Anuncios

Índice de Inteligencia de Amenazas X-Force: el sector industrial se llevó la peor parte de los ciberataques en 2021, lo que agravó los problemas de las cadenas de suministro

- **La región de Asia-Pacífico es la más atacada actualmente**
- **El promedio de vida de los grupos de 'ransomware' es de 17 meses**
- **El 'vishing' triplica la tasa de clics del 'phishing'**

CAMBRIDGE, Massachusetts, 23 de febrero de 2022-IBM (NYSE: IBM) IBM Security ha publicado hoy su Índice Anual de Inteligencia de Amenazas X-Force, en el que se revela cómo el *ransomware* y la explotación de vulnerabilidades han "encarcelado" a las empresas en 2021, contribuyendo a lastrar aún más las cadenas de suministro globales. No en vano, el sector manufacturero ha sido el que más ataques ha sufrido. En cuanto a las formas de los ciberataques, mientras que el *phishing* ha sido el más común, IBM Security X-Force ha detectado un aumento del 33% en los ataques causados por explotación de vulnerabilidades de software sin parches. De hecho, los ciberdelincuentes utilizaron este tipo de vulnerabilidades más que cualquier otro para llevar a cabo sus acciones, suponiendo el 44% de los ataques de *ransomware* de 2021.

" Los ciberdelincuentes suelen perseguir el dinero. Ahora, con el ransomware, buscan ganar poder. Las empresas deben reconocer que las vulnerabilidades las mantienen en un punto

Esta última edición del Índice Anual de Inteligencia de Amenazas X-Force detalla que, en 2021, los actores de *ransomware* intentaron "fracturar" la columna vertebral de las cadenas de suministro mundiales con acciones contra la industria manufacturera, que fue la más atacada (23%), destronando así a los servicios financieros y al sector de los seguros, que se habían mantenido como los más atacados los últimos años. Al experimentar más ataques de *ransomware* que cualquier otra industria, los atacantes apostaron por el efecto dominó que causaría la interrupción de las empresas manufactureras en sus cadenas de suministro derivadas para presionarlas y conseguir el pago de rescates. Es destacable que un alarmante 47% de los ataques a este sector se debió a vulnerabilidades que las compañías atacadas aún no habían parcheado o no habían podido parchear; esto pone una vez más de manifiesto lo necesario que es que las organizaciones den prioridad a la gestión de sus vulnerabilidades.

> *muerto, ya que los actores de ransomware las utilizan a su favor. Se trata de un reto no binario. La superficie de ataque no hace más que crecer, por lo que, en lugar de operar bajo el supuesto de que cada vulnerabilidad en su entorno ha sido parcheada, las empresas deben operar bajo una suposición de riesgo continuo y mejorar su gestión de vulnerabilidades con una estrategia de Zero Trust.* ”

El Índice de Inteligencia de Amenazas de IBM Security X-Force de 2022 traza las nuevas tendencias y patrones de ataque que IBM Security ha observado y analizado a partir de miles de millones de *datapoints*, que van desde los dispositivos de detección de redes y *endpoints*, a los compromisos de respuesta a incidentes, el seguimiento de kits de *phishing* y otros, incluyendo datos proporcionados por Intezer.

Algunos de los aspectos más destacados del informe de este año son:

- **Las bandas de 'ransomware' desafían los desmantelamientos.** El *ransomware* siguió siendo el principal método de ataque en 2021 y, pese al aumento de desmantelamientos por parte de las autoridades, la actividad de estos grupos no ha dado signos de debilitamiento. Según el informe de 2022, el promedio de vida de un grupo de *ransomware* antes de ser desmantelado o cambiar de marca es de 17 meses.

- **Las vulnerabilidades exponen el mayor "vicio" de las empresas.** X-Force revela que el 50% de los ataques en 2021 sufridos por empresas de Europa, Asia, Oriente Medio y África guardó relación con vulnerabilidades sin parchear, lo que vuelve a incidir en que la falta de atención a estas vulnerabilidades supone el talón de Aquiles de la gran mayoría de compañías.

- **Señales de alerta temprana de la crisis cibernética en la nube.** Los ciberdelincuentes están sentando las bases para atacar los entornos en la nube. Así lo desvela el aumento del 146% en el nuevo código de *ransomware* para Linux y un cambio de orientación hacia Docker que ha detectado el informe X-Factor 2021. Este escenario proyecta que cada vez más actores podrían amenazar los entornos en la nube con fines maliciosos.

"Los ciberdelincuentes suelen perseguir el dinero. Ahora, con el *ransomware*, buscan ganar poder", ha afirmado Charles Henderson, director de IBM X-Force. "Las empresas deben reconocer que las vulnerabilidades las mantienen en un punto muerto, ya que los actores de *ransomware* las utilizan a su favor. Se trata de un reto no binario. La superficie de ataque no hace más que crecer, por lo que, en lugar de operar bajo el supuesto de que cada vulnerabilidad en su entorno ha sido parcheada, las empresas deben operar bajo una suposición de riesgo continuo y mejorar su gestión de vulnerabilidades con una estrategia de Zero Trust".

Por su parte, The Charter Of Trust, una iniciativa global destinada a promover los estándares de seguridad y la colaboración intersectorial en ciberseguridad, ha acogido con satisfacción el informe y ha afirmado: "Casi la mitad de los ataques cibernéticos observados por IBM en Europa han estado causados por la explosión de vulnerabilidades durante el año pasado. Por ello, es más importante que nunca para la industria y la política fortalecer su ecosistema de intercambio de inteligencia sobre amenazas, aumentar la estandarización y compartir conocimientos para evolucionar y mejorar las defensas de las organizaciones contra las nuevas ciberamenazas”.

