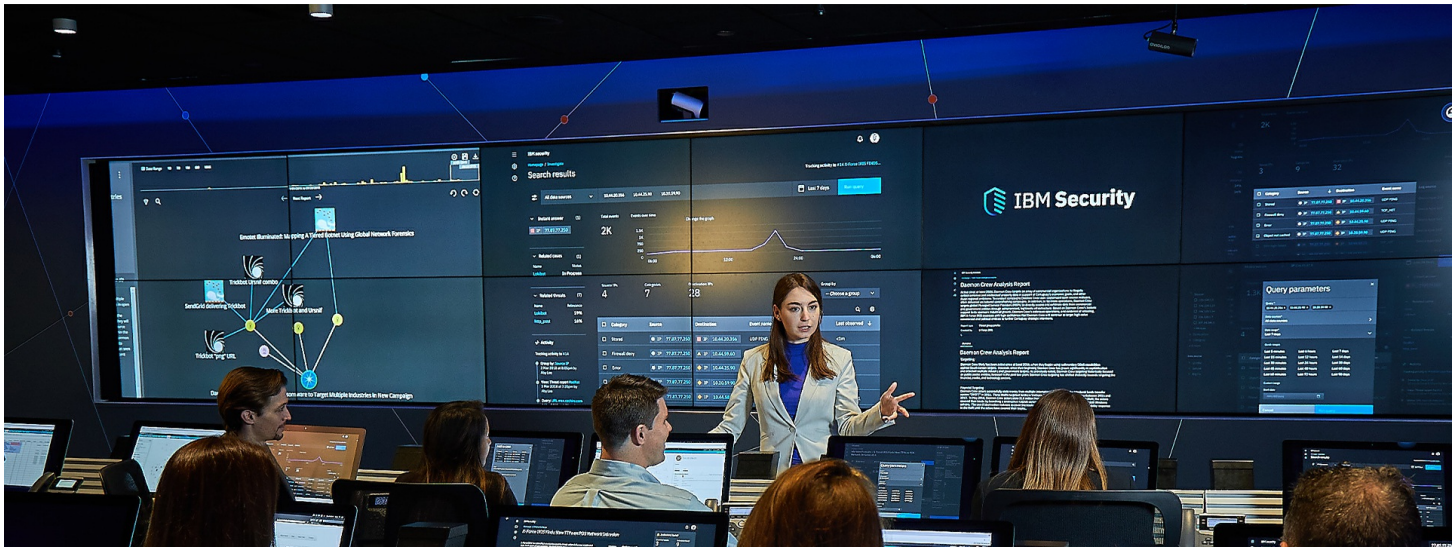
Comunicados

Informe de IBM: el ransomware persiste a pesar mejoras en la detección en 2022

Los intentos de secuestro de conversaciones de e-mail se han intensificado a nivel mundial; los ataques de ransomware ya no se ejecutan en meses sino en días y el comercio minorista y mayorista son los sectores más extorsionados en Latinoamérica



Santiago de Chile, 3 de marzo de 2023 – IBM Security publicó su informe anual X-Force Threat Intelligence Index encontrando que, si bien el porcentaje de incidentes de ransomware a nivel mundial disminuyó levemente (4 puntos porcentuales) de 2021 a 2022, en Latinoamérica aumentó ligeramente (3 puntos porcentuales). Aunque los defensores tuvieron más éxito detectando y previniendo ransomware, los atacantes han seguido innovando. El informe muestra que el tiempo promedio para completar un ataque de ransomware disminuyó de 2 meses a menos de 4 días.

Según el informe de 2023, la implementación de *backdoors* o puertas traseras, que permiten el acceso remoto a los sistemas, surgió como la segunda acción más realizada por los atacantes en el último año en la región. Muchos de esos casos de *backdoors* estuvieron relacionados con intentos de ransomware, en los que los defensores fueron capaces de detectar las puertas traseras antes de la implementación del ransomware. El repunte en implementaciones de *backdoors* se puede atribuir parcialmente a su alto valor de mercado. X-Force observó que los actores de amenazas venden los accesos de *backdoors* existentes en la *dark web* por hasta 10,000 dólares en comparación con los datos de tarjetas de crédito robados, que actualmente se venden por menos de 10 dólares.

"El ransomware es un método bien conocido de extorsión, pero los ciberdelincuentes siempre están explorando nuevas formas de extorsionar. Hoy, el problema de un backdoor puede convertirse en la crisis de ransomware de mañana", dijo Juan Carlos Zevallos, Líder de IBM Security Latinoamérica. "Ya no es suficiente tener una buena defensa. Es fundamental que las empresas accionen una estrategia de seguridad proactiva basada en amenazas y un plan de respuesta a incidentes personalizado que considere también el impacto de un ataque en las víctimas finales".

