IBM **Security**

X-Force Threat Intelligence Index 2022: Resumen ejecutivo

IBM

Contenido

Resumen ejecutivo

El mundo continúa lidiando con una pandemia duradera, pasamos de trabajar en casa a volver a la oficina y viceversa y los cambios geopolíticos favorecen un ambiente de constante desconfianza. Todo esto equivale al caos, y es en momentos de caos cuando afloran los ciberdelincuentes. En 2021, IBM Security® X-Force® observó cómo actores de amenazas aprovechaban de forma oportunista el entorno en constante cambio para adoptar tácticas y técnicas para infiltrarse con éxito en organizaciones de todo el mundo.

El IBM Security X-Force Threat Intelligence Index revela nuevas tendencias y patrones de ataque que hemos observado y analizado a partir de nuestros datos, procedentes de miles de millones de puntos de datos que abarcan desde dispositivos de detección de red y endpoint, detección de respuestas a incidencias (IR), seguimiento de nombres de dominio, etc. Este informe representa la culminación de esta investigación basada en datos recopilados entre enero y diciembre de 2021.

Ponemos estos hallazgos a disposición de clientes de IBM, de investigadores del sector de seguridad, de responsables de establecer políticas, de medios de comunicación y de la amplia comunidad de profesionales de la seguridad y líderes empresariales.

Dada la volatilidad del entorno y la evolución tanto de los tipos de amenazas como de los vectores de amenazas, ahora más que nunca necesita información precisa sobre amenazas para adelantarse a los atacantes y proteger sus activos más valiosos.

Principales puntos del informe

Principal tipo de ataque: El ransomware volvió a ser el principal tipo de ataque en 2021, aunque el porcentaje de este tipo de ataques que ha solventado X-Force ha ido disminuyendo casi un 9 % de año en año. REvil, un tipo de ransomware al que X-Force también se refiere como Sodinokibi, fue el tipo de ransomware más común que X-Force observó por segundo año, y representa el 37 % de los ataques de ransomware, seguido por Ryuk con un 13 %. El mayor control legislativo ha sido probablemente la principal causa de reducción de ataques de ransomware y de IoT botnet en 2021, pero esto no descarta un posible resurgimiento en 2022.

Vulnerabilidades de la cadena de suministro: La seguridad de la cadena de suministro ocupó el primer plano de la atención del gobierno y de los responsables de definir políticas, con órdenes ejecutivas sobre ciberseguridad de la administración Biden y directrices del Departamento de Seguridad Nacional de EE. UU., CISA y el Instituto Nacional de Estándares y Tecnología de multiplicar esfuerzos siguiendo la directriz de zero trust. Estas directrices se centran en las vulnerabilidades y en las relaciones de confianza. El incremento de vulnerabilidades fue el principal vector de ataque inicial en el sector de la fabricación, una industria que lidiaba con los efectos de las presiones y demoras de la cadena de suministro.

Marcas con más suplantaciones de identidad (“phishing”): X-Force ha seguido de cerca la forma en que los ciberdelincuentes han utilizado kits de phising a lo largo de 2021, y nuestra investigación reveló que Microsoft, Apple y Google fueron las tres principales marcas que los delincuentes intentaron imitar. Estas mega marcas se usaron repetidamente en kits de phishing, donde los atacantes probablemente buscaban capitalizar su popularidad y la confianza que depositan en ellas muchos consumidores.

Principales grupos de amenazas: Presunto actor de amenaza del estado-nación iraní ITG17 (MuddyWater), grupo ciberdelincuente ITF23 (Trickbot) y Hive0109 (LemonDuck) son algunos de los grupos de amenazas más activos que los analistas de inteligencia de X-Force han observado durante 2021. Grupos de amenazas de todo el mundo han trabajado en aumentar su destreza y en infiltrarse en más organizaciones. Incorporaban malware con técnicas perfeccionadas de evasión de defensas, que en algunos casos incorporaban en la mensajería de cloud y en plataformas de almacenamiento para sortear los controles de seguridad. Se aprovecharon estas plataformas para ocultar comunicación de control en tráfico de red legítimo. Los actores de amenazas siguieron desarrollando versiones de Linux de malware para infiltrarse en entornos de cloud con mayor facilidad.

