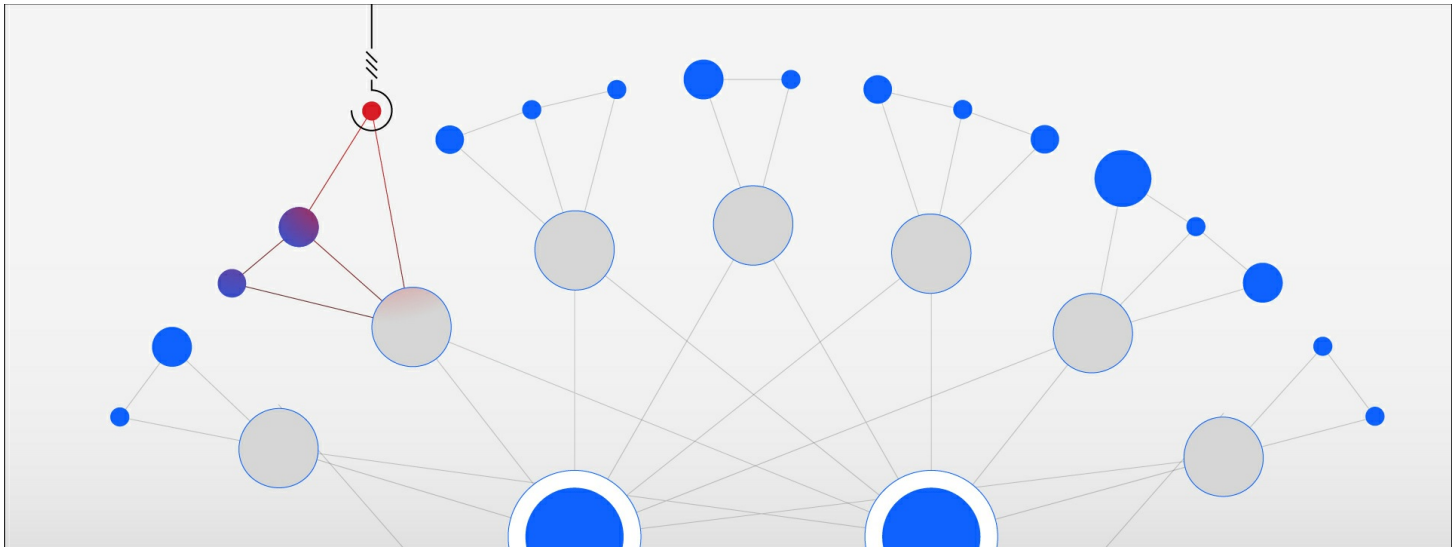
Anuncios

# Los ataques de 'ransomware' persistieron en 2022 a pesar de las mejoras en la detección, según un estudio de IBM

**El sector manufacturero fue el más extorsionado y el que más ataques sufrió**

**Los intentos de secuestro de hilos de correo electrónico aumentaron un 100%**

**El tiempo que tardan los ciberdelincuentes en completar un ataque de ransomware ha pasado en un año de dos meses a cuatro días**



**ARMONK, NY, 22 de febrero de 2023**. IBM Security ha publicado hoy su índice anual de Inteligencia de Amenazas X-Force (X-Force Threat Intelligence Index) entre cuyas conclusiones destaca que, aunque la proporción de incidentes de *ransomware* disminuyó ligeramente de 2021 a 2022 (4 puntos porcentuales), ha aumentado el éxito en la detección y prevención de este tipo de ataques. Pese a ello, los atacantes han continuado innovando en sus capacidades, como muestra el hecho de que hayan pasado de necesitar dos meses de promedio para completar un ataque de *ransomware* a menos de cuatro días.

De acuerdo con el informe, el despliegue de *puertas traseras*, aquellas que permiten el acceso remoto a los sistemas, fue la acción más habitual ejecutada por los atacantes durante 2022. Alrededor del 67% de esos casos de *puertas traseras* estuvieron relacionados con intentos de *ransomware*, frustrados por los equipos de seguridad antes de que se llegara a implementar el ataque. El aumento en los despliegues de *puertas traseras* puede atribuirse, en parte, a su alto valor de mercado. De hecho, X-Force ha observado que los ciberdelincuentes llegan a vender por hasta 10.000 dólares los accesos a *puertas traseras* existentes, mientras que los datos de tarjetas de crédito robadas, se venden hoy día por menos de 10 dólares .