El IBM Security X-Force Threat Intelligence Index monitorea las tendencias y patrones de ataque nuevos y existentes, a partir de miles de millones de puntos de datos procedentes de dispositivos de red y *endpoints*, su

propia participación en respuesta a incidentes y otras fuentes. Estos son algunos de los hallazgos principales del último informe en Latinoamérica:

- **La región gana importancia para los cibercriminales.** Aunque Latinoamérica representó el 12% de los ataques observados por el equipo de respuesta a incidentes de X-Force, la región pasó del quinto lugar entre las regiones más atacadas del mundo al cuarto lugar. Brasil, Colombia, México, Perú y Chile fueron los países latinoamericanos más atacados en 2022.
- **El comercio minorista y mayorista fueron los más atacados.** Los incidentes en Latinoamérica fueron contrarios a las tendencias de industria globalmente. El comercio minorista y mayorista abandonaron el segundo lugar para convertirse en el sector más atacado en 2022, representando el 28% de los casos que X-Force solucionó. Finanzas y seguros fue el segundo sector más atacado con el 24% de los casos, seguido por energía y manufactura, ambos con un 20%.
- **El compromiso de e-mails empresariales (en inglés, BEC) disminuyó en la región.** BEC ocupó el tercer puesto en 2022 con el 11% de los incidentes a los que X-Force respondió. Este tipo de ataques se produce cuando se accede a un servidor para lograr objetivos finales desconocidos. Para obtener acceso, los atacantes usaron principalmente enlaces o links de spearphishing, archivos adjuntos maliciosos y explotación de cuentas válidas.
- **Los ciberdelincuentes explotan las conversaciones por correo electrónico** . El secuestro de hilos de conversación de e-mail aumentó considerablemente en 2022, con atacantes utilizando cuentas comprometidas para responder a conversaciones en curso, haciéndose pasar por el participante original. X-Force observó que la tasa de intentos mensuales a nivel mundial aumentó 100%. En la región, el secuestro de conversaciones de e-mail representó el 11% de los ataques.
- **Extorsión: el método preferido de los actores de amenazas** . En la región, uno de los impactos más comunes de los ciberataques el año pasado fue la extorsión, alcanzada principalmente con ataques de ransomware o BEC, reflejando la tendencia global. Los ciberdelincuentes atacan principalmente a los sectores, empresas y regiones más vulnerables usando esquemas de extorsión y aplicando una alta presión psicológica para forzar a las víctimas a pagar.

Algunos de los hallazgos globales del informe de 2023 incluyen:

- **Los phishers "desisten" de los datos de tarjetas de crédito.** El número de ciberdelincuentes enfocados en la información de las tarjetas de crédito en kits de phishing cayó un 52 % en un año, indicando que los ciberatacantes le están dando prioridad a información de identificación personal como nombres, e-mails y direcciones, que se pueden vender a un precio más alto en la dark web o pueden ser usados para realizar más operaciones.
- **Las vulnerabilidades de seguridad heredadas siguen haciendo el trabajo.** El porcentaje de *exploits* de seguridad relacionados con vulnerabilidades disminuyó 10 puntos porcentuales de 2018 a 2022, debido a que el número de vulnerabilidades alcanzó otro récord en 2022. Los hallazgos indican que las vulnerabilidades de seguridad heredadas permiten que infecciones de malware más antiguas como WannaCry y Conficker sigan existiendo y extendiéndose.
- **Las marcas más suplantadas incluyen las principales empresas de tecnología.** Las credenciales robadas de estos servicios son valiosas para acceder a las cuentas que las víctimas utilizan para gestionar su presencia en línea. X-Force cree que este cambio en la lista hacia una más diversa se debe a la capacidad mejorada para identificar a las marcas que un kit puede suplantar y no solo la que está atacando por defecto.

El informe presenta datos que IBM recopiló globalmente para proporcionar información relevante sobre el panorama de amenazas global e informar a la comunidad de seguridad sobre las amenazas más relevantes para sus organizaciones.

Descargue una copia del Informe IBM Security X-Force Threat Intelligence 2023 aquí.

Acerca de IBM Security

IBM Security ayuda a proteger las empresas y gobiernos más grandes del mundo mediante una cartera integrada de productos y servicios de seguridad, dotados de IA dinámica y capacidades de automatización. La cartera, con el apoyo de la investigación de IBM Security X-Force® de renombre mundial, permite a las organizaciones predecir las amenazas, proteger los datos a medida que se mueven y responder con velocidad y precisión sin frenar la innovación empresarial. expertos mundiales en seguridad, miles de organizaciones confían en IBM como su socio para evaluar, plantear estrategias, implementar y gestionar las transformaciones de seguridad. IBM opera una de las más amplias organizaciones de investigación, desarrollo y entrega de seguridad 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.