Principales estadísticas

21 %

Porcentaje de ataques de ransomware

El ransomware fue el tipo de ataque número uno observado por X-Force durante el año pasado, aunque pasó a ser el 21 % de los ataques, frente al 23 % del año anterior. Los actores del ransomware REvil (también conocido como Sodinokibi) fueron los responsables del 37 % de todos los ataques de ransomware.

17 meses

Tiempo medio de duración de una banda de ransomware antes de renovarse o de disolverse

Las bandas de ransomware que ha estudiado X-Force tuvieron un periodo de vida promedio de 17 meses antes de renovarse o de disolverse. REvil, una de las bandas más exitosas, se disolvió en octubre de 2021, después de 31 meses (dos años y medio).

41 %

Porcentaje de ataques que aprovechan el phishing para el acceso inicial

Las operaciones de phishing constituyeron la principal causa de peligro para la seguridad en 2021; el 41 % de las incidencias que X-Force solventó utilizaban esta técnica para conseguir el acceso inicial.

33 %

Aumento del número de incidencias entre 2020 y 2021 ocasionadas aprovechando vulnerabilidades

Cuatro de cada cinco vulnerabilidades en 2021 fueron nuevas, incluida la vulnerabilidad Log4j CVE-2021-44228, que se convirtió en la número dos a pesar de que solo se divulgó en diciembre.

3X

Efectividad de clic para campañas de phishing que incorporan llamadas telefónicas

La tasa media de clics de las campañas de phishing fue del 17,8 %, pero las campañas de phishing que incorporaban llamadas telefónicas (“vishing” o suplantación por voz) fueron tres veces más efectivas, logrando un 53,2 % de clics de las víctimas.

146 %

Aumento del ransomware de Linux con código nuevo

El porcentaje de ransomware de Linux con código exclusivo (nuevo) ha aumentado año tras año en un 146 %, según Intezer, lo que indica un aumento en el nivel de innovación en el ransomware de Linux.

Número 1

Clasificación del sector industrial en cuanto a ataques

El sector industrial ha sustituido al de servicios financieros como primer objetivo de los ataques en 2021 y ha supuesto el 23,2 % de los ataques que X-Force ha resuelto durante el año pasado. El ransomware ha sido el principal tipo de ataque, con un 23 % de los ataques dirigidos a empresas del sector industrial.

61 %

Porcentaje de incidencias del sector industrial en organizaciones vinculadas a Tecnología Operativa (OT)

Durante el año pasado el sesenta y uno por ciento de las incidencias en organizaciones con entornos OT se produjeron en el sector industrial. Además, el 36 % de los ataques a organizaciones vinculadas a OT fueron de ransomware.

2.204 %

Incremento del reconocimiento sobre OT

Los atacantes aumentaron su capacidad de reconocimiento de dispositivos de OT SCADA Modbus accesibles a través de internet en un 2.204 % entre enero y septiembre de 2021.

74 %

Porcentaje de ataques de IoT procedentes del botnet Mozi

En 2021, los ataques a dispositivos de IoT procedían del botnet Mozi el 74 % de las veces.

26 %

Porcentaje de ataques globales dirigidos a Asia

El veintiséis por ciento de los ataques tenían objetivos en Asia en el punto de mira. Asia fue la zona geográfica más atacada en 2021.

Recomendaciones sobre la mitigación de riesgos

Las amenazas que hemos presentado en este informe pueden parecer preocupantes, ya que se subraya la gravedad y el aumento de amenazas de ransomware, la renovación de las amenazas de BEC y de phishing y diversos ataques de zero-day que los actores de amenazas han aprovechado durante el año pasado. No obstante, nuestro objetivo es que esta información permita a las organizaciones a comprender mejor el panorama actual de amenazas y ayude a generar confianza en las acciones que deben emprender para combatir estas amenazas.

Algunos principios de seguridad que X-Force ha encontrado útiles para combatir las ciberamenazas incluyen el enfoque zero trust, la automatización de la respuesta a incidencias y la mejora de la capacidad de detección y respuesta.