"El giro en la capacidad de detección y respuesta ha permitido a los equipos de seguridad atajar los intentos de ataque con mayor antelación, moderando la progresión del *ransomware* en el corto plazo", ha señalado Charles Henderson, director de IBM Security X-Force. "Pero es solo cuestión de tiempo que el problema que existe hoy con las *puertas traseras* termine siendo la

> *"El giro en la capacidad de detección y respuesta ha permitido a los equipos de seguridad atajar los intentos de ataque con mayor antelación, moderando la progresión del ransomware en el corto plazo. Pero es solo cuestión de tiempo que el problema que existe hoy con las puertas traseras termine siendo la crisis de ransomware de mañana. Los atacantes siempre encuentran nuevas formas de eludir la detección. Ya no basta con una buena capacidad de defensa. Para evitar una lucha interminable con los*

crisis de *ransomware* de mañana. Los atacantes siempre encuentran nuevas formas de eludir la detección. Ya no basta con una buena capacidad de defensa. Para evitar una lucha interminable con los atacantes, las empresas deben impulsar una estrategia de seguridad proactiva y orientada a las amenazas".

> *atacantes, las empresas deben impulsar una estrategia de seguridad proactiva y orientada a las amenazas.* ”

El índice *IBM Security X-Force Threat Intelligence* rastrea tendencias y patrones de ataques nuevos y existentes a partir de millones de datos de dispositivos de red y *endpoints*, datos de respuesta a incidentes y otras fuentes.

Entre las conclusiones del informe de 2023 destacan:

- **La extorsión, el método preferido por los atacantes**. El tipo de golpe más utilizado en 2022 en los ciberataques fue la extorsión, que se llevó a cabo principalmente a partir de ataques de *ransomware* y ataques contra correos electrónicos corporativos. Desde el punto de vista geográfico, Europa fue la región que más sufrió este tipo de golpes, acaparando el 44% de los casos de extorsión detectados, ya que los atacantes buscaron sacar provecho de las tensiones geopolíticas actuales.
- **Los ciberdelincuentes utilizan las conversaciones por correo electrónico como arma** El secuestro de hilos de correos electrónicos experimentó un aumento muy importante en 2022. A lo largo del pasado año, los ciberdelincuentes utilizaron cuentas de correo electrónico comprometidas para responder a conversaciones en curso haciéndose pasar por el interlocutor original. El índice X-Force refleja que los intentos mensuales de ataque con este tipo de táctica aumentaron un 100% en comparación con 2021.
- **Los *exploits* heredados siguen propagándose.** La proporción de *exploits* conocidos que intervinieron en ataques disminuyó 10 puntos porcentuales desde 2018 hasta 2022, en gran medida porque el número de vulnerabilidades alcanzó un nuevo récord en 2022. Aun así, los resultados del índice reflejan que los *exploits* heredados permitieron que infecciones por malware antiguas, como *WannaCry* y *Conficker,* continuaran propagándose.

**La presión de la extorsión se aplica de forma desigual**

A menudo, los ciberdelincuentes actúan contra las industrias, empresas y regiones más vulnerables con complejos modelos de extorsión, que ejercen una alta presión psicológica sobre la víctima para obligarle a pagar. Como ya se ha señalado, de acuerdo con la última edición del índice, el sector manufacturero fue el más extorsionado en 2022 y el que más ataques sufrió por segundo año consecutivo. No en vano, las empresas de este sector son un objetivo atractivo para este tipo de acciones, dada la escasa tolerancia que tienen a los tiempos de inactividad por las características de su industria.

El *ransomware* es un método de extorsión muy conocido, pero los ciberdelincuentes no dejan de explorar nuevos métodos con los que extorsionar a potenciales víctimas. Una de las últimas tácticas detectadas consiste en visibilizar el robo de los datos a las posibles víctimas colaterales. Al incorporar clientes y socios comerciales a esta combinación, los ciberdelincuentes aumentan la presión sobre la empresa atacada ampliando a esas víctimas colaterales la amenaza mediante notificaciones. De esta forma, los atacantes aumentan los costes potenciales y el impacto psicológico de una intrusión, por lo que es fundamental que las empresas tengan un plan de respuesta a incidentes personalizado que también tenga en consideración el impacto que un ataque de estas características puede tener para sus clientes y socios comerciales y evitar así que se conviertan a su vez en víctimas.

**Aumentan los secuestro de hilos de correos electrónicos**

De acuerdo con esta nueva edición del índice, los secuestros de hilos de correos electrónicos aumentaron en 2022, hasta el punto de que el número de intentos mensuales de ataques con este objetivo se duplicó en comparación con 2021. X-Force refleja que, a lo largo de 2022, los atacantes utilizaron esta técnica para distribuir *Emotet, Qakbot* e *IcedID*, un software malicioso que a menudo provoca infecciones de *ransomware*.

