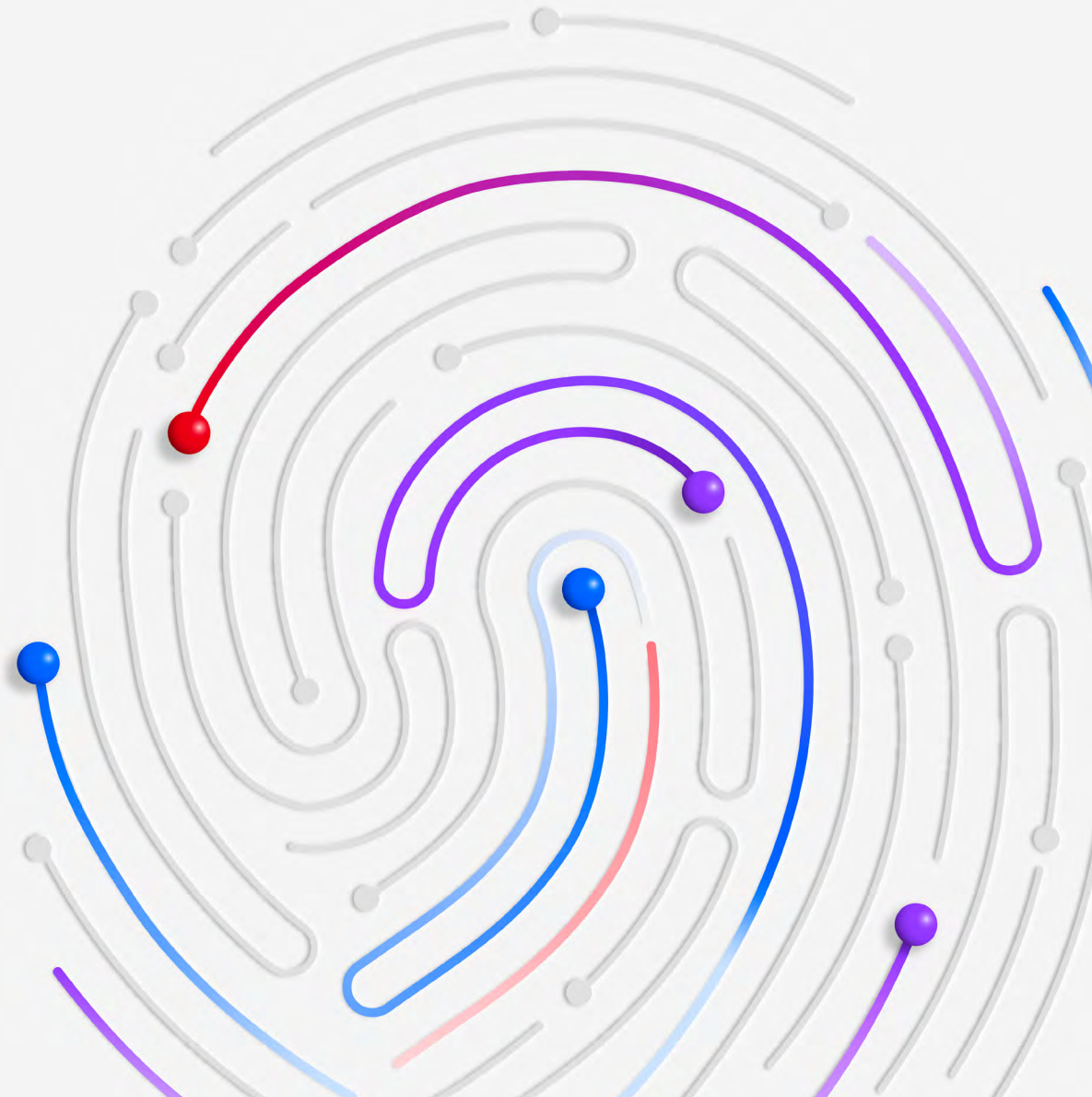
X-Force Threat Intelligence Index 2024

Resumen ejecutivo



IBM

Índice

Resumen ejecutivo

El mayor cambio que el equipo X-Force de IBM observó en 2023 fue un pronunciado aumento de las ciberamenazas dirigidas a identidades. Históricamente, los atacantes tendían a elegir la vía con menor resistencia para conseguir sus objetivos. Hoy en día, el foco se ha desplazado hacia la *información de registro* en lugar *del pirateo*, destacando la relativa facilidad de adquirir credenciales en comparación con explotar vulnerabilidades o ejecutar campañas de phishing. La falta de protección de la identidad fue corroborada por los datos de las pruebas de penetración de IBM X-Force de 2023, las cuales clasificaron *los fallos de identificación y autenticación* como el segundo hallazgo más común.

Además, X-Force observó un aumento del 100 % en "Kerberoasting" durante los compromisos de respuesta a incidentes. El "Kerberoasting" es una técnica centrada en comprometer las credenciales de Microsoft Windows Active Directory a través de tickets Kerberos. Esto indica un cambio en la forma en que los atacantes adquieren identidades para llevar a cabo sus operaciones.

El protagonismo de las *cuentas válidas* como técnica de acceso inicial preferida entre los ciberdelincuentes (empatando por primera vez con el phishing) fue otro hecho notable. Esta técnica de acceso va acompañada de un aumento del malware diseñado para robar información, conocido como "infostealer malware", actividades que refuerzan el mercado de credenciales robadas de la dark web. Este cambio multifacético subraya la relación simbiótica entre varios elementos del ecosistema de la ciberdelincuencia.

Está claro que los atacantes han identificado la dificultad que tienen los defensores para distinguir entre el uso legítimo de la identidad del usuario y el uso indebido no autorizado. Este aumento de ataques contra identidades pone de relieve la importancia crítica de que las organizaciones identifiquen, eliminen y auditen de forma proactiva los posibles vectores de ataque dentro de sus redes dinámicas. Estas medidas son fundamentales para reducir la superficie de ataque, descubrir riesgos latentes y solucionar de forma autónoma incidentes independientemente de que haya amenazas inminentes.

