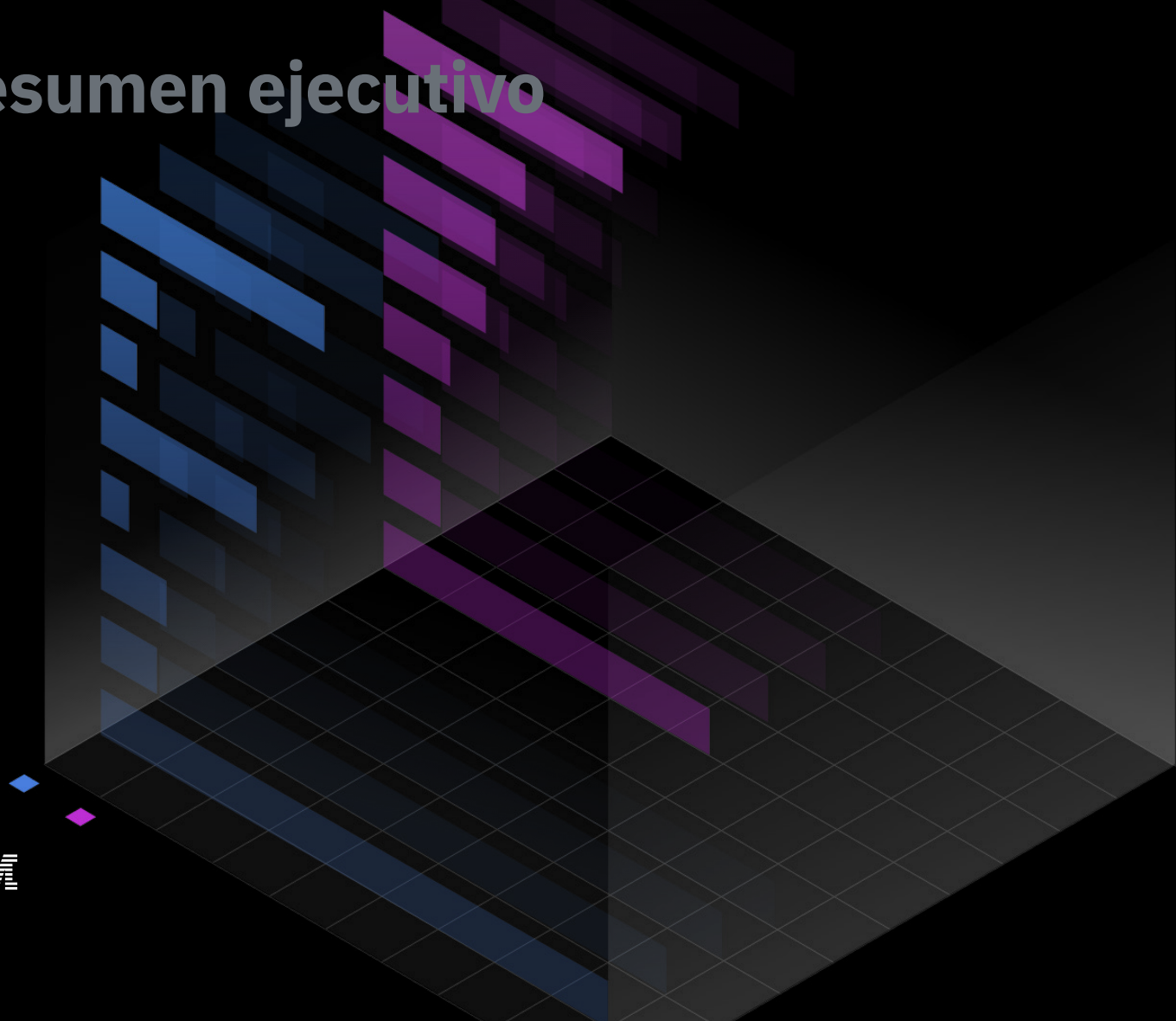
IBM Security

Índice de inteligencia de amenazas X-Force 2021

Resumen ejecutivo



IBM

Introducción

El año 2020 fue, sin duda, uno de los más trascendentales y transformacionales de los últimos tiempos: una pandemia global, una crisis económica que afectó la vida de millones de personas y disturbios sociales y políticos. Las repercuciones de estos eventos afectaron a las empresas de manera profunda y muchas hicieron un cambio importante hacia fuerzas de trabajo distribuidas.