Dado que el phishing fue la principal causa de ataques cibernéticos en 2022 y el secuestro de hilos de correos electrónicos aumentó notablemente, resulta evidente que los ciberdelincuentes se aprovechan de la confianza que sus potenciales víctimas tienen en el correo electrónico. En este sentido, las empresas deben concienciar a sus empleados sobre esta táctica para reducir el riesgo de que se conviertan en víctimas.

**Ojo, la 'I+D' de *exploits* va por detrás de las vulnerabilidades**

La relación entre *exploits* conocidos y vulnerabilidades ha ido disminuyendo en los últimos años; en concreto, ha caído en 10 puntos porcentuales desde 2018. Los ciberdelincuentes ya tienen acceso a más de 78.000 *exploits* conocidos, lo que facilita la explotación de vulnerabilidades más antiguas que no han sido parcheadas. Sirva de ejemplo que, pese a que han pasado cinco años desde que se dio a conocer, las vulnerabilidades que provocaron las infecciones de *WannaCry* siguen suponiendo una amenaza significativa: X-Force reportó hace poco un crecimiento del 800% en el tráfico de *ransomware* proveniente de *WannaCry* a partir de los datos de telemetría MSS desde abril de 2022. El hecho de que se continúen utilizando los *exploits* conocidos más antiguos pone en evidencia la necesidad de que las organizaciones revisen sus programas de gestión de vulnerabilidades, incluida la comprensión del potencial campo de ataques y la priorización de parches en función de los riesgos.

La edición 2023 del informe X-Force también destaca incluye otras conclusiones:

- **Los *phishers* "renuncian" a los datos de las tarjetas de crédito.** El número de ciberdelincuentes interesados en atacar la información de tarjetas de crédito mediante técnicas de phishing cayó un 52% en un año, lo que indica que los atacantes priorizan la obtención de datos de identificación personal como nombres, correos electrónicos y domicilios, ya que pueden venderse a un precio más alto en la *deep web* o utilizarse para llevar a cabo otras acciones.
- **Europa fue la segunda región más atacada del mundo en 2022** el 28% de todos los ataques que contabiliza el informe se produjo en Europa, frente al 24% de 2021. Es especialmente reseñable el repunte que experimentó la región en el despliegue de *puertas traseras* a partir de marzo de 2022, justo después de que Rusia invadiera Ucrania. De hecho, este tipo de casos suponen el 21% de los ataques detectados en Europa. El *ransomware*, por su parte, supuso el 11%.
- **Las aplicaciones de cara al público, principal vector de infección:** en las organizaciones europeas, los *exploits* de aplicaciones accesibles desde internet representaron un 32% de los ataques, dando lugar a infecciones de *ransomware* en varios casos. El ataque a cuentas locales válidas se situó, con un 18%, en segundo lugar, seguido de los enlaces de *spear phishing*, con un 14%, lo que supone un notable descenso con respecto al 42% detectado en 2021.
- **Las tecnológicas, entre las marcas más suplantadas:** Microsoft, Google, Yahoo, Facebook y Outlook ocupan el top 5 de empresas más suplantadas en 2022. Este tipo de claves resultan muy valiosas para los atacantes, pues dan acceso a multitud de servicios de estos proveedores. De hecho, el informe Cloud Threat Landscape Report 2022 señala un aumento exponencial de hasta el 200% del número de cuentas en la nube que se anuncian para su venta en la *deep web* respecto a 2021.

El informe presenta datos que IBM recopiló en 2022 a nivel mundial para ofrecer información detallada sobre el panorama global de amenazas e informar a los equipos de ciberseguridad sobre las más relevantes para sus organizaciones. Puede

descargar una copia del *X-Force Threat Intelligence Index 2023* de IBM Security aquí.

**Fuentes adicionales**

- Más información sobre los principales resultados del informe en esteblog de IBM Security Intelligence.

**Acerca de IBM Security**

IBM Security ayuda a proteger a las empresas y gobiernos más grandes del mundo con una cartera integrada de productos y servicios de seguridad, infundidos con capacidades dinámicas de IA y automatización. El portfolio, respaldado por la investigación de renombre mundial IBM Security X-Force®, permite a las organizaciones predecir amenazas, proteger los datos a medida que circulan y responder con velocidad y precisión sin frenar la innovación empresarial. Expertos en seguridad de todo el mundo y miles de organizaciones confían en IBM como su socio para evaluar, elaborar, implementar y gestionar estrategias de transformación de seguridad. IBM opera una de las organizaciones de investigación, desarrollo y suministro de seguridad más amplias del mundo, monitoriza más de 150.000 millones de eventos de seguridad al día en más de 130 países y ha recibido más de 10.000 patentes de seguridad en todo el mundo.

For further information: Alfonso Mateos Cadenas. Dpto. Comunicación. alfonso.mateos@ibm.com

---