

[Anuncios](#)

Google, Dropbox o Adidas, las marcas más suplantadas de 2020, según el nuevo informe de seguridad de IBM

- **Las herramientas imprescindibles para garantizar la colaboración a distancia, como Google, Dropbox o Microsoft, en el top 10 de las marcas más afectadas por suplantación de identidad o spoofing**
- **Los ciberataques contra el sector sanitario, de manufacturas y el energético se duplicaron respecto a 2019**

CAMBRIDGE, Massachusetts, 24 de febrero de 2021 - IBM (NYSE: [IBM](#)) Security ha publicado hoy el Índice de [Inteligencia de Amenazas X-Force 2021](#), en el que se explica cómo han evolucionado los ciberataques en 2020 causados por ciberdelincuentes que han tratado de aprovecharse de los desafíos socioeconómicos, empresariales y políticos sin precedentes provocados por la pandemia COVID-19. En 2020, IBM Security X-Force observó que los ciberdelincuentes dirigieron sus ataques a las empresas centradas en dar una respuesta a la COVID-19, como hospitales, fabricantes de productos médicos y farmacéuticos, así como empresas energéticas presentes en la cadena de suministro de la COVID-19.

Según el nuevo informe, los ciberataques contra el sector sanitario, de manufacturas y el energético se duplicaron con respecto al año anterior. Los ataques se dirigieron a organizaciones que no podían permitirse parar su actividad, debido al riesgo que supondría interrumpir los esfuerzos médicos o las cadenas de suministro. De hecho, la industria manufacturera y la energía fueron los sectores más atacados en 2020, sólo por detrás del sector financiero y de seguros. En este contexto, cabe destacar el aumento de casi el 50% de las vulnerabilidades en los sistemas de control industrial (ICS), de los que dependen en gran medida la industria manufacturera y la energía.

"La pandemia ha redefinido lo que hoy se considera infraestructura crítica, y los ciberdelincuentes han tomado nota. Muchas organizaciones se han tenido que enfrentar a esta amenaza por primera vez, ya sea para apoyar la investigación de la COVID-19, mantener las cadenas de suministro de vacunas y alimentos o producir equipos de protección personal", señala Nick Rossmann, jefe global de Inteligencia de Amenazas, IBM Security X-Force. "La elección de las víctimas cambió a medida que avanzaba la pandemia, lo que indica una vez más la adaptabilidad, el ingenio y la persistencia de los ciberatacantes".

El Índice de Inteligencia de Amenazas de X-Force se basa en el análisis derivado de supervisar más de 150.000 millones de eventos de seguridad al día en más de 130 países. Además, los datos se recopilan y analizan a partir de múltiples fuentes dentro de IBM, incluyendo IBM Security X-Force Threat Intelligence and Incident Response, X-Force Red, IBM Managed Security Services, y los datos proporcionados por [Quad9](#) e [Intezer](#), que han contribuido al informe de 2021.

Algunos de los aspectos más destacados del informe son:

- **Los ciberdelincuentes aceleran el uso de malware para Linux** : con un aumento del 40% en las

“ La pandemia ha redefinido lo que hoy se considera infraestructura crítica, y los ciberdelincuentes han tomado nota. Muchas organizaciones se han tenido que enfrentar a esta amenaza por primera vez ”

familias de malware relacionadas con Linux en el último año, según Intezer, y un aumento del 500% en el malware Go-written en los primeros seis meses de 2020, por lo que parece que los ciberdelincuentes están acelerando una migración al malware de Linux que puede ejecutarse fácilmente en varias plataformas, incluidos los entornos Cloud.

- **La pandemia impulsa la suplantación de marcas reconocidas** : en medio de un año en el que ha predominado el distanciamiento social y el trabajo a distancia, las marcas que han ofrecido herramientas de colaboración como Google, Dropbox y Microsoft, o las marcas de comercio online como Amazon y PayPal se situaron en el top 10 de las marcas más suplantadas en 2020. YouTube y Facebook, a las que los consumidores recurrieron más para [informarse](#) el año pasado, también encabezaron la lista. Sorprendentemente, Adidas debutó como la séptima marca más suplantada en 2020, probablemente a raíz de la demanda sus modelos de zapatillas Yeezy y Superstar.
- **Los ataques ransomware se aprovechan de un modelo de negocio rentable** : el ransomware fue la causa de casi uno de cada cuatro ataques a los que X-Force dio respuesta en 2020, con ataques que evolucionan para incluir tácticas de doble extorsión. Utilizando este modelo, Sodinokibi -el grupo de ransomware más popular en 2020- tuvo un año muy rentable. El grupo hizo una estimación conservadora de más de 123 millones de dólares en el último año, esto quiere decir que aproximadamente dos tercios de sus víctimas pagaron un rescate, según el informe.

Ciberdelincuentes que se hacen pasar por marcas famosas

El informe de 2021 destaca que los ciberdelincuentes optaron por suplantar con mayor frecuencia las marcas en las que confían los consumidores. En este sentido, Adidas, considerada una de las marcas más influyentes del mundo, ha sido muy atractiva para los ciberdelincuentes, que han intentado aprovecharse de los consumidores para llevar, a quienes buscaban las populares zapatillas, a sitios web maliciosos diseñados para aparentar páginas de compra legítimas. Una vez que el usuario visitaba estos dominios de apariencia legítima, los ciberdelincuentes intentaban llevar a cabo estafas de pago online, robar la información bancaria de los usuarios, recopilar sus contraseñas o infectar los dispositivos de las víctimas con malware.

El informe indica que la mayor parte de la suplantación de identidad de Adidas está asociada a la demanda de los modelos de zapatillas Yeezy y Superstar. Solo la línea Yeezy recaudó, según los informes, 1.300 millones de dólares en 2019 y fue uno de los modelos más vendidos. Es probable que, con la gran expectativa que despertó el lanzamiento de las zapatillas a principios de 2020, los atacantes aprovecharan la demanda para obtener su propio beneficio.

Acerca de IBM Security

IBM Security ofrece una de las carteras más avanzadas e integradas de productos y servicios de seguridad empresarial. La cartera, apoyada por la investigación de renombre mundial de IBM Security X-Force, permite a las organizaciones gestionar eficazmente el riesgo y defenderse de las amenazas emergentes. IBM cuenta con 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: Patricia Núñez IBM Comunicación patricia.nunez@es.ibm.com