El año pasado también pasará a la historia como el año de la inteligencia artificial (IA) generativa. Tanto los responsables políticos como los directivos de empresas y los profesionales de la ciberseguridad sienten la presión de adoptar la IA en sus operaciones. Pero la prisa por adoptar la IA generativa supera ahora mismo la capacidad de los sectores para entender los riesgos de seguridad que estas nuevas capacidades conllevan. No obstante, una vez que la adopción de la IA alcance una masa crítica, se materializará una superficie de ataque universal, lo que obligará a las organizaciones a priorizar las medidas de seguridad que puedan adaptarse a las amenazas de la IA a escala.

En un intento por identificar los hitos clave que indicarán cuándo madurará un panorama común de amenazas de IA, X-Force evaluó anteriores disruptores tecnológicos y sus hitos de madurez de amenazas. Según este análisis, X-Force predice que las amenazas comenzarán a atacar la IA de forma generalizada una vez que el mercado se unifique en torno a modelos de implementación comunes y un número reducido de proveedores. Este análisis sugiere que el dominio del mercado por parte de la IA es el factor que desencadenará que los atacantes inviertan en kits de herramientas para atacar a la IA.

A pesar de las inminentes amenazas generadas por la IA generativa, X-Force no ha observado ninguna prueba concreta de ciberataques creados por IA generativa hasta la fecha ni un cambio rápido en las metas y objetivos de los atacantes con respecto a años anteriores. Aunque X-Force observó un notable descenso de los ataques de ransomware a empresas en 2023, los ataques basados en la extorsión continuaron teniendo una gran importancia en la ciberdelincuencia el año pasado. Estos ataques basados en la extorsión solo fueron superados por *el robo y la fuga de datos* como el impacto más común observado en los compromisos de respuesta a incidentes de X-Force a nivel mundial.

