IBM X-Force: Credenciales robadas y vulnerabilidades se convirtieron en armas contra los negocios en 2019

• Marcas de tecnología de consumo atrapadas en el fuego cruzado de los ataques de phishing

• Servidores en la nube y otros sistemas mal configurados representaron más del 85% de los registros expuestos

CAMBRIDGE, MA. Febrero 11, 2020. – IBM Security lanzó hoy el informe “IBM X-Force Threat Intelligence 2020” (Índice Anual de Inteligencia de Amenazas), que destaca cómo las técnicas de los ciberdelincuentes han evolucionado después de décadas de acceso a decenas de miles de millones de registros corporativos y personales y fallas de software. Según el informe, el 60% de las entradas iniciales en las redes de las víctimas que fueron observadas aprovecharon credenciales previamente robadas o las vulnerabilidades de software conocidas, lo que permitió a los atacantes depender menos del engaño para obtener acceso.

El IBM X-Force Threat Intelligence Index destaca los factores que contribuyen a esta evolución, incluidos los tres principales vectores de ataque iniciales:

- El phishing fue un vector de infección inicial exitoso en menos de un tercio de los incidentes (31%) observados, en comparación con la mitad en 2018.
- El escaneo y la explotación de vulnerabilidades dieron como resultado el 30% de los incidentes observados, en comparación con solo el 8% en 2018. De hecho, las vulnerabilidades más antiguas y conocidas en Microsoft Office y Windows Server Message Block aún encontraban altos índices de explotación en 2019.
- El uso de credenciales previamente robadas también está convirtiéndose en punto de entrada preferido el 29% de las veces observadas. Solo en 2019, el informe señala más de 8,5 mil millones de registros comprometidos, que resultaron en un aumento del 200% en los datos expuestos reportados año tras año, lo que se suma al creciente número de credenciales robadas que los ciberdelincuentes pueden utilizar como material de origen.

"La cantidad de registros expuestos que estamos viendo hoy significa que los ciberdelincuentes están obteniendo más llaves de nuestros hogares y negocios. Los atacantes ya no van a necesitan invertir tiempo para idear formas sofisticadas en un negocio; pueden desplegar sus ataques, simplemente usando entidades conocidas, como realizar el *log in* con credenciales

robadas ", dijo Wendi Whitmore, vicepresidenta de IBM X-Force Threat Intelligence. "Las medidas de protección, como la autenticación multifactor y el inicio de sesión único, son importantes para la ciber resiliencia de las organizaciones y la protección y privacidad de los datos del usuario".

IBM X-Force llevó a cabo su análisis basado en información y observaciones del monitoreo de 70 mil millones de eventos de seguridad por día en más de 130 países. Además, los datos se recopilan y analizan desde múltiples fuentes, incluidos X-Force IRIS, X-Force Red, IBM Managed Security Services y la información de violación de datos divulgada públicamente. IBM X-Force también ejecuta miles de *spam traps* en todo el mundo y monitorea decenas de millones de ataques de *spam* y *phishing* diariamente mientras analiza miles de millones de páginas web e imágenes para detectar cualquier tipo de actividad fraudulenta y abuso de marca.

Algunos de los aspectos más destacados del informe incluyen:

- **Configuración:** El análisis de IBM encontró que de los más de 8,5 mil millones de registros reportados que se violaron en 2019, siete mil millones de ellos, o más del 85%, se debieron a servidores en la nube y otros sistemas mal configurados. Esto representa un cambio radical desde el 2018, cuando los registros constituían menos de la mitad del total de registros.

- **Ransomware en banca:** Algunos de los troyanos bancarios más activos en 2019, por ejemplo, TrickBot, se utilizaron con mayor frecuencia para preparar el escenario para ataques completos de ransomware. De hecho, el nuevo código utilizado por los troyanos bancarios y el ransomware encabezó las listas de ataques en comparación con otras variantes de malware discutidas en el informe.