El modelo Zero Trust ayuda a reducir el riesgo de los principales ataques

El modelo zero trust constituye un nuevo enfoque de los problemas de seguridad en el que se supone que ya se ha producido una brecha y tiene como objetivo aumentar la dificultad de que un atacante se mueva por una red. Se basa en entender dónde residen los datos importantes y quién tiene acceso a dichos datos y en crear potentes medidas de verificación en la red para garantizar que solo las personas adecuadas acceden a dichos datos en la forma correcta.

La investigación realizada por X-Force confirma que los principios relacionados con un modelo zero trust —incluir implementación de MFA y el principio de privilegio mínimo— tienen el potencial de reducir la susceptibilidad de las organizaciones de sufrir los principales tipos de ataques identificados en este informe, en especial ransomware y BEC.

Concretamente, la aplicación del principio de privilegio mínimo a los controladores y administradores de dominio puede aumentar las barreras para los actores de ransomware, ya que muchos de estos actores buscan desplegar el ransomware de una red desde un controlador de dominio comprometido. Además, la implementación de MFA aumenta la dificultad a la que se enfrentan los ciberdelincuentes que buscan apoderarse de cuentas de correo electrónico, ya que exige autenticación adicional, además de las credenciales robadas.

Obtenga más información sobre cómo adoptar una solución zero trust →

La automatización de la seguridad mejora la respuesta a incidencias

El equipo de respuesta a incidencias de X-Force aborda cientos de incidencias al año, en diversas áreas geográficas, prestan su ayuda a los analistas internos de respuesta a incidencias y resuelven una amplia gama de tipos de ataques. La velocidad resulta esencial, tanto en identificar y erradicar a los actores de amenazas antes de que puedan desplegar software de ransomware en una red como en resolver problemas de forma rápida y eficiente para crear ancho de banda para la siguiente incidencia. En este entorno que se mueve a un ritmo acelerado, la automatización de la seguridad resulta esencial: asignar a máquinas tareas que llevaría horas realizar a un analista o a un equipo e identificar mecanismos para mejorar los flujos de trabajo.

A mediados de 2021, IBM donó una herramienta de automatización de caza de amenazas a la Open Cybersecurity Alliance con el objetivo de ayudar a los analistas del centro de operaciones de seguridad (SOC) a ejecutar rápidamente investigaciones forenses y abordar las incidencias cibernéticas. Además, el equipo de X-Force IR utiliza IBM Security QRadar SOAR para mejorar sus prestaciones de respuesta a incidencias.

