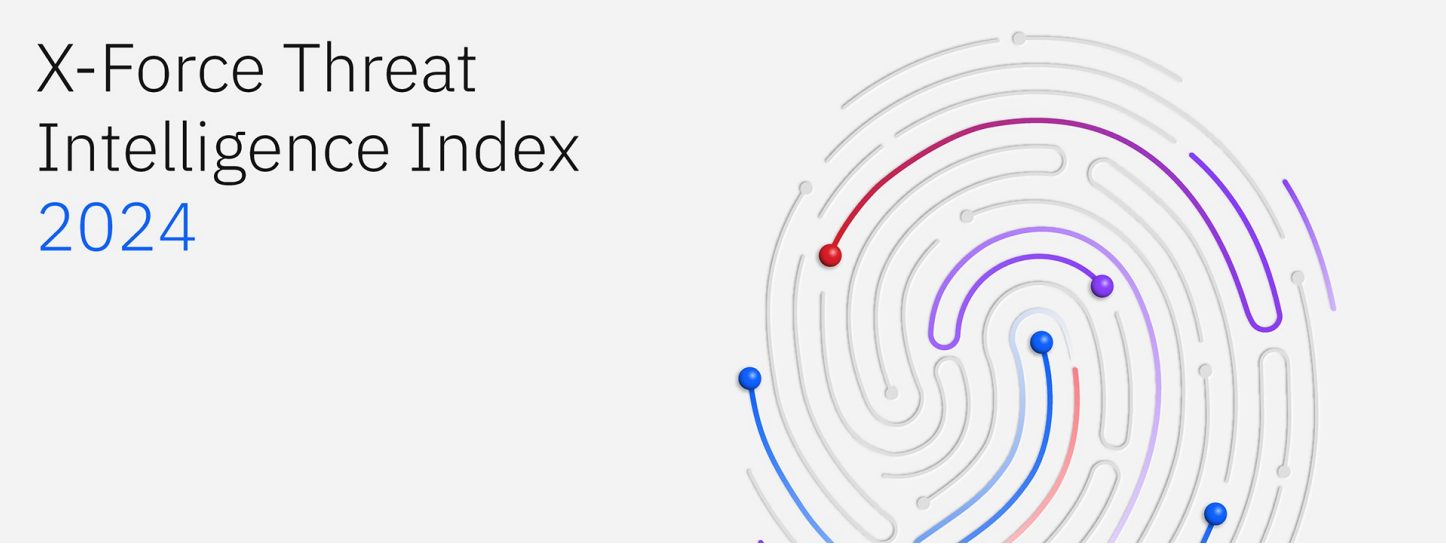
Comunicados

Reporte de IBM: La identidad está bajo ataque en Latinoamérica, reduciendo el tiempo de recuperación de las empresas ante las filtraciones

- La explotación de aplicaciones públicas se convirtió en el principal vector de acceso en América Latina.

- El malware, especialmente el ransomware, continuó como la acción más común en la región.



Bogotá, Febrero 28 de 2024 - IBM Lanzó el X-Force Threat Intelligence Index 2024 resaltando una crisis emergente de identidad global a medida que los cibercriminales están explotando las identidades de los usuarios para comprometer a las empresas en todo el mundo. De hecho, hubo un incremento del 71% en los ciberataques causados por la explotación de la identidad a nivel mundial. De acuerdo con IBM X-Force, el área de servicios de seguridad ofensivos y defensivos de IBM Consulting, en 2023 los ciberdelincuentes vieron más oportunidades de 'iniciar sesión' a través de cuentas válidas en lugar de 'hackear' redes corporativas, lo que convirtió esta táctica en un arma preferida por los cibercriminales en América Latina.

"Los cibercriminales revaluaron las credenciales como un vector de acceso inicial confiable. Con el cambio hacia el 'inicios de sesión', están destacando la relativa facilidad de adquirir credenciales de usuario en comparación con la explotación de vulnerabilidades o la ejecución de campañas de phishing", dijo Juan Carlos Zevallos, Líder de IBM Security Software para América Latina. "Con los ataques generados con IA, las empresas se ven presionadas hacia un nuevo panorama en el que la seguridad impulsada por IA puede elevar las defensas y la productividad a nivel humano, programático y tecnológico".

El X-Force Threat Intelligence Index se basa en insights y observaciones de monitoreo de más de 150 mil millones de eventos de seguridad por día en más de 130 países, incluyendo México, Centroamérica y Sudamérica. Además, los datos se recopilan y analizan de varias fuentes de IBM, incluyendo IBM X-Force Threat Intelligence, Respuesta a Incidentes, X-Force Red, IBM Managed Security Services, y datos proporcionados por Red Hat Insights e Interzer, que contribuyeron al informe de 2024.