El IBM X-Force Threat Intelligence Index ofrece estos conocimientos como recurso a los clientes de IBM, investigadores del sector de la seguridad, responsables políticos, medios de comunicación y la comunidad completa de profesionales de la seguridad y líderes empresariales. Nuestra intención es mantener informados a todos los implicados sobre el panorama actual de amenazas para que puedan tomar las mejores decisiones para reducir riesgos.

Aspectos destacados

71%

Aumento continuado del volumen de ataques con credenciales válidas
Por primera vez, el abuso de cuentas válidas se convirtió en el punto de entrada más común de los ciberdelincuentes en los entornos de las víctimas. Representó el 30 % de todos los incidentes a los que respondió X-Force en 2023.

32 %

Porcentaje de incidentes de robo y filtrado de datos
El robo y la filtración de datos aumentaron hasta convertirse en el impacto más común para las organizaciones, lo que indica que cada vez más grupos prefieren este método para obtener beneficios económicos.

11,5 %

Descenso en los incidentes de ransomware empresarial
A pesar de seguir siendo la acción más común en el objetivo (20 %), X-Force observó un descenso en los incidentes de ransomware empresarial. Es probable que este descenso afecte a las expectativas de ingresos de los adversarios procedentes de la extorsión basada en el cifrado, ya que las organizaciones más grandes están deteniendo los ataques antes de que se implemente el ransomware y optando por no pagar y descifrar en favor de la reconstrucción si el ransomware se afianza.

266 %

Aumento del uso de infostealers
X-Force ha observado que los grupos de amenazas que antes se especializaban en ransomware muestran cada vez más interés por los infostealers. Varios nuevos infostealers destacados debutaron recientemente y demostraron una mayor actividad en 2023, como Rhadamanthys, LummaC2 y StrelaStealer.

30 %

Porcentaje de errores de configuración de seguridad entre las vulnerabilidades de aplicaciones web detectadas
Las pruebas de penetración de X-Force revelaron que el riesgo más observado en las aplicaciones web de los clientes de todo el mundo eran los errores de configuración de seguridad. Entre estos errores de configuración, uno de los principales errores fue permitir múltiples sesiones de usuario simultáneas en la aplicación, lo que podría debilitar la autenticación multifactor (MFA, por sus siglas en inglés) mediante el secuestro de la sesión.

84 %

Porcentaje de incidentes de infraestructuras críticas en los que se podría haber mitigado el vector de acceso inicial
En la mayoría de los incidentes en infraestructuras críticas a los que respondió X-Force, el vector de acceso inicial podría haberse mitigado con buenas prácticas y fundamentos de seguridad, como la gestión de activos y parches, el refuerzo de credenciales y el principio del mínimo privilegio.

32 %

Porcentaje de incidentes relacionados con el uso malintencionado de herramientas legítimas
Casi un tercio de los incidentes a los que respondió X-Force fueron casos en los que se utilizaron herramientas legítimas con fines maliciosos, como robo de credenciales, reconocimiento, acceso remoto o exfiltración de datos.

25,7 %

Porcentaje de ataques a la industria manufacturera entre los 10 sectores más atacados
La industria manufacturera volvió a ser la industria más atacada en 2023 por tercer año consecutivo, representando el 25,7 % de los incidentes dentro de los 10 principales sectores. El malware fue el método más observado, con un 45 %. El ransomware representó el 17 % de los casos.

50 %

Es probable que el umbral de cuota de mercado desencadene ataques contra las plataformas de IA
El análisis de X-Force indica que el asentamiento del dominio del mercado de la IA señalará la madurez de la superficie de ataque de la IA. Este análisis sugiere que una vez que una sola tecnología de IA se acerque al 50 % de la cuota de mercado, o cuando el mercado se consolide en tres o menos tecnologías, el ecosistema de ciberdelincuentes se verá incentivado a invertir en el desarrollo de herramientas y vías de ataque dirigidas a las tecnologías de IA.

