prácticas de detección y mitigación que los equipos de defensa deben conocer e implementar.

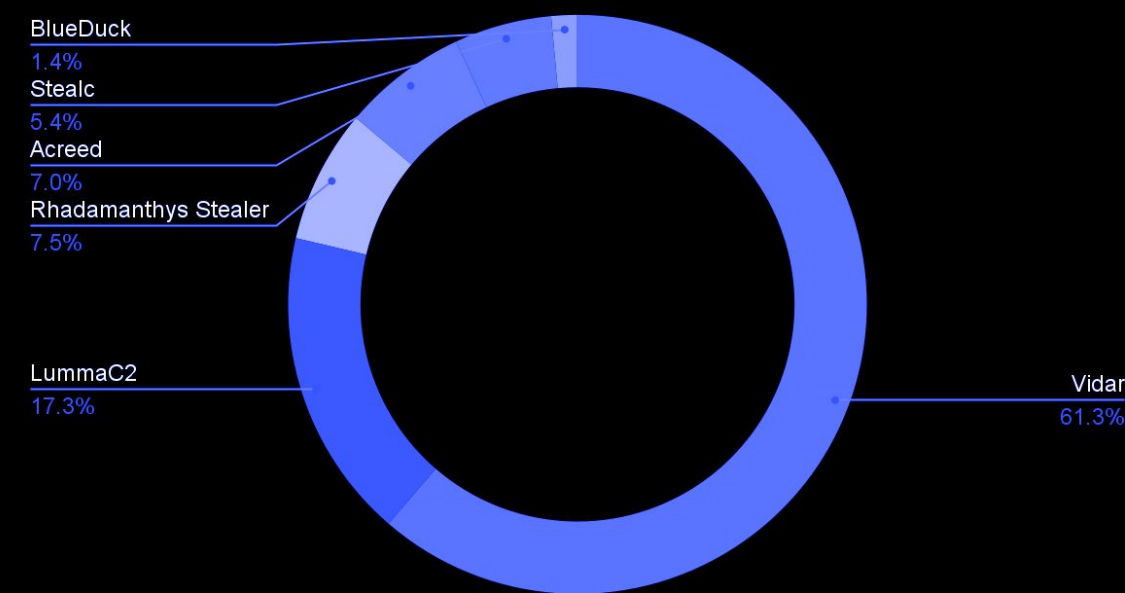
[Click for more information](#)

Estadísticas. Datos comprometidos

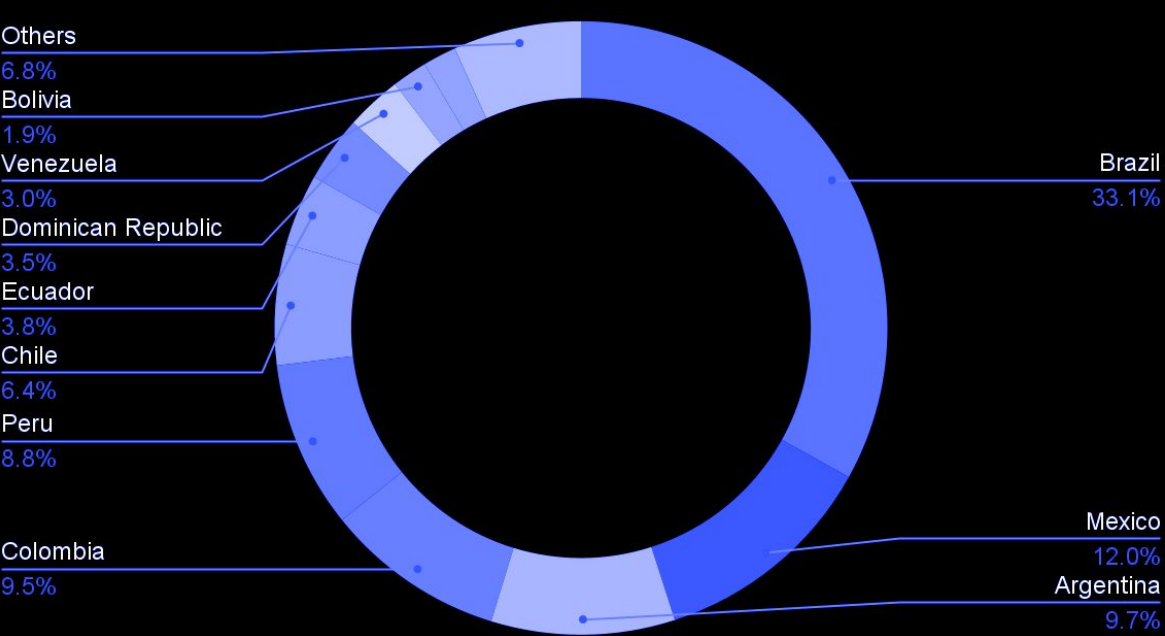
Los *stealers* desempeñan un papel clave en la cadena de suministro del cibercrimen, ya que los datos robados de los equipos infectados por este tipo de malware pueden derivar en incidentes de mayor impacto, como ransomware, extorsión y espionaje. Las cuentas válidas —es decir, las credenciales exfiltradas por *stealers*— son comúnmente utilizadas por actores de amenazas para obtener acceso inicial a las organizaciones, así como para escalar privilegios y evadir mecanismos de defensa.