En el ámbito cibernético, las circunstancias extraordinarias de 2020 brindaron a los criminales cibernéticos oportunidades para explotar las necesidades de las redes de comunicación y proporcionaron objetivos valiosos en las cadenas de suministro y la infraestructura crítica. El año terminó como comenzó, con el descubrimiento de una amenaza de consecuencias globales que requería una respuesta rápida y remediación. Un ataque que se ha atribuido en gran medida a un actor de estado nación, que aprovechó una puerta trasera en un software de monitoreo de red para atacar organizaciones gubernamentales y del sector privado, demostró cómo se debe anticipar el riesgo de terceros, pero también que no se puede predecir.

Para ayudar a enfrentar los desafíos de estos tiempos, IBM Security X-Force evalúa el panorama de las amenazas cibernéticas y ayuda a las organizaciones a comprender las amenazas en evolución, su riesgo asociado y cómo priorizar los esfuerzos de seguridad cibernética. Además de la inteligencia sobre las principales amenazas que brindamos a los clientes, analizamos la gran cantidad de datos que recopilamos para producir el Índice de inteligencia de amenazas X-Force, una revisión anual sobre el panorama de las amenazas y cómo estas están cambiando.

Entre las tendencias que rastreamos, el ransomware continuó su aumento para convertirse en el tipo de amenaza número uno, lo que representa el 23 % de los eventos de seguridad a los que X-Force respondió en 2020. Los atacantes de ransomware aumentaron la presión para extorsionar y obtener pagos mediante la combinación de la encriptación de datos con amenazas para filtrar los datos en sitios públicos. El éxito de estos esquemas ayudó a tan solo una banda de ransomware a obtener ganancias de más de USD 123 millones en 2020[1], según estimaciones de X-Force.

Las organizaciones de manufactura resistieron una avalancha de ransomware y otros ataques en 2020. La industria manufacturera en general fue la segunda más atacada, después de las finanzas y los seguros, siendo la octava industria más atacada en 2019. X-Force descubrió a atacantes sofisticados que utilizaban campañas de suplantación de identidad focalizada (spear phishing) en ataques contra empresas de fabricación y ONG involucradas en la cadena de suministro de la vacuna para la COVID-19.

1. Todas las menciones de moneda que se hacen en este informe son en dólares estadounidenses.

Los actores de amenazas también estaban innovando su software malicioso (malware), en particular el malware dirigido a Linux, el código de fuente abierta que soporta la infraestructura de nube crítica para el negocio y el almacenamiento de datos. El análisis de Intezer descubrió 56 nuevas familias de malware de Linux en 2020, mucho más que el nivel de innovación encontrado en otros tipos de amenazas.

Hay motivos para esperar que 2021 se perfile como un año mejor. Las tendencias son muy difíciles de predecir, pero la única cosa constante en la que podemos confiar es el cambio. La resiliencia frente a los desafíos crecientes y decrecientes en seguridad cibernética requiere inteligencia procesable y una visión estratégica para el futuro de una seguridad más abierta y conectada.

Con el espíritu de resistencia a través de la comunidad, IBM Security se complace en ofrecer el Índice de inteligencia de amenazas X-Force 2021. Los hallazgos de este informe pueden ayudar a los equipos de seguridad, los profesionales de riesgos, los responsables de la toma de decisiones, los investigadores, los medios de comunicación y otros, a comprender dónde han estado las amenazas en el último año y ayudar a prepararse para lo que venga después.

Resumen ejecutivo

IBM Security X-Force se basó en miles de millones de puntos de datos recopilados de nuestros clientes y fuentes públicas entre enero y diciembre de 2020 para analizar tipos de ataques, vectores de infección y comparaciones globales y de la industria. Los siguientes son algunos de los principales hallazgos presentados en el Índice de inteligencia de amenazas X-Force.

23 %

Proporción de ataques de ransomware

El ransomware fue el método de ataque más popular en 2020, representando el 23 % de todos los incidentes a los que IBM Security X-Force respondió y ayudó a remediar.

Más de USD 123 millones

Beneficios estimados del ransomware principal

X-Force estima de manera conservadora que los actores de ransomware de Sodinokibi (también conocido como REvil) obtuvieron al menos USD 123 millones en ganancias en 2020 y robaron alrededor de 21.6 terabytes de datos.

25 %

Mayor porcentaje de vulnerabilidades de ataques en el primer trimestre de 2020

Los actores de amenazas capitalizaron una falla de recorrido de ruta de Citrix, explotando esta vulnerabilidad en el 25 % de todos los ataques de los primeros tres meses del año y el 8 % del total de ataques en 2020.

35 %

Proporción de exploración y explotación de los principales vectores de infección

El escaneo y la explotación de vulnerabilidades subieron al vector de infección más alto en 2020, superando a la suplantación de identidad (phishing), que fue el principal vector en 2019.

