

Reporte IBM: ransomware persistió como el tipo más común de ataque en América Latina en 2021

Entre los hallazgos, las credenciales robadas continúan siendo un problema en la región, el tiempo de vida promedio de los grupos de ransomware es de 17 meses y vishing triplica la tasa de clics de phishing.

América Latina experimentó un aumento del 4% en ciberataques en 2021 en comparación con el año anterior. Brasil, México y Perú fueron los países más atacados en la región en 2021.



CAMBRIDGE, Mass., 23 de febrero de 2022- IBM (NYSE: [IBM](#)) Security publicó hoy su informe anual [X-Force Threat Intelligence Index](#) mostrando cómo el ransomware, e-mails corporativos comprometidos y el robo de credenciales pudieron "aprisionar" a las empresas en Latinoamérica en 2021, agobiando aún más sus cadenas de suministro. Aunque el phishing fue la causa más común de ciberataques en general en la región en el último año, IBM Security X-Force observó un aumento en los ataques provocados por credenciales robadas, un punto de entrada en el que los actores se basaron más para llevar a cabo sus ataques en 2021, representando la causa de 29% de los ciberataques en la región.

El IBM Security X-Force Threat Intelligence Index 2022 identifica las nuevas tendencias y patrones de ataques que IBM Security ha observado y analizado a partir de sus datos – extraídos de miles de millones de *datapoints* que van desde dispositivos de detección de red y *endpoints*, acciones de respuesta a incidentes, seguimiento de kits de phishing y más, incluyendo datos proporcionados por [Intezer](#). Algunos de los principales hallazgos del reporte de este año incluyen:

- **Manufactura, la columna vertebral de las cadenas de suministro, se vuelve la más atacada.** En Latinoamérica, la manufactura (22%) fue la industria más atacada en 2021, reflejando la tendencia global, ya que los ciberdelincuentes encontraron un punto de influencia en el papel crítico que las organizaciones manufactureras juegan en las cadenas de suministro mundiales para presionar a las víctimas a pagar un rescate. El sector mayorista y minorista (20%), y el financiero y de seguros (15%), siguieron a la manufactura como las industrias más atacadas en América Latina.
- **Bandas de ransomware desafían defensas.** El ransomware persistió como el principal método de

ataque observado en 2021, tanto globalmente como en Latinoamérica, representando el 29% de los ataques en América Latina, con grupos de ransomware sin mostrar signos de detenerse, a pesar del repunte en defensas contra el ransomware. Según el informe de 2022, el promedio de vida de una banda antes de cerrar o cambiar su marca es de 17 meses. REvil fue el tipo de ransomware más común que se observó, representando el 50% de los ataques que X-Force remedió.

- **Los ataques de compromiso de e-mails corporativos (BEC) tienen un nuevo objetivo.** La tasa de ataques del BEC contra América Latina es mayor que para cualquier otra geografía en todo el mundo, con un fuerte incremento del 0% en 2019 a 21% en 2021, y sugiriendo que los atacantes del BEC están poniendo una mayor atención en las organizaciones latinoamericanas como objetivos. Según el informe, el BEC fue el segundo ataque más común en la región.
- **Las vulnerabilidades siguen incrementándose:** El reporte de X-Force destaca el número récord de vulnerabilidades reveladas en 2021, sugiriendo que el desafío de gestionarlas persiste. Para las empresas de la región, las vulnerabilidades no corregidas o “parchadas” causaron aproximadamente el 18% de los ataques en 2021, exponiendo la mayor dificultad de las empresas: corregir las vulnerabilidades.
- **Señales de alerta temprana de ciber crisis en la nube.** Los ciberdelincuentes están sentando las bases para apuntar a los entornos en la nube, con el reporte revelando un aumento del 146% en el nuevo código de ransomware Linux y un cambio de enfoque apuntando a Docker a nivel mundial, lo que potencialmente hace que sea más fácil para más actores de amenazas aprovechar los entornos en la nube con fines maliciosos como el malware multi-plataforma y que puede ser utilizado como un salto de un punto hacia otros componentes de la infraestructura de sus víctimas.

"Los ciberdelincuentes suelen perseguir el dinero, ahora con el ransomware, tener la ventaja," dijo Charles Henderson, Líder de IBM X-Force. "Las empresas deben reconocer que las vulnerabilidades las están manteniendo en un bloqueo, ya que los actores de ransomware utilizan eso a su favor. Se trata de un reto no binario. La superficie de ataque es cada vez más grande, por lo que en lugar de operar bajo el supuesto de que cada vulnerabilidad en su entorno ha sido parcheada o corregida, las empresas deben operar bajo una suposición de estar comprometidas, y mejorar su gestión de la vulnerabilidad con una estrategia de confianza cero".

Los resultados adicionales del informe de 2022 incluyen:

- **Quien te llama por primera vez, puede hacer phishing hace mucho tiempo:** El phishing fue la causa más común de los ciberataques en el 2021 globalmente, y representando el 47% de los ataques X-Force remedió en América Latina. En las pruebas de penetración de X-Force Red, la tasa de clics de las campañas de phishing se triplicó cuando se combinó con llamadas telefónicas posteriores a sus víctimas.
- **Países más atacados en la región:** Latinoamérica experimentó un aumento del 4% en ciberataques en 2021 en comparación con el año anterior, con el reporte revelando que en 2021 Brasil, México y Perú fueron los países más atacados en la región.

El informe presenta datos que IBM recopiló a nivel mundial en 2021 para ofrecer información sobre el panorama de amenazas globales y comunicar a los profesionales de seguridad sobre las amenazas más relevantes para sus organizaciones. Para efectos del reporte, IBM considera que Latinoamérica incluye a México, Centroamérica y Sudamérica.

Puede descargar una copia del IBM Security X-Force Threat Intelligence Index [aquí](#).

Fuentes adicionales

- Inscribese en el webinar de IBM Security X-Force Threat Intelligence Index 2022, que ocurrirá el jueves 3 de marzo de 2022, a las 11:00 a.m. ET [aquí](#).
- Lea el blog de los autores del reporte para obtener más información sobre tres de los principales hallazgos, en el [blog IBM Security Intelligence](#).

Acerca de IBM Security

IBM Security ofrece un de los portfolios más avanzados e integrados de productos y servicios de seguridad empresarial. El portfolio, respaldado por la investigación de renombre mundial de IBM Security X-Force, permite a las organizaciones gestionar eficazmente el riesgo y defenderse de las amenazas emergentes. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo, monitorea más de 150 mil millones de eventos de seguridad por día en más de 130 países, y ha recibido más de 10.000 patentes de seguridad en todo el mundo. Para más información, visite www.ibm.com/security, siga [@IBMSecurity](#) en Twitter, o visite el [Blog de IBM Security Intelligence](#).
