IBM X-Force: los ciberdelincuentes utilizaron credenciales robadas y vulnerabilidades de software ya conocidas para atacar a las empresas durante 2019

• En sus estrategias de phishing, los ciberdelincuentes están haciéndose pasar por marcas tecnológicas de confianza para los consumidores El 85% de los archivos expuestos se debió a configuraciones erróneas de sistemas y servidores cloud

• Los troyanos bancarios y los ataques ransomware, cada vez más vinculados

Madrid - 12 feb 2020: IBM (NYSE: IBM) Security ha publicado hoy su informe anual IBM X-Force Threat Intelligence 2020, en el que destaca cómo han evolucionada las técnicas de los ciberdelincuentes tras décadas de haber accedido a decenas de miles de millones de archivos corporativos y personales, y tras explotar cientos de miles de fallos de software. Según el informe, la ciberdelincuencia utilizó credenciales previamente robadas y vulnerabilidades de software ya conocidas para realizar el 60% de los ataques de 2019. Esta estrategia ha permitido que los atacantes tuvieran que hacer un menor uso del engaño para acceder a la información. Los resultados de IBM X-Force Threat Intelligence Index ponen de relieve los factores que han contribuido a esta evolución, incluidos los tres principales vectores de ataque iniciales:

- El phishing tuvo éxito únicamente en menos de un tercio de los incidentes (31%), cuando en 2018 la cifra fue de cerca de la mitad.
- Los ciberdelincuentes explotaron las vulnerabilidades en el 30% de los incidentes observados, en comparación con sólo el 8% de 2018. De hecho, vulnerabilidades más antiguas y de sobras conocidas en Microsoft Office y Windows Server Message Block han seguido teniendo unos niveles de explotación alarmantes en 2019.
- El uso de credenciales previamente robadas también está ganando terreno como punto de entrada predilecto para los ciberdelincuentes, y ya supone un 29% de los casos. Sólo en 2019, más de 8.500 millones de archivos se vieron comprometidos, lo que dio lugar a un aumento del 200% en los datos expuestos reportados en relación al año anterior. Una cifra que se suma al creciente número de credenciales robadas que los ciberdelincuentes ya estaban utilizando.

"El excesivo número de archivos expuestos que vemos hoy en día significa que los ciberdelincuentes tienen en sus manos más herramientas para acceder a nuestras casas y negocios. Los atacantes ya no necesitan invertir tiempo en idear formas sofisticadas de acceder a un negocio; pueden "entrar" en una red y desplegar sus ataques simplemente utilizando recursos conocidos, como por ejemplo iniciando sesión con credenciales robadas", ha comentado Wendi Whitmore, vicepresidenta de IBM X-Force Threat Intelligence. "Utilizar medidas de protección, como la autenticación multifactorial o el inicio de sesión único, es esencial para mejorar la resiliencia de las organizaciones y la protección y privacidad de los datos de los usuarios".

IBM X-Force ha llevado a cabo su análisis basándose en la observación y seguimiento de 70.000 millones de eventos de seguridad en más de 130 países. Además, los datos recopilados y analizados provienen de múltiples fuentes, entre ellas X-Force IRIS, X-Force Red, servicios de seguridad administrados por IBM, o información sobre filtraciones de datos divulgada públicamente. IBM X-Force también ejecuta miles de trampas de spam en todo el mundo, y monitoriza decenas de millones de ataques de spam y de phishing diariamente. Esto le permite analiza miles de millones de páginas web e imágenes para detectar actividades fraudulentas y abusos de marca.

Algunos de los aspectos más destacados del informe también incluyen:

- Sistemas y servidores cloud mal configurados – Las empresas continúan teniendo problemas con la seguridad en la nube. El análisis de IBM ha descubierto que, de los más de 8.500 millones de archivos comprometidos en 2019, siete mil

millones de ellos (cerca del 85%) se debieron a sistemas y servidores cloud mal configurados. Esto supone un cambio significativo con respecto a 2018, donde estos archivos constituían menos de la mitad de las incidencias totales.