2

Rango de fabricación en las principales industrias atacadas

La industria manufacturera fue la segunda industria más atacada en 2020, frente al octavo lugar en 2019, y solo superada por los servicios financieros.

5 horas

Duración de los videos de entrenamiento de ataques en el servidor de un grupo de amenazas

Los errores operativos de los atacantes del estado-nación iraní permitieron a los investigadores de X-Force descubrir alrededor de 5 horas de video en un servidor mal configurado, lo que permitió conocer sus técnicas.

Más de100

Ejecutivos fueron objetivo de una campaña de phishing de precisión

A mediados de 2020, X-Force descubrió una campaña global de phishing que alcanzó a más de 100 ejecutivos de alto rango en funciones de gestión y adquisiciones para un grupo de trabajo que adquiría equipo de protección personal (PPE) en la batalla contra la COVID-19.

49 %

Tasa de crecimiento de la vulnerabilidad relacionada con ICS, 2019-2020

Las vulnerabilidades relacionadas con los sistemas de control industrial (ICS, por sus siglas en inglés) descubiertas en 2020 fueron 49 % más altas con respecto a 2019.

56

Número de nuevas familias de malware de Linux

El número de nuevas familias de malware relacionadas con Linux descubiertas en 2020 fue de 56, su nivel más alto hasta la fecha. Esto representó un aumento del 40 % interanual entre 2019 y 2020.

31 %

Proporción de ataques perpetrados en Europa

La región más atacada en 2020 fue Europa, que sufrió el 31 % de los ataques observados por X-Force, seguida de América del Norte (27 %) y Asia (25 %).

De cara al futuro

En 2021, una combinación de amenazas antiguas y nuevas requerirá que los equipos de seguridad consideren muchos riesgos simultáneamente. Según el análisis de X-Force, estos son algunos de los puntos clave para las prioridades del próximo año.

- **La superficie de riesgo seguirá creciendo en 2021.** Con miles de nuevas vulnerabilidades que probablemente se reporten, tanto en aplicaciones y dispositivos nuevos como antiguos.
- **La doble extorsión por ransomware probablemente persistirá a lo largo de 2021.** Los atacantes que filtran públicamente datos en sitios de denuncia y agravios, aumentan la influencia de los actores de amenazas para imponer precios altos por las infecciones de ransomware.
- **Los actores de amenazas continúan orientando su mirada hacia diferentes vectores de ataque.** Continuará la focalización en los sistemas Linux, la tecnología operativa (OT, por sus siglas en inglés), los dispositivos de la Internet de las Cosas (IoT, por sus siglas en inglés) y los entornos de la nube. A medida que la focalización de estos sistemas y dispositivos se vuelva más avanzada, los actores de amenazas podrán reorientar rápidamente los esfuerzos, especialmente después de cualquier incidente de alto perfil.
- **Cada industria tiene su parte de riesgos.** El cambio año tras año en la focalización específica de la industria destaca el riesgo para todos los sectores de la industria y la necesidad de avances significativos y madurez en los programas de seguridad cibernética en todos los ámbitos.

Recomendaciones para la resiliencia

Según los hallazgos de IBM Security X-Force de este informe, mantenerse al día con la inteligencia de amenazas y desarrollar capacidades de respuesta sólidas son formas efectivas de ayudar a mitigar las amenazas en el panorama en evolución, independientemente de la industria o el país en el que se opere.

X-Force recomienda los siguientes pasos que las organizaciones pueden tomar para prepararse mejor para las amenazas cibernéticas en 2021:

Póngase al frente de la amenaza en lugar de tan solo reaccionar a ella. Aproveche la inteligencia de amenazas para comprender mejor las motivaciones y tácticas de los actores de amenazas para priorizar los recursos de seguridad.

La preparación es clave para responder al ransomware. La planificación de un ataque de ransomware, incluido un plan que aborde técnicas combinadas de ransomware y robo de datos, y la extorsión, y la exploración periódica de este plan pueden marcar la diferencia en la forma en la que su organización responde en el momento crítico.

Verifique la estructura de administración de parches de su organización. Ya que el escaneo y la explotación fueron el vector de infección más común el año pasado, fortalezca su infraestructura y revitalice las detecciones internas para encontrar y detener los intentos de explotación automatizados de manera rápida y efectiva.

Protéjase contra las amenazas internas. Utilice soluciones de prevención de pérdida de datos (DLP, por sis siglas en inglés), capacitación y monitoreo para evitar que personas internas, malintencionada o inadvertidamente, violen la seguridad de su organización.

Cree y capacite un equipo de respuesta a incidentes dentro de su organización. Si eso no es posible, contrate una capacidad de respuesta a incidentes eficaz para una respuesta rápida a incidentes de alto impacto.