Las "nueve vidas" de los grupos de ‘ransomware’

En respuesta a la reciente aceleración de los desmantelamientos de *ransomware* por parte de las Fuerzas y Cuerpos de Seguridad, estos grupos pueden estar activando sus propios planes de recuperación y resiliencia. El análisis de X-Force revela que la vida media de un grupo de *ransomware* antes de que sea detenido o cambie de marca es de 17 meses. Pero eso es la media, REvil, quien fuera responsable del 37% de todos los ataques de *ransomware* de 2021, ha estado sobreviviendo durante cuatro años cambiando de marca, lo que sugiere que no sería descartable que resurja de nuevo tras haber sido desmantelado a mediados de 2021 en una operación internacional.

Si bien la acción de las Fuerzas y Cuerpos de Seguridad puede frenar a los ciberdelincuentes, éstos también están sufriendo la presión derivada de los gastos que requieren sus cambios de marca o la reconstrucción de sus infraestructuras.

En cualquier caso, y teniendo en cuenta que las amenazas continúan, a medida que cambia el campo de juego es importante que las compañías y organizaciones modernicen sus infraestructuras para mantener sus datos en un entorno que pueda ayudar a salvaguardarlos, ya sea en sus propias instalaciones o en la nube. Esto puede ayudar a las empresas a gestionar, controlar y proteger sus cargas de trabajo, así como a eliminar la ventaja de los delincuentes en caso de peligro, dificultando el acceso a datos críticos en entornos de nube híbrida.

Las vulnerabilidades se convierten en una crisis existencial para algunos

Esta edición del informe de X-Force destaca el número récord de vulnerabilidades reveladas en 2021, con un aumento del 50% interanual en los Sistemas de Control Industrial. Aunque en la última década se han detectado más de 146.000 vulnerabilidades, hasta estos últimos años las organizaciones no han acelerado su transformación digital y lo han hecho impulsadas, en gran medida, por la pandemia, lo que sugiere que el reto de la gestión de las vulnerabilidades aún no ha alcanzado su punto óptimo.

Al mismo tiempo, cada vez resulta más habitual la explotación de las vulnerabilidades como método de ataque: X-Force ha detectado un aumento del 33% desde el año anterior. Es reseñable que las dos vulnerabilidades más explotadas en 2021 se encontraron en aplicaciones empresariales muy utilizadas, como son Microsoft Exchange y Apache Log4J Library. El desafío de las empresas para gestionar estas vulnerabilidades puede seguir agravándose a medida que se expanden las infraestructuras digitales y las empresas corren el riesgo de verse abrumadas por los requisitos de auditoría y mantenimiento. Esto vuelve a poner de manifiesto la importancia de que las compañías trabajen sobre la hipótesis permanente de amenaza y apliquen una estrategia de Zero Trust para ayudar a proteger su arquitectura.

Los atacantes apuntan a terrenos comunes entre las nubes

Otro elemento que destaca el informe X-Force es que en 2021 hubo un mayor número de ataques contra contenedores como Docker, que es, con mucho, el motor de ejecución de contenedores más dominante, de acuerdo con RedHat. Los atacantes se han dado cuenta de que los contenedores son un terreno común entre las organizaciones, por lo que están duplicando las formas de maximizar su ROI con malware capaz de cruzar plataformas que usan como cabeza de puente para acceder a otros componentes de la infraestructura de sus víctimas.

El informe de 2022 también advierte de que los atacantes invierten de forma continua en malware único, y hasta ahora inédito, para Linux. Los datos proporcionados por Intezer revelan un aumento del 146% en el ransomware de Linux que tiene código nuevo. Mientras los atacantes siguen buscando formas de escalar sus operaciones a través de los entornos de nube, las empresas deben centrarse en ampliar la visibilidad de su infraestructura híbrida. Los entornos de nube híbrida que se basan en la interoperabilidad y los estándares abiertos pueden ayudar a las organizaciones a detectar puntos ciegos y así acelerar y automatizar las respuestas de seguridad.

Otros hallazgos adicionales del informe de 2022 a destacar son:

- Con uno de cada cuatro ataques que IBM observó a nivel mundial en 2021, Asia se convirtió en la región del mundo con más ciberataques en el último año. Los servicios financieros y las industrias manufactureras experimentaron conjuntamente casi el 60% de los ataques en Asia.

- El *phishing* fue la causa más común de los ciberataques en 2021. En las pruebas de penetración de X-Force Red, la tasa de clics en las campañas de *phishing* se triplicó cuando se combinó con llamadas telefónicas (*vishing*).

El informe presenta datos que IBM recopiló a nivel mundial en 2021 para ofrecer información detallada sobre el panorama de amenazas globales e informar a los profesionales de la seguridad sobre las amenazas más relevantes para sus organizaciones. Puede descargar una copia del Índice de Inteligencia de Amenazas de IBM Security X-Force 2022 aquí.

Acerca de IBM Security

IBM gestiona una de las organizaciones de investigación, desarrollo y suministro de seguridad más amplias del mundo, supervisa más de 150.000 millones de eventos de seguridad al día en más de 130 países y ha obtenido más de 10.000 patentes de seguridad en todo el mundo. Para más información, consulte www.ibm.com/security, siga a @IBMSecurity en Twitter o visite el blog IBM Security Intelligence.

For further information: Alfonso Mateos Cadenas. Dpto. Comunicación IBM España, Portugal, Grecia e Israel. alfonso.mateos@ibm.com