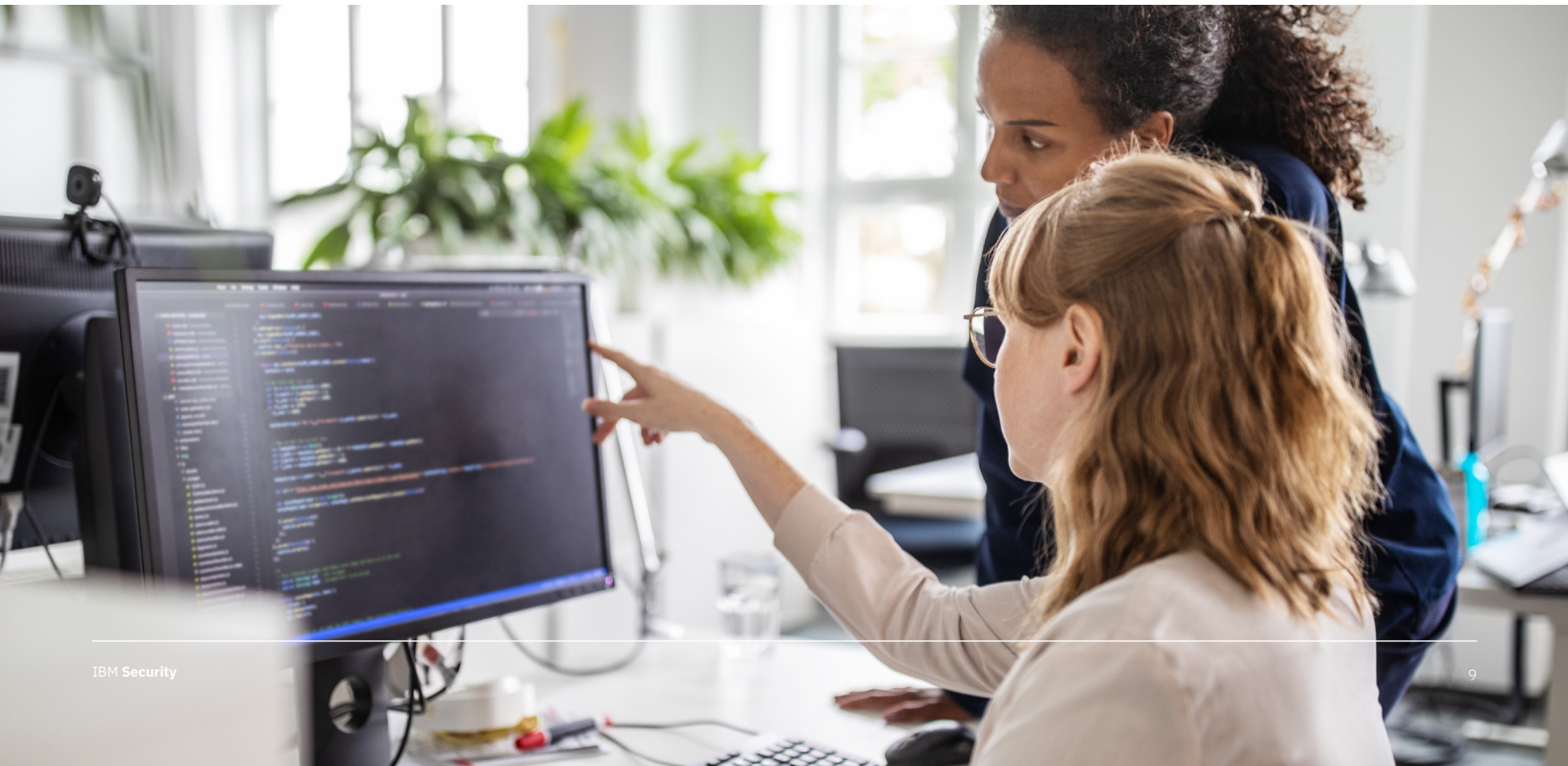
Más información sobre los servicios de respuesta ante incidencias de IBM →

Esta mejora en la detección y respuesta proporciona una ventaja significativa sobre los atacantes

Las tecnologías de detección y respuesta, especialmente cuando se combinan varias soluciones en una solución ampliada de detección y respuesta (XDR), brindan a las organizaciones una ventaja significativa en cuanto a la identificación y erradicación de atacantes desde una red antes de que alcancen la etapa final de su ataque, como el ransomware o el robo de información.

En muchos casos, cuando el equipo de X-Force IR ha desplegado una solución de detección y respuesta de endpoint (EDR) o una solución XDR en la red de un cliente, IR ha obtenido de inmediato información importante que ha ayudado a identificar actividad de atacantes y a abordar rápidamente el problema. Es probable que las tecnologías XDR estén ayudando a gestionar el aumento en el acceso a servidores y otros tipos de ataques que X-Force detecta que indican que se ha identificado a un atacante y se le ha detenido antes de que la operación lograra alcanzar su objetivo.

Más información sobre IBM Security QRadar XDR →



Recomendaciones

Las siguientes recomendaciones incluyen acciones específicas que pueden emprender las organizaciones para proteger mejor sus redes frente a las amenazas que se presentan en este informe.

Desarrollar un plan de respuesta ante ransomware. Cada industria y cada zona geográfica se enfrenta al riesgo de sufrir un ataque de ransomware; la forma en que responde el equipo en el momento crítico puede marcar la diferencia en cuanto a la cantidad de tiempo y de dinero que se pierde en una respuesta.