En esta sección del informe presentamos estadísticas sobre equipos infectados y tarjetas comprometidas, lo que permitirá identificar qué familias de malware son las más activas en la región.

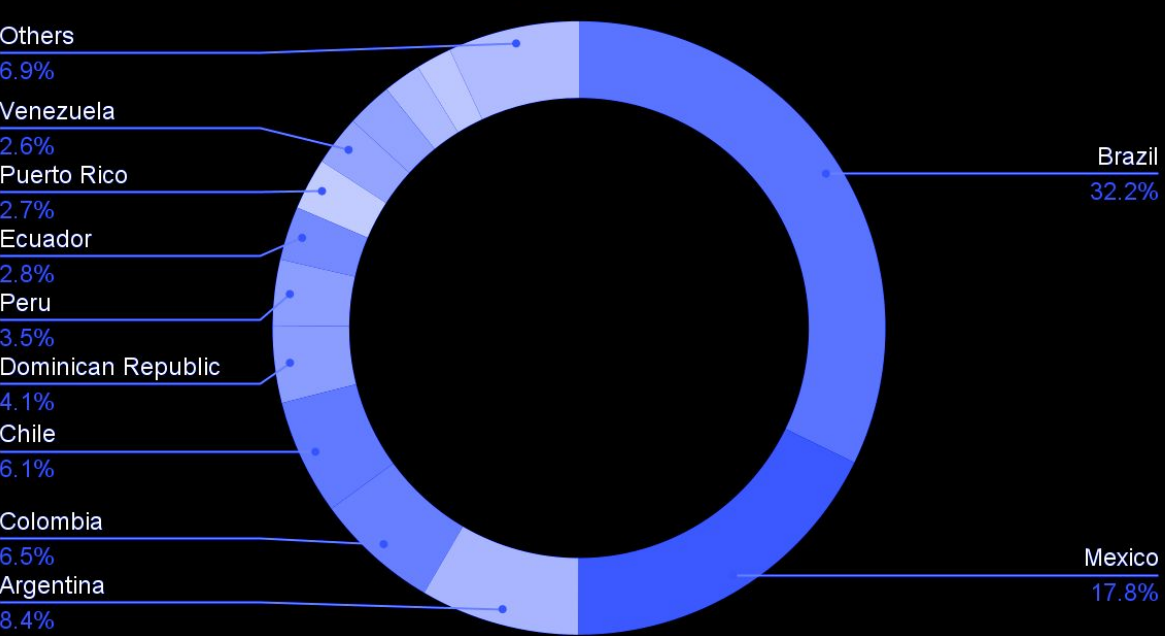
Compromised hosts by malware



Compromised hosts by country



Compromised Bank Cards by Country



Insights Regionales - CERT

Tendencias regionales claves con una breve descripción

01

Campaña de smishing y phishing a gran escala en LATAM con técnicas avanzadas de evasión

Esta campaña identificada por el equipo de Group-IB CERT utiliza SMS localizados y URLs acortadas para suplantar marcas de confianza y robar datos personales y de tarjetas de pago, mientras evade mecanismos de detección.

Aunque la operación apunta a marcas a nivel global, los ataques afectan principalmente a Chile, Colombia y México empleando vinculación por geolocalización y filtrado basado en el dispositivo, que devuelve un Error 524 cuando se accede a los recursos sin el user-agent móvil esperado, junto con infraestructura proxy detrás de CDN para evadir la detección.

