Comunicados

Informe de Seguridad IBM: Ataques a industrias que apoyan la respuesta a COVID-19 se duplican

· Grupos de ransomware acumulan millones; pronóstico nublado con 40% de aumento en malware de código abierto en 2020; las herramientas “imprescindibles” de distanciamiento social encabezan la lista de las marcas más falsificadas.



CAMBRIDGE, Mass., 24 de febrero de 2021 – IBM (NYSE: IBM) Security publicó hoy su informe 2021 X-Force Threat Intelligence Index, que destaca cómo evolucionaron los ciberataques en 2020 a medida que los agentes de amenazas cibernéticas buscaban beneficiarse de los desafíos socioeconómicos, comerciales y políticos sin precedentes provocados por la pandemia de COVID-19. En 2020, IBM Security X-Force observó que los atacantes se centraron en organizaciones vitales para los esfuerzos globales de respuesta a COVID-19, como hospitales, fabricantes de insumos médicos y farmacéuticos, así como compañías de energía que alimentan la cadena de suministro de COVID-19.

Según el nuevo informe, los ataques cibernéticos a organizaciones de atención médica, fabricación y energía se duplicaron con respecto al año anterior, ya que los agentes de amenazas cibernéticas hicieron blanco en organizaciones que no podían permitirse el tiempo de inactividad debido a los riesgos de interrumpir los esfuerzos médicos o cadenas de suministro críticas. De hecho, la industria manufacturera y la energía fueron los sectores más atacados en 2020, solo superados por el sector financiero y de seguros. A esto contribuyeron los atacantes que se aprovecharon del aumento de casi un 50% en las vulnerabilidades en los sistemas de control industrial (ICS), de los que tanto la fabricación como la energía dependen en gran medida.

“En esencia la pandemia ha reformulado lo que hoy se considera infraestructura crítica, y los atacantes tomaron nota. Muchas organizaciones debieron pasar a la línea de frente en los esfuerzos de respuesta por primera vez, ya sea para apoyar la investigación de COVID-19, defender las cadenas de suministro de vacunas y alimentos o producir equipo de protección personal”, comentó Nick Rossmann, Líder de Inteligencia de Amenazas Globales en IBM Security X-Force. “La victimología de los atacantes cambió conforme se fueron sucediendo los hechos en la línea de tiempo de COVID-19, lo que señala, una vez más, la adaptabilidad, el ingenio y la persistencia de los adversarios del ciberespacio”.

El índice de inteligencia de amenazas X-Force se basa en conocimientos y observaciones obtenidos gracias al monitoreo de más de 150 mil millones de eventos de seguridad por día en más de 130 países. Además, los datos se recopilan y analizan de múltiples fuentes dentro de IBM, incluyendo las áreas IBM Security X-Force Threat Intelligence and Incident Response, X-Force Red, IBM Managed Security Services, y los datos proporcionados por Quad9 e Intezer, los cuales contribuyeron al informe 2021.

Algunos de los aspectos más destacados del informe incluyen:

- **Los ciberdelincuentes aceleran el uso de malware Linux:** Con un aumento del 40% en las familias de malware relacionado con Linux en el último año, según Intezer, y un aumento del 500% en el malware escrito en Go en los primeros seis meses de 2020, los atacantes están acelerando una migración a malware de Linux, que se puede ejecutar más fácilmente en varias plataformas, incluidos los entornos de nube.
- **La pandemia impulsa la falsificación de marcas líderes:** En un año de distanciamiento social y trabajo remoto, las marcas que ofrecen herramientas de colaboración como Google, Dropbox y Microsoft, o las de compras en línea como Amazon y PayPal, figuraron entre las 10 principales marcas falsificadas en 2020. YouTube y Facebook, las fuentes a las que más recurrieron los consumidores para la síntesis de noticias el año pasado, también encabezan la lista. Sorprendentemente, Adidas hizo su debut como la séptima marca más imitada en 2020, probablemente como consecuencia de la demanda de las líneas de zapatillas Yeezy y Superstar.
- **Grupos de ransomware aprovechan un modelo de negocio rentable:** El ransomware fue la causa de casi uno de cada cuatro ataques a los que respondió X-Force en 2020, que evidenciaron una evolución agresiva para incluir tácticas de doble extorsión. Con este modelo, X-Force evalúa que Sodinokibi -el grupo de ransomware más observado en 2020- tuvo un año muy rentable. X-Force estima que el grupo ganó, utilizando una estimación conservadora, más de 123 millones de dólares el año pasado y aproximadamente dos tercios de sus víctimas pagaron un rescate, según el informe.

La inversión en malware de código abierto amenaza los entornos de nube

En medio de la pandemia de COVID-19, muchas empresas buscaron acelerar su adopción de la nube. “De hecho, una encuestareciente de Gartner descubrió que casi el 70% de las organizaciones que utilizan servicios en la nube planean aumentar su gasto en la nube a raíz de la disrupción causada por COVID-19”.[1] Pero considerando que Linux actualmente impulsa el 90% de las cargas de trabajo en la nube y que el informe X-Force detalla un aumento del 500% en las familias de malware relacionado con Linux en la última década, los entornos en la nube pueden convertirse en un vector de ataque importante para los agentes de amenazas cibernéticas.