31 %

Incremento año tras año de los ataques en Europa
Europa experimentó el mayor porcentaje de incidentes (32 %) de las cinco regiones geográficas. El malware fue el tipo de ataque más observado, representando el 44 % de los incidentes.

Recomendaciones

En 2023, la combinación del aumento de uso de los infostealers y el abuso de credenciales de cuentas válidas ha convertido la gestión de identidades y accesos en un reto. Esta nueva fijación del panorama de amenazas en las identidades pone en relieve los riesgos que existen para las organizaciones en los dispositivos que no controlan. Las credenciales empresariales se pueden robar de dispositivos comprometidos a través de la reutilización de credenciales, almacenes de credenciales en navegadores o accediendo a cuentas empresariales directamente desde dispositivos personales.

La velocidad de las intrusiones ha aumentado gracias a nuevas vías de ataque eficaces y repetibles (como se ha visto con la explotación masiva de las herramientas MFT y los ataques Kerberoasting) y a la creciente eficiencia en el mercado delictivo gracias a la ventaja competitiva obtenida. Y mientras el ransomware y otros malware continúan plagando las organizaciones, los ciberdelincuentes han comenzado a explorar cómo sacar partido de la IA en sus operaciones.

Dadas estas tendencias, ¿cómo deben responder las organizaciones y por dónde deben empezar?

Reduzca el riesgo de robo de credenciales
Implementar herramientas de detección y respuesta de endpoints (EDR) en todos los servidores y estaciones de trabajo de su entorno ayuda a detectar el malware, incluidos los infostealers y el ransomware. Estas herramientas también pueden detectar comportamientos anómalos, como la exfiltración de datos, la consulta de información sensible o la creación de nuevas cuentas o carpetas en sistemas sensibles.

Recurra a expertos para obtener más información sobre cómo crear y poner en funcionamiento la búsqueda de amenazas en su entorno. Si dispone de recursos limitados, amplíe su equipo utilizando IA para gestionar hasta el 85 % de las alertas y obtenga protección 24x7 con servicios de detección y respuesta a amenazas. Por otra parte, utilice la inteligencia de amenazas para identificar las oportunidades clave y así mitigar nuevas amenazas de atacantes que buscan robar sus credenciales.

Refuerce su gestión de credenciales para proteger las credenciales de su sistema o dominio mediante la implementación de MFA y políticas de contraseñas seguras que incluyan el uso de claves de acceso y aproveche las configuraciones reforzadas de sus sistemas para dificultar el acceso a las credenciales. Los ataques de robo de credenciales a menudo también se llevan a cabo a través de phishing y watering hole.

Ofrezca a sus empleados formaciones periódicas sobre los métodos más modernos de phishing usados por los atacantes. Examine todo el tráfico de terceros: considérelo no fiable hasta que se verifique lo contrario. Los atacantes que usan el método watering hole suelen aprovechar recursos legítimos para distribuir su malware.

Reduzca el alcance de la explosión
En el contexto de la ciberseguridad, el alcance de explosión se refiere al impacto potencial de un incidente dado el compromiso de determinados usuarios, dispositivos o datos. Por ejemplo, si una cuenta con privilegios administrativos se ve comprometida, el radio de explosión es mayor que si a una cuenta normal sin privilegios se le da la capacidad de moverse lateralmente y acceder a datos a través de la red.

Dada la importancia de la seguridad de datos y la gestión de identidades en el panorama actual de amenazas, las organizaciones deberían plantearse implementar soluciones para reducir los daños que podría causar un incidente de seguridad de datos.

Estrategias para reducir el alcance de la explosión:

- Implementar un marco de mínimos privilegios.
- Ofrecer segmentación de identidades y redes.
- Implementar soluciones de seguridad y protección de datos.
- Proporcionar supervisión y respuesta a incidentes continua.