02

Suplantación de páginas web bancarias mexicanas bajo la apariencia de soporte técnico de TI, utilizando la ingeniería social para manipular a los usuarios y habilitar el acceso remoto no autorizado en sus dispositivos.

El equipo de Group-IB CERT observó páginas falsas de soporte técnico que imitaban a bancos mexicanos, donde se instruía a las víctimas a descargar e instalar **Remote Utilities**, una herramienta legítima de monitoreo y gestión remota (RMM).

La campaña se basa en técnicas de ingeniería social, en lugar de phishing tradicional, con el objetivo de obtener acceso remoto a los dispositivos de las víctimas y facilitar el compromiso de credenciales y el robo de fondos. Los instaladores se descargan directamente desde el sitio web oficial de Remote Utilities, lo que obliga a los atacantes a convencer a las víctimas de compartir su ID de Remote Utilities para establecer la conexión remota.

Conclusiones y Recomendaciones

La evolución del panorama de amenazas representa riesgos significativos para su organización. Adopte medidas de seguridad sólidas, una gestión proactiva de amenazas y considere implementar las siguientes recomendaciones:



Reforzar la concienciación frente a ataques de smishing e ingeniería social

Educar a los usuarios para identificar campañas de smishing y fraudes de soporte técnico que imitan a marcas y entidades bancarias confiables.



Restringir el uso de herramientas de acceso remoto en los endpoints

Restringir la instalación y el uso de software de acceso remoto a herramientas aprobadas y prohibir aplicaciones de terceros iniciadas a partir de comunicaciones no solicitadas.



Verificar la autenticidad de los sitios web antes de introducir datos sensibles

Comprobar que el nombre de dominio sea correcto, validar el certificado SSL y detectar posibles inconsistencias en el diseño antes de ingresar cualquier información..



Implementar canales formales de reporte y gestión de incidentes

Asegurar que usuarios y clientes sepan cómo reportar mensajes sospechosos, páginas falsas de soporte y sitios de phishing para permitir una respuesta más rápida y limitar el impacto de campañas en curso.



Mejorar la detección del abuso de dominios y marca

Implementar monitoreo continuo para identificar el uso no autorizado de nombres de marca, logotipos y servicios en dominios, sitios web y contenido en línea.



Implementar autenticación multifactor (MFA)

Exigir el uso de MFA en todas las plataformas que involucren cuentas de usuario y sistemas de pago. Esta medida reduce el riesgo de accesos no autorizados en caso de que las credenciales se vean comprometidas.

Comentarios y recomendaciones para analistas

1. Las campañas identificadas aprovechan la suplantación de marca y el software legítimo de Monitoreo y Gestión Remota (RMM) para obtener acceso remoto directo a los dispositivos de las víctimas, evitando el despliegue tradicional de malware y reduciendo significativamente indicadores técnicos detectables.
2. Las páginas maliciosas presentan marcadores técnicos consistentes que permiten su detección y agrupamiento, entre ellos:
 - Parámetro clave en HTML: `kyop.ntcsh.i.title.rvsInvk.ntCsh`
 - Referencia a iframe incrustado: `guia.html`
 - Reutilización de recurso de imagen: `aea069a17a1cad19aa3b12dc8f419187.png`
(SHA256 : 697d7845b68672bc4d8cdaa2ead4a4d624cf9cc7aa7c83ebb0e4a290f055b229)

Estos patrones recurrentes permiten la identificación de la infraestructura más allá de los indicadores basados únicamente en dominios.

Evaluamos esta actividad como un modelo de acceso remoto de bajo ruido, basado en ingeniería social, que combina herramientas administrativas legítimas con la suplantación de marcas financieras. Este enfoque complica la detección tradicional de phishing y requiere la detección temprana basada en patrones HTML sospechosos y la rápida interrupción de dominios maliciosos.