- **Confianza tecnológica en Phishing:** El informe de IBM X-Force apunta que las marcas de transmisión de contenido, tecnología social y tecnología conforman las "Top 10" falsificadas que los ciber atacantes se están haciendo pasar por intentos de phishing. Este cambio puede demostrar la creciente confianza depositada en los proveedores de tecnología por encima de las marcas minoristas y financieras históricamente confiables. Las principales marcas utilizadas en los esquemas incluyen Google, YouTube y Apple.

Adversarios falsifican a compañías de tecnología y redes sociales en esquemas de phishing

A medida que los consumidores se vuelven más conscientes de los correos electrónicos de phishing, las tácticas de phishing se vuelven más específicas. En colaboración con Quad9, IBM observó una tendencia de allanamiento en las campañas de phishing, en la que los atacantes se

hacen pasar por las marcas de consumo de tecnología más confiables con enlaces tentadores, utilizando tecnología, redes sociales y compañías de transmisión de contenido, para engañar a los usuarios para que hagan clic en enlaces maliciosos en intentos de phishing.

Casi el 60% de las 10 principales marcas falsificadas identificadas eran dominios de Google y YouTube, mientras que los dominios Apple (15%) y Amazon (12%) también fueron falsificados por los atacantes que buscaban robar los datos monetizables de los usuarios. IBM X-Force evalúa que estas marcas se enfocaron principalmente debido a los datos monetizables que poseen.

Facebook, Instagram y Netflix también figuran en la lista de las diez principales marcas falsificadas, pero con una tasa de uso significativamente menor. Esto puede deberse al hecho de que estos servicios no suelen contener datos directamente monetizables. Como los atacantes suelen apostar por la reutilización de credenciales para obtener acceso a cuentas con pagos más lucrativos, IBM X-Force sugiere que la reutilización frecuente de contraseñas es lo que potencialmente convirtió a estas marcas en objetivos. De hecho, el Estudio de IBM Future of Identity encontró que el 41% de los millennials que participaron de la encuesta reutiliza la misma contraseña varias veces, mientras que la Generación Z promedia solo cinco contraseñas, lo que indica una tasa de reutilización más alta.

Discernir dominios falsificados puede ser extremadamente difícil, que es exactamente a lo que apuestan los atacantes. Con casi 10 mil millones de cuentas combinadas, las 10 principales marcas falsificadas que figuran en el informe ofrecen a los atacantes un amplio grupo de objetivos, lo que aumenta la probabilidad de que un usuario desprevenido haga clic en un enlace aparentemente inocente de una marca falsificada.

La industria minorista vuelve a ser el foco

El comercio minorista ha pasado a ser la segunda industria más atacada en el informe del año, muy cerca de la industria de servicios financieros que se mantuvo en primer lugar por el cuarto año consecutivo. Los ataques de Magecart se encuentran entre los ataques más destacados observados contra el comercio minorista, y afectan a 80 sitios de comercio electrónico reportados en el 2019. Los ciberdelincuentes han puesto su mira en los datos personales de los consumidores, los datos de las tarjetas de pago e incluso la valiosa información del programa de lealtad. Los minoristas también experimentaron una alta cantidad de ataques de *ransomware*.

El informe presenta datos recopilados por IBM en 2019 para brindar información detallada sobre el panorama global de amenazas e informar a los profesionales de seguridad sobre las amenazas más relevantes para sus organizaciones. Para descargar una copia del IBM X-Force Threat Intelligence Index 2020, visite: https://ibm.biz/downloadxforcethreatindex

Sobre IBM Security

IBM Security ofrece uno de los portafolios más avanzados e integrados de productos y servicios de seguridad empresarial. Respaldado por la investigación de renombre mundial de IBM X-Force®, las soluciones permiten a las organizaciones gestionar eficazmente los riesgos y defenderse de las amenazas emergentes. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo, monitorea 70 mil millones de eventos de seguridad por día en más de 130 países y se le han otorgado más de 10,000 patentes de seguridad 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.