Algunos de los hallazgos destacados de América Latina incluyen:

- **Latinoamérica sigue ganando importancia.** La región fue la cuarta geografía más atacada en 2023, representando el 12% de los incidentes que X-Force respondió a nivel mundial. X-Force sigue observando campañas nuevas y mejoradas dirigidas específicamente a América Latina, haciendo hincapié en una preocupante tendencia de un mayor riesgo para la región en el futuro.
- **Blancos persistentes en la región.** Desde la perspectiva geográfica, Brasil (68%), Colombia (17%) y Chile (8%) fueron los países más atacados. A nivel de industria, una vez más, retail fue uno de los sectores más atacados, empatando con finanzas y seguros en el primer lugar, con 25% cada uno. Además, X-Force observó un aumento en las campañas que aprovechan extensiones maliciosas de Chrome, la mayoría enfocadas en entidades financieras de la región. IBM también experimentó un mayor desarrollo y actividad de troyanos bancarios basados en .NET dirigidos a clientes bancarios.
- **Rutas de ataque**. En 2023, el vector de acceso inicial preferido de los atacantes en Latinoamérica fue la explotación de aplicaciones públicas, en otras palabras, aprovecharon las debilidades de los computadores o programas con acceso a Internet, comprendiendo 45% de los casos observados por X-Force. El uso de phishing y de cuentas válidas ocuparon el segundo lugar con un 22%.
- **El ransomware no se va.** Globalmente el año pasado, los ataques de ransomware a las empresas registraron una caída de casi 12%, ya que las organizaciones más grandes optaron por la reconstrucción de su infraestructura en lugar de pagar y desencriptar. En la región, el malware, y específicamente el ransomware, fue la acción más común ejecutada por los cibercriminales, representando el 31% de los ataques; seguido por el acceso a servidores y el uso de herramientas con fines maliciosos, ambos con 23%. Respecto a los impactos de los ataques, el 33% de los incidentes estuvieron relacionados con filtraciones de datos y 22% resultaron en extorsión o afectación a la reputación de la marca. Las ganancias financieras ilícitas, los botnets, el robo de datos y la recopilación de credenciales representaron el 11% de los casos cada uno.

Otros hallazgos globales que involucran a América Latina incluyen:

- **Una crisis de identidad global a punto de empeorar.** En 2023, X-Force vio a los atacantes invertir cada vez más en operaciones para obtener las identidades de los usuarios a nivel mundial, con un aumento del 266% en el malware para el robo de información. Esta ‘entrada fácil’ de los atacantes es una de las tácticas más difíciles para detectar, generando altos costos en la respuesta en las empresas.
- **La "seguridad básica" puede ser más difícil de lograr de lo que se cree** . Casi 85% de los ataques a sectores críticos podrían haberse mitigado con parches de seguridad, habilitando la autenticación multifactor u otorgando privilegios mínimos a los usuarios. Esto resalta la necesidad de que las organizaciones realicen frecuentemente pruebas de resistencia en sus entornos tecnológicos para evaluar potenciales exposiciones y desarrollar planes de respuesta ante incidentes.
- **Aun no se llega al ROI de los ataques a la IA Generativa (IAG).** El análisis de X-Force proyecta que, cuando una sola tecnología de IAG se acerque al 50% de participación de mercado o cuando el mercado se consolide en 3 tecnologías o menos, podría llegarse a la madurez de la IA como superficie de ataque, movilizando una mayor inversión en diferentes herramientas por parte de los ciberdelincuentes. Las empresas también deben reconocer que su infraestructura existente es una puerta de entrada a sus modelos de IA que no requiere tácticas novedosas por parte de los ciberdelincuentes, destacando la necesidad de un enfoque holístico para la seguridad en la era de la IA generativa, como se describe en el Framework de IBM para asegurar la IAG.
- **Todo el mundo es vulnerable.** Red Hat Insights encontró que el 92% de los clientes tienen al menos una vulnerabilidad o exposición conocida (CVE), no abordada, que puede ser explotada en su entorno, mientras

que el 80% de las diez vulnerabilidades principales detectadas en todos los sistemas en 2023 recibieron una puntuación de gravedad 'alta' o 'crítica'.

- **Configuraciones incorrectas de seguridad.** Los engagements de pruebas de penetración de X-Force Red indican que las configuraciones incorrectas de seguridad representaron el 30% del total de las exposiciones identificadas, observando más de 140 formas en que los atacantes pueden explotar las configuraciones erróneas.

Recursos adicionales:

- Descargue una copia del **X-Force Threat Intelligence Index 2024.**
- Lea acerca de los principales hallazgos del informe en este blog de **IBM Security Intelligence.**
- Inscríbase en el **webinar** del jueves 7 de marzo a las 11:00 am ET.
- Conecte con el equipo de **IBM X-Force** para una revisión personalizada de los hallazgos.