Ponga a prueba el plan de respuesta a incidentes de su organización para desarrollar memoria muscular. Los ejercicios de simulación o las experiencias de rango cibernético pueden brindarle a su equipo una experiencia crítica para mejorar el tiempo de reacción, reducir el tiempo de inactividad y, en última instancia, ahorrar dinero en caso de una violación de seguridad.

Implemente la autenticación multifactorial (MFA, por sus siglas en inglés). Agregar capas de protección a las cuentas sigue siendo una de las prioridades de seguridad más eficientes para las organizaciones.

Tenga copias de seguridad, pruebe las copias de seguridad y almacene copias de seguridad fuera de línea. No solo garantizar la presencia de copias de seguridad, sino también su efectividad a través de pruebas en el mundo real, marca una diferencia crítica en la seguridad de la organización, especialmente con los datos de 2020 que muestran un resurgimiento en la actividad de ransomware.

Acerca de IBM Security X-Force

IBM Security X-Force ofrece capacidades de información, detección y respuesta para ayudar a los clientes a mejorar su postura de seguridad.

Inteligencia de amenazas de X-Force de IBM Security combina telemetría de operaciones de seguridad de IBM, investigación, investigaciones de respuesta a incidentes, datos comerciales y fuentes abiertas para ayudar a los clientes a comprender las amenazas emergentes y tomar rápidamente decisiones de seguridad informadas.

Además, el equipo altamente capacitado de Respuesta a incidentes de X-Force proporciona soluciones estratégicas que ayudan a las organizaciones a lograr un mejor control sobre los incidentes y las violaciones de seguridad.

X-Force, en combinación con las experiencias de la gama cibernética del centro de mando de seguridad de IBM capacita a los clientes para que estén preparados para las realidades de las amenazas actuales.

A lo largo del año, los investigadores de IBM X-Force también proporcionan investigación y análisis continuos en forma de blogs, informes técnicos, seminarios web y podcasts, destacando nuestra información sobre los actores de amenazas avanzados, el nuevo malware y los nuevos métodos de ataque. Además, proporcionamos una gran cantidad de análisis actuales y de vanguardia a los suscriptores de nuestra plataforma Premier Threat Intelligence.

Dé el siguiente paso

Obtenga información sobre cómo orquestar su respuesta a incidentes con IBM Security >

Acerca de IBM Security

IBM Security trabaja con usted para ayudarle a proteger su empresa con una cartera avanzada e integrada de productos y servicios de seguridad empresarial, integrados con inteligencia artificial, y un enfoque moderno para su estrategia de seguridad que utiliza principios de confianza cero, lo que le ayudará a prosperar frente a la incertidumbre. Al alinear su estrategia de seguridad con su negocio; integrar soluciones diseñadas para proteger a sus usuarios, activos y datos digitales, e implementando tecnología para gestionar sus defensas contra amenazas crecientes, lo ayudamos a gestionar y controlar el riesgo que respalda los entornos de nube híbrida de la actualidad.

Nuestro nuevo enfoque moderno y abierto, la plataforma IBM Cloud Pak for Security, se basa en RedHat Open Shift y es compatible con los entornos híbridos de múltiples nubes de hoy en día con un extenso ecosistema de socios. Cloud Pak for Security es una solución de software en contenedores lista para empresas que le permite gestionar la seguridad de sus datos y aplicaciones, integrando rápidamente sus herramientas de seguridad existentes para generar insights más profundos sobre las amenazas en los entornos de nube híbrida, dejando sus datos donde están, permitiendo una fácil orquestación y automatización de su respuesta de seguridad.

Para obtener más información, visite www.ibm.com/security, siga a @IBMSecurity en Twitter o visite el blog de IBM Security Intelligence.

Colaboradores

Autora principal:
Camille Singleton

Colaboradores:
Allison Wikoff
Ari Eitan (Intezer) Charles DeBeck
Charlotte Hammond Chenta Lee
Chris Sperry
Christopher Kiefer
Claire Zaboeva
David McMillen
David Moulton
Dirk Hartz
Georgia Prassinos
Ian Gallagher (Intezer)
John Zorabedian
Joshua Chung
Kelly Kane
Lauren Jensen
Limor Kessem
Mark Usher
Martin Steigemann
Matthew DeFir
Megan Radogna
Melissa Frydrych
Michelle Alvarez
Mitch Mayne
Nick Rossman
Patty Cahill-Ingraham
Randall Rossi
Richard Emerson
Salina Wuttke
Scott Craig
Scott Moore

IBM Corporation
New Orchard Road
Armonk, NY 10504

Producido en los Estados Unidos de América
Febrero de 2021

IBM **Security**