Estadísticas — ataques

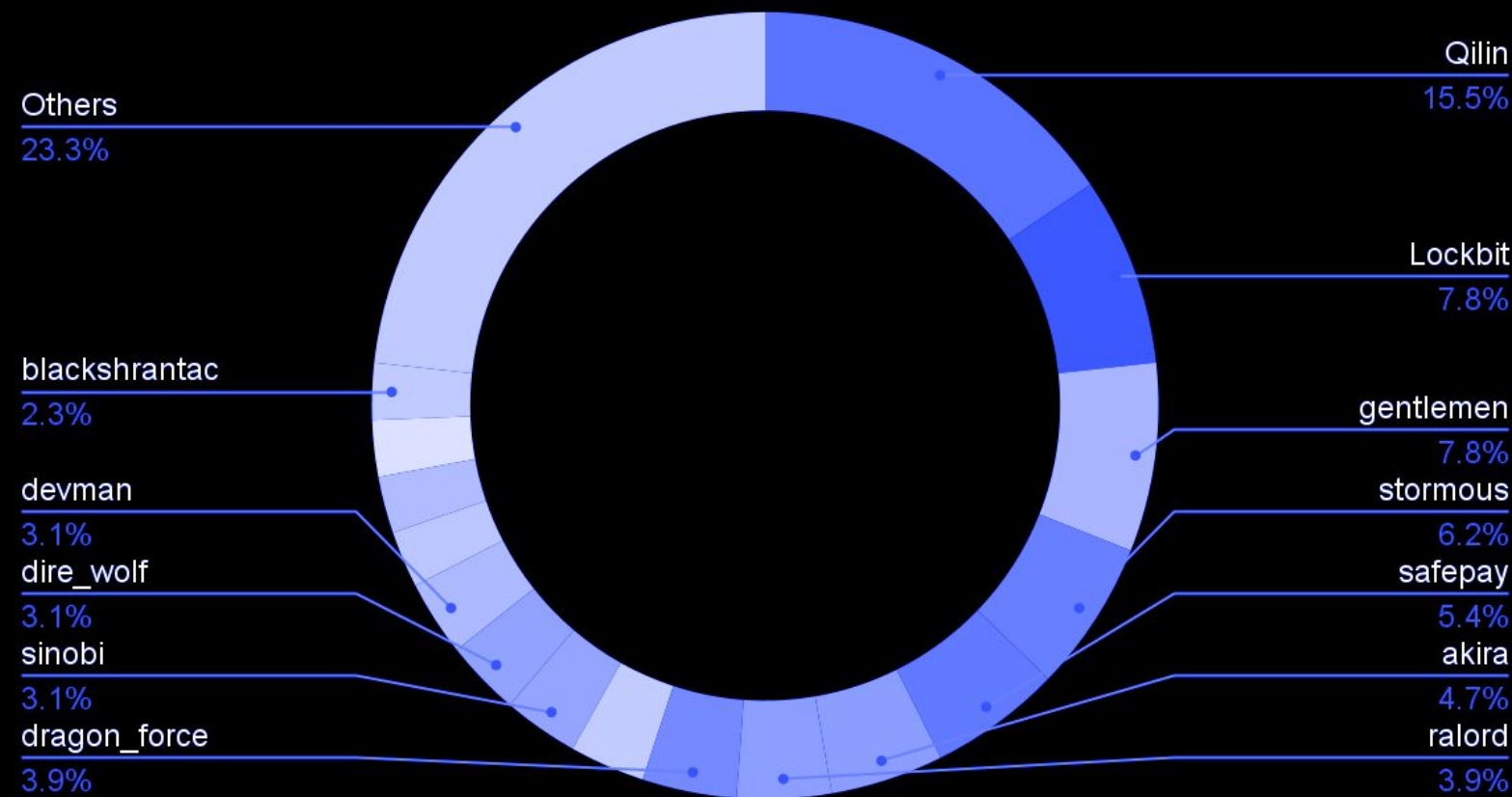
Actividades de ransomware & Extorsión

En los últimos tres meses, **Qilin**, **LockBit** y **The Gentlemen** fueron los grupos de *Ransomware-as-a-Service* (RaaS) que más empresas de América Latina publicaron en sus sitios de filtración de datos (DLS, *Data Leak Sites*).