Identifique su nivel de exposición a la dark web
Los atacantes pueden usar las credenciales robadas para su propio beneficio, venderlas en la dark web o ambas. Los datos disponibles sobre su organización en la dark web ponen de manifiesto el riesgo que reside fuera del control del perímetro de su red. Utilice capacidades para la dark web que:

- Encuentren credenciales y claves de sesión comprometidas.
- Comprueben las identidades digitales de sus ejecutivos para encontrar sobreexposición de PII, críticas contra ejecutivos y creación fraudulenta de perfiles en redes sociales.
- Analicen las redes sociales, los canales relacionados con su sector, blogs y anuncios en busca de usos no autorizados de su marca.
- Identifiquen los datos prioritarios, confidenciales y sensibles filtrados.
- Evalúen foros, mercados de tarjetas de crédito, canales de Telegram, chats y foros de debate, repositorios de código, repositorios de documentos y archivos, rastreadores de web superficial y sitios de copiado y pegado para comprobar la exposición de credenciales y claves de sesión robadas.

Elimine silos de identidad fragmentados
La correcta implementación de un tejido de identidades independiente del producto puede ampliar las capacidades modernas de seguridad, detección y respuesta a aplicaciones y sistemas obsoletos. Simplifique la gestión de identidades a través de un único gestor de identidades y accesos (IAM) para administrar el gobierno de identidades, gestionar la identidad y el acceso de personal y consumidores, y controlar las cuentas con privilegios. Optimice el proceso al contar con la asesoría de expertos en identidad y seguridad, quienes le ayudarán a definir y gestionar soluciones en entornos de cloud híbrido, transformar los flujos de trabajo de gobierno y cumplir con las regulaciones.

Implemente un enfoque de pruebas DevSecOps
X-Force descubrió que el riesgo de las aplicaciones web más observado en los entornos de clientes de todo el mundo en 2023 fue la falta de configuraciones de seguridad y, entre ellas, las principales infracciones incluían permitir sesiones de usuario simultáneas en la aplicación. Limite la posibilidad de secuestro de sesión aplicando un enfoque DevSecOps, utilice conexiones seguras y cifradas (HTTPS), implemente tiempos de espera de sesión y solicite reautenticación. Contrate servicios de pruebas de penetración para probar sus aplicaciones, redes, hardware y personal con el fin de detectar vulnerabilidades y puntos débiles en todos sus activos.

Tenga un plan
A pesar de los esfuerzos de las organizaciones por reducir el riesgo de ataques, pueden producirse incidentes. Disponer de planes de respuesta a incidentes personalizados para su entorno es clave para reducir el tiempo de respuesta, reparación y recuperación tras un ataque. Este tipo de planes deben practicarse con regularidad e incluir una respuesta interorganizativa, incorporar a las partes interesadas ajenas a TI y poner a prueba las líneas de comunicación entre los equipos técnicos y la alta dirección. Por último, el ensayo de su plan en un ejercicio cibernético de inmersión y alta presión puede mejorar en gran medida su capacidad de respuesta ante un ataque.

Use modelos de negocio de IA seguros
El reto de establecer una IA segura. Las organizaciones pueden aprovechar métodos existentes para ayudar a asegurar la canalización de la IA. Los principios clave en los que hay que centrarse son la seguridad de los datos con los que se entrena la IA, los modelos y el uso e inferencia de los modelos, y también toda la infraestructura en torno a los modelos. Los puntos de acceso que los ciberdelincuentes aprovechan para comprometer a las empresas plantean el mismo tipo de riesgo para la IA y, a medida que las organizaciones delegan procesos operativos de negocio en la IA, también necesitan establecer gobierno y hacer que los controles operativos sean fundamentales en su estrategia de IA.