— Incluya en su plan de respuesta acciones de contención inmediata, defina a qué partes interesadas y reguladores se debe informar, establezca la forma en que la organización guardará datos de forma segura y realizará copias de seguridad y designe una ubicación alternativa desde la que se puedan ejecutar las funciones críticas de la empresa durante el proceso de remediación.

— Incluya en su plan un escenario de pérdida y robo de información como parte del ataque de ransomware; se trata de una táctica común muy utilizada hoy en día que se usa en un alto porcentaje de los ataques de ransomware que X-Force soluciona.

— Utilice simulacros de ransomware y piense si su organización pagaría un rescate y qué factores afectarían al cálculo para tomar esta decisión.

— Asegúrese de que su plan de respuesta ante ransomware incluya una contingencia específica correspondiente a una incidencia relacionada con la nube, ya que podría requerir herramientas y habilidades adicionales.

— Evite que sus datos resulten dañados debido a malware o a ataques de ransomware con soluciones de almacenamiento flash que ayudan a evitar la pérdida de datos, facilitan la continuidad operativa y reducen los costes de la infraestructura.

— En la Guía Definitiva de Ransomware de X_Force encontrará más consejos sobre cómo responder ante un ataque de ransomware. El equipo de respuesta a incidencias de X-Force también puede realizar una evaluación de su organización para analizar el nivel de preparación ante un ransomware y a ayudarle a crear y a probar un plan de respuesta ante incidencias de ransomware. El X-Force Command Center también prepara a las organizaciones para un ataque de ransomware, donde se tiene en cuenta la respuesta tanto empresarial como técnica.

Implementar la autenticación de multifactores en cada punto de acceso remoto a una red. X-Force ha detectado que cada vez más organizaciones implementan MFA con más éxito que nunca. Esto está modificando literalmente el panorama de amenazas, está obligando a los actores de amenazas a encontrar nuevas formas de comprometer las redes además de robar credenciales y está reduciendo la eficacia de las campañas de toma de control de cuentas de correo electrónico.

— MFA puede reducir el riesgo de diversos tipos de ataques, incluidos ransomware, robo de información, BEC y acceso al servidor.

— Además, las tecnologías de gestión de identidad y acceso facilitan año tras año la implementación de MFA, tanto para los equipos encargados de la implementación como para los usuarios finales.

Adoptar una solución por capas para combatir el phishing. Lamentablemente, no existe una sola herramienta o solución que impida todos los ataques de phishing, y los actores de amenazas cada vez perfeccionan más las técnicas anti malware para sortear los controles establecidos. Por lo tanto, recomendamos implementar varias capas de soluciones, lo que aumenta la probabilidad de detectar correos electrónicos de phishing.

— En primer lugar, la formación y prevención efectiva de los usuarios resulta clave y debe incluir ejemplos reales.

— En segundo lugar, emplee una solución de seguridad de software de correo electrónico que permita que la máquina identifique y filtre los mensajes maliciosos.

— En tercer lugar, implemente varias defensas que puedan ayuda a detectar malware o movimiento lateral rápidamente en caso de que se cuele un correo electrónico de phishing, lo que incluye detección de malware basada en comportamiento, detección y respuesta de endpoint (EDR), soluciones de detección y prevención de intrusiones (IDPS) y un sistema de gestión de sucesos y de información de seguridad (SIEM).

Mejorar y ajustar su sistema gestión de vulnerabilidades. La gestión de vulnerabilidades constituye un arte que abarca desde identificar las vulnerabilidades aplicables a la arquitectura de red de su organización hasta planificar cómo resolverlas sin interrumpir ningún punto del proceso.

— Contar con un equipo dedicado a la gestión de vulnerabilidades y asegurarse de que este equipo cuente con los recursos y el apoyo necesarios puede marcar la diferencia a la hora de garantizar que su red esté protegida frente a un posible aprovechamiento de vulnerabilidades.

— Recomendamos dar prioridad a las vulnerabilidades que se mencionan en esta evaluación aplicables a su organización.