- Ransomware bancario – Ha habido un aumento en el uso de TrickBot que, junto con cuatro de los troyanos bancarios más activos en 2019, se ha utilizado para preparar el terreno para ataques de ransomware. De hecho, el código nuevo utilizado por los troyanos bancarios y el ransomware encabezó la lista de ataques.
- Aprovechar la confianza en las empresas tecnológicas para hacer phishing – El top 10 de marcas utilizadas para hacer phishing incluye grandes nombres de tecnología, social media y streaming. Esta situación demuestra que el consumidor confía cada vez más en las marcas de tecnología, en detrimento de las marcas financieras y minoristas. Entre las principales marcas afectadas por estos intentos de phishing se incluyen Google, YouTube o Apple.

Los ataques de ransomware evolucionan

El informe analiza, también, los ataques de ransomware en todo el mundo, dirigidos tanto al sector público como al privado. En 2019 se produjo un importante aumento de la actividad de ransomware: IBM X-Force desplegó su equipo de respuesta a incidentes de ransomware en 13 industrias diferentes en todo el mundo, lo que demuestra la potencia de este tipo de ataques, independientemente de la industria objetivo. Durante el año pasado, cerca de 100 entidades del gobierno de los Estados Unidos se vieron afectadas por ataques de ransomware.

Además, IBM X-Force también detectó ataques significativos contra el comercio minorista, el sector industrial y el sector del transporte. Todos estos sectores cuentan con un gran volumen de datos que pueden ser utilizados para obtener un rendimiento económico, y suelen apoyarse en tecnología no tan actualizada, lo que hace que sean más vulnerables a los ataques. De hecho, en el 80% de los intentos de ataque con ransomware observados, los cibercriminales estaban explotando las vulnerabilidades de Windows Server, la misma táctica utilizada para propagar WannaCry, el ataque que afectó a empresas de 150 países en 2017.

Los ataques de ransomware costaron a las organizaciones más de 7.500 millones de dólares en 2019 por lo que, viendo esta cifra, todo parece apuntar a que este tipo de ataques no van a reducirse durante 2020.

El informe de IBM, en colaboración con Intezer, señala que se ha observado nuevo código de malware en el 45% del código de los troyanos bancarios, y en el 36% del código de ransomware. Esto sugiere que, al crear nuevos códigos, los atacantes continúan centrando sus esfuerzos en evitar su detección. Al mismo tiempo, IBM X-Force también ha observado una fuerte relación entre el ransomware y los troyanos bancarios. Estos últimos están siendo utilizados para abrir la puerta a ataques de ransomware selectivos y de alto riesgo, diversificando la forma en que se despliega el ransomware. Así, por ejemplo, se sospecha que TrickBot, el malware financiero más activo según los datos del informe, despliega Ryuk en las redes de las empresas, mientras que otros troyanos bancarios, como por ejemplo QakBot, GootKit y Dridex, también se están diversificando hacia variantes de ransomware.

Los delincuentes centran sus esfuerzos de phishing en empresas de tecnología y redes sociales

A medida que los consumidores son más conscientes de los correos electrónicos de phishing, las tácticas que utilizan los ciberdelincuentes en este tipo de ataques se están volviendo más y más específicas y dirigidas. En colaboración con Quad9, IBM ha observado que los atacantes están tendiendo cada vez más a hacerse pasar por las principales marcas de confianza de los consumidores, utilizando enlaces tentadores y suplantando a empresas de tecnología, redes sociales y plataformas de streaming. El objetivo es engañar a los usuarios para que hagan clic en enlaces maliciosos como parte de una campaña de phishing. Cerca del 60% de las 10 principales marcas suplantadas eran dominios de Google y YouTube, mientras que

dominios de Apple (15%) y Amazon (12%) también fueron víctimas de intentos de ataque por parte de ciberdelincuentes que buscaban robar datos de los usuarios que pudieran rentabilizar. IBM X-Force indica que estas marcas fueron atacadas principalmente por la cantidad de datos monetizables que poseen.