Quiénes somos

IBM X-Force

IBM X-Force es un equipo centrado en las amenazas formado por hackers, expertos en respuestas, investigadores y analistas con décadas de experiencia. La cartera de X-Force incluye productos y servicios ofensivos y defensivos, impulsados por una visión integral de las amenazas.

En una época de ciberataques sin tregua, un mundo siempre conectado y con cada vez más exigencias normativas, las organizaciones necesitan un enfoque de seguridad focalizado. X-Force cree que la amenaza debe ser el punto central. A través de los servicios de pruebas de penetración, gestión de vulnerabilidades y simulación de adversarios, el equipo de hackers Red de IBM X-Force adopta el punto de vista de un atacante para encontrar vulnerabilidades de seguridad, exponiendo sus activos más importantes. Gracias a los servicios de preparación, detección y respuesta ante incidentes y de gestión de crisis, el Equipo de Respuesta a Incidentes (RI) de IBM X-Force sabe dónde encontrar las amenazas y cómo detenerlas. Los investigadores de X-Force crean técnicas ofensivas para detectar y evitar amenazas. Los analistas de X-Force recopilan datos sobre amenazas y los convierten en información útil para reducir riesgos.

Al contar con unos conocimientos profundos sobre cómo piensan, trazan sus estrategias y atacan los actores de amenazas, X-Force puede ayudarle a evitar, detectar, responder y recuperarse de incidentes para que se pueda centrar en las prioridades de su empresa.

Si su organización desea recibir asistencia para reforzar su posición de seguridad, programe una sesión informativa individual con un experto de IBM X-Force.

Programe una sesión informativa →

IBM Security

IBM Security se adapta a su huella en constante expansión y trabaja con usted para mantenerle en el buen camino. Le ayudamos a ir siempre un paso por delante, con mayor rapidez y precisión, gracias a nuestras capacidades dinámicas de IA y automatización. Asegúrese de tomar las decisiones correctas tanto ahora como en el futuro gracias a los consejos de nuestro equipo de expertos líderes en el sector. Tanto si desea anticiparse a amenazas, como proteger datos, colaborar con varios proveedores o expandirse globalmente, IBM Security está preparado para ayudarle a alcanzar sus ambiciosos objetivos empresariales. Proporcionamos soporte para explorar nuevas tecnologías cruciales y mitigar amenazas imprevistas, independientemente de la dirección que tome su negocio.

Más información →

Colaboradores

Christopher Caridi

John Dwyer

Georgia Prassinos

Kat Metrick

Austin Zeizel

Joshua Chung

Dave McMillen

Benjamin Shipley

Charlotte Hammond

Golo Mühr

Ole Villadsen

Joseph Fasulo

Claire Zaboeva

Melissa Frydrych-Dean

Richard Emerson

Camille Singleton

Michelle Alvarez

Andy Piazza

Karlina Bakken

Yannick Bedard

Christopher Bedell

Johnny Shaieb

Scott Lohr

Scott Moore

Guy Vincent Jourdan

Vio Onut

Julien Cassagne

IBM España, S.A.
Santa Hortensia, 26-28
28002 Madrid
IBM Corporation
New Orchard Road
Armonk, NY 10504

Producido en los
Estados Unidos de America
Febrero de 2024

Este documento se actualizó por última vez en la fecha inicial de publicación e IBM puede modificarlo en cualquier momento. No todas las ofertas están disponibles en todos los países en los que opera IBM.

Declaración de buenas prácticas de seguridad: Ningún sistema o producto de TI debe considerarse completamente seguro y ningún producto, servicio o medida de seguridad puede ser completamente efectivo para prevenir el uso o acceso indebido. IBM no garantiza que los sistemas, productos o servicios sean inmunes o vayan a hacer que su empresa sea inmune a la conducta maliciosa o ilegal de terceros.

El cliente es responsable de garantizar el cumplimiento de las leyes y normativas aplicables. IBM no presta asesoramiento legal ni declara o garantiza que sus servicios o productos aseguren que el cliente cumpla con cualquier ley o regulación.