— IBM X-Force Exchange también incluye un repositorio de vulnerabilidades y niveles de gravedad asociados que le ayudarán a identificar las vulnerabilidades más preocupantes; X-Force Red puede proporcionar servicios especializados de exploración y de gestión de vulnerabilidades.

Más información del informe completo →

Acerca de IBM Security X-Force

IBM Security X-Force es un equipo dedicado a la detección de amenazas compuesto por hackers, expertos en respuestas, investigadores y analistas. Nuestra cartera incluye productos y servicios ofensivos y defensivos, respaldados por una visión de las amenazas de 360 grados. Con X-Force como socio en seguridad, puede afirmar con confianza que la probabilidad y el impacto de una brecha en los datos son mínimos.

IBM Security X-Force Threat Intelligence combina telemetría de operaciones de seguridad de IBM, investigación, estudios de respuesta a incidentes, datos comerciales y fuentes abiertas para ayudar a los clientes a entender las amenazas emergentes y tomar decisiones fundamentadas de seguridad rápidamente.

Además, el equipo de respuesta ante incidencias de X-Force ofrece servicios de detección, respuesta, remediación y preparación para ayudarle a minimizar el impacto de una brecha en los datos.

X-Force, junto con IBM Security Command Center, forma a todo su equipo, desde analistas hasta C-suite, para que estén listos para hacer frente a las amenazas actuales. X-Force Red, el equipo de hackers de IBM Security, proporciona servicios de seguridad ofensiva, que incluyen pruebas de intrusión, gestión de vulnerabilidades y simulación de adversidades.

Durante todo el año, los investigadores de IBM X-Force también facilitan estudios y análisis de forma continuada en forma de blogs, informes técnicos, webinars y podcasts, en los que ponen de relieve la información que poseemos sobre los responsables de las amenazas, los nuevos software maliciosos y los nuevos métodos de ataque. Asimismo, ofrecemos una extensa colección de soluciones de análisis avanzadas y actualizadas para los clientes con suscripción a través de nuestras soluciones de X-Force Threat Intelligence.

Programe una consulta con uno de nuestros expertos de X-Force

Acerca de IBM Security

IBM Security colabora con usted para ayudarle a proteger su negocio con una cartera avanzada e integrada de productos y servicios de seguridad empresarial que incorporan inteligencia artificial y un enfoque moderno de su estrategia de seguridad que utiliza los principios de zero trust para ayudarle a hacer frente a la incertidumbre. Para ayudarle a gestionar y controlar el riesgo que recae sobre los entornos de cloud híbrido de hoy en día, ajustamos su estrategia de seguridad a su negocio, integramos soluciones diseñadas para proteger a sus usuarios, activos y datos digitales, y desplegamos la tecnología necesaria para gestionar sus recursos de defensa contra las crecientes amenazas.

Nuestra nueva solución abierta y moderna, la plataforma IBM Cloud Pak for Security, se basa en RedHat Open Shift y se adapta a los entornos actuales de multicloud híbrido con un amplio ecosistema de socios. Cloud Pak for Security es una solución de software empresarial en contenedores que le permite gestionar la seguridad de los datos y las aplicaciones mediante la rápida integración de las herramientas de seguridad existentes para generar información más detallada sobre las amenazas en los entornos de cloud híbrido sin necesidad de trasladar los datos, y facilita la orquestación y la automatización de su respuesta de seguridad.

Para obtener más información, consulte www.ibm.com/security o visita el blog de IBM Security Intelligence.

Colaboradores

Camille Singleton
Charles DeBeck
Joshua Chung
Dave McMillen
Scott Craig
Scott Moore
Charlotte Hammond
John Dwyer
Melissa Frydrych
Ole Villadsen
Richard Emerson
Guy-Vincent Jourdan
Vio Onut
Stephanie Carruthers
Adam Laurie
Michelle Alvarez
Salina Wuttke
Georgia Prassinos
John Zorabedian
Mitch Mayne
Limor Kessem
Ian Gallagher
Ari Eitan

IBM España, S.A
Tel.: +34-91-397-6611
Santa Hortensia, 26-28
28002 Madrid
Spain

Producido en los Estados Unidos de América, febrero de 2022