Con el aumento del malware de código abierto, IBM evalúa que los atacantes pueden estar buscando formas de mejorar sus márgenes de ganancia, posiblemente reduciendo costos, aumentando la efectividad y creando oportunidades para escalar ataques más rentables. El informe destaca varios grupos de amenazas como APT28, APT29 y Carbanak que recurren al malware de código abierto, lo que indica que esta tendencia será un acelerador para más ataques a la nube el próximo año.

El informe también sugiere que los atacantes están explotando la potencia de procesamiento expandible que brindan los entornos de nube, transfiriendo altos cargos por uso de la nube a las organizaciones víctimas, ya que Intezer observó más del 13% de código nuevo, previamente no observado, en el malware de criptominería

de Linux en 2020.

Con la mirada de los atacantes puesta en las nubes, X-Force recomienda que las organizaciones consideren un enfoque de confianza cero para su estrategia de seguridad. Las empresas también deben hacer de la computación confidencial un componente central de su infraestructura de seguridad para proteger sus datos más confidenciales: al cifrar los datos en uso, las organizaciones pueden ayudar a reducir el riesgo de explotación por parte de un agente malintencionado, incluso si pudiera acceder a sus ambientes confidenciales.

Cibercriminales se hacen pasar por marcas famosas

El informe de 2021 destaca que los ciberdelincuentes optaron por hacerse pasar con mayor frecuencia como marcas en las que los consumidores confían. Considerada una de las marcas más influyentes del mundo, Adidas les pareció atractiva a los ciberdelincuentes que intentaron explotar la demanda de consumidores en busca de zapatillas codiciadas, llevándolos a webs maliciosas que simulaban ser sitios legítimos. Una vez que un usuario visitaba estos dominios que parecían legítimos, los ciberdelincuentes intentaban realizar estafas de pago en línea, robar información financiera de los usuarios, recolectar credenciales de usuario o infectar los dispositivos de las víctimas con malware.

El informe indica que la mayoría de las falsificaciones de Adidas están asociadas con las líneas de zapatillas Yeezy y Superstar. La línea Yeezy según estimaciones recaudó USD 1.3 mil millones en 2019 y fue una de las zapatillas más vendidas por el gigante de la fabricación de ropa deportiva. Es probable que, debido a la expectativa generada por el lanzamiento de zapatillas a principios de 2020, los atacantes aprovecharan la demanda de esta rentable marca para obtener sus propias ganancias.

Ransomware, en el podio de los ataques de 2020

Según el informe, en 2020 el mundo experimentó más ataques de ransomware en comparación con 2019. Casi el 60% de los ataques de ransomware a los que X-Force respondió utilizaron una estrategia de doble extorsión en la cual los atacantes cifraban, robaban y luego amenazaban con filtrar datos, si no se pagaba el rescate. De hecho, en 2020, el 36% de las filtraciones de datos que X-Force rastreó provinieron de ataques de ransomware que también implicaban un supuesto robo de datos, lo que sugiere que las filtraciones de datos y los ataques de ransomware están comenzando a colisionar.

El grupo de ransomware más activo reportado en 2020 fue Sodinokibi (también conocido como REvil), responsable del 22% de todos los incidentes de ransomware que X-Force observó. X-Force estima que Sodinokibi robó aproximadamente 21,6 terabytes de datos de sus víctimas, casi dos tercios de las víctimas pagaron un rescate y en aproximadamente el 43% de los casos se filtraron datos. Según las estimaciones de X-Force, se calcula que ese grupo habría ganado más de USD 123 millones el año pasado.

Al igual que Sodinokibi, el informe descubrió que los grupos de ransomware más exitosos en 2020 se dedicaron también a robar y filtrar datos, así como en crear cárteles de ransomware como servicio y subcontratar aspectos clave de sus operaciones a ciberdelincuentes que se especializan en diferentes aspectos de un ataque. En respuesta a estos ataques de ransomware más agresivos, X-Force recomienda que las organizaciones limiten el acceso a los datos confidenciales y protejan las cuentas clave con administración de acceso

privilegiado (PAM) y administración de identidades y accesos (IAM).

Otros hallazgos del informe:

- **Las vulnerabilidades superan al phishing como vector de infección más común:** El informe de 2021 revela que la forma más exitosa en que se accedió a los entornos de víctimas el año pasado fue escanear y explotar vulnerabilidades (35%), superando el phishing (31%), por primera vez en años.
- **Europa se llevó la peor parte de los ataques de 2020:** Representando el 31% de los ataques a los que X-Force respondió en 2020, según el informe, Europa fue la región que tuvo más ataques, y el ransomware fue en el principal culpable. Además, Europa experimentó más ataques de amenazas internas que cualquier otra región, con el doble de ataques que América del Norte y Asia juntos.

El informe presenta datos que IBM recopiló en 2020 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 X-Force Threat Intelligence Index 2021, visite: https://www.ibm.biz/threatindex2021

Acerca de IBM Security
IBM Security ofrece una de las carteras más avanzadas e integradas de productos y servicios de seguridad empresarial. La cartera, respaldada por la investigación de IBM Security X-Force de renombre mundial, permite a las organizaciones gestionar el riesgo de forma eficaz y defenderse de las amenazas emergentes. IBM opera una de las organizaciones de investigación, desarrollo y entrega de seguridad más amplias del mundo, monitorea más de 150 mil millones de eventos de seguridad por 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 @IBMSecurity en Twitter o visite IBM Security Intelligence blog.

---

[1] Comunicado de prensa de Gartner, *Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021*, 17 de noviembre de 2020