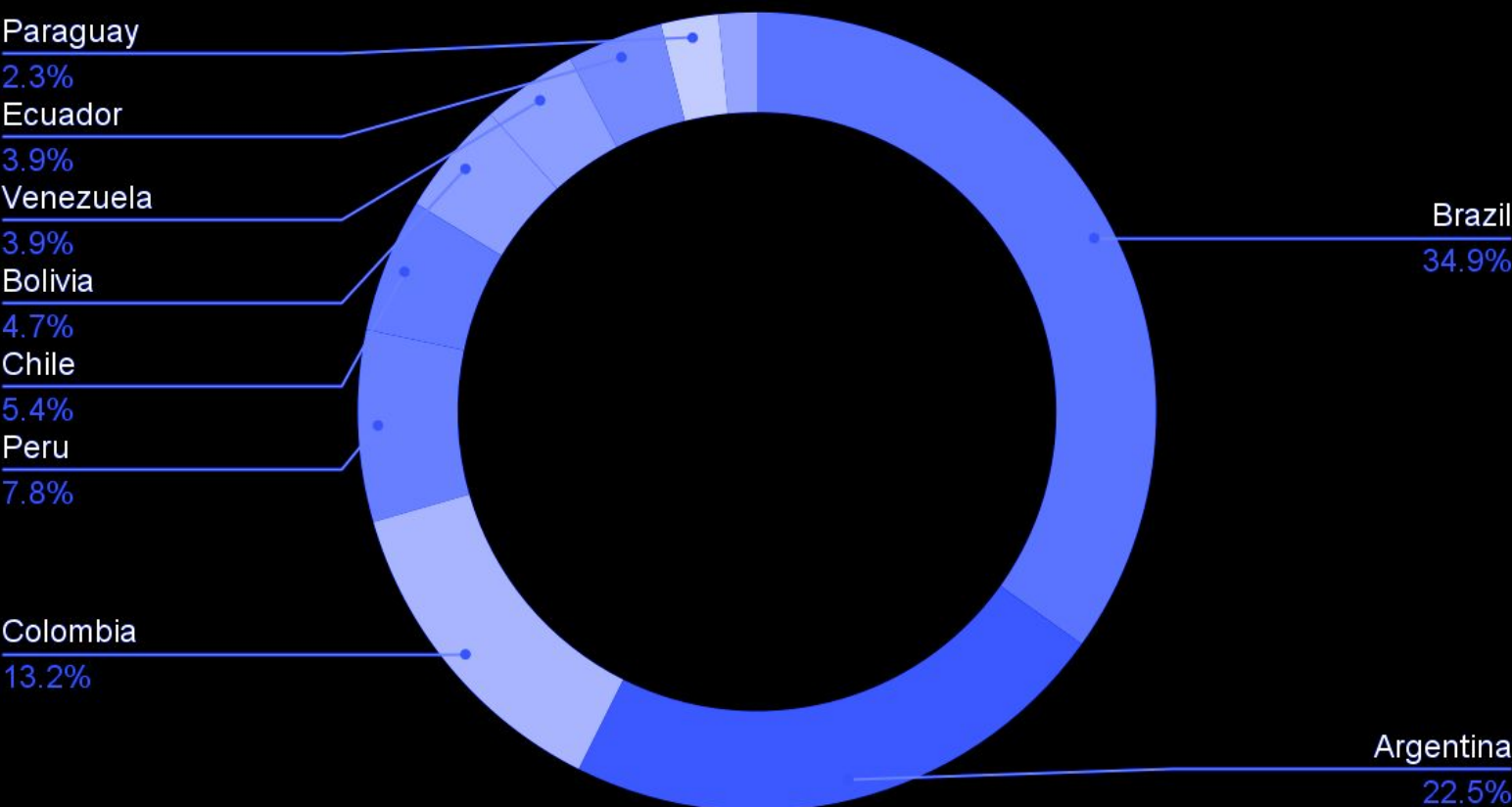
Aunque **The Gentlemen** es un grupo RaaS que surgió en julio de 2025, ha reivindicado un número significativo de ataques contra compañías en e la región. Por este motivo, y con base en TTPs, evaluamos que este grupo representa un **riesgo medio** para las organizaciones de la región.

Entre sus principales TTPs se incluyen: Explotación de vulnerabilidades en dispositivos Fortinet y ataques de fuerza bruta contra credenciales para obtener acceso inicial; uso de la técnica **BYOVD (Bring Your Own Vulnerable Driver)** para evadir soluciones AV/EDR; empleo de **Rclone** para la exfiltración de datos, entre otras técnicas.

Disclosures by group - LATAM



DLS disclosure by country



Incidentes y amenazas destacadas en LATAM

Hallazgos regionales clave con una pequeña descripción

01

Distribución de troyanos bancarios a través de WhatsApp en Brasil

Desde septiembre de 2025, ciudadanos brasileños han sido objetivo de campañas maliciosas agresivas que distribuyen malware a través de WhatsApp con el fin de robar información financiera de titulares de cuentas bancarias y sustraer fondos. Además, los archivos maliciosos distribuidos durante el proceso de infección incorporan capacidades de autopropagación, lo que permite a los ciberdelincuentes secuestrar sesiones de WhatsApp Web y utilizarlas para continuar la distribución del malware.