Facebook, Instagram y Netflix también están en la lista de las diez principales marcas suplantadas, pero con una tasa de uso significativamente menor. Esto puede deberse al hecho de que estos servicios no suelen tener datos directamente monetizables. En estos casos, los atacantes suelen apostar por la reutilización de credenciales para acceder a cuentas con pagos más lucrativos. IBM X-Force sugiere que la reutilización frecuente de las contraseñas es lo que potencialmente convierte a estas marcas en objetivos de los ciberdelincuentes. De hecho, el estudio Future of Identity de IBM reveló que el 41% de los Millenials reutiliza la misma contraseña varias veces, mientras que la Generación Z tiene un promedio de sólo cinco contraseñas, lo que indica una mayor tasa de reutilización. Distinguir dominios falsos puede ser extremadamente difícil, motivo por el cual los delincuentes optan por esta estrategia. Con un conjunto total de casi 10.000 millones de cuentas, las 10 principales marcas suplantadas que aparecen en el informe ofrecen a los atacantes un amplio número de objetivos, lo que aumenta la probabilidad de que un usuario desprevenido pueda hacer clic en un enlace aparentemente inocente, pero fraudulento (Análisis de IBM basado en información pública).

El informe de IBM también incluye las siguientes conclusiones:

- El comercio minorista, uno de los sectores más atacados: En 2019 el comercio minorista se convierte en la segunda industria más atacada, siguiendo de cerca a los servicios financieros, que se mantienen en primer lugar por cuarto año consecutivo. Las ofensivas de Magecart se encuentran entre los ataques más prominentes observados contra el retail, impactando en 80 webs de comercio electrónico en el verano de 2019. Los ciberdelincuentes han centrado sus esfuerzos en información personal de los consumidores, datos de las tarjetas de pago e, incluso, en la valiosa información de los programas de fidelización. Según los datos de IBM, los comercios minoristas también experimentaron una cantidad significativa de ataques ransomware.
- Los ataques en los Sistemas de Control Industrial (ICS) y a la Tecnología de Operaciones (OT), en un máximo histórico – En 2019 los ataques a la OT aumentaron un 2.000%, con más ataques a la infraestructura de los Sistemas de Control Industrial (ICS) y a la Tecnología de Operaciones que en cualquiera de los tres años anteriores. La mayoría de los ataques observados implicaron una combinación de vulnerabilidades conocidas dentro del hardware del SCADA y del ICS, así como password-spraying.
- América del Norte y Asia, las regiones con más ataques – Durante 2019 estas dos regiones experimentaron el mayor número de ataques. Además, también padecieron las mayores pérdidas de datos, con más de 5.000 millones y 2.000 millones de archivos expuestos respectivamente durante el último año.

El informe IBM X-Force Threat Intelligence 2020 presenta los datos que IBM recopiló en 2019 para ofrecer información de valor sobre el panorama de las amenazas de ciberseguridad mundiales, y compartir con los profesionales de la seguridad las amenazas más relevantes para sus organizaciones. Para ver la infografía interactiva con las conclusiones del informe y descargar una copia de IBM X-Force Threat Intelligence 2020, pincha en este enlace.

Acerca de IBM Security

IBM Security ofrece una de las carteras más avanzadas e integradas de productos y servicios de seguridad empresarial. El portfolio, respaldado por la investigación de IBM X-Force®, de renombre mundial, permite a las organizaciones administrar de manera efectiva los riesgos y defenderse contra amenazas emergentes. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo. Supervisa 70.000 millones de eventos de seguridad por día en más de 130 países, y cuenta con más de 10.000 patentes de seguridad otorgadas en todo el mundo. Para obtener

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

Contacto(s)

Patricia Núñez Canal

IBM Comunicación Externa +34 91 3977782 patricia.nunez@es.ibm.com