Se han detectado al menos tres troyanos bancarios: **Coyote**, **Astaroth** y **Casbaneiro**. Aunque presentan grandes similitudes, existen ligeras diferencias en sus cadenas de infección, lo que sugiere que las campañas fueron llevadas a cabo por distintos grupos o actores criminales.

02

Extensión maliciosa Jaguarundi para Chrome

La inteligencia de amenazas de Group-IB detectó la distribución de una extensión maliciosa a través de campañas de *malspam* dirigidas a ciudadanos de Portugal, España, Chile y, especialmente, Brasil.

Identificada como **Jaguarundi**, la extensión cuenta con las siguientes capacidades: captura de pantallas, exfiltración de información de pestañas del navegador, exfiltración de cookies, *localStorage* y *sessionStorage*, inyección de HTML y captura manual de entradas del usuario.

Los equipos infectados son controlados por los ciberdelincuentes mediante un sistema basado en la web conocido como “**Painel Gangster**” o “**Painel de Monitoramento**”.

Conclusiones y Recomendaciones

Los incidentes analizados en este informe subrayan la necesidad de contar con medidas de seguridad sólidas y una gestión proactiva de amenazas. Para proteger su organización, considere implementar las siguientes recomendaciones:



Implementar autenticación multifactor (MFA)

Exigir la autenticación multifactor (MFA) en todos los sistemas, como WhatsApp, cuentas de correo electrónico y servicios financieros. Esta medida añade una capa adicional de protección y ayuda a prevenir accesos no autorizados, incluso si las credenciales han sido comprometidas.



Capacitar a los empleados sobre ataques de phishing

Para que puedan identificar intentos de phishing, especialmente en áreas como finanzas, TI y marketing. El personal debe estar alerta ante tácticas como páginas de inicio de sesión falsas y sitios de phishing que imitan marcas legítimas.



Evitar el uso de sms como método de 2FA

Por diversas razones, no es recomendable utilizar SMS como método de autenticación en dos factores (2FA). Por ello, siempre que sea posible, es preferible usar aplicaciones de autenticación, tokens de hardware o, al menos, verificación por correo electrónico.



Reportar de inmediato mensajes sospechosos

Si recibe un correo electrónico o mensaje que parezca inusual o solicite información personal, repórtelo al equipo de TI o directamente a la empresa. No responda al mensaje.



Revisar sus cuentas periódicamente

Revise regularmente sus cuentas bancarias y de correo electrónico para detectar cualquier actividad inusual. Si identifica algo sospechoso, repórtelo de inmediato para proteger su información.



No confíe en mensajes inesperados

Desconfíe de comportamientos inusuales, incluso si el mensaje proviene de un contacto conocido. En lugar de descargar o ejecutar archivos, verifique la información directamente con la persona que le envió el mensaje sospechoso.

Comentarios y recomendaciones para analistas

1. Es ampliamente conocido que los troyanos bancarios y Troyanos de Acceso Remoto (RATs) para Android son amenazas predominantes en los países de habla hispana y portuguesa, especialmente en aquellos ubicados en América del Sur.
2. Los troyanos bancarios, incluidos Grandoreiro, Ousaban y Astaroth, se distribuyen principalmente — aunque no exclusivamente — a través de correo electrónico (campañas de malspam), mientras que el malware móvil como BTMOB y PhantomCard suele propagarse mediante Google Play Store, páginas de phishing, malvertising y campañas de smishing.
3. En 2023 y 2025 observamos cambios significativos en el panorama de amenazas en LATAM: el aumento en el uso de software de Monitoreo y Gestión Remota (RMM), la proliferación de extensiones maliciosas de navegador basadas en Chrome, así como la distribución de troyanos bancarios a través de WhatsApp.
4. Aunque actualmente nuevas familias de malware y técnicas forman parte del panorama de amenazas en LATAM, los ciberdelincuentes siguen recurriendo a la ingeniería social para alcanzar su objetivo: infectar equipos con malware para el robo de dinero y criptomonedas.

Por ello, destacamos la importancia de brindar capacitación periódica en ingeniería social a los empleados, especialmente a los equipos financieros, con el fin de reducir la probabilidad de que hagan clic en enlaces maliciosos que puedan provocar la infección de sus equipos.

INVESTIGATING, PREVENTING AND FIGHTING CYBERCRIME SINCE 2003